

# Counting and effective rigidity in algebra and geometry

Benjamin Linowitz<sup>1</sup> · D. B. McReynolds<sup>2</sup> ·  
Paul Pollack<sup>3</sup> · Lola Thompson<sup>1</sup>

Received: 2 August 2014 / Accepted: 22 February 2018 / Published online: 15 March 2018  
© Springer-Verlag GmbH Germany, part of Springer Nature 2018

**Abstract** The purpose of this article is to produce effective versions of some rigidity results in algebra and geometry. On the geometric side, we focus on the spectrum of primitive geodesic lengths (resp., complex lengths) for arithmetic hyperbolic 2-manifolds (resp., 3-manifolds). By work of Reid, this spectrum determines the commensurability class of the 2-manifold (resp., 3-manifold). We establish effective versions of these rigidity results by ensuring that, for two incommensurable arithmetic manifolds of bounded volume, the length sets (resp., the complex length sets) must disagree for a length that can be explicitly bounded as a function of volume. We also prove an effective version of a similar rigidity result established by the second author with Reid on a surface analog of the length spectrum for hyperbolic 3-manifolds. These effective results have corresponding algebraic analogs involving maximal subfields and quaternion

---

✉ Benjamin Linowitz  
benjamin.linowitz@oberlin.edu

D. B. McReynolds  
dmcreyno@purdue.edu

Paul Pollack  
pollack@uga.edu

Lola Thompson  
lola.thompson@oberlin.edu

<sup>1</sup> Department of Mathematics, Oberlin College, Oberlin, OH 44074, USA

<sup>2</sup> Department of Mathematics, Purdue University, West Lafayette, IN 47907, USA

<sup>3</sup> Department of Mathematics, University of Georgia, Athens, GA 30602, USA

subalgebras of quaternion algebras. To prove these effective rigidity results, we establish results on the asymptotic behavior of certain algebraic and geometric counting functions which are of independent interest.

## 1 Introduction

### 1.1 Inverse problems

#### 1.1.1 Algebraic problems

Given a degree  $d$  central division algebra  $D$  over a field  $k$ , the set of isomorphism classes of maximal subfields  $\text{MF}(D)$  of  $D$  is a basic and well studied invariant of  $D$ .

**Question 1** *Do there exist non-isomorphic, central division algebras  $D_1, D_2/k$  with  $\text{MF}(D_1) = \text{MF}(D_2)$ ?*

Restricting to the class of number fields  $k$ , by a well-known consequence of class field theory, when  $D/k$  is a quaternion algebra,  $\text{MF}(D) = \text{MF}(D')$  if and only if  $D \cong D'$  as  $k$ -algebras. Unfortunately, for most higher degree division algebras, we have  $\text{MF}(D) = \text{MF}(D^{\text{op}})$  and  $D \not\cong D^{\text{op}}$  where  $D^{\text{op}}$  is the opposite algebra for  $D$ . For a fixed algebra  $D/k$ , the number of isomorphism classes of algebras  $D'/k$  with  $\text{MF}(D) = \text{MF}(D')$  is the genus of  $D$  and is finite in this setting; see [14, 30, 60] for some recent work on genus of  $D/k$  for general fields  $k$ .

The Brauer group  $\text{Br}(k)$  of a field  $k$  is the set of Morita equivalence classes  $[A]$  of central, simple  $k$ -algebras. The group operation is given by tensor product  $\otimes_k$  with inverses given by  $[A^{\text{op}}]$ . Each class  $[A]$  has a unique central division algebra  $D_A$ . Given a finite extension  $L/k$ , we have a homomorphism  $\text{Res}_{L/k} : \text{Br}(k) \rightarrow \text{Br}(L)$  defined by  $\text{Res}_{L/k}([A_0]) = [A_0 \otimes_k L]$ . For a class  $[A] \in \text{Br}(L)$ , the set  $(\text{Res}_{L/k})^{-1}([A])$  is the set of Morita equivalence classes  $[A_0]$  in  $\text{Br}(k)$  such that  $[A] = [A_0 \otimes_k L]$ . Fix a finite extension  $L_1/k$  and algebra  $A/L_1$ .

**Question 2** *Does there exist a finite extension  $L_2/k$  and an algebra  $A'/L_2$  with  $(\text{Res}_{L_1/k})^{-1}(A) = (\text{Res}_{L_2/k})^{-1}(A')$ ?*

In this generality, we cannot hope to conclude that  $L_1 \cong L_2$  and  $A \cong A'$  (see [58]). However, when  $L_1, L_2/k$  are quadratic extensions and  $A$  is a quaternion algebra, we have  $L_1 \cong L_2$  provided  $(\text{Res}_{L_1/k})^{-1}(A)$  is non-empty.

#### 1.1.2 Geometric problems

Given a closed, negatively curved, Riemannian manifold  $M$ , we have an analytic invariant given by the eigenvalue spectrum  $\mathcal{E}(M)$  of the Laplace–Beltrami

operator acting on  $L^2(M)$ . Similarly, we have a geometric invariant given by the primitive geodesic length spectrum  $\mathcal{L}_p(M)$  of lengths  $\ell$  of primitive, closed geodesics. Both geometric invariants of  $M$  are multi-sets of the form

$$\mathcal{E}(M), \mathcal{L}_p(M) = \{(\lambda_j, m_{\lambda_j})\}, \{(\ell_j, m_{\ell_j})\} \subset \mathbf{R}^{\geq 0} \times \mathbf{N}.$$

The integers  $m_{\lambda_j}, m_{\ell_j}$  are called the multiplicities and give the dimension of the associated  $\lambda_j$ -eigenspace or the number of distinct occurrences of the primitive length  $\ell_j$ , respectively. Forgetting the multiplicities, the set of primitive lengths will be called the length set. Two consequences of the manifold being negatively curved are that every free homotopy class of closed loops contains a unique geodesic representative and the length spectrum is discrete; the eigenvalue spectrum is always discrete when  $M$  is closed. Discreteness here means that the sets without multiplicity  $\{\lambda_j\}, \{\ell_j\}$  are discrete and the multiplicities  $m_{\lambda_j}, m_{\ell_j}$  are finite. These spectra are closely related (see [29]). When  $M$  is hyperbolic 2-manifold, these spectra determine one another by Selberg's trace formula (see [12, Chapter 9, Section 5]). When  $M$  is a hyperbolic 3-manifold, each closed geodesic can be assigned a complex length  $\ell = \ell_0 + \theta i$  where  $\theta$  is the angle of rotation and  $\ell_0$  is the length of the geodesic. In this case, we have the complex length spectrum  $\mathcal{L}_c(M)$  and associated complex length set, and the spectra  $\mathcal{E}(M), \mathcal{L}_c(M)$  determine one another by Selberg's trace formula.

**Question 3** *Do there exist non-isometric Riemannian manifolds  $M_1, M_2$  such that  $\mathcal{L}_p(M_1) = \mathcal{L}_p(M_2)$  (resp.,  $\mathcal{L}_c(M_1) = \mathcal{L}_c(M_2)$  or  $\mathcal{E}(M_1) = \mathcal{E}(M_2)$ )?*

Restricting to the class of closed hyperbolic  $n$ -manifolds, starting with the constructions of Vignéras [80], Sunada [76], many papers have constructed arbitrarily large finite families pairwise non-isometric hyperbolic  $n$ -manifolds with identical eigenvalue and (complex) length spectra for all  $n \geq 2$ ; such manifolds are said to be isospectral or (complex) length isospectral. By construction, the pairs produced by Vignéras, Sunada are commensurable; all presently known pairs are commensurable. It is not known if such pairs must be commensurable in any dimension  $n \geq 2$ . For arithmetic hyperbolic 2- or 3-manifolds, they must be. Reid [72] proved that hyperbolic 2-manifolds with identical length spectra are commensurable provided one of the manifolds is arithmetic. Using Selberg's trace formula, Reid also obtained an identical result for eigenvalue spectra. As arithmeticity is a commensurability invariant, the other manifold is also arithmetic. Reid also established this result for arithmetic hyperbolic 3-manifolds with the length spectrum replaced with the complex length spectrum. Chinburg–Hamilton–Long–Reid [18] extended Reid's result on length spectra for arithmetic hyperbolic 2-manifolds to arithmetic hyperbolic 3-manifolds. Prasad–Rapinchuk [69] also extended [72] for many classes of arithmetic, locally symmetric manifolds. Before [69], it was

known that [72] could not be extended to general locally symmetric manifolds as Lubotzky–Samuels–Vishne [50] constructed arbitrarily large finite families of pairwise incommensurable, isospectral arithmetic, compact, locally symmetric manifolds with real rank  $n$  for all  $n$  using a method similar to Vignéras. For a fixed manifold, the number of commensurability classes is always finite by [69] but can be arbitrarily large by [50]. This finiteness is the geometric analog of the finiteness of genera for division algebras over number fields where genera are also arbitrarily large.

## 1.2 Main results: effective rigidity

We refer the reader to the notation list found at the beginning of Sect. 2 for any undefined symbols or terms.

### 1.2.1 Geodesics

Our first result is an effective version of Reid [72].

**Theorem 1.1** *Let  $M_1, M_2$  be compact arithmetic hyperbolic 2-manifolds (resp., 3-manifolds) with volume less than  $V$ . There exist absolute effectively computable constants  $c_1, c_2$  (resp.,  $c_3$ ) such that if the length sets (resp., complex length) of  $M_1$  and  $M_2$  agree for all lengths less than  $c_1 e^{c_2 \log(V)} V^{1/30}$  (resp.,  $c_3 e^{(\log(V))^{1/30}}$ ), then  $M_1$  and  $M_2$  are commensurable.*

Millichap [61, 62] constructed roughly  $(2n)!$  incommensurable hyperbolic 3-manifolds that have the same first  $2n + 1$  (complex) geodesic lengths. Moreover, the manifolds all have the same volume and the volume of these manifolds grows linearly in  $n$ . His examples are non-arithmetic and his methods are geometric/topological. Neither of these constructions produce lower bounds near the upper bound we provide in Theorem 1.1. Since the completion of this paper, Futer–Millichap [28] and [46] have produced additional examples of non-arithmetic and arithmetic hyperbolic 2- and 3-manifolds that share the same geodesic lengths for the first  $n$  lengths or any finite subset of lengths. Additionally, both constructions give control on the volumes of the examples.

We now sketch the proof of Theorem 1.1 in the case that  $M_1, M_2$  are hyperbolic 3-manifolds with  $\pi_1(M_j) = \Gamma_j$  and volumes bounded above by  $V$ . This proof appears in Sect. 5.4 and makes use of a wide variety of effective results in algebraic number theory. For simplicity, we assume that  $M_1, M_2$  are derived from quaternion algebras. To prove Theorem 1.1, it suffices to show that the invariant trace fields and invariant quaternion algebras of  $M_1, M_2$  are isomorphic (see for instance [54, Chapter 8.4]). That the trace fields are isomorphic is relatively straightforward. We show (in Proposition 5.2) that there

exist hyperbolic  $\gamma_1 \in \Gamma_1$ ,  $\gamma_2 \in \Gamma_2$ , all of whose powers have non-real eigenvalues and whose associated geodesics have the same length. It follows that  $\text{tr}(\gamma_1) = \pm \text{tr}(\gamma_2)$  and hence  $\gamma_1, \gamma_2$  generate the same extension  $k$  of  $\mathbf{Q}$ . By [18, Lemma 2.3] this extension  $k$  is isomorphic to the trace fields of both  $M_1, M_2$ .

That  $M_1, M_2$  have isomorphic quaternion algebras  $B_1, B_2$  is more nuanced. To prove that  $B_1, B_2$  are isomorphic it suffices to show that  $\text{MF}(B) = \text{MF}(B')$ . We prove an effective version of this result in Theorem 1.3 by proving that if two quaternion algebras  $B_1, B_2/k$  with  $|\text{disc}(B_1)|, |\text{disc}(B_2)| < x$  admit embeddings of precisely the same quadratic extensions of  $L/k$  with  $|\Delta_{L/k}|$  less than some explicit function  $f(x)$  (which may involve constants depending on  $k$ ), then  $B_1, B_2$  are isomorphic. In order to use Theorem 1.3 with quaternion algebras  $B_1, B_2$  for  $M_1, M_2$ , we first show (in Lemma 4.1) that  $|\text{disc}(B_1)|, |\text{disc}(B_2)|$  are bounded above by an explicit function  $g(V)$ . Setting  $x = g(V)$ , let  $L/k$  be a quadratic extension which embeds into  $B_1$  and has  $|\Delta_{L/k}|$  less than  $f(g(V))$ . Proposition 5.5 shows that there exists  $u_1 \in B_1$  with  $L = k(u_1)$  that has image  $\gamma_1 \in \Gamma_1$  that is associated to a geodesic in  $M_1$  of length less than  $c_3 e^{(\log(V)) \log(V)}$  for some constant  $c_3$ . By hypothesis there exists  $\gamma_2 \in \Gamma_2$  associated to a geodesic with the same complex length as  $\gamma_1$ . The preimage  $u_2 \in B_2$  of  $\gamma_2$  generates a quadratic extension  $k(u_2)/k$  which is isomorphic to  $L$ . Interchanging the roles of  $M_1, M_2$  and applying Theorem 1.3, we conclude that  $B_1, B_2$  are isomorphic.

### 1.2.2 *Totally geodesic surfaces*

For a finite volume hyperbolic 3-manifold  $M$ ,  $GS(M)$  will denote the isometry classes of finite volume, properly immersed, totally geodesic surfaces up to free homotopy. A special case of Thurston [79, Corollary 8.8.6.] implies that  $GS(M)$  contains only finitely many Riemann surfaces of a fixed finite topological type; this also follows from a compactness argument. Reid and the second author [59, Theorem 1.1] prove that if  $M_1, M_2$  are arithmetic hyperbolic 3-manifolds with  $GS(M_1) = GS(M_2) \neq \emptyset$ , then  $M_1, M_2$  are commensurable. Our second result is an effective version.

**Theorem 1.2** *Let  $M_1, M_2$  be arithmetic hyperbolic 3-manifolds with volumes less than  $V$  and  $GS(M_1) \cap GS(M_2) \neq \emptyset$ . Then there exists an absolute, effectively computable constant  $c$  such that if  $GS(M_1), GS(M_2)$  agree for all totally geodesic surfaces with area less than  $e^{cV}$ , then  $M_1$  and  $M_2$  are commensurable.*

There are infinitely many commensurability classes  $\mathcal{C}$  of arithmetic hyperbolic 3-manifolds such that all  $M \in \mathcal{C}$  have  $GS(M) = \emptyset$  (see [53, Corollary 7] and [19, p. 546]). However, once an arithmetic hyperbolic 3-manifold has one such surface, it is a well-known fact that there are necessarily infinitely

many distinct commensurability classes of such surfaces. Below, Theorem 1.11 provides a lower bound for the number of commensurability classes of surfaces up to some volume in these arithmetic hyperbolic 3-manifold and hence implies the infinitude of such surfaces for those manifolds. To the best of our knowledge the lower bound we provide is the first such lower bound.

### 1.2.3 Algebraic

We now turn to algebraic effective rigidity results which, aside from being independently interesting, provide us with tools for proving the above geometric effective rigidity results. Our first result is an effective version of the fact that quaternion algebras over number fields are determined by their maximal subfields.

**Theorem 1.3** *Let  $k$  be a number field and let  $B, B'/k$  be quaternion algebras satisfying  $|\text{disc}(B)|, |\text{disc}(B')| < x$ . If every quadratic field extension  $L/k$  with*

$$|\Delta_{L/k}| < 64^{n_k^3} d_k^{n_k} e^{2n_k \left[ \frac{21x}{\log^3(x)} + x \right]}$$

*embeds into  $B$  if and only if it embeds into  $B'$ , then  $B \cong B'$ .*

We further note that in Theorem 1.3, if the quaternion algebras  $B, B'$  are both unramified at a common real place of  $k$ , then we need only consider quadratic extensions  $L/k$  which are not totally complex.

Our second result is the algebraic counterpart of our effective result, Theorem 1.2, on totally geodesic surfaces.

**Theorem 1.4** *Suppose that  $k$  is a number field and  $B_0/k$  is a quaternion algebra. Let  $L_1, L_2/k$  be quadratic extensions and define  $B_1 = B_0 \otimes_k L_1$  and  $B_2 = B_0 \otimes_k L_2$ . If  $B \otimes_k L_1 \cong B_1$  if and only if  $B \otimes_k L_2 \cong B_2$  for every quaternion algebra  $B/k$  with  $\text{Ram}_\infty(B) = \text{Ram}_\infty(B_0)$  and satisfying*

$$|\text{disc}(B)| \leq d_\ell^{2C} (2 \log (|\text{disc}(B_1)| |\text{disc}(B_2)|))^4 |\text{disc}(B_1)| |\text{disc}(B_2)|,$$

*then  $L_1 \cong L_2$  and  $B_1 \cong B_2$ .*

Here  $C$  is the (absolute) constant appearing in the bound on the least prime ideal in the Chebotarev density theorem [40]. Theorem 1.4 is stronger than the algebraic result deduced in [59]. Consequently, Theorem 1.4 provides similar geometric spectral rigidity results but for a broader class of manifolds modeled on  $(\mathbf{H}^2)^a \times (\mathbf{H}^3)^b$ .

### 1.3 Main tools: counting function and asymptotic behavior

Understanding the asymptotic behavior of counting functions is central to the field of analytic number theory. Our work falls within the subfield of arithmetic statistics, which centers around counting problems on number fields and elliptic curves with bounded discriminant. The analytic method used in our proofs goes at least back to Cohn [22], who used a similar approach to count the number of abelian cubic extensions of  $\mathbf{Q}$  with bounded discriminant. Other seminal works in this area include the classical theorem of Davenport–Heilbronn [24], which provides an asymptotic formula for the number of cubic number fields with bounded discriminant, and its various generalizations to certain classes of number fields of higher degree (for an excellent survey of these results we refer the reader to Bhargava’s lecture from the 2006 ICM [6]). The general philosophy used in all of this work is to introduce a generating function whose coefficients count the object being studied and then apply a Tauberian theorem to convert information about the analytic behavior of these functions near their singularities into useful information about the counts. Although the results in this subsection are functioning as tools for proving our above stated results, they fall naturally within this larger program of study and thus are of independent interest. Specifically, the technical results that we discuss below all involve counting problems on central division algebras with bounded discriminant.

#### 1.3.1 Algebraic

We now turn to the statements of our main algebraic asymptotic results. Let

$$N_{m,n}(x) := \#\{ \text{central simple algebras } A/k \text{ of dimension } n^2 \text{ of the form } A = M(r, D), \text{ where } \dim(D) = d^2 \text{ for some } d|m, \text{ and } |\text{disc}(A)| \leq x \}.$$

We now state our first algebraic asymptotic counting result.

**Theorem 1.5** *If  $N(x)$  denotes the number of division algebras  $D/k$  of dimension  $n^2$  with  $|\text{disc}(D)| \leq x$  and  $\ell$  is the smallest prime divisor of  $n$ , then*

$$N(x) = \sum_{m|n} \mu(n/m) N_{m,n}(x).$$

*Moreover, there is a constant  $\delta_n > 0$ , which may depend on  $k$ , so that*

$$N(x) = (\delta_n + o(1)) x^{\frac{1}{n^2(1-1/\ell)}} (\log x)^{\ell-2} \quad \text{as } x \rightarrow \infty. \quad (1)$$

The key component of this proof is a classical Tauberian theorem of Delange, which allows us to precisely estimate  $N_{m,n}(x)$  provided that we understand the analytic behavior of its associated Dirichlet series. We next provide an asymptotic count of the quadratic extensions that embed in a fixed quaternion algebra over a fixed field  $k$ .

**Theorem 1.6** *Fix a number field  $k$  and a quaternion algebra  $B/k$ . The number of quadratic extensions  $L/k$  which embed into  $B$  and satisfy  $|\Delta_{L/k}| \leq x$  is asymptotic to  $c_{k,B}x$  as  $x \rightarrow \infty$ , where  $c_{k,B} > 0$ . Moreover, if  $\kappa_k$  is the residue at  $s = 1$  of  $\zeta_k(s)$ ,  $r_2$  is the number of pairs of complex embeddings of  $k$ , and  $r'_B$  is the number of places of  $k$  (both finite and infinite) that ramify in  $B$ , then*

$$c_{k,B} \geq \frac{1}{2^{r'_B+r_2}} \frac{\kappa_k}{\zeta_k(2)}.$$

The proof of this result stems from a powerful theorem of Wood [84], which allows us to model the splitting of finitely many primes as mutually independent events, over the class of random extensions of  $k$ . Our final result provides an asymptotic count of the quaternion algebras over  $k$  with a specified finite collection of maximal subfields. Note that we require some conditions on the collection of subfields as some selections might not have any algebra that contains them as maximal subfields.

**Theorem 1.7** *Fix a number field  $k$ , fix quadratic extensions  $L_1, L_2, \dots, L_r/k$ , let  $L$  be the compositum of the  $L_i$ , and suppose that  $[L : k] = 2^r$ . Then the number of quaternion algebras  $B/k$  with  $|\text{disc}(B)|$  less than  $x$  and which admit embeddings of all of the  $L_i$  is  $\sim \delta \cdot x^{1/2}/(\log x)^{1-\frac{1}{2^r}}$  as  $x \rightarrow \infty$ . Here  $\delta$  is a positive constant explicitly given in the proof and depending only on the  $L_i$  and  $k$ .*

In this proof, we make use of the well-developed theory of sums of non-negative multiplicative functions due to Wirsing in order to obtain a precise asymptotic for our counting function. We highlight an explicit value of the constant  $\delta$  in the case where  $r = 1$  below.

*Example 1* When  $r = 1$ , the expression for  $\delta$  can be put in compact form. We find that the number of quaternion algebras  $B/k$  that admit an embedding of a fixed quadratic extension  $L/k$  is

$$\sim 2^{r'_1-\frac{1}{2}} \left( \frac{\kappa}{L(1, \chi)} \right)^{1/2} \cdot \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \text{ not split}}} \left( 1 - \frac{1}{|\mathfrak{p}|^2} \right)^{1/2} \cdot \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \text{ ramified}}} \left( 1 + \frac{1}{|\mathfrak{p}|} \right)^{1/2} \cdot \frac{x^{1/2}}{(\log x)^{1/2}} \quad \text{as } x \rightarrow \infty.$$

Here  $\kappa$  is the residue at  $s = 1$  of  $\zeta_k(s)$ , and  $L(1, \chi)$  is the value at  $s = 1$  of the nontrivial Artin  $L$ -function associated to the extension  $L/k$ .

### 1.3.2 Geometric

The above algebraic counting results have geometric companions. We briefly supply some additional, independent motivation before stating our geometric counting applications. Basic problems like counting arithmetic manifolds of a bounded volume modeled on a fixed symmetric space involve two distinct mechanisms for growth: the growth rate coming from a fixed commensurability class and the growth rate of the number of distinct commensurability classes. Several papers have been written on the growth rate of (arithmetic) lattices in a fixed Lie group and also manifolds modeled on a fixed symmetric space; see [3–5, 11, 32, 34–36, 42, 43], and [49]. Our counting results focus on counting commensurability classes of manifolds with some prescribed features, or counting commensurability classes of geodesics or totally geodesic submanifolds in a fixed manifold.

Our first two results provide upper bounds for the number of commensurability classes of arithmetic hyperbolic 2- or 3-manifolds with a fixed trace field. In the statement of these results, the volume  $V_{\mathcal{C}}$  of a commensurability class  $\mathcal{C}$  is the minimum volume achieved by its members. That this volume is achieved in a commensurability class follows from Borel [7]. Belolipetsky [3, Section 4] gave a polynomial upper bound for the number of commensurability classes of irreducible arithmetic lattices in a fixed isotypic semisimple Lie group  $H$  arising from a fixed number field  $k$  under the assumption that the simple factors are not of type  $A_1$ . When  $H$  has type  $A_1$  factors (i.e.  $H$  is isogenous with  $\mathrm{SL}(2, \mathbf{R})^a \times \mathrm{SL}(2, \mathbf{C})^b$ ), Belolipetsky–Gelander–Lubotzky–Shalev [4, Section 3] gave a polynomial upper bound for the number of commensurability classes of arithmetic lattices in  $H$  arising from a fixed number field  $k$ . Varying  $k$ , both [3, 4] provided super-polynomial upper bounds for the number of classes without restriction on  $k$ . Our first results give upper bounds for the number of commensurability classes of arithmetic hyperbolic 2- or 3-manifolds with trace field  $k$ . These upper bounds are explicit refinements of the upper bounds from [4] in these cases.

**Corollary 1.8** *Let  $k$  be a totally real number field of degree  $n_k$  and let  $N_k(V)$  be the number of commensurability classes  $\mathcal{C}$  of arithmetic hyperbolic 2-orbifolds with trace field  $k$  and  $V_{\mathcal{C}} \leq V$ . Then  $N_k(V) \ll \frac{\kappa 2^{n_k-1} V^{130}}{\zeta_k(2)}$  for sufficiently large  $V$ , where  $\zeta_k(s)$  is the Dedekind zeta function of  $k$  and  $\kappa$  is the residue of  $\zeta_k(s)$  at  $s = 1$ .*

**Corollary 1.9** *Let  $k$  be a number field of degree  $n_k$  with a unique complex place and let  $N_k(V)$  be the number of commensurability classes  $\mathcal{C}$*

of arithmetic hyperbolic 3-orbifolds with trace field  $k$  and  $V_{\mathcal{C}} \leq V$ . Then  $N_k(V) \ll \frac{\kappa 2^{n_k-3} V^7}{\zeta_k(2)}$  for sufficiently large  $V$ , where  $\zeta_k(s)$  is the Dedekind zeta function of  $k$  and  $\kappa$  is the residue of  $\zeta_k(s)$  at  $s = 1$ .

There is one commensurability class of non-compact arithmetic hyperbolic 2-manifolds and for non-compact arithmetic 3-manifolds, the commensurability classes are in bijection with the imaginary quadratic number fields. In particular, for a fixed  $k$ , they do not affect the growth of  $N_k(V)$ .

We say (complex) geodesic lengths  $\ell_1, \ell_2$  are rationally inequivalent if  $\ell_1/\ell_2 \notin \mathbf{Q}$ . Our next result provides a lower bound for the number of rationally inequivalent geodesics of bounded length.

