Quantum Topol. 5 (2014), 225–258
DOI 10.4171/QT/51

Quantum Topology

Irreducible factors of modular representations of mapping class groups arising in Integral TQFT

Patrick M. Gilmer and Gregor Masbaum[1]

Abstract. We find decomposition series of length at most two for modular representations in positive characteristic of mapping class groups of surfaces induced by an integral version of the Witten–Reshetikhin–Turaev SO(3)-TQFT at the p-th root of unity, where p is an odd prime. The dimensions of the irreducible factors are given by Verlinde-type formulas.

Mathematics Subject Classification (2010). Primary 57R56; Secondary 57M99.

Keywords. Lollipop basis, Topological Quantum Field Theory, skein theory, symplectic group, Verlinde formula.

Contents

1. Introduction

The Witten–Reshetikhin–Turaev quantum invariants of 3-manifolds fit into a Topological Quantum Field Theory (TQFT) in the sense of Atiyah and Segal. This means in particular that they give rise to finite-dimensional complex representations of (certain central extensions of) mapping class groups of surfaces. While these *quantum*

[1]The first author was partially supported by NSF-DMS-0905736.

representations of mapping class groups are in general not irreducible (some decompositions into invariant subspaces were already described in Blanchet *et al.* [4]), it was shown by Roberts [17] that in the case of surfaces without boundary, the representations arising from the SU(2)-theory at level k are irreducible provided $k = p-2$ where p is a prime. This irreducibility plays an important role in Andersen's work on whether mapping class groups have Kazhdan's property T [1].

It is a well-known phenomenon in representation theory that "natural" representations of a group can often be defined both in characteristic zero and in positive characteristic. Typically, though, a representation which is irreducible in characteristic zero gives rise in positive characteristic to a representation which may no longer be irreducible. It is the purpose of this paper to study this question for mapping class group representations coming from a TQFT. Specifically, we consider the SO(3)-TQFT at a primitive p-th root of unity, where $p \geq 5$ is a prime, because the theory of *Integral TQFT* developed in Gilmer [5] and Gilmer and Masbaum [6] and [7] implies that this TQFT gives rise in a natural way to modular representations of mapping class groups in positive characteristic. We remark that modular representations in characteristic different from p coming from this SO(3)-TQFT at the p-th root of unity were recently used in work of A. Reid and the second author [15]. But here we will mainly study the modular representations in characteristic p coming from this theory. We will show that these representations often have a nontrivial composition series with interesting irreducible factors.

2. Statement of the main results

Throughout the paper, we fix a prime $p \geq 5$, and let ζ_p be a primitive p-th root of unity. We denote the corresponding ring of cyclotomic integers by

$$\mathcal{O} = \mathbb{Z}[\zeta_p] .$$

The theory of Integral SO(3)-TQFT developed in [5], [6], and [7] associates to a compact oriented surface Σ a free $\mathcal{O}$-lattice (*i.e.,* a free $\mathcal{O}$-module of finite rank) carrying a representation of an appropriate central extension of the orientation-preserving mapping class group of the surface. This theory may be thought of as an integral refinement of the Reshetikhin–Turaev TQFT associated with the Lie group SO(3), a version of which would be obtained if one extends coefficients from $\mathcal{O}$ to the cyclotomic field $\mathbb{Q}(\zeta_p)$. In this paper, we write $\mathcal{S}(\Sigma)$ for the Integral TQFT-lattice associated to Σ. We shall review the definition of $\mathcal{S}(\Sigma)$ in §4. We write Γ_Σ for the mapping class group of the surface, and $\widetilde{\Gamma}_\Sigma^{++}$ for the central extension of Γ_Σ which we will use. Here we follow the construction of $\widetilde{\Gamma}_\Sigma^{++}$ given in our paper [8]. The group $\widetilde{\Gamma}_\Sigma^{++}$ is a central extension of Γ_Σ by $\mathbb{Z}$. It is generated by certain specific lifts of Dehn twists, and we will describe in Proposition 4.2 how such a lift of a Dehn twist acts on $\mathcal{S}(\Sigma)$. It will not be necessary to know more about $\widetilde{\Gamma}_\Sigma^{++}$ in this paper.

