Counting quaternion algebras

Lola Thompson

Oberlin College

June 27, 2018

Collaborators

Joint work with: Ben Linowitz (Oberlin), Ben McReynolds (Purdue), and Paul Pollack (UGA).

Overview

Our Goal: Prove effective versions of rigidity results for arithmetic hyperbolic 2 and 3-manifolds.

Main Idea: We exploit the correspondence between maximal subfields of quaternion algebras and lengths of geodesics on arithmetic hyperbolic 2- and 3-manifolds.

Talk Overview:

- Brief introduction to quaternion algebras
- Our results on counting quaternion algebras
- Geometric background
- Our results on surfaces

Quaternion algebras

In the 1830s and 1840s, William Rowan Hamilton sought a number system which would play a role in three-dimensional geometry analogous to that of the complex numbers in two-dimensional geometry.

"Every morning in the early part of the above-cited month [October 1843], on my coming down to breakfast, your (then) little brother William Edwin, and yourself, used to ask me: 'Well, Papa, can you multiply triplets?' Whereto I was always obliged to reply, with a sad shake of the head: 'No, I can only add and subtract them."'

– Hamilton (in a letter to his son)

Quaternion algebras

Theorem (Hamilton, 1843)

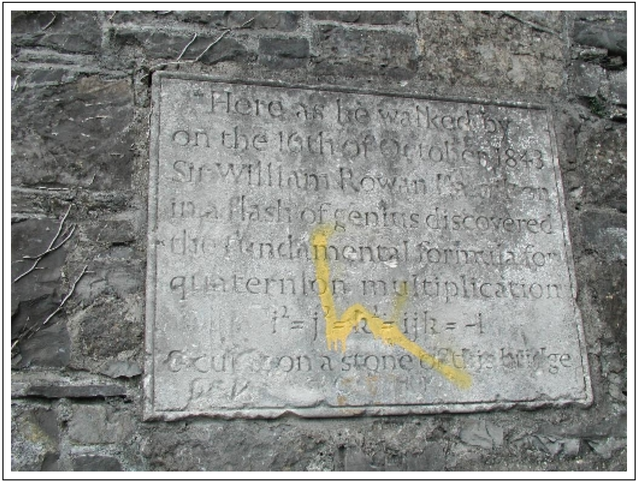
The $\mathbb{R}$-algebra $\mathbb{H}$ with basis $\{1, i, j, ij\}$ and defining relations

$$i^2 = -1 \qquad j^2 = -1 \qquad ij = -ji$$

is a four-dimensional division algebra.

Hamilton was so excited by this discovery that he carved these relations into the stone of the Brougham Bridge!

Quaternion algebras



Quaternion algebras

Write $(-1, -1, \mathbb{R})$ instead of $\mathbb{H}$.

This notation suggests a number of ways to generalize $\mathbb{H}$.

For example, let $(1, 1, \mathbb{R})$ be the $\mathbb{R}$-algebra with basis $\{1, i, j, ij\}$ and defining relations

$$i^2 = 1 \qquad j^2 = 1 \qquad ij = -ji.$$

Then $(1, 1, \mathbb{R}) \cong \mathrm{M}_2(\mathbb{R})$ via $i \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $j \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

Quaternion algebras

More generally, we can define $(a, b, \mathbb{R})$ to be the $\mathbb{R}$-algebra with basis $\{1, i, j, ij\}$ and defining relations

$$i^2 = a \qquad j^2 = b \qquad ij = -ji \qquad a, b \in \mathbb{R}^*.$$

(We can also replace $\mathbb{R}$ with other fields of characteristic 0.)

It's not too hard to show that

- $(a, b, \mathbb{R}) \cong \mathbb{H}$ if $a, b < 0$ and
- $(a, b, \mathbb{R}) \cong \mathrm{M}_2(\mathbb{R})$ otherwise.

Thus $(a, b, \mathbb{R})$ is either a division algebra or isomorphic to $\mathrm{M}_2(\mathbb{R})$.