**Corollary 1.10** *Let  $M$  be an arithmetic hyperbolic 2-manifold (resp., 3-manifold) of covolume  $V$  with invariant trace field  $k$  and invariant quaternion algebra  $B$ . Then for sufficiently large  $V$  and  $x$ ,  $M$  contains at least  $\left[ \frac{\kappa_k}{2} \left( \frac{3}{\pi^2} \right)^{n_k} \right] x$  rationally inequivalent geodesics of length at most  $e^{cV} x^{n_k}$  where  $c$  is an absolute, effectively computable constant.*

An alternative form of this inequality is that there are at least  $\left[ \frac{\kappa_k}{2} \left( \frac{3}{\pi^2} \right)^{n_k} e^{-cV/n_k} \right] \ell^{1/n_k}$  rationally inequivalent geodesics of length at most  $\ell$  provided that  $V$  and  $\ell$  are sufficiently large. By Huber [39], Margulis [56], the asymptotic growth rate for the number of primitive geodesics of length at most  $\ell$  is  $\frac{e^{h\ell}}{h\ell}$  where  $h$  is the entropy of the geodesic flow.

Our final geometric counting result provides a lower bound for the growth rate of incommensurable totally geodesic surfaces of bounded area in an arithmetic hyperbolic 3-manifold that contains at least one totally geodesic surface.

**Theorem 1.11** *Let  $M = \mathbf{H}^3/\Gamma$  be an arithmetic hyperbolic 3-orbifold of volume  $V$  with invariant trace field  $k$  and invariant quaternion algebra  $B$ . If  $M$  contains a totally geodesic surface, then for sufficiently large  $x$ ,  $M$  contains at least  $[c(k)\text{disc}(B)^{1/2}]x/\log(x)^{1/2}$  pairwise incommensurable totally geodesic surfaces with area at most  $[2\pi^2 e^{cV}]x$ . Here  $c(k)$  is a constant depending only on  $k$  and  $c$  is an absolute, effectively computable constant.*

Theorem 1.11 in tandem with Theorem 1.2 gives an estimate on the number of surfaces needed to distinguish a pair of incommensurable, arithmetic hyperbolic 3-manifolds with a totally geodesic surface. We prove that if an arithmetic hyperbolic 3-manifold contains a totally geodesic surface then in fact it contains a totally geodesic surface with area bounded above by data from the manifold (see Proposition 6.3).

## 1.4 Layout

In Sect. 2 we introduce some of the basic concepts, terms, and objects for the paper. In Sect. 3 we prove the main algebraic counting results. In Sect. 4 we prove the main geometric counting results. In Sect. 5 we prove the effective results on geodesic lengths while in Sect. 6 we prove the results involving surfaces, including the asymptotic results on incommensurable, totally geodesic surfaces.

## 2 Background

### Notation

The following notation is utilized throughout this article.

- $\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$  are the natural numbers, integers, and rational, real, and complex fields.  $\varphi(n)$  is the Euler totient function,  $\mu(n)$  is the Möbius function, and  $\log(x)$  is the natural logarithm function.
- $k$  is a number field and  $L/k$  is a finite extension.  $\mathcal{O}_k$ ,  $\mathcal{O}_k^*$ ,  $\mathcal{O}_k^1$  are the ring of integers, the group of units, and the group of norm 1 elements, respectively.  $\widehat{k}$  is the Galois closure of  $k$  and  $k^+$  is the maximal, totally real subfield of  $k$ .  $d_k$  is the absolute discriminant,  $\text{Reg}_k$  is regulator for  $k$ , and  $h_k$  is the class number of  $k$ .
- $\mathcal{P}_k$  is the set of places/primes of  $k$ . For  $\mathfrak{p} \in \mathcal{P}_k$ , we denote the norm by  $|\mathfrak{p}|$  and the associated valuation by  $|\cdot|_{\mathfrak{p}}$ . For a place  $\mathfrak{P} \in \mathcal{P}_L$  residing over a place  $\mathfrak{p} \in \mathcal{P}_k$ , we denote this by  $\mathfrak{P}|\mathfrak{p}$  or simply  $\mathfrak{P}|_{\mathfrak{p}}$ . Occasionally,  $\mathfrak{P}|_k$  will denote the prime  $\mathfrak{p} \in \mathcal{P}_k$  that  $\mathfrak{P}$  is over.
- $n_k$  is the degree of  $k/\mathbf{Q}$ .  $r_1(k)$  and  $r_2(k)$ , or simply  $r_1, r_2$ , are the number of real and complex places.
- $\mathfrak{f}_{L/k}$  is the conductor.  $\Delta_{L/k}$  is the relative discriminant of an extension  $L/k$ .  $\zeta_k(s)$  is the Dedekind  $\zeta$ -function and  $\kappa_k$  is the residue of the pole of  $\zeta_k$  at  $s = 1$ .  $J_k$  is the idèle group for  $k$ .
- $D/k$  is a division algebra over  $k$ .  $B/k$  is a quaternion algebra over  $k$ .  $A/k$  is a central simple algebra over  $k$  with norm  $\text{nr}$ , group of invertible elements  $A^\times$ , group of norm 1 elements  $A^1$ , and discriminant  $\text{disc}(A)$ .
- $\text{Ram}(A) \subset \mathcal{P}_k$  is the set of ramified places of  $A$ ,  $\text{Ram}_f(A)$  is the set of finite ramified places of  $A$ ,  $\text{Ram}_\infty(A)$  is the set of infinite ramified places of  $A$ , and  $r_A = |\text{Ram}_\infty(A)|$ .
- For a quaternion algebra  $B$ ,  $k_B$  is the maximal abelian extension of  $k$  which has 2-elementary Galois group, is unramified outside of the real places in  $\text{Ram}(B)$ , and in which every  $\mathfrak{p} \in \text{Ram}_f(B)$  splits completely.
- $\mathcal{O}, \mathcal{E}, \mathcal{D}$  are  $\mathcal{O}_k$ -orders in a central simple  $k$ -algebra. For each place  $\mathfrak{p} \in \mathcal{P}_k$ ,  $\mathcal{O}_{\mathfrak{p}}$  is the completion of  $\mathcal{O}$  at  $\mathfrak{p}$ .

- $\mathbf{H}^2, \mathbf{H}^3$  are real hyperbolic 2- and 3-spaces.  $M$  is an arithmetic hyperbolic 2- or 3-manifold and  $\Gamma = \pi_1(M) < \mathrm{PSL}(2, \mathbf{R})$  or  $\mathrm{PSL}(2, \mathbf{C})$  is the associated arithmetic lattice. When  $\Gamma = P\rho(\mathcal{O}^1)$ , we write  $\Gamma = \Gamma_{\mathcal{O}}$ .
- $c, C$  and variously decorated versions are constants. We interchangeably use the Landau “Big Oh” notation,  $f = O(g)$ , and the Vinogradov notation,  $f \ll g$ , when there exists a constant  $C > 0$  such that  $|f| \leq C|g|$ .  $f \sim g$  if  $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1$  and  $f = o(g)$  if  $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 0$ .

## 2.1 Algebraic

We refer the reader to [13, 41, 55, 65], and [73] for the below material.

### 2.1.1 Central simple algebras

One main algebraic requisite for later discussion is the theory of central simple algebras  $A/k$  and their orders. By the Artin–Wedderburn Structure Theorem [65, p. 49], every such  $A$  is isomorphic to a matrix algebra over a division algebra  $A = M(r, D)$  where  $r$  and  $D$  are uniquely determined. We require the following theorem in this paper.

**Theorem 2.1** *Let  $k$  be a number field. Let  $S$  be a finite collection of primes of  $k$  consisting of finite primes and real infinite places. Suppose that for each  $\mathfrak{p} \in S$  we are given a reduced fraction  $\frac{a_{\mathfrak{p}}}{m_{\mathfrak{p}}} \in \mathbf{Q} \cap (0, 1)$  such that*

- (i)  $m_{\mathfrak{p}} > 1$  and  $a_{\mathfrak{p}} > 0$ ,
- (ii)  $\frac{a_{\mathfrak{p}}}{m_{\mathfrak{p}}} = \frac{1}{2}$  whenever  $\mathfrak{p}$  is real,
- (iii)  $\sum_{\mathfrak{p} \in S} \frac{a_{\mathfrak{p}}}{m_{\mathfrak{p}}} \in \mathbf{Z}$ .

*There is a unique division algebra  $D/k$  possessing  $S$  as its set of ramified primes and with Hasse invariants  $\frac{a_{\mathfrak{p}}}{m_{\mathfrak{p}}}$  for  $\mathfrak{p} \in S$ . Conversely, every division algebra  $D/k$  arises in this way. The dimension of  $D$  is  $n^2$ , where  $n := \mathrm{lcm}_{\mathfrak{p} \in S} [m_{\mathfrak{p}}]$ . The discriminant of  $D$  is the modulus of  $k$  given by*

$$\mathrm{disc}(D) = \prod_{\substack{\mathfrak{p} \in S \\ \mathfrak{p} \text{ real}}} \mathfrak{p} \prod_{\substack{\mathfrak{p} \in S \\ \mathfrak{p} \text{ finite}}} \mathfrak{p}^{n^2(1 - \frac{1}{m_{\mathfrak{p}}})}.$$

This theorem is a consequence of the Albert–Brauer–Hasse–Noether theorem (see for instance [65, Section 18.4]) and more generally, the short exact sequence of Brauer groups appearing in local class field theory. Moreover, one can show that

$$\text{disc}(A) = \prod_{\substack{\mathfrak{p} \text{ real} \\ \mathfrak{p} \mid \text{disc}(D)}} \mathfrak{p} \cdot \left( \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \mid \text{disc}(D)}} \mathfrak{p} \right)^{r^2} = \prod_{\substack{\mathfrak{p} \in S \\ \mathfrak{p} \text{ real}}} \mathfrak{p} \prod_{\substack{\mathfrak{p} \in S \\ \mathfrak{p} \text{ finite}}} \mathfrak{p}^{n^2(1 - \frac{1}{m_{\mathfrak{p}}})}$$

when  $A = \mathbf{M}(r, D)$ . Thus,

$$|\text{disc}(A)| = |\text{disc}(D)|^{r^2} = \prod_{\substack{\mathfrak{p} \in S \\ \mathfrak{p} \text{ finite}}} |\mathfrak{p}|^{n^2(1 - \frac{1}{m_{\mathfrak{p}}})}. \quad (2)$$

By Theorem 2.1,  $D$  corresponds to certain Hasse invariants  $a_{\mathfrak{p}}/m_{\mathfrak{p}}$  for  $\mathfrak{p} \in \mathcal{P}$ , and the dimension of  $D$  over  $k$  is  $d^2$  for  $d = \text{lcm}_{\mathfrak{p} \in \mathcal{P}} [m_{\mathfrak{p}}]$ . In the future, the Hasse invariants of  $D$  will also be referred to as the Hasse invariants of  $A$ . If the dimension of  $A$  over  $k$  is  $n^2$ , then  $r^2 d^2 = n^2$ .

### 2.1.2 Parametrizing maximal orders

In what follows,  $k$  will be a fixed number field and  $B/k$  a fixed quaternion algebra. Our exposition follows Sections 3–4 of [44]. We refer the reader to [73] for a general treatment on orders.

Let  $J_k$  (respectively  $J_B$ ) denote the idèle group of  $k$  (respectively  $B$ ). In this context, the idèle group  $J_B$  acts on the set of maximal orders of  $B$  as follows. Given  $\tilde{x} \in J_B$  and  $\mathcal{O}$  a maximal order of  $B$  we define  $\tilde{x}\mathcal{O}\tilde{x}^{-1}$  to be the unique maximal order of  $B$  with the property that for every finite prime  $\mathfrak{p}$  of  $k$ , its completion at  $\mathfrak{p}$  is equal to  $x_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}x_{\mathfrak{p}}^{-1}$  (existence and uniqueness follow from the local-to-global correspondence for orders). With this action we see that the set of maximal orders corresponds to the coset space  $J_B/\mathfrak{N}(\mathcal{O})$ , where  $\mathfrak{N}(\mathcal{O}) = J_B \cap \prod_{\mathfrak{p}} N_{B_{\mathfrak{p}}^*}(\mathcal{O}_{\mathfrak{p}})$  and  $N_{B_{\mathfrak{p}}^*}(\mathcal{O}_{\mathfrak{p}})$  is the normalizer in  $B_{\mathfrak{p}}^*$  of  $\mathcal{O}_{\mathfrak{p}}^*$ . The isomorphism classes of maximal orders of  $B$  (which by the Skolem–Noether theorem [65, p. 230] coincide with conjugacy classes) thus correspond to points in the double coset space  $B^* \backslash J_B / \mathfrak{N}(\mathcal{O})$ . The reduced norm  $\text{nr}(\cdot)$  induces a bijection [44, Theorem 4.1] between the latter double coset space and  $k^* \backslash J_k / \text{nr}(\mathfrak{N}(\mathcal{O})) \cong J_k / k^* \text{nr}(\mathfrak{N}(\mathcal{O}))$ . The latter group is finite and, as  $J_k^2 \subset \text{nr}(\mathfrak{N}(\mathcal{O}))$ , is of exponent 2. Hence, there exists an integer  $m \geq 1$  such that the number of isomorphism classes of maximal orders is equal to  $2^m$  and  $J_k / k^* \text{nr}(\mathfrak{N}(\mathcal{O})) \cong (\mathbf{Z}/2\mathbf{Z})^m$ .

We now parameterize the maximal orders of  $B$ . Let  $\mathfrak{p}_1, \dots, \mathfrak{p}_m$  be a set of primes of  $k$  such that  $B_{\mathfrak{p}_i} \cong \mathbf{M}(2, k_{\mathfrak{p}_i})$  for all  $i$  and such that the cosets of  $J_k / k^* \text{nr}(\mathfrak{N}(\mathcal{O}))$  defined by the elements

$$\{e_{\mathfrak{p}_i} = (1, \dots, 1, \pi_{\mathfrak{p}_i}, 1, \dots)\}_{i=1}^m$$

form a generating set. For each prime  $\mathfrak{p}_i$ , let  $\delta_i = \text{diag}(\pi_{\mathfrak{p}_i}, 1)$  and  $\mathcal{O}'_{\mathfrak{p}_i} = \delta_i \mathcal{O}_{\mathfrak{p}_i} \delta_i^{-1}$ . Given  $\gamma = (\gamma_i) \in (\mathbf{Z}/2\mathbf{Z})^m$ , we define a maximal order  $\mathcal{O}^\gamma$  via the local-to-global correspondence:

$$\mathcal{O}_{\mathfrak{p}}^\gamma = \begin{cases} \mathcal{O}_{\mathfrak{p}_i} & \text{if } \mathfrak{p} = \mathfrak{p}_i \text{ and } \gamma_i = 0 \\ \mathcal{O}'_{\mathfrak{p}_i} & \text{if } \mathfrak{p} = \mathfrak{p}_i \text{ and } \gamma_i = 1 \\ \mathcal{O}_{\mathfrak{p}} & \text{otherwise.} \end{cases}$$

By [44, Proposition 4.1], every maximal order of  $B$  is conjugate to one of the orders defined above. Henceforth we will refer to this as a parameterization of the maximal orders of  $B$  relative to  $\mathcal{O}$ .

Let  $L/k$  be a quadratic extension and  $k_B$  be the class field corresponding to  $J_k/k^* \text{nr}(\mathfrak{N}(\mathcal{O}))$  by class field theory. Alternatively,  $k_B$  can be characterized as the maximal abelian extension of  $k$  which has 2-elementary Galois group, is unramified outside of the real places in  $\text{Ram}(B)$  and in which every finite prime of  $\text{Ram}(B)$  splits completely. The following lemma appears as [44, Lemma 3.7]:

**Lemma 2.2** *Let the notation be as above.*

- (i) *If  $L \not\subset k_B$  then there exists a generating set  $\{e_{\mathfrak{p}_i}\}$  of  $J_k/k^* \text{nr}(\mathfrak{N}(\mathcal{O}))$  in which all of the  $\mathfrak{p}_i$  split in  $L/k$ .*
- (ii) *If  $L \subset k_B$  and  $\mathfrak{q}$  is any prime of  $k$  which is inert in  $L/k$  then there exists a generating set  $\{e_{\mathfrak{p}_i}\}$  of  $J_k/k^* \text{nr}(\mathfrak{N}(\mathcal{O}))$  in which  $\mathfrak{p}_1 = \mathfrak{q}$  and  $\mathfrak{p}_2, \dots, \mathfrak{p}_m$  all split in  $L/k$ .*

We conclude this section with a technical result which we will utilize in the proof of Theorem 1.1.

**Proposition 2.3** *Let  $\mathcal{E}, \mathcal{D}$  be maximal orders of  $B$  and suppose that  $u \in \mathcal{E}^1$  with  $u \notin k$  and set  $L = k(u)$ . Then there exists an absolute constant  $C_1 > 0$  and a positive integer  $n \leq d_L^{C_1}$  such that  $\mathcal{D}$  admits an embedding of  $\mathcal{O}_k[u^n]$ .*

In the proof of Proposition 2.3, we require the following lemma, which is an immediate consequence of the bound on the least prime ideal in the Chebotarev density theorem [40].

**Lemma 2.4** *If  $L/k$  is a quadratic extension, then there exists an absolute, effectively computable constant  $C_1$  such that there exists a prime of  $k$  which is inert in  $L/k$  and has norm less than  $d_L^{C_1}$ .*

*Proof of Proposition 2.3* If  $L \not\subset k_B$ , then the selectivity theorem of Chinburg–Friedman [16] (see also [44]) shows that  $\mathcal{D}$  admits an embedding of  $\mathcal{O}_k[u]$ ,

hence we may take  $n = 1$ . Suppose now that  $L \subset k_B$  and let  $q$  be a prime of  $k$  of smallest norm which is inert in  $L/k$ . Let  $\{e_{\mathfrak{p}_i}\}$  be the set of representatives of  $J_k/k^* \text{nr}(\mathfrak{N}(\mathcal{O}))$  from Lemma 2.2(ii) (in which  $\mathfrak{p}_1 = q$  and  $\mathfrak{p}_2, \dots, \mathfrak{p}_m$  all split in  $L/k$ ). We claim that  $q$  does not ramify in  $B$ . Indeed, suppose that  $q$  ramified in  $B$ . By our characterization of  $k_B$ , it would follow that  $q$  would split completely in  $k_B$  and hence in  $L$  as  $L \subset k_B$ . However, this observation contradicts the fact that  $q$  is inert in  $L/k$ , proving our claim.

For each  $i = 2, \dots, m$ , we have an  $k_{\mathfrak{p}_i}$ -isomorphism  $f_{\mathfrak{p}_i} : B_{\mathfrak{p}_i} \rightarrow M(2, k_{\mathfrak{p}_i})$  such that  $f_{\mathfrak{p}_i}(L) \subset \begin{pmatrix} k_{\mathfrak{p}_i} & 0 \\ 0 & k_{\mathfrak{p}_i} \end{pmatrix}$ . Consequently,  $f_{\mathfrak{p}_i}(\mathcal{O}_L) \subset \begin{pmatrix} \mathcal{O}_{k_{\mathfrak{p}_i}} & 0 \\ 0 & \mathcal{O}_{k_{\mathfrak{p}_i}} \end{pmatrix}$ , and so  $\mathcal{O}_k[u]$  is contained in two adjacent vertices in the tree of maximal orders of  $M(2, k_{\mathfrak{p}_i})$ . Upon conjugating  $\mathcal{E}$  if necessary, we may assume that  $\{\mathcal{E}^\gamma\}$  is a parameterization of the maximal orders of  $B$  relative to  $\mathcal{E}$ . Additionally, we have  $u \in \mathcal{E}_{\mathfrak{p}_i}^\gamma$  for all  $\gamma$  and  $i = 2, \dots, m$ . By construction  $\mathcal{E}_q, \mathcal{E}'_q$  are adjacent in the tree of maximal orders of  $M(2, k_q)$ . By [54, p. 340], we have  $[\mathcal{E}_q^1 : \mathcal{E}_q^1 \cap \mathcal{E}'_q^1] = |q|(|q| + 1)$ . Setting  $n = |q|(|q| + 1)$ , we have shown that  $u^n \in \mathcal{E}_{\mathfrak{p}_i}^\gamma$  for all  $\gamma$  and  $1 \leq i \leq m$ . As  $\mathcal{E}_p^\gamma = \mathcal{E}_p$  for all primes  $p \notin \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$ , we conclude that  $u^n \in \mathcal{E}^\gamma$  for all  $\gamma$ . As all maximal orders of  $B$  are conjugate to one of the  $\mathcal{E}^\gamma$ , the proposition follows from Lemma 2.4.  $\square$

## 2.2 Geometric

We refer the reader to Maclachlan–Reid [54] for a thorough treatment of this material.

### 2.2.1 Hyperbolic geometry

Hyperbolic  $n$ -space  $\mathbf{H}^n$  is the real rank one symmetric space associated to the real simple Lie group  $\text{SO}(n, 1)$ . We identify the group of orientation preserving isometries of  $\mathbf{H}^2, \mathbf{H}^3$  with  $\text{PSL}(2, \mathbf{R}), \text{PSL}(2, \mathbf{C})$ , respectively. We view  $\mathbf{H}^2, \mathbf{H}^3$  as the symmetric spaces  $\mathbf{H}^2 = \text{PSL}(2, \mathbf{R})/\text{SO}(2), \mathbf{H}^3 = \text{PSL}(2, \mathbf{C})/\text{SU}(2)$ . Isometries of  $\mathbf{H}^2, \mathbf{H}^3$  split into three classes depending on the trace of the element. An isometry  $\gamma \in \text{PSL}(2, \mathbf{C})$  is *elliptic* if  $\text{Tr}(\gamma) \in (-2, 2)$ , *parabolic* if  $|\text{Tr}(\gamma)| = 2$ , and *hyperbolic* if  $|\text{Tr}(\gamma)| > 2$ .

We will sometimes refer to lattices  $\Gamma$  in  $\text{PSL}(2, \mathbf{R})$  or  $\text{PSL}(2, \mathbf{C})$  as Fuchsian or Kleinian groups. Given a lattice  $\Gamma$  in  $\text{PSL}(2, \mathbf{R}), \text{PSL}(2, \mathbf{C})$ , the associated quotient  $M = \mathbf{H}^2/\Gamma, \mathbf{H}^3/\Gamma$  is a complete finite volume hyperbolic 2- or 3-orbifold. We state an inequality of Gelander [31, Theorem 1.7] involving the volume of a complete, finite volume hyperbolic 3-manifold  $M$  and the rank of the fundamental group  $\pi_1(M) = \Gamma$ .

**Theorem 2.5** (Gelander) *There exists a constant  $C$  such that if  $M$  is a complete, finite volume hyperbolic 3-manifold of volume  $V$  and rank  $r$  fundamental group, then  $r \leq CV$ .*

### 2.2.2 Arithmetic hyperbolic manifolds

Let  $k$  be a totally real field with real places  $\mathfrak{p}_1, \dots, \mathfrak{p}_{r_1}$ . Fix a real place of  $k$  which, reordering if necessary, we denote by  $\mathfrak{p}_1$ . We select a quaternion algebra  $B/k$  with the property that  $\mathfrak{p}_j \in \text{Ram}(B)$  if and only if  $j > 1$ . In particular,  $B_{\mathfrak{p}_1} \cong M(2, \mathbf{R})$  and  $B_{\mathfrak{p}_j} \cong \mathbb{H}$  for  $j > 1$ , where  $\mathbb{H}$  is the quaternions over  $\mathbf{R}$ . Under the first isomorphism, the group of norm one elements  $B^1$  maps into  $\text{SL}(2, \mathbf{R})$ . Selecting a maximal order  $\mathcal{O} \subset B$ , the image of  $\mathcal{O}^1$  in  $\text{SL}(2, \mathbf{R})$  and the image of the projection  $P\mathcal{O}^1$  of  $\mathcal{O}^1$  to  $\text{PSL}(2, \mathbf{R})$  are both lattices. We say  $\Gamma < \text{SL}(2, \mathbf{R})$  or  $\text{PSL}(2, \mathbf{R})$  is an arithmetic lattice if  $\Gamma$  is commensurable in the wide sense with  $\mathcal{O}^1$  or  $P\mathcal{O}^1$  for some totally real number field  $k$ , quaternion algebra  $B/k$ , and maximal order  $\mathcal{O} \subset B$  as above. We use  $\Gamma_{\mathcal{O}}$  to denote  $\mathcal{O}^1$  and we say a lattice  $\Gamma < \text{SL}(2, \mathbf{R})$  is derived from a quaternion algebra if  $\Gamma < \Gamma_{\mathcal{O}}$  for some  $k, B, \mathcal{O}$  as above.

The construction of arithmetic lattices in  $\text{PSL}(2, \mathbf{C})$  is similar. Let  $k$  be a number field with a unique complex place  $\mathfrak{p}_1$  and real places  $\mathfrak{p}_2, \dots, \mathfrak{p}_{r_1+1}$  and let  $B/k$  be quaternion algebra such that  $\mathfrak{p}_j \in \text{Ram}(B)$  if and only if  $j > 1$ . Fixing an isomorphism  $B_{\mathfrak{p}_1} \cong M(2, \mathbf{C})$  and a maximal order  $\mathcal{O} \subset B$ , the groups  $\mathcal{O}^1, P\mathcal{O}^1$  are lattices in  $\text{SL}(2, \mathbf{C}), \text{PSL}(2, \mathbf{C})$ . Any lattice  $\Gamma < \text{SL}(2, \mathbf{C}), \text{PSL}(2, \mathbf{C})$  that is commensurable in the wide sense with  $\mathcal{O}^1, P\mathcal{O}^1$ , for some  $k, B, \mathcal{O}$  as above, will be called an arithmetic lattice in  $\text{SL}(2, \mathbf{C}), \text{PSL}(2, \mathbf{C})$ . We say a lattice  $\Gamma < \text{SL}(2, \mathbf{C})$  is derived from a quaternion algebra if  $\Gamma < \Gamma_{\mathcal{O}}$  for some  $k, B, \mathcal{O}$  as above. Finally, if  $B$  is a division algebra,  $\mathcal{O}^1, P\mathcal{O}^1$  are cocompact.

Given two arithmetic lattices  $\Gamma_1, \Gamma_2$  arising from  $(k_j, B_j)$ ,  $\Gamma_1, \Gamma_2$  will be commensurable in the wide sense if and only if  $k_1 \cong k_2$  and  $B_1 \cong B_2$  (see [54, Theorem 8.4.1]). We will make use of this fact throughout the remainder of this article.

**Theorem 2.6** *Let  $\Gamma_1, \Gamma_2$  be arithmetic lattices in  $\text{PSL}(2, \mathbf{R})$  or  $\text{PSL}(2, \mathbf{C})$  with arithmetic data  $(k_1, B_1), (k_2, B_2)$ , respectively. Then  $\Gamma_1, \Gamma_2$  are commensurable in the wide sense if and only if  $k = k_1 \cong k_2$  and  $B_1 \cong B_2$  as  $k$ -algebras.*

Theorem 2.6 was proven by Takeuchi [77] for Fuchsian groups and for Kleinian groups by Macbeath [52], Reid [71]. We say that  $M$  is an arithmetic hyperbolic 2- or 3-orbifold if the orbifold fundamental group of  $M$  is an arithmetic lattice in  $\text{PSL}(2, \mathbf{R})$  or  $\text{PSL}(2, \mathbf{C})$ . In this case,  $\pi_1(M) = \Gamma$  is commensurable with  $P\mathcal{O}^1$  for some  $k, B, \mathcal{O}$  as above. We call  $k$  the invariant trace

field/trace field and  $B$  the invariant quaternion algebra/quaternion algebra of  $M$ .

