



Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra



Virtual retractions, conjugacy separability and omnipotence

Henry Wilton

Mathematics 253-37, Caltech, Pasadena, CA 91125, United States

ARTICLE INFO

Article history:

Received 2 June 2008

Available online 6 November 2009

Communicated by Martin Liebeck

Keywords:

Fuchsian group

Conjugacy separability

ABSTRACT

We use wreath products to provide criteria for a group to be conjugacy separable or omnipotent. These criteria are in terms of virtual retractions onto cyclic subgroups. We give two applications: a straightforward topological proof of the theorem of Stebe that infinite-order elements of Fuchsian groups (of the first type) are conjugacy distinguished, and a proof that surface groups are omnipotent.

© 2009 Elsevier Inc. All rights reserved.

1. Introduction

Definition 1.1. An element g of a group G is called *conjugacy distinguished* if, whenever $h \in G$ is not conjugate to g , there exists a homomorphism q to a finite group such that $q(g)$ is not conjugate to $q(h)$. A group G is called *conjugacy separable* if every element of G is conjugacy distinguished.

The similar notion of *subgroup separability* has strong connections with topology—work of Scott [8] and Stallings [9] demonstrates its pleasing reformulation in terms of promoting immersions to embeddings in finite-sheeted covers. Moreover, subgroup separability is a commensurability invariant. In contrast, conjugacy separability is not a commensurability invariant, and does not seem to have a simple interpretation as a statement about covering spaces. Whereas much recent work on subgroup separability relates to low-dimensional topology, the field of conjugacy separability has retained a more algebraic flavour.

In connection with the virtually Haken conjecture for hyperbolic 3-manifolds, Long and Reid made the following definitions.

Definition 1.2. (See [5].) A subgroup H of G is a *virtual retract* if there exists a finite-index subgroup of K such that H is a retract of K —that is, $H \subset K$ and the inclusion map has a left inverse.

E-mail address: wilton@caltech.edu.

Definition 1.3. (See [5].) A group G has *property LR over $\mathbb{Z}$* if every infinite cyclic subgroup is a virtual retract of G .

In this paper, we provide a topological approach to proving conjugacy separability. Lemma 2.1 shows how a strengthening of LR over $\mathbb{Z}$ can be used to deduce that a group is conjugacy separable. As an application of Lemma 2.1, we provide a topological proof of the theorem of Stebe [10] that infinite-order elements of Fuchsian groups (of the first type) are conjugacy distinguished. It follows immediately that surface groups are conjugacy separable. Stebe also showed in [10] that certain Fuchsian groups are conjugacy separable, and Fine and Rosenberger [3] extended Stebe's result to all Fuchsian groups.

Two key steps in the proof are interesting in their own right. Let α and β be two non-homotopic curves on a surface Σ . Proposition 3.5 uses Niblo's Theorem that surface groups are double-coset separable [6] to simplify the intersection of the elevations of α and β in a finite cover. And Proposition 3.7 produces a finite-sheeted covering in which no pair of elevations of α and β are homologous.

Our motivation for studying conjugacy separability from a topological point of view is its connection with a famous open problem in geometric group theory.

Question 1.4. Does there exist a non-residually finite hyperbolic group?

Although being conjugacy separable is much stronger than being residually finite, there is a deep connection between the two. Indeed, combinatorial Dehn filling can be used to provide a related property.

Call a set of group elements $g_1, \dots, g_l \in G$ *independent* if $i = j$ whenever g_i has a conjugate that commutes with g_j . Denote by $o(g)$ the order of a group element g . Wise made the following definition in [11].

Definition 1.5. A group G is *omnipotent* if, whenever $g_1, \dots, g_l$ is an independent set of elements, there is an integer K such that for any choice of positive integers $n_1, \dots, n_l$, there is a homomorphism q from G to a finite group Q such that

$$o(q(g_i)) = Kn_i$$

for all i .

If every hyperbolic group is residually finite then every torsion-free hyperbolic group is omnipotent, by a result of Gromov [4], Ol'shanskii [7] and Delzant [2]. Wise [11] observed that any omnipotent group that is also residually odd is conjugacy separable, and asked if there is an omnipotent group that is not conjugacy separable. Because non-residually finite hyperbolic groups seem extremely difficult to construct, one expects many hyperbolic groups to be conjugacy separable and omnipotent.

Lemma 2.6 strengthens the hypotheses of Lemma 2.1, and enables one to deduce omnipotence. As an application, we provide a topological proof that hyperbolic surfaces are omnipotent. This result was also obtained by Jitendra Bajpai in his thesis [1]. Indeed, we prove that such a property holds for any finite, independent set of torsion-free elements of a Fuchsian group.

A similar criterion was used by Wise [11] to prove that free groups are omnipotent. Our techniques are slightly different to his, and when adapted to the setting of compact graphs, provide a different proof of his theorem. To apply Lemma 2.6, we strengthen Proposition 3.7 still further: given non-homotopic curves α and β on a surface, we construct a finite-sheeted cover in which any one elevation of α is linearly independent in homology from the set of all elevations of β .

One advantage of the techniques presented here is that they seem well adapted to dealing with finite extensions. Although conjugacy separability, and presumably omnipotence, are not invariants of commensurability, there is no significant technical difficulty in extending our techniques from surface groups to infinite-order elements of Fuchsian groups.

Throughout this paper, if g and h are group elements then $g^h = h^{-1}gh$.

2. Virtual retractions and wreath products

For a finite-index subgroup K of G and an element $g \in G$, the *degree* of g in K , $\deg_K(g)$, is the minimal positive integer n such that $g^n \in K$.

