Algorithms for the cohomology of compact arithmetic manifolds

Aurel Page
joint work with Michael Lipnowski

2022-05-30
Cogent seminar

Inria / IMB Bordeaux

Plan

1. Arithmetic manifolds
2. Algorithms
3. Practical considerations

Arithmetic manifolds

Arithmetic groups

An **arithmetic group** is a subgroup $\Gamma \subset \mathbb{G}(\mathbb{Z})$ of finite index where $\mathbb{G} \subset \mathrm{SL}_n$ is a (semisimple) algebraic group defined over $\mathbb{Q}$.

Examples: $\Gamma = \mathrm{SL}_n(\mathbb{Z}), \mathrm{SO}(Q, \mathbb{Z})$ with Q quadratic form, $\mathrm{Sp}_{2g}(\mathbb{Z})$ etc.

Γ is usually infinite, but has a finite presentation (Borel – Harish-Chandra)

Arithmetic groups

Γ is finitely presented.

"Proof": Let $X = \mathbb{G}(\mathbb{R})/K$ where $K \subset \mathbb{G}(\mathbb{R})$ is a maximal compact subgroup.
The symmetric space X is contractible and has an action of Γ.

- The quotient $\Gamma\backslash X$ is almost a compact manifold (**arithmetic manifold**).
- Γ is almost $\pi_1(\Gamma\backslash X)$.

In particular, $H^\bullet(\Gamma\backslash X)$ is also finitely generated.

For simplicity: assume both "almost" are literally true.

Hecke operators

From $\delta \in \mathbb{G}(\mathbb{Q})$ we get a correspondence T_δ:

$$\begin{tikzcd} \Gamma \cap \delta\Gamma\delta^{-1}\backslash X \arrow[r, "\delta"] \arrow[d] & \delta^{-1}\Gamma\delta \cap \Gamma\backslash X \arrow[d] \\ \Gamma\backslash X \arrow[r, "T_\delta"] & \Gamma\backslash X \end{tikzcd}$$

(more generally, adélic version).

$\deg T_\delta =$ degree of the cover.

T_δ acts on $H^i(\Gamma\backslash X)$: related to automorphic forms (over $\mathbb{C}$) and Galois representations (including torsion).

Algorithmic problems

Question: Given Γ, can we compute these objects? How fast?

Cohomology:

- Input: equations for $\mathbb{G}$ and a membership test for Γ.
- Output: groups $H^i(\Gamma\backslash X)$.
- Measure of complexity: ~~size of input~~ $V = \mathrm{Vol}(\Gamma\backslash X)$.

Hecke action:

- Input: $\delta \in \mathbb{G}(\mathbb{Q})$.
- Output: matrices of T_δ on $H^i(\Gamma\backslash X)$.
- Measure of complexity: ~~size of input~~ $\deg T_\delta$.

Complexity

Theorem (Grunewald–Segal ’80)

There exists an algorithm which, given Γ, computes a presentation for it.

Unknown complexity, completely impractical.

Theorem (Gromov, Gelander, Frączyk–Hurtado–Raimbault)

The homotopy type of $\Gamma \backslash X$ is of size at most $O_X(V)$.

Optimistically, algorithms running in time $O_X(V)$?

Algorithms

Looking for a general method

Observation: many successful methods for computing with arithmetic groups (Dirichlet domains, Voronoï algorithm, etc) use **special properties** of some symmetric spaces.

If we do not want to use special properties, what is left?

Our attempt: only use the **canonical metric.**

Density of sets of points

Let Y be a metric space. For $x \in Y$ and $R > 0$, let $B_R(x)$ be the open ball of radius R.

Definition

Let $F \subset Y$ and $R > 0$. Say that

- F is R-dense if $Y = \bigcup_{x \in F} B_R(x)$, and
- F is R-separated if $d(x, y) \geq R$ for all $x \neq y \in F$.

Dense sets approximate Y, and separated sets are not too large (by a volume argument).

Cech complex

Let $F \subset Y$. Then **Cech complex** $\mathcal{C}_R(F)$ is the simplicial complex with

- vertices: elements of F, and
- $\{x_0, \ldots, x_k\}$ is a k-simplex iff $\bigcap_i B_R(x_i) \neq \emptyset$.

