PROFINITE COMPLETIONS OF BURNSIDE-TYPE QUOTIENTS OF SURFACE GROUPS

LOUIS FUNAR AND PIERRE LOCHAK

Abstract. We prove that profinite completions of Burnside-type surface group quotients are not virtually prosolvable, in general.

2000 MSC Classification: 57 M 07, 20 F 36, 20 G 20, 22 E 40.
Keywords: Mapping class group, Burnside group, quantum representation, discrete subgroup of semi-simple Lie groups.

1. Introduction and statements

Let π_g denotes the fundamental group $\pi_1(S_g, p)$ of a closed orientable surface S_g of genus g, based at a point $p \in S_g$. Recall that π_g is a one-relator group with the presentation:

$$\pi_g = \langle a_1, a_2, \ldots, a_g, b_1, b_2, \ldots, b_g | \ [a_1, b_1] \cdots [a_2, b_2] \cdots [a_g, b_g] = 1 \rangle$$

Here the classes a_i, b_i are represented by non-separating simple closed loops on S_g based at p.

We denote by Γ_g the mapping class groups of S_g. Further Γ_g^1 denotes the mapping class group of the pair (S_g, p), namely the group of isotopy classes of orientation preserving homeomorphisms of S_g fixing p. It is well-known that Γ_g^1 is isomorphic to the mapping class group of the punctured surface $S_g - \{p\}$. Nielsen proved that the map associating to $\varphi \in \Gamma_g^1$ the automorphism $\varphi_* : \pi_1(S_g, p) \to \pi_1(S_g, p)$ provides an isomorphism between Γ_g^1 and $\mathrm{Aut}^+(\pi_g)$. This map induces an isomorphism $\Gamma_g \to \mathrm{Out}^+(\pi_g)$ according to the commutative diagram, by identifying the two exact sequences below:

$$\begin{array}{ccccccccc}
1 & \to & \pi_g & \to & \Gamma_g^1 & \to & \Gamma_g & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & \pi_g & \to & \mathrm{Aut}^+(\pi_g) & \to & \mathrm{Out}^+(\pi_g) & \to & 1
\end{array}$$

If $M \subset \pi_g$ we denote by $M[n]$ the normal subgroup of π_g generated by $\varphi_*(x^n)$, for all $x \in M$ and $\varphi_* \in \mathrm{Aut}^+(\pi_g)$. Note that $M[n]$ is the characteristic subgroup generated by the subset M^n of n-th powers of elements in M.

The *Burnside-type group* $B(\pi_g, n, M)$ is the quotient $\pi_g/M[n]$. Several choices for M are particularly interesting. An element $x \in \pi_g$ is primitive if it can be represented by a non-separating simple closed curve on S_g. This is equivalent to saying (see [35]) that $x \in \pi_g$ can be mapped into one generator, say a_1, by some automorphism $\varphi_* \in \mathrm{Aut}^+(\pi_g)$, where $a_1, \ldots, a_g, b_1, \ldots, b_g$ are the generators from the standard presentation above.

The set of primitive classes of π_g is then contained in the set $\mathcal{S}(S_g)$ of homotopy classes of simple closed curves on S_g. More generally, we set $\mathcal{S}_n(S_g)$ for the set of homotopy classes of closed curves on S_g with at most n self-intersections.

We denote by $\widehat{G}$ the profinite completion of a group G. We are concerned in this paper with how large the profinite completion of $B(\pi_g, n, M)$ could be. Our main result is:

Theorem 1.1. *Let $g \geq 2$ and $p \equiv 3 (\mathrm{mod}\ 4)$ a large enough prime. Then for every m there exists some d such that the group $\widehat{B(\pi_g, dp, M)}$ is not virtually prosolvable, if $M \subset \mathcal{S}_m(S_g)$. When $m = 1$ then $d = 1$.*

Remark 1.1. The main result also holds for large enough primes $p \equiv 1 (\mathrm{mod}\ 4)$, according to Remark 2.1. An explicit p_0 such that the claim holds for all $p \geq p_0$ can be obtained from effective bounds in Lemma 3.8. Moreover, the claim holds for all primes $p < 10^4$, by a computer check of Lemma 3.8.

Date: February 25, 2017.

The proof shows that under these assumptions $\widehat{B(\pi_g, dp, M)}$ is neither solvable-by-finite nor finite-by-solvable.

Zelmanov [35] considered the group $\widehat{\pi_g}/\langle M[n]\rangle$, where $\langle M^n\rangle$ is the closure in $\widehat{\pi_g}$ of the normal subgroup of $\widehat{\pi_g}$ generated by M^n. Problem 2 from [35] asked whether this group is solvable-by-finite, when M denotes the set of primitive elements of π_g. The result above shows that this is not the case, in general:

Corollary 1.2. *Let $g \geq 2$ and $p \equiv 3 (\mathrm{mod}\ 4)$, a large enough prime. The group $\widehat{\pi_g}/\langle M[n]\rangle$, where $M = \mathcal{S}(S_g)$ contains the set of primitive elements of π_g, is not virtually solvable.*

Proof. The surjective map $\pi_g \to B(\pi_g, p, M)$ induces a surjective continuous homomorphism between the corresponding profinite completions $\widehat{\pi_g} \to \widehat{B(\pi_g, p, M)}$. The kernel of the last map contains $M[n]$ and hence the closure $\langle M^n\rangle$ of the normal subgroup of $\widehat{\pi_g}$ generated by M^n. Therefore we have a surjective continuous map $\widehat{\pi_g}/\langle M[n]\rangle \to \widehat{B(\pi_g, p, M)}$. $\square$

The proof of the main theorem goes as follows. We consider the so-called quantum representations of the mapping class groups Γ_g and Γ_g^1 depending on some root of unity of order $2p$. It was proved in [8] that these representations have infinite image, for $p \geq 5$. The proof was simplified in [20] where explicit elements of infinite order were found. Further, in [18] the authors showed that the images of Γ_g are topologically dense in the corresponding special unitary groups, when $p \geq 5$ is prime. On the other hand the matrices in the images have coefficients in a cyclotomic ring (see [13]). Eventually the restriction of scalars provides Zariski dense discrete representations in semi-simple linear algebraic groups defined over $\mathbb{Q}$ whose images are contained in arithmetic groups of higher rank (see [13]). The aim of [9] and [21] was to construct quotients of Γ_g which are simple finite groups of Lie type of arbitrary large rank.

Our strategy here is to consider the restriction of the quantum representations from Γ_g^1 to the subgroup π_g. These representations were already studied by Koberda and Santharoubane in [16], where it is proved that they still have infinite images, while they factor through the Burnside-type group $B(\pi_g, p, \mathcal{S}(S_g))$. Our aim is to show that the restriction of scalars provides Zariski dense discrete representations of $B(\pi_g, p, \mathcal{S}(S_g))$ in semi-simple linear algebraic groups defined over $\mathbb{Q}$ of higher rank whose images are contained in arithmetic subgroups. The Nori-Weisfeiler approximation theorem (see [23, 34]) then provides many finite quotients of congruence type. This implies that our profinite Burnside-type groups surjects onto an infinite product of simple non-abelian groups, proving our theorem.

Acknowledgements. The authors are indebted to S. Checcoli, P. Eyssidieux, T.Koberda and B. Remy for useful discussions.

2. Preliminaries on quantum mapping class group representations

2.1. The setting of the skein TQFT.

A TQFT is a functor from the category of surfaces into the category of finite dimensional vector spaces. Specifically, the objects of the first category are closed oriented surfaces endowed with colored banded points and morphisms between two objects are cobordisms decorated by uni-trivalent ribbon graphs compatible with the banded points. A banded point on a surface is a point with a tangent vector at that point, or equivalently a germ of an oriented interval embedded in the surface. There is a corresponding surface with colored boundary obtained by deleting a small neighborhood of the banded points and letting the boundary circles inherit the colors of the respective points.

We will use the TQFT functor $\mathcal{V}_p$, for $p \geq 3$ and a primitive root of unity A of order $2p$, as defined in [1]. The vector space associated by the functor $\mathcal{V}_p$ to a surface is called the *space of conformal blocks*. Let S_g denote the genus g closed orientable surface, H_g be a genus g handlebody with $\partial H_g = \Sigma_g$. Assume given a finite set $\mathcal{Y}$ of banded points on S_g. Let G be a uni-trivalent ribbon graph embedded in H_g in such a way that H_g retracts onto G, its univalent vertices are the banded points $\mathcal{Y}$ and it has no other intersections with S_g.

We fix a natural odd number $p \geq 3$, called the *level* of the TQFT. We define the *set of colors* in level p to be $\mathcal{C}_p = \{0, 2, 4, \ldots, p-3\}$.

An edge coloring of G is called *p-admissible* if the triangle inequality is satisfied at any trivalent vertex of G and the sum of the three colors around a vertex is bounded by $2(p-2)$.