Lemma 2.1. *Let G be a group and let $a, b \in G$. Let K be a finite-index normal subgroup of G , let $m = \deg_K(a)$ and $n = \deg_K(b)$. Suppose there exists a retraction $\rho : K \rightarrow \langle a^m \rangle$ with the property that*

$$\rho((b^{mn})^g) \neq a^{mn}$$

for all $g \in G$. Then there exists a homomorphism τ from G to a finite group such that $\tau(a)$ is not conjugate to $\tau(b)$.

Remark 2.2. If $g, h \in K$ then, because the image of ρ is abelian, $\rho(g^h) = \rho(g)$. Therefore, when applying Lemma 2.1, it suffices to check the hypotheses whenever g is one of a fixed set of double-coset representatives for $K \backslash G / Z_G(b)$ (where $Z_G(b)$ is the centraliser of b).

The idea of the proof of the lemma is to use a wreath product to promote ρ to a map from G to a virtually abelian group. We therefore recall the definition of a wreath product.

Let A and B be groups and assume that B is finite. Consider the group A^B of set maps $B \rightarrow A$, with group operation inherited from A —this can be thought of as a direct sum of copies of A indexed by B . Then B acts naturally on A^B by left translation—if $\phi \in A^B$ then $\phi^b(b') = \phi(bb')$ for any $b, b' \in B$.

Definition 2.3. The *wreath product* of A by B , denoted $A \wr B$, is defined as the semidirect product

$$A \wr B = A^B \rtimes B$$

where the action of B on A^B is by left translation. The subgroup A^B is called the *base* of the wreath product.

Wreath products are useful because they enable us to extend homomorphisms from a normal subgroup to the whole group. The following lemma is essentially the Krasner–Kaloujnine Theorem, which asserts that every extension is a subgroup of a wreath product.

Lemma 2.4. *Suppose $K \triangleleft G$ with $Q \cong G/K$ and let $f : K \rightarrow H$ be a homomorphism. Then there is a homomorphism*

$$\hat{f} : G \rightarrow H \wr Q$$

with the property that, whenever $k \in K$, $\hat{f}(k)$ is in the base of the wreath product and, for any $q \in Q$, there is $g_q \in G$ such that

$$\hat{f}(k)(q) = f(k^{g_q}).$$

Proof. Denote by η the quotient map $G \rightarrow Q$, and for each $q \in Q$ fix a corresponding coset representative $g_q \in G$, so that $\eta(g_q) = q$. For any $g \in G$ and $q \in Q$ set

$$\phi_g(q) = g_q^{-1} g g_{\eta(g)^{-1}q}.$$

Note that $\eta(\phi_g(q)) = 1$, so $\phi_g \in K^Q$ and therefore the composition $f \circ \phi_g$ makes sense as an element of H^Q . Now define $\hat{f} : G \rightarrow H \wr Q$ by

$$\hat{f}(g) = (f \circ \phi_g)\eta(g).$$

Let us check that this is a homomorphism. For any $g, g' \in G$,

$$\hat{f}(g)\hat{f}(g') = (f \circ \phi_g)\eta(g)(f \circ \phi_{g'})\eta(g') = (f \circ \phi_g)(f \circ \phi_{g'})^{\eta(g)^{-1}}\eta(gg').$$

For any $q \in Q$,

$$\begin{aligned} (f \circ \phi_g)(f \circ \phi_{g'})^{\eta(g)^{-1}}(q) &= (f \circ \phi_g)(q)(f \circ \phi_{g'})^{\eta(g)^{-1}}(q) \\ &= f(g_q^{-1}gg_{\eta(g)^{-1}q})f(g_{\eta(g)^{-1}q}^{-1}g'g_{\eta(g)^{-1}q}) \\ &= f(g_q^{-1}gg'g_{\eta(gg')^{-1}q}) \\ &= f \circ \phi_{gg'}(q) \end{aligned}$$

and so

$$\hat{f}(g)\hat{f}(g') = (f \circ \phi_{gg'})\eta(gg') = \hat{f}(gg')$$

as required.

That $\hat{f}(k)(q) = f(k^{gq})$ for $k \in K$ and $q \in Q$ is immediate from the construction. $\square$

We will need to test when elements of wreath products are conjugate.

Remark 2.5. Suppose A is abelian. If $\phi_1, \phi_2 \in A^B$ are conjugate in $A \wr B$ then for some $b \in B$ we have $\phi_1^b = \phi_2$. As B acts on A^B by permuting the factors, it follows that the sets

$$\{\phi_1(b) \mid b \in B\}$$

and

$$\{\phi_2(b) \mid b \in B\}$$

are equal.

We now have the tools to prove Lemma 2.1.

Proof of Lemma 2.1. Let $Q = K \setminus G$. Consider the composition

$$\sigma : K \xrightarrow{\rho} \mathbb{Z} \rightarrow \mathbb{Z}/N$$

for N large enough that $\sigma((b^{mn})^g) \neq \sigma(a^{mn})$ for all $g \in G$. Let τ be the extension of σ to a map $G \rightarrow (\mathbb{Z}/N) \wr Q$.

