LENGTH MULTIPLICITIES OF HYPERBOLIC 3-MANIFOLDS

BY

JOSEPH D. MASTERS*

Department of Mathematics, University of Texas at Austin
Austin, TX 78712, USA
e-mail: masters@math.utexas.edu

ABSTRACT

Let $M = \mathbb{H}^3/\Gamma$ be a hyperbolic 3-manifold, where Γ is a non-elementary Kleinian group. It is shown that the length spectrum of M is of unbounded multiplicity.

1. Introduction

This paper is concerned with length multiplicities in hyperbolic 3-manifolds, or more generally, in hyperbolic 3-orbifolds. Let $M = \mathbb{H}^3/\Gamma$ be a hyperbolic 3-orbifold, where Γ is a non-elementary Kleinian group. We say that $\gamma \in \Gamma$ is **loxodromic** if $\mathrm{tr}^2\gamma \notin [0,4]$ (note that this includes "hyperbolic" elements). Every loxodromic element $\gamma \in \Gamma$ has an associated **complex length**, denoted $\ell_0(\gamma) = \ell + i\theta$, which describes the action of γ on $\mathbb{H}^3$: along its invariant axis γ translates a distance ℓ and rotates an angle θ. We say that a complex length has **multiplicity** n if it is shared by exactly n conjugacy classes in Γ. We define the **complex length spectrum**, $\mathcal{L}(M)$, to be the set of complex lengths of loxodromic elements of Γ, counted with multiplicity.

The **real length spectrum** of M is defined to be the set of lengths of closed geodesics of M. The real length spectrum of M is essentially the real part of $\mathcal{L}(M)$ — the only difference being that the classes of γ and γ^{-1} are now equivalent.

[*] *Current address*: Department of Mathematics-MS 136, Rice University, Houston, TX 77005-1892, USA; *e-mail*: mastersj@rice.edu

Received December 7, 1998

Since $\Gamma \subset \mathrm{PSL}_2(\mathbb{C})$, $\mathrm{tr}(\gamma)$ is well-defined, up to sign, for any $\gamma \in \Gamma$. The connection between traces and lengths is given by the following formula:

$$\ell_0(\gamma) = 2\cosh^{-1}\left(\frac{\mathrm{tr}\,\gamma}{2}\right). \tag{1}$$

Following [GR], we define, for any group Γ, the **trace class** of an element $\gamma \in \Gamma$ to be the set of elements $\gamma' \in \Gamma$ for which $\mathrm{tr}\,\rho(\gamma') = \mathrm{tr}\,\rho(\gamma)$ for *all* representations $\rho\colon \Gamma \to \mathrm{SL}_2(\mathbb{C})$. We define the **stable multiplicity** of γ to be the number of conjugacy classes in the trace class of γ. Recall that a representation into $\mathrm{SL}_2(\mathbb{C})$ is called **irreducible** if its image fixes no 1-dimensional subspaces of $\mathbb{C}^2$.

We shall prove:

THEOREM 1.1: *Let Γ be a finitely generated group which admits an infinite irreducible representation into $\mathrm{SL}_2(\mathbb{C})$. Then Γ has trace classes of unbounded stable multiplicity.*

In Section 2 we prove that Theorem 1.1 has the following consequence:

THEOREM 1.2: *Let $M = \mathbb{H}^3/\Gamma$ be a hyperbolic 3-orbifold, where Γ is a finitely generated, non-elementary Kleinian group. Then $\mathcal{L}(M)$ is of unbounded multiplicity.*

COROLLARY 1.3: *If M is a finite-volume, complete hyperbolic 3-manifold, then $\mathcal{L}(M)$ is of unbounded multiplicity.*

COROLLARY 1.4: *If M is a finite-volume, complete hyperbolic 3-manifold, then the real length spectrum of M is of unbounded multiplicity.*

The analogous statement for hyperbolic surfaces was proved by Randol (see [R]). We have reproduced the short proof in Section 3.

It is well-known that the length spectrum of an arithmetic hyperbolic 3-manifold has unbounded multiplicity. In fact, if M is arithmetic, then the mean multiplicity, $n(\ell_0)$, of a length grows exponentially with ℓ_0 (see [M]).

Recent interest in length multiplicities of hyperbolic 3-manifolds has been sparked by connections with chaotic quantum systems. See [Sar] for more information.

ACKNOWLEDGEMENT: I would like to thank Professors Fernando Rodriguez Villegas, John Tate and Cameron Gordon for useful conversations, Professor Peter Sarnak for valuable correspondence, the referee for helpful comments and Professor Alan Reid for his help and encouragement.

2. Theorem 1.1 implies Theorem 1.2

In this section, we prove:

CLAIM: *Theorem 1.1 implies Theorem 1.2.*

Proof of Claim: By Selberg's Lemma, Γ has a torsion-free subgroup Γ' of finite index n, say. Any set of more than n elements which are pairwise non-conjugate in Γ' must contain at least two elements which are non-conjugate in Γ. Also, any representation of Γ restricts to a representation of Γ'. Therefore the stable multiplicities in Γ' will increase by at most a factor of n. So it is enough to consider the case where Γ is torsion-free.

Let π: $\mathrm{SL}_2(\mathbb{C}) \to \mathrm{PSL}_2(\mathbb{C})$ be the natural projection. By [T], a non-elementary, torsion-free Kleinian group Γ admits a faithful representation ρ: $\Gamma \to \pi^{-1}(\Gamma)$ such that $\pi\rho = id$. Note that ρ preserves trace (up to sign), and that ρ is irreducible, since Γ is non-elementary. Then, in the case that Γ contains no parabolic elements, Theorem 1.2 is now an easy consequence of Theorem 1.1 and Equation (1).

In general, however, we must make sure that Γ has trace classes with an unbounded number of *loxodromic* conjugacy classes. The claim will be proved once we show that any trace class in Γ can contain only a bounded number of conjugacy classes of parabolic elements. This is done in the following lemma:

LEMMA 2.1: *Let Γ be a finitely generated Kleinian group. Then there is an integer $N > 0$ such that no trace class of Γ contains more than N conjugacy classes of parabolic elements. Moreover, if Γ is geometrically finite, then a trace class of Γ can contain at most two conjugacy class of parabolic elements.*

The proof of this lemma will require some definitions.

Let Γ be a finitely generated group. The **space of characters**, $V(\Gamma)$, is the set of all characters of representations of Γ into $\mathrm{SL}_2(\mathbb{C})$. By [CS], $V(\Gamma)$ has the structure of an affine algebraic set defined over $\mathbb{Q}$. The character of a representation ρ is denoted χ_ρ.

A **quasiconformal deformation of** Γ is a representation of Γ into $\mathrm{PSL}_2(\mathbb{C})$ which is induced by a quasiconformal homeomorphism of the Riemann sphere $\hat{\mathbb{C}}$. We say that a representation of Γ into $\mathrm{SL}_2(\mathbb{C})$ is quasiconformal if it is the lift of a quasiconformal deformation of Γ into $\mathrm{PSL}_2(\mathbb{C})$.

Proof of Lemma 2.1: Using Selberg's Lemma as above, we may assume Γ is torsion-free, so the identity representation lifts to a representation ρ_0: $\Gamma \to \mathrm{SL}_2(\mathbb{C})$.

By the compact core theorem ([Sc]), Γ can contain only finitely many conjugacy classes of maximal parabolic subgroups. Let $\alpha_1, \beta_1, \ldots, \alpha_n, \beta_n$ generate the conjugacy classes of rank 2 maximal parabolic subgroups and $\gamma_1, \ldots, \gamma_m$ generate the conjugacy classes of rank 1 maximal parabolic subgroups.

First, suppose Γ is finite covolume, so there are no γ_i's. We shall handle this case with Thurston's hyperbolic Dehn surgery theory.

Let $V_0(\Gamma)$ denote the irreducible component of $V(\Gamma)$ containing χ_{ρ_0}. Consider the map τ: $V_0(\Gamma) \to \mathbb{C}^n$ defined by

$$\tau(\chi_\rho) = (\chi_\rho(\alpha_1), \chi_\rho(\alpha_2), \ldots, \chi_\rho(\alpha_n)) = (\operatorname{tr}\rho(\alpha_1), \operatorname{tr}\rho(\alpha_2), \ldots, \operatorname{tr}\rho(\alpha_n)).$$

By Chapter 5 of [T], the image of τ covers an open neighborhood U of $(2, 2, \ldots, 2)$. So given two parabolic elements on distinct cusps, we can make one loxodromic while the other remains parabolic. In particular, for any $i \neq j$, and any integers m_1, n_1, m_2, n_2 (not all 0) there is a representation ρ for which $\operatorname{tr}\rho(\alpha_i^{m_1}\beta_i^{n_1}) \neq \operatorname{tr}\rho(\alpha_j^{m_2}\beta_j^{n_2})$, so $\alpha_i^{m_1}\beta_i^{n_1}$ and $\alpha_j^{m_2}\beta_j^{n_2}$ are not in the same trace class.