Theorem (Nerve theorem)

Assume Y is a compact Riemannian manifold. If $R > 0$ is sufficiently small and $F \subset Y$ is R-dense then $\mathcal{C}_R(F)$ is homotopy-equivalent to Y.

Problem: the intersecting balls condition is not easy to test.

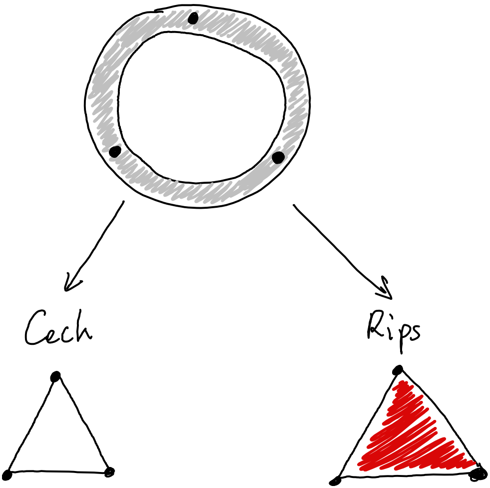
Rips complex

Let $F \subset Y$. Then **Rips complex** $\mathcal{R}_R(F)$ is the simplicial complex with

- vertices: elements of F, and
- $\{x_0, \ldots, x_k\}$ is a k-simplex iff $d(x_i, x_j) < 2R$ for all i, j.

Comparison with the Cech complex:

- same 0-skeleton;
- same 1-skeleton if Y admits midpoints;
- $\mathcal{C}_R(F) \subset \mathcal{R}_R(F) \subset \mathcal{C}_{2R}(F)$.


Cech
Rips

Rips complex

Y is **locally** $CAT(0)$ **of injectivity radius** ρ if every ball of radius ρ is a complete $CAT(0)$ space.

Theorem (Lipnowski-P.)

Assume Y is locally $CAT(0)$ of injectivity radius ρ. Let $F \subset Y$ be R-dense with $17R < 2\rho$. Then $\mathcal{R}_{17R}(F)$ is homotopy-equivalent to Y.

Construction of nets

Question: How do we produce a dense set in a space that we don't know?

Classical argument: Let $F \subset Y$ be a maximal R-separated subset. Then F is R-dense.

Problem: non-effective!

Effective version:

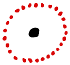
- Let $F' \subset Y$ be $R/2$-dense.
- Let $F \subset F'$ be maximal $R/2$-separated.
- $\Longrightarrow F$ is $R/2$-dense in F'.
- $\Longrightarrow F$ is R-dense in Y.

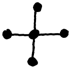
Covering algorithm

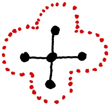
Algorithm:
Start with $F = \{x_0\}$.
Repeat

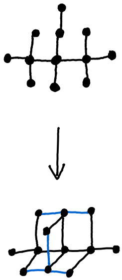
1. Let $F' \supset F$ be $R/2$-dense in the $(R+\varepsilon)$-neighborhood of F;
2. Increase F to be maximal $R/2$-separated in F';

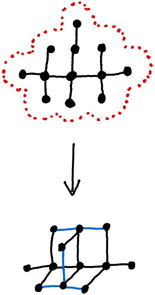
Until F stabilises.

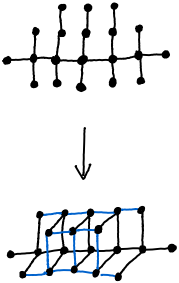


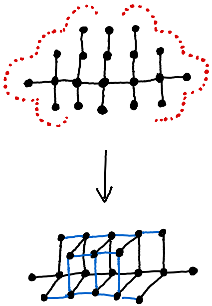


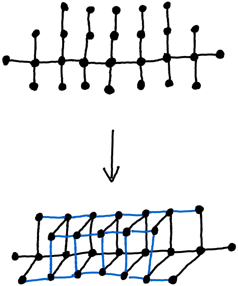


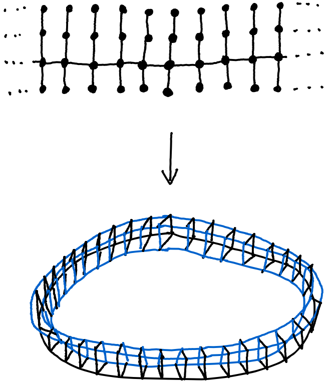












Covering algorithm

Algorithm:
Start with $F = \{x_0\}$.
Repeat

1. Let $F' \supset F$ be $R/2$-dense in the $(R+\varepsilon)$-neighborhood of F;
2. Increase F to be maximal $R/2$-separated in F';

Until F stabilises.