### 2.2.3 Geodesics and quadratic subfields

Let  $M$  be an arithmetic hyperbolic 2- or 3-orbifold arising from  $(k, B)$  with orbifold fundamental group  $\Gamma < \mathrm{PSL}(2, \mathbf{R})$  or  $\mathrm{PSL}(2, \mathbf{C})$ . The closed geodesics  $c_\gamma: S^1 \rightarrow M$  on  $M$  are in bijection with the  $\Gamma$ -conjugacy classes  $[\gamma]_\Gamma$  of hyperbolic elements  $\gamma$  in  $\Gamma$ . The roots of the characteristic polynomial  $p_\gamma(t)$  are given by the eigenvalues of  $\gamma$  and the associated (complex) geodesic length  $\ell(c_\gamma)$  is given by (see [54, p. 372])

$$\cosh\left(\frac{\ell(c_\gamma)}{2}\right) = \pm \frac{\mathrm{Tr}(\gamma)}{2}. \quad (3)$$

When  $\Gamma < \mathrm{PSL}(2, \mathbf{R})$ , (3) gives the length of the geodesic associated to  $\gamma$ . When  $\Gamma < \mathrm{PSL}(2, \mathbf{C})$ , (3) gives the complex length of the geodesic associated to  $\gamma$ . In this case,  $\ell(\gamma) = \ell_0(\gamma) + i\theta(\gamma)$  where  $\theta(\gamma)$  is the angle of rotation about the geodesic axis associated to  $\gamma$  and  $\ell_0(\gamma)$  is the length of the geodesic associated to  $\gamma$ . In particular, when  $\Gamma < \mathrm{PSL}(2, \mathbf{C})$ ,  $\ell(\gamma)$  is the associated complex length and  $\ell_0(\gamma)$  is the length. When  $\Gamma < \mathrm{PSL}(2, \mathbf{R})$ ,  $\ell(\gamma)$  will denote the length of the associated geodesic. We denote by  $\lambda_\gamma$  the unique eigenvalue of  $\gamma$  with  $|\lambda_\gamma| > 1$  and note that  $\lambda_\gamma \in \mathcal{O}_{k_\gamma}^1$  when  $\Gamma$  is arithmetic. Also, each  $\gamma$  determines a maximal subfield  $k_\gamma = k(\lambda_\gamma)$  of the quaternion algebra  $B$ .

### 2.2.4 Totally geodesic surfaces

Associated to an arithmetic hyperbolic 3-orbifold is a pair  $(L, B)$ , where  $L$  is a number field with exactly one complex place and  $B/L$  is a quaternion algebra that is ramified at all of the real places. If there exists a totally real subfield  $k \subset L$  with  $L/k$  quadratic and  $B_0/k$  is a quaternion algebra such that  $B_0 \otimes_k L \cong B$ , then the pair  $(k, B_0)$  will be data for a commensurability class of arithmetic hyperbolic 2-orbifolds provided that  $B_0$  is unramified at the real place  $\mathfrak{p}$  under the complex place  $\mathfrak{P}$  of  $K$ . The following appears as [54, Theorem 9.5.5].

**Theorem 2.7** *Let  $\Gamma$  be an arithmetic lattice in  $\mathrm{PSL}(2, \mathbf{C})$  with arithmetic data  $(L, B)$  and suppose that  $k$  is a totally real subfield of  $L$  with  $[L : k] = 2$ . Suppose  $B_0$  is a quaternion algebra over  $k$  ramified at all real places of  $k$  except at the place under the complex place of  $L$ . Then  $B \cong B_0 \otimes_k L$  if and only if  $\mathrm{Ram}_f(B)$  consists of  $2r$  places (where  $r \geq 0$ )  $\{\mathfrak{P}_{i,j}\}$  where  $j$  ranges over  $\{1, \dots, r\}$  and  $i$  ranges over  $\{1, 2\}$  and satisfy  $\mathfrak{P}_{1,j} \cap \mathcal{O}_k = \mathfrak{P}_{2,i} \cap \mathcal{O}_k = \mathfrak{p}_i$ ,*

where  $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\} \subset \text{Ram}_f(B_0)$  with  $\text{Ram}_f(B_0) \setminus \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$  consisting of primes in  $\mathcal{O}_k$  which are inert or ramified in  $L/k$ .

### 3 Main tools: algebraic counting results

We now begin our first main section, where we will establish our algebraic counting results. For the reader interested only in the applications of these results to the rigidity theorems stated in the introduction, the reader can start at Sect. 5 and refer back to the results from Sects. 3 and 4.

#### 3.1 Proof of Theorem 1.5

Fix a number field  $k$  and fix a positive integer  $n$ . In this section, we estimate the number of division algebras  $D/k$  of dimension  $n^2$  whose discriminant lies below a large bound  $x$ . Our main tool is the following Tauberian theorem of Delange [25, 26].

**Theorem 3.1** (Delange) *Let*

$$G(s) = \sum_{N=1}^{\infty} a_N N^{-s}$$

*be a Dirichlet series satisfying the following conditions for certain real numbers  $\rho > 0$  and  $\beta > 0$ :*

- (i) *each  $a_N \geq 0$ ,*
- (ii)  *$G(s)$  converges for  $\Re(s) > \rho$ ,*
- (iii)  *$G(s)$  can be continued to an analytic function in the closed half-plane  $\Re(s) \geq \rho$ , except possibly for a singularity at  $s = \rho$  itself,*
- (iv) *there is an open neighborhood of  $\rho$ , and functions  $A(s)$  and  $B(s)$  analytic at  $s = \rho$ , with*

$$G(s) = \frac{A(s)}{(s - \rho)^{\beta}} + B(s)$$

*at every point  $s$  in this neighborhood having  $\Re(s) > \rho$ .*

*Then as  $x \rightarrow \infty$ ,*

$$\sum_{N \leq x} a_N = \left( \frac{A(\rho)}{\rho \Gamma(\beta)} + o(1) \right) x^{\rho} (\log x)^{\beta-1}.$$

*Remark* We allow the possibility that  $A(\rho) = 0$ , in which case the conclusion of Theorem 3.1 is that

$$\sum_{N \leq x} a_N = o(x^\rho (\log x)^{\beta-1}),$$

as  $x \rightarrow \infty$ . While Delange's theorem is usually stated with the restriction that  $A(\rho) \neq 0$ , the cases when  $A(\rho) = 0$  follow with no extra difficulty. For instance, suppose that  $\rho$  is the reciprocal of a positive integer, a condition that holds in all of our applications. If  $A(\rho) = 0$ , we can apply the restricted theorem first to  $G(s) + \zeta(s/\rho)^\beta$ , then to  $\zeta(s/\rho)^\beta$ , and then subtract the results to get the assertion we want. If  $\rho$  is not the reciprocal of a positive integer, then  $\zeta(s/\rho)$  need not be a Dirichlet series itself. However, this argument still works, provided we take as our starting point Delange's original Tauberian theorem [25], which is in terms of Laplace transforms, instead of its consequences for Dirichlet series [26].

According to Theorem 2.1, a division algebra  $D$  over  $k$  is uniquely specified by its Hasse invariants (i.e., the set  $S = \text{Ram}(D)$  and the choice of fractions  $\{a_p/m_p\}_{p \in S}$ ). Thus, our task is to count the number of ways of choosing these invariants so that the resulting division algebra  $D$  has dimension  $n^2$  and  $|\text{disc}(D)| \leq x$ . It turns out that this is a difficult problem to attack directly. More natural, from the analytic side, is to first count *all* central simple algebras over  $k$  of dimension  $n^2$ . The count of division algebras can then be obtained by the inclusion-exclusion principle. We now carefully execute the above approach by introducing the following set:

$$N_{m,n}(x) := \# \left\{ \text{central simple algebras } A/k \text{ of dimension } n^2 \text{ of the form} \right. \\ \left. A = M(r, D), \text{ where } \dim(D) = d^2 \text{ for some } d \mid m, \text{ and } |\text{disc}(A)| \leq x \right\}.$$

The remarks earlier in this paragraph show that in general,  $N_{m,n}(x)$  counts the number of choices for Hasse invariants for which  $\text{lcm}_{p \in S}[m_p]$  divides  $m$  and the product in (2) is bounded by  $x$ . Our key lemma is the following estimate for  $N_{m,n}(x)$ . Note that the special case of the lemma when  $m = n$  provides us with asymptotic behavior for the counting function of all dimension  $n^2$  central simple algebras over  $k$ .

**Lemma 3.2** *Let  $k/\mathbf{Q}$  be a number field. Let  $n > 1$  be an integer, and let  $\ell$  be the smallest prime factor of  $n$ . Let  $m$  be a divisor of  $n$ . Then as  $x \rightarrow \infty$ ,*

$$N_{m,n}(x) = (\delta_{m,n} + o(1))x^{\frac{1}{n^2(1-1/\ell)}} (\log x)^{\ell-2}$$

for a certain constant  $\delta_{m,n}$ . If  $\ell \nmid m$ , then  $\delta_{m,n} = 0$ . Suppose now that  $\ell \mid m$ . Let  $\kappa$  denote the residue at  $s = 1$  of the Dedekind zeta function  $\zeta_k(s)$ . If  $m$  is odd,

then

$$\delta_{m,n} = \frac{\kappa^{\ell-1}}{m(\ell-2)!} \cdot \frac{1}{(n^2(1-1/\ell))^{\ell-2}} \cdot \sum_{\substack{0 \leq j < m \\ \ell \mid j}} \left( \prod_{\mathfrak{p} \text{ finite}} \left( 1 + \frac{\ell-1}{|\mathfrak{p}|} + \sum_{\substack{m_{\mathfrak{p}} \mid m \\ m_{\mathfrak{p}} > \ell}} \frac{\mu\left(\frac{m_{\mathfrak{p}}}{(m_{\mathfrak{p}}, j)}\right) \varphi(m_{\mathfrak{p}})/\varphi\left(\frac{m_{\mathfrak{p}}}{(m_{\mathfrak{p}}, j)}\right)}}{|\mathfrak{p}|^{(1-1/m_{\mathfrak{p}})/(1-1/\ell)}} \right) \times \left( 1 - \frac{1}{|\mathfrak{p}|} \right)^{\ell-1} \right). \quad (4)$$

If  $m$  is even, (4) needs to be multiplied by  $2^{r_1}$ , where  $r_1$  is the number of real embeddings of  $k$ .

Broadly, the proof of the above lemma proceeds as follows. We first set up the count for the algebras and produce corresponding Dirichlet series. We then verify that our Dirichlet series satisfy (i)–(iv) of Theorem 3.1. We complete the proof via Theorem 3.1. The latter two steps comprise the bulk of the work.

*Proof* To set up our count, recall that by Theorem 2.1 a division algebra is determined by its collection of Hasse invariants, the rational numbers  $a_{\mathfrak{p}}/m_{\mathfrak{p}}$  for places  $\mathfrak{p} \mid \text{Ram}(D)$ . Thus, we need only count the number of choices for these local invariants. To that end, we will use the orthogonality relations among the roots of unity in an essential way. For each  $d$  dividing  $m$ , we introduce the set

$$\mathfrak{F}(m, d) := \left\{ 1 \leq k \leq m : \frac{k}{m} \text{ has lowest terms denominator } d \right\}.$$

For  $0 \leq j < m$ , let  $\zeta_j = e^{2\pi ij/m}$ , and consider the formal expression

$$\frac{1}{m} \left( \sum_{0 \leq j < m} \left[ \prod_{\mathfrak{p} \text{ finite}} \left( 1 + \sum_{\substack{m_{\mathfrak{p}} \mid m \\ m_{\mathfrak{p}} > 1}} \frac{\sum_{a_{\mathfrak{p}} \in \mathfrak{F}(m, m_{\mathfrak{p}})} \zeta_j^{a_{\mathfrak{p}}}}{\mathfrak{p}^{n^2(1-1/m_{\mathfrak{p}})s}} \right) \prod_{\substack{\mathfrak{p} \text{ real} \\ 2 \mid m}} \left( 1 + \frac{\zeta_j^{m/2}}{\mathfrak{p}^s} \right) \right] \right),$$

where the conditions on the final product mean that this product appears only when  $m$  is even. Expanding, we obtain a formal sum of terms  $c_{\mathfrak{m}}/\mathfrak{m}^s$ , where  $\mathfrak{m}$  ranges over the moduli of  $k$ . For  $c_{\mathfrak{m}}$  to be nonvanishing, it is necessary that every finite prime  $\mathfrak{p}$  dividing  $\mathfrak{m}$  appears to an exponent of the form  $n^2(1-1/m_{\mathfrak{p}})$  for some integer  $m_{\mathfrak{p}} > 1$  dividing  $m$ , and that  $\mathfrak{m}$  is not divisible by real primes except possibly if  $2 \mid m$ . If these conditions are satisfied, then

$$c_{\mathfrak{m}} = \frac{1}{m} \sum_{0 \leq j < m} c_{\mathfrak{m}}^{(j)}, \quad \text{where} \quad c_{\mathfrak{m}}^{(j)} = \sum_{\substack{\{a_{\mathfrak{p}}\}_{\mathfrak{p} \mid \mathfrak{m}, \mathfrak{p} \text{ finite} \\ \text{each } a_{\mathfrak{p}} \in \mathcal{F}(m, m_{\mathfrak{p}})}}} \zeta_j^{\sum_{\mathfrak{p} \mid \mathfrak{m}, \text{ finite}} a_{\mathfrak{p}} + \sum_{\mathfrak{p} \mid \mathfrak{m}, \text{ real}} \frac{m}{2}}.$$

Writing  $a_{\mathfrak{p}}/m = a'_{\mathfrak{p}}/m_{\mathfrak{p}}$ , and substituting in the value of  $\zeta_j$ , this expression for  $c_{\mathfrak{m}}^{(j)}$  can be put in the form

$$\sum_{\substack{\{a'_{\mathfrak{p}}\}_{\mathfrak{p} \mid \mathfrak{m}, \mathfrak{p} \text{ finite} \\ 1 \leq a'_{\mathfrak{p}} \leq m_{\mathfrak{p}}, \gcd(a'_{\mathfrak{p}}, m_{\mathfrak{p}}) = 1}} \exp\left(\frac{2\pi i j}{m} \left(m \sum_{\mathfrak{p} \mid \mathfrak{m}, \text{ finite}} \frac{a'_{\mathfrak{p}}}{m_{\mathfrak{p}}} + m \sum_{\mathfrak{p} \mid \mathfrak{m}, \text{ real}} \frac{1}{2}\right)\right).$$

For each integer  $k$ , the sum  $\sum_{0 \leq j < m} \exp(2\pi i j k / m)$  vanishes unless  $m \mid k$ , in which case the sum takes the value  $m$ . Now

$$m \sum_{\substack{\mathfrak{p} \mid \mathfrak{m} \\ \mathfrak{p} \text{ finite}}} \frac{a'_{\mathfrak{p}}}{m_{\mathfrak{p}}} + m \sum_{\substack{\mathfrak{p} \mid \mathfrak{m} \\ \mathfrak{p} \text{ real}}} \frac{1}{2} \quad \text{is a multiple of } m \iff \sum_{\substack{\mathfrak{p} \mid \mathfrak{m} \\ \mathfrak{p} \text{ finite}}} \frac{a'_{\mathfrak{p}}}{m_{\mathfrak{p}}} + \sum_{\substack{\mathfrak{p} \mid \mathfrak{m} \\ \mathfrak{p} \text{ real}}} \frac{1}{2} \in \mathbf{Z}.$$

Letting  $S$  be the set of primes dividing  $\mathfrak{m}$ , we conclude that  $c_{\mathfrak{m}} = \frac{1}{m} \sum_{0 \leq j < m} c_{\mathfrak{m}}^{(j)}$  counts the number of choices of Hasse invariants for which  $\text{lcm}_{\mathfrak{p} \in S} [m_{\mathfrak{p}}]$  divides  $m$  and

$$\left( \prod_{\substack{\mathfrak{p} \text{ real} \\ \mathfrak{p} \in S}} \mathfrak{p} \right) \left( \prod_{\substack{\mathfrak{p} \mid \mathfrak{m} \\ \mathfrak{p} \in S}} \mathfrak{p}^{n^2(1-1/m_{\mathfrak{p}})} \right) = \mathfrak{m}.$$

There is a one-to-one correspondence between these choices of Hasse parameters and central simple algebras  $A/k$  of dimension  $n^2$  of the form  $M(r, D)$ , where  $\dim(D) = d^2$  for some  $d \mid m$ , and  $\text{disc}(A) = \mathfrak{m}$ . Since  $d = \text{lcm}[m_{\mathfrak{p}}]$  and  $r = n/d$ , we can view the coefficients  $c_{\mathfrak{m}}$  as counting these central simple algebras. Thus,

$$N_{m,n}(x) = \sum_{|\mathfrak{m}| \leq x} c_{\mathfrak{m}}.$$

In order to apply Delange's theorem, Theorem 3.1, we need Dirichlet series. We obtain the needed series by simply replacing the primes  $\mathfrak{p}$  with their norms  $|\mathfrak{p}|$  in the above products; here we set  $|\mathfrak{p}| = 1$  when  $\mathfrak{p}$  is real. For  $j = 0, 1, 2, \dots, m-1$ , the Dirichlet series  $G_j(s)$  is given by the following product expansion:

$$G_j(s) = \prod_{\mathfrak{p} \text{ finite}} \left( 1 + \sum_{\substack{m_{\mathfrak{p}} \mid m \\ m_{\mathfrak{p}} > 1}} \frac{\sum_{a_{\mathfrak{p}} \in \mathfrak{F}(m, m_{\mathfrak{p}})} \zeta_j^{a_{\mathfrak{p}}}}{|\mathfrak{p}|^{n^2(1-1/m_{\mathfrak{p}})s}} \right) \prod_{\substack{\mathfrak{p} \text{ real} \\ 2 \mid m}} \left( 1 + \frac{\zeta_j^{m/2}}{|\mathfrak{p}|^s} \right). \quad (5)$$

If we then set

$$G(s) = \frac{1}{m} \sum_{0 \leq j < m} G_j(s),$$

the coefficient of  $N^{-s}$  in  $G(s)$  is precisely  $\sum_{|\mathfrak{m}|=N} c_{\mathfrak{m}}$ . Hence,  $N_{m,n}(x)$  is precisely the partial sum up to  $x$  of the coefficients of  $G(s)$ .

We now establish that our Dirichlet series satisfy the conditions of Theorem 3.1.

**Claim**  $G(s)$  satisfies (i)–(iv) of Theorem 3.1.

*Proof of Claim* Since the coefficients of  $G(s)$  count central simple algebras, their non-negativity is obvious. This shows that condition (i) of Delange's theorem is satisfied. To verify conditions (ii)–(iv) for  $G(s)$ , it suffices to verify that they hold for each individual  $G_j(s)$ . We will show this with

$$\rho = \frac{1}{n^2(1-1/\ell)} \quad \text{and} \quad \beta = \ell - 1. \quad (6)$$

Proceeding further requires a careful study of the product definition (5) of  $G_j(s)$ . First, we deal with the product over real primes, which is present only when  $2 \mid m$ . By our convention that real primes have norm 1,

$$\left( 1 + \frac{\zeta_j^{m/2}}{|\mathfrak{p}|^s} \right) = (1 + \zeta_j^{m/2})^{r_1};$$

in particular, this factor is independent of  $s$ . For all finite primes  $\mathfrak{p}$ , the  $\mathfrak{p}$ th term in (5) has the form  $1 + A_{\mathfrak{p}}(s)$ , where

$$A_{\mathfrak{p}}(s) = \sum_{\substack{m_{\mathfrak{p}} \mid m \\ m_{\mathfrak{p}} > 1}} \frac{\sum_{a_{\mathfrak{p}} \in \mathfrak{F}(m, m_{\mathfrak{p}})} \zeta_j^{a_{\mathfrak{p}}}}{|\mathfrak{p}|^{n^2(1-1/m_{\mathfrak{p}})s}}. \quad (7)$$

Since  $m$  divides  $n$  and  $\ell$  is the least prime divisor of  $n$ , we have  $n^2(1-1/m_{\mathfrak{p}}) \geq n^2(1-1/\ell)$  for each term in the sum. Moreover, each numerator on the right-hand side of (7) is trivially bounded by  $m$ . It follows that the the formal Dirichlet series expansion of  $G_j(s)$  converges absolutely for  $\Re(s) >$

$\frac{1}{n^2(1-1/\ell)}$  and coincides there with its (absolutely convergent) Euler product. This gives condition (ii). In fact, if  $\ell \nmid m$ , then the smallest nontrivial divisor of  $m$  is strictly larger than  $\ell$ . The argument of the preceding paragraph then implies that  $G_j(s)$  has an Euler product converging absolutely and uniformly in  $\Re(s) > \frac{1}{n^2(1-1/\ell)} - \epsilon$ , for some positive  $\epsilon$ . This shows that conditions (iii) and (iv) hold for  $G_j(s)$ , where in (iv) we may take  $A(s) = 0$  and  $B(s) = G_j(s)$ .

In the case when  $\ell|m$ , we have to analyze the  $A_{\mathfrak{p}}(s)$  more closely. For each  $m_{\mathfrak{p}}$  dividing  $m$ , the corresponding numerator on the right-hand side of (7) coincides with the Ramanujan sum  $c_{m_{\mathfrak{p}}}(j)$ . From Hölder's explicit evaluation of such sums [38, Theorem 272, p. 309],

$$\sum_{a_{\mathfrak{p}} \in \mathfrak{F}(m, m_{\mathfrak{p}})} \zeta_j^{a_{\mathfrak{p}}} = c_{m_{\mathfrak{p}}}(j) = \mu\left(\frac{m_{\mathfrak{p}}}{(m_{\mathfrak{p}}, j)}\right) \frac{\varphi(m_{\mathfrak{p}})}{\varphi(m_{\mathfrak{p}}/(m_{\mathfrak{p}}, j))}.$$

Thus, the first term on the right-hand sum in (7)—corresponding to  $m_{\mathfrak{p}} = \ell$ —is

$$\mu\left(\frac{\ell}{(\ell, j)}\right) \frac{\ell - 1}{\varphi(\ell/(\ell, j))} \frac{1}{|\mathfrak{p}|^{n^2(1-1/\ell)s}}.$$

For all of the remaining terms,  $n^2(1 - 1/m_{\mathfrak{p}}) > n^2(1 - 1/\ell)$ . Now if  $\ell \nmid j$ ,

$$\mu\left(\frac{\ell}{(\ell, j)}\right) \frac{\ell - 1}{\varphi(\ell/(\ell, j))} \frac{1}{|\mathfrak{p}|^{n^2(1-1/\ell)s}} = -\frac{1}{|\mathfrak{p}|^{n^2(1-1/\ell)s}}.$$

Put  $H_j(s) = G_j(s)\zeta_k(n^2(1 - 1/\ell)s)$ . Since

$$\zeta_k(n^2(1 - 1/\ell)s) = \prod_{\mathfrak{p} \text{ finite}} \left(1 + \frac{1}{|\mathfrak{p}|^{n^2(1-1/\ell)s}} + \frac{1}{|\mathfrak{p}|^{2n^2(1-1/\ell)s}} + \dots\right),$$

the  $\mathfrak{p}$ th factor in the Euler product expansion of  $H_j(s)$  has the form  $1 + O(|\mathfrak{p}|^{-Ns})$  for a positive integer  $N$  strictly larger than  $n^2(1 - 1/\ell)$ . Thus,  $H_j(s)$  continues analytically to  $\Re(s) > 1/N$ , and so also to the region  $\Re(s) \geq \frac{1}{n^2(1-1/\ell)}$ . Since  $\zeta_k(s)$  has no zeros on  $\Re(s) = 1$ , this gives an analytic continuation of  $G_j(s) = H_j(s)\zeta_k(n^2(1 - 1/\ell)s)^{-1}$  to  $\Re(s) \geq \frac{1}{n^2(1-1/\ell)}$ . This proves (iii) and (iv) with  $A(s) = 0$  and  $B(s) = G_j(s)$ . Now suppose that  $\ell|j$ .

Then

$$\mu\left(\frac{\ell}{(\ell, j)}\right) \frac{\ell-1}{\varphi(\ell/(\ell, j))} \frac{1}{|\mathfrak{p}|^{n^2(1-1/\ell)s}} = \frac{\ell-1}{|\mathfrak{p}|^{n^2(1-1/\ell)s}}.$$

Now arguing with Euler products as above, we find that if we set  $H_j(s) = G_j(s)\zeta_k(n^2(1-1/\ell)s)^{-(\ell-1)}$ , then  $H_j(s)$  is analytic for  $\Re(s) \geq \frac{1}{n^2(1-1/\ell)}$ . This implies that  $G_j(s) = H_j(s)\zeta_k(n^2(1-1/\ell)s)^{\ell-1}$  continues analytically to the same closed half-plane, except for a pole of order at most  $\ell-1$  at  $s = \frac{1}{n^2(1-1/\ell)}$ . Consequently, (iii) and (iv) hold with

$$A(s) = G_j(s) \left( s - \frac{1}{n^2(1-1/\ell)} \right)^{\ell-1}$$

and  $B(s) = 0$ . Collecting everything, we see that (i)–(iv) all hold for  $G(s)$ , for  $\rho$  and  $\beta$  as in (6). Moreover, we can take the  $A(s)$  in (iv) corresponding to  $G(s)$  as  $\frac{1}{m}$  times the sum of the functions  $A(s)$  corresponding to each  $G_j(s)$ .  $\square$

We now establish the lemma with a few applications of Theorem 3.1. We split into two cases.

*Case 1*  $\ell \nmid m$ . In the case when  $\ell \nmid m$ , the  $A(s)$  corresponding to each  $G_j(s)$  was identically zero, hence our final  $A(s)$  is also 0. Thus, Theorem 3.1 yields

$$N_{m,n}(x) = o(x^{\frac{1}{n^2(1-1/\ell)}} (\log x)^{\ell-2}) \quad \text{as } x \rightarrow \infty.$$

This completes the proof of the lemma in the case  $\ell \nmid m$ .