Now suppose we are given two distinct, non-trivial parabolic elements $\alpha_i^{m_1}\beta_i^{n_1}$ and $\alpha_i^{m_2}\beta_i^{n_2}$ on the same cusp. Suppose also that the elements are not in the same cyclic subgroup. Then Thurston's hyperbolic Dehn surgery theory shows that there is a representation taking one of the elements to the identity and the other to a loxodromic element, so they are in distinct trace classes. If the two elements are in the same cyclic subgroup, then by mapping them to loxodromics we see that they are in distinct trace classes, provided they are not inverses of each other.

It follows that we can find characters of representations in $\tau^{-1}(U)$ which differ on any distinct pair of parabolic elements in Γ which are not inverses of each other, concluding the case where Γ has finite covolume.

If Γ is geometrically finite, then by [Br] there is a quasiconformal deformation Γ' of Γ and a finite covolume Kleinian group Γ^* for which $\Gamma' \subset \Gamma^*$. Since a quasiconformal deformation takes parabolics to parabolics, the proof of this case now follows from the proof of the finite covolume case.

In general, if Γ is any finitely generated Kleinian group, then Γ has a faithful discrete representation ρ for which $\rho(\Gamma)$ is geometrically finite, $\rho(\alpha_i)$ and $\rho(\beta_i)$ are parabolic for all i, and $\rho(\gamma_i)$ is loxodromic for all i; this is Theorem 2.3 of [A] and follows from the Scott core theorem and the Thurston uniformization theorem. By the geometrically finite case, any two elements of the form $\alpha_i^r\beta_j^s$ in the same trace class of Γ must be inverses of each other. So a trace class of Γ can contain at most two elements of the form $\alpha_i^r\beta_j^s$. And since $\rho(\gamma_i)$ is loxodromic,

$\operatorname{tr}\rho(\gamma_i^r) \neq \operatorname{tr}\rho(\gamma_i^s)$ if $|r| \neq |s|$, so γ_i^r and γ_i^s are not in the same trace class in Γ, and a trace class in Γ can contain at most $2m$ elements of the form γ_i^r (as i goes from 1 to m). Therefore a trace class in Γ can contain at most $2(m+1)$ conjugacy classes of parabolic elements, and the lemma is proved. ∎

3. Background and the idea of the proof

Suppose ρ is an irreducible representation of Γ into $\mathrm{SL}_2(\mathbb{C})$. We first must find elements in $\rho(\Gamma)$ with the same trace. This can be done as in [H], with the aid of simple trace identities. For example, it is proved in [H] that $\operatorname{tr}(a^2bab^{-1}) = \operatorname{tr}(ba^2b^{-1}a)$ for any elements a and b in $\mathrm{SL}_2(K)$, where K is any field. Then a^2bab^{-1} and $ba^2b^{-1}a$ are in the same trace class in Γ. In Section 4, we will use these identities to construct sequences of words in Γ, all in the same trace class.

The problem, then, is to show that these words are not conjugate in Γ. This is done by finding a homomorphism of Γ onto a finite group G, and showing that the images of the words are not conjugate in G.

This technique is nicely illustrated in the 2-dimensional case. The proof we give of the following theorem is a slight modification of the one which appears in [R].

THEOREM 3.1 (Randol): *Let $M = \mathbb{H}^2/\Gamma$ be a finite-volume hyperbolic surface. Then Γ contains trace classes of unbounded stable multiplicity, and $\mathcal{L}(M)$ contains lengths of unbounded multiplicity.*

Proof: First, let us assume M is compact.

$\Gamma \subset \mathrm{PSL}_2(\mathbb{R})$ is a Fuchsian group, which can be embedded into $\mathrm{SL}_2(\mathbb{R})$ so that traces are preserved up to sign. Then by Equation (1), it is enough to prove that $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ has trace classes of unbounded stable multiplicity.

Γ has the standard presentation:

$$\Gamma = < a_1, b_1, a_2, b_2, \ldots, a_g, b_g | \; (a_1b_1a_1^{-1}b_1^{-1}) \ldots (a_gb_ga_g^{-1}b_g^{-1}) = 1 > .$$

Note that there is a natural surjection

$$\phi \colon \Gamma \to < a_1 > * < a_2 > * \ldots * < a_g > .$$

In particular, a_1 and a_2 generate a free group F.

It follows from [H] that if x and y freely generate a free subgroup F of Γ, then for any N there are words $w_1, \ldots, w_N$ in x and y such that

1. $w_i(x,y)$ and $w_j(x,y)$ are in the same trace class $\forall i,j \leq N$,

2. $w_i(x,y)$ is not conjugate in F to $w_j(x,y) \forall i \neq j$.

Consider the words $w_1(a_1,a_2),\ldots,w_N(a_1,a_2)$. By 1, we have $w_i(a_1,a_2)$ and $w_j(a_1,a_2)$ are in the same trace class $\forall i,j$. By 2, we have that any distinct pair $w_i(a_1,a_2)$, $w_j(a_1,a_2)$ are not conjugate in F, hence their images are not conjugate in $< a_1 > * \ldots * < a_g >$, hence $w_i(a_1,a_2)$ and $w_j(a_1,a_2)$ are not conjugate in Γ. This proves the theorem in the compact case.

If M is non-compact, then Γ is free. Then the same proof works to show that Γ contains trace classes of unbounded stable multiplicity. The only complication is in passing to the statement about $\mathcal{L}(M)$, for the elements of the trace class may be parabolic. However, Γ admits faithful representations into $\mathrm{SL}_2(\mathbb{C})$ for which every element becomes loxodromic, and therefore, as in the proof of Lemma 2.1, we see that a trace class can contain at most $2n$ conjugacy classes of parabolic elements, where n is the number of cusps, and the result follows. ∎

The proof in three dimensions is more complicated, as hyperbolic 3-manifold groups do not generally surject onto non-abelian free groups. For example, if the manifold has zero first Betti number, such as a non-zero surgery on the figure-eight knot, then its fundamental group cannot surject onto any free group.

However, hyperbolic 3-manifold groups do surject onto groups of the form $\mathrm{PSL}_2(\mathbb{F}_{p^i})$, where $\mathbb{F}_{p^i}$ denotes the finite field of order p^i. In Sections 5 and 6, we shall review the construction of these homomorphisms.

So the idea is to use [H] to construct a sequence of words $w_i(a,b)$ in the free group F on a and b which are not conjugate in F but which are in the same trace class of F. We map these words into Γ; their images will be in the same trace class of Γ. Then we map the words from Γ into a group of the form $\mathrm{PSL}_2(\mathbb{F}_p)$, and hope that these images will be non-conjugate in $\mathrm{PSL}_2(\mathbb{F}_p)$, so the words will be non-conjugate in Γ. However, by [H], the traces of the images are equal (up to sign) in $\mathrm{PSL}_2(\mathbb{F}_p)$, and it is nearly true that two elements of $\mathrm{PSL}_2(\mathbb{F}_p)$ are conjugate if and only if they have the same trace. Therefore care is needed in the choice of the words and the primes.

4. Trace identities

All of the trace identities which we shall use are ultimately based on the following lemma.

Lemma 4.1 (Horowitz): *Suppose K is a field, $a,b \in \mathrm{SL}_2(K)$ with $\mathrm{tr}\, a = \mathrm{tr}\, b$, and $W(x,y)$ is a word in x and y. Then $\mathrm{tr}(W(a,b)) = \mathrm{tr}(W(b,a))$.*

Proof: It is proved in [H] (see also [CS]) that there is a 3-variable polynomial P

over K such that $\operatorname{tr}(W(a,b)) = P(\operatorname{tr} a, \operatorname{tr} b, \operatorname{tr} ab)$, for any elements $a, b \in \mathrm{SL}_2(K)$. Then $\operatorname{tr}(W(b,a)) = P(\operatorname{tr} b, \operatorname{tr} a, \operatorname{tr} ba)$. We have assumed that $\operatorname{tr} a = \operatorname{tr} b$, and for any matrices in $\mathrm{SL}_2(K)$, $\operatorname{tr} ab = \operatorname{tr} ba$, so the lemma follows. ∎

In Section 3, we gave the example $\operatorname{tr}(a^2bab^{-1}) = \operatorname{tr}(ba^2b^{-1}a)$ for any elements $a, b \in \mathrm{SL}_2(K)$. This follows by setting $W(x,y) = x^2y$ and noting that $\operatorname{tr}(W(a, bab^{-1})) = \operatorname{tr}(W(bab^{-1}, a))$ by Lemma 4.1.

