Finite covers of 3-manifolds, I

Marc Lackenby

University of Oxford

Overview

Aim: To develop a systematic theory of finite covers of hyperbolic 3-manifolds.

Throughout, $M = \mathbb{H}^3/\Gamma$ = a finite volume hyperbolic 3-manifold

1. Existence of covers
2. Counting covers
3. The virtually Haken conjecture:
   - (i) Manifolds with boundary
   - (ii) Orbifolds
   - (iii) Arithmetic 3-manifolds
   - (iv) General 3-manifolds

Thanks to: Alex Lubotzky, Darren Long, Alan Reid

We'll focus on mod p homology because

- it's topological
- it relates to the algebra of linear groups
- it behaves in a surprising way for 3-manifolds
- it can be used to construct covers
- fast homology growth is related to the virtually Haken conjecture
- it gives a fairly systematic way of understanding finite covers of 3-manifolds

Motivating conjectures

Virtually Haken conjecture: M has a finite cover that is Haken

$$\Uparrow$$

Positive vb_1 conjecture: M has a finite cover $\tilde{M}$ with $b_1(\tilde{M}) > 0$.

$$\Uparrow$$

Infinite vb_1 conjecture: M has finite covers $\tilde{M}$ where $b_1(\tilde{M})$ is arbitrarily large

$$\Uparrow$$

Γ is large, i.e. some f.i. subgroup admits a surjective hm onto a non-abelian free group

Terminology: $vb_1(M) =$

$$\sup\{b_1(\tilde{M}) : \tilde{M} \text{ is a finite cover of } M\}$$

The landscape of finite covers

What types of covers? How many?

2 main types of covering groups:

- simple groups especially $\mathrm{PSL}(2,q)$, q a prime power
- p-groups ie. their order is a power of p

Proposition 1.1: Let $\tilde{M} \to M$ be a regular cover with degree a power of p. This factorises as

$$\tilde{M} = M_n \to M_{n-1} \to \ldots \to M_0 = M$$

where successive covers are regular with covering group $\mathbb{Z}/p\mathbb{Z}$.

Let $d_p(\Gamma)$ be the dimension of $H_1(\Gamma;\mathbb{Z}/p\mathbb{Z})$.

Theorem 1.2: [Lubotzky] For any prime p,

$$\sup\{d_p(\Gamma_i) : \Gamma_i \text{ is a f.i. subgroup of } \Gamma\} = \infty.$$

Theorem 1.3: [Malcev] Γ is residually finite i.e. for every non-trivial $g \in \Gamma$, there is a hm ϕ from Γ onto a finite group s.t. $\phi(g) \neq 1$.

Theorem 1.4: [Malcev] Any finitely generated, linear group is residually finite.

Proof:

$\Gamma \subset GL(n, k)$, k a field

We will keep track of an example throughout: Γ is the fundamental group of the figure-eight knot complement. Recall that this has two generators given by the matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ \omega & 1 \end{pmatrix}$$

where ω is a cube root of unity.

Let $\{g_1, \dots, g_r\}$ be a generating set for Γ s.t.

(i) $1 \in \{g_1, \dots, g_r\}$

(ii) $g \in \{g_1, \dots, g_r\} \Rightarrow g^{-1} \in \{g_1, \dots, g_r\}$

$$\{g_1, \dots, g_r\} =$$

$$\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ \pm\omega & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Let R be the subring of k generated by the matrix entries of $\{g_1, \dots, g_r\}$.

$R = \mathbb{Z}[\omega]$.

Then $\Gamma \subset GL(n, R)$.

R is an integral domain because it is a subring of a field and contains 1.

Consider an arbitrary non-trivial element $g \in \Gamma$.

$$\text{e.g. } g = \begin{pmatrix} 1 & 0 \\ \omega & 1 \end{pmatrix}$$

We will find a ring homomorphism

$$R \to \mathbb{F}$$

onto a finite field $\mathbb{F}$ which induces a hm

$$\phi\colon \Gamma \to \mathrm{GL}(n, R) \to \mathrm{GL}(n, \mathbb{F}).$$

The aim is ensure $\phi(g) \neq 1$.

Since $g \neq 1$, $g - 1$ has a non-zero entry a. eg. $a = \omega$.

1. For any integral domain R and any non-zero element a of R, there is a maximal ideal I of R such that $a \notin I$;

2. For any ideal I in an integral domain R, R/I is a field if and only if I is maximal.

3. Any field that is finitely generated as a ring is finite.

(1) $\Rightarrow$ there is a maximal ideal I in R s.t. $a \notin I$.

(2) + (3) $\Rightarrow$ R/I is a finite field.

Thus,

$$\phi\colon \Gamma \to \mathrm{GL}(n, R) \to \mathrm{GL}(n, R/I)$$

and $\phi(g) \neq 1$, as required.

Return to our example:

We must find a maximal ideal I in $\mathbb{Z}[\omega]$ not containing ω.

