msp

Geometry & Topology 17 (2013) 2289–2344

Torus bundles not distinguished by TQFT invariants

LOUIS FUNAR
APPENDIX BY LOUIS FUNAR AND ANDREI RAPINCHUK

We show that there exist arbitrarily large sets of non-homeomorphic closed oriented SOL torus bundles with the same quantum (TQFT) invariants. This follows from the arithmetic behind the conjugacy problem in $\mathrm{SL}(2,\mathbb{Z})$ and its congruence quotients, the classification of SOL (polycyclic) 3–manifold groups and an elementary study of a family of Pell equations. A key ingredient is the congruence subgroup property of modular representations, as it was established by Coste and Gannon, Bantay, Xu for various versions of TQFT, and by Ng and Schauenburg for the Drinfeld doubles of spherical fusion categories. In particular, we obtain non-isomorphic 3–manifold groups with the same pro-finite completions, answering a question of Long and Reid. On the other side we prove that two torus bundles over the circle with the same $\mathrm{U}(1)$ and $\mathrm{SU}(2)$ quantum invariants are (strongly) commensurable.

In the appendix (joint with Andrei Rapinchuk) we show that these examples have positive density in a suitable set of discriminants.

20F36, 57M07; 20F38, 57N05

1 Introduction and statements

Two fundamental constructions of TQFTs are due to Reshetikhin and Turaev (see [64]), using link invariants and quantum groups, and to Turaev and Viro [74], using quantum $6j$–symbols. The Reshetikhin–Turaev method was further extended in Turaev [72] to a very general construction of TQFTs, whose input is a modular tensor category, namely an algebraic structure that seems to be the most general data needed for building invariants of arbitrary closed 3–manifolds.

The Drinfeld double construction provides a functor D that associates to every spherical fusion category $\mathcal{C}$ a modular tensor category $D(\mathcal{C})$ (see [50]), sometimes also called the center of $\mathcal{C}$. In the opposite direction, we have the forgetting functor U that associates to the modular tensor category $\mathcal{A}$ the spherical fusion category $U(\mathcal{A})$ underlying $\mathcal{A}$, forgetting the braid structure (see next section for details). Notice that $D(U(\mathcal{C}))=\mathcal{C}\otimes\bar{\mathcal{C}}$, where $\bar{\mathcal{C}}$ is the opposite category and in particular $D(U(\mathcal{C}))$ is anomaly-free. For the

Published: 22 August 2013 DOI: 10.2140/gt.2013.17.2289

sake of simplicity of notation we will drop U in the sequel. If $\mathcal{A}$ is a modular tensor category (see [72]) we denote by $\mathrm{RT}_{\mathcal{A}}$ the Reshetikhin–Turaev TQFT invariant of 3–manifolds constructed out of the category $\mathcal{A}$. In the particular case when the modular tensor category $\mathcal{A}$ is the Drinfeld double $D(\mathcal{C})$ of a spherical fusion category the associated invariant $\mathrm{RT}_{D(\mathcal{C})}$ will be denoted as $\mathrm{TV}_{\mathcal{C}}$ and it will be called the Turaev–Viro TQFT invariant of 3–manifolds associated to $\mathcal{C}$. If $\mathcal{C}$ were itself a modular tensor category then $\mathrm{RT}_{D(\mathcal{C})}$ would indeed coincide with the usual Turaev–Viro invariants $|M|_{\mathcal{C}}$ constructed out of $\mathcal{C}$ by intrinsic methods (see [72, Section V]).

More generally, the Reshetikhin–Turaev construction produces, out of an (anomaly-free) modular tensor category $\mathcal{A}$, a symmetric monoidal 2–functor $\mathrm{RT}_{\mathcal{A}}$ with domain the 2–category of compact oriented 1–, 2– and 3–manifolds (with corners) and target the linear categories. Conjecturally, this construction gives all such 2–functors for which the value of the circles is $\mathcal{A}$ with monoidal structure induced from the pair of pants and braiding coming from the usual half-twist on the pair of pants. On the other hand, the Turaev–Viro construction takes as input a spherical fusion category $\mathcal{C}$ and produces a symmetric monoidal 3–functor with domain the 3–category of compact oriented 0–, 1–, 2– and 3–manifolds (with corners) and target the tensor linear categories. The locality property makes the spherical fusion categories interesting for higher categories. The cobordism hypothesis (which can also be formulated in higher dimensions and was recently proved by Lurie) extends the previous conjecture by claiming that for every fully dualizable object $\mathcal{C}$ of a symmetric monoidal 3–category there exists an essentially unique 3–functor as above, for which the value of a point is $\mathcal{C}$. So the Turaev–Viro construction probably does not lead to all 3–functors, namely, there are more local TQFTs than there are spherical fusion categories.

As a matter of terminology, the Turaev–Viro invariants $\mathrm{TV}_{\mathcal{C}}$ should not be confused with the Turaev–Viro–Barrett–Westbury invariant $|M|_{\mathcal{C}}$, which extends the intrinsic state-sum definition of a 3–manifold invariant associated to an arbitrary spherical fusion category $\mathcal{C}$ (see Barrett and Westbury [6]). Nevertheless this source of confusion is not relevant, as Turaev and Virelizier proved recently (see Turaev and Virelizier [73]) that the Turaev–Viro–Barrett–Westbury invariant $|M|_{\mathcal{C}}$ actually coincides with $\mathrm{RT}_{D(\mathcal{C})}(M)$, for any spherical fusion category $\mathcal{C}$ of non-zero dimension. Notice that, according to (Etingof, Nikshych and Ostrik [21, Theorem 2.3]) all spherical fusion categories over $\mathbb{C}$ have non-zero dimension. All fusion categories considered here will be $\mathbb{C}$–linear categories, unless the opposite is explicitly stated.

A natural question in the area is to what extent the collection of all these 3–manifolds invariants determine the topology of the manifolds. The aim of this article is to solve this question for a particular class of 3–manifolds, namely the SOL manifolds.

Every closed SOL manifold has a finite cover of degree at most 8 that is a torus bundle over a circle. Given $A \in \mathrm{SL}(2,\mathbb{Z})$ we denote by M_A the torus bundle over the circle whose monodromy is given by the matrix A. It is well-known that the manifold has geometry SOL if and only if A is hyperbolic (or Anosov).

The first result of this paper is the following:

Theorem 1.1 *There exist infinitely many pairs of Anosov matrices A, B such that M_A and M_B have non-isomorphic fundamental groups although for every spherical fusion category $\mathcal{C}$ their Turaev–Viro invariants agree:*

$$\mathrm{TV}_{\mathcal{C}}(M_A) = \mathrm{TV}_{\mathcal{C}}(M_B) \tag{1}$$

The simplest series of examples is the following:

$$A = \begin{pmatrix} 1 & kq^2 \\ kv & 1+k^2q^2v \end{pmatrix}, \quad B = \begin{pmatrix} 1 & k \\ kvq^2 & 1+k^2q^2v \end{pmatrix}, \tag{2}$$

where $k \in \mathbb{Z}$, $k \neq 0$, q is an odd prime number $q \equiv 1 \pmod 4$, v is a positive integer such that $-v$ is a non-zero quadratic residue mod q and v is divisible either by a prime p satisfying $p \equiv 3 \pmod 4$, or by 4.

Remark 1.1 Notice that the manifolds M_A and M_B are prime SOL manifolds.

As an immediate consequence we obtain a negative answer to a question due to Turaev (see [72, Problem 5, page 571]).

Corollary 1.1 *There exist infinitely many pairs of matrices A and B as in Theorem 1.1 such that $M_A \# \overline{M_A}$ and $M_B \# \overline{M_B}$ have non-isomorphic fundamental groups but for every modular tensor category $\mathcal{C}$ their Reshetikhin–Turaev TQFT invariants agree:*

$$\mathrm{RT}_{\mathcal{C}}(M_A \# \overline{M_A}) = \mathrm{RT}_{\mathcal{C}}(M_B \# \overline{M_B}) \tag{3}$$

Here $\overline{M}$ denotes the manifold M with the reversed orientation.

Proof This follows from the fact that

$$\mathrm{RT}_{\mathcal{C}}(M_A \# \overline{M_A}) = \mathrm{TV}_{\mathcal{C}}(M_A) \tag{4}$$

according to Proposition 3.4. Moreover prime decomposition of 3–manifolds, as well as splittings of groups as free amalgamated products are unique by classical results of Milnor and Stallings. Therefore the fundamental groups are non-isomorphic since their factors are not isomorphic. □

We will show later (see Theorem 1.3) that there are also (infinitely many) examples of pairs of prime manifolds, but we cannot provide an explicit infinite family as in Theorem 1.1.

Recall now that a quotient of $\mathrm{SL}(2,\mathbb{Z})$ is a *congruence quotient* if it is of the form $\mathrm{SL}(2,\mathbb{Z}/m\mathbb{Z})$ for some non-zero integer m. The key steps in the proof of Theorem 1.1 are the following. We will prove first:

Proposition 1.1 *If M_A and M_B are torus bundles as above then*

$$\mathrm{TV}_{\mathcal{C}}(M_A) = \mathrm{TV}_{\mathcal{C}}(M_B)$$

for any spherical fusion category provided that the matrices A and B are conjugate in every congruence quotient of $\mathrm{SL}(2,\mathbb{Z})$.

The main ingredient needed in the proof is the congruence property for representations associated to Drinfeld doubles of spherical fusion categories (Ng and Schauenburg [53]). Lackenby already noticed in [43] (see also Kania-Bartoszynska [41] and Lickorish [45] for related work) that quantum $\mathrm{SU}(2)$–invariants behave well with respect to modular transformations that belong to congruence subgroups. Specifically, two 3–manifolds are f–congruent, for $f \in \mathbb{Z}_+ \setminus \{0,1\}$, if we can obtain one from the other by Dehn surgeries on framed links which are related by Kirby moves and framing changes adding integral multiples of f. This was further explored and refined (to weak and strong f–congruence) by Gilmer in [34] where it was shown that quantum invariants are natural obstructions to the f–congruence of 3–manifolds. One can prove that torus bundles M_A and M_B as in Proposition 1.1 are f–congruent for *every* integral f.

Now there exists an explicit classification of the manifolds of the form M_A. For the sake of simplicity we will restrict ourselves to Anosov matrices A, B. In this case M_A is a SOL manifold and it is easy to see that it is Haken since the fiber is incompressible. Therefore it suffices to understand its fundamental group, which is the polycyclic group Γ_A with the presentation

$$\Gamma_A = \langle t, a, b \mid ab = ba, tat^{-1} = a^{\alpha_{11}} b^{\alpha_{12}}, tbt^{-1} = a^{\alpha_{21}} b^{\alpha_{22}} \rangle, \tag{5}$$

where:

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}$$

We have then the following:

Proposition 1.2 *Let A and B be matrices from $\mathrm{SL}(2,\mathbb{Z})$ whose traces are different from 2. Then the groups Γ_A and Γ_B are isomorphic if and only if A is conjugate to either B or to B^{-1} within $\mathrm{GL}(2,\mathbb{Z})$.*

Although considered a folklore statement going back as far as Poincaré, the result above seems to have first appeared with a sketch of proof in (Ghys and Sergiescu [33, Appendix 1, Proposition 2]) and then with all details in the unpublished [5] by Barbot. For the sake of completeness we give detailed proofs below. Notice that Proposition 1.2 actually gives the classification of torus bundles up to homeomorphism, since these are aspherical Haken manifolds and hence completely determined by their fundamental groups.

Eventually the problem of finding 3–manifolds M_A and M_B as in the statement of Theorem 1.1 is reduced to a purely arithmetic question on integral matrices. This amounts to find whether there exist Anosov integral matrices which are conjugate in every congruence subgroup but are not conjugate within $\mathrm{GL}(2,\mathbb{Z})$. This question was already answered affirmatively by Stebe in [68], who gave such an example. We are able to give infinitely many such pairs of examples having a slightly stronger property (as needed in Proposition 1.2), as follows:

Proposition 1.3 *There exist infinitely many pairs of matrices A and B in $\mathrm{SL}(2,\mathbb{Z})$ that are conjugate in every congruence quotient, such that A is conjugate neither to B nor to B^{-1} in $\mathrm{GL}(2,\mathbb{Z})$. For instance we can take*

$$A=\begin{pmatrix}1 & kq^2\\ kv & 1+k^2q^2v\end{pmatrix} \quad \text{and} \quad B=\begin{pmatrix}1 & k\\ kvq^2 & 1+k^2q^2v\end{pmatrix}$$

where $k\in\mathbb{Z}$, q is an odd prime number $q\equiv 1 (\mathrm{mod}\, 4)$, v is a positive integer such that first $-v$ is a non-zero quadratic residue mod q, and second v is divisible either by a prime $p\equiv 3 \pmod 4$, or by 4.

Remark 1.2 Stebe's example [68] is:

$$A=\begin{pmatrix}188 & 275\\ 121 & 177\end{pmatrix} \quad \text{and} \quad B=\begin{pmatrix}188 & 11\\ 3025 & 177\end{pmatrix}$$

This implies that any pair of integral Anosov matrices as in Proposition 1.3 gives rise to SOL 3–manifolds which are not distinguished by their Turaev–Viro TQFT invariants, thus proving Theorem 1.1.

In the examples above the manifolds M_A and M_B obtained throughout Proposition 1.3 are actually commensurable SOL manifolds. This is not a fortuitous coincidence since we have the following:

Theorem 1.2 *If the torus bundles SOL manifolds M and N have the same Turaev–Viro invariants for the $\mathrm{U}(1)$ and $\mathrm{SU}(2)$ TQFTs then they are strongly commensurable.*

Let us explain briefly the terminology used for the commensurability above. Two groups are said to be *commensurable* if they have finite index subgroups which are isomorphic.

Barbot [5] (see also Bridson and Gersten [8]) proved that the groups Γ_A and Γ_B are commensurable if and only if the quotient of their discriminants D_A/D_B is the square of a rational number. Here the discriminant of A is $D_A = \mathrm{Tr}(A)^2 - 4\det(A)$ when $\mathrm{Tr}(A)$ is odd. Moreover, this is equivalent to the fact that A^p and B^q are conjugate within $\mathrm{GL}(2,\mathbb{Q})$, for some $p, q \in \mathbb{Z}\setminus\{0\}$. We will call the matrices A and B in $\mathrm{SL}(2,\mathbb{Z})$ *strongly commensurable* if actually A and B are conjugate within $\mathrm{GL}(2,\mathbb{Q})$, namely they have the same trace (and determinant).

Let us introduce some more terminology coming from classical class field theory. We set $\mathcal{I}(M_A)$ for the ideal class group of the order $\mathbb{Z}[(\mathrm{Tr}(A)+\sqrt{D_A})/2]$ of the real quadratic field $\mathbb{Q}(\sqrt{D_A})$. When D_A is square-free the order is the ring of integers of $\mathbb{Q}(\sqrt{D_A})$. An old theorem of Latimer, MacDuffee and Taussky-Todd (see Taussky-Todd [12, Appendix] and Newman [52, III.16]) shows that there is a one-to-one correspondence between $\mathcal{I}(M_A)$ and the set of matrices B from $\mathrm{SL}(2,\mathbb{Z})$ having the same trace as A, which are considered up to conjugacy in $\mathrm{GL}(2,\mathbb{Z})$. In this context the "taking the inverse" map $B \to B^{-1}$ passes to the quotient and gives a well-defined involution $\iota\colon \mathcal{I}(M_A) \to \mathcal{I}(M_A)$.

Let M be a given closed orientable 3–manifold. Denote by $\mathcal{X}^{\mathrm{U}(1),\mathrm{SU}(2)}(M)$ (and $\mathcal{X}^{\mathrm{TV}}(M)$) the set of homeomorphism classes of closed orientable 3–manifolds N having the same abelian, SU(2) Turaev–Viro invariants (and the same Turaev–Viro invariants, for every spherical fusion category, respectively).

Corollary 1.2 *Let M be a SOL torus bundle over the circle. The subset of the torus bundles homeomorphism classes in $\mathcal{X}^{\mathrm{U}(1),\mathrm{SU}(2)}(M)$ injects into $\mathcal{I}(M)/\iota$ and, in particular, its cardinal is bounded by the class number of the corresponding totally real quadratic field.*

Remark 1.3 One might as well consider the set of torus bundles N having the same Turaev–Viro invariants as M, up to an *orientation preserving homeomorphism*. Observe that M_A and M_B are orientation-preserving homeomorphic if and only if A and B are conjugate within $\mathrm{SL}(2,\mathbb{Z})$ or else A and B^{-1} are conjugate in $\mathrm{GL}(2,\mathbb{Z})$ by a matrix of determinant -1.

The few examples we know suggest that the subset of torus bundles homeomorphism classes in $\mathcal{X}^{\mathrm{TV}}(M)$ is a quite small proper subset of $\mathcal{I}(M)/\iota$, in general. As a consequence of our proof of Theorem 1.1 and results of Platonov and Rapinchuk (see

Platonov [57], Rapinchuk [62], and Platonov and Rapinchuk [58, Section 8.8.5]) on the genus problem in arithmetic groups we obtain a stronger (but less precise) statement as follows:

Corollary 1.3 *The number of homeomorphisms classes of torus bundles in $\mathcal{X}^{\mathrm{TV}}(M)$, for M running over all torus bundles, is unbounded. Alternatively, for each $m \geq 2$ there exist examples of m pairwise non-homeomorphic torus bundles having the same Turaev–Viro invariants for all spherical fusion categories.*

We will provide an effective version for this corollary in the Appendix. One can slightly improve the finiteness result in Corollary 1.2, by removing the assumptions that manifolds in a equivalence class be torus bundles, as follows:

Proposition 1.4 *If M is a closed irreducible orientable SOL manifold then $|\mathcal{X}^{\mathrm{TV}}(M)|$ is finite.*

These results give some evidence for the following general conjecture:

Conjecture 1.1 If M and N are closed irreducible geometric 3–manifolds having the same abelian and SU(2) Turaev–Viro invariants, then M and N should be commensurable and, in particular, they share the same geometry.

On the other hand, we do not know whether the unboundedness of the number of classes of torus bundles is a general phenomenon, valid in higher genus as well. In order to dismiss obvious examples constructed out of torus bundles we formulate it as follows:

Conjecture 1.2 The number of homeomorphism classes in $\mathcal{X}^{\mathrm{TV}}(M)$ of hyperbolic fibered 3–manifolds N with fiber of genus $g \geq 1$ is finite for every M. Is this number unbounded when M runs over the set of hyperbolic fibered 3–manifolds with fiber of given genus?

The pairs of manifolds from Theorem 1.1 and Corollary 1.3 also give a negative answer to a question stated by Long and Reid in [46] (see also Calegari, Freedman and Walker [9, Remark 3.7]), as follows:

Corollary 1.4 *For any $m \geq 2$ there exist m torus bundles whose fundamental groups have isomorphic pro-finite completions although they are pairwise non-isomorphic.*

This consequence was independently noticed by Masbaum. Our proof actually shows that, more generally, invariants associated to finite groups determine the pro-finite fundamental groups of closed 3–manifolds. We don't know if the SU(2) Turaev–Viro invariants alone determine already the pro-finite completion of the fundamental group.

Remark 1.4 We expect that the topological content of the Turaev–Viro invariants is precisely this kind of arithmetic information: two fibered manifolds are in the same class of $\mathcal{X}^{\mathrm{TV}}(M)$ if and only if their monodromies are conjugate in the pro-finite completions of the mapping class group, which is slightly stronger than the pro-finite fundamental groups being isomorphic. This would connect the quantum invariants to some version of Grothendieck's problem for 3–manifold groups which is stated in [46].

The result of Theorem 1.1 can also be formulated for Reshetikhin–Turaev invariants:

Theorem 1.3 *There exist infinitely many pairs of Anosov matrices A, B such that M_A and M_B have non-isomorphic fundamental groups although for every modular tensor category $\mathcal{C}$ their Reshetikhin–Turaev invariants agree:*

$$\mathrm{RT}_{\mathcal{C}}(M_A) = \mathrm{RT}_{\mathcal{C}}(M_B). \tag{6}$$

The simplest four examples are the following:

$$A = \begin{pmatrix} 1 & 21 \\ 21 & 442 \end{pmatrix}, \quad B = \begin{pmatrix} 106 & 189 \\ 189 & 337 \end{pmatrix} \tag{7}$$

$$A = \begin{pmatrix} 1 & 51 \\ 51 & 2602 \end{pmatrix}, \quad B = \begin{pmatrix} 562 & 1479 \\ 1479 & 2041 \end{pmatrix} \tag{8}$$

$$A = \begin{pmatrix} 1 & 53 \\ 53 & 2810 \end{pmatrix}, \quad B = \begin{pmatrix} 425 & 1007 \\ 1007 & 2386 \end{pmatrix} \tag{9}$$

$$A = \begin{pmatrix} 1 & 55 \\ 55 & 3026 \end{pmatrix}, \quad B = \begin{pmatrix} 881 & 1375 \\ 1375 & 2146 \end{pmatrix} \tag{10}$$

The proof follows similar lines to that of Theorem 1.1, but now we use the congruence property for representations associated to modular tensor categories (Dong, Lin and Ng [18]) in order to obtain the corresponding version of Proposition 1.1 and a more detailed arithmetic study of Rademacher function φ in relation with the reciprocal and inert classes of binary quadratic forms.