Suppose $\tau(a)$ and $\tau(b)$ are conjugate. Then $\tau(a^{mn})$ and $\tau(b^{mn})$ are conjugate. But a^{mn} and b^{mn} are both in K , so it follows from Remark 2.5 that for some $q \in Q$,

$$\sigma(a^{mn}) = \sigma((b^{mn})^{g_q}),$$

a contradiction. $\square$

To provide a criterion for omnipotence, we need to analyse the order of $\tau(b)$. Let $\sigma' : K \rightarrow (\mathbb{Z}/N)^Q$ be the restriction of τ to K . Thinking of ρ as a map $K \rightarrow \mathbb{Z}$, let $d_b = \gcd\{\rho((b^n)^g) \mid g \in G\}$. Then, as long as N is sufficiently large, $\sigma'(b^n)$ is a primitive element of $(\mathbb{Z}/N)^Q$ multiplied by d_b . So $o(\sigma'(b^n)) = \text{lcm}(N, d_b)/d_b$ (adopting the convention that $0/0 = 1$). As $o(q(b)) = n$, it follows that

$$o(\tau(b)) = n \frac{\text{lcm}(N, d_b)}{d_b}.$$

As $\rho(a^m) = 1$, we have that $d_a = 1$ and therefore $o(\tau(a)) = mN$. Therefore

$$\frac{o(\tau(a))}{o(\tau(b))} = \frac{mNd_b}{n \text{lcm}(N, d_b)}$$

and so, unless $d_b = 0$,

$$\frac{m}{n} \leq \frac{o(\tau(a))}{o(\tau(b))} \leq \frac{md_b}{n}.$$

To prove omnipotence, we shall need the ratio of the orders of $\tau(a)$ and $\tau(b)$ to vary unrestrictedly with N ; we therefore need $d_b = 0$.

Bearing this in mind, Lemma 2.6 provides a criterion to prove omnipotence for groups.

Lemma 2.6. *Let G be a group and let $\{a_1, \dots, a_l\}$ be an independent set of elements. Suppose that there is a finite-index normal subgroup $K \triangleleft G$, with $m_i = \deg_K(a_i)$, and suppose further that for each i there exists a retraction $\rho_i : K \rightarrow \langle a_i^{m_i} \rangle$ with the property that whenever $j \neq i$,*

$$\rho_i((a_j^{m_j})^g) = 1$$

for all $g \in G$. Then for any choice of positive integers $p_1, \dots, p_l$ there exists a homomorphism η from G to a finite group such that

$$o(\eta(a_i)) = p_i \prod_j m_j$$

for all i .

Proof. Applying the wreath product construction above to each ρ_i , we see that for any choices of positive integer N_i , for each i there is a homomorphism σ_i from G to a finite group Q_i such that

$$o(\sigma_i(a_i)) = N_i m_i$$

whereas

$$o(\sigma_i(a_j)) = m_j$$

whenever $j \neq i$. For each i let

$$N_i = p_i \prod_{j \neq i} m_j$$

and let $\sigma_i : G \rightarrow Q_i$ be the resulting homomorphism to a finite group. Now

$$\eta = \prod_i \sigma_i : G \rightarrow \prod_i Q_i$$

is easily seen to be as required. $\square$

3. Conjugacy separability

We shall use the ideas of section 1 to give a topological proof of the theorem of Stebe [10] that infinite-order elements of Fuchsian groups of the first type are conjugacy distinguished.

Definition 3.1. A Fuchsian group of the first type is a discrete subgroup of $PSL_2(\mathbb{R})$ of finite covolume.

In what follows, for brevity's sake we shall simply refer to Fuchsian groups, when we really mean Fuchsian groups of the first type.

We can think of a Fuchsian group Γ as acting properly discontinuously on the hyperbolic plane $\mathbb{H}^2$, such that the quotient is a 2-orbifold. By Selberg's Lemma Γ has a torsion-free normal subgroup Γ_0 of finite index, and the quotient of $\mathbb{H}^2$ by Γ_0 is a surface Σ . Because Γ and hence Γ_0 is finitely generated we can restrict our attention to a compact subsurface (which we also denote Σ), possibly with boundary, whose fundamental group is Γ_0 . The proof that Fuchsian groups are conjugacy separable (and, later, omnipotent) proceeds by analysing closed curves on the compact surface Σ .

Given a closed curve γ on Σ , the homology class (with $\mathbb{Z}$ coefficients) of γ is denoted $[\gamma]$. A closed curve γ that is not null-homotopic is called *primitive* if it is simple and $[\gamma]$ is primitive in $H_1(\Sigma)$. (So either γ is non-separating or γ is boundary parallel and Σ has more than one boundary component.) If α, β are closed curves on Σ then $i(\alpha, \beta)$ is the geometric intersection number of α and β .

Throughout the following we shall use the language of *elevations*, which for the purposes of this paper we define as follows.

Definition 3.2. Let γ be a closed curve on Σ and let $\Sigma' \rightarrow \Sigma$ be a finite-sheeted covering map. Fix a basepoint on Σ' and take its image as a basepoint for Σ . If g is a based curve on Σ that is freely homotopic to γ and $n = \deg_{\pi_1(\Sigma')}(g)$ then, by standard covering space theory, g^n lifts to a (based) curve γ' on Σ' . Such a curve γ' , defined up to free homotopy on Σ' , is called an *elevation* of γ to Σ' .

As free homotopy corresponds to conjugation in the fundamental group, one can equivalently think of γ' as the $\pi_1(\Sigma')$ -conjugacy class of the element of $\pi_1(\Sigma')$ represented by g^n .

Note that the set of all elevations of γ to Σ' is independent of the choice basepoint.¹

Scott famously proved that surface groups are subgroup separable [8]. We shall use Niblo's extension of this result. He proved that surface groups are double-coset separable.

Theorem 3.3. (See [6].) Suppose that H, H' are finitely generated subgroups of $\pi_1(\Sigma)$ and $\gamma \notin HH'$. There exists a finite-index subgroup $K \subset \pi_1(\Gamma)$ such that $H \subset K$ but $\gamma \notin KH'$.

¹ Wise uses a slightly different definition of elevations extensively in [11]. His definition is better adapted to more general contexts, although for our purposes the two definitions will usually coincide.