Fix a coloring of the banded points $\mathcal{Y}$. Then there exists a basis of the space of conformal blocks associated to the surface $(\Sigma_g, \mathcal{Y})$ with the colored banded points (or the corresponding surface with colored boundary) which is indexed by the set of all p-admissible colorings of G extending the boundary coloring. We denote by $W_{g,(i_1,i_2,\ldots,i_r)}$ the vector space associated to the closed surface Σ_g with r banded points colored by $i_1, i_2, \ldots, i_r \in \mathcal{C}_p$. Note that banded points colored by 0 do not contribute.

Observe that an admissible p-coloring of G provides an element of the skein module $S_\zeta(H_g)$ of the handlebody with banded boundary points colored $(i_1, i_2, \ldots, i_r)$, evaluated at a primitive $2p$-th root of unity A. This skein element is obtained by cabling the edges of G by the Jones-Wenzl idempotents prescribed by the coloring and having banded points colors fixed. Let $\overline{H}_g$ denote the complementary handlebody in the 3-sphere S^3. There is then a sesquilinear form:

$$\langle\ ,\ \rangle : S_A(H_g) \times S_A(\overline{H}_g) \to \mathbb{C}$$

defined by

$$\langle x, y\rangle = \langle x \sqcup y\rangle.$$

Here $x \sqcup y$ is the element of $S_A(S^3)$ obtained by the disjoint union of x and y in $H_g \cup \overline{H}_g = S^3$, and $\langle\ \rangle : S_A(S^3) \to \mathbb{C}$ is the Kauffman bracket invariant.

Eventually the space of conformal blocks $W_{g,(i_1,i_2,\ldots,i_r)}$ is the quotient $S_A/\ker\langle\ ,\ \rangle$ by the left kernel of the sesquilinear form above. It follows that $W_{g,(i_1,i_2,\ldots,i_r)}$ is endowed with an induced *Hermitian form* H_A.

The projections of skein elements associated to the p-admissible colorings of a trivalent graph G as above form an orthogonal basis of $W_{g,(i_1,i_2,\ldots,i_r)}$ with respect to H_ζ. It is known ([1]) that H_A only depends on the p-th root of unity $\zeta_p = A^2$ and that in this orthogonal basis the diagonal entries belong to the totally real maximal subfield $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$.

Let $G' \subset G$ be a uni-trivalent subgraph whose degree one vertices are colored, corresponding to a sub-surface Σ' of Σ_g with colored boundary. The projections in W_g of skein elements associated to the p-admissible colorings of G' form an orthogonal basis of the space of conformal blocks associated to the surface Σ' with colored boundary components.

There is a geometric action of the mapping class groups of the handlebodies H_g and $\overline{H}_g$ respectively on their skein modules and hence on the space of conformal blocks. Moreover, these actions extend to a projective action $\rho_{p,A}$ of Γ_g^r on $W_{g,(i_1,i_2,\ldots,i_r)}$ respecting the Hermitian form $H_{\zeta_p} = H_A$. Notice that the mapping class group of an essential (i.e. without annuli or disks complements) sub-surface $\Sigma' \subset \Sigma_g$ is a subgroup of Γ_g which preserves the subspace of conformal blocs associated to Σ' with colored boundary. It is worthy to note that again $\rho_{p,A}$ only depends on $\zeta_p = A^2$, so we can unambigously shift the notation for this representation to ρ_{p,ζ_p}.

There is a central extension $\widetilde{\Gamma_g}$ of Γ_g by $\mathbb{Z}$ and a linear representation $\widetilde{\rho}_{p,\zeta_p}$ on W_g which resolves the projective ambiguity of ρ_{p,ζ_p}. The largest such central extension has class 12 times the Euler class (see [12, 22]), but the central extension considered in this paper is an index 12 subgroup of it, called $\widetilde{\Gamma}_1$ in [22]. When $g \geq 3$ it is a perfect group which therefore coincides with the universal central extension.

We denote by $S_{g,n}^r$ the compact orientable surface of genus g with n boundary components and r marked points. Then $\Gamma_{g,n}^r$ denotes the pure mapping class group of $S_{g,n}^r$ which fixes pointwise boundary components and marked points.

Let $\widetilde{\Gamma_g^r}$ be the pull-back of the central extension $\widetilde{\Gamma_g}$ to the subgroup $\Gamma_{g,r} \subset \Gamma_g$. Then $\widetilde{\Gamma_{g,r}}$ is also a central extension, which we denote $\widetilde{\Gamma_g^r}$ of Γ_g^r by $\mathbb{Z}^{r+1}$. From [12, 22] we derive $\widetilde{\Gamma_g^r}$ is perfect, when $g \geq 3$ and of order 10, when $g = 2$.

Definition 2.1. *Let $p \in \mathbb{Z}_+$, $p \geq 3$ and ζ_p be a primitive p-th root of unity. We denote by $\widetilde{\rho}_{p,(i_1,i_2,\ldots,i_r),\zeta_p}$ the linear representation of the central extension $\widetilde{\Gamma_g^r}$ which acts on the vector space $W_{g,p,(i_1,i_2,\ldots,i_r)}$ associated by the TQFT to the surface with the corresponding colored banded points (see* [12, 22]*).*

The functor $\mathcal{V}_p$ associates to a handlebody H_g the projection of the skein element corresponding to the trivial coloring of the trivalent graph G by 0. The invariant associated to a closed 3-manifold is given by pairing the two vectors associated to handlebodies in a Heegaard decomposition of some genus g and taking into account the twisting by the gluing mapping class action on W_g.

One should notice that the skein TQFT $\mathcal{V}_p$ is unitary, in the sense that H_{ζ_p} is a positive definite Hermitian form when $\zeta_p = (-1)^p \exp\left(\frac{2\pi i}{p}\right)$, corresponding to $A_p = (-1)^{\frac{p-1}{2}} \exp\left(\frac{(p+1)\pi i}{2p}\right)$. Note that for a general primitive p-th root of unity, the isometries of H_ζ form a pseudo-unitary group.

Now, the image $\rho_{p,g}(T_\gamma)$ of a right hand Dehn twist T_γ in a convenient basis given by a trivalent graph is easy to describe. Assume that the simple curve γ is the boundary of a small disk intersecting once transversely an edge e of the graph G. Consider $v \in W_g$ be a vector of the basis given by colorings of the graph G and assume that edge e is labeled by the color $c(e) \in \mathcal{C}_p$. Then the action of the lift $\widetilde{T_\gamma}$ of the Dehn twist T_γ in $\widetilde{\Gamma_g}$ is given by (see [1], 5.8) :

$$\widetilde{\rho}_{g,p}(\widetilde{T_\gamma})v = (-1)^{c(e)}\zeta^{c(e)(c(e)+2)}v$$

2.2. **Unitary groups of spaces of conformal blocks.** For a prime $p \geq 5$ we denote by $\mathcal{O}_p$ the ring of cyclotomic integers $\mathcal{O}_p = \mathbb{Z}[\zeta_p]$, if $p \equiv 3(\text{mod}4)$ and $\mathcal{O}_p = \mathbb{Z}[\zeta_{4p}]$, if $p \equiv 1(\text{mod}4)$ respectively, where ζ_r denotes a primitive r-th root of unity (the subscript r will sometimes be omitted). The main result of [13] states that there exists a free $\mathcal{O}_p$-lattice $\Lambda_{g,p}$ in the $\mathbb{C}$-vector space of conformal blocks associated by the TQFT $\mathcal{V}_p$ to the genus g closed orientable surface and a non-degenerate Hermitian $\mathcal{O}_p$-valued form on $\Lambda_{g,p}$ both invariant under the action of $\widetilde{\Gamma_g}$ via the representation $\widetilde{\rho}_{p,\zeta}$. Therefore the image of the mapping class group consists of unitary matrices (with respect to the Hermitian form) with entries in $\mathcal{O}_p$. Let $\mathbb{U}_{g,p,\zeta}(\mathcal{O}_p)$ and $P\mathbb{U}_{g,p,\zeta}(\mathcal{O}_p)$ be the group of all such matrices and respectively its quotient by scalars.

When p is prime $p \geq 5$ and $g \geq 2$, $(g,p) \neq 5$, then $\widetilde{\rho}_{p,\zeta_p}$ takes values in the special unitary group $S\mathbb{U}_{g,p,\zeta_p}$ (see [3, 10]). It is known that $S\mathbb{U}_{g,p,\zeta}(\mathcal{O}_p)$ is an irreducible lattice in a semi-simple algebraic group $\mathbb{G}_{g,p}$ obtained by the so-called restriction of scalars construction from the totally real cyclotomic field $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$ to $\mathbb{Q}$. Specifically, the group $\mathbb{G}_{g,p}$ is a product $\prod_{\sigma \in S(p)} S\mathbb{U}_{g,p,\sigma(\zeta)}$. Here $S(p)$ stands for a set of representatives of the classes of complex embeddings σ of $\mathcal{O}_p$ modulo complex conjugacy. The factor $S\mathbb{U}_{g,p,\sigma(\zeta)}$ is the special unitary group associated to the Hermitian form conjugated by σ, thus corresponding to some Galois conjugate root of unity.