The equivalence relation on torus bundles induced by the equality of all Turaev–Viro invariants is the local equivalence of matrices determining a fixed *genus*, in the sense studied by Platonov and Rapinchuk (see [57; 62; 58, Section 8.8.5]). Specifically,

M_B and M_A represent the same class in $\mathcal{X}^{\mathrm{TV}}(M)$ if and only if A and B are locally conjugate, namely their images mod m are conjugate in $\mathrm{GL}(2,\mathbb{Z}/m\mathbb{Z})$, for any positive integer m. Notice that this implies automatically that A and B are conjugate in $\mathrm{GL}(2,\mathbb{Q})$.

A related equivalence relation is the one corresponding to the *Pickel genus* of groups (see Pickel [56]). Two finitely generated groups are in the same Pickel genus if the corresponding sets of finite quotients are the same. This is equivalent, following a deep result of Nikolov and Segal (see [54]) to the fact that their pro-finite completions are isomorphic. The groups of torus bundles $\pi_1(M_B)$ and $\pi_1(M_A)$ have isomorphic pro-finite completions if and only if the subgroups $\langle A\rangle$ and $\langle B\rangle$ are locally conjugate, namely their images mod m are conjugate in $\mathrm{GL}(2,\mathbb{Z}/m\mathbb{Z})$, for any positive integer m. This is coarser than the former equivalence relation.

Acknowledgements

We are indebted to Christian Blanchet, Thierry Barbot, François Costantino, Michael Freedman, Stefan Friedl, Terry Gannon, Jürgen Klüners, Greg Kuperberg, Gregor Masbaum, Greg McShane, Alan Reid, Chris Schommer-Pries, Vlad Sergiescu, Peter Stevenhagen, Vladimir Turaev, Zhenghan Wang, Henry Wilton and Maxime Wolff for useful discussions and comments. The author was partially supported by the ANR grant 2011 BS 01 020 01 ModGroup.

2 Preliminaries about modular tensor categories

2.1 Fusion categories

For simplicity we will only consider *strict* monoidal categories below, meaning that the associativity morphisms are identities. We follow the definitions from Bakalov and Kirillov [3] and Müger [50].

A *left/right rigid* monoidal category is a strict monoidal category $\mathcal{C}$ with unit object $\mathbb{1}$ such that to each object $X\in\mathrm{Ob}(\mathcal{C})$ there are associated a dual object $X^*\in\mathrm{Ob}(\mathcal{C})$ and four morphisms

$$\mathrm{ev}_X\colon X^*\otimes X\to\mathbb{1},\qquad \mathrm{coev}_X\colon \mathbb{1}\to X\otimes X^*,$$
$$\widetilde{\mathrm{ev}}_X\colon X\otimes X^*\to\mathbb{1},\qquad \widetilde{\mathrm{coev}}_X\colon \mathbb{1}\to X^*\otimes X,$$

such that, for every $X\in\mathrm{Ob}(\mathcal{C})$, the pair $(\mathrm{ev}_X,\mathrm{coev}_X)$ is a left duality for X and the pair $(\widetilde{\mathrm{ev}}_X,\widetilde{\mathrm{coev}}_X)$ is a right duality for X, namely:

$$(\mathbb{1}_X\otimes\mathrm{ev}_X)(\mathrm{coev}_X\otimes\mathbb{1}_X)=\mathbb{1}_X\quad\text{and}\quad(\mathrm{ev}_X\otimes\mathbb{1}_{X^*})(\mathbb{1}_{X^*}\otimes\mathrm{coev}_X)=\mathbb{1}_{X^*}$$

The category is rigid if it is both left and right rigid.

A *pivotal* category is a left rigid monoidal category equipped with an isomorphism j of monoidal functors between identity and $(\cdot)^{**}$, called pivotal structure. One should notice that the formulas

$$\widetilde{\mathrm{ev}}_X = \mathrm{coev}_X(\mathbb{1}_{X^*} \otimes j_X^{-1}), \quad \widetilde{\mathrm{coev}}_X = (j_X \otimes \mathbb{1}_{X^*})\mathrm{ev}_X$$

define a right duality so that a pivotal category is rigid.

It is known that every pivotal category is equivalent to a strict pivotal category, namely one where the associativity isomorphisms, the pivotal structure and the canonical isomorphisms $(V \otimes W)^* \to W^* \otimes V^*$ are identities.

The morphisms $\mathrm{ev}_{\mathbb{1}}$ and $\mathrm{coev}_{\mathbb{1}}$ (respectively, $\widetilde{\mathrm{ev}}_{\mathbb{1}}$ and $\widetilde{\mathrm{coev}}_{\mathbb{1}}$) are mutually inverse isomorphisms and $\mathrm{ev}_{\mathbb{1}} = \widetilde{\mathrm{ev}}_{\mathbb{1}} \colon \mathbb{1}^* \to \mathbb{1}$.

Now, for an endomorphism f of an object X of a pivotal category $\mathcal{C}$, one defines the *left/right traces* $\mathrm{tr}_l(f), \mathrm{tr}_r(f) \in \mathrm{End}_{\mathcal{C}}(\mathbb{1})$ by

$$\mathrm{tr}_l(f) = \mathrm{ev}_X(\mathbb{1}_{X^*} \otimes f)\widetilde{\mathrm{coev}}_X \quad \text{and} \quad \mathrm{tr}_r(f) = \widetilde{\mathrm{ev}}_X(f \otimes \mathbb{1}_{X^*})\mathrm{coev}_X.$$

Both traces are symmetric: $\mathrm{tr}_l(gh) = \mathrm{tr}_l(hg)$ and $\mathrm{tr}_r(gh) = \mathrm{tr}_r(hg)$ for any morphisms $g\colon X \to Y$ and $h\colon Y \to X$ in $\mathcal{C}$. Also $\mathrm{tr}_l(f) = \mathrm{tr}_r(f^*) = \mathrm{tr}_l(f^{**})$ for any endomorphism f of an object (and similarly for l exchanged with r).

The left and right dimensions of $X \in \mathrm{Ob}(\mathcal{C})$ are defined by $\dim_l(X) = \mathrm{tr}_l(\mathbb{1}_X)$ and $\dim_r(X) = \mathrm{tr}_r(\mathbb{1}_X)$. Note that isomorphic objects have the same dimensions and $\dim_l(\mathbb{1}) = \dim_r(\mathbb{1}) = \mathbb{1}_{\mathbb{1}}$.

A *spherical category* is a pivotal category whose left and right traces are equal, ie, $\mathrm{tr}_l(f) = \mathrm{tr}_r(f)$ for every endomorphism f of an object. Then they are denoted $\mathrm{tr}(f)$ and called the trace of f. The left (and right) dimensions of an object X are denoted $\dim(X)$ and called the dimension of X. In a (strict) spherical category we can make free use of the graphical calculus.

Let $\mathbb{K}$ be a field, which for the moment is not supposed to be of characteristic zero, although in the next section we will consider $\mathbb{K} = \mathbb{C}$.

A monoidal $\mathbb{K}$*–linear category* is a monoidal category $\mathcal{C}$ such that its Hom-sets are (left) $\mathbb{K}$–modules and the composition and monoidal product of morphisms are $\mathbb{K}$–bilinear. An object $V \in \mathrm{Ob}(\mathcal{C})$ is called *simple* if the map $\mathbb{K} \to \mathrm{End}_{\mathcal{C}}(\mathbb{1}), a \mapsto a\,\mathbb{1}_{\mathbb{1}}$ is a $\mathbb{K}$–algebra isomorphism.

An additive category is said to be *semi-simple* if every object is a direct sum of finitely many simple objects. In the case of Ab–categories from [72] we can weaken our

requirements by asking that every object be dominated by finitely many simple objects. A monoidal $\mathbb{K}$–linear category is called *semi-simple* if the underlying $\mathbb{K}$–linear category is semi-simple with finite-dimensional Hom spaces and $\mathbb{1}$ is a simple object.

Now a *fusion* category over $\mathbb{K}$ is a rigid semi-simple $\mathbb{K}$–linear category $\mathcal{C}$ with finitely many simple objects. The fusion categories which are considered in the next sections will always be spherical.

A monoidal category $\mathcal{C}$ is *braided* if there exist natural isomorphisms $c_{V,W}\colon V\otimes W\to W\otimes V$ for every pair of objects V, W, such that for any $U, V, W \in \mathrm{Ob}(\mathcal{C})$ we have

$$c_{U,V\otimes W} = (\mathbb{1}_V \otimes c_{U,W})(c_{U,V}\otimes \mathbb{1}_W),\ c_{U\otimes V,W} = (c_{U,W}\otimes \mathbb{1}_V)(\mathbb{1}_U \otimes c_{V,W}).$$

Let now $\mathcal{C}$ be a left rigid braided monoidal category. We do not require that $V^{**} = V$. A twist of $\mathcal{C}$ is an automorphism θ of the identity functor of $\mathcal{C}$ satisfying

$$\theta_{V\otimes W} = c_{W,V}c_{V,W}(\theta_V\otimes\theta_W), \quad \text{and} \quad \theta_{\mathbb{1}} = \mathbb{1}_{\mathbb{1}}.$$

The twist θ is a *ribbon* structure on $(\mathcal{C}, c)$ if it also satisfies $\theta_V^* = \theta_{V^*}$ for every $V\in\mathrm{Ob}(\mathcal{C})$, and the (left) duality is compatible with the ribbon and twist structures, namely:

$$(\theta_V\otimes\mathbb{1}_{V^*})\mathrm{coev}_V = (\mathbb{1}_V\otimes\theta_{V^*})\mathrm{coev}_V$$

In this case $(\mathcal{C}, c, \theta)$ is called a *ribbon* category. In a ribbon category one associates naturally a pivotal structure by using the (canonical) isomorphism $u_X\colon X\to X^{**}$ given by:

$$u_X = (\mathrm{ev}_{X^*}\otimes\mathbb{1}_X)(\mathbb{1}_{X^*}\otimes c^{-1}_{X,X^{**}})(\mathrm{coev}_X\otimes\mathbb{1}_{X^{**}})$$

and setting $\theta = u^{-1}j$. Moreover this pivotal structure j is spherical.

A *modular tensor category* over $\mathbb{K}$ is a ribbon fusion category $(\mathcal{A}, c, \theta)$ over $\mathbb{K}$ such that the matrix S having entries $S_{ij} = \mathrm{tr}((c_{U_j,U_i^*}c_{U_i^*,U_j})$ is non-singular, where $i, j\in I$ and I is the set indexing the simple objects $U_i, i\in I$ in $\mathcal{A}$. This matrix is called the S–matrix of the category $\mathcal{A}$. Notice that I has induced a duality $*$ such that $U_{i^*} = U_i^*$, for any $i\in I$ and there exists a label (also called color) $0\in I$ such that $U_0 = \mathbb{1}$. Since the object U_i is simple the twist θ_{U_i} acts on U_i as a scalar $\omega_i\in\mathbb{K}$.

The (left) *Drinfeld double* (also called the center) of a (strict) monoidal category $\mathcal{C}$ is a category $D(\mathcal{C})$ whose objects are pairs (V,σ_V), where $V\in\mathrm{Ob}(\mathcal{C})$ and the half-braiding $\sigma_V(W)\colon V\otimes W\times W\otimes V$ is a set of natural isomorphisms satisfying for every $U, V, W\in\mathrm{Ob}(\mathcal{C})$ the identities

$$(V\otimes\sigma_U(W))(\sigma_U(V)\otimes W) = \sigma_U(V\otimes W), \quad \sigma_V(\mathbb{1}) = \mathbb{1}_X.$$

There is a natural monoidal structure on $D(\mathcal{C})$ by defining the tensor product $(U,\sigma_U)\otimes(V,\sigma_V)=(U\otimes V,\sigma_{U\otimes V})$, where

$$\sigma_{U\otimes V}(W)=(\sigma_U(W)\otimes V)(U\otimes\sigma_V(W))$$

and the unit object is $(\mathbb{1},\sigma_{\mathbb{1}})$, where $\sigma_{\mathbb{1}}(V)=\mathbb{1}_V$, for any $U,V,W\in\mathrm{Ob}(\mathcal{C})$. More interesting is the fact that $D(\mathcal{C})$ has a braiding given by $c_{(V,\sigma_V),(W,\sigma_W)}=\sigma_V(W)$ so that $\mathcal{C}$ is a braided monoidal category. If $\mathcal{C}$ is left rigid/pivotal/spherical then $D(\mathcal{C})$ is also left rigid/pivotal/spherical, respectively.

2.2 SL(2, ℤ)–representations from modular tensor categories

Any modular tensor category $\mathcal{C}$ defined over the algebraically closed field $\mathbb{K}$ has associated the modular data (see Gannon [31]), which contains a *projective* representation $\overline{\rho}_{\mathcal{C}}\colon \mathrm{SL}(2,\mathbb{Z})\to\mathrm{PGL}(\mathcal{K}_0(\mathcal{C}))$, where $\mathcal{K}_0(\mathcal{C}))$ is the Grothendieck ring of $\mathcal{C}$ with $\mathbb{C}$–coefficients. However, we have slightly more than that, namely a lift of $\overline{\rho}_{\mathcal{C}}$ to an almost linear representation, by means of the matrices S and T. The almost linear representation comes with a 2–cocycle which was completely described by Turaev. An essential feature of the genus 1 situation is that projective representations could always be lifted (in more than one way) to genuine linear representations, which contrasts with the higher genus case.

The matrices entering in the definition of $\overline{\rho}_{\mathcal{C}}$ are the S–matrix defined above and the T–matrix associated to the twist. Specifically, T has the entries $T_{ij}=\omega_i\delta_{ij}$, $i,j\in I$. Moreover there is also the so-called charge conjugation matrix C having entries $C_{ij}=\delta_{i\,j^*}$, $i,j\in I$, which is actually S^2.

The Gauss sums of $\mathcal{C}$ are given by $p_{\mathcal{C}}^{\pm}=\sum_{i\in I}\omega_i^{\pm 1}\dim(U_i)^2$ and these are non-zero scalars satisfying

$$p_{\mathcal{C}}^{+}\,p_{\mathcal{C}}^{-}=\sum_{i\in I}\dim(U_i)^2=\dim(\mathcal{C}). \tag{11}$$

In [72], Turaev used the notation $\Delta_{\mathcal{C}}=p_{\mathcal{C}}^{-}$ so that $p_{\mathcal{C}}^{+}=\dim(\mathcal{C})\Delta_{\mathcal{C}}^{-1}$. Further, one chooses a *rank* (also called quantum order), which is an element $\lambda\in\mathbb{K}$ such that $\lambda^2=\dim\mathcal{C}$. This was denoted by $\mathcal{D}$ in [72].

The group $\mathrm{SL}(2,\mathbb{Z})$ is generated by the matrices

$$\mathfrak{s}=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\quad\text{and}\quad \mathfrak{t}=\begin{pmatrix}1&1\\0&1\end{pmatrix}.$$

The usual presentation of $\mathrm{SL}(2,\mathbb{Z})$ in the generators $\mathfrak{s},\mathfrak{t}$ has the relations $(\mathfrak{s}\mathfrak{t})^3=\mathfrak{s}^2$ and $\mathfrak{s}^4=1$.

The projective representation $\overline{\rho}_{\mathcal{C}}\colon \mathrm{SL}(2,\mathbb{Z}) \to \mathrm{PGL}(\mathcal{K}_0(C))$ is defined by

$$\overline{\rho}_{\mathcal{C}}(\mathfrak{s}) = S, \quad \overline{\rho}_{\mathcal{C}}(\mathfrak{t}) = T. \tag{12}$$

However the choice of a rank λ and a third root of unity $\zeta \in \mathbb{K}$ of the anomaly $\zeta^3 = \mathcal{D}\Delta^{-1} = p_{\mathcal{C}}^{+}\lambda^{-1}$ enables us to define a lift of $\overline{\rho}_{\mathcal{C}}$ to an ordinary linear representation $\rho_{\mathcal{C}}^{\lambda,\zeta}\colon \mathrm{SL}(2,\mathbb{Z}) \to \mathrm{GL}(\mathcal{K}_0(C))$ by setting

$$\rho_{\mathcal{C}}^{\lambda,\zeta}(\mathfrak{s}) = \lambda^{-1}S, \quad \rho_{\mathcal{C}}^{\lambda,\zeta}(\mathfrak{t}) = \zeta^{-1}T. \tag{13}$$

These lifts are called the modular representations associated to $\mathcal{C}$. It is known that, given a rank λ then the modular tensor category defines a TQFT with anomaly in the group generated by ζ^3, so that 3–manifold invariants associated to the data $(\mathcal{C},\lambda)$ do not depend on the particular choice of ζ.

3 Proof of Proposition 1.1

3.1 TQFT coming from centers of spherical fusion categories

In the case when the modular tensor category is the Drinfeld double $D(\mathcal{C})$ of a spherical fusion category $\mathcal{C}$ a number of simplifications occur.

For every $\mathrm{SL}(2,\mathbb{Z})$–representation ρ we define its dual representation $\widetilde{\rho}$ by means of $\widetilde{\rho}(x) = \rho(JxJ^{-1})$, where

$$J = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z})$$

acts by conjugacy as an outer automorphism of $\mathrm{SL}(2,\mathbb{Z})$.

Notice that in this case we have the following:

Lemma 3.1 (i) *The anomaly of the TQFT coming from $D(\mathcal{C})$ is trivial, ie, $\zeta^3 = 1$ and thus there exists a privileged modular representation $\rho_{\mathcal{C}}^{\lambda,1}$.*

(ii) *Further we have $\rho_{D(\mathcal{C})}^{\lambda,1} = \rho_{\mathcal{C}}^{\lambda,\zeta} \otimes \widetilde{\rho^{\lambda,\zeta}}_{\mathcal{C}}$. Here ζ is arbitrary and in fact the right hand side tensor product is well-defined even when we have only projective representations.*

Proof See [53, Lemma 6.2]. □

The invariants of mapping tori have a very simple expression when the TQFT is anomaly-free. In fact we have the following well-known result:

Lemma 3.2 *Assume that the TQFT associated to the modular tensor category $\mathcal{C}$ is anomaly-free, namely that $\zeta^3 = 1$. Then the invariant of the mapping torus M_A of $A \in \mathrm{SL}(2,\mathbb{Z})$ is expressed as*

$$\mathrm{RT}_{\mathcal{C}}(M_A) = \mathrm{Tr}(\rho_{\mathcal{C}}^{\lambda,1}(A)). \tag{14}$$

Proof For the sake of completeness here is the proof. Turaev defined in [72, Section IV.5, (5.1.a)] an almost linear representation $\epsilon\colon \mathrm{SL}(2,\mathbb{Z}) \to \mathrm{GL}(\mathcal{K}_{\mathbb{K}}(\mathcal{C}))$ satisfying the cocycle law

$$\epsilon(A_1A_2) = \zeta^{3\mu(A_{2*}(L),L,A_{1*}^{-1}(L))}\epsilon(A_1)\epsilon(A_2), \tag{15}$$

where $\mu(L_1,L_2,L_3)$ denotes the Maslov index (see [72, Section IV.3, page 179]) of the triple (L_1,L_2,L_3) of Lagrangian subspaces of $H_1(\Sigma_g;\mathbb{R})$ and L a fixed Lagrangian subspace. Further ϵ is determined by its values on the generators $\epsilon(\mathfrak{s}) = \lambda^{-1}S$ and $\epsilon(\mathfrak{t}) = T$. If $\zeta^3 = 1$ then ϵ is a linear representation that coincides with $\rho_{\mathcal{C}}^{\lambda,1}$. Moreover, one also knows from [72, Section III.2.8, Example 1] that

$$\mathrm{RT}_{\mathcal{C}}(M_A) = \mathrm{Tr}(\epsilon(A)).$$

This proves the claim. □

We will prove now:

Proposition 3.1 *Let $\mathcal{C}$ be an anomaly-free modular tensor category such that the modular representation $\rho_{\mathcal{C}}^{\lambda,1}$ factors through $\mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$. Let A and B be two integral matrices from $\mathrm{SL}(2,\mathbb{Z})$ whose reductions mod N are conjugate. Then $\mathrm{RT}_{\mathcal{C}}(M_A) = \mathrm{RT}_{\mathcal{C}}(M_B)$.*

Proof According to the Lemma 3.2 the invariant $\mathrm{RT}_{\mathcal{C}}(M_A)$ is the trace of the endomorphism $\rho_{\mathcal{C}}^{\lambda,\zeta}(A)$. By hypothesis $\rho_{\mathcal{C}}^{\lambda,\zeta}$ factors as $\rho_{\mathcal{C}}^{\lambda,\zeta} = \rho_{\mathcal{C}}^{\lambda,\zeta,N} \circ \nu_N$, where $\nu_N\colon \mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$ is the homomorphism of reduction mod N.