*Case 2*  $\ell|m$ . If  $\ell|m$ , our work shows that

$$A(s) = \left( s - \frac{1}{n^2(1-1/\ell)} \right)^{\ell-1} \cdot \frac{1}{m} \left( \sum_{\substack{0 \leq j < m \\ \ell|j}} G_j(s) \right).$$

To evaluate this  $A(s)$  at  $s = \frac{1}{n^2(1-1/\ell)}$ , we recall that  $\kappa$  denotes the residue at  $s = 1$  of the simple pole of  $\zeta_k(s)$ . Writing

$$\begin{aligned} \left( s - \frac{1}{n^2(1-1/\ell)} \right)^{\ell-1} G_j(s) &= \left( \zeta_k(n^2(1-1/\ell)s) \left( s - \frac{1}{n^2(1-1/\ell)} \right) \right)^{\ell-1} \\ &\quad \cdot G_j(s) \zeta_k(n^2(1-1/\ell)s)^{-(\ell-1)}, \end{aligned}$$

we see that

$$A\left(\frac{1}{n^2(1-1/\ell)}\right) = \left(\frac{\kappa}{n^2(1-1/\ell)}\right)^{\ell-1} \cdot \frac{1}{m} \left[ \sum_{\substack{0 \leq j < m \\ \ell|j}} \left( \lim_{\substack{s \rightarrow \frac{1}{n^2(1-1/\ell)}}} G_j(s) \zeta_k(n^2(1-1/\ell)s)^{-(\ell-1)} \right) \right].$$

It remains to evaluate the limits inside the final sum. For the values of  $j$  and  $m$  under consideration,  $\ell|j$  and  $\ell|m$ . So for each finite prime  $\mathfrak{p}$ , the  $\mathfrak{p}$ th term in the product expansion (5) of  $G_j(s)$  begins as

$$1 + (\ell-1)/|\mathfrak{p}|^{n^2(1-1/\ell)s} + \dots.$$

Now consider the factors corresponding to infinite primes. If  $m$  is odd, then there are no such factors in (5). If  $m$  is even, then we must have  $\ell = 2$ , and since  $\ell|j$ ,

$$1 + \zeta_j^{m/2} = 1 + e^{\pi i j} = 1 + (-1)^j = 2;$$

thus, the factor in (5) giving the contribution of the infinite primes is precisely  $2^{r_1}$ . We conclude that if  $m$  is odd, then

$$\begin{aligned} & \lim_{s \rightarrow \frac{1}{n^2(1-1/\ell)}} G_j(s) \zeta_k(s)^{-(\ell-1)} \\ &= \prod_{\mathfrak{p} \text{ finite}} \left( 1 + \frac{\ell-1}{|\mathfrak{p}|} + \sum_{\substack{m_{\mathfrak{p}}|m \\ m_{\mathfrak{p}}>\ell}} \frac{\mu\left(\frac{m_{\mathfrak{p}}}{(m_{\mathfrak{p}},j)}\right) \frac{\varphi(m_{\mathfrak{p}})}{\varphi(m_{\mathfrak{p}}/(m_{\mathfrak{p}},j))}}{|\mathfrak{p}|^{(1-1/m_{\mathfrak{p}})/(1-1/\ell)}} \right) \left( 1 - \frac{1}{|\mathfrak{p}|} \right)^{\ell-1}, \end{aligned}$$

while if  $m$  is even, this must be multiplied by  $2^{r_1}$ . So if  $m$  is odd, then

$$\begin{aligned} & A\left(\frac{1}{n^2(1-1/\ell)}\right) = \left(\frac{\kappa}{n^2(1-1/\ell)}\right)^{\ell-1} \cdot \frac{1}{m} \\ & \cdot \sum_{\substack{0 \leq j < m \\ \ell|j}} \left( \prod_{\mathfrak{p} \text{ finite}} \left( 1 + \frac{\ell-1}{|\mathfrak{p}|} + \sum_{\substack{m_{\mathfrak{p}}|m \\ m_{\mathfrak{p}}>\ell}} \frac{\mu\left(\frac{m_{\mathfrak{p}}}{(m_{\mathfrak{p}},j)}\right) \frac{\varphi(m_{\mathfrak{p}})}{\varphi(m_{\mathfrak{p}}/(m_{\mathfrak{p}},j))}}{|\mathfrak{p}|^{(1-1/m_{\mathfrak{p}})/(1-1/\ell)}} \right) \left( 1 - \frac{1}{|\mathfrak{p}|} \right)^{\ell-1} \right), \end{aligned}$$

while if  $m$  is even, this expression should be multiplied by  $2^{r_1}$ . According to Theorem 3.1, we have

$$N_{m,n}(x) = \left( \frac{A\left(\frac{1}{n^2(1-1/\ell)}\right)}{\frac{1}{n^2(1-1/\ell)}\Gamma(\ell-1)} + o(1) \right) x^{\frac{1}{n^2(1-1/\ell)}} (\log x)^{\ell-2} \quad \text{as } x \rightarrow \infty. \quad (8)$$

Comparing Eq. (8) with the definition of  $\delta_{m,n}$  in the statement of the lemma, we see the proof is complete.  $\square$

We now prove Theorem 1.5 from the introduction.

*Proof of Theorem 1.5* We view  $N(x)$  as counting central simple algebras of the form  $M(r, D)$  where  $r = 1$ . To single these out, we make use of the well-known identity  $\sum_{d|r} \mu(d) = 1$  if  $r = 1$  and 0 otherwise. Writing  $\sum_A$  for a sum on central simple algebras  $A$  of dimension  $n^2$ , and  $\sum_A^{(r)}$  for such a sum restricted to  $A$  of the form  $M(r, D)$ , we find that

$$N(x) = \sum_A^{(1)} 1 = \sum_{m|n} \mu(m) \sum_{\substack{r|n \\ m|r}} \sum_A^{(r)} 1.$$

Writing  $r^2 \dim(D) = n^2$ , we see that  $m$  divides  $r$  if and only if  $\dim(D) = d^2$  for divisor  $d$  of  $n/m$ . Hence,

$$\sum_{\substack{r|n \\ m|r}} \sum_A^{(r)} 1 = N_{n/m,n}(x).$$

Putting the last two displays together, we find that

$$N(x) = \sum_{m|n} \mu(m) N_{n/m,n}(x).$$

Replacing  $m$  with  $n/m$  gives the first statement in the lemma. The asymptotic formula (1) with

$$\delta_n = \sum_{m|n} \mu(n/m) \delta_{m,n}$$

now follows from Lemma 3.2.

It remains to show that  $\delta_n > 0$ . Consider first the case when  $n = \ell$  is prime. In that case,  $\delta_n = \delta_{\ell,n} - \delta_{1,n} = \delta_{\ell,n}$ . We used here that  $\delta_{1,n} = 0$  since  $\ell \nmid 1$ .

From Lemma 3.2,  $\delta_{\ell,n}$  is given by a product of nonzero factors together with

$$\prod_{\mathfrak{p} \text{ finite}} \left(1 + \frac{\ell - 1}{|\mathfrak{p}|}\right) \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{\ell-1}.$$

This final product is absolutely convergent and contains only nonzero terms, and so also represents a nonzero real number. This settles the case when  $n = \ell$ .

Now we treat the case of general  $n$ . To prove that  $\delta_n > 0$ , it is enough to construct  $\gg x^{\frac{1}{n^2(1-1/\ell)}} (\log x)^{\ell-2}$  division algebras  $A'/k$  of dimension  $n^2$  with  $|\text{disc}(A')| \leq x$ . The following crude argument suffices for this purpose. Fix (arbitrarily) finite primes  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  of  $k$ . We first count division algebras  $A/k$  of dimension  $\ell^2$  which are unramified at any of  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  and which satisfy  $|\text{disc}(A)| \leq X$ . Without the ramification condition, we have just seen (the case  $n = \ell$ ) that the number of these  $A$  is

$$\gg X^{\frac{1}{\ell^2(1-1/\ell)}} (\log X)^{\ell-2} \quad (9)$$

for large  $X$ . An entirely analogous proof—omitting the factors corresponding to  $\mathfrak{p} = \mathfrak{p}_1, \dots, \mathfrak{p}_n$  from the Euler products appearing previously—shows that this lower bound continues to hold with the restrictions on ramification imposed. Now for each such  $A$ , there is an associated  $n^2$ -dimensional division algebra  $A'/k$  determined by enlarging the set of ramified primes to include  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  and correspondingly enlarging the collection of Hasse invariants to include the numbers  $a_{\mathfrak{p}_i}/m_{\mathfrak{p}_i} = 1/n$ . (Note that the sum of the numbers  $a_{\mathfrak{p}}/m_{\mathfrak{p}}$  for  $\mathfrak{p} \mid \text{Ram}(A')$  is one more than the corresponding sum over  $\mathfrak{p} \mid \text{Ram}(A)$ , so is still an integer.) Clearly, distinct  $A$  correspond to distinct  $A'$ . Moreover,

$$|\text{disc}(A')| = |\mathfrak{p}_1 \cdots \mathfrak{p}_n|^{n^2(1-1/n)} |\text{disc}(A)|^{(n/\ell)^2}.$$

Thus,  $|\text{disc}(A')| \leq x$  precisely when  $|\text{disc}(A)| \leq X$ , where

$$X := (x/|\mathfrak{p}_1 \cdots \mathfrak{p}_n|^{n^2(1-1/n)})^{(\ell/n)^2}.$$

Plugging this value of  $X$  into (9), we see that we have constructed  $\gg x^{\frac{1}{n^2(1-1/\ell)}} (\log x)^{\ell-2}$  division algebras  $A'/k$  of dimension  $n^2$  with  $|\text{disc}(A')| \leq x$ , for all large  $x$ .  $\square$

*Examples 1* The explicit expression for  $\delta_n$  is, in general, exceedingly complicated. However, it can be written fairly compactly in certain special cases. To begin with, suppose that the smallest prime factor  $\ell$  of  $n$  is odd. If  $n = \ell$ , then  $\delta = \delta_{\ell,n}$ , where

$$\delta_{\ell,n} = \frac{\kappa^{\ell-1}}{\ell(\ell-2)!} \frac{1}{(n^2(1-1/\ell))^{\ell-2}} \prod_{\mathfrak{p} \text{ finite}} \left(1 + \frac{\ell-1}{|\mathfrak{p}|}\right) \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{\ell-1}. \quad (10)$$

Next, suppose that  $n = \ell^2$ . Then  $\delta_n = \delta_{\ell^2,\ell^2} - \delta_{\ell,\ell^2}$ . The second term can be calculated with (10), while

$$\begin{aligned} \delta_{\ell^2,\ell^2} &= \frac{\kappa^{\ell-1}}{\ell^2(\ell-2)!} \cdot \frac{1}{(\ell^4(1-1/\ell))^{\ell-2}} \\ &\cdot \left( \prod_{\mathfrak{p} \text{ finite}} \left(1 + \frac{\ell-1}{|\mathfrak{p}|} + \frac{\ell(\ell-1)}{|\mathfrak{p}|^{1+1/\ell}}\right) \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{\ell-1} \right. \\ &\left. + (\ell-1) \prod_{\mathfrak{p} \text{ finite}} \left(1 + \frac{\ell-1}{|\mathfrak{p}|} - \frac{\ell}{|\mathfrak{p}|^{1+1/\ell}}\right) \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{\ell-1} \right). \end{aligned}$$

Finally, suppose that  $n = \ell\ell'$ , where  $\ell'$  is a prime larger than  $\ell$ . Then  $\delta_n = \delta_{\ell\ell',\ell\ell'} - \delta_{\ell,\ell\ell'} - \delta_{\ell',\ell\ell'}$ , where the second and third terms can be computed with (10), and

$$\begin{aligned} \delta_{\ell\ell'} &= \frac{\kappa^{\ell-1}}{\ell\ell'(\ell-2)!} \cdot \frac{1}{(\ell^2\ell'^2(1-1/\ell))^{\ell-2}} \\ &\cdot \left( \prod_{\mathfrak{p} \text{ finite}} \left(1 + \frac{\ell-1}{|\mathfrak{p}|} + \frac{\ell'-1}{|\mathfrak{p}|^{\frac{1-1/\ell'}{1-1/\ell}}} + \frac{\ell(\ell-1)}{|\mathfrak{p}|^{1+1/\ell}}\right) \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{\ell-1} \right. \\ &\left. + (\ell'-1) \prod_{\mathfrak{p} \text{ finite}} \left(1 + \frac{\ell-1}{|\mathfrak{p}|} - \frac{1}{|\mathfrak{p}|^{\frac{1-1/\ell'}{1-1/\ell}}} - \frac{\ell'-1}{|\mathfrak{p}|^{1+1/\ell}}\right) \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{\ell-1} \right). \end{aligned}$$

If  $\ell = 2$ , the same analysis applies, but all of these expressions for  $\delta_n$  must be multiplied by  $2^{r_1}$ .

### 3.2 Proof of Theorem 1.6

In this section, we fix a number field  $k$  and a quaternion algebra  $B$  defined over  $k$  and count the number of quadratic extensions  $L/k$  with norm of relative discriminant less than  $X$  which embed into  $B$ . In what follows, denote by  $\Delta_{L/k}$  the relative discriminant of  $L$  over  $k$ . If  $P$  is any property a quadratic extension of  $k$  may have, we make the definition

$$\mathbf{Prob}(P) := \lim_{x \rightarrow \infty} \frac{\#\{\text{quadratic extensions } L/k \text{ for which } P \text{ holds and } |\Delta_{L/k}| \leq x\}}{\#\{\text{quadratic extensions } L/k \text{ with } |\Delta_{L/k}| \leq x\}}, \quad (11)$$

provided that this limit exists. The next result, which is a special case of results of Wood [84], asserts that for certain properties  $P$  related to splitting behavior, these “probabilities” behave as one might naively expect.

**Proposition 3.3** (Wood) *Fix a finite collection  $S$  of real or finite places of  $k$ . For each  $\mathfrak{p} \in S$ , let  $P_{\mathfrak{p}}$  be one of the properties “ $\mathfrak{p}$  ramifies in  $L$ ”, “ $\mathfrak{p}$  splits in  $L$ ”, or “ $\mathfrak{p}$  is inert in  $L$ ”, subject to the restriction that  $P_{\mathfrak{p}}$  is one of the first two if  $\mathfrak{p}$  is a real place. Then:*

- (i)  $\mathbf{Prob}(P_{\mathfrak{p}})$  exists for each  $\mathfrak{p} \in S$ .
- (ii)  $\mathbf{Prob}(\text{all } P_{\mathfrak{p}} \text{ hold at once}) = \prod_{\mathfrak{p} \in S} \mathbf{Prob}(P_{\mathfrak{p}})$ .
- (iii) If  $\mathfrak{p}$  is real, then  $\mathbf{Prob}(\mathfrak{p} \text{ ramifies}) = \mathbf{Prob}(\mathfrak{p} \text{ splits}) = \frac{1}{2}$ .
- (iv) If  $\mathfrak{p}$  is finite, then  $\mathbf{Prob}(\mathfrak{p} \text{ splits}) = \mathbf{Prob}(\mathfrak{p} \text{ is inert}) = \frac{1}{2}(1 - \mathbf{Prob}(\mathfrak{p} \text{ ramifies}))$ .

It is worth saying a few words about how Proposition 3.3 follows from the more general results of Wood. In Wood’s terminology, we are counting  $\mathbf{Z}/2\mathbf{Z}$ -extensions of  $k$  with local specifications. We note however that Wood’s definition of a local specification differs from our simplified picture above, but only in the sense that it is strictly finer; she allows one to specify the  $k$ -algebra  $L \otimes_k k_{\mathfrak{p}}$ , which gives us more information than we are measuring. When  $G = \mathbf{Z}/2\mathbf{Z}$ , all local specifications are viable (see [84, start of Section 2.2]), and counting by discriminant defines a fair counting function (in the sense of [84, Section 2.1]). The existence of each  $\mathbf{Prob}(P_{\mathfrak{p}})$  in Proposition 3.3 can be seen as a special case of [84, Theorem 2.1]. The independence result follows from [84, Corollary 2.4]. The statement about the splitting behavior of real primes comes from [84, Corollary 2.2], while the statement about the behavior of finite primes is guaranteed by [84, Corollary 2.3].

Theorem 1.6 follows easily from Proposition 3.3 and the following estimate of Datskovsky and Wright [23] for the denominator appearing in the definition (11) (see [21, Section 2.2] for an alternative proof of this proposition).

**Proposition 3.4** *The number of quadratic extensions  $L/k$  with  $|\Delta_{L/k}| \leq x$  is  $\sim \frac{1}{2^{r_2}} \frac{\kappa_k}{\zeta_k(2)} x$  as  $x \rightarrow \infty$ , where  $\kappa_k$  denotes the residue at  $s = 1$  of  $\zeta_k(s)$  and  $r_2$  is the number of pairs of complex embeddings of  $k$ .*

*Deduction of Theorem 1.6* Recall that  $L$  embeds into  $B$  precisely when every prime dividing the discriminant of  $B$  is non-split in  $L$ . The probability that a fixed real prime of  $k$  ramifies in  $L$  is  $\frac{1}{2}$  (from Proposition 3.3(iii)), while

the probability that a fixed finite prime of  $k$  is inert or ramified in  $L$  is (from Proposition 3.3(iv))

$$\frac{1}{2} (1 + \mathbf{Prob}(\mathfrak{p} \text{ ramifies})) \geq \frac{1}{2}.$$

So from Proposition 3.3(ii), the probability that  $L$  embeds into  $B$  exists and is at least  $\frac{1}{2^{r'}}$ , where  $r'$  is the number of distinct places dividing the discriminant of  $B$ . Theorem 1.6 now follows from the estimate of Proposition 3.4.  $\square$

### 3.3 Proof of Theorem 1.7

For a number field  $k$  and a quadratic extension  $L/k$ , our present goal is to count the number of quaternion algebras over  $k$  which have discriminant less than  $x$  and which admit an embedding of  $L$ . In fact, we solve a more general problem. Specifically, in this subsection we prove Theorem 1.7 from the introduction.

#### 3.3.1 Setup

From Theorem 2.1, a quaternion algebra  $B/k$  is uniquely specified by a finite set  $S \subset \mathcal{P}_k$  of real and finite places of  $k$ , along with a reduced fraction  $0 < a_{\mathfrak{p}}/m_{\mathfrak{p}} < 1$  for each prime  $\mathfrak{p} \in S$ , where  $\text{lcm}_{\mathfrak{p} \in S}[m_{\mathfrak{p}}] = 2$  and  $\sum_{\mathfrak{p} \in S} a_{\mathfrak{p}}/m_{\mathfrak{p}} \in \mathbf{Z}$ . The least common multiple condition forces each  $a_{\mathfrak{p}}/m_{\mathfrak{p}} = 1/2$ , and the integrality condition on the sum forces the cardinality of  $S$  to be even. We conclude that there is a bijection between quaternion algebras over  $k$  and square-free moduli  $\mathfrak{m}$  of  $k$  containing a nonzero even number of factors. Moreover, if  $B$  corresponds to  $\mathfrak{m}$  under this bijection, then

$$\text{disc}(B) = \left( \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \mid \mathfrak{m}}} \mathfrak{p} \right)^2 \cdot \prod_{\substack{\mathfrak{p} \text{ real} \\ \mathfrak{p} \mid \mathfrak{m}}} \mathfrak{p}.$$

Now let  $\mathcal{Q}$  be the set of finite or real primes of  $k$  that do not split in any of the  $L_i$ . Asking that all of our quadratic extensions  $L_i$  embed into the quaternion algebra  $B/k$  amounts to requiring that  $\mathfrak{m}$  only be divisible by primes residing in  $\mathcal{Q}$ . We count the number of such  $B$  with  $|\text{disc}(B)| \leq x$  by modifying the approach of the last section. We now provide the details. Define  $G(s) = \frac{1}{2}(G_0(s) + G_1(s))$ , where

$$G_0(s) = \prod_{\substack{\mathfrak{p} \text{ real} \\ \mathfrak{p} \in \mathcal{Q}}} \left( 1 + \frac{1}{|\mathfrak{p}|^s} \right) \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \in \mathcal{Q}}} \left( 1 + \frac{1}{|\mathfrak{p}|^{2s}} \right) \quad (12)$$

and

$$G_1(s) = \prod_{\substack{\mathfrak{p} \text{ real} \\ \mathfrak{p} \in \mathcal{Q}}} \left(1 - \frac{1}{|\mathfrak{p}|^s}\right) \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \in \mathcal{Q}}} \left(1 - \frac{1}{|\mathfrak{p}|^{2s}}\right). \quad (13)$$

The infinite factors in the definitions of  $G_0(s)$  and  $G_1(s)$  are in fact independent of  $s$ . If  $r'_1$  is the number of real primes of  $k$  that do not split in any of the  $L_i$ , the contribution of the infinite factors is given by  $2^{r'_1}$  and  $0^{r'_1}$ , respectively, where

$$0^{r'_1} = \begin{cases} 1, & r'_1 = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Now observe that if  $G(s)$  is identified with its formal Dirichlet series expansion, then the coefficient of  $N^{-s}$  counts quaternion algebras  $B/k$  with  $|\text{disc}(B)| = N$  admitting an embedding of all  $L_i$ .

To estimate the partial sums of the  $G(s)$ -coefficients for  $N \leq x$ , we work with the corresponding sums for  $G_0(s)$  and  $G_1(s)$  individually. For  $G_0(s)$ , we will apply Theorem 3.1 to obtain an asymptotic formula with main term proportional to  $x^{1/2}/(\log x)^{1-\frac{1}{2^r}}$ . We then use a result of Wirsing [83, Satz 2] to show that the partial sums of the  $G_1$ -coefficients are in fact  $o(x^{1/2}/(\log x)^{1-\frac{1}{2^r}})$  as  $x \rightarrow \infty$ . Putting these estimates together yields Theorem 1.7.

### 3.3.2 The partial sums of the coefficients of $G_0(s)$

Let us check that the hypotheses of Theorem 3.1 hold with  $\rho = \frac{1}{2}$  and  $\beta = \frac{1}{2^r}$ . Conditions (i) and (ii) of that theorem are clear from the product definition of  $G_0$ , and so we may focus on (iii) and (iv). Let  $L$  be the composite field of the  $L_i$ , for  $i = 1, 2, \dots, r$ . The essential idea is to express  $G_0(s)$  in terms of benign factors and Artin  $L$ -functions attached to  $\text{Gal}(L/k)$ . We now implement this idea. Our assumption that  $[L_1 \cdots L_r : k] = 2^r$  easily implies that  $\text{Gal}(L/k)$  is canonically isomorphic to the elementary abelian 2-group

$$\bigoplus_{i=1}^r \text{Gal}(L_i/k) = \bigoplus_{i=1}^r \mathbf{Z}/2\mathbf{Z} = (\mathbf{Z}/2\mathbf{Z})^r.$$

For  $1 \leq i \leq r$ , let  $\tilde{\chi}_i$  denote the unique character of  $\text{Gal}(L/k)$  whose kernel is the subgroup fixing  $L_i$ . For every subset  $T$  of  $\{1, \dots, r\}$ , let  $\tilde{\chi}_T = \prod_{i \in T} \tilde{\chi}_i$ . It is a simple matter that  $\tilde{\chi}_T$  is nontrivial provided  $T$  is non-empty. Consequently, the field  $L_T$  left fixed by  $\ker \tilde{\chi}_T$  is a quadratic extension of  $k$  in the event  $T$  is non-empty. For each finite prime  $\mathfrak{p}$  of  $k$ , we let  $\chi_T(\mathfrak{p}) = 1, 0$ , or  $-1$  according to whether  $\mathfrak{p}$  splits, ramifies, or remains inert in  $L_T$ . When  $T$  consists of a

single element  $1 \leq i \leq r$ , we will write  $\chi_i$  instead of the more cumbersome  $\chi_{\{i\}}$ . In that notation, unless  $\mathfrak{p}$  belongs to

$$\mathcal{R} := \{\text{finite primes of } k \text{ that ramify in } L\},$$

we have the expression

$$\chi_T(\mathfrak{p}) = \tilde{\chi}_T(\text{Frob}(\mathfrak{p})) = \prod_{i \in T} \tilde{\chi}_i(\text{Frob}(\mathfrak{p})) = \prod_{i \in T} \chi_i(\mathfrak{p}),$$

where  $\text{Frob}(\mathfrak{p}) \in \text{Gal}(L/k)$  is the associated Frobenius automorphism for  $\mathfrak{p}$ .

Now we relate the  $\chi_i$  to the definition of  $G_0$ . If  $\mathfrak{p}$  is finite and not an element of  $\mathcal{R}$ , then

$$\frac{1}{2^r} \prod_{i=1}^r (1 - \chi_i(\mathfrak{p})) = 1$$

if  $\mathfrak{p} \in \mathcal{Q}$  and = 0 otherwise. Hence, setting  $\mathcal{Q}_0 := \mathcal{Q} \cap \mathcal{R}$ , we have the expression

$$G_0(s) = 2^{r_1'} \prod_{\mathfrak{p} \in \mathcal{Q}_0} \left( 1 + \frac{1}{|\mathfrak{p}|^{2s}} \right) \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \notin \mathcal{R}}} \left( 1 + \frac{\frac{1}{2^r} \prod_{i=1}^r (1 - \chi_i(\mathfrak{p}))}{|\mathfrak{p}|^{2s}} \right). \quad (14)$$

For  $\mathfrak{p} \notin \mathcal{R}$ , we have

$$\prod_{i=1}^r (1 - \chi_i(\mathfrak{p})) = \sum_{T \subset \{1, 2, \dots, r\}} (-1)^{\#T} \chi_T(\mathfrak{p}). \quad (15)$$

For  $\Re(s) > 1/2$ , let

$$\begin{aligned} Z_0(s) := & \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \notin \mathcal{R}}} \left( \left( 1 + \frac{\frac{1}{2^r} \prod_{i=1}^r (1 - \chi_i(\mathfrak{p}))}{|\mathfrak{p}|^{2s}} \right)^{2^r} \right. \\ & \times \left. \prod_{T \subset \{1, 2, \dots, r\}} \left( 1 - \frac{\chi_T(\mathfrak{p})}{|\mathfrak{p}|^{2s}} \right)^{(-1)^{\#T}} \right). \end{aligned}$$

Recalling that  $\log(1 + t) = \sum_{j \geq 1} (-1)^{j-1} t^j / j$  for  $|t| < 1$ , we see that

$$\begin{aligned} \log Z_0(s) &= \sum_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \notin \mathcal{R}}} \sum_{j \geq 1} \left( \frac{(-1)^{j-1}}{j} 2^r \left( \frac{1}{2^r} \prod_{i=1}^r (1 - \chi_i(\mathfrak{p})) \right)^j \right. \\ &\quad \left. - \sum_{T \subset \{1, 2, \dots, r\}} \frac{(-1)^{\#T} \chi_T(\mathfrak{p})^j}{j} \right) |\mathfrak{p}|^{-2js} \\ &= \sum_{\substack{\mathfrak{p}, j \\ \mathfrak{p} \text{ finite}, \mathfrak{p} \notin \mathcal{R} \\ j \geq 2}} \left( \frac{(-1)^{j-1}}{j} 2^r \left( \frac{1}{2^r} \prod_{i=1}^r (1 - \chi_i(\mathfrak{p})) \right)^j \right. \\ &\quad \left. - \sum_{T \subset \{1, 2, \dots, r\}} \frac{(-1)^{\#T} \chi_T(\mathfrak{p})^j}{j} \right) |\mathfrak{p}|^{-2js}. \end{aligned}$$

Here we used (15) to pass from the first line to the second. The final sum is absolutely convergent for  $\Re(s) > \frac{1}{4}$ , and any arrangement of the sum converges uniformly on compact subsets of  $\Re(s) > \frac{1}{4}$ . Thus,  $\log Z_0(s)$  continues analytically to  $\Re(s) > \frac{1}{4}$ , implying that  $Z_0(s)$  can be extended to a function that is analytic and nonzero there.

