A representation theoretic characterization of simple closed curves on a surface

THOMAS KOBERDA AND RAMANUJAN SANTHAROUBANE

Abstract. We produce a sequence of finite dimensional representations of the fundamental group $\pi_1(S)$ of a closed surface where all simple closed curves act with finite order, but where each non–simple closed curve eventually acts with infinite order. As a consequence, we obtain a representation theoretic algorithm which decides whether or not a given element of $\pi_1(S)$ is freely homotopic to a simple closed curve. The construction of these representations combines ideas from TQFT representations of mapping class groups with effective versions of LERF for surface groups.

1. Introduction

Let $S = S_g$ be a closed and orientable surface of genus $g \geq 2$. A *simple closed curve* on S is a homotopically essential embedding of the circle S^1 into S. Fixing a basepoint in the interior of S, an element $1 \neq \gamma \in \pi_1(S)$ is called *simple* if it is freely homotopic to a simple closed curve, and *non–simple* otherwise. A homotopy class of loops $\gamma\colon S^1 \to S$ is called an *proper power* if there is a loop $\gamma_0\colon S^1 \to S$ and an $n > 1$ such that $\gamma = \gamma_0^n$, i.e. γ_0 concatenated with itself n times. In this article, we propose a representation theoretic characterization of the simple elements in $\pi_1(S)$, which thus relates a topological property of a conjugacy class in $\pi_1(S)$ with the representation theory of $\pi_1(S)$. Precisely:

Theorem 1.1. *Let X be a fixed finite generating set for $\pi_1(S)$, and let ℓ_X be the corresponding word metric on $\pi_1(S)$. There exists an explicit sequence of finite dimensional complex representations $\{\rho_i\}_{i\geq 1}$ and a computable function f depending only on X such that:*

(1) For each simple element $1 \neq \gamma \in \pi_1(S)$ and each i, the linear map $\rho_i(\gamma)$ has finite order bounded by a constant which depends only on i;
(2) An element $1 \neq \gamma \in \pi_1(S)$ which is not a proper power is non–simple if and only if $\rho_i(\gamma)$ has infinite order for all $i \geq f(\ell_X(\gamma))$.

Date: March 10, 2016.

Corollary 1.2. *Let $\gamma \in \pi_1(S)$ be non–simple and not a proper power. Then there is a finite dimensional linear representation ρ of $\pi_1(S)$ under which all simple elements have finite order, but where $\rho(\gamma)$ has infinite order.*

Algebraic and algorithmic characterizations of simple closed curves on surfaces have been studied by many authors for quite some time. The first group–theoretic characterization of simplicity of elements in $\pi_1(S)$ was given by Zieschang (see [21], [22]). Algorithms, among them ones of both algebraic and geometric nature, were given by Chillingworth in [10] and [11], Turaev–Viro [20], Birman–Series [3] with extensions by Cohen–Lustig [9], Hass–Scott [13], Arettines [2], Cahn [4], and Chas–Krongold in [5] and [6]. The foundational work of Goldman [12] has guided much of the progress in the study of algebraic characterizations of simple closed curves (see also [19]).

Corollary 1.3. *There exists an algorithm which, by computing a certain representation of $\pi_1(S)$, decides whether or not an element $1 \neq \gamma \in \pi_1(S)$ is simple.*

The representations in Theorem 1.1 and Corollary 1.2 come from TQFT representations of mapping class groups, combined with certain canonical representation theoretic constructions. To the authors' knowledge, Corollary 1.3 gives the first representation theoretic and the first topological quantum field theoretic characterization of simple closed curves on a surface.

We remark that Theorem 1.1 and its corollaries all hold for compact orientable surfaces with boundary. We have limited our discussion to closed surfaces in order to make some of the statements cleaner, but the arguments work for surfaces with boundary in a manner which is essentially unchanged.

2. Acknowledgements

The authors thank J. Aramayona, V. Krushkal, G. Masbaum, and H. Parlier for helpful discussions.

3. Background

3.1. **Hyperbolic geodesics.** Let S be a closed, orientable surface with a fixed complete hyperbolic metric. It is a standard fact that in every free homotopy class of closed curves on S there is a unique hyperbolic geodesic. Whereas we think of homotopy classes of loops as maps $S^1 \to S$, we think of closed geodesics as subsets $\gamma \subset S$. Thus, when speaking of geodesics, we do not distinguish between the geodesic representative of a homotopy class $\gamma \colon S^1 \to S$ and any of its nonzero powers $\gamma^n \colon S^1 \to S$.