Denote by $\widetilde{\rho}_p$ and ρ_p the representations $\prod_{\sigma \in S(p)} \widetilde{\rho}_{p,\sigma(A_p^2)}$ and $\prod_{\sigma \in S(p)} \rho_{p,\sigma(A_p^2)}$, respectively. Notice that the real Lie group $\mathbb{G}_{g,p}$ is a semi-simple algebraic group defined over $\mathbb{Q}$.

In [9] it is proved that $\widetilde{\rho}_p(\widetilde{\Gamma_g})$ is a discrete Zariski dense subgroup of $\mathbb{G}_{g,p}(\mathbb{R})$ whose projections onto the simple factors of $\mathbb{G}_{g,p}(\mathbb{R})$ are topologically dense, for $g \geq 3$ and $p \geq 7$ prime, $p \equiv -1(\text{mod } 4)$.

Remark 2.1. When $p \equiv 1(\text{mod } 4)$ the image of the central extension of Γ_g from [22] by $\widetilde{\rho}_p$ is contained in $\mathbb{G}_{g,p}(\mathbb{Z}[i])$ and thus it is a discrete Zariski dense subgroup of $\mathbb{G}_{g,p}(\mathbb{C})$. However, if we restrict to the universal central extension $\widetilde{\Gamma_g}$ coefficients are reduced from $\mathbb{Z}[\zeta_{4p}]$ to $\mathbb{Z}[\zeta_p]$ (see [13], section 13). Note that the corresponding invariant form H_{ζ_p} should be suitably rescaled and after rescaling it will be skew-Hermitian when g is odd and Hermitain for even g.

As mentioned in ([21], Rem.3.5) for the proof of our main result we don't need the integral TQFT of [13] as the Burnside-type groups are finitely generated and hence only finitely primes could appear in the denominators of matrices in their image.

3. Quantum surface group representations

3.1. **Zariski density of quantum representations.** Our aim is to find the Zariski closures of $\rho_{p,(i)}(\pi_g)$. We follow closely the strategy from [9], where we proved that $\rho_{p,(i)}(\Gamma_g)$ is Zariski dense in $P\mathbb{G}_p(\mathbb{R})$.

The mapping class group $\Gamma_{g,1}$ is a subgroup of Γ_{g+1}, by identifying S_{g+1} with the result of gluing of $S_{g,1}$ and $S_{1,1}$. It is well-known that

$$W_{g+1,p} = \bigoplus_i W_{g,p,(i)} \otimes W_{1,p,(i)}$$

The decomposition corresponds to the eigenspaces for the Dehn twist $\widetilde{T_c}$ along the curve $c = \partial S_{g,1}$. Let $\mathbb{U}_{g,p,\zeta,(i)} = U(W_{g,p,(i)}, H_\zeta)$ be the unitary subgroup keeping invariant the subspace $W_{g,p,(i)}$, when endowed with the (restriction of the) Hermitian form H_ζ. The group $\mathbb{U}_{g,p,\zeta,(i)}$ is a closed linear algebraic subgroup of $\mathbb{U}_{g+1,p,\zeta}$ and it is also defined over the maximal totally real algebraic field $\mathbb{Q}(\zeta + \overline{\zeta})$ of $\mathbb{Q}(\zeta)$.

Since $\widetilde{\Gamma_g^1}$ is perfect when $g \geq 3$ and of order 10 for $g = 2$, it follows that $\widetilde{\rho}_{p,(i)}(\widetilde{\Gamma_g^1})$ is contained within the special unitary group $S\mathbb{U}_{g,p,\zeta,(i)}$, if $(g,p) \neq (2,5)$, as in [3, 10].

We denote by $\mathbb{G}_{g,p,(i)}$ the group obtained by scalar restriction from $\mathbb{Q}(\zeta+\zeta^{-1})$ to $\mathbb{Q}$ of the special linear algebraic group $S\mathbb{U}_{g,p,\zeta,(i)}$, namely the product $\mathbb{G}_{g,p,(i)} = \prod_{\sigma\in S(p)} S\mathbb{U}_{g,p,\sigma(\zeta),(i)}$. It follows that the product representation $\widetilde{\rho}_{p,(i)} = \prod_{\sigma\in S(p)} \widetilde{\rho}_{p,(i),\sigma(A_p^2)}$ of $\widetilde{\Gamma_g^1}$ takes values in $\mathbb{G}_{g,p,(i)}$. Since the boundary Dehn twist acts as a scalar this descends to a representation $\rho_{g,p,(i)} : \Gamma_g^1 \to P\mathbb{G}_{g,p,(i)}$.

Our main result in this section is:

Theorem 3.1. *Let $g \geq 3$ and $p \equiv 3 (\mathrm{mod}\ 4)$, p a large enough prime. Then the Zariski closure of $\widetilde{\rho}_{p,(p-3)}(\widetilde{\pi_g})$ is $\mathbb{G}_{g,p,(p-3)}(\mathbb{R})$. Moreover, if $g \geq 4$ every non-compact factor of $\mathbb{G}_{g,p,(p-3)}(\mathbb{R})$ has real rank at least 2.*

The key ingredient is the following proposition, whose rather technical proof is postponed to the next sections:

Proposition 3.1. *Let $g \geq 2$ and $p \equiv 3 (\mathrm{mod}\ 4)$, p a large enough prime. The representation $\widetilde{\rho}_{p,(p-3),\zeta}$ of $\widetilde{\Gamma_{g,1}}$ into $W_{g,p,(p-3)}$ has dense image in the special unitary group $S\mathbb{U}_{g,p,\zeta,(p-3)}$.*

Proposition 3.2. *Suppose that $\widetilde{\rho}_{p,(i),\zeta}(\widetilde{\Gamma_{g,1}})$ is Zariski dense in $S\mathbb{U}_{g,p,\zeta,(i)}$. Then $\widetilde{\rho}_{p,(i),\zeta}(\widetilde{\pi_g})$ is Zariski dense in the special unitary group $S\mathbb{U}_{g,p,\zeta,(i)}$.*

Proof of Proposition 3.2. As π_g is a normal subgroup of Γ_g^1, we derive that the topological closure of its image is a closed normal Lie subgroup of the projective unitary group $PSU(W_{g,p,(i)})$. Therefore the image of $\widetilde{\pi_g}$ is a closed normal subgroup of $SU(W_{g,p,(i)})$. Since the Lie algebra of $SU(W_{g,p,(i)})$ is simple it follows that the Lie group has dimension zero and hence it is a discrete subgroup. However a normal discrete subgroup of $SU(W_{g,p,(i)})$ must be contained in its center, which is cyclic of order $\dim W_{g,p,(i)}$.

Now, the result of [16] for $i = 2$ shows that the image of π_g by $\rho_{p,(i),\zeta}$ is infinite non-abelian. We claim that this holds true for all $i \neq 0$, in particular we give a detailed proof for $i = p - 3$.

The $k+1$-holed sphere $S_{0,k+1}$, whose boundary circles are colored by $\mathbf{c} = (a, a, \ldots, a, ak-2)$ has associated a space of conformal blocks $W_{0,\mathbf{c}}$ of dimension k which has a natural action of the braid group B_k on k strings. Note that $\Sigma_{0,k+1}$ can be embedded into $\Sigma_{g,1}$ such that the homomorphism $B_k \to \Gamma_{g,1}$ is injective, if $k \leq g$. It is well-known that this braid group action coincides with the Burau representation at a suitable root of unity (see [11]) twisted by a character. Specifically, the Burau representation is the one for which the standard braid generators have eigenvalues -1 and $A_p^{2a^2}$. Moreover, in [11] one proved that the image of the Burau representation of B_3 is infinite non-abelian if $A_p^{2a^2}$ is not a primitive root of unity of order $2, 3, 4$ or 5, while the image of B_4 is infinite non-abelian (see e.g. [8]) if $A_p^{2a^2}$ is not a primitive root of unity of order 2 or 3.

It suffices to consider $i \geq 4$. If we can write $i = ak - 2$, $3 \leq k \leq g$, $a \in \mathcal{C}_p$, the image of B_k is infinite. Further $\pi_1(S_{0,3}) \subset \pi_1(S_{0,k+1})$, if $k \geq 2$ and the restriction of the Burau representation to the pure braid group PB_3 is infinite non-abelian. But $PB_3 = \mathbb{F}_2 \times \mathbb{Z}$, where the factor $\mathbb{Z}$ is central and its image by the Burau representation is of finite order, while the free factor $\mathbb{F}_2$ can be identified with $\pi_1(S_{0,3})$. We derive that the image of $\pi_1(S_{g,1})$ by the subrepresentation of $\rho_{p,(i)}$ corresponding to the Burau representation contains the image of $\mathbb{F}_2$, namely a triangle group (see [11]).