Since ν_N is surjective there exists $T \in \mathrm{SL}(2,\mathbb{Z})$ such that $\nu_N(A) = \nu_N(T^{-1}BT)$. Therefore:

$$\begin{aligned}\mathrm{Tr}(\rho_{\mathcal{C}}^{\lambda,\zeta}(A)) &\\ = \mathrm{Tr}\big(\rho_{\mathcal{C}}^{\lambda,\zeta,N}(\nu_N(T)) \cdot \rho_{\mathcal{C}}^{\lambda,\zeta,N}(\nu_N(B)) \cdot \big(\rho_{\mathcal{C}}^{\lambda,\zeta,N}(\nu_N(T))\big)^{-1}\big) &= \mathrm{Tr}(\rho_{\mathcal{C}}^{\lambda,\zeta}(B))\end{aligned} \tag{16}$$

Then Lemma 3.2 yields the equality of quantum invariants of M_A and M_B. □

The final ingredient in the proof of Proposition 1.1 is the following result due to Ng and Schauenburg for modular tensor categories that are centers of spherical fusion categories [53], to Peng Xu for conformal field theories derived from vertex operator algebras (see [76]) and to Coste and Gannon [13], and Bantay [4] for RCFT. Recall that a *congruence* subgroup of $\mathrm{SL}(2,\mathbb{Z})$ is the kernel of one of the reducing mod m homomorphism $\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}(2,\mathbb{Z}/m\mathbb{Z})$, for some non-zero integer m.

Theorem 3.1 *Let $D(\mathcal{C})$ be the Drinfeld double of a spherical fusion category $\mathcal{C}$. Then the modular representations $\rho^{\lambda,1}_{D(\mathcal{C})}$ have the congruence property, namely the kernels contain congruence subgroups.*

This proves Proposition 1.1, namely if A and B are conjugate in *every* congruence quotient of $\mathrm{SL}(2,\mathbb{Z})$, then $\mathrm{TV}_{\mathcal{C}}(M_A) = \mathrm{TV}_{\mathcal{C}}(M_B)$ for any spherical tensor category $\mathcal{C}$.

3.2 General modular tensor categories

Turaev constructed in [72, pages 198–199] some almost linear representations of the mapping class group $\mathfrak{M}_g$ of genus g surfaces, for every g. We have to choose first some Lagrangian subspace $L \subset H_1(\Sigma_g;\mathbb{R})$ with respect to the usual symplectic form ω in homology coming from the intersection form. We denote by $Z_{\mathcal{C}}(\Sigma_g)$ the space of conformal blocks in genus g associated to the modular tensor category $\mathcal{C}$.

It is known that there exist maps (which will be called almost linear representations) $f^{\lambda,L}_{\mathcal{C}}\colon \mathfrak{M}_g \to GL(Z_{\mathcal{C}}(\Sigma_g))$ into the automorphisms of the space of conformal blocks $Z_{\mathcal{C}}(\Sigma_g)$, satisfying the following 2–cocycle condition:

$$f^{\lambda,L}_{\mathcal{C}}(\varphi_1\varphi_2) = \zeta^{3\mu(\varphi_{2*}(L),L,\varphi_{1*}^{-1}(L))} f^{\lambda,L}_{\mathcal{C}}(\varphi_1) f^{\lambda,L}_{\mathcal{C}}(\varphi_2) \tag{17}$$

where $\mu(L_1,L_2,L_3)$ denotes the Maslov index (see [72, Section IV.3, page 179]) of the triple (L_1,L_2,L_3) of Lagrangian subspaces of $H_1(\Sigma_g;\mathbb{R})$. This can be found for instance either in [72, Section IV.5, (5.1.a)], and also in a rather equivalent context in [72, Section IV.6, Lemma 6.3.2, (6.3.c)].

We introduce now the Rademacher Phi function (see Rademacher and Grosswald [61]) $\phi_R\colon \mathrm{SL}(2,\mathbb{Z}) \to \mathbb{Z}$, defined as follows:

$$\Phi_R\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} = \begin{cases}(\alpha+\delta)/\gamma - 12\,\mathrm{sgn}(\gamma)s(\alpha,|\gamma|) & \text{if } \gamma \neq 0,\\ \beta/\gamma & \text{otherwise.}\end{cases} \tag{18}$$

Here $s(m,n)$, for $n>0$, denotes the Dedekind sum

$$s(m,n) = \sum_{j=1}^{n-1} = \left(\!\left(\frac{j}{n}\right)\!\right)\left(\!\left(\frac{jm}{n}\right)\!\right), \quad s(0,1)=0, \tag{19}$$

where

$$(20)\qquad ((x)) = \begin{cases} 0, & \text{if } x \in \mathbb{Z}, \\ x - [x] - \frac{1}{2} & \text{otherwise.} \end{cases}$$

Alternatively, we have

$$(21)\qquad s(m,n) = \frac{1}{4n} \sum_{j=1}^{n-1} \cot\left(\frac{\pi j}{n}\right) \cot\left(\frac{\pi j m}{n}\right),$$

We have then the following result, which seems to be well-known to the specialists:

Lemma 3.3 *Let L_0 be the integral Lagrangian subspace of the homology group $H_1(\Sigma_1;\mathbb{R}) = \mathbb{R}^2$ generated by the vector $(1,0)$. Then Turaev's almost linear representation $f_{\mathcal{C}}^{\lambda,L_0}$ in genus $g=1$ is related to the modular representation $\rho_{\mathcal{C}}^{\lambda,\zeta}$ of $\mathrm{SL}(2,\mathbb{Z})$, by means of the formula*

$$(22)\qquad \rho_{\mathcal{C}}^{\lambda,\zeta}(A) = \zeta^{-\Phi_R(A)} f_{\mathcal{C}}^{\lambda,L_0}(A)$$

for every $A \in \mathrm{SL}(2,\mathbb{Z})$.

Proof Consider

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} \quad \text{and let } BA = \begin{pmatrix} \alpha'' & \beta'' \\ \gamma'' & \delta'' \end{pmatrix}.$$

By direct computation we obtain

$$(23)\qquad \mu(BA(L_0), B(L_0), L_0) = -\operatorname{sgn}(\gamma\gamma'\gamma'').$$

On the other hand Rademacher proved that Φ_R is a 1–cocycle whose boundary is 3 times the signature 2–cocycle, in other words we have the identities

$$(24)\qquad \Phi_R(BA) = \Phi_R(A) + \Phi_R(B) - 3\operatorname{sgn}(\gamma\gamma'\gamma'')$$

for A, B as above. Therefore the equation above, the cocycle identity (17) for $f_{\mathcal{C}}^{\lambda,L_0}$ and (23) yield:

$$(25)\qquad \zeta^{-\Phi_R(BA)} f_{\mathcal{C}}^{\lambda,L_0}(BA) = \zeta^{-\Phi_R(B)} f_{\mathcal{C}}^{\lambda,L_0}(B) \cdot \zeta^{-\Phi_R(A)} f_{\mathcal{C}}^{\lambda,L_0}(A)$$

This means that $\zeta^{-\Phi_R} f_{\mathcal{C}}^{\lambda,L_0}$ is a linear representation of $\mathrm{SL}(2,\mathbb{Z})$. Since $\Phi_R(\mathfrak{s}) = 0$ and $\Phi_R(\mathfrak{t}) = 1$ the two linear representations $\zeta^{-\Phi_R} f_{\mathcal{C}}^{\lambda,L_0}$ and $\rho_{\mathcal{C}}^{\lambda,\zeta}$ agree. □

Proposition 3.2 *The quantum invariant of a mapping torus M_A of*

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$$

is given by the formula

$$\mathrm{RT}_{\mathcal{C}}(M_A) = \zeta^{-3\varphi(A)} \operatorname{Tr}(\rho_{\mathcal{C}}^{\lambda,\xi}(A)) \tag{26}$$

where $\varphi\colon \mathrm{SL}(2,\mathbb{Z}) \to \mathbb{Z}$ *is the modified Meyer function*

$$3\varphi(A) = \Phi_R(A) - 3\,\mathrm{sgn}(\gamma(\alpha+\delta-2)). \tag{27}$$

Proof The main reason to introduce the almost linear representations $f_{\mathcal{C}}^{\lambda,L}$ is the following result of Turaev (see [72, Section IV.7, Theorem 7.2.1, page 209]), which expresses the quantum invariant of a mapping torus as follows:

Proposition 3.3 *Let M_h be the mapping torus of some homeomorphism whose mapping class is $h \in \mathfrak{M}_g$. Then*

$$\mathrm{RT}_{\mathcal{C}}(M_h) = \zeta^{3\mu(\Lambda(h_*),L\oplus h_*(L),\mathrm{Diag})} \operatorname{Tr}(f_{\mathcal{C}}^{\lambda,L}(h)) \tag{28}$$

where μ is the Maslov index of the Lagrangian subspace of $-H_1(\Sigma_g;\mathbb{R})\oplus H_1(\Sigma_g;\mathbb{R})$ endowed with the symplectic form $-\omega\oplus\omega$, $\Lambda(h_*)$ denotes the graph of h_*, ie, the subspace of vectors $x\oplus h_*(x)$, where $x\in H_1(\Sigma_g;\mathbb{R})$, and Diag *is the diagonal subspace $\Lambda(1_{H_1(\Sigma_g;\mathbb{R})})$.*

Observe that the manifold M_h and its invariant $\mathrm{RT}_{\mathcal{C}}(M_h)$ do not depend on the choice of the Lagrangian L, although $f_{\mathcal{C}}^{\lambda,L}(h)$ does.

Now it suffices to check that

$$\mu(\Lambda(A), L_0\oplus A(L_0), \mathrm{Diag}) = -\,\mathrm{sgn}\,((\alpha+\delta-2)\gamma) \tag{29}$$

when $A\in\mathrm{SL}(2,\mathbb{Z})$. If $\gamma=0$ then one verifies that the Maslov index is 0. Suppose now that $\gamma\neq 0$. A direct inspection shows that $(\Lambda(A)+L_0\oplus A(L_0))\cap\mathrm{Diag}$ is the one-dimensional subspace generated by the vector $e=(\alpha-1,\gamma)\oplus(\alpha-1,\gamma)$. The quadratic form associated to e has value $\omega(e_2,e)$, where $e=e_1+e_2$ is any decomposition with $e_1\in\Lambda(A)$ and $e_2\in L_0\oplus A(L_0)$. We can take $e_1=(0,\gamma)\oplus(\beta\gamma,\delta\gamma)$ and $e_2=(\alpha-1,0)\oplus(\alpha(1-\delta),\gamma(1-\delta))$. This implies that

$$\omega(e_2,e) = (2-\alpha-\delta)\gamma. \tag{30}$$

Now the signature of this quadratic form is the value of the Maslov index and the formula above follows. □

Since the orientation preserving homeomorphism type of the manifolds M_A depends only on the conjugacy class of A, we obtain immediately the following property of Meyer's function:

Corollary 3.1 *Meyer's function φ is conjugacy invariant.*

Remark 3.1 There exists a slight difference between the usual Meyer's function φ_M from Kirby and Melvin [42] and the modified Meyer function $\varphi(M)$ considered here, following Turaev. This does not makes a big difference since it only affects the invariants for M_A where A is parabolic. Specifically we have:

$$\varphi(A)-\varphi_M(A)=\begin{cases}\frac{1}{2}(1+\operatorname{sgn}(\delta))\operatorname{sgn}(\beta) & \text{if } \gamma=0,\\ 0 & \text{otherwise.}\end{cases} \tag{31}$$

However the function $\phi-\phi_M$ is an integral 1–cocycle so that the boundaries $\delta(\phi)$ and $\delta(\phi_M)$ are cohomologous. Notice that $\delta(\phi_M)$ is Meyer's signature 2–cocycle (see Atiyah [2] and Meyer [48]).

3.3 Reshetikhin–Turaev invariants vs Turaev–Viro invariants

Proposition 3.4 *For any modular tensor category $\mathcal{C}$ we have the identity*

$$\mathrm{RT}_{\mathcal{C}}(M_A\#\overline{M_A})=\mathrm{TV}_{\mathcal{C}}(M_A). \tag{32}$$

Proof Since $\mathrm{RT}_{\mathcal{C}}$ behaves multiplicatively with respect to connected sums, we have

$$\mathrm{RT}_{\mathcal{C}}(M_A\#\overline{M_A})=\mathrm{RT}_{\mathcal{C}}(M_A)\cdot\mathrm{RT}_{\mathcal{C}}(\overline{M_A})=\mathrm{RT}_{\mathcal{C}}(M_A)\cdot\mathrm{RT}_{\bar{\mathcal{C}}}(M_A) \tag{33}$$

from [72, II.2, (2.5.a)]. Here $\bar{\mathcal{C}}$ denotes the mirror category of the modular tensor category $\mathcal{C}$ according to [72, I.1.4]. It is known that the rank $\lambda=\lambda_{\mathcal{C}}$ for $\mathcal{C}$ is equally a rank $\lambda=\lambda_{\bar{\mathcal{C}}}$ for $\bar{\mathcal{C}}$, although the roles of $p^{\pm}_{\mathcal{C}}$ are inverted, namely we have $p^{+}_{\mathcal{C}}=p^{-}_{\bar{\mathcal{C}}}$ and $p^{-}_{\mathcal{C}}=p^{+}_{\bar{\mathcal{C}}}$. It follows also that $\dim_{\mathcal{C}} i=\dim_{\bar{\mathcal{C}}} i$, for every $i\in I$, but $\omega^{-1}_{\mathcal{C},i}=\omega_{\bar{\mathcal{C}},i}$. Furthermore the anomalies $\zeta^3_{\mathcal{C}}=p^{+}_{\mathcal{C}}/\lambda_C$ are inverse to each other, namely $\zeta^3_{\bar{\mathcal{C}}}=\zeta^{-3}_{\mathcal{C}}$. Therefore the S matrix associated to the mirror category has its entries $S(\bar{\mathcal{C}})_{ij}$ equal to $S(\mathcal{C})_{i^*j}$ (from [72, II.1.9, Example 1.9.(2)]). At the last the matrix $T(\bar{\mathcal{C}})_{ij}$ is the inverse of $T(\mathcal{C})_{ij}$ since $T(\bar{\mathcal{C}})_{ij}=\omega^{-1}_{\mathcal{C},i}\delta_{ij}$.

On the other hand we have the representation

$$\widetilde{\rho^{\lambda,\zeta}_{\mathcal{C}}}(x)=\rho^{\lambda,\zeta}_{\mathcal{C}}(JxJ^{-1})$$

defined above. We have the following identities, where ζ stands for $\zeta_{\mathcal{C}}$:

$$\rho^{\lambda,\zeta^{-1}}_{\bar{\mathcal{C}}}(\mathfrak{s})=\lambda^{-1}(S(\mathcal{C})_{i^*j})=\lambda^{-1}S(\mathcal{C})^{-1}=\widetilde{\rho^{\lambda,\zeta}_{\mathcal{C}}}(\mathfrak{s}) \tag{34}$$

$$\rho^{\lambda,\zeta^{-1}}_{\bar{\mathcal{C}}}(\mathrm{t})=\zeta T(\mathcal{C})^{-1}=\widetilde{\rho^{\lambda,\zeta}_{\mathcal{C}}}(\mathrm{t}) \tag{35}$$

Therefore the two representations agree on every element

$$\rho_{\bar{\mathcal{C}}}^{\lambda,\xi^{-1}}(x) = \widetilde{\rho_{\mathcal{C}}^{\lambda,\xi}}(x) \quad \text{for any } x \in \mathrm{SL}(2,\mathbb{Z}). \tag{36}$$

Now using Proposition 3.2 and Lemmas 3.1 and 3.2 we obtain the identities

$$\begin{aligned} \mathrm{RT}_{\mathcal{C}}(M_A)\cdot \mathrm{RT}_{\bar{\mathcal{C}}}(M_A) &= \mathrm{Tr}(\rho_{\mathcal{C}}^{\lambda,\xi}(A))\,\mathrm{Tr}(\widetilde{\rho_{\mathcal{C}}^{\lambda,\xi}}(A)) \\ &= \mathrm{Tr}(\rho_{\mathcal{C}}^{\lambda,\xi}\otimes\widetilde{\rho_{\mathcal{C}}^{\lambda,\xi}}(A)) = \mathrm{Tr}(\rho_{D(\mathcal{C})}^{\lambda,1}(A)) = \mathrm{TV}_{\mathcal{C}}(M_A). \end{aligned} \tag{37}$$

A more direct proof of Proposition 3.4 comes from the recent proof by Turaev and Virelizier (see [73]) of the formula $|M|_{\mathcal{C}} = \mathrm{RT}_{D(\mathcal{C})}(M)$ for any oriented 3–manifold, and spherical fusion category of non-zero dimension $\mathcal{C}$. Here $|M|_{\mathcal{C}}$ is the simplicial $6j$–symbol state sum defined in [72, Section 4]. According to [72, Section IV, Theorem 4.1.1], we have $|M|_{\mathcal{C}} = \mathrm{RT}_{\mathcal{C}}(M)\,\mathrm{RT}_{\mathcal{C}}(\overline{M})$. □

Corollary 3.2 *For pairs of matrices A, B as in Theorem 1.1, M_A and M_B are not homeomorphic but $|\mathrm{RT}_{\mathcal{C}}(M_A)| = |\mathrm{RT}_{\mathcal{C}}(M_B)|$ for any Hermitian modular tensor category $\mathcal{C}$.*

Proof It is known that $\mathrm{RT}_{\mathcal{C}}(\overline{M}) = \overline{\mathrm{RT}_{\mathcal{C}}(M)}$, for any Hermitian modular tensor category $\mathcal{C}$ [72, II.5, Theorem 5.4], so the previous proposition gives us $|\mathrm{RT}_{\mathcal{C}}(M)|^2 = \mathrm{TV}_{\mathcal{C}}(M)$. Also the TQFT associated to $D(\mathcal{C})$ is anomaly-free. This follows from the fact that the mapping class group representations in genus g associated to $\mathcal{C}$ and $D(\mathcal{C})$ satisfy $\rho_{g,D(\mathcal{C})} = \rho_{g,\mathcal{C}}\otimes\widetilde{\rho}_{g,\mathcal{C}}$, in every genus g. In fact the right hand side tensor product is well-defined even when we have only projective representations and this shows that $\rho_{D(\mathcal{C})}$ is a genuine linear representation so that the associated TQFT is anomaly-free.

Finally, the so-called Vafa Theorem (see Vafa [75] and Etingof [20]) shows that the anomaly ζ^3 of the TQFT associated to $D(\mathcal{C})$ is a root of unity for every modular tensor category $\mathcal{C}$ (actually it is enough to know that $|\zeta^3| = 1$) and hence the associated invariants verify the claim. □

3.4 Congruence subgroups

We will prove now:

Proposition 3.5 *Suppose that some modular representation $\rho_{\mathcal{C}}^{\lambda,\zeta}$ associated to the modular tensor category $\mathcal{C}$ factors through $\mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$. Let A and B be two integral matrices whose reductions mod N are conjugate. If $\varphi(A) = \varphi(B)$ then $\mathrm{RT}_{\mathcal{C}}(M_A) = \mathrm{RT}_{\mathcal{C}}(M_B)$.*

Henceforth, if A and B are conjugate in every *congruence quotient of* $\mathrm{SL}(2,\mathbb{Z})$ *then* $\mathrm{RT}_{\mathcal{C}}(M_A)=\mathrm{RT}_{\mathcal{C}}(M_B)$ *for any modular tensor category $\mathcal{C}$ with the congruence property if and only if*

$$\varphi(A)=\varphi(B). \tag{38}$$

Proof According to the Proposition 3.2 the invariant $\mathrm{RT}_{\mathcal{C}}(M_A)$ is the trace of the endomorphism $\rho_{\mathcal{C}}^{\lambda,\zeta}(A)$ up to the factor $\zeta^{-3\varphi(A)}$. By hypothesis, $\rho_{\mathcal{C}}^{\lambda,\zeta}$ factors as

$$\rho_{\mathcal{C}}^{\lambda,\zeta}=\rho_{\mathcal{C}}^{\lambda,\zeta,N}\circ\nu_N,$$

where $\nu_N\colon \mathrm{SL}(2,\mathbb{Z})\to\mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$ is the homomorphism of reduction mod N.