3.2. **Effective LERF.** Let G be a group. We say that G is *locally extended residually finite* or *LERF* if every finitely generated subgroup G is closed in the profinite topology on G. The topological meaning of LERF is given by the following well–known fact:

Lemma 3.1. *Let X be a simplicial complex such that $\pi_1(X)$ is LERF, let K be a finite simplicial complex, and let $f\colon K \to X$ be a simplicial map such that some lift*

$$\tilde{f}\colon \widetilde{K} \to \widetilde{X}$$

of f to the universal covers of K and X respectively is an embedding. Then there exists a finite cover $X' \to X$ and a lift $f'\colon K \to X'$ of f such that f' is an embedding.

We recall a proof for the convenience of the reader.

Proof of Lemma 3.1. The failure of the embedding of K via f can be quantified by a finite collection of simplices $K_X \subset X$, i.e. the simplices $\sigma \subset K$ for which there exists another simplex $\tau \subset K$ such that $f(\sigma) = f(\tau)$. Note that if $X' \to X$ is a cover and if $f'\colon K \to X'$ is a lift of f then $K_{X'} \subset K_X$, though $K_{X'}$ may depend on the choice of lift f' if the cover $X' \to X$ is not regular.

We can proceed by induction on $|K_X|$. If $|K_X| = 0$ then f is an embedding. Otherwise, choose a non–closed simplicial path $\gamma \subset K$ such that $f(\gamma)$ is a closed loop. By definition, both endpoints of γ lie in simplices in K_X. Note that, after choosing a basepoint for $\pi_1(X)$, the loop $f(\gamma)$ is homotopic to an element in $\pi_1(X) \setminus f_*(\pi_1(K))$. Since $\pi_1(X)$ is LERF, there is a finite cover $X' \to X$ and a lift f' of f such that K lifts to X' but the loop $f(\gamma)$ does not lift to a closed loop in X'. It follows that the simplices containing the endpoints of γ no longer lie in $K_{X'}$, completing the inductive step. □

A famous result of P. Scott [18] says that closed surface groups are LERF. We will require an effective version of Scott's theorem, which was obtained by P. Patel [17]. To state the effective version, let S be a compact surface of negative Euler characteristic. Following Patel, we give S the *standard* hyperbolic metric, one which comes from a tiling by right-angled hyperbolic pentagons. If $H < \pi_1(S)$ is an infinite index, finitely generated subgroup, we let $X \to S$ be the corresponding cover and $C(X)$ the *convex core* of X. That is to say, $C(X)$ is the smallest, closed, convex subsurface of X with geodesic boundary for which the inclusion into X is a homotopy equivalence. Note that H is a finitely generated free group of rank n. Let β be the total length of the geodesic boundary of $C(X)$, which is finite since H has finite rank.

Theorem 3.2 ([17], Theorem 7.1)**.** *Suppose $n \geq 2$, let $\gamma \in \pi_1(S) \setminus H$, and let ℓ_γ be the length of the geodesic representative of γ. There exists a finite index subgroup*

$K < \pi_1(S)$ containing H but not γ such that

$$[\pi_1(S) : K] < 4n - 4 + \frac{2\sinh[d \cdot (\ell_\gamma/e + 2)]}{\pi} \cdot \beta,$$

where d and e are fixed positive constants.

3.3. **Word metrics and quasi–isometry.** Recall that a map $f\colon X \to Y$ between two metric spaces is a *quasi–isometry* if there exist constants $\lambda \geq 1$ and $C, D \geq 0$ such that for all $a, b \in X$ we have

$$\frac{1}{\lambda} \cdot d_X(a,b) - C \leq d_Y(f(a), f(b)) \leq \lambda \cdot d_X(a,b) + C,$$

and if for each $y \in Y$ there is an $x \in X$ such that $d_Y(f(x), y) \leq D$. The classical Milnor–Schwarz Lemma says that if a finitely generated group G acts properly and cocompactly by isometries on a proper geodesic metric space X then the Cayley graph for G with respect to any finite generating set is quasi–isometric to X. It follows that the word metric on any closed surface group is quasi–isometric to the hyperbolic metric on $\mathbb{H}^2$.

Fix a finite generating set X for $\pi_1(S)$. Note that if $1 \neq \gamma \in \pi_1(S)$ then $\ell_X(\gamma) \geq 1$. The following is an immediate consequence of the definition of a quasi–isometry:

Lemma 3.3. *Let $\gamma \in \pi_1(S)$, and assume that γ is not a proper power. Let ℓ_γ denote the length of a geodesic representative for γ, and let $\ell_X(\gamma)$ denote the length of γ in the generating set X. Then for some $\lambda = \lambda(X, S)$, we have $\ell_\gamma \leq \lambda \cdot \ell_X(\gamma)$.*

In Lemma 3.3, we are justified in deleting the additive constant C on the right because ℓ_X only takes positive integer values on nontrivial elements of $\pi_1(S)$ and because we are free to replace the multiplicative constant λ by $\lambda + C$.