Otherwise we consider the subsurface $\Sigma_{g-1,1} \subset \Sigma_{g,1}$ with boundary circle labeled by $2(g-2)$, which corresponds to $a = 2, k = g - 1$. If $g \geq 3$ then the image of $\pi_1(\Sigma_{g-1,1})$ by the quantum representation of Γ_{g-1}^1 on $W_{g-1,p,(2)}$ is infinite non-abelian by [16]. However the later is a subrepresentation of the representation of Γ_g^1 on $W_{g-1,p,(p-3)}$. Since $\pi_1(\Sigma_{g-1,1})$ is a subgroup of $\pi_1(\Sigma_{g,1})$ we derive that $\rho_{p,(i)}(\pi_1(\Sigma_g)$ is infinite non-abelian. Similar arguments work when $g = 2$; although the map $B_3 \to \Gamma_{2,1}$ is not injective, its restriction to a free subgroup generated by Dehn twists along curves with intersection 2 remains injective.

Alternatively, when $g = 2$ and $i = p - 3$ we consider the image of $\pi_1(\Sigma_{1,2})$ by the quantum representation of Γ_2^1, where $\Sigma_{1,2} \subset \Sigma_{2,1}$ is the complementary of a one holed torus with boundary label 2. Then $\Gamma_{1,2}$ acts on $W_{1,p,(2,p-3)}$ which has dimension 3 and an explicit calculation shows that the image of $\pi_1(\Sigma_{1,2})$ is infinite non-abelian. □

Let now $\Gamma \to H_i$, $i = 1, \dots, m$, be a collection of representations of the group Γ. The subgroup $H \subset \prod_{i=1}^m H_i$ is called Γ-diagonal, if there exists a partition $A_1, \dots, A_s$ of $\{1, 2, \dots, m\}$ such that:

(1) All factors H_i, with $i \in A_t$, $1 \le t \le s$ are equivalent as representations of Γ. Pick up some $i_t \in A_t$. Given some intertwining isomorphisms $L_{j,i_t} : H_j \to H_{i_t}$, $j \in A_t \setminus \{i_t\}$, we set:
$$H_{A_t} = \{(x, (L_{j,i_t}(x))_{j\in A_t\setminus\{i_t\}}),\ \ x \in H_{i_t}\},$$
which is the graph of the homomorphism $\oplus_{j\in A_t\setminus\{i_t\}} L_{j,i_t}$.

(2) Then there exist intertwining isomorphisms as above with the property that the group H contains $\prod_{1\le t\le s} H_{A_t}$. In particular, if all representations H_i of Γ are pairwise inequivalent, then $H = \prod_{i=1}^m H_i$.

We then have the following Hall lemma from [17]:

Lemma 3.1 (Hall Lemma)**.** *Let Γ be a subgroup of the product $\prod_{i=1}^m H_i$ of the adjoint simple (i.e. connected, without center and whose Lie algebra is simple) Lie groups H_i. Assume that the projection of Γ on each factor H_i is Zariski dense. Then the Zariski closure of Γ in $\prod_{i=1}^m H_i$ is a Γ-diagonal subgroup.*

Lemma 3.2. *Let A and B be primitive $2p$-th roots of unity, p odd and $i \neq 0$. If $\widetilde{\rho}_{p,(p-3),A}|_{\widetilde{\pi_g}}$ and $\widetilde{\rho}_{p,(p-3),B}|_{\widetilde{\pi_g}}$ are linearly or anti-linearly equivalent, then either $A = B$ or $A = \overline{B}$.*

Proof. According to classical results of Dieudonné and Rickart (see [27]) two representations in the same unitary group $U(W)$ are equivalent if there exists an intertwiner map $V : W \to W$, either linear or anti-linear, which conjugates the two representations, possibly up to twisting by a character $\chi : U(W) \to U(1)$. In our case the representations take values into the special unitary group and hence χ is central and hence finite. It follows that we can take $\chi = 1$.

Observe that V should send eigenspaces for $\rho_{p,(i),A}(\gamma)$ to eigenspaces for $\widetilde{\rho}_{p,(i),B}(\gamma)$ of the same eigenvalues. If γ a simple non-separating based loop on the surface, let γ_+, γ_- denote the curves obtained by slightly pushing left and right respectively. Then γ_+, γ_- and a small circle around the base point determine a pair of pants $S_{0,3}$ whose complement $S_{g-1,2}$ is a genus $g-1$ surface with two boundary components. Therefore
$$\widetilde{\rho}_{p,(i),A}(\widetilde{\gamma})x = A^{j(j+2)-k(k+2)}x, \text{ if } x \in W_{0,(i,j,k)} \otimes W_{g-1,(j,k)}$$
where the lift $\widetilde{\gamma} \in \widetilde{\pi_g}$ is given by $\widetilde{T_{\gamma_+}}\widetilde{T_{\gamma_-}}^{-1} \in \widetilde{\Gamma_g^1}$.

It follows that V should send vector spaces of the form $W_{0,(i,j,k)} \otimes W_{g-1,(j,k)}$ into spaces of the same form associated to possibly different labels.

Consider $i = p - 3$. Therefore the only possibilities for j, k such that $\dim W_{0,(i,j,k)}$ be non-zero is $j = p - 3 - 2m, k = 2m$, for some $2m \in \mathcal{C}_p$. Now, the symmetry exchanging the two boundary components induces an isomorphism between $W_{g-1,(j,k)}$ and $W_{g-1,(k,j)}$. Further, consider a circle embedded in $S_{g-1,2}$ which bounds a pair of pants along with the two boundary circles. If ℓ is a label for the third circle then the set of p-admissible ℓ for boundary labels (j, k), where $j > k$ is strictly contained in the set of p-admissible values of ℓ for the boundary labels $(j - 2, k + 2)$. It follows that $\dim W_{g-1,(j,k)}$ are distinct for all values $j \ge k$, with $j + k = p - 3$.

Therefore either V keeps invariants the spaces $W_{0,(i,j,k)} \otimes W_{g-1,(j,k)}$ or else they send $W_{0,(i,j,k)} \otimes W_{g-1,(j,k)}$ onto $W_{0,(i,k,j)} \otimes W_{g-1,(k,j)}$. Since the corresponding eigenvalues should be the same we derive that either $A = B$ or $A = \overline{B}$. □

Therefore, the Hall lemma above shows that the Zariski closure of $\rho_p(\pi_g)$ is all of $\mathbb{PG}_{p,(i)}(\mathbb{R})$. Now using ([17], Lemma 3.6) we obtain that $\widetilde{\rho}_p(\widetilde{\pi_g})$ is Zariski dense in $\mathbb{G}_{p,(i)}(\mathbb{R})$.

Finally notice that $\mathbb{G}_{g,p,(i)}$ contains $\mathbb{G}_{g-1,p}$ as a subgroup. In particular, for $g \geq 5$ each non-compact factor has rank at least 2, by [10]. We can follow the proof of this result in [10] for $i = 0$ to obtain the result for $g = 4$ as well. This proves the theorem.

3.2. **Preliminaries on Verlinde formulas.** We start by collecting a few properties of the dimensions of the space of conformal blocks. The main tool is the combinatorial description of the space of conformal blocks which admit a basis indexed by the set of p-admissible colorings of any uni-trivalent graph associated to the surface, possibly with colored boundary components, as explained in 2.1. As a consequence, if we split a surface $S_{g,k}$ by cutting along r essential pairwise non isotopic simple curves into the subsurfaces $S_{h,s+r}$ and $S_{g-h-r+1,k-s+r}$ then we have a corresponding decomposition for the spaces of conformal blocks:

$$W_{g,p,(i_1,\ldots,i_k)} = \sum_{j_1,\ldots j_r \in \mathcal{C}_p} W_{h,p,(i_1,\ldots,i_s,j_1,\ldots,j_r)} \otimes W_{g-h-r+1,p,(i_{s+1},\ldots,i_s,j_1,\ldots,j_r)}$$

Lemma 3.3.

$$\dim W_{1,p,(j,i)} = \frac{(p-1-\max(i,j))(\min(i,j)+1)}{2}$$

Proof. Direct computation using the combinatorial description of the vector space. □

Lemma 3.4. *For $k \in \mathcal{C}_p$ we have:*

$$\dim W_{2,p(k)} = \frac{1}{24} \cdot ((k+1)p^3 - \frac{3}{2}k(k+2)p^2 + \frac{1}{2}(k^3 + 3k^2 - 4)p)$$

and, in particular,

$$\dim W_{2,p,(p-3)} = \frac{p^3 - p}{24}$$

Proof. We have

$$\dim W_{2,p(k)} = \sum_{j \in \mathcal{C}_p} \dim W_{1,p,(j)} \cdot \dim W_{1,p,(j,k)}$$

then expand all terms using Lemma 3.3. □

Lemma 3.5.

$$\dim W_{3,p,(p-3)} = \frac{1}{5760} \cdot p(p-1)(p-3)(7p^3 + 28p^2 + 101p + 80) + \frac{1}{24} \cdot (p^3 - p)$$

Proof. This is a consequence of Lemmas 3.3 and 3.4 along with

$$\dim W_{3,p,(p-3)} = \sum_{j \in \mathcal{C}_p} \dim W_{2,p,(j)} \cdot \dim W_{1,p,(j,p-3)}$$

□

Lemma 3.6. *We have* $\dim W_{g,p,(p-3)} > \dim W_{g,p,(0)}$*, if* $g \geq 3$*.*

Proof. We will prove by induction on g that $\dim W_{g,p,(k)} \geq \dim W_{g,p,(0)}$, for any $k \in \mathcal{C}_p$, with equality only if $k = 0$, $g \geq 3$ or $g = 2$ and $k = p - 3$.