Scott's Theorem has the well known consequence that any closed curve on a surface can be lifted to a simple curve in a finite-sheeted cover. We shall use Niblo's Theorem to simplify the intersections of a pair of curves. It is also well known that any separating simple closed curve can be lifted to be non-separating in a finite cover. It will be important later to understand this fact, so we recall the details here.

Lemma 3.4. *Let γ be a separating curve on a surface Σ , let $\Sigma' \rightarrow \Sigma$ be a finite-sheeted abelian covering and let γ' be the lift of γ to Σ' . If γ' is separating then the restriction of the covering map $\Sigma' \rightarrow \Sigma$ to some component of $\Sigma' \setminus \gamma'$ is a homeomorphism.*

Proof. Let A be the abelian group of covering transformations of Σ' and let Σ'_1 and Σ'_2 be the components of $\Sigma' \setminus \gamma'$. For a contradiction, suppose that there are non-trivial $a_1, a_2 \in A$ such that $a_i \gamma' \subset \Sigma'_i$ for $i = 1, 2$. Without loss of generality, we can assume that both $a_i \gamma'$ are closest to γ' , in the sense that there is a path from γ' to $a_i \gamma'$ that does not cross any other translates of γ' .

An easy induction shows that $a_1^n \gamma' \subset \Sigma'_1$ for any positive integer n and hence, because A is finite, $a_1^{-1} \gamma' \subset \Sigma'_1$. It follows that $a_1 \Sigma'_2 \subset \Sigma'_1$. Likewise, $a_2 \Sigma'_1 \subset \Sigma'_2$. Therefore

$$a_1 a_2 \gamma' \subset \Sigma'_1$$

and, symmetrically,

$$a_2 a_1 \gamma' \subset \Sigma'_2.$$

Because A is abelian, $a_1 a_2 = a_2 a_1$ so $a_1 a_2$ maps γ' to itself. As A acts freely on the elevations of γ it follows that $a_1 a_2 = 1$ and $a_2 = a_1^{-1}$. But we have already seen that $a_1^{-1} \gamma' \subset \Sigma'_1$, so it follows that a_1 and a_2 fix γ' , a contradiction.

We conclude that, without loss of generality, every translate of γ' by A is contained in Σ'_2 . Hence the restriction of the covering map to Σ'_1 is a homeomorphism. $\square$

We are now ready to apply Niblo's Theorem to simplify the intersections of a pair of closed curves.

Proposition 3.5. *Let Σ be a compact surface and let α, β be closed curves in Σ that are not null-homotopic. There is a finite-sheeted covering $\Sigma' \rightarrow \Sigma$ and a primitive elevation α' of α to Σ' such that, for any elevation β' of β to Σ' :*

1. β' is primitive; and
2. $i(\alpha', \beta') \leq 1$.

Proof. By passing to a double cover if necessary, it is easy to ensure that if Σ has non-empty boundary then it has at least two boundary components. It follows from Scott's Theorem that there is an orientable finite-sheeted covering $\hat{\Sigma}$ of Σ to which α has a lift $\hat{\alpha}$ that is a simple closed curve.

If α is boundary parallel then, as $\hat{\Sigma}$ has at least two boundary components, $\hat{\alpha}$ is primitive. If α is separating then it is easy to apply Lemma 3.4 and pass to a double cover so that $\hat{\alpha}$ is non-separating and hence primitive. Likewise we can pass to a further finite-sheeted cover to ensure that some elevation of β is also primitive. Replacing $\hat{\Sigma}$ by a normal covering, we can ensure that every elevation of α and β is primitive.

We now need to simplify the intersections of an elevation $\hat{\alpha}$ of α with the elevations of β . If $\hat{\alpha}$ is boundary parallel then any curve in $\hat{\Sigma}$ can be homotoped off $\hat{\alpha}$. We shall therefore concentrate on the case in which $\hat{\alpha}$ is non-separating.

Let $\{\hat{\beta}_j\}$ be the set of all elevations of β to $\hat{\Sigma}$. The proof is by induction on the quantity

$$c(\hat{\alpha}, \hat{\Sigma}) = \sum_j \max(i(\hat{\alpha}, \hat{\beta}_j) - 1, 0).$$

Clearly, if $c(\hat{\alpha}, \hat{\Sigma}) = 0$ then $i(\hat{\alpha}, \hat{\beta}_j) \leq 1$ for all j .

If $c(\hat{\alpha}, \hat{\Sigma}) > 0$ then without loss of generality $i(\hat{\alpha}, \hat{\beta}_1) > 1$. After modifying $\hat{\alpha}$ and $\hat{\beta}_1$ by a homotopy we may assume that $|\hat{\alpha} \cap \hat{\beta}_1| = i(\hat{\alpha}, \hat{\beta}_1)$. Fix a basepoint $\hat{x} \in \hat{\alpha} \cap \hat{\beta}_1$. Then $\hat{\beta}_1$ is homotopic (respecting the basepoint) to a concatenation $\gamma\delta$ where $i(\hat{\alpha}, \gamma) \leq 1$ and $i(\hat{\alpha}, \delta) < i(\hat{\alpha}, \hat{\beta}_1)$.