Recall that a collection $\{\alpha_i\}_{i \in I}$ of curves is called *filling* if

$$S \setminus \bigcup_i \alpha_i$$

is a union of disks.

Lemma 3.4. *Let X be a finite generating set for $\pi_1(S)$ and let $\gamma \in \pi_1(S)$. Then there is a constant $C = C(X, S)$ such that the geodesic representative for γ has at most $C \cdot (\ell_X(\gamma))^2$ self–intersections.*

Lemma 3.4 is proved in a slightly different form and by different methods by Malestein–Putman (See [16], Lemma 3.1). More precise self–intersection bounds are also studied in [9], [7], and [8].

If δ and α are two closed (though not necessarily simple nor essential) curves on S which intersect transversely, we will write $i(\alpha, \delta)$ for the geometric intersection number of α and δ, counted will multiplicity. That is to say, if we view δ as a map

$$\delta\colon S^1 \to S,$$

then

$$i(\alpha, \delta) = |\delta^{-1}(\delta \cap \alpha)|.$$

Observe that with this definition the function i is not symmetric in its arguments, though it is symmetric if both δ and α are simple.

Proof of Lemma 3.4. Without loss of generality, we may assume that γ is not a proper power. Writing γ as a product of elements of X and ℓ for $\ell_X(\gamma)$, we have that the geodesic representative for γ has length at most $\lambda \cdot \ell$ for some appropriately chosen constant λ, by Lemma 3.3. We will abuse notation and refer to the geodesic representative for γ by γ as well.

We fix $\mathcal{A} = \{\alpha_i\}_{i \in I}$ a finite filling collection of simple closed geodesic curves with no triple intersections of curves. Let N be the minimal width of a collar neighborhood of any α_i, chosen thinly enough so that no point on S lies in three collars. Evidently, N can be chosen in a way which depends only on S. If δ is any closed geodesic on S with

$$i(\mathcal{A}, \delta) := \sum_i i(\alpha_i, \delta),$$

we have the *a priori* estimate

$$\frac{N}{2} \cdot i(\mathcal{A}, \delta) \leq \ell_\delta.$$

It follows that

$$i(\mathcal{A}, \gamma) \leq \frac{2\lambda \cdot \ell}{N}.$$

Note that the self–intersections of γ must occur either on α or in the interior of $S \setminus \mathcal{A}$. If D is a component of $S \setminus \mathcal{A}$ then any two arcs in $\gamma \cap D$ intersect at most once, since D is contractible and since γ is a geodesic. Thus, we see that the number of self–intersections of γ in the interior of D is bounded by the number of components of $\gamma \cap D$ choose two, which is a quadratic function in $i(\partial D, \gamma)$. The lemma now follows easily. □

3.4. **Finding roots of elements in $\pi_1(S)$.** Let $1 \neq \gamma \in \pi_1(S)$ be an element, written as a word in the generating set X. We can algorithmically determine whether or not γ is a proper power.

Lemma 3.5. *There is an algorithm which decides if $\gamma \in \pi_1(S)$ is a proper power, which has exponential complexity in $\ell_X(\gamma)$.*

Proof. We have that for some $\lambda > 0$, the geodesic representative for γ has length at most $\lambda \ell_X(\gamma)$. We have that γ is a proper power if and only if the map $S^1 \to S$ whose image is the geodesic in the free homotopy class of γ wraps around the geodesic at least twice. If $Y \subset \pi_1(S)$ is the set of (exponentially many in $\ell_X(\gamma)$) elements whose geodesic representatives have length at most $\lambda \ell_X(\gamma)$, we have that γ is a proper power if and only if some $\gamma' \in Y$ with $\gamma' \neq \gamma$ commutes with γ in $\pi_1(S)$. To check whether or not a given γ' commutes with γ has linear complexity in $\ell_X(\gamma) + \ell_X(\gamma')$, since $\pi_1(S)$ is hyperbolic and thus has a linear Dehn function. □

3.5. **Embedded figure eight loops.** Let $\gamma \subset S$ be closed geodesic with exactly one self–intersection, so that γ can be termed a *figure eight loop*. Fixing a basepoint for S on γ (say the self–intersection point), we can orient γ and identify it with an element of $\pi_1(S)$. Note that the requirement that γ be geodesic automatically guarantees that this figure eight loop is *essential*, i.e. that the two simple subloops of γ generate a copy of the free group $F_2 < \pi_1(S)$. The following is a straightforward consequence of the main technical result of the authors [15]:

Lemma 3.6. *Let $S_g = S$ a closed surface of genus g. There is a linear representation $\rho\colon \pi_1(S) \to GL_n(\mathbb{C})$ such that:*

1. *If $\gamma \in \pi_1(S)$ has an embedded essential figure eight loop as its geodesic representative, then $\rho(\gamma)$ has infinite order;*
2. *The image of each simple element in $\pi_1(S)$ under ρ has finite order bounded by k, where k depends only on ρ;*
3. *We have $n \leq K^g$, where K is a constant independent of g.*

In the interest of brevity, we will not describe the representation ρ in any detail. However, ρ can be written down explicitly and is thus computable.

Proof of Lemma 3.6. In [15], we considered a sequence of representations

$$\rho_p : \pi_1(S_g) \to \mathrm{PGL}_{d(p,g)}(\mathbb{C})$$

indexed by odd integers $p \geq 3$.

It is straightforward to adjust the proof of Theorem 1.1 of [15] to establish the following: if γ is an arbitrary figure eight loop then there exists $p_0(\gamma)$ such that for $p \geq p_0(\gamma)$ we have $\rho_p(\gamma)$ has infinite order.

These representations were obtained from restrictions of quantum SO(3) representations of mapping class groups. This clearly implies that if $\rho_p(\gamma)$ has infinite order for some p, then $\rho_p(\gamma')$ has infinite order for all γ' in the mapping class group orbit of γ.

Now since there are only finitely many figure eight loops in $\pi_1(S_g)$ up to the action of the mapping class group, we can choose one p_0 such that if γ is an arbitrary figure eight loop then $\rho_{p_0}(\gamma)$ is an infinite order element.

Following the discussion in Section 4.4 of [15], we can choose p_0 independently of g, and we have $d(g, p_0) \leq K^g$ for some constant K which is also independent of g. Finally, the image of any simple element in $\pi_1(S_g)$ under ρ_{p_0} has order at most $2p_0$. □

3.6. **Induced representations.** We will require some well–known fact from representation theory, which we gather here for the convenience of the reader. We will restrict to complex representations, though the discussion works over any field of characteristic zero.

Let G be a group, let H be a finite index subgroup of G, and let V be a finite dimensional complex representation of H. The *induced representation* of G is a canonical way to turn V into a finite dimensional representation of G. Precisely, we take

$$\mathrm{Ind}_H^G V := \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V.$$

It is standard that the complex dimension of $\mathrm{Ind}_H^G V$ is given by $[G : H] \cdot \dim V$. Frobenius reciprocity, suitably generalized to infinite groups, guarantees that if $h \in H$ acts with infinite order on V then h also acts with infinite order on $\mathrm{Ind}_H^G V$.

Lemma 3.7. *Let $H < \pi_1(S)$ be a finite index subgroup, classifying a finite cover $S' \to S$. Let V be a finite dimensional representation of H such that each simple element of $H = \pi_1(S')$ acts with finite order. Then if $1 \neq \gamma \in \pi_1(S)$ is simple, we have that γ acts with finite order on* $\mathrm{Ind}_H^G V$.

Proof. Let $\gamma \in \pi_1(S)$ be a given simple element. Since H classifies a finite cover $S' \to S$, there is a smallest positive integer N such that γ^N lies in every conjugate of H, so that each conjugate of γ^N is freely homotopic to a power of a simple closed curve on S'.

If $\{t_1, \ldots, t_k\}$ are coset representatives for H in G, we have that

$$\mathrm{Ind}_H^G V \cong \bigoplus_{i=1}^{k} t_i \otimes V.$$

We then have for each i,

$$\gamma^N \cdot (t_i \otimes V) = t_i \otimes ((t_i^{-1} \gamma^N t_i) \cdot V).$$

Since γ^N is a power of a lift of a simple element of $\pi_1(S)$, it acts with finite order on V. Since conjugating γ^N is simply a different choice of lift, we have that $t_i^{-1}\gamma^N t_i$ also acts with finite order on V. □

4. Immersed figure eight loops

Let $E \cong S^1 \vee S^1$ be a figure eight. Though E is not a manifold, it will be useful for our purposes to speak of a smooth structure on E. Away from the wedge point w, we will think of E as a smooth one–manifold. The smooth structure at w will simply be this: a chart defined on the neighborhood of w maps to the intersection of the x–axis and y–axis in a neighborhood of the origin in $\mathbb{R}^2$, which we will think of as inheriting a smooth structure from $\mathbb{R}^2$. Thus, the tangent space at w consists of the union $T_1 \cup T_2$ of two one–dimensional spaces. A smooth path in a neighborhood of w thus has a unique (unoriented) direction of travel through w. It is convenient for us to think of the neighborhood of w as a union of two smooth intervals c_1 and c_2 which meet at w, and whose tangent spaces at w are T_1 and T_2 respectively. A map $f\colon E \to M$, where M is a smooth manifold, is called *smooth* at w if it is smooth when restricted to c_1 and c_2 separately.