When $g = 2$ the explicit formula from Lemma 3.4 allows for a direct verification. Assume that our claim holds true for all genera up to g. We can write from Lemma 3.3:

$$\dim W_{g+1,p,(k)} = \sum_{j \in \mathcal{C}_p} \dim W_{g,p,(j)} \cdot \frac{(p-1-\max(k,j))(\min(k,j)+1)}{2}$$

to be compared with

$$\dim W_{g+1,p,(0)} = \sum_{j \in \mathcal{C}_p} \dim W_{g,p,(0)} \cdot \frac{(p-1-j)}{2}$$

Now the induction hypothesis $\dim W_{g+1,p,(0)} \leq \dim W_{g,p,(j)}$ for all $j \in \mathcal{C}_p$ implies the claim for $g + 1$. □

Lemma 3.7. *For any $g \geq 3$, $p \geq 7$ we have*

$$\dim W_{g+1,p,(p-3)} < \frac{\dim W_{g,p,(p-3)}(\dim W_{g,(p-3)} - 1)}{2}$$

Further, for $g = 2$ we have the weaker inequality:

$$\dim W_{3,p,(p-3)} < (\dim W_{2,p,(p-3)})^2$$

Proof. Recall the Verlinde formula (see [14]) computing the dimension of the space of conformal blocks:

$$\dim W_{g,p,(k)} = \left(\frac{p}{4}\right)^{g-1} \sum_{s=1}^{\frac{p-1}{2}} \sin\left(\frac{(k+1)\pi s}{p}\right) \sin\left(\frac{\pi s}{p}\right)^{1-2g}$$

Set $\alpha_s = \left(\frac{p}{4}\right) \sin\left(\frac{\pi s}{p}\right)$. If $g \geq 4$ we have the following inequalities:

$$\sum_s \alpha_s^g \leq \sum_s \alpha_s^{4(g-1)/3} < (\sum_s \alpha_s)^{4/3}$$

which imply that:

$$\dim W_{g+1,p,(0)} < (\dim W_{g,p,(0)})^{4/3}, \text{ whenever } g \geq 4$$

We derive from Lemma 3.6 that whenever $g \geq 4$ we have:

$$\dim W_{g+1,p,(p-3)} < \dim W_{g+2,p,(0)} \leq (\dim W_{g+1,p,(0)})^{4/3} < (\dim W_{g,p,(0)})^{16/9} < (\dim W_{g,p,(p-3)})^{16/9}$$

On the other hand

$$(\dim W_{g,p,(p-3)})^{16/9} < \frac{\dim W_{g,p,(p-3)}(\dim W_{g,p,(p-3)} - 1)}{2}$$

if $g \geq 4$ and $p \geq 5$, since $\dim W_{g,p,(p-3)} \geq \dim W_{4,5,(2)} = 75$.

Eventually, we have to check the case when $g = 3$. From Lemma 3.4

$$\dim W_{2,p,(k)} < \frac{1}{24}\left((k+1)p^3 + \frac{k^3+3k^2}{2}p\right) < \frac{p^3(3p+5)}{48}$$

We have the following crude upper bound:

$$\sum_{j \in \mathcal{C}_p} \frac{(p-1-\max(k,j))(\min(k,j)+1)}{2} < \frac{1}{4}p^3$$

which leads to the upper bounds:

$$\dim W_{3,p,(k)} < \frac{p^3(3p+5)}{48} \sum_{j \in \mathcal{C}_p} \frac{(p-1-\max(k,j))(\min(k,j)+1)}{2} < \frac{p^6(3p+5)}{192}$$

and further

$$\dim W_{4,p,(k)} < \frac{p^6(3p+5)}{192} \sum_{j \in \mathcal{C}_p} \frac{(p-1-\max(k,j))(\min(k,j)+1)}{2} < \frac{p^9(3p+5)}{728}$$

Now, if $p > 35$ we have that

$$\dim W_{4,p,(p-3)} < \frac{p^9(3p+5)}{728} < \frac{7p^{12}}{32 \times (5760)^2} < \frac{\dim W_{3,p,(p-3)}(\dim W_{3,p,(p-3)} - 1)}{2}$$

The cases when $5 \leq p \leq 35$ can be verified by a direct computer search.

Finally, the inequality claimed for $g = 2$ is a consequence of Lemmas 3.4 and 3.5.

Note that the inequality for $g \geq 3$ is actually valid with the same proof for all labels i on the boundary circle. □

Remark 3.1. The inequality stated in Lemma 3.7 for $g \geq 3$ does not hold when $g = 2$. Indeed we have the following asymptotical behavior, derived from Lemma 3.5:

$$\frac{\dim W_{3,p,(p-3)}}{(\dim W_{2,p,(p-3)})^2} \simeq 0.7$$

Lemma 3.8. *There exist only finitely many p such that $1 + 8\dim W_{3,p,(p-3)}$ is a perfect square.*

Proof. The function $1 + 8\dim W_{3,p,(p-3)}$ is a degree 6 square free polynomial in p. The projective curve given by the affine equation $y^2 = f(x)$ is a hyperelliptic curve of genus 2. According to Faltings' solution of Mordell's conjecture this equation has only finitely many rational solutions (see [5]).

Alternatively, we can use a classical theorem of Siegel, which asserts that a polynomial with integer coefficients and at least 3 distinct roots takes only finitely many square values on the integers. Although $(24)^2(1 + 8\dim W_{3,p,(p-3)})$ has rational coefficients, by considering the change of variable $p = 5q + s$, for each $s \in \{0, 1, 2, 3, 4\}$ we obtain five polynomials with integer coefficients to each of which Siegel's theorem applies. □

3.3. **Proof of Proposition 3.1.** Larsen and Wang in [18] proved the topological density of the image of the mapping class group of a closed surface of genus g. This result corresponds to the case when $i = 0$ and $\zeta = A_p$. We will show that their proof suitably amended actually works for $i = p - 3$ and $g \geq 2$. Some of the steps below are valid for every color i, but for the sake of simplicity we stick to $i = p - 3$. In this section p is an odd prime, $p \geq 5$.

The start point is the irreducibility of $\widetilde{\rho}_{g,p,(i),\zeta}$, for any i, according to (the proof given by) Roberts ([28], see also [14], Cor. 3.2).

Consider the topological closure $\mathcal{G}_{g,p,(i)}$ of $\widetilde{\rho}_{p,(i),A_p}(\widetilde{\Gamma_{g,1}})$. We know, from [8], that when $g \geq 2$, $p \geq 7$ the group $\mathcal{G}_{g,p,(i)}$ is infinite and non-abelian. Denote by $V_{g,p,(i)}$ the representation of $\mathcal{G}_{g,p,(i)}$ into $U(W_{g,p,\zeta,(i)})$.

If the representation $V_{g,p,(i)}$ were self-dual, its restriction to $\widetilde{\Gamma_{g-1,1} \times \Gamma_{1,1}}$ would be a direct sum of self-dual and pairs of dual representations. The invariant subspace $W_{g-1,(0)} \otimes W_{1,(0,i)}$ is not self-dual (see [18], step 10), as $W_{g-1,(0)}$ is not self-dual. Moreover, it is not dual to $W_{g-1,(j)} \otimes W_{1,(j,i)}$, for any other values of j, since these subspaces are tensor products of irreducible representations and the corresponding dimensions of $W_{1,(j,i)}$ do not agree with that for $j = 0$ unless $j = 0$.

We wish now to prove our claim by induction on g. When $g = 2$ we choose $i = p - 3$. From above it follows that $\dim W_{2,p,(p-3)} = \frac{p^3-p}{24}$. Now the results from ([18], section 4) show that $\rho_{p,(p-3),A_p}(\Gamma_g^1)$ is topologically dense into $PSU(W_{2,p,(p-3)})$. We can show using the same lines that the result holds for large enough p, for any i. We skip the details, as it is will be not needed later.