Our Number Theory Results

Counting Central Division Algebras

Let k be a number field and n a positive integer. We are interested in counting the number of central division algebras of dimension n^2 over k which have (norm of) discriminant less than x.

For example, if $k = \mathbb{Q}$ and $n = 2$, we are counting the number of **rational quaternion algebras** with discriminant less than x.

Our main tool in counting central division algebras will be the following Tauberian theorem of Delange.

Delange's Tauberian Theorem

Theorem (Delange's Tauberian Theorem)

Let $G(s) = \sum \frac{a_N}{N^s}$ be a Dirichlet series satisfying:

1. $a_N \geq 0$ *for all* N *and* $G(s)$ *converges for* $\Re e(s) > \rho$.
2. $G(s)$ *can be continued to an analytic function in the closed half-plane* $\Re e(s) \geq \rho$ *except possibly for a singularity at* $s = \rho$.
3. *There is an open neighborhood of* ρ *and functions* $A(s), B(s)$ *analytic at* $s = \rho$ *with* $G(s) = A(s)/(s-\rho)^\beta + B(s)$ *at every point in this neighborhood having* $\Re e(s) > \rho$.

Then as $x \to \infty$ *we have*

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

Growth Rate of Division Algebras




Theorem (Linowitz, McReynolds, Pollack, T.)

If $N(x)$ denotes the number of division algebras of dimension n^2 over k with $|\mathrm{disc}| < x$ and ℓ is the smallest prime divisor of n, then there is a constant $\delta_n > 0$ so that

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

as $x \to \infty$.

Proof Sketch

Main idea:

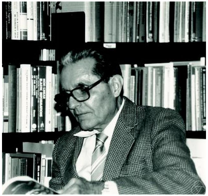
- Create a Dirichlet series whose coefficients count the central division algebras with fixed discriminant.

Proof Sketch

Main idea:

- Create a Dirichlet series whose coefficients count the central division algebras with fixed discriminant.

- Apply Delange's Theorem in order to estimate the partial sums of these coefficients.



Theorem (Linowitz, McReynolds, Pollack, T.)

Fix a number field k and a quaternion algebra B defined over 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 $x \to \infty$, where $c_{k,B} > 0$. Moreover, if κ_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

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

Proof Sketch

- Recall: If B/k is a quaternion algebra and L/k is a quadratic extension, then L embeds into B iff no prime of k that divides the discriminant of B splits in L/k.

Proof Sketch

- Recall: If B/k is a quaternion algebra and L/k is a quadratic extension, then L embeds into B iff no prime of k that divides the discriminant of B splits in L/k.

- A result of Matchett Wood allows us to model the splitting of finitely many primes as mutually independent events over the class of random quadratic extensions of k.

Proof Sketch

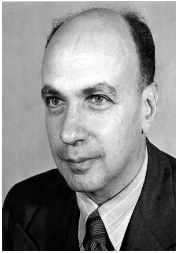
- Recall: If B/k is a quaternion algebra and L/k is a quadratic extension, then L embeds into B iff no prime of k that divides the discriminant of B splits in L/k.

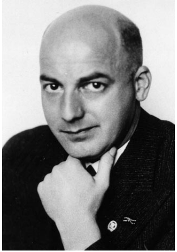
- A result of Matchett Wood allows us to model the splitting of finitely many primes as mutually independent events over the class of random quadratic extensions of k.

- Use this along with the proof of the previous theorem.

Counting Quaternion Algebras

A similar problem is to count the number of quaternion algebras over k which admit embeddings of specified quadratic extensions $L_1, \ldots, L_r$ of k.





Theorem (Albert-Brauer-Hasse-Noether, 1931)

There is an embedding of L into A if and only if no prime $\mathfrak{p}$ of K for which $A \otimes_k k_{\mathfrak{p}}$ is a division algebra splits in L/k.

The idea used to prove the previous theorems can be adapted to show:

Theorem (Linowitz, McReynolds, Pollack, T.)

Fix a number field k, and fix quadratic extensions $L_1, L_2, \ldots, L_r$ of k. Let L be the compositum of the L_i, and suppose that $[L : k] = 2^r$. The number of quaternion algebras over k with discriminant having norm 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 $x \to \infty$. Here δ is a positive constant depending only on the L_i and k.