Facts:

- If Y is compact, then the algorithm terminates.
- Under a connectedness hypothesis, the output F is R-dense in Y.
- The output F is $R/2$-separated.

Routines

The algorithm uses only two elementary routines:

- **Local cover**: given $x \in Y$, compute F' that is $R/2$-dense in $B_{R+\varepsilon}(x)$.
- **Bounded distance test**: given $x, y \in Y$ and $r > 0$, determine whether $d(x, y) < r$.

Local cover for arithmetic manifolds

We need to instanciate the routines for arithmetic manifolds. We start with the easiest one.

Local cover: given $x \in Y$, compute F' that is $R/2$-dense in $B_{R+\varepsilon}(x)$.

Apply the exponential map

$$\exp\colon \mathfrak{g} \to \mathbb{G}(\mathbb{R})$$

to a ball in a dense enough **Euclidean lattice** in $\mathfrak{g}$.

Bounded distance test for arithmetic manifolds

Bounded distance test: given $x, y \in Y$ and $r > 0$, determine whether $d(x, y) < r$.

In $Y = \Gamma \backslash X$, points are given as elements of X.
Quasi-equivalence mod Γ: given $x, y \in X$ and $r > 0$, determine whether there exists $\gamma \in \Gamma$ such that $d(x, \gamma y) < r$.

$$X \hookrightarrow X_{\mathrm{SL}_n} = \{\text{positive definite quadratic forms on } \mathbb{R}^n, \det = 1\}$$

Observation: if $Q, Q' \in X_{\mathrm{SL}_n}$, then for all $v \in \mathbb{R}^n \setminus \{0\}$

$$|\log Q(v) - \log Q'(v)| \leq d(Q, Q').$$

Bounded distance test for arithmetic manifolds

Quasi-equivalence mod Γ: given $x, y \in X$ and $r > 0$, determine whether there exists $\gamma \in \Gamma$ such that $d(x, \gamma y) < r$.

If $\gamma \in \mathbb{G}(\mathbb{Z})$ and $d(Q', \gamma Q) < r$, then for all $v \in \mathbb{R}^n$

$$Q'(v)e^{-r} \leq Q(\gamma v) \leq Q'(v)e^{r}.$$

In other words,

$$\gamma\colon (\mathbb{Z}^n, Q) \to (\mathbb{Z}^n, Q')$$

is an e^r**-quasi-isometry** between two lattices.

Isometry algorithm : Plesken-Souvignier

Why is it good to reduce to a quasi-isometry problem?

Isometry problem: given two lattices $L = (\mathbb{Z}^n, Q)$ and $L' = (\mathbb{Z}^n, Q')$, determine all isometries $\gamma\colon L \to L'$.

Algorithm (Plesken–Souvignier):

- $b_1, \dots, b_n$ basis of L.
- $Q'(\gamma b_i) = Q(b_i) \implies \gamma b_i \in$ finite computable set.
- Use a basis of short vectors.
- Prune the search tree using well-chosen invariants.
- Use the group structure.

Quasi-isometry algorithm

Quasi-isometry problem: given two lattices $L = (\mathbb{Z}^n, Q)$ and $L' = (\mathbb{Z}^n, Q')$, determine all e^r-quasi-isometries $\gamma\colon L \to L'$.

Algorithm:

- $b_1, \ldots, b_n$ basis of L.
- $Q'(\gamma b_i) \leq Q(b_i)e^r \implies \gamma b_i \in$ finite computable set.
- Use a basis of short vectors.

Open problems:

- Quasi-invariants?
- Quasi-group structure?