For every ideal $I \subset \mathcal{O}$, we have an induced representation of $\widetilde{\Gamma}_\Sigma^{++}$ on the $\mathcal{O}/I$-module $\mathcal{S}(\Sigma)/I\mathcal{S}(\Sigma)$. In this way, we can get modular representations of $\widetilde{\Gamma}_\Sigma^{++}$, namely when $\mathcal{O}/I$ is a finite field. We will see in Corollary 3.4 that in the case where Σ has at most one boundary component, such a modular representation, say in characteristic ℓ, is always irreducible except possibly if $\ell = p$. In this paper, however, we are interested in non-trivial decompositions of the representation. Therefore we consider the case where $I = (1-\zeta_p)$. It is well-known that this is a prime ideal in $\mathcal{O} = \mathbb{Z}[\zeta_p]$, and the quotient ring is the finite field $\mathbb{F}_p$. Thus we get a representation of $\widetilde{\Gamma}_\Sigma^{++}$ on the $\mathbb{F}_p$-vector space

$$F(\Sigma) = \mathcal{S}(\Sigma)/(1-\zeta_p)\mathcal{S}(\Sigma)\,. \tag{1}$$

This is the modular representation referred to in the title of this paper. As shown in §12 of our paper [8], it factors through a representation of the ordinary mapping class group Γ_Σ. (We shall explain the reason for this in §4.[1]) In Corollary 2.6, we will show that in the case where Σ is either closed, or has one boundary component, the modular representation $F(\Sigma)$ has a composition series with at most two irreducible factors, which we will describe explicitly and whose dimensions we will compute.

In order to state our results more precisely, recall that if Σ has boundary, the quantum representation depends on the choice of a *color* on each boundary component, and we get a representation of the mapping class group of Σ *rel. boundary* (meaning that Γ_Σ consists of orientation preserving diffeomorphisms which are the identity on the boundary, modulo isotopies which are also the identity on the boundary). In our situation, the color on the boundary can be any even integer $2c$ satisfying $0 \le 2c \le p-3$. We will indicate this in our notation by writing $\Sigma_g(2c)$ for a genus g surface with one boundary component colored $2c$. As usual in TQFT, the case $2c = 0$ corresponds to the case where Σ has empty boundary.

Convention 2.1. *Throughout most of the paper, g and c are fixed, and we simply write Σ for $\Sigma_g(2c)$.*

The lattice $\mathcal{S}(\Sigma)$ has a basis $\{\mathfrak{b}_\sigma\}$ indexed by small admissible colorings σ of the edges of a lollipop tree [6]. This is pictured in Figure 1 in the case $g = 3$.

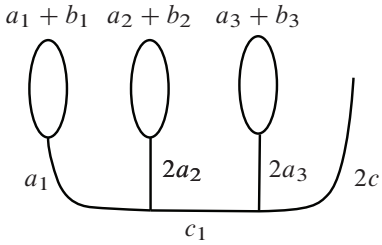


Figure 1. Lollipop tree $T_g^{(2c)}$.

[1] See footnote 11.

Here, the color $2c$ on the free (or *trunk*) edge is fixed, whereas the colors $2a_i$, $a_i + b_i$, and c_i on the other edges are numbers in $\{0, 1, \dots, p-2\}$. A coloring is *admissible* if whenever i, j and k are the colors of edges which meet at a vertex

$$i + j + k \equiv 0 \pmod 2,$$

$$|i - j| \le k \le i + j,$$

$$i + j + k \le 2p - 4.$$

A coloring is *small* if the colors $a_i + b_i$ of the loop edges satisfy $0 \le a_i + b_i \le (p-3)/2$ (see §3 of our paper [6]).

Convention 2.2. *From now on, whenever we say coloring, we mean small admissible coloring.*

Here is a crucial definition for this paper.