Since ν_N is surjective (see Lemma 5.1) there exists $T\in\mathrm{SL}(2,\mathbb{Z})$ such that $\nu_N(A)=\nu_N(T^{-1}BT)$. Therefore:

$$\begin{aligned}&\mathrm{Tr}(\rho_{\mathcal{C}}^{\lambda,\zeta}(A))\\ &\quad=\mathrm{Tr}\big(\rho_{\mathcal{C}}^{\lambda,\zeta,N}(\nu_N(T))\cdot\rho_{\mathcal{C}}^{\lambda,\zeta,N}(\nu_N(B))\cdot\big(\rho_{\mathcal{C}}^{\lambda,\zeta,N}(\nu_N(T))\big)^{-1}\big)=\mathrm{Tr}(\rho_{\mathcal{C}}^{\lambda,\zeta}(B))\end{aligned} \tag{39}$$

Thus we have equality of quantum invariants of M_A and M_B if and only if $\zeta^{-3\varphi(A)}=\zeta^{-3\varphi(B)}$. Since there are modular categories whose anomaly ζ^3 is a root of unity of arbitrary large degree, the claim follows. □

Ng and Schauenburg proved in [53] that the projective representation $\bar{\rho}_{\mathcal{C}}$ has the congruence property for every modular tensor category $\mathcal{C}$. However this does not imply that some linear lift $\rho_{\mathcal{C}}^{\lambda,\zeta}$ of it also has the congruence property (see [53, Section 7]). Moreover, it is not clear whether the fact that $\rho_{\mathcal{C}}^{\lambda,\zeta}$ has the congruence property for one particular value of (λ,ζ) would imply that all modular representations $\rho_{\mathcal{C}}^{\lambda,\zeta}$ do have it.

Eholzer conjectured in [19] that modular representations $\rho_{\mathcal{C}}^{\lambda,\zeta}$ have the congruence property for every RCFT, or in somewhat equivalent terms, for every modular tensor category. This was recently proved to be true for all modular tensor categories in Dong, Lin and Ng [18].

Theorem 3.2 *Let $\mathcal{C}$ be a modular tensor category. Then the modular representations $\rho_{D(\mathcal{C})}^{\lambda,\zeta}$ have the congruence property, namely the kernels contain congruence subgroups.*

Then Proposition 3.5 implies that $\mathrm{RT}_{\mathcal{C}}(M_A)=\mathrm{RT}_{\mathcal{C}}(M_B)$ for every modular tensor category $\mathcal{C}$ if A and B are conjugate in every congruence quotient of $\mathrm{SL}(2,\mathbb{Z})$ and $\varphi(A)=\varphi(B)$.

Example 3.1 The torus bundles M_A and M_B, where

$$A = \begin{pmatrix} 188 & 275 \\ 121 & 177 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 188 & 11 \\ 3025 & 177 \end{pmatrix}$$

have the same absolute values of quantum invariants, but their phase factors are distinct, in general. The reciprocity law for Dedekind sums,

$$12s(\alpha,\gamma) + 12s(\gamma,\alpha) = \frac{\gamma}{\alpha} + \frac{\alpha}{\gamma} + \frac{1}{\alpha\gamma} - 3\operatorname{sgn}(\alpha\gamma), \tag{40}$$

and the equality $s(\alpha,\gamma) = s(\alpha',\gamma)$, for $\alpha \equiv \alpha' (\mathrm{mod}\, \gamma)$, give us $\varphi(A) = -1$, $\varphi(B) = -21$.

4 Proof of Proposition 1.2

Recall from the introduction that

$$\Gamma_A = \langle t, a, b \mid ab = ba, tat^{-1} = a^{\alpha_{11}} b^{\alpha_{12}}, tbt^{-1} = a^{\alpha_{21}} b^{\alpha_{22}} \rangle, \tag{41}$$

where $A \in \mathrm{SL}(2,\mathbb{Z})$ is a matrix with entries α_{ij}, $1 \le i, j \le 2$, such that $\mathrm{Tr}(A) \neq 2$. We have the following exact sequence:

$$1 \to \mathbb{Z}^2 \xrightarrow{i_A} \Gamma_A \xrightarrow{p_A} \mathbb{Z} \to 1, \tag{42}$$

defined by

$$i_A(1,0) = a, \quad i_A(0,1) = b, \quad p_A(t) = 1, \quad p_A(a) = p_A(b) = 0. \tag{43}$$

Proposition 4.1 *The abelian subgroup $i_A(\mathbb{Z}^2) \subset \Gamma_A$ is the radical set R_A of $[\Gamma_A, \Gamma_A]$ in Γ_A, namely the set of those $x \in \Gamma_A$ for which there exists some $k \neq 0$ such that $x^k \in [\Gamma_A, \Gamma_A]$.*

Proof Consider $x \in R_A$. By the definition of the radical set there exists $k \neq 0$ such that $x^k \in [\Gamma_A, \Gamma_A]$ and thus the image of x^k vanishes in every abelian quotient of Γ_A. This implies that $p_A(x^k) = 0$. Since $k \neq 0$ we have $p_A(x) = \frac{1}{k} p_A(x^k) = 0$, which means that $x \in \ker p_A = i_A(\mathbb{Z}^2)$.

Lemma 4.1 *Every element of Γ_A can be uniquely written in the form $t^s a^n b^m$.*

Proof For every $x \in \mathbb{Z}^2$ the conjugacy by the stable letter t can be expressed as follows:

$$t i_A(x) t^{-1} = i_A(A(x)), \quad t^{-1} i_A(x) t = i_A(A^{-1}(x)), \tag{44}$$

where $A(x)$ denotes the left multiplication by the matrix A of the vector $x \in \mathbb{Z}^2$.

Consider now a word in the generators containing at least one letter t. We use the conjugacy relations above to move to the left every occurrence of the letter t (or t^{-1}). If a leftmost sub-word of the new word is of the form $i_A(x)t^\varepsilon$, with non-zero $x \in \mathbb{Z}^2$, then rewrite it as $t^\varepsilon(t^{-\varepsilon}i_A(x)t^\varepsilon) = t^\varepsilon \cdot i_A(A^{-\varepsilon}(x))$ and continue. This process will stop eventually because there are only finitely many occurrences of t and the resulting word will have the desired form.

For the uniqueness it suffices to see that Γ_A is a HNN extension with one stable letter and conclude by the classical Britton's Lemma. □

Lemma 4.2 *Let U denote the integral matrix $A - \mathbb{1}$. Then $[\Gamma_A, \Gamma_A]$ is the subgroup $i_A(U(\mathbb{Z}^2))$ of R_A.*

Proof If $x \in \mathbb{Z}^2$ then we have the identities

$$[t, i_A(x)] = t i_A(x) t^{-1} i_A(x^{-1}) = i_A(A(x) - x). \tag{45}$$

This shows that $i_A(U(\mathbb{Z}^2)) \subset [\Gamma_A, \Gamma_A]$.

Conversely, let us consider $u \in i_A(U(\mathbb{Z}^2))$. Then $tut^{-1} \in i_A(U(\mathbb{Z}^2))$ and $t^{-1}ut \in i_A(U(\mathbb{Z}^2))$ because

$$t i_A(A(x) - x) t^{-1} = i_A(A^2(x) - A(x)) = i_A(A(y) - y), \quad \text{where } y = Ax \tag{46}$$

and

$$t^{-1} i_A(A(x) - x) t = i_A(x - A^{-1}(x)) = i_A(A(y) - y), \quad \text{where } y = A^{-1}x. \tag{47}$$

Further $p_A([\Gamma_A, \Gamma_A]) = 0$ so that $[\Gamma_A, \Gamma_A]$ is a subgroup of R_A; in particular, it is abelian. Thus the action of a and b (or any $x \in i_A(\mathbb{Z}^2)$) by conjugacy on $i_A(U(\mathbb{Z}^2))$ is trivial.

Now $[\Gamma_A, \Gamma_A]$ is generated by the commutators of elements of Γ_A. The Hall identities hold:

$$[xy, z] = y^{-1}[x, z]y \cdot [y, z], \quad [x, yz] = [x, z] \cdot z^{-1}[x, y]z \tag{48}$$

Then a double recurrence on the number of letters in the words representing $x, y \in \Gamma_A$ and the previous observations about the conjugacy by generators prove that $[x, y] \in i_A(U(\mathbb{Z}^2))$. □

Lemma 4.3 *If A has no eigenvalue equal to 1 then $[\Gamma_A, \Gamma_A]$ is a finite index subgroup of R_A.*

Proof Since $\mathrm{Tr}(A) \neq 2$ we have $|\det(U)| = |\mathrm{Tr}(A) - 2| \neq 0$ so that $U\mathbb{Z}^2 \subset \mathbb{Z}^2$ is a subgroup of index $|\det(U)|$. Since i_A is an isomorphism the lemma follows. □

In particular, for every $x \in i_A(\mathbb{Z}^2)$ there exists some k (which divides $|\det(U)|$) for which $x^k \in [\Gamma_A, \Gamma_A]$, as claimed. □

Now any isomorphism $\phi\colon \Gamma_A \to \Gamma_B$ should restrict to an isomorphism $\phi\colon i_A(\mathbb{Z}^2) \to i_B(\mathbb{Z}^2)$. In fact, if $x \in R_A$ there exists $k \neq 0$ such that $x^k \in [\Gamma_A, \Gamma_A]$ so that $\phi(x)^k \in [\Gamma_B, \Gamma_B]$, meaning that $\phi(x) \in R_B$. Now isomorphisms ϕ between free abelian groups are determined by some invertible matrix, namely

$$\phi(i_A(x)) = i_B(V(x)), \quad \text{for } x \in \mathbb{Z}^2, \tag{49}$$

where $V \in \mathrm{GL}(2, \mathbb{Z})$.

Lemma 4.4 *There exists $E \in \mathbb{Z}^2$ such that either $\phi(t) = t i_B(E)$ or $\phi(t) = t^{-1} i_B(E)$.*

Proof In fact ϕ induces an isomorphism $\phi_* = \Gamma_A/R_A \to \Gamma_B/R_B$. Now both groups Γ_A/R_A and Γ_B/R_B are isomorphic to $\mathbb{Z}$ and so ϕ_* is $\varepsilon \mathbb{1}_{\mathbb{Z}}$ where $\varepsilon \in \{-1, 1\}$. This is precisely the claim of the lemma. □

In order to get rid of the translation factor in ϕ, we need the following extension result:

Lemma 4.5 *For every $E \in \mathbb{Z}^2$ there exists an automorphism $L_E\colon \Gamma_B \to \Gamma_B$ such that:*

$$L_E(t i_B(x)) = t i_B(x + E), \quad L_E(i_B(x)) = i_B(x), \quad \text{for every } x \in \mathbb{Z}^2. \tag{50}$$

Proof We have to show that the homomorphism defined on the generators by:

$$L_E(t) = t i_B(E), \quad L_E(a) = a, \quad L_E(b) = b, \tag{51}$$

is well-defined. First we compute:

$$L_E(t^{-1}) = (t i_B(E))^{-1} = i_B(-E) t^{-1} = t^{-1} \cdot t i_B(-E) t^{-1} = t^{-1} i_B(-B(E)) \tag{52}$$

It suffices now to verify that the relations in Γ_B are preserved, namely at first:

$$\begin{aligned} &L_E(t x t^{-1}) \\ &\quad = t i_B(x + E) t^{-1} i_B(-B(E)) = i_B(B(x + E)) i_B(-B(E)) = i_B(B(x)) \end{aligned} \tag{53}$$

for $x \in \mathbb{Z}^2$, and second $L_E(ab) = L_E(ba)$, which is obvious. Hence L_E defines a homomorphism, whose inverse is L_{-E}, which implies that L_E is an automorphism of Γ_B. An immediate computation shows that

$$L_C(t^s i_B(x)) = \begin{cases} t^s i_B(x + E + B(E) + B^2(E) + \cdots + B^{s-1}(E)) & \text{if } s \geq 1, \\ x & \text{if } s = 0, \\ t^s i_B(x - B^{-1}(E) - B^{-2}(E) - \cdots - B^{-s}(E)) & \text{if } s \leq -1. \end{cases} \tag{54}$$

This proves the lemma. □

We replace now the isomorphism ϕ by the composition $L_{-E} \circ \phi \colon \Gamma_A \to \Gamma_B$, which has trivial translation part, and keep the same notation ϕ for the new isomorphism, which has the property that

$$\phi(t) = t^{\varepsilon}, \quad \text{where } \phi_* = \varepsilon \mathbb{1}_{\mathbb{Z}}. \tag{55}$$

Recall now that $t i_A(x) t^{-1} = i_A(A(x))$, for any $x \in \mathbb{Z}^2$. If $\varepsilon = 1$ then on one hand we have

$$\phi(t i_A(x) t^{-1}) = t \phi(i_A(x)) t^{-1} = t i_B(V(x) t^{-1} = i_B(BV(x)) \tag{56}$$

and on the other hand

$$\phi(t i_A(x) t^{-1}) = \phi(i_A(A(x)) = i_B(VA(x)). \tag{57}$$

The two right hand side terms from above must coincide, so $i_B(VA(x)) = i_B(BV(x))$ for every $x \in i(\mathbb{Z}^2)$, which implies $VA = BV$ so that A and B are conjugate within $\mathrm{GL}(2, \mathbb{Z})$.

Lemma 4.6 *There is an automorphism $J \colon \Gamma_B \to \Gamma_{B^{-1}}$ given by $J(t) = t^{-1}$, $J(a) = a$, $J(b) = b$.*

Proof Clear, by direct computation. □

Assume now that $\varepsilon = -1$. We consider then the isomorphism $J \circ \phi \colon \Gamma_A \to \Gamma_{B^{-1}}$, which satisfies

$$J \circ \phi(t) = t, \quad J \circ \phi(i_A(x)) = i_B(V(x)), \quad \text{for } x \in \mathbb{Z}^2. \tag{58}$$

The argument from above shows now that A and B^{-1} are conjugate by the matrix $V \in \mathrm{GL}(2, \mathbb{Z})$. This proves Proposition 1.2.

Now, we will give also a second, simpler proof, due to S Friedl and H Wilton. Given $C \in \mathrm{SL}(2, \mathbb{Z})$ the abelianization of Γ_C is given by $\mathbb{Z} \oplus \mathbb{Z}^2/(\mathbb{1} - C)\mathbb{Z}^2$. In particular, if

the trace of C is different from 2, then the abelianization of Γ_C is isomorphic to $\mathbb{Z}\oplus T$ where T is a finite group. Therefore, up to sign, there exists a unique epimorphism from Γ_C onto $\mathbb{Z}$. Now suppose that A and B are matrices from $\mathrm{SL}(2,\mathbb{Z})$ whose traces are different from 2 such that there exists an isomorphism $\phi\colon \Gamma_A \to \Gamma_B$. The uniqueness of epimorphisms onto $\mathbb{Z}$ implies first that $\phi(t) = t^\epsilon i_B(v))$ for some $\epsilon \in \{-1, 1\}$ and some $v \in \mathbb{Z}^2$, and second that the restriction $\phi|_{i_A(\mathbb{Z}^2)}\colon i_A(\mathbb{Z}^2) \to i_B(\mathbb{Z}^2)$ is an isomorphism, ie, there exists a $Q \in \mathrm{GL}(2,\mathbb{Z})$ such that $\phi(i_A(w)) = i_B(Qw)$. Now, for any $w \in \mathbb{Z}^2$ we have:

$$\begin{aligned} i_B(QAw) &= \phi(i_A(Aw)) = \phi(ti_A(w)t^{-1}) = \phi(t)\phi(i_A(w))\phi(t^{-1}) \\ &= t^\epsilon i_B(v) i_B(Qw)(t^\epsilon i_B(v))^{-1} \\ &= t^\epsilon i_B(v) i_B(Qw) t^{-\epsilon} i_B(-B^{-\epsilon}v) = t^\epsilon i_B(v + B^\epsilon Qw) t^{-\epsilon} i_B(-B^{-\epsilon}v) \\ &= i_B(v + B^\epsilon Qw - B^\epsilon B^{-\epsilon} v) = i_B(B^\epsilon Qw) \end{aligned}$$

Since w was arbitrary we obtain $QA = B^\epsilon Q$, namely $QAQ^{-1} = B^\epsilon$.

Remark 4.1 The result holds more generally when A and $B \in \mathrm{GL}(2,\mathbb{Z})$ and $|\mathrm{Tr}(A)| \neq 2 \neq |\mathrm{Tr}(B)|$, with the same proof.

5 Proof of Proposition 1.3

Proposition 5.1 *Let*

$$A = \begin{pmatrix} 1 & kq^2 \\ kv & 1 + k^2q^2v \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & k \\ kvq^2 & 1 + k^2q^2v \end{pmatrix}$$

denote matrices from $\mathrm{SL}(2,\mathbb{Z})$, *where* $k \in \mathbb{Z}$, q *is an odd prime number* $q \equiv 1 \pmod 4$, v *is a positive integer such that* $-v$ *is a non-zero quadratic residue mod* q, *which is divisible either by a prime* $p \equiv 3 \pmod 4$, *or by* 4. *Then the following hold:*

(i) *For every natural* N *there exists* $T_N \in \mathrm{SL}(2,\mathbb{Z})$ *such that* $\nu_N(A)$ *and* $\nu_N(B)$ *are conjugate by the matrix* $\nu_N(T)$, *where* $\nu_N\colon \mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ *is the reduction mod* N.

(ii) *The matrix* A *is conjugate neither to* B *nor to* B^{-1} *within* $\mathrm{GL}(2,\mathbb{Z})$.

Proof The conjugacy condition $TA = BT$ is equivalent to a linear system of equations having the 2–parameter family of solutions:

$$T(x,y) = \begin{pmatrix} x & y \\ vy & q^2x + kq^2vy \end{pmatrix}$$

The matrix T belongs to $\mathrm{SL}(2,\mathbb{Z})$ if and only if $x, y \in \mathbb{Z}$ and the determinant of T is 1, namely if and only if the quadratic Diophantine equation

$$q^2x^2 + kq^2vxy - vy^2 = 1 \tag{59}$$

has integral solutions.

In a similar way $\nu_N(A)$ and $\nu_N(B)$ are conjugate by a matrix $T \in \mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$ if and only if the equation (59) has solutions $x, y \in \mathbb{Z}/N\mathbb{Z}$. We can improve this last statement as follows:

Lemma 5.1 *The homomorphism $\nu_N\colon \mathrm{SL}(m,\mathbb{Z}) \to \mathrm{SL}(m,\mathbb{Z}/N\mathbb{Z})$ is surjective.*

Proof It is known that the group $\mathrm{SL}(m,\mathbb{Z}/N\mathbb{Z})$ is generated by the matrices of the form $\mathbb{1} + E_{ij}$, where E_{ij} has only one non-zero entry, which is 1, sitting in position ij. See Hahn and O'Meara [37, Theorem 4.3.9] for a proof.

Here is an explicit construction when $m = 2$. Let

$$U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}$$

be an integral matrix whose reduction mod N is a given matrix of $\mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$. There exist integers α, β such that $\alpha u_{12} - \beta u_{11} = \gcd(u_{11}, u_{12})$. Set then:

$$T = \begin{pmatrix} u_{11} + N(\alpha + u_{11}\gamma) + 1 - \det U & u_{12} + Nb + N(\beta + u_{12}\gamma) + 1 - \det U \\ u_{21} - \dfrac{1}{\gcd(u_{11},u_{12})} u_{11}\gamma(\det U - 1) & u_{22} - \dfrac{1}{\gcd(u_{11},u_{12})} u_{12}\gamma(\det U - 1) \end{pmatrix}$$

where $\gamma = \beta t_{21} - \alpha u_{22}$. Now $\nu_N(T) = \nu_N(U)$ because $\nu_N(\det U) \equiv 1 \in \mathbb{Z}/N\mathbb{Z}$, and $\det T = 1$ so that $T \in \mathrm{SL}(2,\mathbb{Z})$. □

Therefore, if the Diophantine equation (59) has solutions in $\mathbb{Z}/q^s\mathbb{Z}$ for every prime q, then for every natural N there exists $T_N \in \mathrm{SL}(2,\mathbb{Z})$ such that $\nu_N(A)$ and $\nu_N(B)$ are conjugate by the matrix $\nu_N(T)$.

Lemma 5.2 *If $-v$ is a non-zero quadratic residue mod q then the equation* (59) *has solutions in $\mathbb{Z}/N\mathbb{Z}$ for every N.*

Proof Let us show that this equation has solutions mod p^l for every prime p and positive integer l, which will imply that there exist solutions mod N for every N.