We shall now construct the required elements of the same trace in $\rho(\Gamma)$ which we need to prove Theorem 1.1. We remark that one can construct much simpler sequences of elements of equal trace; however, in Section 6 we shall require the words to be of this special form in order to prove they are non-conjugate.

We now recursively define words $w_{n,i}$, for $i \le n+1$. In what follows, we routinely supress the dependence of these words on a,b, p_i, q_i and k_i; we will explain how to choose them later.

Let

$$\begin{aligned}
W_n(x,y) &= (x^{p_n-1+q_n}y^{-q_n})^{k_n}x(x^{p_n-1+q_n}y^{-q_n})x^{-1},\\
\bar{W}_n(x,y) &= x(x^{p_n-1+q_n}y^{-q_n})^{k_n}x^{-1}(x^{p_n-1+q_n}y^{-q_n}),\\
w_{1,1} &= W_1(a,b)\\
&= (a^{p_1-1+q_1}b^{-q_1})^{k_1}a(a^{p_1-1+q_1}b^{-q_1})a^{-1},\\
w_{1,2} &= \bar{W}_1(a,b).\\
&= a(a^{p_1-1+q_1}b^{-q_1})^{k_1}a^{-1}(a^{p_1-1+q_1}b^{-q_1}),\\
w_{2,1} &= W_2(w_{1,1},w_{1,2})\\
&= (w_{1,1}^{p_2-1+q_2}w_{1,2}^{-q_2})^{k_2}w_{1,1}(w_{1,1}^{p_2-1+q_2}w_{1,2}^{-q_2})w_{1,1}^{-1},\\
w_{2,2} &= \bar{W}_2(w_{1,1},w_{1,2})\\
&= w_{1,1}(w_{1,1}^{p_2-1+q_2}w_{1,2}^{-q_2})^{k_2}w_{1,1}^{-1}(w_{1,1}^{p_2-1+q_2}w_{1,2}^{-q_2}),\\
w_{2,3} &= W_2(w_{1,2},w_{1,1})\\
&= (w_{1,2}^{p_2-1+q_2}w_{1,1}^{-q_2})^{k_2}w_{1,2}(w_{1,2}^{p_2-1+q_2}w_{1,1}^{-q_2})w_{1,2}^{-1}.
\end{aligned}$$

Assume that $w_{n-1,i}$ has been defined for $i \le n$, and that $w_{n-1,1}$ and $w_{n-1,2}$ are both words in $w_{n+1-i,1}$ and $w_{n+1-i,2}$ for each i with $3 \le i \le n$ (note that this property is vacuous for $n = 2$, the base case of the recursion).

Define

$$w_{n,1} = W_n(w_{n-1,1}, w_{n-1,2}), \quad w_{n,2} = \bar{W}_n(w_{n-1,1}, w_{n-1,2}).$$

We claim that $w_{n,1}$ and $w_{n,2}$ are both words in $w_{n+2-i,1}$ and $w_{n+2-i,2}$ for $3 \leq i \leq n+1$.

Indeed, since $w_{n-1,1}$ and $w_{n-1,2}$ are words in $w_{n+1-i,1}$ and $w_{n+1-i,2}$ for $3 \leq i \leq n$, then $w_{n,1}$ and $w_{n,2}$ are both words in $w_{n+2-i,1}$ and $w_{n+2-i,2}$ for $4 \leq i \leq n+1$. And for $i = 3$, it is obvious that $w_{n,1}$ and $w_{n,2}$ are words in $w_{n-1,1}$ and $w_{n-1,2}$.

Then we define:

$$w_{n,i} = w_{n,1}^{[i]} \quad \text{for } 3 \leq i \leq n+1,$$

where, if $w_{n,j}$ is a word in $w_{n+2-i,1}$ and $w_{n+2-i,2}$, $w_{n,j}^{[i]}$ denotes the word obtained by switching $w_{n+2-i,1}$ and $w_{n+2-i,2}$.

This gives a well-defined sequence of words $w_{n,i}$ for any positive integers $n, i \leq n+1$.

The following formulas, which are just formal consequences of our notation, will be useful:

$$\begin{aligned}
w_{n,3} =& w_{n,1}^{[3]}\\
=& W_n(w_{n-1,2}, w_{n-1,1})\\
=& (w_{n-1,2}^{p_n-1+q_n} w_{n-1,1}^{-q_n})^{k_n} w_{n-1,2} (w_{n-1,2}^{p_n-1+q_n} w_{n-1,1}^{-q_n}) w_{n-1,2}^{-1} \quad \text{for } n \geq 2,\\
w_{n,i} =& w_{n,1}^{[i]}\\
=& W_n(w_{n-1,1}^{[i-1]}, w_{n-1,2}^{[i-1]})\\
=& [(w_{n-1,1}^{[i-1]})^{p_n-1+q_n} (w_{n-1,2}^{[i-1]})^{-q_n}]^{k_n}\\
& \qquad w_{n-1,1}^{[i-1]} [(w_{n-1,1}^{[i-1]})^{p_n-1+q_n} (w_{n-1,2}^{[i-1]})^{-q_n}] (w_{n-1,1}^{[i-1]})^{-1},\\
& \text{for } n \geq 3 \text{ and } 4 \leq i \leq n+1.
\end{aligned}$$

Regardless of the choices of a, b, p_i and q_i, we have:

PROPOSITION 4.2: *Let K be a field, and let $a, b \in \mathrm{SL}_2(K)$. Then $\mathrm{tr}(w_{i,j}) = \mathrm{tr}(w_{i,k})$ for all $j, k \leq i+1$.*

We shall require the following lemma:

LEMMA 4.3: $\mathrm{tr}(W_n(x,y)) = \mathrm{tr}(\bar{W}_n(x,y))$ *for any n and any $x, y \in K$.*

Proof: Letting $U_n(x,y) = x^{k_n} y$, we have

$$\begin{aligned}
\mathrm{tr}(W_n(x,y)) &= \mathrm{tr}(U_n(x^{p_n-1+q_n} y^{-q_n}, x(x^{p_n-1+q_n} y^{-q_n}) x^{-1}))\\
&= \mathrm{tr}(U_n(x(x^{p_n-1+q_n} y^{-q_n}) x^{-1}, x^{p_n-1+q_n} y^{-q_n}))\\
&\qquad\qquad\qquad\qquad \text{(by Lemma 4.1)}\\
&= \mathrm{tr}(\bar{W}_n(x,y)). \qquad ∎
\end{aligned}$$

Proof of Proposition 4.2: We proceed by induction. By Lemma 4.3, $\mathrm{tr}(w_{1,1}) = \mathrm{tr}(w_{1,2})$.

Now, suppose that $\mathrm{tr}(w_{n-1,i}) = \mathrm{tr}(w_{n-1,j})$ for all $i, j \leq n$.

By Lemma 4.3, $\mathrm{tr}(w_{n,1}) = \mathrm{tr}(w_{n,2})$. For $3 \leq i \leq n+1$, recall that $w_{n,1} = U(w_{n+2-i,1}, w_{n+2-i,2})$ for some word U; therefore we have:

$$\begin{aligned}\mathrm{tr}(w_{n,1}) &= \mathrm{tr}(U(w_{n+2-i,1}, w_{n+2-i,2})) \text{ for some word } U\\ \mathrm{tr}(w_{n,i}) &= \mathrm{tr}(w_{n,1}^{[i]})\\ &= \mathrm{tr}(U(w_{n+2-i,2}, w_{n+2-i,1})).\end{aligned}$$

By the inductive hypothesis, $\mathrm{tr}(w_{n+2-i,1}) = \mathrm{tr}(w_{n+2-i,2})$, so $\mathrm{tr}(w_{n,1}) = \mathrm{tr}(w_{n,i})$, by Lemma 4.1. ∎

5. Algebraic representations

The existence of maps from Γ onto the groups $\mathrm{PSL}_2(\mathbb{F}_{p_i})$ depends on the existence of an algebraic representation of Γ, defined as follows:

ρ: $\Gamma \to \mathrm{SL}_2(\mathbb{C})$ is an **algebraic representation** if it is irreducible and its image is an infinite subgroup of $\mathrm{SL}_2(\bar{\mathbb{Q}})$, where $\bar{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$. Note that this differs slightly from the definition given in [LR].