Whenever $g \in \langle \hat{\alpha} \rangle \langle \hat{\beta}_1 \rangle$, either $g \in \langle \hat{\alpha} \rangle$ or $g = \hat{\alpha}^m \hat{\beta}_1^n$ for some integer m and some $n \neq 0$, so

$$i(\hat{\alpha}, g) = i(\hat{\alpha}, \hat{\beta}_1^n) > 1.$$

But $\gamma \notin \langle \hat{\alpha} \rangle$, as otherwise a homotopy would reduce $|\hat{\alpha} \cap \hat{\beta}_1|$, so $\gamma \notin \langle \hat{\alpha} \rangle \langle \hat{\beta}_1 \rangle$. Therefore by Niblo's Theorem there exists a (based) finite-sheeted covering

$$(\bar{\Sigma}, \bar{x}) \rightarrow (\hat{\Sigma}, \hat{x})$$

such that $\hat{\alpha}$ lifts to a (based) loop $\bar{\alpha}$ on $\bar{\Sigma}$ but $\gamma \notin \pi_1(\bar{\Sigma}) \langle \bar{\beta}_1 \rangle$.

We aim to show that $c(\bar{\alpha}, \bar{\Sigma}) < c(\hat{\alpha}, \hat{\Sigma})$. Fix j , and consider the set $\{\bar{\beta}_{j,k}\}$ of elevations of $\hat{\beta}_j$ to $\bar{\Sigma}$. Then it is clear that

$$\sum_k i(\bar{\alpha}, \bar{\beta}_{j,k}) = i(\hat{\alpha}, \hat{\beta}_j).$$

Therefore $c(\bar{\alpha}, \bar{\Sigma}) \leq c(\hat{\alpha}, \hat{\Sigma})$.

Let $\bar{\beta}_1$ be the elevation of $\hat{\beta}_1$ to $\bar{\Sigma}$ that covers the based loop $\hat{\beta}_1$ and let $\bar{\beta}'_1$ be the elevation that covers $\hat{\beta}'_1$. Both $\bar{\beta}_1$ and $\bar{\beta}'_1$ intersect $\bar{\alpha}$ non-trivially. But $\bar{\beta}_1$ and $\bar{\beta}'_1$ are not freely homotopic in $\pi_1(\bar{\Sigma})$. This shows that $\hat{\beta}_1$ has at least two elevations to $\bar{\Sigma}$ that intersect $\bar{\alpha}$ non-trivially. It follows that

$$c(\bar{\alpha}, \bar{\Sigma}) < c(\hat{\alpha}, \hat{\Sigma})$$

as required.

By induction, there exists a finite-sheeted covering $\Sigma' \rightarrow \Sigma$ with an elevation α' of α , such that $c(\alpha', \Sigma') = 0$. This is the required covering. $\square$

To apply the results of Section 1, we need to separate elevations of α and β in an abelian quotient, and hence in homology. Our first step is the following observation.

Remark 3.6. If α and β are disjoint, primitive curves in Σ that are homologous but not homotopic then there exists a 2-sheeted cover Σ' of Σ to which α and β both lift, such that no pair of elevations α' and β' of α and β respectively are homologous in Σ' . Let us describe this covering.

As usual, the easier case is when α is boundary parallel. In this case β is also boundary parallel, and Σ only has these two boundary components. A double cover Σ' with four boundary components is as required.

In the case when α and β are non-separating, note that $\Sigma \setminus \alpha \cup \beta$ has two components Σ_1 and Σ_2 , each of which is a surface of positive genus with two boundary components. Each Σ_i has a double cover Σ'_i with four boundary components. Gluing Σ'_1 and Σ'_2 suitably creates Σ' .

This remark enables us to improve Proposition 3.5 to ensure that the elevations of α and β differ in homology.

Proposition 3.7. *Let Σ be a surface and let α, β be closed curves in Σ that are not freely homotopic. There is a finite-sheeted normal covering $\tilde{\Sigma} \rightarrow \Sigma$ such that, for any elevations $\tilde{\alpha}$ and $\tilde{\beta}$ of α and β respectively to $\tilde{\Sigma}$:*

1. $\tilde{\alpha}$ and $\tilde{\beta}$ are primitive; and
2. $[\tilde{\alpha}] \neq \pm[\tilde{\beta}]$ in $H_1(\tilde{\Sigma})$.

Proof. Let Σ' be the covering space of Σ given by Proposition 3.5, with the provided elevation α' of α . Let $\{\beta'_j\}$ be the set of all elevations of β to Σ' . For each j , define a covering space Σ'_j as follows. If α' is not homologous to β'_j or $(\beta'_j)^{-1}$ in Σ' then $\Sigma'_j = \Sigma'$. Otherwise, α' and $(\beta'_j)^{\pm 1}$ are (homotopic to) disjoint primitive curves in Σ' that are homologous but not homotopic, so by Remark 3.6 we can take Σ'_j to be the double cover of Σ' in which no pair of elevations of α' and $(\beta'_j)^{\pm 1}$ are homologous. Define $\tilde{\Sigma}$ by

$$\pi_1(\tilde{\Sigma}) = \bigcap_j \pi_1(\Sigma'_j).$$

Then whenever $\tilde{\alpha}$ is a lift of α' to $\tilde{\Sigma}$ and $\tilde{\beta}$ is an elevation of β to $\tilde{\Sigma}$, $\tilde{\beta}$ is also an elevation of some intermediate β'_j and hence is homologous to neither α' nor its inverse.

Finally, let $\tilde{\Sigma}$ be the covering space whose fundamental group is the intersection of all conjugates of $\pi_1(\tilde{\Sigma})$ in $\pi_1(\Sigma)$. This is the covering required. For, after composing the covering map $\tilde{\Sigma} \rightarrow \Sigma$ with a deck transformation, any pair $\tilde{\alpha}$ and $\tilde{\beta}$ of elevations (of α and β respectively) cover a lift $\tilde{\alpha}$ of α' and some elevation $\tilde{\beta}$ of β . Hence $\tilde{\alpha}$ and $\tilde{\beta}^{\pm 1}$ are not homologous. $\square$

Combining this proposition with the results of Section 1, we are now in a position to prove that surface groups are conjugacy separable. Like Stebe, we shall start by proving that elements of infinite order in Fuchsian groups are conjugacy distinguished.