Further it follows from [18] that:

(1) the restriction of $V_{g,p,(i)}$ to the identity component $\mathcal{G}^\circ_{g,p,(i)}$ of $\mathcal{G}_{g,p,(i)}$ is isotypic.
(2) For any normal subgroup $H \subset \mathcal{G}_{g,p,(i)}$ with the property that all homomorphisms $SL_2(\mathbb{Z}/p\mathbb{Z}) \to \mathcal{G}_{g,p,(i)}/H$ are trivial, the representation of H into $V_{g,p,(i)}$ is tensor indecomposable.
(3) Moreover, $V_{g,p,(i)}$ is irreducible as a $\mathcal{G}^\circ_{g,p,(i)}$-representation.

Further the content of Lemma 3.7 is the extension of ([18], Lemma 12) to the case of surfaces with boundary. This is the main condition needed to prove the induction step from g to $g + 1$. It actually works for all $g \geq 3$, except for $g = 2$.

When $g = 2$ we only obtain that $\mathcal{G}^\circ_{3,p,(p-3)}$ is a simple compact Lie group of type A_n and the representation $V_{3,p,(p-3)}$ is either the standard one or else the exterior or the symmetric square. In particular, if this representation were not the standard one, then $\dim W_{3,p,(p-3)}$ would be of the form $m(m + 1)/2$, for some natural number $m \in \{n, n + 1\}$. This situation could only occur for finitely many p, according to Lemma 3.8.

Eventually the arguments from ([18], step 14 and 15) show that the identity component $\mathcal{G}^\circ_{g,p,(p-3)}$ is a simple compact Lie group and for $g \geq 3, p \geq 7$ we have the equality $\mathcal{G}_{g,p,(p-3)} = SU(W_{g,p,(p-3)})$. Thus $\widetilde{\rho}_{p,(p-3),A_p}(\widetilde{\Gamma_{g,1}})$ is topologically dense into $SU(W_{g,p}(i))$. This implies that $\widetilde{\rho}_{p,(i),\zeta}(\widetilde{\Gamma^1_g})$ is Zariski dense into $S\mathbb{U}_{g,p,\zeta,(p-3)}$ for all primitive roots of unity ζ.

3.4. **Trace fields.** Recall that $S\mathbb{U}_{g,p,(i)}$ is an absolutely almost simple simply connected algebraic group defined over $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$ (i.e. its proper normal algebraic subgroups are finite). The adjoint trace field of a subgroup $\Delta \subset S\mathbb{U}_{g,p,(i)}$ is the field $\mathbb{Q}(\mathrm{tr}(Ad(x)), x \in \Lambda)$, where Ad is the adjoint representation of $S\mathbb{U}_{g,p,(i)}$. We have the following extension of the corresponding result for mapping class groups of closed surfaces from ([21], section 4.3):

Lemma 3.9. *Up to rescaling $\rho_{p,(p-3)}$ by some $2p$-th root of unity we can insure that the adjoint trace field of $\widetilde{\rho}_{p,(p-3)}(\widetilde{\pi_g})$ is $\mathbb{Q}(\zeta_p+\overline{\zeta_p})$.*

Proof. If ℓ denotes the adjoint trace field in the statement then $\ell \subset \mathbb{Q}(\zeta_p+\overline{\zeta_p})$. The Zariski density and classical theorems of Vinberg (see [21], Prop.4.2) show that $S\mathbb{U}_{g,p,(i)}$ is defined over ℓ and $Ad(\widetilde{\rho}_{p,(p-3)}(\widetilde{\pi_g}))$ is contained in the group $Ad(S\mathbb{U}_{g,p,(i)})(\ell)$ of ℓ points of the adjoint group $Ad(S\mathbb{U}_{g,p,(i)})$. If we show that $\widetilde{\rho}_{p,(p-3)}(\widetilde{\pi_g}))$ is contained in the group $S\mathbb{U}_{g,p,(i)}(\ell)$ then the argument of ([21], section 4.3) will imply that $\ell=\mathbb{Q}(\zeta_p+\overline{\zeta_p})$.

If Z is the center of $S\mathbb{U}_{g,p,(i)}$, then we have an exact sequence

$$Z(\mathbb{Q}(\zeta_p+\overline{\zeta_p}))\to S\mathbb{U}_{g,p,(i)}(\mathbb{Q}(\zeta_p+\overline{\zeta_p}))\to Ad(S\mathbb{U}_{g,p,(i)})(\mathbb{Q}(\zeta_p+\overline{\zeta_p}))$$

Let $\sigma\in Gal(\mathbb{Q}(\zeta_p+\overline{\zeta_p})/\ell)$. Then we have a homomorphism

$$f:\widetilde{\rho}_{p,(p-3)}(\widetilde{\pi_g})\to Z^1(Gal(\mathbb{Q}(\zeta_p+\overline{\zeta_p})/\ell), Z(\mathbb{Q}(\zeta_p+\overline{\zeta_p}))$$

$$f(\gamma)(\sigma)=\gamma\sigma(\gamma^{-1}),\ \text{for } \gamma\in\widetilde{\rho}_{p,(p-3)}(\widetilde{\pi_g}), \sigma\in Gal(\mathbb{Q}(\zeta_p+\overline{\zeta_p})/\ell)$$

The group of 1-cocycles Z^1 is an abelian group and hence f factors through the abelianization $H_1(\widetilde{\rho}_{p,(p-3)}(\widetilde{\pi_g})$ which is a quotients of $(\mathbb{Z}/p\mathbb{Z})^{2g}$. On the other hand the group cohomology $H^1(H,Z)$ is killed by the order of the finite group H. Now, the order of the group $Gal(\mathbb{Q}(\zeta_p+\overline{\zeta_p})/\ell)$ is a divisor of $\frac{p-1}{2}$. Thus elements in the image of the map induced by f:

$$f_*:\widetilde{\rho}_{p,(p-3)}(\widetilde{\pi_g})\to H^1(Gal(\mathbb{Q}(\zeta_p+\overline{\zeta_p})/\ell), Z(\mathbb{Q}(\zeta_p+\overline{\zeta_p}))$$

should be killed by both p and some divisor of $\frac{p-1}{2}$ and hence they are trivial in cohomology. Therefore there exists a in the center $Z(\mathbb{Q}(\zeta_p+\overline{\zeta_p})$ such that

$$f(\gamma)(\sigma)=a\cdot\sigma(a^{-1})$$

and thus rescaling $\rho_{p,(p-3)}$ by a will insure that $f(\gamma)$ is trivial for every γ and hence $\widetilde{\rho}_{p,(p-3)}(\widetilde{\pi_g}))$ is contained in the group $S\mathbb{U}_{g,p,(i)}(\ell)$. Note now that the center $Z(\mathbb{Q}(\zeta_p+\overline{\zeta_p}))$ consists of scalars which are roots of unity in $\mathbb{Q}(\zeta_p+\overline{\zeta_p})$, and thus they are $2p$-th roots of unity. □

3.5. **Proof of Theorem 1.1.**

Proposition 3.3. *Let $g\geq 2$ and $p\equiv 3(\text{mod } 4)$, p large enough prime. Then, for all but finitely many primes q there exist surjective homomorphisms $B(\widetilde{\pi_g},p,\mathcal{S}(S_g))\to\mathbb{G}_{g,p,(p-3)}(\mathbb{Z}/q^k\mathbb{Z})$ and $B(\pi_g,p,\mathcal{S}(S_g))\to\mathbb{P}G_{g,p,(p-3)}(\mathbb{Z}/q^k\mathbb{Z})$. Moreover, for infinitely many q the finite groups on the right hand side surject onto $PSL(N,\mathbf{F}_q)$, where $\mathbf{F}_q$ denotes the finite field on q elements and $N=\dim W_{g,p,(p-3)}$.*

Proof. We use the following version of the strong approximation theorem due to Nori-Weisfeiler (see ([23], Thm.5.4 and [34]): Let G be a connected linear algebraic group G defined over $\mathbb{Q}$ and $\Lambda\subset G(\mathbb{Z})$ be a Zariski dense subgroup. Assume that $G(\mathbb{C})$ is simply connected. Then the completion of Λ with respect to the congruence topology induced from $G(\mathbb{Z})$ is an open subgroup in the group $G(\widehat{\mathbb{Z}})$ of points of G over the pro-finite completion $\widehat{\mathbb{Z}}$ of $\mathbb{Z}$. We now consider the group $G=\mathbb{G}_{g,p,(i)}$ which satisfies the assumptions of Nori's theorem. If we take Λ to be a finite index subgroup of $\widetilde{\rho}_p(\widetilde{\pi_g})$ the strong approximation theorem implies our claim for $k=1$.