The purpose of this section is to show that any group Γ satisfying the hypotheses of Theorem 1.1 admits an algebraic representation.

LEMMA 5.1: *Let Γ be a finitely generated group which admits an infinite irreducible representation ρ_0: $\Gamma \to \mathrm{SL}_2(\mathbb{C})$. Then Γ admits an algebraic representation.*

Proof of Lemma 5.1: Let $V_0(\Gamma)$ be the irreducible component of $V(\Gamma)$ containing the character χ_{ρ_0} of the representation ρ_0 (recall the definition of $V(\Gamma)$ in Section 2).

If $\dim(V_0(\Gamma)) = 0$, then it is a well known fact that the coordinates of χ_{ρ_0} must be algebraic; in other words the image of χ_{ρ_0} must lie in $\bar{\mathbb{Q}}$. Then it follows from [Ba] that ρ_0 is conjugate to an algebraic representation.

So suppose $\dim(V_0(\Gamma)) > 0$. For $\gamma \in \Gamma$, define the function τ_γ: $V_0(\Gamma) \to \mathbb{C}$ by $\tau_\gamma(\chi_\rho) = \chi_\rho(\gamma) = \mathrm{tr}\,\rho(\gamma)$. Recall, by [H] or [CS], that a character is determined by the values it takes on a finite set of elements $\gamma_1, \ldots, \gamma_n \in \Gamma$. Then since $\dim(V_0(\Gamma)) > 0$, there is some γ_i for which τ_{γ_i} is non-constant; let us assume it is γ_1. Since τ_{γ_1} is a non-constant polynomial map, it is surjective. Now, all the characters in some neighborhood U of χ_{ρ_0} will correspond to infinite irreducible representations. $\tau_{\gamma_1}(U)$ is an open set in $\mathbb{C}$, and therefore contains an algebraic number α. Let $\rho_1 \in \tau_{\gamma_1}^{-1}(\alpha)$; ρ_1 is infinite and irreducible, because it is in U.

Suppose α has a minimal polynomial f with coefficients in $\mathbb{Z}$. Consider the algebraic subset $A_1(\Gamma) \subset V_0(\Gamma)$ obtained by adding the polynomial condition $f(\tau_{\gamma_1}(\chi_\rho)) = 0$. $A_1(\Gamma)$ is non-empty, since it contains ρ_1. Let $V_1(\Gamma)$ denote the irreducible component of $A_1(\Gamma)$ containing χ_{ρ_1}. Note that any character in $V_1(\Gamma)$ will map γ_1 to an algebraic number (in fact to a root of f).

If $\dim(V_1(\Gamma)) = 0$, then, as above, we have that ρ_1 is conjugate to an algebraic representation, and we are done. If $\dim(V_1(\Gamma)) > 0$, then we can assume that τ_{γ_2} is non-constant on V_1, and then, as above, we can find an infinite irreducible representation $\rho_2 \in V_1$ for which χ_{ρ_2} is algebraic. Then we form the set $V_2(\Gamma)$, and so on. Eventually, the process will terminate, when

i. $\dim(V_m(\Gamma)) = 0$ for some m, in which case we will get an algebraic representation, or

ii. we have found an infinite irreducible representation ρ such that $\chi_\rho(\gamma_i)$ is algebraic for all $i \leq n$. Since χ_ρ is a polynomial in the $\chi_\rho(\gamma_i)$'s, then $\chi_\rho(\gamma)$ is algebraic for all $\gamma \in \Gamma$, and therefore by [Ba], ρ is conjugate to an algebraic representation. ∎

6. Lemmas from group theory and number theory

In this section we prove some lemmas which will be useful later, and we review the construction of the homomorphisms of Γ into $\mathrm{PSL}_2(\mathbb{C})$ alluded to in Section 3. For a more complete treatment of this construction, see [LR]. For background on algebraic number theory, see [N].

Let ρ be an algebraic representation of Γ (see Section 5), and let $\mathbb{Q}(\mathrm{tr}\,\rho(\Gamma)) = \mathbb{Q}(\{\mathrm{tr}\,\rho(\gamma) | \gamma \in \Gamma\})$. Since ρ is algebraic, this is a finite extension of $\mathbb{Q}$. It will be more convenient to work with the Galois closure, denoted $\overline{\mathbb{Q}(tr\rho\Gamma)}$. This is also a finite extension, of degree N, say. Let $\mathcal{O}$ denote the ring of integers of $\overline{\mathbb{Q}(\mathrm{tr}\,\rho(\Gamma))}$. It follows from the general theory of linear groups that for all but finitely many primes $p \in \mathbb{Z}$, there is a homomorphism $\phi_p\colon \Gamma \to \mathrm{PSL}_2(\mathbb{F}_{p^i})$, where $\mathbb{F}_{p^i}$ is the residue field of a prime ideal $P \subset \mathcal{O}$ lying over p. In particular, if p **splits completely** in $\overline{\mathbb{Q}(\mathrm{tr}\,\rho(\Gamma))}$ — i.e. factors into N distinct prime ideals in $\mathcal{O}$ — then ϕ_p maps into $\mathrm{PSL}_2(\mathbb{F}_p)$.

Since we shall require maps into groups of the form $\mathrm{PSL}_2(\mathbb{F}_p)$, it will be useful to know how many primes in $\mathbb{Z}$ split completely in $\overline{\mathbb{Q}(\mathrm{tr}\,\rho(\Gamma))}$. To give a precise answer requires the notion of natural density.

Let A be a set of primes in $\mathbb{Z}$. A is said to have **natural density** δ if

$$\lim_{t\to\infty}\left(\frac{\#\text{ of primes in } A < t}{\#\text{ of primes in } \mathbb{Z} < t}\right) = \delta.$$

We may now state a simple version of the Tchebotarev Density Theorem (see [L] p. 128).

THEOREM 6.1 (Tchebotarev density): *Let K be a Galois extension of $\mathbb{Q}$ of degree N, and let $P = \{$primes in $\mathbb{Z}$ which split completely in $K\}$. Then the natural density of P is $1/N$. In particular, P is infinite.*

In fact, if p splits completely, then ϕ_p will almost always *surject* onto $\mathrm{PSL}_2(\mathbb{F}_p)$. The following theorem follows directly from the proof of Theorem 1.2 in [LR]:

THEOREM 6.2 (Long–Reid): *Let Γ be a finitely generated group which admits an algebraic representation ρ. Let $\mathcal{P} = \{$primes in $\mathbb{Z}$ which split completely in $\mathbb{Q}(\mathrm{tr}\,\rho(\Gamma))\}$, so that, for all but finitely many $p \in P$, the map $\phi_p\colon \Gamma \to \mathrm{PSL}_2(\mathbb{F}_p)$ exists (see above). Then for all but finitely many $p \in \mathcal{P}$, ϕ_p is a surjection.*

We will in fact require Γ to surject onto a product of finite linear groups, prompting the following group theoretic lemma:

LEMMA 6.3: *Let Γ be a group, and supppose Γ surjects onto a sequence $G_1, \ldots, G_n$ of distinct, finite simple groups. Then Γ surjects onto the direct product $\Pi_{i=1}^n G_i$.*

Proof: We are given surjections $\phi_i\colon \Gamma \to G_i$. Let $\phi_1 \times \cdots \times \phi_n\colon \Gamma \to \Pi_{i=1}^n G_i$ denote the natural map induced by the ϕ_i's. Let H denote the image of Γ under $\phi_1 \times \cdots \times \phi_n$.

Let

$$(*) \quad 1 = N_k \lhd N_{k-1} \lhd \cdots \lhd N_1 \lhd N_0 = H$$

be a chief series for H — i.e. each N_i is normal in N_{i-1}, and each quotient N_{i-1}/N_i is simple. The Jordan–Holder Theorem (see [I], p. 132) guarantees that such a series exists, and that the quotient groups are unique up to re-ordering.

Let $\pi_i\colon H \to G_i$ be the natural projection map. Since ϕ_i surjects Γ onto G_i, π_i surjects H onto G_i. Since $H/\ker\pi_i \cong G_i$ is simple, it follows that H has another chief series in which $\ker\pi_i$ is the first term (again see [I]). Therefore for each i, G_i must appear as one of the quotients in the series $(*)$. Therefore

$$\begin{aligned}|H| \geq& \Pi_{i=0}^{k-1}|N_i/N_{i+1}| \leq \Pi_{i=1}^n |G_i|\\ =&|\Pi_{i=1}^n G_i|.\end{aligned}$$

Therefore $H = \Pi_{i=1}^{n} G_i$, and so $\phi_1 \times \cdots \times \phi_n$ is onto, proving the lemma. ∎

LEMMA 6.4: *Let K be a Galois extension of degree N over $\mathbb{Q}$, and let $\mathcal{P} = \{$primes in $\mathbb{Z}$ which split completely in $K\}$. Let $p_1, \ldots, p_{n-1} \in \mathcal{P}$ with the property that $p_1 > 8N$ and $p_i > 2p_{i-1}$ for all $1 < i < n$. Then, given any two integers r and s, there exist infinitely many primes in $\mathcal{P}$ which are not congruent to r or s mod p_i for any $i < n$.*

Proof: By Theorem 6.1, $\mathcal{P}$ has natural density $1/N$ in $\mathbb{Z}$.