Geometric Background

Geometric Background

Let M be a compact Riemannian manifold.

The **Laplace eigenvalue spectrum** of M, denoted $\mathcal{E}(M)$, is the multiset of eigenvalues of the Laplacian of M.

The **geodesic length spectrum**, denoted $LS(M)$, is the multiset of lengths of closed geodesics on M with fundamental group $\pi_1(M)$.

Inverse spectral geometry asks for the extent to which the spectra of M determine its geometry and topology.

Geometric terminology

Definition

Two manifolds are **commensurable** if and only if they have a common finite degree covering space.

Definition

Two manifolds are **isometric** if there is an isometry between them.

Definition

M and N are **isospectral** if $\mathcal{E}(M) = \mathcal{E}(N)$, and **length isospectral** if $LS(M) = LS(N)$.

Inverse Problems

Some natural inverse problems:

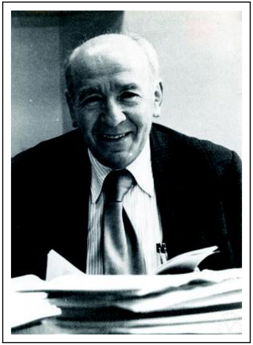
- If $\mathrm{LS}(M) = \mathrm{LS}(N)$, is M isometric to N?
- If $\mathrm{LS}(M) = \mathrm{LS}(N)$, are M and N commensurable?
- If $\mathrm{LS}(M) = \mathrm{LS}(N)$, what can be said about N?

We can ask the same questions for $\mathcal{E}(M)$.

Can you hear the shape of a drum?

Leon Green (1960) asked if the spectrum of M determines its isometry class.

The spectrum of M is essentially the collection of frequencies produced by a drumhead shaped like M.



Mark Kac (1966) popularized this question for planar domains:

Can you hear the shape of a drum?

Kac's question was finally answered in 1992.

Theorem (Gordon, Webb, Wolpert, 1992)

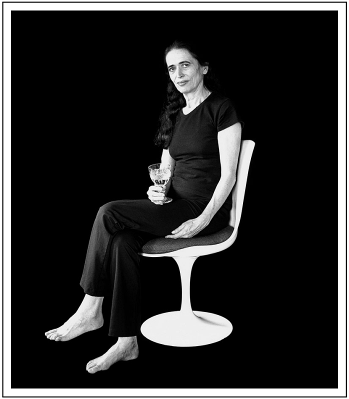
One cannot hear the shape of a drum.

Hyperbolic surfaces

The *hyperbolic plane* $\mathbf{H}^2$ is a simply connected surface with constant curvature -1 and can be be modeled by the disc (*Circle Limit IV*, by M.C. Escher):

The symmetries of this diagram, mapping one angel to any other angel, form a group of isometries acting on $\mathbf{H}^2$.

Results for hyperbolic surfaces

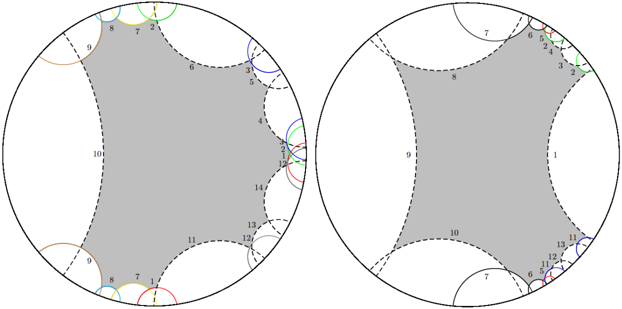


Theorem (Vigneras, 1980)

There exist isospectral non-isometric hyperbolic 2- and 3-manifolds.

Vigneras' examples arise from quaternion algebras!

Isospectral but non-isometric



A pair of isospectral but non-isometric hyperbolic 2-orbifolds (due to B. Linowitz and J. Voight).