In fact $\widetilde{\rho}_{g,p}|_{\widetilde{\pi_g}}$ factors through $B(\widetilde{\pi_g},p,\mathcal{S}(S_g))$, since homotopy classes of simple closed curves on S_g are sent into commuting Dehn twists in $\widetilde{\Gamma_g}$. Moreover, the center of $\widetilde{g}$ corresponds to a Dehn twist along the boundary curve $c=\partial S_g$, and hence its image by $\widetilde{\rho}_{g,p}$ is a central element of finite order p.

Then a classical result due to Serre (see [29]) for $GL(2)$ and extended by Vasiu (see [32]) to all reductive linear algebraic groups defined over $\mathbb{Q}$ improves the surjectivity statement to all $k\geq 1$.

An alternate approach for $k=1$ would be to use directly the Nori-Weisfeiler approximation theorem on $\mathbb{U}_{g,p,(i)}$. Specifically in ([21], Thm. 2.6) the authors stated the following consequence of ([34], Thm. 10.5, Cor. 10.6): If $\Delta\subset\mathbb{U}_{g,p,(i)}(\mathbb{Q}(\zeta+\overline{\zeta})$ is a Zariski dense subgroup of $\mathbb{U}_{g,p,(i)}$ such that the adjoint trace field of Δ is $\mathbb{Q}(\zeta+\overline{\zeta})$, then for all but finitely many primes $\mathfrak{p}$ in $\mathbb{Q}(\zeta+\overline{\zeta})$

the reduction homomorphism $\Delta \to \mathbb{U}_{g,p,(i)}(\mathbf{F}_\mathfrak{p})$ is surjective, where $\mathbf{F}_\mathfrak{p}$ denotes the residue field $\mathbb{Q}(\zeta+\overline{\zeta})/\mathfrak{p}$. From Lemma 3.9 the group $\widetilde{\rho}_{p,(i),A_p}(\widetilde{\pi_g}) \subset \mathbb{U}_{g,p,(i)}$ has trace field $\mathbb{Q}(\zeta+\overline{\zeta})$, up to possibly translating it by a root of unity. Therefore, for all but finitely many primes $\mathfrak{p}$ in the trace field the reduction mod $\mathfrak{p}$ is well-defined and provides a surjection $\widetilde{\rho}_{p,(i),A_p}(\widetilde{\pi_g}) \to \mathbb{U}_{g,p,(i)}(\mathbf{F}_\mathfrak{p})$. According to the discussion in ([30], p.55; [24], 2.3.3) the group $U_{g,p,(i)}(\mathbf{F}_\mathfrak{p})$ is either a special unitary group, when $\mathfrak{p}$ is prime or ramified in $\mathbb{Q}(\zeta)$ or else a special linear group, when $\mathfrak{p}$ splits completely in $\mathbb{Q}(\zeta)$. In particular, if q is a rational prime which splits completely in $\mathbb{Q}(\zeta)$ and $\mathfrak{p}$ a prime in $\mathbb{Q}(\zeta+\overline{\zeta})$ which divides q, then $U_{g,p,(i)}(\mathbf{F}_\mathfrak{p})$ is isomorphic to $SL(N,\mathbf{F}_q)$, for all but finitely many $\mathfrak{p}$. □

Corollary 3.2. *For large enough prime $p \equiv 3 (\mathrm{mod}\ 4)$ and $g \geq 2$ the group $B(\widehat{\pi_g, p, \mathcal{S}}(S_g))$ is neither prosolvable, nor solvable-by-finite.*

Proof. For large enough prime q the surjective maps $B(\pi_g, p, \mathcal{S}(S_g)) \to \mathbb{P}G_{p,(p-3)}(\mathbb{Z}/q^k\mathbb{Z})$ induce a continuous surjective homomorphism: $B(\widehat{\pi_g, p, \mathcal{S}}(S_g)) \to P\mathbb{G}_{p,(p-3)}(\mathbb{Z}_q)$.

Let $\mathbb{G}^c_{g,p,(p-3)}$ be a simple component of the linear semi-simple algebraic group $\mathbb{G}_{g,p,(p-3)}$. It is well-known that $P\mathbb{G}^c_{g,p,(p-3)}(\mathbb{Z}/q\mathbb{Z})$ are finite simple groups. More precisely, by Proposition 3.3 we can find infinitely many finite groups of the form $PSL(N,\mathbf{F}_q)$ among these quotients.

In particular, a normal solvable subgroup of $P\mathbb{G}^c_{g,p,(p-3)}(\mathbb{Z}_q)$ must project to the trivial subgroup of $P\mathbb{G}^c_{g,p,(p-3)}(\mathbb{Z}/q\mathbb{Z})$ and hence has index at least the size of the later. This is optimal, as

$$P\mathbb{G}_{g,p,(p-3)}(q\mathbb{Z}_q) = \ker(P\mathbb{G}_{g,p,(p-3)}(\mathbb{Z}_q) \to P\mathbb{G}_{g,p,(p-3)}(\mathbb{Z}/q\mathbb{Z}))$$

is a pro-q group and hence it is prosolvable.

Now, letting q go to infinity we obtain that a solvable subgroup should be of infinite index in $B(\widehat{\pi_g, p, \mathcal{S}}(S_g))$, as claimed. □

Proof of the theorem 1.1. We start with the case $m=1$. If $B(\widehat{\pi_g, p, \mathcal{S}}(S_g))$ had a prosolvable normal subgroup of finite index at most N, then $P\mathbb{G}_{g,p,(p-3)}(\mathbb{Z}_q)$ would also have a prosolvable normal subgroup of index at most N. But the index of the largest normal prosolvable group within $P\mathbb{G}_{g,p,(p-3)}(\mathbb{Z}_q)$ goes to infinity with q. Therefore $B(\widehat{\pi_g, p, M})$ is not virtually prosolvable.

Alternatively we can use another version of Hall lemma (see [15]), for finite groups (see e.g. [4], Lemma 3.7):

Lemma 3.10. *Suppose that we have a set of epimorphisms $f_i : G \to H_i$, where $H_1, H_2, \ldots, H_k$ are non-abelian simple groups. If f_i are pairwise non-equivalent, namely there is no isomorphism between $\alpha : H_i \to H_j$ such that $\alpha \circ f_i = f_j$, for $i \neq j$, then the map*

$$(f_1, f_2, \ldots, f_k) : G \to H_1 \times H_2 \times \cdots \times H_k$$

is surjective.

Since $P\mathbb{G}^c_{g,p,(i)}(\mathbb{Z}/qZ)$ is a simple non-abelian q-group, for large q they are pairwise non-isomorphic. From Hall's lemma we derive that the product homomorphism

$$B(\widehat{\pi_g, p, \mathcal{S}}(S_g)) \to \oplus_{q \geq m(p)} P\mathbb{G}_{g,p,(i)}(\mathbb{Z}/q\mathbb{Z})$$

is surjective.

According to ([26], Corollary 4.2.4) a prosolvable group has all its finite quotients solvable. In our case any finite index subgroup of $B(\widehat{\pi_g, p, \mathcal{S}}(S_g))$ surjects onto infinitely many simple groups, and hence it cannot be virtually prosolvable.

Now, in order to prove a similar statement for $B(\pi_g, p, \mathcal{S}_m(S_g))$, where $m \geq 2$ we have to pass to a finite cover of S_g. Indeed the classes of closed immersed based loops in S_g with no more than m self-intersections up to a homeomorphism of S_g form a finite set. Choose a set of based loops M of representatives of this set. There exists then a finite characteristic cover, say of degree d, of pointed surfaces $f : (S_h, \tilde{z}) \to (S_g, z)$ so that the based loops from M admit simple lifts based at $\tilde{z}$. It follows that all based loops from $\mathcal{S}_n(S_g)$ lift to simple based loops in S_h.

Observe that the restriction of any automorphism of π_g to the (image of) π_h, viewed as a subgroup, is an automorphism of π_h. This defines a homomorphism $F : \Gamma^1_g \to \Gamma^1_h$. If $\varphi \in \Gamma^1_g$ is such that $\varphi(x) = x$, for any $x \in \pi_h$, then $\varphi(x^d) = x^d$, for any $x \in \pi_g$. Since surface groups are bi-orderable (this goes back to Magnus) we have $\varphi(x) = x$ for any $x \in \pi_g$, as a strict inequality for some x would imply a strict inequality for its d-th powers. Therefore F is injective.

Recall that for any based loop γ on S_g we have $f(f^{-1}(\gamma)) = \gamma^d \in \pi_1(S_g, z)$, as the loop γ is traveled d-times. If $\gamma \in \mathcal{S}_m(S_g)$, there exists some simple lift $\widetilde{\gamma}$ based at $\tilde{z}$. It follows that $f(\widetilde{\gamma}) = \gamma^{m(\gamma)} \in \pi_1(S_g, z)$, where $m(\gamma)$ is a divisor of d.