For each  $T \subset \{1, 2, \dots, r\}$  and all  $s$  with real part greater than 1, put

$$L(s, \chi_T) = \prod_{\substack{\mathfrak{p} \text{ finite}}} \left( 1 - \frac{\chi_T(\mathfrak{p})}{|\mathfrak{p}|^s} \right)^{-1}.$$

$L(s, \chi_T)$  is the Artin  $L$ -function attached to the character  $\tilde{\chi}_T$  of  $\text{Gal}(L/k)$ . When  $T = \emptyset$ , we have  $L(s, \chi_T) = \zeta_k(s)$ , and for all other choices of  $T$ , the function  $L(s, \chi_T)$  is analytic and nonzero for  $\Re(s) \geq 1$ .

We chose  $Z_0(s)$  so that

$$\begin{aligned} &\prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \notin \mathcal{R}}} \left( 1 + \frac{\frac{1}{2^r} \prod_{i=1}^r (1 - \chi_i(\mathfrak{p}))}{|\mathfrak{p}|^{2s}} \right)^{2^r} \\ &= Z_0(s) \prod_{T \subset \{1, 2, \dots, r\}} \left( L(2s, \chi_T) \prod_{\mathfrak{p} \in \mathcal{R}} \left( 1 - \frac{\chi_T(\mathfrak{p})}{|\mathfrak{p}|^{2s}} \right) \right)^{(-1)^{\#T}}. \end{aligned}$$

The right-hand products over  $\mathfrak{p} \in \mathcal{R}$  are analytic and nonzero for  $\Re(s) > 0$ . Keeping in mind that  $L(s, \chi_T)$  is analytic and nonzero for  $\Re(s) \geq 1$  as long as  $T \neq \emptyset$ , we see that the expression

$$\left(s - \frac{1}{2}\right) Z_0(s) \prod_{T \subset \{1, 2, \dots, r\}} \left( L(2s, \chi_T) \prod_{\mathfrak{p} \in \mathcal{R}} \left(1 - \frac{\chi_T(\mathfrak{p})}{|\mathfrak{p}|^{2s}}\right) \right)^{(-1)^{\#T}} \quad (16)$$

is analytic and nonzero for  $\Re(s) \geq \frac{1}{2}$ . We note for the reader that the factor of  $s - \frac{1}{2}$  here is used to cancel the simple pole of  $\zeta_k(2s)$  at  $s = \frac{1}{2}$ . A function which is nonzero and analytic on a simply connected domain possesses an analytic logarithm on the same domain, and hence also an analytic  $N$ th root for every  $N$ . (See, e.g., [74, Theorem 13.11, p. 274].) In particular, we can extract a  $2^r$ th root  $H_0(s)$  of (16) which is also analytic and nonzero in  $\Re(s) \geq \frac{1}{2}$ . The choice of  $H_0$  is uniquely specified if we insist that  $H_0(s) > 0$  for  $s > \frac{1}{2}$ . Referring back to (14), we find that for  $\Re(s) > \frac{1}{2}$ ,

$$G_0(s) = \frac{1}{(s - \frac{1}{2})^{1/2^r}} \left( 2^{r'_1} \cdot \prod_{\mathfrak{p} \in \mathcal{D}_0} \left(1 + \frac{1}{|\mathfrak{p}|^{2s}}\right) \cdot H_0(s) \right),$$

where  $(s - \frac{1}{2})^{1/2^r}$  is the principal  $2^r$ th root. This immediately implies (iii). If we let

$$A_0(s) := 2^{r'_1} \cdot \prod_{\mathfrak{p} \in \mathcal{D}_0} \left(1 + \frac{1}{|\mathfrak{p}|^{2s}}\right) \cdot H_0(s),$$

we see that  $G_0(s)$  satisfies (iv) with  $\rho = \frac{1}{2}$ ,  $\beta = \frac{1}{2^r}$ ,  $A(s) = A_0(s)$ , and  $B(s) = 0$ .

So by Theorem 3.1, the sum up to  $x$  of the coefficients of  $G_0(s)$  is asymptotic to

$$\frac{A_0\left(\frac{1}{2}\right)}{\frac{1}{2}\Gamma\left(\frac{1}{2^r}\right)} x^{\frac{1}{2}} / (\log x)^{1 - \frac{1}{2^r}} \quad \text{as } x \rightarrow \infty.$$

### 3.3.3 The coefficients of $G_1(s)$

We now show that the contribution from the coefficients of  $G_1(s)$  is negligible. Define arithmetic functions  $a(N)$  and  $b(N)$  by expanding

$$\prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \in \mathcal{D}}} \left(1 + \frac{1}{|\mathfrak{p}|^s}\right) = \sum_{N=1}^{\infty} \frac{a(N)}{N^s} \quad \text{and} \quad \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \in \mathcal{D}}} \left(1 - \frac{1}{|\mathfrak{p}|^s}\right) = \sum_{n=1}^{\infty} \frac{b(N)}{N^s}.$$

The functions  $a(N)$  and  $b(N)$  are multiplicative and satisfy  $|b(N)| \leq a(N)$  for all  $N$ . Referring back to the earlier definitions of  $G_0$  and  $G_1$ , we see that the partial sum of the  $G_0(s)$ -coefficients up to  $x$  is given by

$$2^{r_1} \sum_{N \leq \sqrt{x}} a(N),$$

while that of the  $G_1$ -coefficients is given by

$$0^{r_1} \sum_{N \leq \sqrt{x}} b(N).$$

Thus, if we can show that

$$\sum_{N \leq x} b(N) = o \left( \sum_{N \leq x} a(N) \right) \quad \text{as } x \rightarrow \infty, \quad (17)$$

then the partial sums of the  $G_1$ -coefficients are  $o(x^{1/2}/(\log x)^{1-\frac{1}{2r}})$ , as desired. For that task, we use the following result, which is a slight variant of a theorem of Wirsing [83, Satz 2].

**Proposition 3.5** (Wirsing) *Let  $a(N)$  be a multiplicative function taking only nonnegative values. Assume*

- (i) *there is a constant  $\tau > 0$  for which  $\sum_{p \leq x} a(p) \log p = (\tau + o(1))x$  as  $x \rightarrow \infty$ ,*
- (ii)  *$a(p^\ell)$  is bounded uniformly on prime powers  $p^\ell$  with  $\ell \geq 2$ .*

*Let  $b(N)$  be a complex-valued multiplicative function satisfying  $|b(N)| \leq a(N)$  for all  $N$ . Suppose moreover that*

- (iii) *there is a constant  $\tau' \neq \tau$  with  $\sum_{p \leq x} b(p) \log p = (\tau' + o(1))x$  as  $x \rightarrow \infty$ ,*

$$\text{then } \sum_{N \leq x} b(N) = o \left( \sum_{N \leq x} a(N) \right).$$

Here we have replaced the original condition (7) in [83, Satz 2] with the simpler condition that  $\tau \neq \tau'$ ; this is justified in the remarks immediately following the statement of Satz 2 in [83]. Wirsing's original formulation also assumes asymptotics for the sums  $\sum_{p \leq x} f(p)$  rather than  $\sum_{p \leq x} f(p) \log p$ . The conditions that Wirsing needs follow from our (i), (iii) after applying partial summation. (A similar partial summation argument can be seen in the second displayed equation in the proof of Theorem 4.4 on p. 79 of [1].)

These remarks allow us to replace condition (7) in [83, Satz 2] with the simpler condition that  $\tau \neq \tau'$ . We now return to deducing (17).

*Proof of (17)* Let us check that the hypotheses of Proposition 3.5 are satisfied for our choice of  $a(N)$  and  $b(N)$  above. We have

$$\begin{aligned} \sum_{p \leq x} a(p) \log p &= \sum_{p \leq x} \left( \sum_{\substack{\mathfrak{p} \in \mathcal{Q}, \text{ finite} \\ |\mathfrak{p}| = p}} \log |\mathfrak{p}| \right) = \sum_{\substack{\mathfrak{p} \in \mathcal{Q}, \text{ finite} \\ \mathfrak{p} \text{ abs. degree 1} \\ |\mathfrak{p}| \leq x}} \log |\mathfrak{p}| \\ &= \sum_{\substack{\mathfrak{p} \in \mathcal{Q}, \text{ finite} \\ |\mathfrak{p}| \leq x}} \log |\mathfrak{p}| + O(x^{1/2}). \end{aligned}$$

Now  $\mathfrak{p} \in \mathcal{Q}$  if and only if  $\mathfrak{p}$  does not split in any of the  $L_i$ . Excluding the finitely many primes in  $\mathcal{R}$ , this condition on  $\mathfrak{p}$  is equivalent to the requirement that  $\text{Frob}(\mathfrak{p})$  not restrict to the identity on  $L_i$  for any  $i = 1, 2, \dots, r$ . Recalling that

$$\text{Gal}(L/k) \cong \prod_{i=1}^r \text{Gal}(L_i/k),$$

we see that this condition uniquely determines  $\text{Frob}(\mathfrak{p})$ . Since  $\#\text{Gal}(L/k) = 2^r$ , we can apply partial summation along with the Chebotarev density theorem for natural density (see [2, Satz 4]) to obtain

$$\sum_{\substack{\mathfrak{p} \in \mathcal{Q}, \text{ finite} \\ |\mathfrak{p}| \leq x}} \log |\mathfrak{p}| = \left( \frac{1}{2^r} + o(1) \right) x \quad \text{as } x \rightarrow \infty.$$

(An analogous partial summation argument appears in the first displayed equation in the proof of Theorem 4.4 on p. 79 of [1]; we use the Chebotarev prime counting function from [2, Satz 4] in lieu of  $\pi(x)$ .) So (i) holds with  $\tau = \frac{1}{2^r}$ .

For each prime power  $p^\ell$ ,

$$a(p^\ell) \leq \# \left\{ \text{square-free ideals of } \mathcal{O}_k \text{ of norm } p^\ell \right\}.$$

However, any square-free ideal of norm  $p^\ell$  must be a square-free product of the primes lying above  $p$ , and there are at most  $2^{[k:\mathbb{Q}]}$  such products. This gives (ii).

Finally, our work towards (i) shows that

$$\sum_{p \leq x} b(p) \log p = - \sum_{p \leq x} \sum_{\substack{\mathfrak{p} \in \mathcal{Q}, \text{ finite} \\ |\mathfrak{p}| = p}} \log |\mathfrak{p}| = - \left( \frac{1}{2^r} + o(1) \right) x \quad \text{as } x \rightarrow \infty.$$

Hence, (iii) holds with  $\tau' = -\frac{1}{2^r}$ .  $\square$

### 3.3.4 Denouement

Since  $G(s) = \frac{1}{2}(G_0(s) + G_1(s))$ , combining the results of the previous two sections shows that the number of quaternion algebras  $B/k$  admitting embeddings of all of the  $L_i$  and having  $|\text{disc}(B)| \leq x$ , is asymptotically

$$\frac{A_0\left(\frac{1}{2}\right)}{\Gamma\left(\frac{1}{2^r}\right)} \cdot x^{1/2} / (\log x)^{1-\frac{1}{2^r}}.$$

The leading coefficient here is nonzero and can be given explicitly in terms of the leading terms in the Laurent series expansions for the functions  $L(s, \chi_T)$ . Specifically, tracing back through the definitions, we see that with  $\kappa$  equal to the residue at  $s = 1$  of  $\zeta_k(s)$ ,

$$\begin{aligned} \frac{A_0\left(\frac{1}{2}\right)}{\Gamma\left(\frac{1}{2^r}\right)} &= \frac{2^{r_1' - \frac{1}{2^r}}}{\Gamma\left(\frac{1}{2^r}\right)} \prod_{\mathfrak{p} \in \mathcal{Q}_0} \left(1 + \frac{1}{|\mathfrak{p}|}\right) \\ &\cdot \left( \kappa \prod_{\mathfrak{p} \in \mathcal{R}} \left(1 - \frac{1}{|\mathfrak{p}|}\right) \prod_{\substack{T \subset \{1, 2, \dots, r\} \\ T \neq \emptyset}} \left( L(1, \chi_T) \prod_{\mathfrak{p} \in \mathcal{R}} \left(1 - \frac{\chi(\mathfrak{p})}{|\mathfrak{p}|}\right) \right)^{(-1)^{\#T}} \right)^{1/2^r} \\ &\cdot Z^{1/2^r}, \end{aligned}$$

where

$$\begin{aligned} Z := Z_0\left(\frac{1}{2}\right) &= \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p} \notin \mathcal{R}}} \left( \left(1 + \frac{\frac{1}{2^r} \prod_{i=1}^r (1 - \chi_i(\mathfrak{p}))}{|\mathfrak{p}|}\right)^2 \right. \\ &\times \left. \prod_{T \subset \{1, 2, \dots, r\}} \left(1 - \frac{\chi_T(\mathfrak{p})}{|\mathfrak{p}|}\right)^{(-1)^{\#T}} \right). \end{aligned}$$

It is clear that in general, the explicit form of this leading coefficient is rather complicated, but in the case  $r = 1$  it simplifies nicely to the formula given in Example 1.

*Remark* Without the assumption that  $[L_1 \cdots L_r : k] = 2^r$ , it is possible for there to be *no* quaternion division algebras  $B/k$  into which all of the  $L_i$  embed. For example, take  $k = \mathbf{Q}$  and consider the collection of  $L_i$  given by  $\mathbf{Q}(\sqrt{-3})$ ,  $\mathbf{Q}(\sqrt{-1})$ ,  $\mathbf{Q}(\sqrt{3})$ ,  $\mathbf{Q}(\sqrt{10})$ ,  $\mathbf{Q}(\sqrt{17})$ . One can check that every finite prime of  $\mathbf{Q}$  splits in at least one of these  $L_i$ , and so a quaternion algebra into which all of these fields embeds must have a discriminant not divisible by any finite prime at all. As a quaternion algebra must ramify at a finite even number of primes, up to isomorphism, the only quaternion algebra admitting embeddings of all of the above extensions is  $M(2, \mathbf{Q})$ , which is not a division algebra.

For the general situation, we proceed as follows. Suppose we are given a finite collection of distinct quadratic extensions  $L_i/k$ . Let  $L$  be the compositum of all of the  $L_i$ , and define  $r$  by the condition  $[L : k] = 2^r$ . Note, we are not assuming here that  $r$  is the total number of  $L_i$ . For each  $i$ , let  $\tilde{\chi}_i$  be the character of  $\text{Gal}(L/k)$  whose kernel is the subgroup fixing  $L_i$ . For there to be infinitely many quaternion algebras  $B/k$  into which all of the  $L_i$  embed, it is necessary and sufficient that there is no finite odd order subset of the  $\tilde{\chi}_i$  which multiply to the identity. If this condition holds, then the number of  $B/k$  with  $|\text{disc}(B)| \leq x$  into which all of the  $L_i$  embed is again asymptotic to  $\delta x^{1/2}/(\log x)^{1-\frac{1}{2^r}}$  for some positive  $\delta > 0$ . This can be established by slight modifications to the proof of Theorem 1.7.

## 4 Main tools: geometric counting results

In this section, we derive the geometric counting results from the introduction using the tools from the previous section.

### 4.1 Proof of Corollaries 1.8 and 1.9

As an application of Theorem 1.5 we consider the problem of counting commensurability classes of arithmetic hyperbolic 2- and 3-manifolds with a fixed trace field  $k$ . As Selberg's lemma ensures every complete, finite volume hyperbolic  $n$ -orbifold has a finite manifold cover, counting commensurability classes of arithmetic orbifolds is the same as counting commensurability classes of arithmetic manifolds. Consequently, we will not fret about whether our representatives are manifolds or orbifolds. It is well-known [54, Chapter 11] that given such a commensurability class  $\mathcal{C}$ , there is a real number  $V_{\mathcal{C}} > 0$  which occurs as the smallest volume achieved by an orbifold belonging to this class. A consequence of Borel's classification of maximal arithmetic Fuchsian and

Kleinian groups and their volumes [7] is that we can derive a precise formula for  $V_{\mathcal{C}}$  in terms of the number theoretic invariants of  $\mathcal{C}$ . The proofs of Corollary 1.8 and Corollary 1.9 will rely crucially on Theorem 2.6. Namely, every commensurability class of arithmetic hyperbolic 2- or 3-manifolds both determines and is determined by the associated trace field and quaternion algebra.

We begin by proving a lemma which bounds the norm of the discriminant of the quaternion algebra of a compact arithmetic hyperbolic 2- or 3-manifold as a function of the volume  $V$  of the manifold.

**Lemma 4.1** *Let  $M$  be a compact arithmetic hyperbolic 2-manifold (resp., 3-manifold) of volume  $V$  with trace field  $k$  and quaternion algebra  $B$ . Then  $|\text{disc}(B)| \leq [10^{93}V^{13}]^{10}$  (resp.,  $|\text{disc}(B)| \leq 10^{57}V^7$ ).*

*Proof* We establish the lemma for 3-manifolds as the case of hyperbolic surfaces is similar. Towards that goal, set  $V'$  to be the covolume of a minimal covolume maximal arithmetic subgroup in the commensurability class associated to  $B$  and  $k$ . It is known by Chinburg–Friedman [17, p. 8] that

$$V' = \frac{2\pi^2 \zeta_k(2) d_k^{\frac{3}{2}} \Phi(\text{disc}(B))}{(4\pi^2)^{n_k} [k_B : k]}, \quad (18)$$

where

$$\Phi(\text{disc}(B)) = \prod_{\mathfrak{p} \mid \text{disc}(B)} \left( \frac{|\mathfrak{p}| - 1}{2} \right)$$

and  $k_B$  is the maximal abelian extension of  $k$  which has 2-elementary Galois group, is unramified at all finite primes of  $k$  and in which all (finite) prime divisors of  $\text{disc}(B)$  split completely. As  $k_B$  is contained in the strict class field of  $k$ ,

$$[k_B : k] \leq 2^{r_1(k)} h_k = 2^{n_k - 2} h_k.$$

Let  $\omega_2(B)$  denote the number of prime divisors of  $\text{disc}(B)$  which have norm 2. From the Euler product expansion of  $\zeta_k(s)$ , we deduce that  $\zeta_k(2) \geq (\frac{4}{3})^{\omega_2(B)}$ . In combination with (18), we conclude that

$$V' \geq \frac{(\frac{4}{3})^{\omega_2(B)} d_k^{\frac{3}{2}} |\text{disc}(B)|}{(4\pi^2)^{n_k} 4^{\omega_2(B)} 2^{n_k - 2} h_k} \geq \frac{d_k^{\frac{3}{2}} |\text{disc}(B)|}{(8\pi^2)^{n_k} 3^{\omega_2(B)} h_k}. \quad (19)$$

Now, we have the trivial bound  $\omega_2(B) \leq n_k$  and the inequality  $h_k \leq 242d_k^{\frac{3}{4}}$  found in [45, Lemma 3.1]. Coupling these two inequalities with (19) produces

$$V' \geq \frac{d_k^{\frac{3}{2}} |\text{disc}(B)|}{242(24\pi^2)^{n_k} d_k^{\frac{3}{4}}} \geq \frac{|\text{disc}(B)|}{242(24\pi^2)^{n_k}}. \quad (20)$$

Our proof is now complete upon applying [15, Lemma 4.3], which implies that  $n_k \leq 23 + \log(V')$ , to (20) in tandem with the fact that  $V \geq V'$ .  $\square$

*Proof of Corollary 1.8* Let  $k$  be a totally real number field and  $B$  be a quaternion division algebra over  $k$  which is ramified at all but one real places of  $k$ . If  $\rho: B \rightarrow \text{M}(2, \mathbf{R})$  is a representation and  $\mathcal{O}$  is an order of  $B$ , then it is easy to see that the trace field of  $\Gamma_{\mathcal{O}}$  is  $k$ ; recall that  $\Gamma_{\mathcal{O}}$  is defined to be  $P\rho(\mathcal{O}^1)$ . It is similarly clear that the quaternion algebra of  $\Gamma_{\mathcal{O}}$  is  $B$ . Namely, since this algebra is a quaternion algebra over  $k$  that is visibly contained in  $B$ , the asserted isomorphism follows from comparing dimensions. By definition, a Fuchsian group is arithmetic if it is commensurable with a group of the form  $\Gamma_{\mathcal{O}}$ , hence by Lemma 4.1 and the preceding discussion, to prove Corollary 1.8 it suffices to bound the number of quaternion division algebras  $B$  over  $k$  which are ramified at all real places of  $k$  and satisfy  $|\text{disc}(B)| \leq [10^{93}V^{13}]^{10}$ . The corollary now follows from Theorem 1.5.  $\square$

The proof of Corollary 1.9 is similar and is left to the reader.

## 4.2 Lengths of geodesics arising from quadratic extensions

We begin this subsection with a result that will permit us to work with Kleinian groups derived from a quaternion algebra.

**Proposition 4.2** *Let  $\Gamma$  be a Kleinian group with covolume  $V$  and let  $\Gamma^{(2)}$  be the subgroup of  $\Gamma$  generated by squares. Then there exists an absolute, effectively computable constant  $C$  such that the covolume of  $\Gamma^{(2)}$  is at most  $e^{CV}$ .*

*Proof* It is well-known that as  $\Gamma$  has finite covolume it is finitely generated. Let  $d(\Gamma)$  denote the minimal number of generators of  $\Gamma$ . By Theorem 2.5, there exists an absolute constant  $C$  such that  $d(\Gamma) < C_0 V$ . Now  $\Gamma/\Gamma^{(2)}$  is a finite elementary abelian 2-group of order at most  $2^{d(\Gamma)}$ . As the covolume of  $\Gamma^{(2)}$  is  $[\Gamma : \Gamma^{(2)}] \cdot V$ , the result follows.  $\square$

**Lemma 4.3** *Let  $\Gamma'$  be an arithmetic Fuchsian or Kleinian group derived from a quaternion algebra  $B/k$  which has covolume  $V'$  and is contained in  $\Gamma_{\mathcal{O}}$ , where  $\mathcal{O}$  is a maximal order of  $B$ . Then  $[\Gamma_{\mathcal{O}} : \Gamma] \leq V'$ .*

*Proof* We prove the lemma in the case that  $\Gamma'$  is an arithmetic Kleinian group. The proof in the Fuchsian case is virtually identical. By Borel [7] (see also [54, Chapter 11]), the covolume  $V_{\mathcal{O}}$  of  $\Gamma_{\mathcal{O}}$  is equal to

$$\frac{d_k^{3/2} \zeta_k(2) \prod_{\mathfrak{p} \mid \text{disc}(B)} (|\mathfrak{p}| - 1)}{(4\pi^2)^{n_k - 1}}. \quad (21)$$

As  $V_{\mathcal{O}} \cdot [\Gamma_{\mathcal{O}} : \Gamma'] = V'$  we see that

$$[\Gamma_{\mathcal{O}} : \Gamma] = \frac{V'(4\pi^2)^{n_k - 1}}{d_k^{3/2} \zeta_k(2) \prod_{\mathfrak{p} \mid \text{disc}(B)} (|\mathfrak{p}| - 1)} \leq \frac{V'(4\pi^2)^{n_k - 1}}{d_k^{3/2}}. \quad (22)$$

The discriminant bounds of Odlyzko [64] and Poitou [68] (see also [10, Theorem 2.4]) show that  $\log(d_k) \geq 4r_1 + 6r_2$  where  $r_1$  is the number of real places of  $k$  and  $r_2$  is the number of complex places of  $k$ . It is well-known that in our situation it must be the case that  $k$  has a unique complex place, hence  $r_1 = n_k - 2$  and  $r_2 = 1$ . We conclude that  $d_k^{3/2} \geq e^{6(n_k - 2)} e^9$ . Applying this bound to Eq. (22) and simplifying finishes the proof.  $\square$

*Remark* It is implicit in the statement of Lemma 4.3 and in any event follows from the ideas of the lemma's proof that if  $\mathcal{O}$  is a maximal order of  $B$  then  $\Gamma_{\mathcal{O}}$  has covolume at least 1.

We next need a simple lemma that provides a bound for the regulator of a maximal subfield.

**Lemma 4.4** *Let  $k$  be a number field with a unique complex place,  $B/k$  a quaternion algebra which is ramified at all real places of  $k$  and  $L$  a maximal subfield of  $B$ . Then  $\text{Reg}_L \leq d_L^{n_k}$ .*

*Proof* Let  $r_1(L)$  (resp.,  $r_2(L)$ ) be the number of real (resp., complex) places of  $L$ . As  $L$  embeds into  $B$ , the Albert–Brauer–Hasse–Noether theorem implies that  $r_1(L) = 0$ ,  $r_2(L) = n_k$ . The class number formula [41, p. 300] yields

$\text{Reg}_L = \frac{\omega_L d_L^{\frac{1}{2}} \kappa_L}{(2\pi)^{n_k} h_L}$ , where  $\omega_L$  is the number of roots of unity lying in  $L$ ,  $\kappa_L$  is the residue at  $s = 1$  of the Dedekind zeta function  $\zeta_L(s)$  and  $h_L$  is the class number of  $L$ . As  $h_L \geq 1$ ,  $\omega_L \leq 2n_L^2 = 8n_k^2$  and  $8n^2 \leq (2\pi)^n$  for all  $n \geq 2$ , we see that

$$\text{Reg}_L \leq d_L^{\frac{1}{2}} \kappa_L \leq d_L^{\frac{1}{2}} \log(d_L^{\frac{1}{2}})^{n_L - 1} \leq d_L^{\frac{1}{2}} d_L^{n_k - \frac{1}{2}} = d_L^{n_k},$$

where the second inequality follows from [48, Proposition 2].  $\square$

We will also need the following analog of Lemma 4.4, whose proof is virtually identical to that of Lemma 4.4.