Definition 2.3. A coloring σ is called *even or odd* according as $c + \sum a_i$ is even or odd.[2]

We write

$$\mathcal{S}(\Sigma) = \mathcal{S}^{\mathrm{ev}}(\Sigma) \oplus \mathcal{S}^{\mathrm{odd}}(\Sigma)\,, \tag{2}$$

where $\mathcal{S}^{\mathrm{ev}}(\Sigma)$ is the submodule spanned by the $\mathfrak{b}_\sigma$ corresponding to even colorings, and $\mathcal{S}^{\mathrm{odd}}(\Sigma)$ is the submodule spanned by the $\mathfrak{b}_\sigma$ corresponding to odd colorings. Note that while $\mathcal{S}(\Sigma)$ is defined intrinsically and does not depend on the choice of the lollipop tree, the submodules $\mathcal{S}^{\mathrm{ev}}(\Sigma)$ and $\mathcal{S}^{\mathrm{odd}}(\Sigma)$ depend on this choice.

The following is the key result of this paper.

Theorem 2.4. *Let $\Sigma = \Sigma_g(2c)$. With respect to the decomposition (2), the image of the group algebra $\mathcal{O}[\widetilde{\Gamma}^{++}_\Sigma]$ in $\mathrm{End}_{\mathcal{O}}(\mathcal{S}(\Sigma))$ is*

$$\left[\begin{array}{c|c} \mathrm{End}_{\mathcal{O}}(\mathcal{S}^{\mathrm{ev}}(\Sigma)) & (1-\zeta_p)\,\mathrm{Hom}_{\mathcal{O}}(\mathcal{S}^{\mathrm{odd}}(\Sigma), \mathcal{S}^{\mathrm{ev}}(\Sigma)) \\ \hline \mathrm{Hom}_{\mathcal{O}}(\mathcal{S}^{\mathrm{ev}}(\Sigma), \mathcal{S}^{\mathrm{odd}}(\Sigma)) & \mathrm{End}_{\mathcal{O}}(\mathcal{S}^{\mathrm{odd}}(\Sigma)) \end{array}\right] \tag{3}$$

The proof of Theorem 2.4 will be given in §4–6. It has the following immediate corollary for the modular representation $F(\Sigma)$ of Γ_Σ defined in (1).

Corollary 2.5. *Let*

$$F(\Sigma) = F^{\mathrm{ev}}(\Sigma) \oplus F^{\mathrm{odd}}(\Sigma)$$

be the decomposition induced from (2). With respect to this decomposition, the image of the group algebra $\mathbb{F}_p[\Gamma_\Sigma]$ in $\mathrm{End}_{\mathbb{F}_p}(F(\Sigma))$ is

$$\left[\begin{array}{c|c} \mathrm{End}_{\mathbb{F}_p}(F^{\mathrm{ev}}(\Sigma)) & 0 \\ \hline \mathrm{Hom}_{\mathbb{F}_p}(F^{\mathrm{ev}}(\Sigma), F^{\mathrm{odd}}(\Sigma)) & \mathrm{End}_{\mathbb{F}_p}(F^{\mathrm{odd}}(\Sigma)) \end{array}\right] \tag{4}$$

[2] In the special case that $(g, c) = (2, 0)$, we take $c + \sum a_i$ to be $2a_1$.

From (4) it is easy to get a composition series for $F(\Sigma)$.

Corollary 2.6. *Let $\Sigma = \Sigma_g(2c)$. If $g \le 1$ or if $(g,c) = (2,0)$, then $F^{\mathrm{odd}}(\Sigma) = 0$ and the representation $F(\Sigma)$ is irreducible. Otherwise, $F(\Sigma)$ has a composition series with two irreducible factors: the subspace $F^{\mathrm{odd}}(\Sigma)$ is the unique irreducible subrepresentation of $F(\Sigma)$, and the quotient $F(\Sigma)/F^{\mathrm{odd}}(\Sigma)$ is again irreducible.*

We will explain how one deduces this corollary from (4) in §3.

Let us denote the dimensions of these irreducible factors by

$$\mathfrak{o}_g^{(2c)} = \dim_{\mathbb{F}_p}(F^{\mathrm{odd}}(\Sigma)) = \mathrm{rank}_{\mathcal{O}}(\mathcal{S}^{\mathrm{odd}}(\Sigma)),$$

$$\mathfrak{e}_g^{(2c)} = \dim_{\mathbb{F}_p}(F(\Sigma)/F^{\mathrm{odd}}(\Sigma)) = \mathrm{rank}_{\mathcal{O}}(\mathcal{S}^{\mathrm{ev}}(\Sigma)),$$