View $\mathbb{Z}[\omega]$ as $\mathbb{Z}[t]/(t^2 + t + 1)$. Then

$$\{\text{ideals in } \mathbb{Z}[\omega]\}$$

$$\updownarrow$$

$$\{\text{ideals in } \mathbb{Z}[t] \text{ containing } (t^2 + t + 1)\}$$

eg $I = (2, t^2 + t + 1)$.

Claim: I is maximal and $t \notin I$.

Use (2), and verify that $\mathbb{Z}[t]/(2, t^2 + t + 1)$ is a field:

Note that

$$\begin{aligned}\mathbb{Z}[t]/(2, t^2 + t + 1) &\cong \mathbb{Z}_2[t]/(t^2 + t + 1) \\ &\cong \mathbb{Z}_2(t)/(t^2 + t + 1).\end{aligned}$$

This is a field, since $t^2 + t + 1$ has no roots in $\mathbb{Z}_2$ and hence $t^2 + t + 1$ is an irreducible polynomial. Hence $t \notin (t^2 + t + 1) \subset \mathbb{Z}_2(t)$.

Thus, $\mathbb{F} = \mathbb{Z}[\omega]/(2) \cong \mathbb{Z}_2(t)/(t^2 + t + 1)$, which is the finite field with characteristic 2 and dimension 2 over $\mathbb{Z}_2$, i.e. $|\mathbb{F}| = 4$.

The required homomorphism is

$$
\begin{aligned}
\Gamma &\to SL(2,\mathbb{F}) \\
\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} &\mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\
\begin{pmatrix} 1 & 0 \\ \omega & 1 \end{pmatrix} &\mapsto \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}.
\end{aligned}
$$

$\square$ Thms 1.3 & 1.4

Fact. Γ may be conjugated by an element of $PSL(2,\mathbb{C})$ so that it lies in $PSL(2,k)$, for some number field k. e.g. $k = \mathbb{Q}(\omega)$.

The ring of integers R_k consists of those elements of the field that satisfy a monic polynomial equation

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0,$$

where each $a_i \in \mathbb{Z}$. (e.g. R_k is $\mathbb{Z}[\omega]$.)

Fact. R_k is a finitely generated ring.

Now redefine R: set it to be the ring generated by the matrix entries of $\{g_1, \ldots, g_r\}$, together with R_k. Then, still R is finitely generated and $\Gamma \subset PSL(2,R)$.

In our example, R is unchanged because it already contains R_k.

Prime ideals

Recall that an ideal I is prime if

$$xy \in I \Rightarrow x \in I \text{ or } y \in I.$$

The basic examples are the ideals (p) in $\mathbb{Z}$, where p is a prime number.

Fact. Non-zero prime ideals in R_k are maximal.

Fact. If $I \subset J$ are ideals in R_k, then $I = JJ'$ for some ideal J'.

Fact. In R_k, any non-zero ideal I_k factorises uniquely as

$$I_k = P_1^{a_1} \dots P_n^{a_n},$$

where the P_i are distinct prime ideals in R_k and each $a_i \in \mathbb{Z}_{>0}$.

Consequence 1. Any element r of R_k lies in only finitely many prime ideals.

Proof: Write $(r) = P_1^{a_1} \dots P_n^{a_n}$.

Consequence 2. For any prime $p \in \mathbb{Z}$, there is a prime ideal I_k in R_k such that R_k/I_k is a finite field of characteristic p.

Proof. Let (p) be the ideal in R_k generated by p.

Then $(p) \neq R_k$ because $1/p \notin R_k$.

Then (p) is a product of prime ideals $P_1^{a_1} \dots P_n^{a_n}$.

We claim that we may let I_k be any P_i.

R_k/P_i is a finite field.

Now, $\mathbb{Z} \cap P_i$ is an ideal in $\mathbb{Z}$ containing p, but not containing 1. Hence, $\mathbb{Z} \cap P_i = p\mathbb{Z}$.

So, for any prime $p' \neq p$, p' represents a non-zero element of R_k/P_i.

Thus, the characteristic of R_k/P_i is p. □

Reduction homomorphisms

A reduction homomorphism is

$$\Gamma \to \mathrm{PSL}(2, R) \to \mathrm{PSL}(2, R/I)$$

for some non-zero ideal I in R. 'Reduce mod I'

A principal congruence subgroup of Γ is the kernel of a reduction hm. 'Congruent to 1 mod I'

A congruence subgroup is one that contains a principal congruence subgroup.

Thm 1.5: For all but finitely many primes p, there is a reduction hm $\phi_p \colon \Gamma \to \mathrm{PSL}(2, q)$ where q is some power of p. Moreover:

1. for any non-trivial $g \in \Gamma$, $\phi_p(g) = 1$ for at most finitely many p;
2. for any f.i. subgroup Γ_1 of Γ, $\phi_p(\Gamma_1)$ is isomorphic to $\mathrm{PSL}(2, q_1)$ or $\mathrm{PGL}(2, q_1)$, where $q_1 | q$, for all but finitely many primes p.