Theorem 3.8. (See [10].) *If Γ is a Fuchsian group and $a \in \Gamma$ is of infinite order then a is conjugacy distinguished.*

Proof. By Selberg's Lemma, Γ has a torsion-free normal subgroup of finite index, which can be taken to be $\pi_1(\Sigma)$ for some compact surface Σ , possibly with boundary. Suppose that $b \in \Gamma$ is not conjugate to a . Let $p = \deg_{\pi_1(\Sigma)}(a)$ and $q = \deg_{\pi_1(\Sigma)}(b)$, and represent a^p by a closed curve α on Σ . Fix representatives $g_1, \dots, g_n$ for the set of double cosets $\pi_1(\Sigma) \backslash \Gamma / Z_\Gamma(b)$ and, for each i , let β_i be a closed curve on Σ that represents $(b^q)^{g_i}$.

If b is of finite order then every β_i is null-homotopic. By Proposition 3.5 there is a finite-sheeted cover Σ' to which α has a primitive elevation α' . Because α' is primitive in $H_1(\Sigma')$ there is a retraction $\rho: \pi_1(\Sigma') \rightarrow \langle \alpha' \rangle$, and

$$\rho(\beta'_i) = 1$$

whenever β'_i is an elevation of some β_i to Σ' . It now follows from Lemma 2.1 that there is a homomorphism to a finite group under which the images of a and b are non-conjugate.

We can therefore assume that b is of infinite order. For each i , let $\tilde{\Sigma}_i$ be the finite-sheeted covering provided by Proposition 3.7, in which no elevation of α is homologous to an elevation of $\beta_i^{\pm 1}$. Now let $\tilde{\Sigma}$ be the covering defined by

$$\pi_1(\tilde{\Sigma}) = \bigcap_i \pi_1(\tilde{\Sigma}_i).$$

Intersecting $\pi_1(\tilde{\Sigma})$ with its conjugates, we can assume furthermore that $\pi_1(\tilde{\Sigma})$ is a normal subgroup of Γ . Let $m = \deg_{\pi_1(\tilde{\Sigma})}(a)$ and let $\tilde{\alpha}$ be a closed curve representing a^m in $\pi_1(\tilde{\Sigma})$.

If $n = \deg_{\pi_1(\tilde{\Sigma})}(b)$ then any Γ -conjugate of b^n is conjugate in $\pi_1(\tilde{\Sigma})$ to some elevation of some β_i . Hence, to satisfy the hypotheses of Lemma 2.1, we must construct a retraction $\rho : \pi_1(\tilde{\Sigma}) \rightarrow \langle \tilde{\alpha} \rangle$ such that $\rho(\tilde{\beta}_i^m) \neq \tilde{\alpha}^n$ whenever $\tilde{\beta}_i$ is an elevation of some β_i .

Suppose that $n[\tilde{\beta}_i] = m[\tilde{\alpha}]$ in $H_1(\tilde{\Sigma})$. Then, as $\tilde{\alpha}$ and $\tilde{\beta}_i$ are both primitive in homology, $m = n$ and $[\tilde{\alpha}] = \pm[\tilde{\beta}_i]$. But this contradicts the properties of $\tilde{\Sigma}$. Therefore, choosing a suitable projection $H_1(\tilde{\Sigma}) \rightarrow \langle \tilde{\alpha} \rangle$ and defining ρ to be the concatenation

$$\rho : \pi_1(\tilde{\Sigma}) \rightarrow H_1(\tilde{\Sigma}) \rightarrow \langle \tilde{\alpha} \rangle$$

we obtain a retraction that satisfies the hypotheses of Lemma 2.1. It follows that there exists a homomorphism σ from $\pi_1(\Sigma)$ to a finite group such that $\sigma(a)$ and $\sigma(b)$ are not conjugate, as required. $\square$

Because surface groups are torsion-free, it follows immediately that hyperbolic surface groups are conjugacy separable. Indeed, the proof did not use the hyperbolic structure on Σ , and applies just as well to Euclidean surfaces.

Corollary 3.9. *Surface groups are conjugacy separable.*

Remark 3.10. That free groups are conjugacy separable is a special case of Theorem 3.8. Indeed, one can provide a very quick proof of this fact using Lemma 2.1 and the topology of graphs. The idea is to pass to a finite-sheeted cover in which every elevation of a pair of non-conjugate elements is a simple closed curve. It is then clear that they differ in homology.

4. Omnipotence

In this section we improve further upon the results of the previous section to prove omnipotence. To apply Lemma 2.6, we need a criterion to ensure that elevations are linearly independent in homology. The next proposition provides this.

Proposition 4.1. *Let Σ be a hyperbolic surface and let $\alpha, \beta_1, \dots, \beta_l$ be a collection of primitive curves with the property that no β_i is homologous to α or its inverse. Then there exists a finite-sheeted cyclic covering space $\tilde{\Sigma}$ such that any elevation $\tilde{\alpha}$ of α is linearly independent in homology of the set of all elevations of all the β_i . Hence, there exists a retraction*

$$\rho : \pi_1(\tilde{\Sigma}) \rightarrow \langle \tilde{\alpha} \rangle$$

such that $\rho(\tilde{\beta}_i) = 1$ whenever $\tilde{\beta}_i$ is an elevation of some β_i .