It follows from a more general version of Theorem 6.1 (see [L], p. 128) that if p_i does not divide r or s, then the set of primes in $\mathbb{Z}$ which are congruent to r mod p_i has natural density $1/(p_i - 1)$, as does the set congruent to s mod p_i.

Therefore, for large integers m we have:

$$\begin{aligned}
&\frac{|\text{primes } p < m\colon p \in P \text{ and } p \not\equiv r \text{ or } s (\operatorname{mod} p_1, \ldots, \text{ or } p_{n-1})|}{|\text{primes} < m|} \\
&= \frac{|\text{primes } p < m\colon p \in P|}{|\text{primes } p < m|} \\
&\qquad - \frac{|\text{primes } p < m\colon p \equiv r \text{ or } s (\operatorname{mod} p_1, \ldots, \text{ or } p_n)|}{|\text{primes } p < m|} \\
&\geq \frac{1}{|\text{primes } p < m|}[|\text{primes } p < m\colon p \in P| \\
&\quad - |\text{primes } p < m\colon p \equiv r (\operatorname{mod} p_1)| - \cdots \\
&\quad - |\text{primes } p < m\colon p \equiv r (\operatorname{mod} p_{n-1})| \\
&\quad - |\text{primes } p < m\colon p \equiv s (\operatorname{mod} p_1)| \\
&\quad - \cdots - |\text{primes } p < m\colon p \equiv s (\operatorname{mod} p_{n-1})|] \\
&= \frac{1}{N} - \frac{1}{p_1 - 1} - \cdots - \frac{1}{p_{n-1} - 1} - \frac{1}{p_1 - 1} - \cdots - \frac{1}{p_{n-1} - 1} \pm \epsilon, \\
&\qquad \text{for some small } \epsilon, \text{ by the above density statements,} \\
&= \frac{1}{N} - \frac{2}{p_1 - 1} - \cdots - \frac{2}{p_{n-1} - 1} \pm \epsilon \\
&\geq \frac{1}{N} - \frac{2}{8N} - \cdots - \frac{2}{2^{n+3}N} \pm \epsilon, \quad \text{because } p_1 > 8N, p_i > 2p_{i-1} \\
&> \frac{1}{N} - \frac{1}{2N} \pm \epsilon \\
&= \frac{1}{2N} \pm \epsilon.
\end{aligned}$$

So the ratio is bounded away from zero, and therefore there must be infinitely many primes in $\mathcal{P}$ which are not congruent to either r or s mod p_i for any $i < n$. ∎

7. Proving nonconjugacy

In Section 4 we showed how to construct elements $w_{n,i} \in \Gamma$ in the same trace class. Now we shall prove that these elements are pairwise non-conjugate.

It will be convenient to have the words written out in explicit form here:

$$\begin{aligned} w_{1,1} &= (a^{p_1-1+q_1}b^{-q_1})^{k_1}a(a^{p_1-1+q_1}b^{-q_1})a^{-1}, \\ w_{1,2} &= a(a^{p_1-1+q_1}b^{-q_1})^{k_1}a^{-1}(a^{p_1-1+q_1}b^{-q_1}), \end{aligned}$$

$$\begin{aligned} w_{2,1} &= (w_{1,1}^{p_2-1+q_2}w_{1,2}^{-q_2})^{k_2}w_{1,1}(w_{1,1}^{p_2-1+q_2}w_{1,2}^{-q_2})w_{1,1}^{-1}, \\ w_{2,2} &= w_{1,1}(w_{1,1}^{p_2-1+q_2}w_{1,2}^{-q_2})^{k_2}w_{1,1}^{-1}(w_{1,1}^{p_2-1+q_2}w_{1,2}^{-q_2}), \end{aligned}$$

$$\begin{aligned} w_{2,3} = w_{2,1}^{[3]} &= (w_{1,2}^{p_2-1+q_2}w_{1,1}^{-q_2})^{k_2}w_{1,2}(w_{1,2}^{p_2-1+q_2}w_{1,1}^{-q_2})w_{1,2}^{-1}, \\ w_{n,1} &= (w_{n-1,1}^{p_n-1+q_n}w_{n-1,2}^{-q_n})^{k_n}w_{n-1,1}(w_{n-1,1}^{p_n-1+q_n}w_{n-1,2}^{-q_n})w_{n-1,1}^{-1}, \\ w_{n,2} &= w_{n-1,1}(w_{n-1,1}^{p_n-1+q_n}w_{n-1,2}^{-q_n})^{k_n}w_{n-1,1}^{-1}(w_{n-1,1}^{p_n-1+q_n}w_{n-1,2}^{-q_n}), \\ w_{n,3} = w_{n,1}^{[3]} &= W_n(w_{n-2,2}, w_{n-1,1}) \\ &= (w_{n-1,2}^{p_n-1+q_n}w_{n-1,1}^{-q_n})^{k_n}w_{n-1,2}(w_{n-1,2}^{p_n-1+q_n}w_{n-1,1}^{-q_n})w_{n-1,2}^{-1}, \quad \text{for } n \geq 2, \\ w_{n,i} &= w_{n,1}^{[i]} \\ &= [(w_{n-1,1}^{[i-1]})^{p_n-1+q_n}(w_{n-1,2}^{[i-1]})^{-q_n}]^{k_n} \\ &\quad w_{n-1,1}^{[i-1]}[(w_{n-1,1}^{[i-1]})^{p_n-1+q_n}((w_{n-1,2}^{[i-1]})^{-q_n})](w_{n-1,1}^{[i-1]})^{-1}, \\ &\quad \text{for } n \geq 3 \text{ and } 4 \leq i \leq n+1. \end{aligned}$$

Let Γ be as in the statement of Theorem 1.1, and let $\rho: \Gamma \to \mathrm{SL}_2(\mathbb{C})$ be the algebraic representation guaranteed by Lemma 5.1. Let $\mathbb{Q}(\operatorname{tr}\rho(\Gamma))$ be as in Section 6, let $\overline{\mathbb{Q}(\operatorname{tr}\rho(\Gamma))}$ denote the Galois closure of $\mathbb{Q}(\operatorname{tr}\rho(\Gamma))$, and let $N = |\overline{\mathbb{Q}(\operatorname{tr}\rho(\Gamma))}: \mathbb{Q}|$. For primes p which split completely in $\overline{\mathbb{Q}(\operatorname{tr}\rho(\Gamma))}$, let the map $\phi_p: \Gamma \to \mathrm{PSL}_2(\mathbb{F}_p)$ be as discussed in Section 6.

Let $\mathcal{Q} = \{\text{primes } p \in \mathbb{Z} \text{ for which } \phi_p \text{ is a surjection}\}$. Note that $\mathcal{Q}$ is infinite by Theorem 6.2. The proof of Theorem 1.1 follows from:

PROPOSITION 7.1: *The words $w_{n,i}$ can be chosen such that for every n there exist $a_n, b_n \in \Gamma$ for which $w_{n,i}(a_n, b_n)$ is not conjugate to $w_{n,j}(a_n, b_n)$ or $w_{n,j}(a_n, b_n)^{-1}$ whenever $i \neq j$. Indeed, the words $w_{n,i}$ and elements a_n, b_n can be chosen such that the following properties hold, for all n:*

P1(n): The primes $\{p_1, p_2, \ldots, p_n\}$ are in $\mathcal{Q}$, $p_1 > 8N$, and $p_i > 2p_{i-1}$ for all $i \leq n$.

P2(n): For all $i \leq n$, $\phi_{p_i}(a_n) = \left[\begin{smallmatrix}2 & 1\\ 0 & 1/2\end{smallmatrix}\right]$ and $\phi_{p_i}(b_n) = \left[\begin{smallmatrix}2 & 0\\ 0 & 1/2\end{smallmatrix}\right]$.