Denote by $ad_{S_g,\gamma}$ the action by conjugacy by γ, namely the image of γ into $\Gamma_g^1 = \mathrm{Aut}^+(\pi_g)$. As γ^d belongs to the image of π_h we can compute:

$$F(ad_{S_g,\gamma^d}) = ad_{S_h,\widetilde{\gamma}^{d/m(\gamma)}}$$

It follows that the image by F of the group $\mathcal{S}_m(S_g)[nd]$ is contained into $\mathcal{S}(S_h)[n]$.

Although $F(\pi_g)$ is not contained into π_h, it contains π_h of finite index dividing d since for any element $\gamma \in \pi_g$ its image $F(ad_{S_g,\gamma})^d \in \pi_h$.

Further the map F induces a homomorphism

$$\overline{F} : B(\pi_g, nd, \mathcal{S}_m(S_g)) \to \Gamma_h^1/F(\mathcal{S}_m(S_g)[nd])$$

Now, the subgroup $\pi_h/F(\mathcal{S}_m(S_g)[nd])$ is of finite index into the image $\overline{F}(B(\pi_g, nd, \mathcal{S}_m(S_g)))$. As

$$F(\mathcal{S}_m(S_g)[nd]) \subset \mathcal{S}(S_h)[n] \subset \pi_h$$

and π_h is a normal subgroup in Γ_h^1, the group $\pi_h/F(\mathcal{S}_m(S_g)[nd])$ surjects onto the Burnside-type group $B(\pi_h, n, \mathcal{S}(S_h))$.

It follows that the group $B(\pi_g, nd, \mathcal{S}_m(S_g))$ has a finite index subgroup which surjects onto $B(\pi_h, n, \mathcal{S}(S_h))$, and in particular it is not virtually prosolvable nor solvable-by-finite or finite-by-solvable. □

Remark 3.2. If we had proven that $d = 1$ is convenient for all m then the family of finite quotients of $B(\pi_g, nd, \mathcal{S}_m(S_g))$ would provide a negative answer to Problem 4' from [35].

Remark 3.3. It would be interesting to know whether the image of $B(\widehat{\pi_g, p,} M) \to \prod_{q \geq m(p)} \mathbb{G}_{p,(i)}(\mathbb{Z}_q)$ is open.

Remark 3.4. The arithmetic group $\mathbb{G}_{p,(p-3)}(\mathbb{Z})$, for $g \geq 3$ and prime $p \geq 5$ has the congruence property. This follows from results of Tomanov (see [31], Main Thm. (a)) and Prasad and Rapinchuk (see [25], Thm. 2.(1) and Thm. 3) on the congruence kernel for $\mathbb{Q}$-anisotropic algebraic groups of type ${}^2A_{n-1}$, with $n \geq 4$. Moreover, $\mathbb{G}_{p,(p-3)}(\mathbb{Z})$ is cocompact in $\mathbb{G}_{p,(p-3)}(\mathbb{R})$, since it is $\mathbb{Q}$-anisotropic, by a classical result of Borel and Harish-Chandra (see [2]).

References

[1] C. Blanchet, N. Habegger, G. Masbaum and P. Vogel, *Topological quantum field theories derived from the Kauffman bracket*, Topology 34 (1995), 883–927.
[2] A. Borel and Harish-Chandra, *Arithmetic subgroups of algebraic groups*, Ann. of Math. (2) 75 (1962), 485–535.
[3] N. Dunfield and H. Wong, *Quantum invariants of random 3-manifolds*, Algebr. Geom. Topol. 11 (2011), no. 4, 2191–2205.
[4] N. Dunfield and W. Thurston, *Finite covers of random 3-manifolds*, Invent. Math. 166(2006), 457–521.
[5] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366, Erratum 75(1984), 381.
[6] M. H. Freedman, M. Larsen and Z. Wang, *The two-eigenvalue problem and density of Jones representation of braid groups*, Comm. Math. Phys. 228 (2002), 177–199.
[7] M. H. Freedman, K. Walker and Z. Wang, *Quantum* SU(2) *faithfully detects mapping class groups modulo center*, Geom. Topol. 6 (2002), 523–539.
[8] L. Funar, *On the TQFT representations of the mapping class groups*, Pacific J. Math. 188 (2)(1999), 251–274.
[9] L. Funar, *Zariski density and finite quotients of mapping class groups*, International Mathematics Research Notices 2013, no.9, 2078-2096.
[10] L. Funar and W. Pitsch, *Finite quotients of symplectic groups vs mapping class groups*, 33p., arxiv:1103.1855.
[11] L. Funar and T. Kohno, *On Burau representations at roots of unity*, Geometriae Dedicata 169(2014), 145–163.
[12] S. Gervais, *Presentation and central extensions of mapping class groups*, Trans. Amer. Math. Soc. 348 (1996), 3097–3132.
[13] P. Gilmer and G. Masbaum, *Integral lattices in TQFT*, Ann. Sci. Ecole Norm. Sup. (4) 40 (2007), 815–844.

[14] P. Gilmer and G. Masbaum, *Irreducible factors of modular representations of mapping class groups arising in Integral TQFT*, Quantum Topology, 5 (2014), 225–258.
[15] P.Hall, *The Eulerian functions of a group*, Quarterly J. Math. 7(1936), 134–151.
[16] T.Koberda, R. Santharoubane, *Quotients of surface groups and homology of finite covers via quantum representations*, Invent. Math. 206(2016), 262–292.
[17] G. Kuperberg, *Denseness and Zariski denseness of Jones braid representations*, Geom. Topol. 15 (2011), 11–40.
[18] M. Larsen and Z. Wang, *Density of the SO(3) TQFT representation of mapping class groups*, Comm. Math. Phys. 260 (2005), 641–658.
[19] G. A. Margulis, Discrete subgroups of semisimple Lie groups, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 17, Springer-Verlag, Berlin-New York, 1991, x+388 pp.
[20] G. Masbaum, *An element of infinite order in TQFT-representations of mapping class groups*, Low-dimensional topology (Funchal, 1998), 137–139, Contemp. Math., 233, Amer. Math. Soc., Providence, RI, 1999.
[21] G. Masbaum and A. Reid, *All finite groups are involved in the mapping class groups*, Geom.Topol. 16 (2012) 1393–1411.
[22] G. Masbaum and J. Roberts, *On central extensions of mapping class groups*, Math. Ann. 302 (1995), 131–150.
[23] M. Nori, *On subgroups of* $GL_n(\mathbb{F}_p)$, Invent. Math. 88 (1987), 257–275.
[24] V. Platonov and A. S. Rapinchuk, Algebraic Groups and Number Fields, Pure and Appl. Math Monographs 139, Academic Press 1994.
[25] G. Prasad and A.S. Rapinchuk, *Developements on the congruence subgroup problem after the work of Bass, Milnor and Serre*, in "Collected papers of John Milnor", vol. V, Amer. Math. Soc. (2010), 307–325.
[26] L.Ribes and P.Zalesskii, Profinite groups, second edition. 40, Series of Modern Surveys in Math., 2010.
[27] C.E. Rickart, *Isomorphic groups of linear transformations. II.*, Amer. J. Math. 73 (1951), 697–716.
[28] J.Roberts, *Irreduciblity of some quantum representations of mapping class groups*, J.K.T.R. 10 (2001), 763–767.
[29] J.-P. Serre, Abelian l-adic representations and elliptic curves, AddisonWesley Publ. Co., 1989.
[30] J. Tits, *Classification of algebraic semisimple groups, in Algebraic Groups and Discon- tinuous Subgroups*, Proc. Sympos. Pure Math., 9, 33–62, Amer. Math. Soc., 1966.
[31] G. Tomanov, *On the congruence-subgroup problem for some anisotropic algebraic groups over number fields*, Journal reine angew. Math. 402 (1989), 138–152.
[32] A. Vasiu, *Surjectivity criteria for p-adic representations I*, Manuscripta Math. 112 (2003), 325–355.
[33] John H. Walter, *Isomorphisms between projective unitary groups*, Amer. J. Math. 77 (1955), 805–844.
[34] B. Weisfeiler, *Strong approximation for Zarsiki-dense subgroups of semi-simple algebraic groups*, Ann. of Math. 120(1984), 271–315.
[35] E.Zelmanov, *On some open problems related to the restricted Burnside problem*, Contemporary Mathematics 224, 1999, 237–243.

Institut Fourier, Laboratoire de Mathematiques UMR 5582, Université Grenoble Alpes, CS 40700, 38058 Grenoble, France
E-mail address: `louis.funar@univ-grenoble-alpes.fr`

Centre de Mathématiques de Jussieu, Université Paris Pierre et Marie Curie 4, place Jussieu, F-75252 Paris cedex 05, France
E-mail address: `pierre.lochak@imj-prg.fr`