If $p \neq q$ then take $x = \bar{q}$ and $y = 0$, where $\bar{a}$ denotes the inverse of a mod p^s. If $p = q$ then $-v$ is also a quadratic residue mod q^l for every positive l, by the quadratic reciprocity law and the fact that $q \equiv 1 \pmod 4$. Thus there exists an invertible z such that $-v \equiv z^2 \pmod q^l$. Therefore $x = 0$ and $y = \bar{z}$ is a solution mod h^l. □

Lemma 5.3 *If q is an odd prime and v is a positive integer then the equation* (59) *has non-integral solutions.*

Proof The discriminant is a perfect square w^2 such that

$$w^2-(k^2q^4v^2+4q^2v)y^2=4q^2. \tag{60}$$

If $k=2n$ is even then w is even and divisible by q so that we can put $w=2qu$, for some integer u satisfying

$$u^2-(n^2q^2v^2+v)y^2=1. \tag{61}$$

If k is odd then $w=qu$ and the equation reads

$$u^2-(k^2q^2v^2+4v)y^2=4. \tag{62}$$

Lemma 5.4 *If (u,y) is an integer solution for either one of the equations* (61) *or* (62) *then y is divisible by q.*

Proof Consider first k even when the equation (61) is a Pell equation. Let us remind briefly the theory of the Pell equation

$$u^2-Dy^2=1, \tag{63}$$

where D is a positive integer which is not a square. There exists only one minimal solution that can be constructed following classical results (see Mollin [49], and Niven, Zuckerman and Montgomery [55]) as follows. We set:

$$P_0=0,\quad Q_0=1,\quad a_0=[\sqrt{D}] \tag{64}$$

$$H_{-2}=1,\quad H_{-1}=0,\quad G_{-2}=-P_0,\quad G_{-1}=Q_0 \tag{65}$$

We define inductively:

$$H_i=a_iH_{i-1}+H_{i-2},\quad G_i=a_iG_{i-1}+G_{i-2} \tag{66}$$

$$P_i=a_{i-1}Q_{i-1}-P_{i-1},\quad Q_i=(D-P_i^2)/Q_{i-1} \tag{67}$$

$$a_i=\left[\frac{P_i+\sqrt{D}}{Q_i}\right] \tag{68}$$

We have therefore:

$$G_{i-1}^2-DH_{i-1}^2=(-1)^iQ_i \tag{69}$$

The algorithm for solving the Pell equation is as follows. Find the smallest even integer $l\geq 1$ such that $Q_l=1$. Then (G_{l-1},H_{l-1}) is the minimal non-trivial solution (u_0,y_0) to the Pell equation (63).

Moreover, any other (positive) integral solution can be obtained from the minimal one by means of the following recurrence:

$$u_{s+1} = u_0 u_s + D y_0 y_s, \quad y_{s+1} = y_0 u_s + x_0 y_s \quad \text{for } s \geq 0. \tag{70}$$

The previous algorithm (notice that D is not a square) gives us the minimal solution for (61):

$$u_0 = 2n^2 q^2 v + 1, \quad y_0 = 2nq. \tag{71}$$

A recurrence on s shows that y_s is a multiple of q for every $s \geq 0$.

Assume now that k is odd where the equation (62) is a Pell-type equation.

When v is odd we can use the same algorithm as used for the Pell equation above to solve (62) but starting from the initial data

$$P_0 = 1, \quad Q_0 = 2 \tag{72}$$

because we are in the situation when $D \equiv 1 \pmod 4$. Then the minimal solution is

$$u_0 = k^2 q^2 v + 2, \quad y_0 = kq \tag{73}$$

and the same arguments show that all solutions y are multiple of q.

Finally, assume that v is even, $v = 2v'$, such that $u = 2u'$ for some integer u' and the equation (62) becomes

$$u'^2 - (k^2 q^2 v'^2 + 2v') y^2 = 1. \tag{74}$$

One finds the minimal solutions

$$u'_0 = k^2 q^2 v' + 1, \quad y_0 = kq. \tag{75}$$

Thus all solutions y are multiple of y. This proves Lemma 5.4. □

Remark 5.1 If v is negative the minimal solutions are different, for instance when $v = -1$ and k is even we have $u_0 = (k/2)q$, $y_0 = 1$, so that the previous lemma cannot be extended to negative v.

Going back to the original equation (59), if y were a multiple of q it would imply that q divides 1, which is a contradiction. Thus (59) has non-integral solutions and hence Lemma 5.3 is proved. □

Further $-v$ was assumed to be a quadratic residue modulo q. Thus Lemma 5.2 shows that the equation (59) has solutions in $\mathbb{Z}/N\mathbb{Z}$ for every N but has non-integral solutions. In particular, the matrices A and B are not conjugate in $\mathrm{SL}(2,\mathbb{Z})$. In order to show that they are not conjugate in $\mathrm{GL}(2,\mathbb{Z})$ either it amounts to prove that the equation corresponding to $\det(T) = -1$, namely

$$q^2x^2 + 2kq^2vxy - vy^2 = -1 \tag{76}$$

has non-integral solutions. If v is divisible by a prime number p that is congruent to 3 mod 4 then the reduction mod p of the equation (76) reads $q^2x^2 \equiv -1 \pmod{p}$. But -1 is not a quadratic residue mod p when p is as above. The same argument works when v is divisible by 4. This shows that the matrices A and B are not conjugate in $\mathrm{GL}(2,\mathbb{Z})$.

Finally, consider the conjugacy between A and

$$B^{-1} = \begin{pmatrix} 1+4k^2q^2v & -2k \\ -2kq^2v & 1 \end{pmatrix}.$$

The system of linear equations $VA = B^{-1}V$ has the solutions

$$V(x,y) = \begin{pmatrix} x & y \\ -vy + 2kq^2vx & -q^2x \end{pmatrix}.$$

The condition $\det(V) = \pm 1$ is actually the same couple of equations

$$q^2x^2 + 2kq^2vxy - vy^2 = \mp 1 \tag{77}$$

studied above. Therefore A and B^{-1} are not conjugate within $\mathrm{GL}(2,\mathbb{Z})$, as claimed. □

Remark 5.2 We have $\varphi(A) - \varphi(B) = 2k(q^2-1)(v+1)$. Since v is positive all pairs (A, B) furnished by Proposition 5.1 have $\varphi(A) \neq \varphi(B)$ and hence the manifolds M_A and M_B can be distinguished by their Reshetikhin–Turaev invariants.

Remark 5.3 There exist always rational solutions to the Diophantine equation above and thus the matrices A and B are always conjugate within $\mathrm{SL}(2,\mathbb{Q})$. This implies that the associated 3–manifolds M_A and M_B are commensurable.

6 Proof of Theorem 1.3

6.1 Outline of the proof

According to Proposition 3.5 and Theorem 3.2, it suffices to show that there exist pairs of Anosov matrices A and B such that their images A and B are conjugate

within $\mathrm{SL}(2,\mathbb{Z}/m\mathbb{Z})$ for every m, neither A and B, nor A and B^{-1}, are conjugate in $\mathrm{GL}(2,\mathbb{Z})$ (thus satisfying the claims of Proposition 5.1) and moreover $\varphi(A)=\varphi(B)$. We reformulate these requirements, in a stronger form, as follows:

Proposition 6.1 *There exist infinitely many pairs of Anosov matrices A and B such that:*

(i) *A and B are conjugate in $\mathrm{SL}(2,\mathbb{Z}/m\mathbb{Z})$ for every m,*

(ii) *A and B are reciprocal, namely they are conjugate in $\mathrm{SL}(2,\mathbb{Z})$ to A^{-1} and B^{-1}, respectively,*

(iii) *A and B are inert, namely they are conjugate in $\mathrm{SL}(2,\mathbb{Z})$ to wAw^{-1} and wBw^{-1}, respectively, where*

$$w=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},$$

(iv) *A and B are not conjugate in $\mathrm{SL}(2,\mathbb{Z})$.*

Proof of Theorem 1.3 assuming Proposition 6.1 If A were conjugate to B in $\mathrm{GL}(2,\mathbb{Z})$, namely $A=sBs^{-1}$, with $s\in\mathrm{GL}(2,\mathbb{Z})$, then $\det(s)=-1$ and $wAw^{-1}=wsB(ws)^{-1}$, with $\det(ws)=1$. Since A is inert, this would imply that A is conjugate in $\mathrm{SL}(2,\mathbb{Z})$ to B, which contradicts our assumption. Since A and B are reciprocal, A cannot be conjugate to B^{-1} in $\mathrm{GL}(2,\mathbb{Z})$ either.

Recall that φ is constructed from Φ_R in such a way that it becomes a quasi-homomorphism $\varphi\colon \mathrm{SL}(2,\mathbb{Z})\to\mathbb{Z}$. Namely, the following hold (see [48]):

$$\varphi(CAC^{-1})=\varphi(A)\quad \text{for } C\in\mathrm{SL}(2,\mathbb{Z}), \tag{78}$$

$$\phi(A^{-1})=-\varphi(A). \tag{79}$$

In particular, if A and B are reciprocal, then $\varphi(A)=\varphi(B)=0$ and this actually holds for any quasi-homomorphism φ. This will settle Theorem 1.3. □

6.2 Proof of Proposition 6.1

Reciprocal (conjugacy) classes in $\mathrm{SL}(2,\mathbb{Z})$ were recently discussed by Sarnak in [67]. Let $A^{\perp}$ denote the transpose of A. Since the transpose is given by

$$(A^{-1})^{\perp}=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}A\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},$$

it follows that A is reciprocal if and only if it is conjugate to its transpose $A^{\perp}$ (see also [67], page 218). Recall that A is ambiguous if A is conjugate within $\mathrm{SL}(2,\mathbb{Z})$ to $w^{-1}A^{-1}w$.

We say that A and B are in the same *genus* (see Borevich and Shafarevich [7]) if their images are conjugate within $\mathrm{SL}(2,\mathbb{Z}/m\mathbb{Z})$, for every m. Our aim is to find reciprocal and inert conjugacy classes in the same genus.

Let D be an odd (square-free) fundamental discriminant. Following Gauss (see [7]) there are $2^{\sigma(D)-1}$ genera of primitive integral binary forms, where $\sigma(D)$ is the number of distinct prime divisors of D.

Denote by $\mathcal{D}^-$ the set of those D for which the negative Pell equation

$$X^2 - DY^2 = -4 \tag{80}$$

has integral solutions. It is known that $D \in \mathcal{D}^-$ if and only if the narrow class group C_D coincides with the class group Cl_D of $\mathbb{Q}(\sqrt{D})$ (see Stevenhagen [69, Lemma 2.1]). Recall that the 4–rank of an abelian group C is the rank of C^2/C^4, which counts the number of distinct cyclic factors of order 4.

Lemma 6.1 *Every $D \in \mathcal{D}^-$ such that the 4–rank of C_D is non-trivial gives raise to a pair of non-conjugate reciprocal matrices in the same principal genus.*

Proof According to Gauss (see [7]) the group of genera is isomorphic to C_D/C_D^2. The classes in the kernel of the projection $C_D \to C_D/C_D^2$ form the principal genus. The set of ambiguous classes is identified with the kernel of the square homomorphism $\delta\colon C_D \to C_D$ given by $\delta(x) = x^2$. Therefore the elements of order 2^n in C_D with $n \geq 2$ are ambiguous classes in the principal genus.

When $D \in \mathcal{D}^-$ it is known that every class is inert and every ambiguous class is reciprocal and vice-versa (see [67, page 214]). In particular, if the 4–rank of C_D is positive then there are at least two inert and reciprocal classes in the principal genus. They are non-conjugate as they are distinct classes in C_D. □

There exists a simple method developed by Rédei and Reichardt (see [63]) to find the 4–rank of the narrow class group C_D. Let $D = p_1 p_2 \cdots p_n$ be the decomposition in odd prime numbers of D. The Rédei matrix M_D is the $n \times n$ matrix over $\mathbb{Z}/2\mathbb{Z}$

whose entries a_{ij} are:

$$a_{ij} = \begin{cases} 1 & \text{if } i \neq j \text{ and } \left(\frac{p_i}{p_j}\right) = -1, \\ 0 & \text{if } i \neq j \text{ and } \left(\frac{p_i}{p_j}\right) = 1, \end{cases} \tag{81}$$

$$a_{jj} = \sum_{i \neq j, 1 \leq i \leq n} a_{ij}. \tag{82}$$

Here $\left(\frac{p}{q}\right) \in \{-1, 1\}$ is the Legendre symbol, equal to 1 if and only if p is a quadratic residue mod q. Following [63], the 4–rank of C_D is given by $\sigma(D) - 1 - \text{rank}_{\mathbb{Z}/2\mathbb{Z}} M_D$.

We will consider from now on D of the form $D = u^2 + 4$, so that the negative Pell equation has obvious solutions $X = u$, $Y = 1$. We seek those D that are odd square-free and such that the associated Rédei matrix is identically zero. If D has at least two prime factors then the 4–rank of C_D is non-trivial. In this case it is easy to find explicit matrices A and B corresponding to ambiguous, inert and reciprocal pairs of classes in the principal genus. The trace t of A will be

$$t = D - 2 \tag{83}$$

so that it verifies

$$t^2 - Du^2 = 4. \tag{84}$$

For each positive integral solution (a, b) of the equation $4a^2 + b^2 = D$, we have associated the classes of binary forms $(a, b, -a)$, which correspond to the symmetric matrices

$$A_{a,b} = \begin{pmatrix} \frac{1}{2}(t - ub) & au \\ au & \frac{1}{2}(t + ub) \end{pmatrix}. \tag{85}$$

These are obviously reciprocal classes in the principal genus C_D^2 of C_D. The examples in Theorem 1.3 arise when choosing $u \in \{21, 51, 53, 55\}$ for which $\sigma(D) = 2$ and $M_D = 0$.

Finally, there are infinitely many $D \in \mathcal{D}^-$ for which the 4–rank of C_D is positive. Let $\mathcal{D}$ denote the set of special discriminants, namely the set of those D whose prime factorization has only distinct odd primes of the form $p \equiv 1 \pmod 4$ and possibly 8. Then in Fouvry and Klüners [24, Theorem 2], the authors state that the subset of those $D \in \mathcal{D}$ for which the 4–rank of C_D equals 1 and the 8–rank vanishes (and hence $D \in \mathcal{D}^-$) has positive density within the set $\mathcal{D}$. In particular this set is infinite.

Remark 6.1 We think that the number of distinct cyclic factors of order $2^m \geq 4$ of the class group C_D, where D runs over the odd square-free D of the form n^2+4, is unbounded.

7 Proof of Theorem 1.2

7.1 Abelian invariants

We will consider the U(1) gauge theory as defined in Funar [27; 29], Gocho [35], and Murakami, Ohtsuki and Okada [51], and then generalized in Deloup [14; 15]. One chooses a root of unity q of order k for odd k and of order $2k$ for even k. Then in [51] there is defined the invariant $Z_k(M,q)$ for 3–manifolds M as follows. Set L be a framed link with n components in S^3 such that the 3–manifold M is obtained by Dehn surgery on L. Let A_L denote the linking matrix of L. We define then after [51, (1.1)] the *MOO invariant* of the 3–manifold M as being:

$$Z_k(M,q) = \left(\frac{G_k(q)}{|G_k(q)|}\right)^{-\sigma(A_L)} |G_k(q)|^{-n} \sum_{x\in(\mathbb{Z}/k\mathbb{Z})^n} q^{{}^T x A_L x}, \tag{86}$$

where σ denotes the signature of the matrix and the Gaussian sums are given by

$$G_k(q) = \sum_{h\in\mathbb{Z}/k\mathbb{Z}} q^{h^2}. \tag{87}$$

Notice that for even k the value of $q^{{}^T x A_L x}$ is defined by taking arbitrary lifts $\widetilde{x} \in (\mathbb{Z}/2k\mathbb{Z})^n$ and setting

$$q^{{}^T x A_L x} = q^{{}^T \widetilde{x} A_L \widetilde{x}},$$

which is independent on the choice of the lifts, since A is symmetric.

These invariants where further extended by Deloup in [14] by making use of general quadratic forms and finally extended to TQFTs in [15]. These TQFTs correspond to suitable modular tensor categories, which are related to the Drinfeld double $D(\mathbb{Z}/k\mathbb{Z})$ of the finite group $\mathbb{Z}/k\mathbb{Z}$ and to the geometric U(1) Chern–Simons gauge theories. A more precise statement is given in [14, Appendix A], where the invariants Z_k and their generalizations are identified with the Reshetikhin–Turaev invariants associated to a modular category $\mathcal{A}$ coming from an abelian group, which is described by Turaev in [72, page 29].

The Turaev–Viro invariants $\mathrm{TV}_{\mathcal{A}}$ are therefore the absolute values of $|Z_k(M,q)|$. The main result of this section is the following:

Proposition 7.1 *Let M_A and M_B be SOL torus bundles with the same absolute value MOO invariants $|Z_k(M,q)|$, for all k. Then, either*

$$\mathrm{Tr}(A) = \mathrm{Tr}(B) \tag{88}$$

or else

$$\mathrm{Tr}(A) + \mathrm{Tr}(B) = 4. \tag{89}$$

Consequently those torus bundles having the same abelian Turaev–Viro invariants as M_A fall into two commensurability classes.

Proof We have first the following explicit computation of the MOO invariants from [51]:

Lemma 7.1 *If k is odd then we have*

$$|Z_k(M,q)| = |H^1(M,\mathbb{Z}/k\mathbb{Z})|^{1/2}. \tag{90}$$

If k is even then

$$|Z_k(M,q)| = \begin{cases} |H^1(M,\mathbb{Z}/k\mathbb{Z})|^{1/2} & \text{if } \alpha\cup\alpha\cup\alpha = 0 \text{ for every } \alpha \in H^1(M,\mathbb{Z}/k\mathbb{Z}), \\ 0 & \text{otherwise.} \end{cases} \tag{91}$$

Proof See [51, Theorem 3.2]. □

Further the cohomology of SOL torus bundles is given by:

Lemma 7.2 *If $M = M_A$ with $A \in \mathrm{SL}(2,\mathbb{Z})$ hyperbolic then*

$$H^1(M_A,\mathbb{Z}/k\mathbb{Z}) \cong \mathbb{Z}/k\mathbb{Z} \oplus \ker \nu_k(A^T - \mathbb{1}), \tag{92}$$

where A^T denotes the transpose of the matrix A.

Proof By the Universal Coefficient Theorem,

$$H^1(M_A,\mathbb{Z}/k\mathbb{Z}) \cong \mathrm{Hom}(H_1(M_A),\mathbb{Z}/k\mathbb{Z}).$$

Since A is hyperbolic, $H_1(M_A) = \mathbb{Z} \oplus \mathrm{Tors}(H_1(M_A))$. The torsion part can be computed by abelianizing Γ_A and we find $\mathrm{Tors}(H_1(M_A)) = \mathbb{Z}^2/(A-\mathbb{1})(\mathbb{Z}^2)$, which is a finite abelian group of order $|\det(A-\mathbb{1})| = |\mathrm{Tr}(A)-2|$.

Then $\mathrm{Hom}(\mathrm{Tors}(H_1(M_A)),\mathbb{Z}/k\mathbb{Z})$ is naturally identified with $\ker(A-\mathbb{1})^*_k$, where

$$(A-\mathbb{1})^*_k\colon \mathrm{Hom}(\mathbb{Z}^2,\mathbb{Z}/k\mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}^2,\mathbb{Z}/k\mathbb{Z})$$

is the linear map given by $(A-\mathbb{1})_k^*(f) = f\circ(A-\mathbb{1})$, for $f\in \mathrm{Hom}(\mathbb{Z}^2,\mathbb{Z}/k\mathbb{Z})$. We have a (non-canonical) isomorphism $(\mathbb{Z}/k\mathbb{Z})^2 \to \mathrm{Hom}(\mathbb{Z}^2,\mathbb{Z}/k\mathbb{Z})$, which sends $(a,b)\in(\mathbb{Z}/k\mathbb{Z})^2$ to the homomorphism $f_{a,b}$ satisfying

$$\left(f_{a,b}\begin{pmatrix}1\\0\end{pmatrix}, f_{a,b}\begin{pmatrix}0\\1\end{pmatrix}\right) = (a,b)\in(\mathbb{Z}/k\mathbb{Z})^2.$$

Then $f_{a,b}\in\ker(A-\mathbb{1})_k^*$ if and only if $(a,b)\in\ker\nu_k(A^T-\mathbb{1})$. This proves the claim. □

Consider now two SOL manifolds M_A and M_B having the same absolute value MOO invariants. If the MOO invariants as well as their generalizations from [14] were the same for the two manifolds then the result would be a simple consequence of the main theorem from Deloup and Gille [16]. In fact these invariants determine the linking pairing of the 3–manifold and in particular the torsion group $\mathrm{Tors}(H_1(M))$.

The case where we only know that the absolute values of the MOO invariants agree is only slightly more complicated. First, when k is odd, Lemma 7.1 and Lemma 7.2 imply that:

$$|\ker\nu_k(A^T-1)| = |\ker\nu_k(B^T-1)| \tag{93}$$

In order to compute the orders of the kernels above we have to recall some standard facts concerning the normal forms of integral matrices. Let $C\colon \mathbb{Z}^n\to\mathbb{Z}^n$ be a non-singular linear map $C\colon \mathbb{Z}^n\to\mathbb{Z}^n$. Then there exists a (unique) collection of positive integers $r_1, r_2, \dots, r_n$, called the invariant factors of C with r_j dividing r_{j+1} (when $j\le n-1$) such that $C = VDW$, where $V, W\in \mathrm{GL}(n,\mathbb{Z})$ are invertible integral matrices and D is diagonal with entries $r_1, r_2, \dots, r_n$. Moreover $|\det(C)| = r_1 r_2\cdots r_n$. This is the so-called Smith normal form (see [52, II.15]).