Lemma 4.1. *Let $\gamma \subset S$ be a closed geodesic with at least one self–intersection. Then γ is the image of a smooth immersion $f\colon E \to S$.*

Proof. Choose an arbitrary orientation on γ and an arbitrary self–intersection point $p \in \gamma$. In a small neighborhood U of p, we have that $\gamma \cap U$ is a pair of transversely intersecting oriented arcs α and β. We start at p and travel along α in the direction of the orientation. We follow γ until we return to p for the first time. Note that this will happen along the arc β, since geodesics are uniquely determined by a point and a direction. We denote the resulting loop on S by γ_1. Continuing from p along β, we eventually return to p for a second time along α, tracing another closed loop γ_2. We have thus decomposed γ as a union of two distinct closed curves on S which meet at p. Therefore, $\gamma_1 \cup \gamma_2$ is the image of a smooth immersion $E \to S$ sending the wedge point $w \in E$ to p. □

Note that since γ is itself a geodesic, it is shortest within its homotopy class. This immediately implies that the subloops γ_1 and γ_2 are homotopically essential and not homotopic to each other, even after reversing one of their orientations. Viewing γ_1 and γ_2 as oriented homotopy classes of loops based at p, we see that they generate a copy of the free group $F_2 < \pi_1(S)$.

Lemma 4.2. *Let $\gamma \subset S$ be a closed geodesic with at least one self–intersection, and let $f\colon E \to S$ be an immersion with image γ. Then there is a finite cover $S' \to S$ and a lift $f'\colon E \to S'$ of f which is an embedding. In particular, γ lifts to a figure eight loop in S'.*

Proof. Let p be a self–intersection of γ, which we use as a basepoint for $\pi_1(S)$. We have that $\pi_1(E) \cong F_2$, and $f_*(\pi_1(E))$ is a copy of $F_2 < \pi_1(S)$. The claim of the lemma follows from Scott's Theorem that surface groups are LERF. □

Let $X \to S$ be the cover of S corresponding to the subgroup $f_*(\pi_1(E)) < \pi_1(S)$. We have that X is homeomorphic to a thrice punctured sphere, though from a geometric point of view we have that X has a compact *core* (cf. Subsection 3.2) which is homeomorphic to a pair of pants, together with three flaring ends. The boundary curves (i.e. *cuffs*) of the compact core $C(X) \cong P$ are closed geodesics. Observe that if $f'\colon E \to S'$ is a lift of f which is an embedding, then the natural extension of f' to P will also be an embedding, since the cuffs of P have simple and pairwise disjoint representatives inside of a tubular neighborhood of $f'(E)$.

Lemma 4.3. *Let $f\colon E \to S$ be an immersion with geodesic image γ, let $X \to S$ be the cover of S corresponding to the subgroup $f_*(\pi_1(E))$, and let $P = C(X)$ be the core of X. Write $\{\ell_i \mid 1 \le i \le 3\}$ for the lengths of the geodesic cuffs of P. Then for each i, we have $\ell_i \le \ell_\gamma$.*

Proof. Writing E as a wedge of two circles, these two circles trace out two subloops γ_1 and γ_2 of γ, the sum of whose lengths is ℓ_γ. Orienting these loops appropriately and thinking of γ_1 and γ_2 as homotopy classes of loops based at p, the homotopy classes of the cuffs of P are $\{\gamma_1, \gamma_2, \gamma_1\gamma_2\}$. Since the geodesic representative of a curve is the shortest curve in its free homotopy class, we see that the cuff lengths of P are each at most ℓ_γ, the desired conclusion. □

Lemma 4.4. *Let γ' be a geodesic on S which is freely homotopic to a simple subloop of γ. Then $\ell_{\gamma'} \le \ell_\gamma$.*

Proof. This is almost clear. Performing a homotopy of γ' into a subloop in γ, we have that γ' traverses no subarc of γ more than once, so the length estimate is immediate. □

As before, we use the self–intersection point p of γ as a basepoint for $\pi_1(S)$, so that $f_*(\pi_1(E))$ is unambiguously identified with a rank two free subgroup of $\pi_1(S)$. Recall that we have chosen a finite generating set X for $\pi_1(S)$.