where $\Sigma = \Sigma_g(2c)$. These numbers are simply the numbers of odd or even colorings of the lollipop tree $T_g^{(2c)}$ shown in Figure 1. Here, the superscript indicates that the trunk color is fixed to be $2c$ in the colorings we are counting. We also define

$$D_g^{(2c)} = \mathfrak{e}_g^{(2c)} + \mathfrak{o}_g^{(2c)},$$

$$\delta_g^{(2c)} = \mathfrak{e}_g^{(2c)} - \mathfrak{o}_g^{(2c)}.$$

In the case $c = 0$ corresponding to a surface without boundary, we simply write $\mathfrak{e}_g$ for $\mathfrak{e}_g^{(0)}$, and similarly for the other numbers just defined.

We will give recursion formulas for $\mathfrak{o}_g^{(2c)}$ and $\mathfrak{e}_g^{(2c)}$ in §7, where we will also prove the following explicit expression for $\delta_g^{(2c)}$.

Theorem 2.7. *One has*

$$(-1)^c \delta_g^{(2c)} = \frac{4^{1-g}}{p} \sum_{j=1}^{(p-1)/2} \Big(\sin\frac{\pi j(2c+1)}{p}\Big)\Big(\sin\frac{\pi j}{p}\Big)\Big(\cos\frac{\pi j}{p}\Big)^{-2g}. \tag{5}$$

We think of (5) as an analog of the celebrated Verlinde formula for the dimension of the SO(3)-TQFT vector space called $V_p(\Sigma)$ in Blanchet *et al.* [4]. In our current notation, this dimension is

$$\dim V_p(\Sigma) = \mathrm{rank}_{\mathcal{O}}(\mathcal{S}(\Sigma)) = \dim_{\mathbb{F}_p}(F(\Sigma)) = \mathfrak{o}_g^{(2c)} + \mathfrak{e}_g^{(2c)} = D_g^{(2c)},$$

and the Verlinde formula (for p odd) says[3]

$$D_g^{(2c)} = \Big(\frac{p}{4}\Big)^{g-1} \sum_{j=1}^{(p-1)/2} \Big(\sin\frac{\pi j(2c+1)}{p}\Big)\Big(\sin\frac{\pi j}{p}\Big)^{1-2g}. \tag{6}$$

[3]The formula for D_g obtained by substituting $c = 0$ in (6) is different from the formula for $d_g(p)$ in [4], p. 896, but they have the same sum when p is odd.

One can, of course, combine (5) and (6) to get similar expressions for the numbers $\mathfrak{e}_g^{(2c)}$ and $\mathfrak{o}_g^{(2c)}$. Note also that if one substitutes $p/\sin^2(\pi j/p)$ for $1/\cos^2(\pi j/p)$ in the right hand side of our formula (5), one gets the right hand side of the Verlinde formula (6). This will be explained in the proof of Theorem 2.7 in §7.2.

It is well-known that for $g \geq 2$, the number D_g when viewed as a function of p is a polynomial of degree $3g-3$ in p (see for example Zagier [21] or [4]). Moreover, the number $D_g^{(2c)}$ is a polynomial in p and c of total degree $3g-2$. (This follows from a residue formula for $D_g^{(2c)}$ which we shall give in §7.4.) We have a similar result for $\delta_g^{(2c)}$. To state it, let B_n be the Bernoulli numbers defined by

$$\frac{t}{e^t-1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!} \,. \tag{7}$$

Note $B_1 = -1/2$ and $B_k = 0$ for all odd $k \geq 3$. It will be convenient to denote (see *e.g.* Ireland and Rosen [12], p. 231)

$$\widetilde{B}_n = \frac{1}{2}\frac{(-1)^{n+1}B_{2n}}{(2n)!} = \frac{\zeta(2n)}{(2\pi)^{2n}} \,.$$

Theorem 2.8. *For $g \geq 1$, we have that $\delta_g^{(2c)}$ is an (inhomogeneous) polynomial in c and p of total degree $2g-1$. The homogeneous part of degree $2g-1$ in this polynomial is given by*

$$(-1)^{g-1} \sum_{k=1}^{2g} 2(2^k-1)\,\frac{B_k}{k!}\,\frac{c^{2g-k}}{(2g-k)!}\,p^{k-1} \,. \tag{8}$$

In particular, for any fixed value of $c \in \{0,1,\ldots,(p-3)/2\}$, the polynomial $\delta_g^{(2c)}(p)$ has degree $2g-1$ in p. Moreover, the leading coefficient of this polynomial is $4(2^{2g}-1)\widetilde{B}_g$.