This normal form is particularly useful if one seeks for counting the solutions of the congruences system $C(x)\equiv 0 \pmod k$. By above this is equivalent to the system of congruences $r_j x_j \equiv 0 \pmod k$, for $1\le j\le n$. Each congruence above gives $\gcd(r_j,k)$ distinct solutions $x_j \pmod k$, so that the total number of solutions of the system is $\prod_{j=1}^n \gcd(r_j,k)$.

Notice that the invariant factors for a 2×2 matrix

$$A = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$$

are simply $r_1(A) = \gcd(a,b,c,d)$ and $r_2(A) = \det(A)/r_1(A)$.

Now, for fixed C and k of the form $k = p^r$, with prime p, if we choose r large enough such that $r \geq m_{j,p}(C)$, where $r_j = p^{m_{j,p}(C)} s_j$, with $\gcd(p, s_j) = 1$ then the previous discussion shows that

$$|\ker \nu_k(C)| = \gcd(|\det(C)|, k). \tag{94}$$

We will apply this formula to $C = A - \mathbb{1}$ and, respectively, $C = B - \mathbb{1}$, where $k = p^r$ for odd prime p and r is chosen large enough such that

$$r \geq \max(m_{j,p}(A - \mathbb{1}), m_{j,p}(B - \mathbb{1})). \tag{95}$$

Then the relations above imply that

$$\gcd(\mathrm{Tr}(A) - 2, p^r) = \gcd(\mathrm{Tr}(B) - 2, p^r) \tag{96}$$

for every odd prime p and r large enough. Therefore the numbers $|\mathrm{Tr}(A) - 2|$ and $|\mathrm{Tr}(B) - 2|$ have the same odd divisors.

Let us now call the even number k *good for* M if we have $\alpha \cup \alpha \cup \alpha = 0$, for every $\alpha \in H^1(M, \mathbb{Z}/k\mathbb{Z})$. Lemma 7.1 shows that k is good if and only if $|Z_k(M, q)| \neq 0$. On the other hand in [51, Corollary 5.3], one founds the following explicit criterion. The number k is not good for M, ie, $Z_k(M, q) = 0$, if and only if there exists $x \in \mathrm{Tors}(H_1(M))$ of order 2^m such that $L_M(x, x) = c/2^m$, where $k = 2^m b$, with odd b, L_M denotes the linking pairing L_M: $\mathrm{Tors}(H_1(M)) \times \mathrm{Tors}(H_1(M)) \to \mathbb{Q}/\mathbb{Z}$, and c is odd.

Now, if M_A and M_B have the same absolute value of MOO invariants, then k is good for M_A if and only if k is good for M_B. On the other hand, we know that $|\mathrm{Tr}(A) - 2| = 2^{m_A} s$ and $|\mathrm{Tr}(A) - 2| = 2^{m_B} s$, with odd s. Observe that any k of the form $k = 2^r$ with $r \geq m_A + 1$ is good for M_A since the torsion $\mathrm{Tors}(H_1(M_A))$ has no elements of order 2^r. In particular if $r \geq \max(m_A, m_B) + 1$ then 2^r is good for both M_A and M_B.

Choose now $p = 2$, $k = 2^r$ with r large enough as in (95) and such that 2^r is good for both M_A and M_B. Then the equality of MOO invariants of M_A and M_B implies

$$|\ker \nu_k(A^T - \mathbb{1})| = |\ker \nu_k(B^T - \mathbb{1})|, \tag{97}$$

which, by above, is equivalent to the following:

$$\gcd(\mathrm{Tr}(A) - 2, 2^r) = \gcd(\mathrm{Tr}(B) - 2, 2^r) \tag{98}$$

Thus $m_A = m_B$ and this completes the proof of the fact that

$$|\mathrm{Tr}(A) - 2| = |\mathrm{Tr}(B) - 2|. \tag{99}$$

If $\mathrm{Tr}(A) = \mathrm{Tr}(B)$ then A and B have the same trace and the same determinant and thus the equation $XA = BX$ has solutions in $\mathrm{GL}(2,\mathbb{Q})$, so that M_A and M_B are (strongly) commensurable.

In fact, recall that Barbot [5] and later Bridson and Gersten [8] proved the following:

Lemma 7.3 *The groups Γ_A and Γ_B are commensurable if and only if the quotient of their discriminants D_A/D_B is the square of an rational. Here the discriminant of A is $D_A = \mathrm{Tr}(A)^2 - 4\det(A)$. Moreover, this is equivalent to the fact that A^p and B^q are conjugate within $\mathrm{GL}(2,\mathbb{Q})$, for some $p, q \in \mathbb{Z}$.*

Further if $\mathrm{Tr}(A) + \mathrm{Tr}(B) = 4$ we have again only one (strong) commensurability class allowed for B. Thus the torus bundles as in the statement of the proposition fall into two commensurability classes. □

We will give now several examples to show that all abelian invariants (of Reshetikhin–Turaev type, not only their absolute values) fail to distinguish the two distinct commensurability classes above.

Proposition 7.2 *Set*

$$A = \begin{pmatrix} 1 & n \\ 1 & n+1 \end{pmatrix}, \quad B = \begin{pmatrix} 1-2n & n \\ -1-2n & n+1 \end{pmatrix}, \quad n \in \mathbb{Z}_+. \tag{100}$$

The manifolds M_A and M_B have the same quantum abelian invariants although $\mathrm{Tr}(A) + \mathrm{Tr}(B) = 4$ and $\mathrm{Tr}(A) \neq \mathrm{Tr}(B)$, if $n \geq 1$ and $n \neq 4$. In particular the trace is not detected by the quantum abelian invariants of torus bundles. Moreover, if $(n+4)/(n-4) \notin \mathbb{Q}^2$ then M_A and M_B (equivalently Γ_A and Γ_B) are not commensurable.

Proof The quantum abelian invariants from [14] are identical for two manifolds if and only if their first Betti numbers agree and their linking pairings are isomorphic (see [16]).

Let T be the torus fiber of M_A. The we have the exact sequence

$$H_2(M_A) \to H_1(T) \xrightarrow{A-\mathbb{1}} H_1(T) \to H_1(M_A) \to \mathbb{Z}. \tag{101}$$

Therefore $H_1(M_A) = \mathbb{Z} \oplus \mathrm{Tors}(H_1(M_A))$, where the torsion $\mathrm{Tors}(H_1(M_A))$ is the image of $H_1(T)$ into $H_1(M_A)$.

The linking pairing $L_A\colon \mathrm{Tors}(H_1(M_A)) \times \mathrm{Tors}(H_1(M_A)) \to \mathbb{Q}/\mathbb{Z}$ is defined as follows. For every $\xi \in \mathrm{Tors}(H_1(M_A))$ we choose a lift of it as an element in $H_2(M_A; \mathbb{Q}/\mathbb{Z})$,

namely an element $\widehat{\xi}$ whose image by the boundary connecting homomorphism $\delta_*\colon H_2(M_A;\mathbb{Q}/\mathbb{Z}) \to H_1(M_A,\mathbb{Z})$ is exactly ξ. Here the connecting homomorphism comes from the long exact sequence associated to the coefficients exact sequence:

$$\cdots \to H_2(M_A;\mathbb{Q}) \to H_2(M_A;\mathbb{Q}/\mathbb{Z}) \to H_1(M_A,\mathbb{Z}) \to H_1(M_A,\mathbb{Q}) \to \cdots \tag{102}$$

We take then $L_A([\eta],[\xi]) = \eta \cdot \widehat{\xi} \in \mathbb{Q}/\mathbb{Z}$ where the intersection product is the one induced by $H_1(M_A,\mathbb{Z}) \times H_2(M_A;\mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$.

If we have a 1–cycle ξ representing the class $[\xi] \in H_1(T^2)$, then its product with $[0,1]$ yields a 2–chain whose boundary is $(A-\mathbb{1})\xi$. This implies that the linking pairing of M_A is given by

$$L_A([\eta],[\xi]) = \omega((A-\mathbb{1})^{-1}(\eta),\xi) \in \mathbb{Q}/\mathbb{Z}, \tag{103}$$

where $\eta,\xi \in H_1(T) \cong \mathbb{Z}^2$ are representing (torsion) classes in $\mathbb{Z}^2/(A-\mathbb{1})(\mathbb{Z}^2) \subset H_1(M_A)$ and ω is the usual (symplectic) intersection form on $H_1(T)$, namely

$$\omega((v_1,v_2),(w_1,w_2)) = v_1w_2 - v_2w_1. \tag{104}$$

The torsion group of 1–homologies of M_A and M_B are both cyclic groups of order $|\mathrm{Tr}(A)-2|$ since the first invariant factors for the integral matrices $A-\mathbb{1}$ and $B-\mathbb{1}$ are both equal to 1. Thus the torsion homology groups are isomorphic. Now we can verify that $(A-\mathbb{1})^{-1}-(B-\mathbb{1})^{-1}$ is the integral matrix

$$\begin{pmatrix} 2 & -2 \\ 2 & -2 \end{pmatrix}$$

such that the linking pairings of M_A and M_B are isomorphic. If $n \geq 1$ and $n \neq 4$ then these torus bundles are SOL manifolds. Their Betti numbers coincide as all SOL manifolds have their first Betti number equal to 1.

The statement concerning the commensurability is a consequence of the commensurability criterion for the polycyclic groups from Lemma 7.3 saying that Γ_A and Γ_B are commensurable if and only if $\mathcal{D}_A/\mathcal{D}_B \in \mathbb{Q}^2$. □

Remark 7.1 If $n=4$ then M_A is a SOL torus bundle but M_B is a nilmanifold. Although their linking pairings are isomorphic their first Betti numbers are different, as the nilmanifold has Betti number 2. Another pairs with the same property are:

$$A = \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & 2 \\ -8 & -5 \end{pmatrix} \tag{105}$$

7.2 SU(2)–invariants and the metaplectic representations

Denote by $\rho_{\mathrm{SU}(2),k}$ (and respectively $\rho_{\mathrm{U}(1),k}$) the $\mathrm{SL}(2,\mathbb{Z})$–representation associated to the modular tensor category constructed out of SU(2) (and respectively U(1) or $\mathbb{Z}/k\mathbb{Z}$) in level k (see [72]). It should be noticed that the parameters $\lambda_{\mathrm{SU}(2),k}, \zeta_{\mathrm{SU}(2),k}$ do not agree with $\lambda_{\mathrm{U}(1),k}, \zeta_{\mathrm{U}(1),k}$. For instance $\zeta_{\mathrm{U}(1),k} = \exp(\pi i/4)$ is independent on k. The choice of the rank and anomaly will be irrelevant in the arguments below.

Recall first that both representations $\rho_{\mathrm{SU}(2),k}$ and $\rho_{\mathrm{U}(1),k}$ factor through the finite congruence group $\mathrm{SL}(2,\mathbb{Z}/k\mathbb{Z})$.

Now explicit formulas for the values of SU(2) quantum invariants of torus bundles were obtained in [39] by Jeffrey. Nevertheless it seems difficult to extract explicit topological information out of them.

The key point in our computation is the existence of simple formulas for the characters of the SU(2) quantum representations:

Proposition 7.3 *We have:*

$$2\,\mathrm{Tr}(\rho_{\mathrm{SU}(2),k}(A)) = \mathrm{Tr}(\rho_{\mathrm{U}(1),k}(A)) - \mathrm{Tr}(\rho_{\mathrm{U}(1),k}(-A)) \tag{106}$$

Proof The finite symplectic groups $\mathrm{Sp}(2g,\mathbb{Z}/k\mathbb{Z})$ are endowed with (projective) representations into some complex vector space V_k, which are known under the name of Segal–Shale–Weil metaplectic representations. Although these were classically constructed only for prime k there exist now several constructions valid for every k. In [27; 29; 35], such representations were constructed for every even k (and for a congruence quotient of the Theta group $\Gamma[2]$ when k is odd) in any dimension g using level k theta functions. The monodromy representations from [51] agree with the previous constructions and work for every odd k as well. Later in Feichtinger, Hazewinkel, Kaiblinger, Matusiak and Neuhauser [23], a direct construction of the metaplectic $\mathrm{SL}(2,\mathbb{Z}/k\mathbb{Z})$–representations was described, which were further generalized in [40] to higher dimensions.

The following seems to be widely known among experts:

Lemma 7.4 *The* $\mathrm{SL}(2,\mathbb{Z})$ *quantum representations* $\rho_{\mathrm{U}(1),k}$ *are lifts of the projective metaplectic representations.*

The theta functions construction was generalized in Funar [28] to quantizations of multidimensional tori endowed with Coxeter group actions. This leads to finite symplectic group representations depending on a semi-simple Lie group G or, equivalently, on

a Coxeter group W (corresponding to the Weyl group of G). It was already noticed in [28] that the $\mathrm{SL}(2,\mathbb{Z}/k\mathbb{Z})$–representations associated to $W=\mathbb{Z}/2\mathbb{Z}$ coincide (projectively) with $\rho_{\mathrm{SU}(2),k}$.

Lemma 7.5 *Let*

$$\tau=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\in \mathrm{SL}(2,\mathbb{Z}).$$

The space V_k splits into eigenspaces for the metaplectic action of τ as $V_k=V_k^+\oplus V_k^-$, where

$$V_k^{\pm}=\{x\in V_k \mid \rho_{\mathrm{U}(1),k}(\tau)(x)=\pm x\}. \tag{107}$$

Then the representation $\rho_{\mathrm{SU}(2),k}$ of $\mathrm{SL}(2,\mathbb{Z})$ is isomorphic to the restriction $\rho_{\mathrm{U}(1),k}|_{V_k^-}$ of the metaplectic representation to the invariant sub-module V_k^-.

Proof This was made so by the explicit construction in [28]. The result was also formulated explicitly in Freedman and Krushkal [26, Section 5] for prime k, but the same argument is valid for all k when comparing with the formulas in [23]. A more precise result was given by Larsen and Wang in [44] and independently by Gilmer in [34, Theorem 5.2]. □

The two lemmas above prove the claim, since the characters of the factors $V^{\pm}$ are precisely the $\pm$–invariant part of the character of V_k. □

Recall now from Proposition 3.2 and equation (26) that the Reshetikhin–Turaev quantum invariants of the torus bundle M_A are suitable multiples of the corresponding characters, as follows:

$$\begin{aligned}\mathrm{RT}_{\mathrm{SU}(2),k}(M_A)&=\zeta_{\mathrm{SU}(2),k}^{-3\varphi(A)}\,\mathrm{Tr}(\rho_{\mathrm{SU}(2),k}(A)),\\ \mathrm{RT}_{\mathrm{U}(1),k}(M_A)&=\zeta_{\mathrm{U}(1),k}^{-3\varphi(A)}\,\mathrm{Tr}(\rho_{\mathrm{U}(1),k}(A)).\end{aligned} \tag{108}$$

The Turaev–Viro abelian invariant is known to be the same as the absolute value of the MOO invariant (up to a scalar) and this can be extended as follows:

Lemma 7.6 *For any oriented 3–manifolds we have:*

$$\mathrm{RT}_{\mathrm{U}(1),k}(M)=k^{-1/2}Z_k(M,q) \tag{109}$$

Proof We know that $\mathrm{TV}_{\mathrm{U}(1),k}(M_A)=k^{-1/2}|Z_k(M,q)|$ and the associated projective representations are isomorphic (see [51; 27; 29; 35]). The anomalies are the same and thus the associated Reshetikhin–Turaev invariants agree.

Another proof is given in [14, Appendix A], where one uses the modular tensor category from [72, page 29]. □

Assume now that

$$\mathrm{RT}_{\mathrm{SU}(2),k}(M_A) = \mathrm{RT}_{\mathrm{SU}(2),k}(M_B) \quad \text{and} \quad \mathrm{RT}_{\mathrm{U}(1),k}(M_A) = \mathrm{RT}_{\mathrm{U}(1),k}(M_B).$$

Then Proposition 7.3 and relations (108) imply that $\mathrm{RT}_{\mathrm{U}(1),k}(M_{\tau A}) = \mathrm{RT}_{\mathrm{U}(1),k}(M_{\tau B})$. In particular, applying the result of Proposition 7.1, we obtain that either $\mathrm{Tr}(A) = \mathrm{Tr}(B)$, or else $\mathrm{Tr}(-A) + \mathrm{Tr}(-B) = 4$. The only possibility is that $\mathrm{Tr}(A) = \mathrm{Tr}(B)$.

The case when the Turaev–Viro invariants of the two manifolds agree is only slightly more complicated. The key point is that Proposition 7.3 leads to a closed formula for the SU(2) quantum invariants of torus bundles. We restrict, for the sake simplicity, to the case of Turaev–Viro invariants, which are central in our argument.

Proposition 7.4 *Let $A \in \mathrm{SL}(2,\mathbb{Z})$ and k be large enough such that whenever p^m, with prime p and $m \geq 1$, divides some invariant factors of $A - \mathbb{1}$ or $A + \mathbb{1}$ then it also divides k. Then the* SU(2)*–Turaev–Viro invariant of M_A is given by*

$$\begin{aligned}(110)\quad |\mathrm{Tr}(\rho_{\mathrm{SU}(2),k}(A))|^2 &= TV_{\mathrm{SU}(2),k}(M_A)\\ &= \Big(\sqrt{\gcd(\mathrm{Tr}(A)-2,k)} - \exp\Big(\frac{\pi i}{4}(f_k(M_A))\Big)\sqrt{\gcd(\mathrm{Tr}(A)+2,k)}\Big)^2\end{aligned}$$

where $f_k(M_A) = \phi_k(M_{\tau A}) - \phi_k(M_A)$, $\tau A = -A$, and $\phi_k(M_A) \in \mathbb{Z}/8\mathbb{Z}$ is the function introduced in [51, Section 4].

Proof We need first the following:

Lemma 7.7 *If A is hyperbolic then $\varphi(A) = \varphi(\tau A)$.*

Proof By definition $\Phi_R(A) = \Phi_R(-A)$ since the Rademacher function is defined on $\mathrm{PSL}(2,\mathbb{Z})$. Further, by (27), the function $\varphi(A) - \Phi_R(A)$ is equal to $\mathrm{sgn}(\gamma(\alpha+\delta-2))$ when

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

and so it also satisfies $\varphi(A) - \Phi_R(A) = \varphi(-A) - \Phi_R(-A)$ when A is hyperbolic, by direct inspection. □

The last lemma implies that

$$(111)\quad Z_k(M_A,q) - Z_k(M_{\tau A},q) = \zeta_{\mathrm{U}(1),k}^{-3\varphi(A)}(\mathrm{Tr}(\rho_{\mathrm{U}(1),k}(A)) - \mathrm{Tr}(\rho_{\mathrm{U}(1),k}(\tau A))).$$

We have the following:

Lemma 7.8 *If A is hyperbolic and k is good for M_A and sufficiently large, then*

$$\mathrm{Tr}(\rho_{\mathrm{U}(1),k}(A)) = \exp\Big(\frac{\pi i}{4}(\varphi(A)+\phi_k(M_A))\Big)|\ker \nu_k(A-\mathbb{1})| \tag{112}$$

where $\phi_k(M_A)\in \mathbb{Z}/8\mathbb{Z}$ is the function introduced in [51, Section 4].

Proof The MOO invariant was computed in [51, Theorem 4.5], for those k for which the invariant is non-zero, as being:

$$Z_k(M_A,q) = \exp\Big(\frac{\pi i}{4}(\varphi(A)+\phi_k(M_A))\Big)|H^1(M_A,\mathbb{Z}/k\mathbb{Z})| \tag{113}$$

Since $\xi^3_{\mathrm{U}(1),k} = \exp(\pi i/4)$ we obtain:

$$\begin{aligned}\mathrm{Tr}(\rho_{\mathrm{U}(1),k}(A)) &= \zeta^{3\varphi(A)}\,\mathrm{RT}_{\mathrm{U}(1),k}(M_{\tau A}) \\ &= \exp\Big(\frac{\pi i}{4}(\varphi(A)+\phi_k(M_A))\Big)k^{-1/2}|H^1(M_A,\mathbb{Z}/k\mathbb{Z})|^{1/2},\end{aligned} \tag{114}$$

which implies the claim. □

Now, if A is hyperbolic and k is large enough then use Lemma 7.8 to derive:

$$\begin{aligned}|\mathrm{Tr}(\rho_{\mathrm{SU}(2),k}(A))|^2 &= \mathrm{TV}_{\mathrm{SU}(2),k}(M_A) \\ &= |\,\mathrm{RT}_{\mathrm{SU}(2),k}(M_A)|^2 = k^{-1}|Z_k(M_A,q)-Z_k(M_{\tau A},q)|^2 \\ &= \Big||\ker \nu_k(A^T-\mathbb{1})|^{\frac12} - \exp\Big(\frac{\pi i}{4}(\phi_k(M_{\tau A})-\phi_k(M_A))\Big)|\ker \nu_k(A+\mathbb{1})|^{\frac12}\Big|^2\end{aligned} \tag{115}$$

Then the closed formula (110) follows. □

7.3 End of the proof of Theorem 1.2

It remains to prove the following:

Proposition 7.5 *If the SOL torus bundles M_A and M_B have the same abelian and* SU(2) *Turaev–Viro invariants then* $\mathrm{Tr}(A)=\mathrm{Tr}(B)$.