**Lemma 4.5** *Let  $k$  be a totally real number field,  $B/k$  a quaternion algebra which is ramified at all but one real places of  $k$  and  $L$  a maximal subfield of  $B$  which is not totally complex. Then  $\text{Reg}_L \leq d_L^{n_k}$ .*

We briefly survey some basic results about logarithmic heights of algebraic numbers. For a number field  $k$  and  $\mathfrak{p} \in \mathcal{P}_k$ , we normalize the associated valuation  $|\cdot|_{\mathfrak{p}}$  in the usual way so that for each  $\alpha$  in  $k$ , we have

$$\prod_{\mathfrak{p} \mid \infty} |\alpha|_{\mathfrak{p}} = |\text{Norm}_{k/\mathbf{Q}}(\alpha)|$$

and  $\prod_{\mathfrak{p} \in \mathcal{P}_k} |\alpha|_{\mathfrak{p}} = 1$ . We define the logarithmic height of  $\alpha$  relative to  $k$  to be

$$h_k(\alpha) = \sum_{\mathfrak{p} \in \mathcal{P}_k} \log \left( \max \{1, |\alpha|_{\mathfrak{p}}\} \right).$$

The absolute height of  $\alpha$  is  $H(\alpha) = [k : \mathbf{Q}]^{-1} h_k(\alpha)$  and is independent of the field  $k$ . We remark that the height of  $\alpha$  relative to  $\mathbf{Q}(\alpha)$  is the logarithm of the Mahler measure of the minimal polynomial of  $\alpha$ . We also remark that the height of  $\alpha$  can be computed using only infinite places. The proof of the following lemma is straightforward.

**Lemma 4.6** *Let the notation be as above.*

- (i) *For all nonzero  $n \in \mathbf{Z}$ ,  $H(\alpha^n) = |n| \cdot H(\alpha)$ .*
- (ii) *For all algebraic numbers  $\beta$ ,  $H(\alpha\beta) \leq H(\alpha) + H(\beta)$ .*
- (iii) *If  $\alpha$  and  $\beta$  are Galois conjugates then  $H(\alpha) = H(\beta)$ .*

**Proposition 4.7** *Let  $\Gamma$  be an arithmetic Fuchsian or Kleinian group which has covolume  $V$  and with trace field  $k$  and quaternion algebra  $B$ . Let  $L/k$  be a quadratic extension which embeds into  $B$  and suppose further that  $L$  is not totally complex if  $k$  is totally real. Then there exist absolute, effectively computable constants  $C_1, C_2$  such that  $L = k_{\gamma}$  for some hyperbolic  $\gamma \in \Gamma$  with length at most  $e^{C_1 V} d_L^{C_2 + \log(V)}$ .*

*Proof* We prove the proposition in the case that  $k$  has a unique complex place. The case in which  $k$  is totally real has an identical proof. As every real place of  $k$  is ramified in  $B$ , we see that  $L$  embeds into  $B$  implies, by the Albert–Brauer–Hasse–Noether theorem, that  $L$  is totally complex. By Dirichlet’s unit theorem, the  $\mathbf{Z}$ -rank of  $\mathcal{O}_L^*$  is strictly greater than that of  $\mathcal{O}_k^*$ . From this we conclude that every system of fundamental units of  $\mathcal{O}_L^*$  contains a fundamental unit  $u_0 \in \mathcal{O}_L^*$  such that  $u_0^n \notin k$  for any  $n \geq 1$ . Hence, we have  $L = k(u^n)$  for all  $n \neq 0$ . Let  $\sigma$  denote the non-trivial automorphism of  $\text{Gal}(L/k)$  and define  $u = u_0/\sigma(u_0)$ . It is clear that  $\text{Norm}_{L/k}(u) = 1$  and that  $u^n \notin \mathcal{O}_k^*$  for any  $n \geq 1$ .

By [37] (see also [9]) we may take  $u_0$  to have logarithmic height (relative to  $L$ )  $h_L(u_0) \leq n_k^{11n_k} \text{Reg}_L$ . It follows from Lemma 4.6 that  $h_L(u) \leq 2n_k^{11n_k} \text{Reg}_L$ , and since  $[L : \mathbf{Q}] = 2n_k$  we see as well that  $H(u) \leq n_k^{11n_k-1} \text{Reg}_L$ .

As  $\Gamma^{(2)}$  is derived from the quaternion algebra  $B$  [54, Chapter 3], there exists a maximal order  $\mathcal{O}$  of  $B$  such that  $\Gamma^{(2)} \subset \Gamma_{\mathcal{O}}^1$ . Recall that  $k_B$  is the maximal abelian extension of  $k$  of exponent 2 in which all prime divisors of  $\text{disc}(B)$  split completely. We have two cases. Suppose first that  $L \not\subset k_B$ . Then every maximal order of  $B$  admits an embedding of  $\mathcal{O}_k[u]$  ([16, Theorem 3.3]; see also [44, Proposition 5.4]), hence we may assume that  $u \in \mathcal{O}$ . Let  $\gamma'$  be the image in  $\Gamma_{\mathcal{O}}^1$  of  $u$ . Proposition 4.2 and Lemma 4.3 show that  $\gamma = \gamma'^n \in \Gamma^{(2)} \subset \Gamma$  for some  $n \leq e^{C_0 V}$  and constant  $C_0$ . By Lemma 4.6 we have  $H(\gamma) \leq e^{C_0 V} n_k^{11n_k-1} \text{Reg}_L$ . As the logarithm of the Mahler measure of the minimal polynomial of  $\gamma$  is less than  $2n_k H(\gamma)$ , by [54, Lemma 12.3.3] we have  $\ell_0(\gamma) \leq 4e^{C_0 V} n_k^{11n_k} \text{Reg}_L$ . By Lemma 4.4, we have  $\ell_0(\gamma) \leq 4e^{C_0 V} n_k^{11n_k} d_L^{n_k}$ . By [15, Lemma 4.3], we have  $n_k \leq 23 + \log(V)$ . Hence there exists a constant  $C_1$  such that  $\ell_0(\gamma) \leq e^{C_1 V} d_L^{23+\log(V)}$ .

Suppose now that  $L \subset k_B$  and  $\mathcal{E}$  is a maximal order of  $B$  containing  $u$ . By Proposition 2.3 there exists an absolute constant  $C_2 > 0$  and an integer  $n \leq d_L^{C_2}$  such that  $u^n \in \mathcal{O}^1$ . The arguments of the previous paragraph show that there exists  $\gamma \in \Gamma^{(2)} \subset \Gamma$  with length at most  $e^{C_1 V} d_L^{C_2+\log(V)}$ , finishing our proof.  $\square$

*Remark* Proposition 4.7 is an effective version of Theorem 12.2.6 of [54].

### 4.3 Proof of Corollary 1.10

**Theorem 4.8** *Let  $k$  be a number field of degree  $n_k$ , discriminant  $d_k$  that is totally real (resp., has a unique complex place). Let  $B/k$  be a quaternion algebra which is ramified at all but one real places of  $k$  (resp., at all real places of  $k$ ) and let  $\mathcal{O}$  be a maximal order of  $B$ . Then for all sufficiently large  $x$ , the orbifold  $H^2/\Gamma_{\mathcal{O}}$  (resp.,  $H^3/\Gamma_{\mathcal{O}}$ ) contains at least  $\left[ \frac{\kappa_k}{2} \left( \frac{3}{\pi^2} \right)^{n_k} \right] x$  rationally inequivalent geodesics of length at most  $\left[ 2n_k^{11n_k-1} d_k^{2n_k} \right] x^{n_k}$ .*

*Proof* By Theorem 1.6 and the well-known fact that  $\zeta_k(s) \leq \zeta(s)^{n_k}$ , for all sufficiently large real  $x > 0$  there are at least  $\left[ 2\kappa_k \left( \frac{3}{\pi^2} \right)^{n_k} \right] x$  quadratic extensions  $L/k$  which embed into  $B$  and satisfy  $|\Delta_{L/k}| < x$ . When  $k$  is totally real, if an extension  $L/k$  embeds into  $B$  then  $L$  is either totally complex or else has 2 real places and  $n_k - 2$  complex places. Combining Theorem 1.6 with Proposition 3.3(iii) now shows that when  $k$  is totally real there are at least  $\left[ \kappa_k \left( \frac{3}{\pi^2} \right)^{n_k} \right] x$  quadratic extensions  $L/k$  which embed into  $B$ , satisfy

$|\Delta_{L/k}| < x$ , and are not totally complex. The proof of Proposition 4.7 shows that with at most finitely many exceptions, the extensions described above are all of the form  $L = k\gamma$ , where  $\gamma \in \Gamma_{\mathcal{O}}$  is hyperbolic with length at most  $2n_k^{11n_k-1} \text{Reg}_L$ . By [18, Lemma 6.3], if  $\lambda_1, \lambda_2$  are eigenvalues of hyperbolics  $\gamma_1, \gamma_2 \in \Gamma_{\mathcal{O}}$  whose complex lengths are rationally equivalent then either  $k(\lambda_1) = k(\lambda_2)$  or  $k(\lambda_1) = k(\overline{\lambda_2})$ . It follows that for  $x$  sufficiently large, at least  $\left[ \frac{\kappa_k}{2} \left( \frac{3}{\pi^2} \right)^{n_k} \right] x$  of the geodesics associated to the hyperbolic  $\gamma$  are rationally inequivalent. The theorem now follows from Lemma 4.4 and  $d_L = |\Delta_{L/k}| d_k^2$ .  $\square$

*Proof of Corollary 1.10* By Proposition 4.2 (which follows from Gauss–Bonnet when  $\Gamma$  is a Fuchsian group) the covolume of  $\Gamma^{(2)}$  is at most  $e^{CV}$  for some absolute, effectively computable constant  $C$ . It is well-known [54, Corollary 8.3.5] that there is a maximal order  $\mathcal{O}$  of  $B$  such that  $\Gamma^{(2)} \leq \Gamma_{\mathcal{O}}$ , and it was shown in Lemma 4.3 that the index of  $\Gamma^{(2)}$  in  $\Gamma_{\mathcal{O}}$  is at most  $e^{CV}$ . It follows immediately from Theorem 4.8 that for  $x$  sufficiently large, the orbifold  $\mathbf{H}^3/\Gamma$  contains at least  $\left[ \frac{\kappa_k}{2} \left( \frac{3}{\pi^2} \right)^{n_k} \right] x$  rationally inequivalent geodesics of length at most  $e^{CV} (2n_k^{11n_k-1} d_k^{2n_k}) x^{n_k}$ . The corollary now follows from  $n_k \leq 23 + \log(V)$  [15, Lemma 4.3],  $d_k \leq V^{22}$  [45, proof of Thm 4.1], and logarithm inequalities.  $\square$

#### 4.4 Counting manifolds with prescribed geodesic lengths

Let  $M$  be an arithmetic hyperbolic 2-orbifold (resp., 3-orbifold) with  $\pi_1(M) = \Gamma$  that has geodesics with lengths (resp., complex length)  $\ell_1, \dots, \ell_N$ . For  $V > 0$ ,  $N_{\ell_1, \dots, \ell_N}^2(V)$  (resp.,  $N_{\ell_1, \dots, \ell_N}^3(V)$ ) is the maximum cardinality of a family of arithmetic, pairwise non-commensurable, hyperbolic 2-orbifolds (resp., 3-orbifolds) all of which have geodesics with lengths (resp., complex lengths)  $\ell_1, \dots, \ell_N$  and volume at most  $V$ . By Borel [7, Theorem 8.2], both  $N_{\ell_1, \dots, \ell_N}^2(V), N_{\ell_1, \dots, \ell_N}^3(V)$  finite. As an application of Theorem 1.7 we provide lower and upper bounds for these functions. [47] establish estimates for similarly defined counting functions.

Before proceeding, we fix some notation which we will use for the remainder of this section. With  $\ell_1, \dots, \ell_N$  as above, let  $\gamma_i \in \Gamma$  be hyperbolic with associated geodesic of length  $\ell_i$  and let  $\lambda_i$  denote the eigenvalue of a pre-image of  $\gamma_i$  in  $\text{SL}(2, \mathbf{R}), \text{SL}(2, \mathbf{C})$  satisfying  $|\lambda_i| > 1$ .

We now state our bounds for  $N_{\ell_1, \dots, \ell_N}^2(V)$  and  $N_{\ell_1, \dots, \ell_N}^3(V)$ . Theorem 4.9 deals with the case in which  $\{\lambda_1, \dots, \lambda_N\} \not\subset \mathbf{R}$  and Theorem 4.10 deals with the case in which  $\{\lambda_1, \dots, \lambda_N\} \subset \mathbf{R}$ .

**Theorem 4.9** *Let  $M$  be an arithmetic hyperbolic 3-manifold which is derived from a quaternion algebra and has geodesics with complex lengths  $\ell_1, \dots, \ell_N$ . If  $\lambda_i$  is not real for some  $i$ , then exactly one of the following is true:*

- (i) *There are only finitely many quaternion algebras defined over the trace field  $k$  of  $\Gamma$  which are ramified at all real places of  $k$  and admit embeddings of  $k(\lambda_i)$  for all  $i$ . In this case there are positive real numbers  $c$  and  $V_0$  such that  $N_{\ell_1, \dots, \ell_N}^3(V) = c$  for all  $V > V_0$ .*
- (ii) *There are infinitely many commensurability classes of hyperbolic 3-orbifolds that contain an orbifold that has geodesics with complex lengths  $\ell_1, \dots, \ell_N$ . In this case there exist integers  $1 \leq r, s \leq N$  such that*

$$V/\log(V)^{1-\frac{1}{2^s}} \ll N_{\ell_1, \dots, \ell_N}^3(V) \ll V/\log(V)^{1-\frac{1}{2^r}},$$

where the implicit constants depend only on  $k$  and  $\ell_1, \dots, \ell_N$ .

*Remark* We remark that [18, Lemma 2.3] shows that if  $k$  is not a quadratic extension of  $k^+$  then  $\Gamma$  will have no hyperbolics with real eigenvalue. In this situation the hypotheses of Theorem 4.9 will always be satisfied.

The techniques used to prove Theorem 4.9 can be applied, in much the same manner, to prove the following result.

**Theorem 4.10** *Let  $M$  be an arithmetic hyperbolic 2-manifold (resp., 3-manifold) which is derived from a quaternion algebra and contains geodesics with lengths (resp., complex lengths)  $\ell_1, \dots, \ell_N$ . If  $\lambda_i$  is real for all  $i$ , then exactly one of the following is true:*

- (i) *There are only finitely many quaternion algebras defined over the trace field  $k$  of  $\Gamma$  which are ramified at all but one real places of  $k$  (resp., at all real places of  $k$ ) and admit embeddings of  $k(\lambda_i)$  for all  $i$ .*
- (ii) *There are infinitely many commensurability classes of hyperbolic 2-orbifolds (resp., 3-orbifolds) that contain an orbifold that has geodesics with lengths (resp., complex lengths)  $\ell_1, \dots, \ell_N$  and trace field  $k$ . In this case there exist integers  $1 \leq r, s, t \leq N$  such that*

$$V/\log(V)^{1-\frac{1}{2^r}} \gg N_{\ell_1, \dots, \ell_N}^2(V) \gg V/\log(V)^{1-\frac{1}{2^s}} \\ (\text{resp., } N_{\ell_1, \dots, \ell_N}^3(V) \gg V/\log(V)^{1-\frac{1}{2^t}}).$$

Note that Theorems 4.9 and 4.10 both deal with geodesics on arithmetic hyperbolic 2- and 3-manifolds which are derived from quaternion algebras, as opposed to arbitrary arithmetic hyperbolic 2- and 3-manifolds. The reason for this restriction amounts to the following observation (which will be made more precise and proven as part of the proof of Theorem 4.9). Let  $M$  be as

in Theorem 4.9. The commensurability classes of arithmetic hyperbolic 3-orbifolds that contain an orbifold that has geodesics with complex lengths  $\ell_1, \dots, \ell_N$  are in one-to-one correspondence with quaternion algebras over  $k$  which ramify at all real places of  $k$  and admit embeddings of  $k(\lambda_1), \dots, k(\lambda_N)$ . This correspondence breaks down however, when the manifold  $M$  is arithmetic but not necessarily derived from a quaternion algebra. In this more general setting however, we are able to prove the following.

**Theorem 4.11** *Let  $M$  be an arithmetic hyperbolic 2-manifold (resp., 3-manifold) that has geodesics with lengths (resp., complex lengths)  $\ell_1, \dots, \ell_N$ . If there are infinitely many primes of  $k$  which do not split in any of the extensions  $k(\lambda_i)/k$  then there are infinitely many commensurability classes of hyperbolic 2-orbifolds (resp., 3-orbifolds) that contain an orbifold that has geodesics with lengths (resp., complex lengths)  $\ell_1, \dots, \ell_N$ .*

*Remark* If there are only finitely many primes of  $k$  which do not split in any of the extensions  $k(\lambda_i)/k$ , then there are at most finitely many commensurability classes of hyperbolic 2- or 3-orbifolds that contain an orbifold that has geodesics with (complex) lengths  $\ell_1, \dots, \ell_N$  and trace field  $k$ . In many situations however (for instance if  $M$  is a 2- or 3-manifold such that  $\{\lambda_1, \dots, \lambda_N\} \not\subset \mathbf{R}$ ), any arithmetic hyperbolic 2-orbifold (resp., 3-orbifold) that has geodesics with lengths (resp., complex lengths)  $\ell_1, \dots, \ell_N$  must have trace field  $k$ . See for instance Proposition 4.13 and [18, Lemma 2.3]. In these situations the hypothesis in Theorem 4.11 is necessary and sufficient.

#### 4.4.1 Proof of Theorem 4.9

We begin with a proposition that will be needed in the proof of Theorem 4.9.

**Proposition 4.12** *Let  $B/k$  be a quaternion algebra which admits embeddings of  $k(\lambda_1), \dots, k(\lambda_N)$  and  $\mathcal{O} \subset B$  be a maximal order. If  $\text{Ram}_f(B) \neq \emptyset$ , then the orbifold associated to  $\Gamma_{\mathcal{O}}$  has geodesics with (complex) lengths  $\ell_1, \dots, \ell_N$ .*

*Proof* For each  $i = 1, \dots, N$ , fix a quadratic  $\mathcal{O}_k$ -order  $\Omega_i \subset k(\lambda_i)$  which contains a pre-image in  $k(\lambda_i)$  of  $\gamma_i$ . As  $B$  ramifies at a finite prime of  $k$ , by [16, Theorem 3.3], every maximal order of  $B$ , in particular  $\mathcal{O}$ , contains a conjugate of all of the quadratic orders  $\Omega_i$ . The proposition now follows from the fact that the (complex) length of the geodesic associated to  $\gamma_i$  coincides with the (complex) length of the geodesic associated to any conjugate of  $\gamma_i$ .  $\square$

*Proof of Theorem 4.9* Let  $k, B$  denote the trace field and quaternion algebra of  $\Gamma$  and for  $i = 1, \dots, N$ , let  $L_i$  denote the quadratic extension  $k(\lambda_i)$  of  $k$ . By hypothesis there exists an  $i$  such that  $\lambda_i \notin \mathbf{R}$ . By [18, Lemma 2.3],

the image in  $\mathbf{C}$  of  $k$  is  $\mathbf{Q}(\text{tr}(\gamma_i)) = \mathbf{Q}(\lambda_i + \lambda_i^{-1})$ . Throughout the remainder of this proof we will identify  $k$  with its image in  $\mathbf{C}$ . Suppose that  $\Gamma'$  is an arithmetic Kleinian group such that the quotient orbifold has geodesics with complex lengths  $\ell_1, \dots, \ell_N$ . Taking powers of the elements  $\gamma_i$  as needed, we may assume that  $\Gamma'$  is derived from a quaternion algebra. Let  $k', B'$  denote the trace field and quaternion algebra of  $\Gamma'$ . By (3), if  $\gamma'_i \in \Gamma'$  is hyperbolic with associated geodesic of complex length  $\ell_i$ , then  $\text{tr}(\gamma_i) = \pm \text{tr}(\gamma'_i)$ . In particular, up to complex conjugation, we have  $k = \mathbf{Q}(\text{tr}(\gamma_i)) = \mathbf{Q}(\text{tr}(\gamma'_i)) = k'$ . We may therefore suppose that  $B'$  is defined over  $k$ . The results of [54, Chapter 12] now imply that  $B'$  admits embeddings of  $L_1, \dots, L_N$ . Conversely, suppose that  $B'/k$  is a quaternion algebra which satisfies the following two conditions:

- (i)  $B'$  is ramified at all real places and at at least one finite prime of  $k$ ,
- (ii)  $B'$  admits embeddings of  $L_1, \dots, L_N$ .

Proposition 4.12 then shows that if  $\mathcal{O}'$  is a maximal order of  $B'$  then  $\Gamma_{\mathcal{O}'}$  is an arithmetic Kleinian group whose quotient orbifold has geodesics with complex lengths  $\ell_1, \dots, \ell_N$ . Putting these together, we see that  $N_{\ell_1, \dots, \ell_N}(V)$  is asymptotic to the number of isomorphism classes of quaternion algebras over  $k$  which are ramified at all real places of  $k$  and which admit embeddings of  $L_1, \dots, L_N$ . (Note that all but finitely many quaternion algebras over  $k$  ramify at a finite prime of  $k$ .) The first assertion is an immediate consequence of this.

In order to prove the second assertion we first show that  $N_{\ell_1, \dots, \ell_N}^3(V) \ll V/\log(V)^{1-\frac{1}{2r}}$  for some  $1 \leq r \leq N$ . Suppose that  $\Gamma'$  is an arithmetic Kleinian group whose quotient orbifold has geodesics with complex lengths  $\ell_1, \dots, \ell_N$  and let  $V'$  denote the covolume of  $\Gamma'$ . If we let  $V_{\mathcal{C}}$  denote the volume of a minimal volume orbifold in the commensurability class  $\mathcal{C}$  of  $\Gamma$ , then  $V' \geq V_{\mathcal{C}}$ . Borel's formula [7] for  $V_{\mathcal{C}}$  makes it clear that there exists a constant  $c$ , which depends on  $k$ , such that  $V_{\mathcal{C}} \geq c|\text{disc}(B')|$  where  $B'$  is the quaternion algebra of  $\Gamma'$  and  $|\text{disc}(B')|$  the norm of its discriminant. It follows from the discussion above that  $B'$  is defined over  $k$  and it is clear that  $B'$  admits embeddings of  $L_1, \dots, L_N$ . Hence, the number of commensurability classes of arithmetic hyperbolic 3-orbifolds that contain an orbifold that has geodesics with complex lengths  $\ell_1, \dots, \ell_N$  is at most a constant multiple of the number of quaternion algebras over  $k$  which admit embeddings of  $L_1, \dots, L_N$ . As  $|\text{disc}(B')| \leq cV'$ , that  $N_{\ell_1, \dots, \ell_N}^3(V) \ll V^{1/2}/\log(V)^{1-\frac{1}{2r}}$  for some  $1 \leq r \leq N$  now follows from Theorem 1.7. The proof that  $N_{\ell_1, \dots, \ell_N}^3(V) \gg V/\log(V)^{1-\frac{1}{2s}}$  for some  $1 \leq s \leq N$  follows from the same ideas though applied to orbifolds of the form considered in Proposition 4.12.  $\square$

#### 4.4.2 Remarks about the proof of Theorem 4.10

The proof of Theorem 4.10 follows from the same arguments that were used to prove the analogous statements in Theorem 4.9, hence we omit it. We do, however, record the following proposition which serves as a substitute for Lemma 2.3 of [18] in the Fuchsian case.

**Proposition 4.13** *Let  $\Gamma$  be an arithmetic Fuchsian group derived from a quaternion algebra  $B/k$ . If  $\gamma \in \Gamma$  is a hyperbolic with eigenvalue  $\lambda_\gamma$  then  $k = \mathbb{Q}(\text{tr}(\gamma))$ .*

*Proof* Let  $\Gamma_0$  be an arithmetic Kleinian group derived from a quaternion algebra which contains  $\Gamma$  and whose trace field  $k_0$  is a quadratic extension of  $k$ . Note, the existence of such a group  $\Gamma_0$  follows from the results in [54, Chapter 9]. Set  $F = \mathbb{Q}(\text{tr}(\gamma))$ . Since  $\gamma \in \Gamma_0$  and  $\lambda_\gamma \in \mathbb{R}$ , [18, Lemma 2.3] shows that  $[k_0 : F] = 2$  and that  $F$  is the maximal totally real subfield of  $k_0$ . It is now clear that  $F = k$ , completing the proof.  $\square$

We now make a few comments about why the techniques used to prove Theorem 4.9 do not suffice to prove an upper bound for  $N_{\ell_1, \dots, \ell_N}^3(V)$ . The upper bound for  $N_{\ell_1, \dots, \ell_N}^3(V)$  in Theorem 4.9 relied upon the fact that any arithmetic hyperbolic 3-orbifold that has geodesics with complex lengths  $\ell_1, \dots, \ell_N$  necessarily has  $k$  as its trace field. Hence, it is obtained from counting quaternion algebras over  $k$  admitting embeddings of  $k(\lambda_1), \dots, k(\lambda_N)$ . Whereas this is the case for arithmetic Fuchsian groups by Proposition 4.13, it is not necessarily the case for 3-orbifolds in the context of Theorem 4.10. Indeed, let  $k^+$  denote the maximal totally real subfield of  $k$  and assume that  $k$  is a quadratic extension of  $k^+$ . Lemma 2.3 of [18] shows that  $k = \mathbb{Q}(\text{tr}(\gamma_i))$  if  $\lambda_i$  is not real and  $k^+ = \mathbb{Q}(\text{tr}(\gamma_i))$  if  $\lambda_i$  is real. As a consequence the trace field of an arithmetic hyperbolic 3-orbifold that has geodesics with complex lengths  $\ell_1, \dots, \ell_N$  is a quadratic extension of  $k^+$ . This does not imply that this trace field is equal to  $k$ . In theory one could obtain an upper bound for  $N_{\ell_1, \dots, \ell_N}^3(V)$  by counting the number of quadratic extensions of  $k^+$  with norm of relative discriminant less than some bound and having a unique complex place and then multiplying this count by the number of quaternion algebras defined over each field. The former count has been computed by Cohen–Diaz–Olivier [20, Corollary 3.14]. The latter count is given by Theorem 1.7 and contains a constant which depends on the invariants of the particular quadratic extension of  $k^+$  chosen. It is not clear how one could bound this constant with invariants of only  $k^+$  due to the complexity of this constant. Those invariants also need to be directly related to the volume of the 3-orbifold. Another difficulty is the complexity of the error terms implicit in Theorem 1.7. Specifically, Theorem 1.7 requires that  $x \rightarrow \infty$ , and the rate at which  $x \rightarrow \infty$  that is needed could vary along with the quadratic extension of  $k^+$ .