Lemma 4.5. *If γ has at least two self–intersections then there is an element $\gamma' \in \pi_1(S) \setminus f_*(\pi_1(E))$ such that γ' is freely homotopic into $f(P)$ and such that $\ell_X(\gamma') \le 3\lambda \cdot \ell_\gamma$.*

Proof. Let $\gamma' \subset \gamma$ be an arbitrary essential subloop. By passing to a shorter essential subloop if necessary, we assume that aside from the self–intersection points of γ, the subloop γ' traverses each subarc of γ at most once, which immediately implies that γ' is not a proper power. Choose a minimal length path $\delta \subset \gamma$ from p to γ'. Note that the total length of the loop $\delta^{-1} \circ \gamma' \circ \delta$ is at most $3\ell_\gamma$, so that by Lemma 3.3, we have that $\ell_X(\delta^{-1} \circ \gamma' \circ \delta) \le 3\lambda \cdot \ell_\gamma$.

We claim that the homotopy class at least one such loop $\delta^{-1} \circ \gamma' \circ \delta$ does not lie in $f_*(\pi_1(E))$, which will establish the lemma. Note that if the homotopy class of each such element $\delta^{-1} \circ \gamma' \circ \delta$ was in $f_*(\pi_1(E))$ then the immersion $f\colon P \to X$ would in fact be an embedding, since every essential loop in $f(P)$ would lift to the cover of X corresponding to $f_*(\pi_1(E)) = f_*(\pi_1(P))$. Since E is the core of the pair of pants P and therefore has one self–intersection, we see that then γ would have exactly one self–intersection, a contradiction. □

5. Identifying non–simple curves

In this section, we prove Theorem 1.1 and Corollary 1.3. The representation ρ_i in the statement of Theorem 1.1 will be as follows: let $\{S_k \to S\}_{k\in\mathbb{N}}$ be a computable enumeration of the finite covers of S, arranged so that if

$$\deg\{S_j \to S\} < \deg\{S_k \to S\}$$

then $j < k$. We let ω_j be the representation ρ in Lemma 3.6, corresponding to the surface S_j, and let σ_j be then the induced representation of ω_j given by the inclusion $\pi_1(S_j) < \pi_1(S)$. We then set

$$\rho_i = \prod_{j \leq i} \sigma_j.$$

It is clear from the construction that for each i, the representation ρ_i is finite dimensional, and of a dimension which is a computable function of i.

The following is straightforward, but we record it for completeness:

Lemma 5.1. *Let G be a finitely generated group, and let $\nu_G(n)$ be the number of finite index subgroups of index at most n. Then ν_G is a computable function of n.*

Proof of Theorem 1.1. We will assume that, applying Lemma 3.5 and replacing γ by a word of comparable or shorter length if necessary, that γ is not a proper power.

Note that if γ is a simple element of S then $\rho_i(\gamma)$ will have finite order for each i, by Lemma 3.7. Note furthermore that the order of $\rho_i(\gamma)$ depends only on i and not on γ.

If the geodesic representative for γ has exactly one self–intersection then γ is a figure eight loop. We then have that $\rho_1(\gamma)$ has infinite order. If γ has more than one self–intersection then it suffices to show that γ can be lifted to a figure eight loop on a cover $S' \to S$, where the degree of this cover is a computable function of $\ell_X(\gamma)$, by Lemma 5.1.

Let $\gamma \in \pi_1(S)$, let $\ell_X(\gamma)$ be its length as a word in the generating set X, and let ℓ_γ be the length of the geodesic representative of γ. We will abuse notation and write γ for the geodesic representative. By Lemma 3.4, we have that γ has at most $C \cdot (\ell_X(\gamma))^2$ self–intersections.

Since now γ has at least two self–intersections by assumption, we think of a regular neighborhood of γ as an immersion $f\colon P \to S$ of a geodesic pair of pants which is not an embedding. By Lemma 4.3, we have that the sum of the lengths of the boundary curves of P is at most $3\ell_\gamma$.