This should be compared to the fact that the leading coefficient of the polynomial $D_g(p)$ is $\widetilde{B}_{g-1}$ (see formula (6) in Zagier [21][4] or Corollary 2.10 below). This leading coefficient is closely related to the volume of a certain moduli space (see Witten [20], §3). Moreover, the dimension of this moduli space is equal to the degree of the polynomial $D_g(p)$, by the Riemann–Roch formula. We wonder whether there is an algebro-geometric interpretation of the degree and the leading coefficient of the polynomial $\delta_g(p)$. We remark that in the related but different situation of SU(2)-TQFT at even level, a similar question about an algebro-geometric interpretation of the difference of the number of even and odd colorings (albeit for a quite different notion of even and odd colorings) was answered affirmatively in Andersen and Masbaum [2] in terms of certain geometrically defined involutions on the moduli space.

[4] Our D_g is 2^{-g} times Zagier's $D(g,p)$, which is the dimension of the SU(2)-TQFT vector space $V_{2p}(\Sigma_g)$. This fact comes from a tensor product formula, see Theorem 1.5 of [4]. The V_{2p}-theory corresponds in Conformal Field Theory to SU(2) at level $k = p-2$.

Theorem 2.8 will be proved in §7.3. It implies that the dimensions $\mathfrak{o}_g^{(2c)}$ and $\mathfrak{e}_g^{(2c)}$ of our irreducible factors $F^{\mathrm{odd}}(\Sigma)$ and $F(\Sigma)/F^{\mathrm{odd}}(\Sigma)$ are polynomials in p and c which coincide with the polynomial $D_g^{(2c)}/2$ in degrees higher than $2g-1$. This leads to the following corollary, which will be proved in §7.4.

Corollary 2.9. *For $g \geq 2$, both $\mathfrak{e}_g^{(2c)}$ and $\mathfrak{o}_g^{(2c)}$ are polynomials of total degree $3g-2$ in p and c. For $g \geq 3$, the leading terms of these polynomials are given by*

$$\mathfrak{e}_g^{(2c)} \equiv \mathfrak{o}_g^{(2c)} \equiv \frac{(-1)^g}{4} \sum_{k=0}^{2g-2} \frac{B_k}{k!} \frac{c^{2g-2-k}}{(2g-2-k)!} \Big(1 + \frac{2c}{2g-1-k}\Big) p^{g-1+k} \qquad (9)$$

where $\equiv$ means equality up to addition of a polynomial in p and c of total degree $\leq 3g-4$.

Knowing the terms of total degree $3g-2$ and $3g-3$ in $\mathfrak{e}_g^{(2c)}$ and $\mathfrak{o}_g^{(2c)}$ (as given in the preceding Corollary 2.9) allows one to compute the leading term of $\mathfrak{e}_g^{(2c)}$ and $\mathfrak{o}_g^{(2c)}$ when viewed as polynomials in p, with c held fixed. Corollary 2.9 implies that these leading terms are given as follows.

Corollary 2.10. *Assume $c \in \{0, 1, \ldots, (p-3)/2\}$ is fixed. If $g \geq 3$, then both $\mathfrak{e}_g^{(2c)}$ and $\mathfrak{o}_g^{(2c)}$ are polynomials of degree $3g-3$ in p with leading coefficient $(c+\frac{1}{2})\widetilde{B}_{g-1}$.*

For $g = 2$, we will write down $\mathfrak{e}_2^{(2c)}$ and $\mathfrak{o}_2^{(2c)}$ in (21) and (22) in §7.1. In this case, the leading terms are slightly different: for fixed c, one has that $\mathfrak{e}_2^{(2c)}$ and $\mathfrak{o}_2^{(2c)}$ are polynomials of degree 3 in p, with leading coefficient $(c+1)/24$ and $c/24$, respectively, except for $\mathfrak{o}_2 = \mathfrak{o}_2^{(0)}$ which is identically zero.