#### 4.4.3 Proof of Theorem 4.11

We prove the theorem in the case in which  $M$  is a 3-manifold. The surface case has a proof which is virtually identical and thus left to the reader. Let  $\Gamma$  be the fundamental group of  $M$  and  $B$  the associated quaternion algebra. We may assume without loss of generality that  $\Gamma$  is a maximal arithmetic subgroup of  $B^\times/k^\times$  and hence is of the form  $\Gamma = \Gamma_{S,\mathcal{D}}$  (in the notation of [16, Section 4]), where  $S$  is a finite set of primes of  $k$  and  $\mathcal{D}$  is a maximal order of  $B$ . For  $i = 1, \dots, N$ , let  $\bar{y}_i \in \Gamma_{S,\mathcal{D}}$  be a pre-image of  $y_i$  in  $B^\times/k^\times$  and  $y_i \in k(\lambda_i)$  be a pre-image of  $y_i$  in  $B^\times$ . In order to prove the existence of infinitely many pairwise non-commensurable arithmetic hyperbolic 3-orbifolds that contain geodesics with complex lengths  $\ell_1, \dots, \ell_N$ , we first construct an infinite number of quaternion algebras  $B_j/k$  (each of which ramifies at all real places of  $k$ ) with the property that for every  $j$ , the finite part of  $\text{disc}(B)$  is a proper divisor of the finite part of  $\text{disc}(B_j)$ . We will then construct, for every  $j$ , a maximal arithmetic subgroup  $\Gamma_j$  of  $B_j^\times/k^\times$  such that  $\Gamma_j$  contains, for  $i = 1, \dots, N$ , an element with the same trace and norm as  $\bar{y}_i$ . It will follow that the associated orbifold will have geodesics with complex lengths  $\ell_1, \dots, \ell_N$ .

Our construction of the algebras  $B_j$  is straightforward. Let  $\mathfrak{p}_1, \mathfrak{p}_2, \dots$  be an infinite sequence of primes of  $k$  which do not split in any of the extensions  $k(\lambda_i)/k$ . Pruning this sequence as needed, we may assume that none of the primes  $\mathfrak{p}_i$  lie in the finite set  $S$  of primes mentioned in the previous paragraph nor do they divide  $\text{disc}(B)$ . Consider the sequence of moduli  $\{\text{disc}(B)\mathfrak{p}_1\mathfrak{p}_j\}_{j \geq 1}$ . As  $\text{disc}(B)$  must have an even number of divisors, as do the discriminants of all quaternion algebras over number fields, each of these moduli has an even number of divisors. Hence, there exist quaternion algebras  $B_1, B_2, B_3, \dots$  having these as their discriminants and these algebras are pairwise non-isomorphic. Also note that by the Albert–Brauer–Hasse–Noether theorem, the quadratic extension  $k(\lambda_i)/k$  will embed into  $B_j$  if and only if no prime which ramifies in  $B_j$  splits in  $k(\lambda_i)/k$ . As the extension  $k(\lambda_i)/k$  embeds into  $B$ , none of the divisors of  $\text{disc}(B)$  split in any of the extensions  $k(\lambda_i)/k$ . Further, by hypothesis no prime in the sequence  $\mathfrak{p}_1, \mathfrak{p}_2, \dots$  splits in any of the extensions  $k(\lambda_i)/k$ . We conclude that all of the algebras  $B_j$  admit embeddings of all of the extensions  $k(\lambda_i)/k$ .

To construct the maximal arithmetic subgroups  $\Gamma_j$  of  $B_j^\times/k^\times$ , we need the following result from [16, Theorem 4.4]:

**Theorem 4.14** (Chinburg–Friedman) *Let  $k$  be a number field and  $B/k$  be a quaternion algebra in which at least one archimedean place of  $k$  is unramified. Suppose that  $y \in B^\times$  and consider the maximal arithmetic subgroup  $\Gamma_{S,\mathcal{D}}$  of  $B^\times/k^\times$ . If a conjugate of the image  $\bar{y} \in B^\times/k^\times$  of  $y$  is contained in  $\Gamma_{S,\mathcal{D}}$  then the following three conditions hold:*

- (i)  $\text{disc}(y)/\text{Norm}(y) \in \mathcal{O}_k$ ,
- (ii) If an odd power of  $\mathfrak{p}$  appears in the prime factorization of  $n(y)$  ( $y$  is odd at  $\mathfrak{p}$ ), then  $\mathfrak{p} \in S \cup \text{Ram}_f(B)$ ,
- (iii) For each  $\mathfrak{p} \in S$  at least one of the following four conditions hold:
  - (a)  $y \in k$ ;
  - (b)  $y$  is odd at  $\mathfrak{p}$ ;
  - (c)  $k(y) \otimes_k k_{\mathfrak{p}}$  is not a field;
  - (d)  $\mathfrak{p}$  divides  $\text{disc}(y)/\text{Norm}(y)$ .

Conversely, if conditions (1), (2) and (3) hold, then a conjugate of  $\bar{y}$  is contained in  $\Gamma_{S,\mathcal{D}}$  except possibly when the following three conditions hold:

- (iv)  $k(y) \subset B$  is a quadratic field extension of  $k$ .
- (v) The extension  $k(y)/k$  and the algebra  $B$  are both unramified at all finite primes of  $k$  and ramify at precisely the same (possibly empty) set of real places of  $k$ . Further, all primes  $\mathfrak{p} \in S$  split in  $k(y)/k$ .
- (vi) All primes  $\mathfrak{p}$  dividing  $\text{disc}(y)/\text{Norm}(y)$  split in  $k(y)/k$ .

Suppose now that (1)–(6) hold. In this case the number of  $S$ -types of maximal orders  $\mathcal{D}$  of  $B$  is even and the  $\mathcal{D}$  for which a conjugate  $\bar{y}$  belongs to  $\Gamma_{S,\mathcal{D}}$  comprise exactly half of the  $S$ -types.

We now return to the proof of Theorem 4.11. Fix an integer  $j \geq 1$  and consider the quaternion algebra  $B_j$  defined above. Let  $\mathcal{O} \subset B_j$  be a maximal order and consider the maximal arithmetic subgroup  $\Gamma_j = \Gamma_{S,\mathcal{O}}$  of  $B_j^\times/k^\times$ . As  $B_j$  admits embeddings of  $k(\lambda_i)/k$  for all  $i$ , we abuse notation and identify these extensions with their images in  $B_j$ . We view the  $y_i$  above (in the context of the algebra  $B$ ) as being contained in  $B_j$ . As the  $y_i$  were all contained in  $\Gamma_{S,\mathcal{D}} \subset B^\times/k^\times$ , we see by Theorem 4.14 (and because  $B_j$  ramifies at a finite prime of  $k$ , hence condition (5) of Theorem 4.14 is not satisfied, and  $\text{Ram}_f(B) \subset \text{Ram}_f(B_j)$ ) that conjugates of the  $\bar{y}_i$  lie in  $\Gamma_j \subset B_j^\times/k^\times$ . Theorem 4.11 follows.

## 5 Proof of Theorem 1.1

### 5.1 A technical lemma

Let  $k$  be a number field of degree  $n_k$  with integral basis  $\Omega = \{\omega_1, \dots, \omega_{n_k}\}$ . We endow  $\mathcal{O}_k$  with the  $T_2$ -norm by setting  $T_2(x) = \sum_{\sigma:k \hookrightarrow \mathbb{C}} |\sigma(x)|^2$ . An immediate consequence of the arithmetic-geometric mean inequality is that  $T_2(x) \geq n_k$  for all  $x \neq 0$ . Define

$$B(\Omega) = \prod_{\sigma:k \hookrightarrow \mathbb{C}} \sum_{i=1}^{n_k} |\sigma(\omega_i)|.$$

**Lemma 5.1** *Let  $k$  be a number field of degree  $n_k \geq 2$ . Then  $B(\Omega) \leq 2^{n_k^3} d_k^{n_k}$ .*

*Proof* The proof follows from the following inequalities:

$$\begin{aligned} B(\Omega) &= \prod_{\sigma: k \hookrightarrow \mathbb{C}} \sum_{i=1}^{n_k} |\sigma(\omega_i)| \leq \prod_{\sigma: k \hookrightarrow \mathbb{C}} \sum_{i=1}^{n_k} T_2(\omega_i) \leq \prod_{\sigma: k \hookrightarrow \mathbb{C}} \prod_{i=1}^{n_k} T_2(\omega_i) \\ &\leq \prod_{\sigma: k \hookrightarrow \mathbb{C}} \left( 2^{n_k^2} d_k \right) \leq 2^{n_k^3} d_k^{n_k}, \end{aligned}$$

where the second to last inequality follows from [66, Theorem 3].  $\square$

## 5.2 Geodesics of bounded length arising from maximal subfields

**Proposition 5.2** *Let  $\Gamma$  be an arithmetic Kleinian group with trace field  $k$ , quaternion algebra  $B$ , and covolume  $V$ . Then there exists a hyperbolic  $\gamma \in \Gamma$  with eigenvalue  $\lambda = \lambda_\gamma$  such that  $\lambda^n$  is not real for any  $n \geq 1$  and  $\gamma$  has length at most  $Ke^{(\log(V)\log(V))}$  for some absolute constant  $K$ .*

*Proof* To begin, we make effective an argument from [18, p. 10]. We start by proving the existence of a hyperbolic  $\gamma \in \Gamma$  with eigenvalue  $\lambda$  such that  $\lambda^n$  is not real for any  $n > 1$  and has length at most  $e^{C_1 V} d_L^{C_2 + \log(V)}$ . We first consider the case in which  $k/k^+$  is a quadratic extension. By the Chebotarev density theorem, there are infinitely many rational primes  $p$  which split completely in  $k/\mathbb{Q}$  and do not divide  $|\text{disc}(B)|$ . To obtain an upper bound we use a modification [81, Theorem 2-C] of the bound on the least prime ideal in the Chebotarev density theorem in [40]:

**Theorem 5.3** (Wang) *Let  $L/k$  be a finite Galois extension of number fields of degree  $n$ ,  $S$  a finite set of primes of  $K$  and  $[\theta]$  a conjugacy class in  $\text{Gal}(L/k)$ . Then there is a prime ideal  $\mathfrak{p}$  of  $K$  such that*

- (i)  $\mathfrak{p}$  is unramified in  $L$  and is of degree 1 over  $\mathbb{Q}$ ;
- (ii)  $\mathfrak{p} \notin S$ ;
- (iii)  $\left( \frac{L/k}{\mathfrak{p}} \right) = [\theta]$ , and
- (iv)  $|\mathfrak{p}| \leq d_L^C (n \log(N_S))^2$ ,

where  $C$  is an absolute, effectively computable constant and  $N_S = \prod_{\mathfrak{q} \in S} |\mathfrak{q}|$ .

We would like to apply Theorem 5.3 to the extension  $k/\mathbb{Q}$  but cannot as  $k/\mathbb{Q}$  need not be Galois. Let  $\widehat{k}$  be the Galois closure of  $k$ . The extension  $\widehat{k}/\mathbb{Q}$  is by definition Galois, has degree at most  $n_k!$ , and has the property that a prime  $p$  of  $\mathbb{Q}$  splits completely in (resp. ramifies in)  $k$  if and only if  $p$  splits completely in (resp. ramifies in)  $\widehat{k}$ . Moreover, Serre [75, Proposition 6] shows

that  $d_{\widehat{k}} \leq d_k^{n_k!-1} n_k!^{n_k!}$ . Let  $p$  be a fixed rational prime which splits completely in  $k$  and does not lie below any prime ramifying in  $B$ . By Theorem 5.3 (applied with  $K = \mathbf{Q}$  and  $L = \widehat{k}$ ), we may assume that

$$p \leq \left[ d_k^{n_k!-1} n_k!^{n_k!} \right]^A \cdot [n_k! \log |\text{disc}(B)|]^2.$$

Let  $\mathfrak{q}^+$  be a fixed prime of  $k^+$  lying above  $\mathfrak{p}$  and  $\mathfrak{q}_1, \mathfrak{q}_2$  be distinct primes of  $k$  lying above  $\mathfrak{q}^+$ . Let  $L/k$  be a quadratic extension which is ramified at every prime divisor of  $\text{disc}(B)$  and furthermore satisfies that  $\mathfrak{q}_1$  ramifies in  $L/k$  and  $\mathfrak{q}_2$  splits in  $L/k$ . Then there exist primes  $\mathfrak{q}'_1, \mathfrak{q}'_2, \mathfrak{q}'_3$  of  $L$  such that  $\mathfrak{q}_1 \mathcal{O}_L = (\mathfrak{q}'_1)^2$  and  $\mathfrak{q}_2 \mathcal{O}_L = \mathfrak{q}'_2 \mathfrak{q}'_3$ . By Proposition 4.7 there exist absolute, effectively computable constants  $C_1, C_2$  such that  $L = k(\lambda(\gamma))$  for some hyperbolic  $\gamma \in \Gamma$  with length at most  $e^{C_1 V} d_L^{C_2 + \log(V)}$ . As the primes  $\mathfrak{q}'_1$  and  $\mathfrak{q}'_2$  both lie above  $\mathfrak{q}^+$  and have different ramification degrees, we can infer that the extension  $L/k^+$  is not Galois, hence  $\lambda(\gamma)$  is not real by [18, Lemma 2.3]. As  $k(\lambda(\gamma)) = k(\lambda(\gamma)^n)$  for all  $n \geq 1$ , our assertion that no power of  $\lambda(\gamma)$  is real follows from an identical argument.

If  $k/k^+$  is not quadratic, then [18, Lemma 2.3] implies that every hyperbolic  $\gamma \in \Gamma$  has a non-real eigenvalue. Therefore, the existence of the needed hyperbolic  $\gamma \in \Gamma$  follows directly from Proposition 4.7.

In light of the above it remains only to bound  $d_L$  in terms of  $V$  and put all of our estimates together. By [81, Theorem 4-A] (see also [82]) we may assume that the conductor  $\mathfrak{f}_{L/k}$  of the extension  $L/k$  satisfies

$$\begin{aligned} |\mathfrak{f}_{L/k}| &\leq 64^{n_k} B(\Omega_k) |\text{disc}(B)|^{2n_k} \cdot \left[ d_k^{n_k!-1} n_k!^{n_k!} \right]^{2A} \cdot [n_k! \log |\text{disc}(B)|]^4 \\ &\leq 64^{n_k} 2^{n_k^3} d_k^{n_k} |\text{disc}(B)|^{2n_k} \cdot \left[ d_k^{n_k!-1} n_k!^{n_k!} \right]^{2A} \cdot [n_k! \log |\text{disc}(B)|]^4, \end{aligned}$$

where the latter inequality follows from Lemma 5.1. The conductor-discriminant formula [63, Chapter VII, (11.9)] and the fact that  $d_L = |\Delta_{L/k}| d_k^2$  implies that

$$d_L \leq 64^{n_k} 2^{n_k^3} d_k^{n_k+2} |\text{disc}(B)|^{2n_k} \cdot \left[ d_k^{n_k!-1} n_k!^{n_k!} \right]^{2A} \cdot [n_k! \log |\text{disc}(B)|]^4.$$

It now follows that

$$\begin{aligned} \ell(\gamma) &\leq e^{C_1 V} \left[ 64^{n_k} 2^{n_k^3} d_k^{n_k+2} |\text{disc}(B)|^{2n_k} \cdot \left[ d_k^{n_k!-1} n_k!^{n_k!} \right]^{2A} \right. \\ &\quad \left. \cdot [n_k! \log |\text{disc}(B)|]^4 \right]^{C_2 + \log(V)}. \end{aligned}$$

In order to bound this expression from above we will make use of the following three inequalities:

- (i)  $n_k \leq 23 + \log(V)$  (proven in [15, Lemma 4.3]),
- (ii)  $d_k \leq V^{22}$  (proven as a part of [45, Theorem 4.1]),
- (iii)  $|\text{disc}(B)| \leq 10^{57} V^7$  (proven in Lemma 4.1).

Substituting in these upper bounds, an elementary computation shows that  $\ell_0(\gamma) \leq C e^{(\log(V)\log(V))}$  for some absolute constant  $C$ . We use here that the term  $n_k!^{n_k!}$  essentially dominates over all of the others and that its size can be estimated using Stirling's formula. The proposition follows.  $\square$

### 5.3 Proof of Theorem 1.3

We begin with a lemma which is needed in the proof of Theorem 1.3.

**Lemma 5.4** *For all  $x > 2$  we have  $\prod_{p \leq x} p \leq e^{\frac{21x}{\log^3(x)} + x}$ .*

Setting  $P(x) = \prod_{p \leq x} p$ ,  $\log(P(x))$  is the Chebyshev theta function and the lemma follows from [27, Theorem 5.2]. We now prove Theorem 1.3 from the introduction.

*Proof of Theorem 1.3* If  $B \not\cong B'$ , interchanging  $B, B'$  if necessary, we may assume that there exists a prime  $\mathfrak{p}$  of  $k$  which ramifies in  $B$  but not in  $B'$ . By hypothesis if  $\mathfrak{p}$  is not real archimedean then  $|\mathfrak{p}| < x$ . Let  $L/k$  be a quadratic extension such that:

- (i)  $[L_{\mathcal{Q}} : k_{\mathfrak{q}}] = 2$  for all primes  $\mathfrak{q}$  of  $k$  with  $|\mathfrak{q}| < x$ ,  $\mathfrak{q} \neq \mathfrak{p}$  and all primes  $\mathcal{Q}$  of  $L$  lying above  $\mathfrak{q}$ ;
- (ii)  $[L_{\mathcal{P}} : k_{\mathfrak{p}}] = 1$  for all primes  $\mathcal{P}$  of  $L$  lying above  $\mathfrak{p}$ ; and
- (iii) all real places of  $k$  not equal to  $\mathfrak{p}$  ramify in  $L/k$ .

The existence of such an extension  $L/k$  follows from the Grunwald–Wang theorem. Using [81, Chapter 4] (see also [82]), we can find such an extension  $L/k$  whose conductor  $\mathfrak{f}_{L/k}$  satisfies

$$|\mathfrak{f}_{L/k}| \leq (32)^{n_k^2} B(\Omega) \left( \prod_{p \leq x} p \right)^{2n_k}. \quad (23)$$

Lemmas 5.1, 5.4, and the conductor-discriminant formula imply that the relative discriminant  $\Delta_{L/k}$  has norm less than the bound given in the theorem's statement. The proof of the theorem now follows from the Albert–Brauer–Hasse–Noether theorem, which implies that  $B'$  admits an embedding of  $L/k$  whereas  $B$  does not.  $\square$

## 5.4 Proof of Theorem 1.1

In this subsection, we prove Theorem 1.1. We start with a proposition.

**Proposition 5.5** *Let  $\Gamma$  be an arithmetic Fuchsian or Kleinian group with trace field  $k$ , quaternion algebra  $B$ , and covolume less than  $V$ . Let  $L/k$  be a quadratic extension which embeds into  $B$ . We additionally suppose that  $L$  is not totally complex in the case that  $\Gamma$  is a Fuchsian group. If  $|\Delta_{L/k}|$  is less than the bound in the statement of Theorem 1.3 (applied with  $X = 10^{930}V^{130}$  if  $\Gamma$  is a Fuchsian group and  $X = 10^{57}V^7$  if  $\Gamma$  is a Kleinian group), then there exists a hyperbolic  $\gamma \in \Gamma$  and absolute, effectively computable constants  $c_1, c_2$  such that  $L = k(\lambda(\gamma))$  and  $\ell_0(\gamma) \leq c_1 e^{c_2 \log(V)^{\alpha}}$ , where  $\alpha = 130$  if  $\Gamma$  is a Fuchsian group and is equal to 7 otherwise.*

*Proof* By Proposition 4.7, there exists a hyperbolic  $\gamma \in \Gamma$  such that  $L = k(\lambda_\gamma)$  and with length at most  $e^{C_1 V} d_L^{C_2 + \log(V)}$  for absolute, effectively computable constants  $C_1, C_2$ . The result now follows from our hypothesis about  $|\Delta_{L/k}|$ , the formula  $d_L = |\Delta_{L/k}| d_k^2$  and the fact that  $d_k \leq V^{22}$ .  $\square$

We are now ready to prove Theorem 1.1. In what follows,  $c_1, c_2$  are the constants appearing in Proposition 5.5,  $C$  is the constant appearing in Proposition 5.2 and  $c \geq C$  is such that  $c_1 e^{c_2 \log(V)^7} \leq c e^{(\log(V))^{\log(V)}}$  for all  $V \geq 0.9$ . Note that by Chinburg–Friedman–Jones–Reid [17], every arithmetic hyperbolic 3-manifold has volume  $V > 0.94$ .

*Proof of Theorem 1.1* We prove Theorem 1.1 in the case that the manifolds  $M_i$  are 3-manifolds and then make a few remarks regarding the (minor) modifications needed for the 2-manifold case. Let  $\Gamma_j = \pi_1(M_j)$  for  $j = 1, 2$ . As in Reid’s proof that isospectral arithmetic 3-manifolds are commensurable [72], it suffices to show that the quaternion algebras from which  $\Gamma_1, \Gamma_2$  arise are isomorphic. To that end, let  $(k_1, B_1)$  and  $(k_2, B_2)$  be the number fields and quaternion algebras associated to  $\Gamma_1, \Gamma_2$ . By Proposition 5.2 there are hyperbolic  $\gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2$  with non-real eigenvalues  $\lambda_{\gamma_1}$  and  $\lambda_{\gamma_2}$  whose associated geodesics have the same complex length. Taking powers of  $\gamma_1, \gamma_2$  if necessary, we may assume that  $\gamma_1 \in \Gamma_1^{(2)}, \gamma_2 \in \Gamma_2^{(2)}$ . By (3), we have  $\text{tr}(\gamma_1) = \pm \text{tr}(\gamma_2)$  and consequently that the images in  $\mathbf{C}$  of  $k_1, k_2$  coincide [18, Lemma 2.3]. Hence,  $B_1, B_2/k$  are defined over a common number field  $k$ . To prove that  $B_1, B_2$  are isomorphic, by Lemma 4.1 we have  $|\text{disc}(B)|, |\text{disc}(B')| < 10^{57}V^7$ . Let  $L/k$  be a quadratic extension which embeds into  $B_1$  and with  $|\Delta_{L/k}|$  less than the bound given in Theorem 1.3; we take  $x = 10^{57}V^7$ . By Proposition 5.5, there exists  $u_1 \in B$  such that  $L = k(u_1)$  with the property that the image  $\gamma_1 \in \Gamma_1$  of  $u_1$  in  $M(2, \mathbf{C})$  is a hyperbolic and satisfies

$$\ell_0(\gamma_1) \leq c_1 e^{c_2 \log(V)V^7} \leq c e^{(\log(V)\log(V))}.$$

By hypothesis, there exists  $\gamma_2 \in \Gamma_2$  such that  $\ell(\gamma_1) = \ell(\gamma_2)$ . Let  $u_2$  be a preimage of  $\gamma_2$  in  $B_2$ . By (3), we see that  $\text{tr}(\gamma_1) = \pm \text{tr}(\gamma_2)$ . Since the fields  $k(u_1)$  and  $k(u_2)$  are both isomorphic to  $L$ , we see that  $B_2$  admits an embedding of  $L$ . The same argument shows that if  $L'/k$  is a quadratic extension which embeds into  $B_2$  and has  $|\Delta_{L'/k}|$  less than the bound given in Theorem 1.3 with  $x = 10^{57}V^7$ , then  $B_1$  admits an embedding of  $L'$ . Theorem 1.3 now shows that  $B_1 \cong B_2$ , finishing our proof.  $\square$

*Remark* We briefly comment on the modifications needed for the 2-dimensional case of Theorem 1.1.

As was noted in the 3-dimensional case, it suffices to show that the quaternion algebras associated to  $\Gamma_1, \Gamma_2$  are isomorphic. By Proposition 5.5 there exists a hyperbolic  $\gamma \in \Gamma_1$  such that  $\ell(\gamma) \leq c_1 e^{c_2 \log(V)V^{130}}$ . Proposition 4.13 shows that we further have  $k_1 = \mathbf{Q}(\text{tr}(\gamma))$ . By hypothesis there exists  $\gamma' \in \Gamma_2$  such that  $\ell(\gamma) = \ell(\gamma')$ , hence  $\text{tr}(\gamma) = \pm \text{tr}(\gamma')$ . Since  $\mathbf{Q}(\text{tr}(\gamma)) = \mathbf{Q}(\text{tr}(\gamma'))$ , we may assume, as above, that  $k_1 = k_2$ . The remainder of the proof is analogous to the proof of the 3-dimensional case; here, we can show that  $B_1 \cong B_2$  by proving that all maximal subfields  $L$  of these algebras that are not totally complex and have  $|\Delta_{L/k}|$  less than the bound in Theorem 1.3 coincide.

We conclude this section by proving the following strengthening of Theorem 1.1 in the case that the groups  $\Gamma_i$  are derived from orders in quaternion algebras.

**Theorem 5.6** *Let  $k_1, k_2$  be totally real number fields (resp., number fields with a unique complex place),  $B_1, B_2$  be quaternion division algebras over  $k_1, k_2$  which are ramified at all but one real place (resp., all real places) of  $k_1, k_2$ ,  $\mathcal{O}_1, \mathcal{O}_2$  be maximal orders in  $B_1, B_2$ , and  $V$  be such that  $\text{covol}(\Gamma_{\mathcal{O}_1}), \text{covol}(\Gamma_{\mathcal{O}_2}) \leq V$ . There exist absolute effectively computable constants  $c_1, c_2, c_3$  such that if the length sets (resp., complex length sets) of  $\mathbf{H}^2/\Gamma_{\mathcal{O}_1}, \mathbf{H}^2/\Gamma_{\mathcal{O}_2}$  (resp.,  $\mathbf{H}^3/\Gamma_{\mathcal{O}_1}, \mathbf{H}^3/\Gamma_{\mathcal{O}_2}$ ) agrees for all lengths less than  $c_1 e^{c_2 \log(V)V^{130}}$  (resp.,  $c_3 e^{(\log(V)\log(V))}$ ) then  $\mathbf{H}^2/\Gamma_{\mathcal{O}_1}$  and  $\mathbf{H}^2/\Gamma_{\mathcal{O}_2}$  (resp.,  $\mathbf{H}^3/\Gamma_{\mathcal{O}_1}$  and  $\mathbf{H}^3/\Gamma_{\mathcal{O}_2}$ ) are length-isospectral (resp., complex length-isospectral).*

*Proof* Theorem 1.1 and its proof show that  $k_1 \cong k_2$ ,  $B_1 \cong B_2$ , hence  $\mathcal{O}_2$  is isomorphic to a maximal order  $\mathcal{O} \subset B_1$ . If  $\mathcal{O} \cong \mathcal{O}_1$ , then  $\mathbf{H}^2/\Gamma_{\mathcal{O}_1}, \mathbf{H}^2/\Gamma_{\mathcal{O}_2}$  (or  $\mathbf{H}^3/\Gamma_{\mathcal{O}_1}, \mathbf{H}^3/\Gamma_{\mathcal{O}_2}$ ) will be isometric, hence isospectral. Suppose that  $\mathcal{O} \not\cong \mathcal{O}_1$  and  $\mathbf{H}^2/\Gamma_{\mathcal{O}_1}, \mathbf{H}^2/\Gamma_{\mathcal{O}_2}$  (or  $\mathbf{H}^3/\Gamma_{\mathcal{O}_1}$  and  $\mathbf{H}^3/\Gamma_{\mathcal{O}_2}$ ) are not isospectral. By [16, Theorem 3.3] and [54, Theorem 12.4.5], there exists a quadratic extension  $L/k$  which is unramified at all finite places (and which is not totally complex if the field  $k_1$  is totally real) and a quadratic order  $\Omega = \mathcal{O}_k[\gamma] \subset L$  such that  $\Omega$

embeds into exactly one of  $\{\mathcal{O}_1, \mathcal{O}\}$ . By Proposition 4.7, there exist absolute constants  $C_1, C_2$  and a length (resp., complex length)

$$\ell_0(\gamma) \leq e^{C_1 V} d_k^{2C_2 + 2\log(V)} \leq e^{C_1 V} V^{44(C_2 + 2\log(V))}, \quad (24)$$

which lies in the length set (resp., complex length set) of exactly one of  $\{\mathbf{H}^2/\Gamma_{\mathcal{O}}, \mathbf{H}^2/\Gamma_{\mathcal{O}_1}\}$  (resp.,  $\{\mathbf{H}^3/\Gamma_{\mathcal{O}}, \mathbf{H}^3/\Gamma_{\mathcal{O}_1}\}$ ). We note that the latter inequality (24) follows from the proof of [45, Theorem 4.1]. By choosing constants appropriately, we contradict our hypothesis that the length set (resp., complex length sets) of  $\mathbf{H}^2/\Gamma_{\mathcal{O}_1}$  and  $\mathbf{H}^2/\Gamma_{\mathcal{O}_2}$  (or  $\mathbf{H}^3/\Gamma_{\mathcal{O}_1}$  and  $\mathbf{H}^3/\Gamma_{\mathcal{O}_2}$ ) coincide for all sufficiently small lengths.  $\square$

## 6 Geometric submanifolds: effective rigidity and asymptotic growth of surfaces

We now turn our attention to an effective version of [59, Theorem 1.1] which stated that two arithmetic hyperbolic 3-manifolds with the same totally geodesic surfaces are commensurable provided they have a totally geodesic surface.