Main theorem I

Theorem (Lipnowski–P.)

There exists an algorithm that, given Γ such that $\Gamma\backslash X$ is a compact manifold, computes

- *a simplicial complex S homotopy-equivalent to $\Gamma\backslash X$ with $O_{\dim}(V)$ simplices, and*
- *an explicit isomorphism $\pi_1(S) \to \Gamma$,*

and terminates in time $O_{\dim}(V^2)$.

Open problem: quasi-linear time complexity in V?

Remark: cost of linear algebra to compute $H^\bullet(S)$?
Dense: $O(V^\omega)$, $\omega > 2$. But the matrices are sparse.

Hecke action

Common structure of algorithms computing Hecke action on cohomology of arithmetic groups:

1. Geometric data.
2. Finite complex with no natural Hecke action.
3. Infinite complex with Hecke action.
4. Explicit equivalence between the two complexes.

Hecke action

Common structure of algorithms computing Hecke action on cohomology of arithmetic groups:

1. Geometric data: dense set F.
2. Finite complex with no natural Hecke action: $\mathcal{R}_R(F)$.
3. Infinite complex with Hecke action: $\mathcal{R}_R(\Gamma\backslash X)$.
4. Explicit equivalence between the two complexes: $\mathcal{R}_R(\Gamma\backslash X) \to \mathcal{R}_{R'}(F) \supset \mathcal{R}_R(F)$ from subdivision and projection to the closest point.

Main theorem II

Theorem (Lipnowski–P., continued)

Moreover, there exists an algorithm that, given a chain $\sigma \in C^\bullet(S)$ and a Hecke operator T, computes a chain $\tau \in C^\bullet(S)$ that is homologous to $T\sigma$, in time $O_{\dim}(V \cdot \deg T + (\deg T)^2)$.

Remarks:

- $T\sigma \notin C^\bullet(S)$;
- "homologous": same image in $H^\bullet(\Gamma\backslash X)$.

Practical considerations

Implementation

Proof-of-concept implementation in Magma

- $\mathbb{G} =$ orthogonal group of indefinite quadratic forms over number fields.
- Partially heuristic.

Goal: efficient implementation in libpari.

- More general groups $\mathbb{G}$.
- Use all improvements we know.
- Certification?

Bounds for homotopy reconstruction

The bounds for homotopy reconstruction are too large to use.

- Injectivity radius.
- Local contractibility.

Bounds for homotopy reconstruction

The bounds for homotopy reconstruction are too large to use.

- Injectivity radius $\rightsquigarrow$ work Γ**-equivariantly.**
- Local contractibility $\rightsquigarrow$ **heuristic implementation** (Rips is very stable). Possible **certification** using

$$H_\bullet(\mathcal{C}_R(F)) \hookrightarrow H_\bullet(\mathcal{R}_R(F)) \twoheadrightarrow H_\bullet(\mathcal{C}_{2R}(F)) \hookrightarrow H_\bullet(\mathcal{R}_{2R}(F)).$$

Speed of quasi-isometry tests

Quasi-isometry tests are too slow.

$\rightsquigarrow$ store set of $\gamma \in \Gamma$ computed from previous quasi-isometry tests, and use it to **quickly eliminate** many points without a full quasi-isometry test.

Size of Rips complexes

Rips complexes are very large.

$\rightsquigarrow$ use **complex simplification** algorithms (edge contraction, discrete Morse theory). In progress: combine them with Γ-equivariance.

Examples and timings

$\dim X$	|local cover|	time	$\lvert S^0\rvert$	$\lvert S^1\rvert$	$\lvert S^2\rvert$	$\lvert S^3\rvert$	$\lvert S^4\rvert$
2	2.10^3	< 1s	3	23	48	50	26
3	4.10^4	850	13	200	1400	4000	6500
4	4.10^5	2.10^3	61	3.10^3	4.10^4	3.10^5	2.10^6
5	2.10^6	$> 10^5$					

Remarks:

- Homology looks like a manifold of the correct dimension.
- Observe quadratic scaling in the volume.
- Most Betti numbers are 0 (would need congruence covers).
- Hecke action on points, but not on chains of dimension > 1 so far.

Questions?

Thank you!