Constructing arithmetic manifolds

Elementary results from geometric group theory:

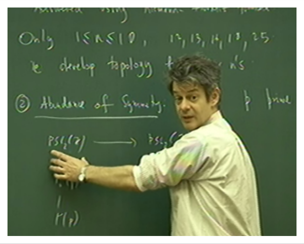
- $Isom^+(\mathbf{H}^2) \cong PSL_2(\mathbb{R})$.
- Every orientable hyperbolic 2-manifold is of the form $\mathbf{H}^2/\Gamma$ for some discrete subgroup Γ of $PSL_2(\mathbb{R})$.

We want to generalize the following construction of $PSL_2(\mathbb{Z})$:

$$M_2(\mathbb{Q}) \supset M_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}) \longrightarrow PSL_2(\mathbb{Z}).$$

We can replace $M_2(\mathbb{Q})$ with a *quaternion algebra* over a number field and $M_2(\mathbb{Z})$ with a *quaternion order*. Manifolds that arise in this manner are called *arithmetic manifolds*.

Results for arithmetic, hyperbolic 2-manifolds



Theorem (Reid, 1992)

If M is an arithmetic, hyperbolic 2-manifold and $\mathrm{LS}(M) = \mathrm{LS}(N)$ then M and N are commensurable.

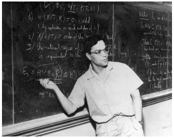
Our Geometric Results

Motivating Questions:

- Can we make Reid's result effective?
- How quickly does the number of commensurability classes of arithmetic, hyperbolic 2-manifolds grow?
- If the length spectra have a great deal of overlap, must the corresponding arithmetic, hyperbolic 2-manifolds be commensurable?

Effective Rigidity

To describe what we mean by **effective rigidity** some arithmetic facts will be useful.



Borel's finiteness result. For each $V \in \mathbb{R}_{\geq 0}$ there are only finitely many arithmetic hyperbolic 2- manifolds of volume at most V.

A consequence of Borel's result is that there exists $\mathrm{L}(V) \in \mathbb{R}_{\geq 0}$ such that if M and N are arithmetic surfaces of area at most V and have the same geodesic lengths up to $\mathrm{L}(V)$ then M and N are commensurable.

Our Geometric Results

The following is an effective version of Reid's "isospectral implies commensurable" result.

Theorem (Linowitz, McReynolds, Pollack, T.)

If M is an arithmetic hyperbolic surface then

$$L(V) \leq c_1 e^{c_2 \log(V) V^{130}}$$

for absolute, effectively computable constants c_1 and c_2.

Growth Rate of Commensurability Classes

Given a commensurability class $\mathcal{C}$ of arithmetic hyperbolic 2-manifolds, we define the volume $V_{\mathcal{C}}$ of $\mathcal{C}$ to be the minimum volume achieved by its members.

Theorem (Linowitz, McReynolds, Pollack, T.)

Let k be a totally real number field of degree n_k and let $N_k(V)$ denote the number of commensurability classes $\mathcal{C}$ of compact arithmetic hyperbolic 2-manifolds arising from quaternion algebras over k with $V_{\mathcal{C}} \leq V$. Then for all sufficiently large V we have

$$N_k(V) \ll \frac{\kappa 2^{n_k - 1} V^{130}}{\zeta_k(2)},$$

where $\zeta_k(s)$ is the Dedekind zeta function of k and κ is the residue of $\zeta_k(s)$ at $s = 1$.

Let $\pi(V, S)$ denote the maximum cardinality of a collection of pairwise non-commensurable arithmetic hyperbolic 2–orbifolds derived from quaternion algebras, each of which has volume less than V and geodesic length spectrum containing S.

Theorem (Linowitz, McReynolds, Pollack, T., 2014)

If $\pi(V, S) \to \infty$ as $V \to \infty$, then there are integers $1 \leq r, s \leq |S|$ and constants $c_1, c_2 > 0$ such that

$$\frac{c_1 V}{\log(V)^{1-\frac{1}{2^r}}} \leq \pi(V, S) \leq \frac{c_2 V}{\log(V)^{1-\frac{1}{2^s}}}$$

for all sufficiently large V.

Thank you!