P3(n): For all $i \leq n$ and $j \leq n+1-i$, $\phi_{p_i}(w_{n,j}(a_n,b_n)) = id$ and $\phi_{p_i}(w_{n,n+2-i}(a_n,b_n)) = \left[\begin{smallmatrix}1 & x\\ 0 & 1\end{smallmatrix}\right] \neq id$.

We say that p_i "distinguishes" $w_{n,j}(a_n,b_n)$ from $w_{n,n+2-i}(a_n,b_n)$.

For example, taking $n=3$, we have that p_1 distinguishes $w_{3,4}$ from $w_{3,3}, w_{3,2}$ and $w_{3,1}$; p_2 distinguishes $w_{3,3}$ from $w_{3,2}$ and $w_{3,1}$; and p_3 distinguishes $w_{3,2}$ from $w_{3,1}$.

Proof of Proposition 7.1: The proof is by induction. We begin by distinguishing $w_{1,1}$ from $w_{1,2}$. We must first pick the prime p_1 and the integers q_1 and k_1 which define $w_{1,1}$ and $w_{1,2}$.

Let $q_1 = 1$, let $p_1 > \max\{8N, 30\}$ be a prime in $\mathcal{Q}$, and let $k_1 = p_1 - 4$. p_1, q_1 and k_1 are now fixed, and will not change for the remainder of the proof. Note that P1(1) is immediately satisfied.

Let $a_1 \in \phi_{p_1}^{-1}(\left[\begin{smallmatrix}2 & 1\\ 0 & 1/2\end{smallmatrix}\right])$ and $b_1 \in \phi_{p_1}^{-1}(\left[\begin{smallmatrix}2 & 0\\ 0 & 1/2\end{smallmatrix}\right])$, so P2(1) is satisfied.

Note that the images of a_1 and b_1 under ϕ_{p_1} generate a semi-direct product of cyclic groups, that words of the form $\left[\begin{smallmatrix}1 & x\\ 0 & 1\end{smallmatrix}\right]$ $(x \neq 0)$ have order p_1, and that words of the form $\left[\begin{smallmatrix}z & x\\ 0 & z^{-1}\end{smallmatrix}\right]$ $(x \neq 0,\ z \neq 0, 1)$ have order dividing $p_1 - 1$. This all follows from the structure theory of the groups $\mathrm{PSL}_2(\mathbb{F}_p)$, and can be checked by explicit computation.

We have:

$$\begin{aligned}
\phi_{p_1}(w_{1,1}(a,b)) &= \left[\begin{pmatrix}2 & 1\\ 0 & 1/2\end{pmatrix}^{p_1}\begin{pmatrix}1/2 & 0\\ 0 & 2\end{pmatrix}\right]^{p_1-4} \\
&\quad \begin{pmatrix}2 & 1\\ 0 & 1/2\end{pmatrix}\left[\begin{pmatrix}2 & 1\\ 0 & 1/2\end{pmatrix}^{p_1}\begin{pmatrix}1/2 & 0\\ 0 & 2\end{pmatrix}\right]\begin{pmatrix}1/2 & -1\\ 0 & 2\end{pmatrix} \\
&= \left[\begin{pmatrix}2 & 1\\ 0 & 1/2\end{pmatrix}\begin{pmatrix}1/2 & 0\\ 0 & 2\end{pmatrix}\right]^{p_1-4} \\
&\quad \begin{pmatrix}2 & 1\\ 0 & 1/2\end{pmatrix}\left[\begin{pmatrix}2 & 1\\ 0 & 1/2\end{pmatrix}\begin{pmatrix}1/2 & 0\\ 0 & 2\end{pmatrix}\right]\begin{pmatrix}1/2 & -1\\ 0 & 2\end{pmatrix} \\
&\quad \text{since } \begin{pmatrix}2 & 1\\ 0 & 1/2\end{pmatrix} \text{ has order dividing } p_1 - 1 \\
&= \begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}^{p_1-4}\begin{pmatrix}2 & 1\\ 0 & 1/2\end{pmatrix}\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}\begin{pmatrix}1/2 & -1\\ 0 & 2\end{pmatrix} \\
&= \begin{pmatrix}1 & 2p_1 - 8\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 8\\ 0 & 1\end{pmatrix} \\
&= \begin{pmatrix}1 & 2p_1\\ 0 & 1\end{pmatrix}
\end{aligned}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

However,

$$\begin{aligned}
\phi_{p_1}(w_{1,2}(a,b)) &= \begin{pmatrix} 2 & 1 \\ 0 & 1/2 \end{pmatrix} \left[\begin{pmatrix} 2 & 1 \\ 0 & 1/2 \end{pmatrix}^{p_1} \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix} \right]^{p_1-4} \begin{pmatrix} 1/2 & -1 \\ 0 & 2 \end{pmatrix} \\
&\quad \left[\begin{pmatrix} 2 & 1 \\ 0 & 1/2 \end{pmatrix}^{p_1} \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix} \right] \\
&= \begin{pmatrix} 2 & 1 \\ 0 & 1/2 \end{pmatrix} \left[\begin{pmatrix} 2 & 1 \\ 0 & 1/2 \end{pmatrix} \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix} \right]^{p_1-4} \begin{pmatrix} 1/2 & -1 \\ 0 & 2 \end{pmatrix} \\
&\quad \left[\begin{pmatrix} 2 & 1 \\ 0 & 1/2 \end{pmatrix} \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix} \right] \\
&= \begin{pmatrix} 2 & 1 \\ 0 & 1/2 \end{pmatrix} \begin{pmatrix} 1 & 2(p_1-4) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1/2 & -1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 8(p_1-4) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & -30 \\ 0 & 1 \end{pmatrix} \\
&\neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{since } p_1 > 30.
\end{aligned}$$

Therefore p_1 distinguishes $w_{1,1}(a_1, b_1)$ from $w_{1,2}(a_1, b_1)$, and P3(1) is satisfied.

Now, suppose that we have picked $a_{n-1}, b_{n-1} \in \Gamma$ and, for $i \leq n-1$, integers k_i, p_i, q_i with corresponding words $w_{i,j}$, so that the following is true:
P1($n-1$): The primes $\{p_1, \ldots, p_{n-1}\}$ are in $\mathcal{Q}$, and $p_i > 2p_{i-1}$ for all $i \leq n-1$.
P2($n-1$): For all $i \leq n-1$, $\phi_{p_i}(a_{n-1}) = \begin{bmatrix} 2 & 1 \\ 0 & 1/2 \end{bmatrix}$ and $\phi_{p_i}(b_{n-1}) = \begin{bmatrix} 2 & 0 \\ 0 & 1/2 \end{bmatrix}$.
P3($n-1$): For all $i \leq n-1$ and $j \leq n-i$, $\phi_{p_i}(w_{n-1,j}(a_{n-1}, b_{n-1})) = id$ and $\phi_{p_i}(w_{n-1,n+1-i}(a_{n-1}, b_{n-1})) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \neq id$.

We shall show how to pick k_n, q_n, p_n, a_n and b_n so that Properties P1(n), P2(n) and P3(n) are satisfied.

Since $\mathcal{Q}$ is infinite by Theorem 6.2, Property P1(n) may be satisfed simply by taking p_n to be large enough.

Observe that, by Lemma 6.3, Γ surjects onto $\Pi_{i=1}^{n} \mathrm{PSL}_2(\mathbb{F}_{p_i})$. Therefore we can satisfy Property P2(n) by picking $a_n \in \bigcap_{i=1}^{n} \phi_{p_i}^{-1}\left(\begin{bmatrix} 2 & 1 \\ 0 & 1/2 \end{bmatrix}\right)$ and $b_n \in \bigcap_{i=1}^{n} \phi_{p_i}^{-1}\left(\begin{bmatrix} 2 & 0 \\ 0 & 1/2 \end{bmatrix}\right)$.

To satisfy Property P3(n), we must show that, for all $i \leq n$ and $j \leq n+1-i$, $\phi_{p_i}(w_{n,j}) = id$ and $\phi_{p_i}(w_{n,n+2-i}) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \neq id$.

Let $q_n = \Pi_{j=1}^{n-1} p_j(p_j - 1)$.

We will break the proof up into two cases; first we will see what happens when we reduce by the primes p_i, $i < n$, which we have already picked, and then we show how to pick p_n.