### 6.1 Proof of Theorem 1.4

To prove Theorem 1.4, we require the following easy extension of [54, Theorem 9.55].

**Theorem 6.1** *Let  $L$  be a number field and let  $B/L$  be a quaternion algebra which is ramified precisely at the real places  $v_1, \dots, v_s$  of  $L$ , let  $k < L$  such that  $[L : k] = 2$ , and  $B_0/k$  be a quaternion algebra which is ramified at  $v_1|_k, \dots, v_s|_k$  and at no other real places of  $k$ . Then  $B \cong B_0 \otimes_k L$  if and only if  $\text{Ram}_f(B)$  consists of the  $2r$  distinct places  $\{\mathfrak{P}_1, \mathfrak{P}'_1, \dots, \mathfrak{P}_r, \mathfrak{P}'_r\}$ , where  $\mathfrak{P}_i \cap \mathcal{O}_k = \mathfrak{P}'_i \cap \mathcal{O}_k = \mathfrak{p}_i$  and  $\text{Ram}_f(B_0) \supset \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$  with  $\text{Ram}_f(B) \setminus \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$  consisting of primes in  $\mathcal{O}_k$  which are either ramified or inert in the extension  $L/k$ .*

*Proof of Theorem 1.4* Let  $R_1$  denote the set of places of  $L_1$  which ramify in  $B_1$ ,  $R_2$  denote the set of places of  $L_2$  which ramify in  $B_2$  and  $R'_i$  (for  $i = 1, 2$ ) denote the set of places of  $k$  lying below a place in  $R_i$ . As  $B_0 \otimes_k L_1 \cong B_1$  and  $B_0 \otimes_k L_2 \cong B_2$ , it suffices to show that  $L_1 \cong L_2$ . To that end, suppose that  $L_1 \not\cong L_2$  and let  $L = L_1 L_2$ , which is Galois over  $k$  with Galois group  $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$ . Elementary properties of Frobenius elements [41, Chapter 10] show that if  $\mathfrak{p}_k$  is a prime of  $k$  which is unramified in  $L/k$  and whose Frobenius element  $(\mathfrak{p}_k, L/k)$  corresponds to the element  $(1, 1)$  of  $\text{Gal}(L/k)$  then  $\mathfrak{p}_k$  is inert in both  $L_1/k$  and  $L_2/k$ . Similarly, if the Frobenius element

$(\mathfrak{p}_k, L/k)$  corresponds to the element  $(1, 0)$  of  $\text{Gal}(L/k)$  then  $\mathfrak{p}_k$  is inert in  $L_1/k$  and splits in  $L_2/k$ . It now follows from the bound on the least prime ideal in the Chebotarev density theorem [40] (see also Theorem 5.3) that there exist primes  $\omega_1, \omega_2$  of  $k$  such that

- (i)  $\omega_1$  is inert in  $L_1/k$  and splits in  $L_2/k$ ,
- (ii)  $\omega_2$  is inert in both  $L_1/k$  and  $L_2/k$ ,
- (iii) Neither  $\omega_1$  nor  $\omega_2$  lie in  $R'_1 \cup R'_2$ ,
- (iv)  $|\omega_1|, |\omega_2| \leq d_k^C (2 \log(|\text{disc}(B_1)| |\text{disc}(B_2)|))^2$ .

Let  $B'/k$  be a quaternion algebra such that  $\text{Ram}_\infty(B') = \{v|_k : v \in \text{Ram}_\infty(B_1)\}$  and which ramifies at all primes lying in  $R'_1 \cup \{\omega_1\}$  (and possibly at  $\omega_2$  as well if needed for parity reasons). As  $B_0 \otimes_k L_1 \cong B_1$ , we deduce from Theorem 6.1 that  $B' \otimes_k L_1 \cong B_1$ . Recall that  $\omega_1$  splits in  $L_2/k$ . We can therefore write  $\omega_1 = v_1 v_2$  for primes  $v_1, v_2$  of  $L_2$ . Then  $(L_2)_{v_1} \cong k_{\omega_1}$ , which implies that  $B_2 \otimes_{L_2} (L_2)_{v_1} \cong B' \otimes_k k_{\omega_1}$ , as by assumption we have  $B' \otimes_k L_2 \cong B_2$ . As  $\omega_1$  ramifies in  $B'$  we deduce that  $v_1$  ramifies in  $B_2$ , hence  $\omega_1 \in R'_2$ . This is a contradiction and so  $L_1 \cong L_2$ .  $\square$

## 6.2 Proof of Theorem 1.2

We begin with lemma about the coarea of certain arithmetic Fuchsian groups.

**Lemma 6.2** *Let  $k$  be totally real,  $B/k$  be a quaternion algebra, and  $\mathcal{O} \subset B$  be a maximal order. Then  $\text{coarea}(\Gamma_{\mathcal{O}}) \leq 2\pi^2 |\text{disc}(B)|$ .*

*Proof* Borel's volume formula [7] (see also [54, Chapter 11]) shows that

$$\text{coarea}(\Gamma_{\mathcal{O}}) = \frac{8\pi^2 \zeta_k(2) \prod_{\mathfrak{p} \mid \text{disc}(B)} (|\mathfrak{p}| - 1)}{(4\pi^2)^{n_k}}.$$

The lemma now follows from the well-known inequality  $\zeta_k(s) \leq \zeta(s)^{n_k}$ .  $\square$

**Proposition 6.3** *Let  $M = \mathbf{H}^3 / \Gamma$  be an arithmetic hyperbolic 3-manifold with trace field  $L$ , quaternion algebra  $B$ , and volume  $V$ . Suppose that  $k = L^+$  is the maximal totally real subfield of  $L$  and that  $[L : k] = 2$ . Let  $B_0$  be a quaternion algebra over  $k$  such that  $B_0 \otimes_k L \cong B$ . Then there exists an absolute effectively computable constant  $C$  such that  $M$  contains a totally geodesic surface with area at most  $2\pi^2 |\text{disc}(B_0)| e^{CV}$ .*

*Proof* Let  $\mathcal{O}_0 \subset B_0$  be a maximal order,  $\mathcal{O} \subset B$  a maximal order such that  $\Gamma_{\mathcal{O}_0} \subset \Gamma_{\mathcal{O}}$ , and define  $\Delta = \Gamma_{\mathcal{O}_0} \cap \Gamma^{(2)}$ . Then  $\Delta$  is a Fuchsian group contained in  $\Gamma$  and we have  $[\Gamma_{\mathcal{O}_0} : \Delta] \leq [\Gamma : \Gamma^{(2)}]$ . By Lemma 4.3,  $[\Gamma : \Gamma^{(2)}] \leq e^{CV}$ , where  $C$  is an absolute effectively computable constant. The proposition now follows from Lemma 6.2.  $\square$

For a hyperbolic 3-manifold  $M$ , we denote by  $GS(M)$  the collection of isometry types of totally geodesic surfaces. We can prove our main result of this section, an effective version of [59, Theorem 1.1].

*Proof of Theorem 1.2* Let  $M_1 = \mathbf{H}^3/\Gamma_1$ ,  $M_2 = \mathbf{H}^3/\Gamma_2$  and  $B_1/L_1$ ,  $B_2/L_2$  be the quaternion algebras and trace fields of  $M_1$ ,  $M_2$ . Since  $GS(M_1) \neq \emptyset$ ,  $\Gamma_1$  contains a non-elementary Fuchsian group. By considering the quaternion algebra and trace field of this Fuchsian group we see that the maximal totally real subfield  $k$  of  $L_1$  satisfies  $[L_1 : k] = 2$ . As  $GS(M_1) \cap GS(M_2)$  is non-empty, we see that  $[L_2 : k] = 2$  and also that there exists a quaternion algebra  $B_0$  over  $k$  such that  $B_0 \otimes_k L_1 \cong B_1$  and  $B_0 \otimes_k L_2 \cong B_2$ . Let  $C$  be the constant appearing in the bound on the least prime ideal in the Chebotarev density theorem [40] (see also Theorem 5.3). By combining the estimates  $d_k \leq d_{L_1} \leq V^{22}$  and  $|\text{disc}(B_1)|, |\text{disc}(B_2)| \leq 10^{57}V^7$  with an elementary computation, there exists an absolute constant  $C_1$  such that

$$V^{C_1} \geq d_k^{2C} (2 \log(|\text{disc}(B_1)| |\text{disc}(B_2)|))^4 |\text{disc}(B_1)| |\text{disc}(B_2)|.$$

Let  $C_2$  be the constant appearing in Proposition 6.3 and choose  $C_3$  so that  $2\pi^2 V^{C_1} e^{C_2 V} \leq e^{C_3 V}$ ; note that  $C_3$  may be chosen independently of  $M_1$ ,  $M_2$  and  $V$ . We will now show that if a finite type hyperbolic surface  $X$  lies in  $GS(M_1)$  if and only if it lies in  $GS(M_2)$  whenever the area of  $X$  is less than  $e^{C_3 V}$ , then  $M_1$  and  $M_2$  are commensurable. Let  $B'$  be a quaternion algebra over  $k$  which is ramified at all real places of  $k$  except the identity and satisfies

$$|\text{disc}(B')| \leq d_k^{2C} (2 \log(|\text{disc}(B_1)| |\text{disc}(B_2)|))^4 |\text{disc}(B_1)| |\text{disc}(B_2)|$$

as well as  $B' \otimes_k L_1 \cong B_1$ . Proposition 6.3 and the discussion above show that  $M_1$  contains a totally geodesic surface  $X$  (arising from the quaternion algebra  $B$ ) with area at most  $e^{C_3 V}$ . Our assumption implies that  $M_2$  contains a totally geodesic surface isometric to  $X$  as well. Consequently we must have  $B' \otimes_k L_2 \cong B_2$ . Interchanging the roles of  $B_1$ ,  $B_2$ , we see that by Theorem 1.4,  $L_1 \cong L_2$  and  $B_1 \cong B_2$ . Hence by Theorem 2.6,  $M_1$ ,  $M_2$  are commensurable.  $\square$

### 6.3 Proof of Theorem 1.11

We conclude this section with a proof of Theorem 1.11.

*Proof of Theorem 1.11* Setting  $k = L^+$ , as  $M$  contains a totally geodesic surface, we have  $[L : k] = 2$ . Theorem 2.7, along with a slight modification to the proof of Theorem 1.7 in the case that  $r = 1$ , shows that there exists a constant  $c(L)$  depending only on  $L$  (the constant only depends on  $k$ ) such that

for sufficiently large  $x$  the number of quaternion algebras  $B'/k$  satisfying  $B' \otimes_k L \cong B$  and  $|\text{disc}(B')| \leq x$  is asymptotic to  $[c(L)\text{disc}(B)^{1/2}]x/\log(x)^{1/2}$ . The theorem now follows from Proposition 6.3.  $\square$

**Acknowledgements** The authors thank Jayadev Athreya, Richard Canary, Ted Chinburg, Britain Cox, Peter Doyle, Daniel Fiorilli, Tsachik Gelander, Grant Lakeland, Chris Leininger, Jeff Meyer, Nick Miller, Gopal Prasad, Alan Reid, and Matthew Stover for conversations on the material in this article. We also thank the anonymous referee for detailed comments on an earlier version that corrected a mistake in Theorem 1.1 and helped improve the exposition. BL was partially supported by NSF RTG Grant DMS-1045119 and an NSF Mathematical Sciences Postdoctoral Fellowship. DBM was partially supported by NSF Grant DMS-1105710. PP was partially supported by NSF Grant DMS-1402268. LT was partially supported NSF VIGRE Grant DMS-0738586 and by an AMS Simons Travel Grant.

## References

1. Apostol, T.M.: *Introduction to Analytic Number Theory*. Undergraduate texts in mathematics. Springer, Berlin (1976)
2. Artin, E.: Über eine neue Art von L-Reihen. *Abh. Math. Sem. Univ. Hambg.* **3**, 89–108 (1923)
3. Belolipetsky, M., Ellenberg, J., Venkatesh, A.: Counting maximal arithmetic subgroups, with an appendix. *Duke Math. J.* **140**, 1–33 (2007)
4. Belolipetsky, M., Gelander, T., Lubotzky, A., Shalev, A.: Counting arithmetic lattices and surfaces. *Ann. Math.* **172**, 2197–2221 (2010)
5. Belolipetsky, M., Lubotzky, A.: Manifolds counting and class field towers. *Adv. Math.* **229**, 3123–3146 (2012)
6. Bhargava, M.: Higher composition laws and applications. *Int. Congr. Math. Eur. Math. Soc.* **2**, 271–294 (2006)
7. Borel, A.: Commensurability classes and volumes of hyperbolic 3-manifolds. *Ann. Sc. Norm. Sup. Pisa Cl. Sci. (4)* **8**(1), 1–33 (1981)
8. Borel, A., Prasad, G.: Finiteness theorems for discrete subgroups of bounded covolume in semi-simple groups. *Inst. Hautes Études Sci. Publ. Math.* **69**, 119–171 (1989)
9. Brindza, B.: On the generators of  $S$ -unit groups in algebraic number fields. *Bull. Austral. Math. Soc.* **43**, 325–329 (1991)
10. Brueggeman, S., Doud, D.: Local corrections of discriminant bounds and small degree extensions of quadratic base fields. *Int. J. Number Theory* **4**, 349–361 (2008)
11. Burger, M., Gelander, T., Lubotzky, A., Mozes, S.: Counting hyperbolic manifolds. *Geom. Funct. Anal.* **12**, 1161–1173 (2002)
12. Buser, P.: *Geometry and spectra of compact Riemann surfaces*. Birkhäuser, Basel (2010)
13. Cassels, J.W.S., Fröhlich, A.: *Algebraic Number Theory*. London Mathematical Society, London (1967)
14. Chernousov, V.I., Rapinchuk, A.S., Rapinchuk, I.A.: On the genus of a division algebra. *C. R. Math. Acad. Sci. Paris* **350**, 17–18 (2012)
15. Chinburg, T., Friedman, E.: The smallest arithmetic hyperbolic three-orbifold. *Invent. Math.* **86**, 507–527 (1986)
16. Chinburg, T., Friedman, E.: An embedding theorem for quaternion algebras. *J. Lond. Math. Soc.* **60**, 33–44 (1999)
17. Chinburg, T., Friedman, E., Jones, K.N., Reid, A.W.: The arithmetic hyperbolic 3-manifold of smallest volume. *Ann. Sc. Norm. Sup. Pisa Cl. Sci. (4)* **30**, 1–40 (2001)

18. Chinburg, T., Hamilton, E., Long, D.D., Reid, A.W.: Geodesics and commensurability classes of arithmetic hyperbolic 3-manifolds. *Duke Math. J.* **145**, 25–44 (2008)
19. Chinburg, T., Reid, A.W.: Closed hyperbolic 3-manifolds whose closed geodesics all are simple. *J. Differ. Geom.* **38**, 545–558 (1993)
20. Cohen, H., Diaz, F.D.Y., Olivier, M.: Enumerating quartic dihedral extensions of  $\mathbb{Q}$ . *Compos. Math.* **133**, 65–93 (2002)
21. Cohen, H.: Constructing and counting number fields. *Int. Congr. Math.* **II**, 129–138 (2002)
22. Cohn, H.: The density of abelian cubic fields. *Proc. Am. Math. Soc.* **5**, 476–477 (1954)
23. Datskovsky, B., Wright, D.J.: Density of discriminants of cubic extensions. *J. Reine Angew. Math.* **386**, 116–138 (1988)
24. Davenport, H., Heilbronn, H.: On the density of discriminants of cubic fields. II. *Proc. R. Soc. Lond. Ser. A* **322**, 405–420 (1971)
25. Delange, H.: Théorèmes taubériens et applications arithmétiques. *Mém. Soc. R. Sci. Liège* (4) **16**, 87 (1955)
26. Delange, H.: Généralisation du théorème de Ikehara. *Ann. Sci. Ecole Norm. Sup. (3)* **71**, 213–242 (1954)
27. Dusart, P.: Explicit estimates of some functions over primes. *Ramanujan J.* **45**(1), 227–251. <https://doi.org/10.1007/s11139-016-9839-4> (2018)
28. Futer, D., Millican, C.: Spectrally similar incommensurable 3-manifolds. *Proc. Lond. Math. Soc.* **115**, 411–447 (2017)
29. Gangolli, R.: The length spectra of some compact manifolds. *J. Differ. Geom.* **12**, 403–424 (1977)
30. Garibaldi, S., Saltman, D.: Quaternion algebras with the same subfields. In: Colliot-Thélène, J.-L., Garibaldi, S., Ramdorai, S., Suresh, V. (eds.) *Quadratic Forms, Linear Algebraic Groups, and Cohomology: Developments in Mathematics*, vol. 18. Springer, Berlin, pp. 225–238 (2010)
31. Gelander, T.: Homotopy type and volume of locally symmetric manifolds. *Duke Math. J.* **124**, 459–515 (2004)
32. Gelander, T., Glasner, Y.: Countable primitive groups. *Geom. Funct. Anal.* **17**, 1479–1523 (2008)
33. Godement, R.: Domaines fondamentaux des groupes arithmétiques, Séminaire Bourbaki (1962/63). Fasc. 3(257), 25 pp. Secrétariat mathématique, Paris
34. Goldfeld, D., Lubotzky, A., Nikolov, N., Pyber, L.: Counting primes, groups, and manifolds. *Proc. Natl. Acad. Sci. U.S.A.* **101**, 13428–13430 (2004)
35. Goldfeld, D., Lubotzky, A., Pyber, L.: Counting congruence subgroups. *Acta Math.* **193**, 73–104 (2004)
36. Gosefidy, A.S.: Counting lattices in simple Lie groups: the positive characteristic case. *Duke Math. J.* **161**, 431–481 (2012)
37. Hajdu, L.: A quantitative version of Dirichlet's  $S$ -unit theorem in algebraic number fields. *Publ. Math. Debrec.* **42**, 239–246 (1993)
38. Hardy, G.H., Wright, E.M.: *An Introduction to the Theory of Numbers*. Oxford University Press, Oxford (2008)
39. Huber, H.: Zur analytischen theorie hyperbolischer Raumformen und Bewegungsgruppen. II. *Math. Ann.* **143**, 463–464 (1961)
40. Lagarias, J.C., Montgomery, H.L., Odlyzko, A.M.: A bound for the least prime ideal in the Chebotarev density theorem. *Invent. Math.* **54**, 271–296 (1979)
41. Lang, S.: *Algebraic Number Theory*. Springer, Berlin (1994)
42. Larsen, M., Lubotzky, A.: Representation growth of linear groups. *J. Eur. Math. Soc.* **10**, 351–390 (2008)
43. Liebeck, M., Shalev, A.: Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks. *J. Algebra* **276**, 552–601 (2004)
44. Linowitz, B.: Selectivity in quaternion algebras. *J. Number Theory* **132**, 1425–1437 (2012)

45. Linowitz, B.: Families of mutually isospectral Riemannian orbifolds. *Bull. Lond. Math. Soc.* **47**, 47–54 (2015)
46. Linowitz, B., McReynolds, D.B., Pollack, P., Thompson, L.: Bounded gaps between primes and the length spectra of arithmetic hyperbolic 3-orbifolds. *C. R. Math. Acad. Sci. Paris* **355**, 1121–1126 (2017)
47. Linowitz, B., Meyer, J.S., Pollack, P.: The length spectra of arithmetic hyperbolic 3-manifolds and their totally geodesic surfaces. *N.Y. J. Math.* **21**, 955–972 (2015)
48. Louboutin, S.: The Brauer–Siegel theorem. *J. Lond. Math. Soc.* **72**, 40–52 (2005)
49. Lubotzky, A., Nikolov, N.: Subgroup growth of lattices in semisimple Lie groups. *Acta Math.* **193**, 105–139 (2004)
50. Lubotzky, A., Samuels, B., Vishne, U.: Division algebras and non-commensurable isospectral manifolds. *Duke Math. J.* **135**, 361–379 (2006)
51. Lubotzky, A., Segal, D.: Subgroup Growth. Birkhäuser, Basel (2003)
52. Macbeath, A.: Commensurability of cocompact three dimensional hyperbolic groups. *Duke Math. J.* **50**, 1245–1253 (1983)
53. Maclachlan, C., Reid, A.W.: Commensurability classes of arithmetic Kleinian groups and their Fuchsian subgroups. *Math. Proc. Camb. Philos. Soc.* **102**, 251–257 (1987)
54. Maclachlan, C., Reid, A.W.: The Arithmetic of Hyperbolic 3-Manifolds. Springer, Berlin (2003)
55. Marcus, D.A.: Number Fields. Springer, Berlin (1977)
56. Margulis, G.A.: Certain applications of ergodic theory to the investigation of manifolds of negative curvature. *Funkc. Anal. i Prilozv.* **3**, 89–90 (1969)
57. Margulis, G.A.: Discrete Subgroups of Semisimple Lie Groups. Springer, Berlin (1991)
58. McReynolds, D.B.: Geometric spectra and commensurability. *Can. J. Math.* **67**, 184–197 (2015)
59. McReynolds, D.B., Reid, A.W.: The genus spectrum of a hyperbolic 3-manifold. *Math. Res. Lett.* **21**, 169–185 (2014)
60. Meyer, J.S.: Division algebras with infinite genus. *Bull. Lond. Math. Soc.* **46**, 463–468 (2014)
61. Millichap, C.: Factorial growth rates for the number of hyperbolic 3-manifolds of a given volume. *Proc. Am. Math. Soc.* **143**, 2201–2214 (2015)
62. Millichap, C.: Mutations and short geodesics in hyperbolic 3-manifolds. *Commun. Anal. Geom.* **25**, 625–683 (2017)
63. Neukirch, J.: Algebraic Number Theory. Springer, Berlin (1999)
64. Odlyzko, A.M.: Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results. *Sém. Théor. Nombres Bordeaux (2)* **2**, 119–141 (1990)
65. Pierce, R.S.: Associative Algebras. Springer, Berlin (1982)
66. Pethő, A., Schmitt, S.: Elements with bounded height in number fields. *Period. Math. Hung.* **43**, 31–41 (2001)
67. Platonov, V., Rapinchuk, A.: Algebraic Groups and Number Fields. Academic Press, London (1994)
68. Poitou, G.: Sur les petits discriminants. In: *Séminaire Delange–Pisot–Poitou, 18e année: (1976/77), Théorie des nombres, Fasc. 1 (French)*, pages Exp. No. 6, 18. Secrétariat Math., Paris (1977)
69. Prasad, G., Rapinchuk, A.: Weakly commensurable arithmetic groups and isospectral locally symmetric spaces. *Publ. Math. Inst. Hautes Étud. Sci.* **109**, 113–184 (2009)
70. Raghunathan, M.S.: Discrete Subgroups of Lie Groups. Springer, Berlin (1972)
71. Reid, A.W.: A note on trace fields of Kleinian groups. *Bull. Lond. Math. Soc.* **22**, 349–352 (1990)
72. Reid, A.W.: Isospectrality and commensurability of arithmetic hyperbolic 2- and 3-manifolds. *Duke Math. J.* **65**, 215–228 (1992)

73. Reiner, I.: *Maximal Orders*. Oxford University Press, Oxford (2003)
74. Rudin, W.: *Real and Complex Analysis*. McGraw-Hill Book Co., New York (1987)
75. Serre, J.-P.: Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.* **54**, 323–401 (1981)
76. Sunada, T.: Riemannian coverings and isospectral manifolds. *Ann. Math.* **121**, 169–186 (1985)
77. Takeuchi, K.: Commensurability classes of arithmetic triangle groups. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **24**, 201–212 (1977)
78. Tits, J.: Classification of algebraic semisimple groups. In: Borel, A., Mostow, G.D. (eds.) *Algebraic Groups and Discontinuous Subgroups. Proceedings of Symposia in Pure Mathematics*, vol. 9, pp. 33–62. American Mathematical Society, Providence, RI (1966)
79. Thurston, W.P.: *The Geometry and Topology of 3-Manifolds*. Princeton University, Princeton (1979)
80. Vignéras, M.-F.: Variétés riemanniennes isospectrales et non isométriques. *Ann. Math.* **112**, 21–32 (1980)
81. Wang, S.: An effective version of the Grunwald–Wang theorem. Ph.D. thesis, Caltech (2001)
82. Wang, S.: Grunwald–Wang theorem, an effective version. *Sci. China Math.* **58**, 1589–1606 (2015)
83. Wirsing, E.: Das asymptotische Verhalten von Summen über multiplikative Funktionen. *Math. Annalen* **143**, 75–102 (1961)
84. Wood, M.M.: On the probabilities of local behaviors in abelian field extensions. *Compos. Math.* **146**, 102–128 (2010)