Since f is not an embedding, there is an essential closed curve $\gamma' \subset f(P)$ which does not lie in $f_*(\pi_1(P))$, by Lemma 4.5. Moreover, we may assume that the geodesic representative for γ' has length at most $3\ell_\gamma$. We can thus apply Theorem 3.2 to get control over the index of a finite cover of $S' \to S$ to which γ' does not lift. Observe that any lift of γ to S' has smaller self–intersection number than $\gamma \subset S$, but the geodesic length of the lift is unchanged. Therefore, we may repeatedly apply Theorem 3.2 until γ becomes a figure eight loop. We thus obtain a cover

$S' \to S$ and a lift of γ to a figure eight loop on S', where the degree of $S' \to S$ is a computable function of $\ell_X(\gamma)$. This completes the proof. □

Proof of Corollary 1.3. Let $1 \neq \gamma \in \pi_1(S)$ be given as a word in X. We use Lemma 3.5 to replace γ by a word which is not a proper power, if necessary. We apply the finitely many representations $\{\rho_1, \ldots, \rho_{f(\ell_X(\gamma))}\}$ to γ, where f is the computable function furnished by Theorem 1.1. It is computable whether or not $\rho_i(\gamma)$ has finite order for each of these representations. Theorem 1.1 implies that if γ is not a simple element of $\pi_1(S)$ then $\rho_i(\gamma)$ will have infinite order for some $i \leq f(\ell_X(\gamma))$. If $\rho_i(\gamma)$ has finite order for each $i \leq f(\ell_X(\gamma))$ then γ is a simple element of $\pi_1(S)$. □

6. Theoretical complexity estimates

In this short section, we estimate an upper bound on the theoretical complexity of the algorithm given by Corollary 1.3.

Corollary 6.1. *The complexity of the algorithm given by Corollary 1.3 is super-exponential.*

We will not give a detailed proof of Corollary 6.1, and instead we will note complexity estimates for each step of the algorithm. We start with a finite generating set X for $\pi_1(S)$ and $\gamma \in \pi_1(S)$ with $\ell_X(\gamma) = N$. We argued in Lemma 3.5 that deciding if γ is a proper power has at most exponential complexity, so that we will assume from the beginning that γ is not a proper power.

(1) The geodesic representative for γ (also called γ) has length $O(N)$.
(2) The bound on the number of self–intersections of γ is $O(N^2)$.
(3) To lift γ to a figure eight loop, we need to resolve $O(N^2)$ loops of length $O(N)$.
(4) A loop of length $O(N)$ can be resolved on a cover of degree $O(e^N)$ by Theorem 3.2.
(5) A bound on the degree of a cover which resolves $O(N^2)$ loops of length $O(N)$ is $O(e^{N^3})$.
(6) The number of subgroups of index k in $\pi_1(S)$ grows faster than $k!$.

Thus, we see that the most straightforward implementation of the algorithm requires, for γ of length N, a number of computations which is super-exponential in N. In practice, many of the steps above can be made more efficient, so that the "practical" complexity of this algorithm may be somewhat better.

7. Remarks on the AMU Conjecture for surface groups

In this short section, we explain the motivation behind the work in this paper. The starting point is to use certain representations of surface groups under which figure eight loops have infinite order, and under which simple loops have finite order. In order to prove the results of this paper, we only need the existence of one such representation. However, each representation used here is part of an infinite sequence of representations

$$\rho_p : \pi_1(S) \to \mathrm{PGL}_{d_p}(\mathbb{C})$$

indexed by odd integers p, as considered in [15]. For the present algorithm, we only need the following : if γ is geodesic figure eight loop, then $\rho_p(\gamma)$ has infinite order for p big enough (cf. Lemma 3.6). In general, it is expected that any non–simple element of $\pi_1(S)$ which is not a proper power will have infinite order under ρ_p for all but finitely many values of p. More precisely :

Conjecture 7.1 (AMU Conjecture for surface groups)**.** *If $1 \neq \gamma \in \pi_1(S)$ is a non–simple element which is not a proper power then $\rho_p(\gamma)$ has infinite order for $p \gg 0$.*

This conjecture is implied by the AMU Conjecture as stated by Andersen, Masbaum, and Ueno [1]. We will briefly explain how this works.

Let $x_0 \in S$ be a fixed marked point and let $\mathrm{Mod}^1(S)$ be the mapping class group of S fixing the marked point x_0. The Witten–Reshetikhin–Turaev SO(3) topological quantum field theory gives a representation

$$\tilde{\rho}_p : \mathrm{Mod}^1(S) \to \mathrm{PGL}_{d_p}(\mathbb{C})$$

for each odd integer $p \geq 3$. Using the Birman exact sequence, we can view $\pi_1(S)$ as a subgroup of $\mathrm{Mod}^1(S)$. This allows us to define a representation ρ_p by restricting $\tilde{\rho}_p$ to $\pi_1(S)$. The AMU conjecture as stated in [1] reads as follows:

Conjecture 7.2. *If $\phi \in \mathrm{Mod}^1(S)$ has a pseudo-Anosov piece then $\tilde{\rho}_p(\phi)$ has infinite order for $p \gg 0$.*

To see how Conjecture 7.2 implies Conjecture 7.1, we use a result of Kra (see Theorem 1.1 of [14]): if $1 \neq \gamma \in \pi_1(S)$ is non–simple and not a proper power then the corresponding mapping class in $\mathrm{Mod}^1(S)$ is pseudo-Anosov on the subsurface of S filled by γ. It is now clear that Conjecture 7.2 implies Conjecture 7.1.