Proof We have to recall (see eg [72, Section VI]) that the modular tensor category $\mathcal{C}_{\mathrm{SU}(2)}$, which is leading to the SU(2) invariants, is defined only when the level is of the form $4n$, with $n\geq 3$.

We assume that $a=\mathrm{Tr}(A)\neq \mathrm{Tr}(B)$. According to Proposition 7.1 we must have $\mathrm{Tr}(B)=4-a$. Let k be large enough in order to be good for M_A and M_B and also

to verify (95). We put $\gcd(a-2,k)=u$, $\gcd(a+2,k)=v$ and $\gcd(a-6,k)=w$. Then (115) implies that

$$-2\cos\Big(\frac{\pi i}{4}f_A\Big)\sqrt{uv}+v=-2\cos\Big(\frac{\pi i}{4}f_A\Big)\sqrt{uw}+w \tag{116}$$

where $f_A=\phi_k(M_{\tau A})-\phi_k(M_A)$.

This is equivalent to the equation

$$(\sqrt{v}-\sqrt{w})\Big(\sqrt{v}+\sqrt{w}-2\cos\Big(\frac{\pi i}{4}f_A\Big)\sqrt{u}\Big)=0. \tag{117}$$

Lemma 7.9 *The prime divisors of $a-6$ are the same as the prime divisors of $a+2$.*

Proof Suppose that there exists some odd p, which divides $a-6$ but not $a+2$. We write $a-6=2^s p^r c$, with c odd and coprime with p, $r\geq 1$.

Assume first $s\geq 3$. We chose k of the form $k=2^m p^m$ (with m large with respect to r and s). Then $w=2^s p^r$, $u=\gcd(4(2^{s-2}p^r c+1),2^m p^m)=4$, $v=\gcd(8(2^{s-3}p^r c+1),2^m p^m)=2^t$, where $t\geq 3$. Actually we have $t=3$ if $s\geq 4$. Then equation (117) implies that

$$\sqrt{2^s p^r}+\sqrt{2^t}=4\cos\Big(\frac{\pi i}{4}f_A\Big). \tag{118}$$

Since $4\cos((\pi i/4)f_A)\in\{0,\pm 2\sqrt{2},\pm 4\}$, this equation is impossible for any odd prime p.

Consider now $s=1$. We choose again k of the form $k=2^m p^m$, with m large with respect to r. Then $w=2p^r$, $u=\gcd(2(p^r c+2),2^m p^m)=2$, $v=\gcd(2(p^r c+4),2^m p^m)=2$, so that equation (117) implies that

$$\sqrt{2^s p^r}+\sqrt{2}=2\cos\Big(\frac{\pi i}{4}f_A\Big)\sqrt{2}. \tag{119}$$

Its only integral solution is $p=1$, which is not convenient.

Let now $s=0$. Then, again, choose k of the form $k=2^m p^m$ (with m large with respect to r). We find that $w=p^r$, $u=\gcd(p^r c+4,2^m p^m)=1$, $v=\gcd(p^r c+8,2^m p^m)=1$, so that equation (117) above yields

$$\sqrt{p^r}+1=2\cos\Big(\frac{\pi i}{4}f_A\Big). \tag{120}$$

The only integral solution is again $p=1$.

Let us consider the case when $s=2$. We write $p^r c+1=2^u d$, with odd d. Choose now $k=2^m p^m c^m$, for some large enough m so that k is good for M_A and M_B

and (95) holds. Then $w = 4p^r c$, $u = \gcd(4(p^r c+1), 2^m p^m c^m) = 2^{u+2}$, $v = \gcd(4(p^r c+2), 2^m p^m c^m) = 4$. In this case equation (117) gives us

$$\sqrt{p^r c} + 1 = 2\cos\Big(\frac{\pi i}{4} f_A\Big)\sqrt{2^u}. \tag{121}$$

Suppose that $\cos((\pi i/4) f_A) = 1$ so that we have to find integral solutions of

$$1 + \sqrt{2^u d - 1} = \sqrt{2^{u+2}}. \tag{122}$$

If $d \geq 5$, then for every $u \geq 1$ we have

$$1 + \sqrt{2^u d - 1} \geq 1 + \sqrt{5 \cdot 2^u - 1} > 2\sqrt{2^u}. \tag{123}$$

If $d = 3$ then the previous equation is equivalent to

$$1 + \sqrt{3 \cdot 2^u - 1} = 2\sqrt{2^u}. \tag{124}$$

By taking the square and collecting together the terms, we derive that $2^{2u-2} = 3 \cdot 2^u - 1$. This is impossible when $u \geq 1$ because of modulo 2 considerations. If $d = 1$, then

$$1 + \sqrt{2^u - 1} < 2\sqrt{2^u}. \tag{125}$$

The only possibility left is that $2\cos((\pi i/4) f_A) = \sqrt{2}$ so that the equation reads

$$1 + \sqrt{2^u d - 1} = \sqrt{2^{u+2}}. \tag{126}$$

If $d \geq 3$, as $u \geq 1$, we have

$$1 + \sqrt{2^u d - 1} \geq 1 + \sqrt{3 \cdot 2^u - 1} > 2\sqrt{2^u}. \tag{127}$$

If $d = 1$ then the equation reads

$$1 + \sqrt{2^u - 1} = 2\sqrt{2^u}. \tag{128}$$

Squaring both sides and collecting the terms we obtain $2^{2u-2} = 2^u - 1$, which is impossible by mod 2 considerations. This proves that any odd prime dividing $a-6$ also divides $a+2$. A similar proof shows that conversely, if an odd prime p divides $a+2$ then p divides $a-6$. This proves the lemma. □

Thus the prime divisors of $a-6$ and $a+2$ are the same and this implies that they divide their difference, so actually the only prime divisor of these two numbers is 2. Thus $a-6 = \pm 2^m$ and $a+2 = \pm 2^n$, for some integers m, n. This is impossible when $m \geq 5$ since it implies that $8(\pm 2^{m-3} + 1) = \pm 2^n$, but $\pm 2^{m-3} + 1$ is a non-trivial odd number. Inspecting the remaining cases when $0 \leq m \leq 4$ leads us to the following solutions $a = 2$, $a = 14$ and $a = -10$. The first is not convenient since A was supposed

hyperbolic. The other ones do not satisfy the constraint (117). This contradiction shows that the only possibility is that $\mathrm{Tr}(A) = \mathrm{Tr}(B)$, as claimed. □

7.4 Ideal class groups and proofs of Corollaries 1.2 and 1.3

We want to prove that the set of those M_B having the same abelian and SU(2) Turaev–Viro invariants as M_A is finite, and it can be identified with a subset of a quotient of $\mathcal{I}(M_A)$ by the involution ι which acts as $X \to X^{-1}$ on matrices with given trace.

Let α be a root of $x^2 - \mathrm{Tr}(A)x + 1 = 0$, where $|\mathrm{Tr}(A)| \neq 2$. A construction due to Latimer, MacDuffee and Taussky-Todd (see [12, Appendix] and [52, III.16] for details) establishes a one-to-one correspondence between the ideal class group $\mathcal{I}(M_A)$ of the order $\mathbb{Z}[\alpha]$ and the classes of matrices $C \in \mathrm{SL}(2,\mathbb{Z})$ with trace $\mathrm{Tr}(C) = \mathrm{Tr}(A)$, considered up to conjugacy in $\mathrm{GL}(2,\mathbb{Z})$.

The order $\mathbb{Z}[\alpha]$ is sometimes (though not always) the ring of integers of a real quadratic field. Specifically, set $D_A = \mathrm{Tr}(A)^2 - 4$ for odd $\mathrm{Tr}(A)$, and $D_A = \frac{1}{4}\mathrm{Tr}(A)^2 - 1$ for even $\mathrm{Tr}(A)$, respectively. If D_A is square-free, then $\mathbb{Z}[\alpha]$ is the ring of integers $\mathcal{O}_{\sqrt{D_A}}$ of the real quadratic field $\mathbb{Q}(\sqrt{D_A})$.

For any $\mathrm{SL}(2,\mathbb{Z})$ matrix C having trace $\mathrm{Tr}(A)$, one defines an ideal of $\mathbb{Z}[\alpha]$ as follows. Consider an eigenvector (u_1, u_2) of C associated to the eigenvalue α, which could be chosen to lie within $\mathbb{Z}[\alpha] \times \mathbb{Z}[\alpha]$. Therefore $\{u_1, u_2\}$ form the basis of an ideal $I(C) \subset \mathbb{Z}[\alpha]$. Conversely, the choice of a basis of an ideal $I \subset \mathbb{Z}[\alpha]$ determines a matrix $C(I) \in \mathrm{SL}(2,\mathbb{Z})$ corresponding to the multiplication by α. This matrix is uniquely determined by I, up to conjugacy in $\mathrm{GL}(2,\mathbb{Z})$.

In the ideal class group $\mathcal{I}(M_A)$ of $\mathbb{Z}[\alpha]$, two ideals I and J are identified if there exist nonzero elements $v, w \in \mathbb{Z}[\alpha]$ such that $vI = wJ$. Further, if $B = UCU^{-1}$, with $U \in \mathrm{GL}(2,\mathbb{Z})$, then the ideals $I(B)$ and $I(C)$ are equivalent. Therefore the class of $I(C)$ is well-defined in $\mathcal{I}(M_A)$, independently on the representative C in its conjugacy class.

Now recall that two torus bundles M_A and M_B are homeomorphic if and only if their fundamental groups are isomorphic, since they are aspherical. According to Proposition 1.2 this corresponds to the fact that A is conjugate to B or to B^{-1} within $\mathrm{GL}(2,\mathbb{Z})$. If we take into account the involution $B \to B^{-1}$, we obtain the first claim of the Corollary 1.2. Dedekind's Theorem states the finiteness of the ideal class group and it permits to conclude.

Although the statement of Proposition 1.2 was only stated for hyperbolic matrices A and B this extends naturally to all matrices from $\mathrm{SL}(2,\mathbb{Z})$.

Stronger results dues to Platonov and Rapinchuk (see [57; 62; 58, Section 8.8.5]) show that the number of classes in an arithmetic group belonging to the same G–genus (where G is a connected linear algebraic group defined over $\mathbb{Q}$) is finite and unbounded. In particular, the number of classes in $\mathcal{X}^{\mathrm{TV}}(M)$ is unbounded. This settles Corollary 1.3.

7.5 Proof of Corollary 1.4

Manifolds as in the statement of Theorem 1.1, or those arising in Corollary 1.3, have isomorphic pro-finite fundamental groups, since the pro-finite completion of Γ_A is determined by the conjugacy class of the subgroup $\langle A\rangle$ in $\mathrm{GL}(2,\widehat{\mathbb{Z}})$, where $\widehat{\mathbb{Z}}$ denotes the pro-finite completion of $\mathbb{Z}$.

But this is also a consequence of the fact that quantum invariants associated to finite groups determine the pro-finite completions of closed 3–manifolds. Specifically, for every finite group F there is associated a modular category whose associated invariants are the so-called Dijkgraaf–Witten invariants (see eg [72]). The simplest of them is the untwisted Dijkgraaf–Witten invariant RT_F given by the following explicit counting formula in terms of the fundamental group of the closed 3–manifold M (according to Turaev [72], or Freed and Quinn [25, (5.14)]):

$$\mathrm{RT}_F(M)=\frac{1}{|F|}|\mathrm{Hom}(\pi_1(M),F)|. \tag{129}$$

We have now the following easy lemma:

Lemma 7.10 *Let Γ_1 and Γ_2 be finitely generated groups such that:*

$$|\mathrm{Hom}(\Gamma_1,F)|=|\mathrm{Hom}(\Gamma_2,F)| \tag{130}$$

holds for any finite group F. Then the sets of finite quotients of Γ_1 and Γ_2, respectively, coincide.

Recall that the pro-finite completions of two finitely generated groups are isomorphic as topological groups if and only if the sets of their finite quotients are the same (see Dixon, Formanek, Poland and Ribes [17]). However, two pro-finite completions are isomorphic as topological groups if and only if they are isomorphic as discrete groups, because finite index subgroups in pro-finite groups are open, according to a fundamental result of Nikolov and Segal ([54] and the discussion in [17]). This settles Corollary 1.4.

Proof of Lemma 7.10 Let $\mathrm{Hom}^{\mathrm{surj}}(\Gamma,F)$ denotes the set of surjective homomorphisms between the groups Γ and F. We claim first that, under the assumptions of the lemma, we have for any finite group F the equality:

$$|\mathrm{Hom}^{\mathrm{surj}}(\Gamma_1,F)|=|\mathrm{Hom}^{\mathrm{surj}}(\Gamma_2,F)| \tag{131}$$

Otherwise, pick some F for which the claim above is false and such that F is a minimal group, with respect to the inclusion, with this property. Then F is nontrivial and

$$|\mathrm{Hom}^{\mathrm{surj}}(\Gamma_1, F)| \neq |\mathrm{Hom}^{\mathrm{surj}}(\Gamma_2, G)|. \tag{132}$$

By the induction hypothesis we have

$$|\mathrm{Hom}^{\mathrm{surj}}(\Gamma_1, G)| = |\mathrm{Hom}^{\mathrm{surj}}(\Gamma_2, G)| \tag{133}$$

for any subgroup $G \subset F$ such that $G \neq F$. However, we also have

$$|\mathrm{Hom}(\Gamma_i, F)| = \sum_{G \subset F} |\mathrm{Hom}^{\mathrm{surj}}(\Gamma_i, G)|. \tag{134}$$

The inequality above implies then

$$|\mathrm{Hom}(\Gamma_1, F)| \neq |\mathrm{Hom}(\Gamma_2, G)| \tag{135}$$

contradicting our assumptions. This proves the claim.

Finally, note that F is a finite quotient of the group Γ_i if and only if $|\mathrm{Hom}^{\mathrm{surj}}(\Gamma_i, F)| \neq 0$. Then the claim above implies that the set of finite quotients of the groups Γ_i should coincide. □

7.6 Proof of Proposition 1.4

Let G be the fundamental group of a closed orientable irreducible SOL manifold M. Then G is solvable and, according to a result of Evans and Moser (see [22, Theorem 5.2]), G is polycyclic.

Consider the fundamental group H of a closed 3–manifold whose class is in $\mathcal{X}^{\mathrm{TV}}(M)$. According to Lemma 7.10 the finite quotients of H coincide with the finite quotients of G. Moreover, by classical results of Hempel and Perelman's solution to the geometrization conjecture the 3–manifold groups are residually finite. Sabbagh and Wilson have proved in [66] that any residually finite group H having the same quotients as a polycyclic group is also polycyclic. In particular H is polycyclic. Now the finiteness statement is a consequence of a deep theorem of Grunewald, Pickel and Segal (see [36]), which states that the number of polycyclic groups with the same pro-finite completion is finite.

8 Comments

8.1 Higher genus

A direct extension of these results to higher genus surface bundles does not seem to work. In the case of the closed torus the kernel of all modular representations of level k

is a congruence subgroup of level k and hence strictly larger than the normal subgroup generated by the k^{th} powers of Dehn twists. In higher genus one expects the kernel of SU(2) quantum representation to be precisely the normal subgroup generated by the k^{th} powers of Dehn twists.

The first case to analyze is the mapping class group of the 1–punctured torus $\mathcal{M}_1^1$ (isomorphic to $\mathrm{SL}(2,\mathbb{Z})$). Its quantum representations are known to not always be congruence. Moreover, the kernel of the quantum SU(2)–representations (where the puncture is colored with every possible color) is now the subgroup $\mathcal{M}_1^1[k]$ generated by the k^{th} powers of Dehn twists (see Funar and Kohno [30], and Masbaum [47]). The following shows that the analog of Proposition 1.3 does not hold:

Proposition 8.1 *If two matrices $A, B \in \mathrm{SL}(2,\mathbb{Z}) = \mathcal{M}_1^1$ are conjugate in each quotient $\mathcal{M}_1^1/\mathcal{M}_1^1[k]$ then A and B are conjugate in $\mathrm{SL}(2,\mathbb{Z})$.*

Proof Let F be a finite quotient of $\mathrm{SL}(2,\mathbb{Z})$. Then the image of the Dehn twist corresponding to a parabolic in $\mathrm{SL}(2,\mathbb{Z})$ is of finite order, say k. The Dehn twists on Σ_1^1 are conjugate so that F is a quotient of $\mathcal{M}_1^1/\mathcal{M}_1^1[k]$. This implies that the images of A and B are conjugate in any finite quotient F. According to Stebe (see [68]) the group $\mathrm{SL}(2,\mathbb{Z})$ is conjugacy separable and this implies that A and B are conjugate. □

8.2 Equivalence relations on 3–manifolds

There are some natural equivalence relations on the set of closed 3–manifolds, which are inspired by the present constructions. At first there is Lackenby's congruence relation from the introduction. Further, two manifolds are said to be Turaev–Viro equivalent if their Turaev–Viro invariants agree for every spherical fusion category. From [34; 43] one derives that congruent manifolds are also Turaev–Viro equivalent and we don't know if the converse also holds. It would be interesting to find examples of non-homeomorphic congruent hyperbolic 3–manifolds, if they exist.

Appendix: Counting matrices in a given genus

For $t \in \mathbb{Z}$, we let

$$\mathcal{M}_t = \{A \in \mathrm{SL}(2,\mathbb{Z}) \mid \mathrm{tr}(A) = t\},$$

and let $\mathcal{X}_t$ denote the set of $\mathrm{GL}(2,\mathbb{Z})$–conjugacy classes of matrices in $\mathcal{M}_t$. We define the *discriminant* of $A \in \mathcal{M}_t$ to be

$$D = D(t) = \begin{cases} t^2 - 4 & \text{for } t \text{ even,} \\ t^2/4 - 1 & \text{for } t \text{ odd.} \end{cases}$$

Furthermore, the *genus* $\mathfrak{G}(A)$ of $A \in \mathcal{M}_t$ is the set of $B \in \mathrm{SL}(2,\mathbb{Z})$ that are conjugate to A in $\mathrm{SL}(2,\widehat{\mathbb{Z}})$ where $\widehat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$ (we note that obviously $\mathfrak{G}(A) \subset \mathcal{M}_t$). Equivalently, $B \in \mathfrak{G}(A)$ if the images of A and B are conjugate in $\mathrm{SL}(2,\mathbb{Z}/m\mathbb{Z})$ for all $m > 1$. It may appear that to comply with the general definition of genus adopted in Platonov and Rapinchuk [58, Section 8.5], we would also need to require that B must also be conjugate to A in $\mathrm{SL}(2,\mathbb{Q})$, but here this condition follows automatically from local conjugacy in view of the Hasse norm theorem for quadratic extensions. On the other hand, one can consider a variation of this definition of genus by requiring that the images of A and B in $\mathrm{SL}(2,\mathbb{Z}/m\mathbb{Z})$ be conjugate in $\mathrm{SL}^{\pm}(2,\mathbb{Z}/m\mathbb{Z})$, the group of matrices over $\mathbb{Z}/m\mathbb{Z}$ with determinant ± 1, for all $m > 1$; the genus of A thus defined will be denoted by $\mathfrak{G}^{\pm}(A)$. Finally, we let $\mathfrak{A}(A)$ denote the set of $\mathrm{SL}(2,\mathbb{Z})$–conjugacy classes in $\mathfrak{G}(A)$.

Our main result is the following.

Theorem A.1 *There exists an increasing sequence of integers $\{t_n\}$ such that:*

(i) *$D_n := D(t_n)$ is square-free for all n.*

(ii) *We have:*

$$\max_{A\in\mathcal{M}_{t_n}} |\mathfrak{A}(A)| \geqslant 0.1023\cdot 10^{-4}\cdot D_n^{0.49}\frac{1}{2\log 2+\log(D_n+2)} \tag{136}$$

and therefore $\max_{A\in\mathcal{M}_{t_n}} |\mathfrak{A}(A)| \longrightarrow \infty$ as $n\to\infty$.