Sketch proof

Start with a prime ideal I_k in R_k. We can arrange that R_k/I_k is a field of char any prime p. Let

$$I = \{r \in R : \exists a \in I_k, b \in R_k - I_k \text{ s.t. } r = a/b\}.$$

Can show that I is an ideal and $R/I \cong R_k/I_k$, provided we avoid finitely many p (must avoid those ideals containing denominators of the matrix entries).

Proof of 1: $g - 1 \neq 0$, and so $g - 1 \equiv 0 \bmod I$ for only finitely many I.

Proof of 2: Subgroups of $\mathrm{PSL}(2, q)$ are classified:

- soluble with derived length ≤ 2
- A_4, S_4 or A_5
- $\mathrm{PSL}(2, q_1)$ or $\mathrm{PGL}(2, q_1)$, for $q_1|q$.

Let $g \in \Gamma_1$ be a non-trivial elt in the 3^{rd} term of the derived series of Γ_1. (NB: Γ is not soluble).

Then $\phi_p(g^{60}) \neq 1$ for all but finitely many p.
So $\phi_p(\Gamma_1) \neq$ any of 1^{st} two possibilities.
So $\phi_p(\Gamma_1) \cong \mathrm{PSL}(2, q_1)$ or $\mathrm{PGL}(2, q_1)$, for $q_1 | q$.

$\square$ Thm 1.5

A version of Strong Approximation

Thm 1.6: Let $\mathcal{P}$ be any infinite set of primes. Then, for each $n \geq 1$, there is a surjective hm

$$\Gamma \to G(p_1) \times \ldots \times G(p_n)$$

where $G(p_i) \cong \mathrm{PSL}(2, q_i)$ or $\mathrm{PGL}(2, q_i)$, where q_i is a power of p_i, and each $p_i \in \mathcal{P}$.

Compare: Chinese remainder theorem:
for any distinct primes $p_1, \ldots, p_n$, reduction mod p_i gives a surjective hm

$$\mathbb{Z} \to (\mathbb{Z}/p_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/p_n\mathbb{Z}).$$

Proof

Construct the hms $\psi_n\colon \Gamma \to G(p_1) \times \ldots \times G(p_n)$ by induction on n. For $n = 1$, this is Thm 1.5. Suppose we have constructed ψ_n. Let $\Gamma_n = \ker(\psi_n)$.

By Thm 1.5, there is $p_{n+1} \in \mathcal{P}$ s.t. $\phi_{p_{n+1}}(\Gamma_n) = \mathrm{PSL}(2, q_{n+1})$ or $\mathrm{PGL}(2, q_{n+1})$, and where q_{n+1} is a power of p_{n+1}.

Claim: $\psi_n \times \phi_{p_{n+1}}$ is surjective.

Let $(A_1, \ldots, A_{n+1}) \in G(p_1) \times \ldots \times G(p_{n+1})$.

Since ψ_n is surjective, $\exists\ g \in \Gamma$ s.t. $\psi_n(g) = (A_1, \ldots, A_n)$. Let $B_{n+1} = \phi_{p_{n+1}}(g)$.

$\exists k \in \ker(\psi_n)$ s.t. $\phi_{p_{n+1}}(k) = A_{n+1}(B_{n+1})^{-1}$.

$$(\psi_n \times \phi_{p_{n+1}})(kg) = (A_1, \ldots, A_{n+1}).$$

$\square$ Thm 1.6

Theorem 1.2: [Lubotzky] For any prime p,

$$\sup\{d_p(\Gamma_i) : \Gamma_i \text{ is a f.i. subgroup of } \Gamma\} = \infty.$$

We need:

Theorem: [Dirichlet] For any coprime integers a and q, there infinitely many primes congruent to a mod q.

Proof of Thm 1.2: Let $\mathcal{P}$ be the primes congruent to 1 mod p. (When $p = 2$, define $\mathcal{P}$ to be the primes congruent to 1 mod 4.)

By Dirichlet, $|\mathcal{P}| = \infty$.

By 1.6, can find a surj hm

$$\psi\colon \Gamma \to G(p_1) \times \ldots \times G(p_n)$$

where each $p_i \in \mathcal{P}$.

The diagonal subgroup of $G(p_i)$ is isomorphic to $\mathbb{F}_{q_i}^*/\{\pm 1\}$ (where $\mathbb{F}_{q_i}^*$ is the group of units in $\mathbb{F}_{q_i}$). This contains $\mathbb{F}_{p_i}^*/\{\pm 1\}$. This is cyclic of order $(p_i - 1)/2$, and so contains a cyclic group C_i of order p (by our choice of $\mathcal{P}$).

Let $\Gamma_1 = \psi^{-1}(C_1 \times \ldots \times C_n)$.

Let $\Gamma_2 = \ker(\psi)$.

Then $\Gamma_2 \triangleleft \Gamma_1$ are f.i. subgps of Γ, and $\Gamma_1/\Gamma_2 \cong (\mathbb{Z}_p)^n$.

So, $d_p(\Gamma_1) \geq n$.

$\square$ Thm 1.2.