Case 1: $i < n$
$\phi_{p_i}(a_n) = \begin{bmatrix} 2 & 1 \\ 0 & 1/2 \end{bmatrix}$ and $\phi_{p_i}(b_n) = \begin{bmatrix} 2 & 0 \\ 0 & 1/2 \end{bmatrix}$ are contained in the subgroup $B \subset \mathrm{PSL}_2(\mathbb{F}_{p_i})$ consisting of matrices whose lower left entry is 0. The order of B is $p_i(p_i - 1)/2$, which divides q_n. Therefore, $\phi_{p_i}(U(a_n, b_n)^{q_n}) = id$, where U is any word on two letters. So we have, for $j \leq n + 1 - i$:

Case 1a: $j = 1$

$$\begin{aligned}\phi_{p_i}(w_{n,1}) =&\phi_{p_i}([w_{n-1,1}^{p_n-1+q_n} w_{n-1,2}^{-q_n}]^{k_n} w_{n-1,1}[w_{n-1,1}^{p_n-1+q_n} w_{n-1,2}^{-q_n}]w_{n-1,1}^{-1}\\ =&\phi_{p_i}(w_{n-1,1}^{(p_n-1)(k_n+1)})\\ =&id, \quad \text{by Property P3}(n-1).\end{aligned}$$

Case 1b: $j = 2$

$$\begin{aligned}\phi_{p_i}(w_{n,2}) =&\phi_{p_i}(w_{n-1,1}[w_{n-1,1}^{p_n-1+q_n} w_{n-1,2}^{-q_n}]^{k_n} w_{n-1,1}^{-1}[w_{n-1,1}^{p_n-1+q_n} w_{n-1,2}^{-q_n}])\\ =&\phi_{p_i}(w_{n-1,1}^{(p_n-1)(k_n+1)})\\ =&id, \quad \text{by Property P3}(n-1).\end{aligned}$$

Case 1c: $j = 3$

$$\begin{aligned}\phi_{p_i}(w_{n,3}) =&\phi_{p_i}(w_{n,1}^{[3]})\\ &\quad\text{(recall the definition of } w_{n,i}^{[j]} \text{ from Section 4)}\\ =&\phi_{p_i}(W_n(w_{n-2,2}, w_{n-1,1}))\\ =&\phi_{p_i}([w_{n-1,2}^{p_n-1+q_n} w_{n-1,1}^{-q_n}]^{k_n} w_{n-1,2}[w_{n-1,2}^{p_n-1+q_n} w_{n-1,1}^{-q_n}]w_{n-1,2}^{-1})\\ =&\phi_{p_i}(w_{n-1,2}^{(p_n-1)(k_n+1)})\\ =&id, \quad \text{by Property P3}(n-1)\text{, since } j-1 = 2 \leq n-i.\end{aligned}$$

Case 1d: $4 \leq j \leq n + 1 - i$

$$\begin{aligned}\phi_{p_i}(w_{n,j}) =&\phi_{p_i}(w_{n,1}^{[j]})\\ =&\phi_{p_i}([(w_{n-1,1}^{[j-1]})^{p_n-1+q_n}(w_{n-1,2}^{[j-1]})^{-q_n}]^{k_n}\\ &\qquad w_{n-1,1}^{[j-1]}[(w_{n-1,1}^{[j-1]})^{p_n-1+q_n}(w_{n-1,2}^{[j-1]})^{-q_n}](w_{n-1,1}^{[j-1]})^{-1})\\ =&\phi_{p_i}((w_{n-1,1}^{[j-1]})^{(p_n-1)k_n+p_n-1})\\ =&\phi_{p_i}(w_{n-1,j-1}^{(p_n-1)(k_n+1)})\\ =&id, \quad \text{by Property P3}(n-1)\text{, since } j-1 \leq n-i.\end{aligned}$$

However,

$$\begin{aligned}
\phi_{p_i}(w_{n,n+2-i}) =& \phi_{p_i}(w_{n,1}^{[n+2-i]}), \quad \text{since } i \leq n-1, \text{so } n+2-i \geq 3. \\
(\text{for } i < n-1) =& \phi_{p_i}([(w_{n-1,1}^{[n+1-i]})^{p_n-1+q_n}(w_{n-1,2}^{[n+1-i]})^{-q_n}]^{k_n} w_{n-1,1}^{[n+1-i]} \\
& [(w_{n-1,1}^{[n+1-i]})^{p_n-1+q_n}(w_{n-1,2}^{[n+1-i]})^{-q_n}](w_{n-1,1}^{[n+1-i]})^{-1}) \\
=& \phi_{p_i}([w_{n-1,1}^{[n+1-i]}]^{(p_n-1)(k_n+1)}) \\
=& \phi_{p_i}(w_{n-1,n+1-i}^{(p_n-1)(k_n+1)}) \\
=& \begin{pmatrix} 1 & (p_n-1)(k_n+1)x \\ 0 & 1 \end{pmatrix} \\
& \text{where } x \neq 0 \text{ by Property P3}(n-1)
\end{aligned}$$

$$\begin{aligned}
(\text{for } i = n-1) =& \phi_{p_{n-1}}(w_{n,1}^{[3]}) \\
=& \phi_{p_{n-1}}([w_{n-1,2}^{p_n-1+q_n} w_{n-1,1}^{-q_n}]^{k_n} \\
& w_{n-1,2}[w_{n-1,2}^{p_n-1+q_n} w_{n-1,1}^{-q_n}] w_{n-1,2}^{-1}) \\
=& \phi_{p_{n-1}}(w_{n-1,2}^{(p_n-1)(k_n+1)}) \\
=& \begin{pmatrix} 1 & (p_n-1)(k_n+1)x \\ 0 & 1 \end{pmatrix} \\
& \text{where } x \neq 0 \text{ by Property P3}(n-1).
\end{aligned}$$

So to satisfy Property P3(n), we must pick $p_n \in \mathcal{Q}$ and k_n such that:

(I) p_i does not divide $k_n + 1$ or $p_n - 1$ for $i < n$.

Let m be the sum of the exponents on a_n and b_n in $w_{n-1,1}(a_n, b_n)$. We shall also require:

(II) $p_n > \max\{2^{4m}, q_n\}$.

We set $k_n = p^n - 2^{2m}$.

We claim that we can pick p_n to satisfy properties (I) and (II). Indeed, (I) is equivalent to the statement

(I′) $p_n \not\equiv 1$ or $2^{2m} - 1 \pmod{p_i}$ for any $i < n$.

Property P1($n - 1$) guarantees that $p_i > 2p_{i-1}$ for all $i < n$ and $p_1 > 8N$, so Lemma 6.4 implies that (I′) can be satisfied by infinitely many primes $p \in \mathcal{Q}$. Therefore we can pick an arbitrarily large prime p_n to satisfy (I) and (II), and still satisfy Property P1(n).

This concludes the proof in Case 1.

Case 2: $i = n$

We now show how to distinguish $w_{n,1}$ from $w_{n,2}$.

Since $\phi_{p_n}(a_n) = \begin{bmatrix} 2 & 1 \\ 0 & 1/2 \end{bmatrix}$ and $\phi_{p_n}(b_n) = \begin{bmatrix} 2 & 0 \\ 0 & 1/2 \end{bmatrix}$, it is easy to see that $\phi_{p_n}(w_{n-1,1})$ will have the form $\begin{bmatrix} 2^m & w \\ 0 & 2^{-m} \end{bmatrix}$. Note $2^m \neq 1(\operatorname{mod} p_n)$, since $p_n > 2^{4m}$. Therefore, $\phi_{p_n}(w_{n-1,1}^{p_n-1}) = id$, and we have:

$$\begin{aligned} \phi_{p_n}(w_{n,1}) &= \phi_{p_n}((w_{n-1,1}^{p_n-1+q_n} w_{n-1,2}^{-q_n})^{k_n} w_{n-1,1}(w_{n-1,1}^{p_n-1+q_n} w_{n-1,2}^{-q_n}) w_{n-1,1}^{-1}) \\ &= \phi_{p_n}((w_{n-1,1}^{q_n} w_{n-1,2}^{-q_n})^{k_n} w_{n-1,1}(w_{n-1,1}^{q_n} w_{n-1,2}^{-q_n}) w_{n-1,1}^{-1}). \end{aligned} \tag{2}$$

Lemma 7.2: *If p_n is chosen to be large enough, then*

$$\phi_{p_n}(w_{n-1,1}^{q_n} w_{n-1,2}^{-q_n}) = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix},$$

where $z \neq 0$.

Proof: Recall that p_{n-1} distinguishes $w_{n-1,1}$ from $w_{n-1,2}$. Therefore, $w_{n-1,1}(\bar{a}, \bar{b}) \neq w_{n-1,2}(\bar{a}, \bar{b})$ for $\bar{a} = \begin{bmatrix} 2 & 1 \\ 0 & 1/2 \end{bmatrix}$, $\bar{b} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in \mathrm{PSL}_2(\mathbb{F}_{p_{n-1}})$.