References

[1] J.E. Andersen, G. Masbaum, K. Ueno. Topological quantum field theory and the Nielsen-Thurston classification of M(0, 4). *Math. Proc. Cam. Phil. Soc.* 141(2006) 447–488.

[2] C. Arettines. A combinatorial algorithm for visualizing representatives with minimal self-intersection. *J. Knot Theory Ramifications* 24 (2015), no. 11, in press.

[3] J. Birman and C. Series. An algorithm for simple curves on surfaces. *J. London Math. Soc.* (2) 29 (1984), no. 2, 331–342.

[4] P. Cahn. A generalization of the Turaev cobracket and the minimal self-intersection number of a curve on a surface. *New York J. Math.* 19 (2013), 253–283.

[5] M. Chas and F. Krongold. An algebraic characterization of simple closed curves on surfaces with boundary. *J. Topol. Anal.* 2 (2010), no. 3, 395–417.

[6] M. Chas and F. Krongold. Algebraic characterization of simple closed curves via Turaev's cobracket. *J. Topology* (2015), in press.

[7] M. Chas and A. Phillips. Self-intersection numbers of curves on the punctured torus. *Experiment. Math.* 19 (2010), no. 2, 129–148.

[8] M. Chas and A. Phillips. Self-intersection numbers of curves in the doubly punctured plane. *Exp. Math.* 21 (2012), no. 1, 26–37.

[9] M. Cohen and M. Lustig. Paths of geodesics and geometric intersection numbers. I. *Combinatorial Group Theory and Topology*, Alta, Utah, 1984. Ann. of Math. Studies 111, *Princeton University Press, Princeton, NJ*, (1987), 479–500.

[10] D. Chillingworth. Winding numbers on surfaces. I. *Math. Ann.* 196 (1972), 218–249.

[11] D. Chillingworth. Winding numbers on surfaces. II. *Math. Ann.* 199 (1972), 131–153.

[12] W. Goldman. The symplectic nature of fundamental groups of surfaces. *Adv. in Math.* 54 (1984), no. 2, 200–225.

[13] J. Hass and P. Scott. Intersections of curves on surfaces. *Israel J. Math.* 51 (1985), no. 1–2, 90–120.

[14] I. Kra. On the Nielsen-Thurston-Bers type of some self maps of Riemann surfaces. *Acta Math.* 134(3-4):231-270,(1981).

[15] T. Koberda and R. Santharoubane. Quotients of surface groups and homology of finite covers via quantum representations. *Invent. Math.*, in press.

[16] J. Malestein and A. Putman. On the self-intersections of curves deep in the lower central series of a surface group. *Geom. Dedicata* 149 (2010), 73–84.

[17] P. Patel. On a theorem of Peter Scott. *Proc. Amer. Math. Soc.* 142 (2014), no. 8, 2891–2906.

[18] P. Scott. Subgroups of surface groups are almost geometric. *J. London Math. Soc.* (2) 17 (1978), no. 3, 555–565.

[19] V. Turaev. Algebras of loops on surfaces, algebras of knots, and quantization. *Braid group, knot theory and statistical mechanics*, 59–95, Adv. Ser. Math. Phys., 9, *World Sci. Publ., Teaneck, NJ*, 1989.

[20] V. Turaev and O. Viro. Intersection of loops in two–dimensional manifolds. II. Free loops. *Mat. Sbornik* 121(163) (1983), no. 3, 359–369.

[21] H. Zieschang. Algorithmen für einfache Kurven auf Flächen. *Math. Scand.* 17 (1965), 17–40.

[22] H. Zieschang. Algorithmen für einfache Kurven auf Flächen. II. *Math. Scand.* 25 (1969), 49–58.

Department of Mathematics, University of Virginia, Charlottesville, VA 22904-4137, USA
E-mail address: `thomas.koberda@gmail.com`

Institut de Mathématiques de Jussieu (UMR 7586 du CNRS), Equipe Topologie et Géométrie Algébriques, Case 247, 4 pl. Jussieu, 75252 Paris Cedex 5, France
E-mail address: `ramanujan.santharoubane@imj-prg.fr`