Proof. Consider first the case when α is non-separating. Let γ_1 be a non-separating simple closed curve with $i(\alpha, \gamma_1) = 1$. The commutator $\delta = [\alpha, \gamma_1]$ is a separating simple closed curve, because Σ is hyperbolic. Let γ_2 be a primitive curve in the component of $\Sigma \setminus \delta$ that does not contain γ_1 . Neither γ_1 nor γ_2 is homologous to α or its inverse.

By the hypotheses on homology there exists a homomorphism $\pi_1(\Sigma) \rightarrow \mathbb{Z}$ that kills α but kills none of the β_i and neither of the γ_k . Consider the composition

$$\psi : \pi_1(\Sigma) \rightarrow \mathbb{Z} \rightarrow \mathbb{Z}/p$$

where p is a prime large enough that all the $\psi(\beta_i)$ and both the $\psi(\gamma_k)$ are non-zero. Let $\iota : \tilde{\Sigma} \rightarrow \Sigma$ be the covering map with $\pi_1(\tilde{\Sigma}) = \ker \psi$. Then α has p elevations to $\tilde{\Sigma}$, which we denote by $\tilde{\alpha}_1, \dots, \tilde{\alpha}_p$, whereas each β_i only has one elevation, denoted $\tilde{\beta}_i$.

Without loss of generality we can take each $\check{\alpha}_j$ to be a lift of $\alpha\gamma_1^{1-j}$. In particular, $\check{\alpha}_1\check{\alpha}_2^{-1} = \delta$ in $\pi_1(\Sigma)$. But because neither γ_1 nor γ_2 lift to $\check{\Sigma}$, it follows from Lemma 3.4 that δ lifts to a non-separating curve $\check{\delta}$ in $\check{\Sigma}$. Hence

$$[\check{\alpha}_1] - [\check{\alpha}_2] = [\check{\delta}] \neq 0$$

so the elevations $\check{\alpha}_1$ and $\check{\alpha}_2$ are not homologous.

Associated to the covering map ι there is the induced map $\iota_* : H_1(\check{\Sigma}) \rightarrow H_1(\Sigma)$ and the transfer map $\tau^* : H_1(\Sigma) \rightarrow H_1(\check{\Sigma})$, which maps a curve to the sum of its elevations. The composition $\iota_* \circ \tau^*$ is equal to multiplication by p . We shall use the transfer map to show that $[\check{\alpha}_1]$ is linearly independent from the $[\check{\beta}_i]$.

Suppose that there are constants κ and λ_i such that the equation

$$\kappa[\check{\alpha}_1] = \sum_i \lambda_i[\check{\beta}_i]$$

holds in $H_1(\check{\Sigma})$. Applying ι_* to both sides gives

$$\kappa[\alpha] = p \sum_i \lambda_i[\beta_i]$$

so $\kappa = p\kappa'$ for some κ' . Dividing by p and applying τ^* to both sides this becomes

$$\kappa' \sum_j [\check{\alpha}_j] = \sum_i \lambda_i[\check{\beta}_i] = \kappa[\check{\alpha}_1].$$

The action of $\mathbb{Z}/p$ on $\check{\Sigma}$ is transitive on the set of elevations of α , so unless $\kappa = 0$ it follows that

$$[\check{\alpha}_1] = [\check{\alpha}_j]$$

for any j . But this contradicts our previous observation that $\check{\alpha}_1$ and $\check{\alpha}_2$ are not homologous, so $\kappa = 0$. This completes the proof when α is non-separating.

Suppose now that α is boundary-parallel. The proof proceeds similarly to the previous case. As before, let $\psi : \pi_1(\Sigma) \rightarrow \mathbb{Z}/p$ be a homomorphism that kills α but kills none of the β_i , and let $\check{\Sigma}$ be the covering corresponding to $\ker \psi$. Now, because $p \geq 2$, we see that $\check{\Sigma}$ has at least four boundary components, and hence no pair of elevations of α is homologous. The same argument using the transfer map again implies that an elevation $\check{\alpha}_1$ of α is linearly independent from the set of elevations of the β_i . $\square$

Let $\alpha_1, \dots, \alpha_l$ be an independent collection of elements of $\pi_1(\Sigma)$, viewed as closed curves on Σ . We can apply Proposition 4.1 pairwise to the α_i .

Remark 4.2. Fix $i \neq j$. By Proposition 3.7 there exists a finite-sheeted cover $\tilde{\Sigma}_{i,j}$ of Σ in which, whenever $\tilde{\alpha}_i$ and $\tilde{\alpha}_j$ are elevations of α_i and α_j respectively:

1. $\tilde{\alpha}_i$ is a non-separating simple closed curve; and
2. $\tilde{\alpha}_i$ and $\tilde{\alpha}_j^{\pm 1}$ are not homologous.

Let $\tilde{\Sigma}$ be the finite-sheeted cover of Σ such that

$$\pi_1(\tilde{\Sigma}) = \bigcap_{i \neq j} \pi_1(\tilde{\Sigma}_{i,j}).$$

Then $\tilde{\Sigma}$ has the property that every elevation of an $\tilde{\alpha}_i$ is a non-separating simple closed curve, and no pair of elevations of $\tilde{\alpha}_i$ and $\tilde{\alpha}_j^{\pm 1}$ are homologous when $i \neq j$.

Fix i and an elevation $\tilde{\alpha}_i$ of α_i . Let $\{\tilde{\alpha}_{j,k} \mid i \neq j\}$ be the set of all elevations of all α_j (where $i \neq j$) to $\tilde{\Sigma}$. Applying Proposition 4.1 to $\tilde{\alpha}_i$ together with the set $\{\tilde{\alpha}_{j,k} \mid i \neq j\}$, it follows that there exists a finite-sheeted normal covering $\check{\Sigma}_i \rightarrow \tilde{\Sigma}$ with the property that any elevation $\check{\alpha}_i$ of $\tilde{\alpha}_i$ is linearly independent from the set of all elevations $\{\check{\alpha}_{j,k} \mid i \neq j\}$ of all the $\tilde{\alpha}_{j,k}$ (with $i \neq j$).