(iii) *We have*

$$\frac{\max_{A\in\mathcal{M}_{t_n}} |\mathfrak{A}(A)|}{|\mathcal{X}_{t_n}|} \geqslant \frac{1}{64}. \tag{137}$$

In particular,

$$\limsup_{t\to\infty}\frac{1}{|\mathcal{X}_t|}\max_{A\in\mathcal{M}_t}|\mathfrak{A}(A)| \geqslant \frac{1}{64}. \tag{138}$$

According to Propositions 1.1 and 1.2 above, matrices $A_1, A_2 \in \mathfrak{G}(A)$ such that neither of $A_1^{\pm 1}$ and $A_2^{\pm 1}$ are conjugate in $\mathrm{GL}(2,\mathbb{Z})$ (we will call such matrices *strongly non-conjugate*) give rise to nonhomeomorphic torus bundles having the same quantum invariants. This, in particular, yields nonisomorphic 3–manifold groups having the same profinite completion, answering the Grothendieck-type question raised in Long and Reid [46]. Theorem A.1 above implies an asymptotic lower bound on the size of a set of *pairwise* strongly non-conjugate matrices in a genus inquired about in the paper above, which gives an effective version of Corollary 1.3. This effective version is closely related to the more general results of the second author from Prasad and

Rapinchuk [59; 60]. The proof below is based on the (well-known) connection between the conjugacy of 2×2 matrices and the equivalence of binary quadratic forms (see Cassels [10]), although one can also give a direct argument.

Proof Assume henceforth that $|t|\geq 3$ and set $D=D(t)$. First, we prove the following result about the number of genera, which is based on the analysis of local conjugacy (it should be noted that there are easy algorithms to determine if two matrices in $\mathrm{SL}(n,\mathbb{Z}_p)$ are conjugate, for any n (see Appelgate and Onishi [1]), but all we need for $n=2$ is the classical result about binary quadratic forms).

Proposition A.2 *Let $D=2^m p_1^{r_1}p_2^{r_2}\cdots p_n^{r_n}$ be the prime factorization of D.*

(i) *The number of distinct genera $\mathfrak{G}(A)$ contained in $\mathcal{M}_t$ is*

$$s(t)=2^{n+\nu(D)}\cdot\tau(D)$$

where $\tau(D)$ is the number of divisors of D and

$$\nu(D)=\begin{cases}0 & \text{if } D\equiv 1 \pmod 2,\\ 0 & \text{if } D=4d,\ d\equiv 1 \pmod 4,\\ 2 & \text{if } D\equiv 0 \pmod{32},\\ 1 & \text{otherwise.}\end{cases}$$

(Note that $2^{n+\nu(D)}$ is the number of genera of primitive binary quadratic forms of discriminant D.)

(ii) *The number of distinct genera $\mathfrak{G}^{\pm}(A)$ in $\mathcal{M}_t$ is*

$$s_{\pm}(t)=2^{n_1+\nu(D)}\cdot\tau(D)$$

where $\tau(D)$ and $\nu(D)$ are the same as above and n_1 is the number of odd prime factors $p_i\equiv 1 \pmod 4$.

Proof For a matrix

$$A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$$

that is not scalar, one defines the *Jorgensen invariant* to be

$$J(A)=\gcd(a-d,b,c).$$

As pointed out in Traina [71], $J(A)$ is an invariant of the conjugacy class of A.

Furthermore, if one associates to the matrix A the primitive bilinear form

$$\frac{\mathrm{sgn}(\mathrm{tr}(A))}{J(A)}(bx^2-(a-d)xy-cy^2),$$

then conjugacy classes in $\mathrm{SL}(2,\mathbb{Z})$ will correspond to equivalence classes of bilinear forms.

Then $J(A)$ can take $\tau(D)$ distinct values. Moreover the number of genera of primitive bilinear forms over $\mathbb{Z}$ was basically computed by Gauss [32]; see [10, Chapter 14, Section 3, pages 339–340, Lemmas 3.1–3.3] for a modern treatment. The case of improper equivalence classes is similar. □

Denote by ω the element

$$\omega = \begin{cases} \dfrac{1+\sqrt{D}}{2} & \text{for odd } t, \\ \sqrt{D} & \text{for even } t. \end{cases} \tag{139}$$

According to the Latimer–MacDuffee–Taussky correspondence (see Newman [52]) there is a bijection between the elements of $\mathcal{X}_t$ and the ideal class group $\mathcal{I}(\mathbb{Z}[\omega])$ of the order $\mathbb{Z}[\omega]$. Denote then by $h(D) = |\mathcal{I}(\mathbb{Z}[\omega])|$ the class number of $\mathbb{Z}[\omega]$. Notice that $\mathbb{Z}[\omega]$ might not be the maximal order in $\mathbb{Q}(\sqrt{D})$ unless D is square-free.

Therefore there exists some $A \in \mathcal{M}_t$ such that the number of conjugacy classes in $\mathfrak{A}(A)$ is at least:

$$N(t) = 2^{-s(t)} h(D) \tag{140}$$

According to a celebrated theorem of Jing Run Chen (see [11]) revisited by Halberstam (see [38]) and Richert (see [65, Theorem 13.2]) there exist infinitely many primes p_n such that $p_n + 4$ has at most two factor primes. Assuming that $p_n > 5$ the two factor primes have to be distinct and different from p_n. If we set $t_n = p_n + 2$ then $D_n = t_n^2 - 4$ are odd square-free and have at most 3 prime divisors (counted with their multiplicities). In particular $h(D_n) = h_{D_n}$ where this time h_D denotes the class number of the quadratic field $\mathbb{Q}(\sqrt{D})$ (namely of its ring of integers).

It remains to prove that for this subsequence we also have $\limsup h(D_n) = \infty$. This is already classical. Indeed the Dirichlet class number formula for real quadratic fields reads:

$$h_d = \frac{1}{2\log \epsilon_D} \sqrt{d} \cdot L(1, \chi_d), \tag{141}$$

where $d = 4^{\delta_D} D$ is the discriminant of $\mathbb{Q}(\sqrt{D})$, ϵ_D is the fundamental unit, χ_d is the mod d Dirichlet primitive character and $L(\cdot, \chi_d)$ the associated L–series. In our case $D_n \equiv 1 \pmod 4$ so that $\delta_{D_n} = 0$ and the fundamental unit is $\epsilon_D = (t + \sqrt{D})/2$ if $D = t^2 - 4$. Thus $\epsilon_D < 2\sqrt{D+2}$.

The Tatuzawa effective version of Siegel's Theorem (see [70, Theorem 2]) states the following lower bound for the L–series:

$$L(1,\chi_d) > 0.655 \cdot \frac{s^{-1}}{d^{1/s}} \tag{142}$$

for all $d \geq \max(\exp(s), \exp(11.2))$ with one possible exception and all $s > 2$. Consider $s = 100$ and t_n large enough for which the inequality above holds. This gives our estimate. □

Remark A.1 The congruence subgroup property implies that the estimates of Theorem A.1 also hold in $\mathrm{SL}(n,\mathbb{Z})$, with $n \geq 3$, by considering matrices of the form $A \oplus \mathbb{1}_{n-2}$, with $A \in \mathrm{SL}(2,\mathbb{Z})$.

References

[1] **H Appelgate**, **H Onishi**, *Similarity problem over* $\mathrm{SL}(n, \mathbf{Z}_p)$, Proc. Amer. Math. Soc. 87 (1983) 233–238 MR681827

[2] **M Atiyah**, *The logarithm of the Dedekind η–function*, Math. Ann. 278 (1987) 335–380 MR909232

[3] **B Bakalov**, **A Kirillov, Jr**, *Lectures on tensor categories and modular functors*, University Lecture Series 21, Amer. Math. Soc. (2001) MR1797619

[4] **P Bantay**, *The kernel of the modular representation and the Galois action in RCFT*, Comm. Math. Phys. 233 (2003) 423–438 MR1962117

[5] **T Barbot**, *Extensions de $\mathbb{Z} \oplus \mathbb{Z}$ par $\mathbb{Z}$*, Mémoire DEA, ENS Lyon, UMPA (1990)

[6] **J W Barrett**, **B W Westbury**, *Invariants of piecewise-linear 3–manifolds*, Trans. Amer. Math. Soc. 348 (1996) 3997–4022 MR1357878

[7] **A I Borevich**, **I R Shafarevich**, *Number theory*, Pure and Applied Mathematics 20, Academic Press, New York (1966) MR0195803

[8] **M R Bridson**, **S M Gersten**, *The optimal isoperimetric inequality for torus bundles over the circle*, Quart. J. Math. Oxford Ser. 47 (1996) 1–23 MR1380947

[9] **D Calegari**, **M H Freedman**, **K Walker**, *Positivity of the universal pairing in 3 dimensions*, J. Amer. Math. Soc. 23 (2010) 107–188 MR2552250

[10] **J W S Cassels**, *Rational quadratic forms*, London Mathematical Society Monographs 13, Academic Press, London (1978) MR522835

[11] **J R Chen**, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica 16 (1973) 157–176 MR0434997

[12] **H Cohn**, *A classical invitation to algebraic numbers and class fields*, Springer, New York (1978) MR506156 with an appendix by O Taussky-Todd

[13] **A Coste**, **T Gannon**, *Congruence subgroups and rational conformal field theory* arXiv:math/9909080

[14] **F Deloup**, *Linking forms, reciprocity for Gauss sums and invariants of* 3*–manifolds*, Trans. Amer. Math. Soc. 351 (1999) 1895–1918 MR1603898

[15] **F Deloup**, *An explicit construction of an abelian topological quantum field theory in dimension* 3, from: "Proceedings of the Pacific Institute for the Mathematical Sciences workshop "Invariants of three-manifolds"", (J Bryden, editor), Topology Appl. 127 (2003) 199–211 MR1953327

[16] **F Deloup**, **C Gille**, *Abelian quantum invariants indeed classify linking pairings*, from: "Proceedings of the conference Knots in Hellas '98, Vol. 2", (C M Gordon, V F R Jones, L H Kauffman, S Lambropoulou, J H Przytycki, editors), J. Knot Theory Ramifications 10 (2001) 295–302 MR1822493

[17] **J D Dixon**, **E W Formanek**, **J C Poland**, **L Ribes**, *Profinite completions and isomorphic finite quotients*, J. Pure Appl. Algebra 23 (1982) 227–231 MR644274

[18] **C Dong**, **X Lin**, **S-H Ng**, *Congruence property in conformal field theory* arXiv:1201.6644

[19] **W Eholzer**, *On the classification of modular fusion algebras*, Comm. Math. Phys. 172 (1995) 623–659 MR1354262

[20] **P Etingof**, *On Vafa's theorem for tensor categories*, Math. Res. Lett. 9 (2002) 651–657 MR1906068

[21] **P Etingof**, **D Nikshych**, **V Ostrik**, *On fusion categories*, Ann. of Math. 162 (2005) 581–642 MR2183279

[22] **B Evans**, **L Moser**, *Solvable fundamental groups of compact* 3*–manifolds*, Trans. Amer. Math. Soc. 168 (1972) 189–210 MR0301742

[23] **H G Feichtinger**, **M Hazewinkel**, **N Kaiblinger**, **E Matusiak**, **M Neuhauser**, *Metaplectic operators on* $\mathbb{C}^n$, Q. J. Math. 59 (2008) 15–28 MR2392499

[24] **É Fouvry**, **J Klüners**, *The parity of the period of the continued fraction of* $\sqrt{d}$, Proc. Lond. Math. Soc. 101 (2010) 337–391 MR2679695

[25] **D S Freed**, **F Quinn**, *Chern–Simons theory with finite gauge group*, Comm. Math. Phys. 156 (1993) 435–472 MR1240583

[26] **M H Freedman**, **V Krushkal**, *On the asymptotics of quantum* SU(2) *representations of mapping class groups*, Forum Math. 18 (2006) 293–304 MR2218422

[27] **L Funar**, *Représentations du groupe symplectique et variétés de dimension* 3, C. R. Acad. Sci. Paris Sér. I Math. 316 (1993) 1067–1072 MR1222974

[28] **L Funar**, *Theta functions, root systems and* 3*–manifold invariants*, J. Geom. Phys. 17 (1995) 261–282 MR1358739

[29] **L Funar**, *Some abelian invariants of* 3*–manifolds*, Rev. Roumaine Math. Pures Appl. 45 (2000) 825–861 MR1865997

[30] **L Funar**, **T Kohno**, *On Burau representations at roots of unity*, to appear in Geometriae Dedicata (2013) `arXiv:0907.0568`

[31] **T Gannon**, *Modular data: the algebraic combinatorics of conformal field theory*, J. Algebraic Combin. 22 (2005) 211–250 MR2164398

[32] **C F Gauss**, *Disquisitiones arithmeticae*, Yale University Press, New Haven, Conn. (1966) MR0197380

[33] **E Ghys**, **V Sergiescu**, *Stabilité et conjugaison différentiable pour certains feuilletages*, Topology 19 (1980) 179–197 MR572582

[34] **P M Gilmer**, *Congruence and quantum invariants of* 3*–manifolds*, Algebr. Geom. Topol. 7 (2007) 1767–1790 MR2366177

[35] **T Gocho**, *The topological invariant of three-manifolds based on the* U(1) *gauge theory*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 39 (1992) 169–184 MR1157982

[36] **F J Grunewald**, **P F Pickel**, **D Segal**, *Polycyclic groups with isomorphic finite quotients*, Ann. of Math. 111 (1980) 155–195 MR558400

[37] **A J Hahn**, **O T O'Meara**, *The classical groups and K–theory*, Grundl. Math. Wissen. 291, Springer, Berlin (1989) MR1007302

[38] **H Halberstam**, *A proof of Chen's theorem*, from: "Journées Arithmétiques de Bordeaux", Astérisque 24–25, Soc. Math. France, Paris (1975) 281–293 MR0389815

[39] **L C Jeffrey**, *Chern–Simons–Witten invariants of lens spaces and torus bundles, and the semiclassical approximation*, Comm. Math. Phys. 147 (1992) 563–604 MR1175494

[40] **N Kaiblinger**, **M Neuhauser**, *Metaplectic operators for finite abelian groups and* $\mathbb{R}^d$, Indag. Math. 20 (2009) 233–246 MR2599814

[41] **J Kania-Bartoszynska**, *Examples of different* 3*–manifolds with the same invariants of Witten and Reshetikhin–Turaev*, Topology 32 (1993) 47–54 MR1204405

[42] **R Kirby**, **P Melvin**, *Dedekind sums, μ–invariants and the signature cocycle*, Math. Ann. 299 (1994) 231–267 MR1275766

[43] **M Lackenby**, *Fox's congruence classes and the quantum-*SU(2) *invariants of links in* 3*–manifolds*, Comment. Math. Helv. 71 (1996) 664–677 MR1420515

[44] **M Larsen**, **Z Wang**, *Density of the* SO(3) *TQFT representation of mapping class groups*, Comm. Math. Phys. 260 (2005) 641–658 MR2183960

[45] **W B R Lickorish**, *Distinct* 3*–manifolds with all* $\mathrm{SU}(2)_q$ *invariants the same*, Proc. Amer. Math. Soc. 117 (1993) 285–292 MR1129882

[46] **D D Long**, **A W Reid**, *Grothendieck's problem for* 3*–manifold groups*, Groups Geom. Dyn. 5 (2011) 479–499 MR2782181

[47] **G Masbaum**, *On representations of mapping class groups in integral TQFT*, Oberwolfach Reports 5 (2008) 1202–1205

[48] **W Meyer**, *Die Signatur von Flächenbündeln*, Math. Ann. 201 (1973) 239–264 MR0331382

[49] **R A Mollin**, *Fundamental number theory with applications*, 2nd edition, Discrete Mathematics and its Applications, Chapman & Hall/CRC, Boca Raton (2008) MR2404578

[50] **M Müger**, *From subfactors to categories and topology, II: the quantum double of tensor categories and subfactors*, J. Pure Appl. Algebra 180 (2003) 159–219 MR1966525

[51] **H Murakami**, **T Ohtsuki**, **M Okada**, *Invariants of three-manifolds derived from linking matrices of framed links*, Osaka J. Math. 29 (1992) 545–572 MR1181121

[52] **M Newman**, *Integral matrices*, Pure and Applied Mathematics 45, Academic Press, New York (1972) MR0340283

[53] **S-H Ng**, **P Schauenburg**, *Congruence subgroups and generalized Frobenius–Schur indicators*, Comm. Math. Phys. 300 (2010) 1–46 MR2725181

[54] **N Nikolov**, **D Segal**, *On finitely generated profinite groups, I: strong completeness and uniform bounds*, Ann. of Math. 165 (2007) 171–238 MR2276769

[55] **I Niven**, **H S Zuckerman**, **H L Montgomery**, *An introduction to the theory of numbers*, 5th edition, John Wiley & Sons, New York (1991) MR1083765

[56] **P F Pickel**, *Finitely generated nilpotent groups with isomorphic finite quotients*, Trans. Amer. Math. Soc. 160 (1971) 327–341 MR0291287

[57] **V Platonov**, *On the genus problem in arithmetic groups*, Dokl. Akad. Nauk SSR 200 (1971) 793–796 In Russian; translated in Soviet. Math. Dokl. 12 (1975), 1503–1507

[58] **V Platonov**, **A Rapinchuk**, *Algebraic groups and number theory*, Pure and Applied Mathematics 139, Academic Press, Boston, MA (1994) MR1278263

[59] **G Prasad**, **A Rapinchuk**, *Weakly commensurable arithmetic groups and isospectral locally symmetric spaces*, Publ. Math. IHÉS (2009) 113–184 MR2511587

[60] **G Prasad**, **A Rapinchuk**, *Number-theoretic techniques in the theory of Lie groups and differential geometry*, from: "Fourth International Congress of Chinese Mathematicians", (L Ji, K Liu, L Yang, S-T Yau, editors), AMS/IP Stud. Adv. Math. 48, Amer. Math. Soc. (2010) 231–250 MR2744224

[61] **H Rademacher**, **E Grosswald**, *Dedekind sums*, The Carus Mathematical Monographs 16, The Mathematical Association of America, Washington, DC (1972) MR0357299

[62] **A Rapinchuk**, *Platonov's conjecture on genus in arithmetic groups*, Dokl. Akad. Nauk BSSR 25 (1981) 101–104, 187 MR613414 In Russian; translated in Amer. Math. Soc. Translations–Series 2 128 (1986), 117–122

[63] **L Redei**, **H Reichardt**, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. 170 (1933) 69–74

[64] **N Reshetikhin**, **V G Turaev**, *Invariants of 3–manifolds via link polynomials and quantum groups*, Invent. Math. 103 (1991) 547–597 MR1091619

[65] **H-E Richert**, *Lectures on sieve methods*, Lectures on Mathematics and Physics 55, Bombay: Tata Institute of Fundamental Research (1976)

[66] **G Sabbagh**, **J S Wilson**, *Polycyclic groups, finite images, and elementary equivalence*, Arch. Math. (Basel) 57 (1991) 221–227 MR1119894

[67] **P Sarnak**, *Reciprocal geodesics*, from: "Analytic number theory", (W Duke, Y Tschinkel, editors), Clay Math. Proc. 7, Amer. Math. Soc. (2007) 217–237 MR2362203

[68] **P F Stebe**, *Conjugacy separability of groups of integer matrices*, Proc. Amer. Math. Soc. 32 (1972) 1–7 MR0289666

[69] **P Stevenhagen**, *The number of real quadratic fields having units of negative norm*, Experiment. Math. 2 (1993) 121–136 MR1259426

[70] **T Tatuzawa**, *On a theorem of Siegel*, Jap. J. Math. 21 (1951) 163–178 MR0051262

[71] **C Traina**, *A note on trace equivalence in* $\mathrm{PSL}(2,\mathbf{Z})$, Rend. Istit. Mat. Univ. Trieste 26 (1994) 233–237 MR1363921

[72] **V G Turaev**, *Quantum invariants of knots and 3–manifolds*, de Gruyter Studies in Mathematics 18, Walter de Gruyter & Co, Berlin (1994) MR1292673

[73] **V G Turaev**, **A Virelizier**, *On two approaches to 3–dimensional TQFTs* `arXiv:1006.3501`

[74] **V G Turaev**, **O Y Viro**, *State sum invariants of 3–manifolds and quantum 6j–symbols*, Topology 31 (1992) 865–902 MR1191386

[75] **C Vafa**, *Toward classification of conformal theories*, Phys. Lett. B 206 (1988) 421–426 MR944264

[76] **F Xu**, *Some computations in the cyclic permutations of completely rational nets*, Comm. Math. Phys. 267 (2006) 757–782 MR2249790

Institut Fourier, University of Grenoble I
BP 74, UMR 5582, 38402 Saint-Martin d'Hères cedex, France

Department of Mathematics, University of Virginia
141 Cabell Drive, Kerchof Hall, PO Box 400137, Charlottesville, VA 22904-4137, USA

`louis.funar@ujf-grenoble.fr, asr3x@virginia.edu`

`http://www-fourier.ujf-grenoble.fr/~funar,`
`http://pi.math.virginia.edu/Faculty/Rapinchuk/`

Proposed: Vaughan Jones Received: 3 March 2011
Seconded: Cameron Gordon, Peter Teichner Revised: 23 April 2013