Now let $\mathbb{Z}(1/2)$ denote the ring obtained by adjoining $1/2$ to $\mathbb{Z}$, and let $\tilde{a} = \begin{bmatrix} 2 & 1 \\ 0 & 1/2 \end{bmatrix}$, $\tilde{b} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in \mathrm{PSL}_2(\mathbb{Z}(1/2))$. There is a well-defined reduction map $\theta_{p_{n-1}}\colon \mathrm{PSL}_2(\mathbb{Z}(1/2)) \to \mathrm{PSL}_2(\mathbb{F}_{p_{n-1}})$, since $p_{n-1} \neq 2$. Then

$$\begin{aligned} \theta_{p_{n-1}}(w_{n-1,1}(\tilde{a}, \tilde{b})) =& w_{n-1,1}(\bar{a}, \bar{b}) \\ &\neq w_{n-1,2}(\bar{a}, \bar{b}) = \theta_{p_{n-1}}(w_{n-1,2}(\tilde{a}, \tilde{b})), \end{aligned}$$

so $w_{n-1,1}(\tilde{a}, \tilde{b}) \neq w_{n-1,2}(\tilde{a}, \tilde{b})$ in $\mathrm{PSL}_2(\mathbb{Z}(1/2))$.

Using the definition of $w_{n-1,i}$ one may easily verify that the words have the following forms:

$$\begin{aligned} w_{n-1,1}(\tilde{a}, \tilde{b}) &= \begin{pmatrix} 2^m & x \\ 0 & 2^{-m} \end{pmatrix}, \\ w_{n-1,2}(\tilde{a}, \tilde{b})) &= \begin{pmatrix} 2^m & y \\ 0 & 2^{-m} \end{pmatrix}, \quad \text{where } x \neq y. \end{aligned}$$

Then we compute:

$$\begin{aligned} (w_{n-1,1}(\tilde{a}, \tilde{b}))^{q_n} &= \begin{pmatrix} 2^m & x \\ 0 & 2^{-m} \end{pmatrix}^{q_n} \\ &= \begin{pmatrix} 2^{mq_n} & x(2^{m(q_n-1)} + 2^{m(q_n-3)} + \cdots + 2^{m(3-q_n)} + 2^{m(1-q_n)}) \\ 0 & 2^{-mq_n} \end{pmatrix} \\ &\neq \begin{pmatrix} 2^{mq_n} & y(2^{m(q_n-1)} + 2^{m(q_n-3)} + \cdots + 2^{m(3-q_n)} + 2^{m(1-q_n)}) \\ 0 & 2^{-mq_n} \end{pmatrix} \\ &= \begin{pmatrix} 2^m & y \\ 0 & 2^{-m} \end{pmatrix}^{q_n} \\ &= (w_{n-1,2}(\tilde{a}, \tilde{b}))^{q_n}. \end{aligned}$$

Then for a large enough prime p_n, these words are different mod p_n:

$$\begin{aligned}
\phi_{p_n}(w_{n,1}(a,b))^{q_n} =&\theta_{p_n}(w_{n,1}(\tilde{a},\tilde{b}))^{q_n}\\
=&\begin{pmatrix} v & x' \\ 0 & 1/v \end{pmatrix}, \quad \text{for some } v,\\
\phi_{p_n}(w_{n,2}(a,b))^{q_n} =&\theta_{p_n}(w_{n,2}(\tilde{a},\tilde{b}))^{q_n}\\
=&\begin{pmatrix} v & y' \\ 0 & 1/v \end{pmatrix} \quad \text{where } x' \neq y' \in \mathbb{F}_{p_n}.
\end{aligned}$$

Then

$$\begin{aligned}
\phi_{p_n}(w_{n,1}^{q_n} w_{n,2}^{-q_n}) = &\begin{pmatrix} 1 & v(x'-y') \\ 0 & 1 \end{pmatrix}\\
\neq &id,
\end{aligned}$$

completing the proof of Lemma 7.2. ∎

Then, returning to Equation (2), we have

$$\phi_{p_n}(w_{n-1,1}^{q_n} w_{n-1,2}^{-q_n}) = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \neq id.$$

So,

$$\begin{aligned}
\phi_{p_n}(w_{n,1}) =&\begin{pmatrix} 1 & k_n z \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2^m & w \\ 0 & 2^{-m} \end{pmatrix}\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2^{-m} & -w \\ 0 & 2^m \end{pmatrix} \quad \text{for some } w.\\
=&\begin{pmatrix} 1 & k_n z \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2^{2m}z \\ 0 & 1 \end{pmatrix}\\
=&\begin{pmatrix} 1 & (k_n+2^{2m})z \\ 0 & 1 \end{pmatrix}\\
=&\begin{pmatrix} 1 & (p_n-2^{2m}+2^{2m})z \\ 0 & 1 \end{pmatrix} \quad \text{by our choice of } k_n\\
=&\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.
\end{aligned}$$

However

$$\begin{aligned}
\phi_{p_n}(w_{n,2}) =&\phi_{p_n}(w_{n-1,1}(w_{n-1,1}^{p_n-1+q_n} w_{n-1,2}^{-q_n})^{k_n} w_{n-1,1}^{-1}(w_{n-1,1}^{p_n-1+q_n} w_{n-1,2}^{-q_n}))\\
=&\phi_{p_n}(w_{n-1,1}(w_{n-1,1}^{q_n} w_{n-1,2}^{-q_n})^{k_n} w_{n-1,1}^{-1}(w_{n-1,1}^{q_n} w_{n-1,2}^{-q_n}))\\
=&\begin{pmatrix} 2^m & w \\ 0 & 2^{-m} \end{pmatrix}\begin{pmatrix} 1 & k_n z \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2^{-m} & -w \\ 0 & 2^m \end{pmatrix}\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}\\
=&\begin{pmatrix} 1 & 2^{2m}k_n z + z \\ 0 & 1 \end{pmatrix}
\end{aligned}$$

$$= \begin{pmatrix} 1 & (2^{2m}(p_n - 2^{2m}) + 1)z \\ 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & (-2^{4m} + 1)z \\ 0 & 1 \end{pmatrix}.$$

Since $p_n > 2^{4m}$, $-2^{4m} + 1 \neq 0 \pmod{p_n}$. Also, $z \neq 0$, so $\phi_{p_n}(w_{n,2}) \neq 0$. Hence Property P3($n$) is satisfied, and we are done. ∎

References

[A] J. Anderson, *A brief survey of the deformation theory of Kleinian groups*, preprint.

[Ba] H. Bass, *Groups of integral representation type*, Pacific Journal of Mathematics **86** (1980), 15–51.

[Br] R. Brooks, *Circle packings and co-compact extensions of Kleinian groups*, Inventiones Mathematicae **86** (1986), 461–469.

[CS] M. Culler and P. B. Shalen, *Varieties of group representations and splittings of 3-manifolds*, Annals of Mathematics **117** (1983), 109–146.

[GR] D. Ginzburg and Z. Rudnick, *Stable multiplicities in the length spectrum of Riemann surfaces*, Israel Journal of Mathematics **104** (1998), 129–144.

[H] R. D. Horowitz, *Characters of free groups represented in the two-dimensional special linear group*, Communications on Pure and Applied Mathematics **25** (1972), 635–649.

[I] I. M. Isaacs, *Algebra: A Graduate Course*, Brooks/Cole, 1994.

[L] R. L. Long, *Algebraic Number Theory*, Marcel Dekker, New York, 1977.

[LR] D. D. Long and A. W. Reid, *Simple quotients of hyperbolic 3-manifold groups*, Proceedings of the American Mathematical Society **126** (1998), 877–880.

[M] J. Marklof, *On multiplicities in length spectra of arithmetic hyperbolic three-orbifolds*, Nonlinearity **9** (1996), 517–536.

[N] W. Narkiewicz, *Algebraic Numbers*, Polish Scientific Publishers, Warsaw, 1974.

[R] B. Randol, *The length spectrum of a Riemann surface is always of unbounded multiplicity*, Proceedings of the American Mathematical Society **78** (1980), 455–456.

[Sar] P. Sarnak, *Arithmetic quantum chaos*, The Schur Lectures (1992), Israel Mathematical Conference Proceedings, Vol. 8, 1995.

[Sc] P. Scott, *Compact submanifolds of 3-manifolds*, Journal of the London Mathematical Society **7** (1973), 246–250.

[Su] M. Suzuki, *Group Theory I*, Springer-Verlag, Berlin, 1982.

[T] W. Thurston, *Geometry and Topology of Hyperbolic 3-Manifolds*, mimeographed lecture notes, 1978.