Let $\check{\Sigma}$ be the cover of Σ such that

$$\pi_1(\check{\Sigma}) = \bigcap_i \pi_1(\check{\Sigma}_i).$$

This has the required property for all i —that is, whenever $\check{\alpha}_i$ is an elevation of α_i to $\check{\Sigma}$, there is a retraction $\rho_i : \check{\Sigma} \rightarrow \langle \check{\alpha}_i \rangle$ such that $\rho_i(\check{\alpha}_j) = 1$ for any elevation $\check{\alpha}_j$ of any α_j with $i \neq j$. Furthermore, by intersecting $\pi_1(\check{\Sigma})$ with all its conjugates, we can assume that $\check{\Sigma} \rightarrow \Sigma$ is a regular covering.

We can now prove our main theorem.

Theorem 4.3. *Let Γ be a Fuchsian group (of the first kind) and let $a_1, \dots, a_l$ be an independent set of elements of infinite order in Γ . Then there is a constant K such that, whenever $p_1, \dots, p_l$ are positive integers, there is a homomorphism η from Γ to a finite group such that*

$$o(\eta(a_i)) = Kp_i$$

for each i .

Proof. By Selberg's Lemma, Γ has a torsion-free normal subgroup of finite index, which we can think of as $\pi_1(\Sigma)$ where Σ is a hyperbolic surface. For each i , let $m_i = \deg_{\pi_1(\Sigma)}(a_i)$ and fix a set of representatives $\{g_{i,k}\}$ for $\pi_1(\Sigma) \backslash \Gamma / Z_\Gamma(a_i)$. For each i and k , let $\alpha_{i,k}$ be a closed curve on Σ representing $(a_i^{m_i})^{g_{i,k}}$.

The set of $\alpha_{i,k}$ correspond to an independent set of elements of $\pi_1(\Sigma)$, so by Remark 4.2 there is a finite-sheeted covering $\check{\Sigma} \rightarrow \Sigma$ such that any elevation $\check{\alpha}_{i,k}$ of $\alpha_{i,k}$ is linearly independent in homology from the set of homology classes of all elevations of the set $\{\alpha_{j,k'} \mid (i,k) \neq (j,k')\}$. It follows that there exists a retraction $\rho_i : \pi_1(\check{\Sigma}) \rightarrow \langle \check{\alpha}_{i,k} \rangle$ such that

$$\rho_i(\check{\alpha}_{j,k'}) = 1$$

whenever $j \neq i$ (indeed, whenever $(j,k') \neq (i,k)$). It follows that ρ_i satisfies the hypotheses of Lemma 2.6 and hence, setting $K = \prod_i m_i$, there exists a map η from Γ to a finite group such that

$$o(\eta(a_i)) = Kp_i$$

for each i , as required. $\square$

It follows immediately that surface groups are omnipotent.

Corollary 4.4. (See Bajpai [1].) *If Σ is a compact hyperbolic surface (possibly with boundary) then $\pi_1(\Sigma)$ is omnipotent.*

The theorem of Wise that free groups are omnipotent [11] is a corollary. His proof of this fact uses a similar criterion to that of Lemma 2.6, although he does not use wreath products to achieve it. He then proceeds to construct the required retraction explicitly, using a refinement of Stallings' proof of Marshall Hall's Theorem [9]. The methods of this paper provide a simple alternative proof of omnipotence for free groups. The ideas of Proposition 4.1 work just as well in the context of graphs, and omnipotence follows immediately from Lemma 2.6.

Acknowledgments

Thanks to Alan Reid and to Martin Bridson for patient conversations. Thanks also to Eric Katerman for some useful comments.

References

- [1] Jitendra Bajpai, Omnipotence of surface groups, Masters Thesis, McGill University, 2007.
- [2] Thomas Delzant, Sous-groupes distingués et quotients des groupes hyperboliques, *Duke Math. J.* 83 (1996) 661–682.
- [3] Benjamin Fine, Gerhard Rosenberger, Conjugacy separability of Fuchsian groups and related questions, in: *Contemp. Math.*, vol. 109, Amer. Math. Soc., Providence, RI, 1990, pp. 11–18.
- [4] M. Gromov, Hyperbolic groups, in: *Math. Sci. Res. Inst. Publ.*, vol. 8, Springer, New York, 1987, pp. 75–263.
- [5] D.D. Long, A.W. Reid, Subgroup separability and virtual retractions of groups, *Topology* 47 (2008) 137–159.
- [6] G.A. Niblo, Separability properties of free groups and surface groups, *J. Pure Appl. Algebra* 78 (1992) 77–84.
- [7] A.Yu. Ol'shanskii, On residualizing homomorphisms and G-subgroups of hyperbolic groups, *Internat. J. Algebra Comput.* 3 (1993) 365–409.
- [8] Peter Scott, Subgroups of surface groups are almost geometric, *J. London Math. Soc.* (2) 17 (1978) 555–565.
- [9] John R. Stallings, Topology of finite graphs, *Invent. Math.* 71 (1983) 551–565.
- [10] P.F. Stebe, Conjugacy separability of certain Fuchsian groups, *Trans. Amer. Math. Soc.* 163 (1972) 173–188.
- [11] Daniel T. Wise, Subgroup separability of graphs of free groups with cyclic edge groups, *Q. J. Math.* 51 (2000) 107–129.