In §7.5, we will give a residue formula for $\delta_g^{(2c)}$ similar to the residue formula for $D_g^{(2c)}$ mentioned above.

Remarks 2.11. (1) One can show [14] that the modular representations $F^{\mathrm{odd}}(\Sigma)$ and $F(\Sigma)/F^{\mathrm{odd}}(\Sigma)$ of the mapping class group Γ_Σ factor through the natural map

$$\Gamma_\Sigma \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Sp}(2g, \mathbb{Z}) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Sp}(2g, \mathbb{F}_p)\ .$$

(But this is in general not the case for the representation $F(\Sigma)$ itself.) We wonder about how to characterize our irreducible factors among the modular representations of the symplectic group $\mathrm{Sp}(2g, \mathbb{F}_p)$ in characteristic p. As a step in this direction, in the case $p = 5$, we have identified our dimensions $\mathfrak{e}_g^{(2c)}(5)$ and $\mathfrak{o}_g^{(2c)}(5)$ with the dimensions of some known modular representations (see §8).

(2) In the genus one case, where $F(\Sigma)$ itself is irreducible, we have $\mathfrak{e}_1^{(2c)}(p) = (p-1)/2-c$, and $\mathfrak{o}_1^{(2c)}(p) = 0$. In this case, we computed the modular representation $F(\Sigma_1(2c))$ for any p and c already in [7], where we showed that $F(\Sigma_1(2c))$ (which was denoted by $\mathcal{S}^+_{p,0}(\mathcal{T}_c)$ in [7]) is isomorphic to the space of homogeneous polynomials over $\mathbb{F}_p$ in two variables of total degree $(p-3)/2-c$. It is well-known that this representation of $\mathrm{Sp}(2,\mathbb{F}_p) = \mathrm{SL}(2,\mathbb{F}_p)$ is irreducible for every $c \le (p-3)/2$.

(3) Theorem 2.4 also gives information on the representations of the extended mapping class group on the quotients

$$\mathcal{S}(\Sigma)/(1-\zeta_p)^N \mathcal{S}(\Sigma)$$

for any $N \ge 1$. The study of these higher quotient representations is interesting, because they factor through finite quotients of the extended mapping class group, but approximate the TQFT-representation better and better as N increases. This is discussed in more detail in [7].

(4) The proper irreducible subrepresentation $F^{\mathrm{odd}}(\Sigma)$ of $F(\Sigma)$ (in the case $g \ge 2$ and $(g,c) \ne (2,0)$) is the radical of a certain Γ_Σ-invariant bilinear form on the $\mathbb{F}_p$-vector space $F(\Sigma)$. This form is symmetric if $c \equiv ((p+1)/2)\, g \pmod 2$. Otherwise this form is skew-symmetric. It is induced (after rescaling by $(1-\zeta_p)^{-c}$) from a natural $\mathbb{Z}[\zeta_p]$-valued form on the lattice $\mathcal{S}(\Sigma)$. See §14 of our paper [6] for an explicit description of this form in the case $c = 0$ (*i.e.* when the surface has empty boundary). This description generalizes to the case $c \ne 0$. [5]

3. Proof of Corollary 2.6 and irreducibility in characteristic $\ne p$

This is based on the following well-known lemma, whose proof we omit.

Lemma 3.1. *Suppose a group G is represented on a vector space V over a field k. If the associated algebra morphism $k[G] \to \mathrm{End}_k(V)$ is surjective, then the representation is irreducible.*

Proof of Corollary 2.6 assuming Theorem 2.4. If $g \le 1$ or if $(g,c) = (2,0)$, all colorings are even and hence $F^{\mathrm{odd}}(\Sigma) = 0$. Thus, by (4) (which follows immediately from Theorem 2.4), the image of $\mathbb{F}_p[\Gamma_\Sigma]$ is $\mathrm{End}_{\mathbb{F}_p}(F(\Sigma))$ and Lemma 3.1 implies that the representation is irreducible in this case. Otherwise, both $F^{\mathrm{odd}}(\Sigma)$ and $F^{\mathrm{ev}}(\Sigma)$ are non-zero. Applying again Lemma 3.1, it follows from (4) that $F^{\mathrm{odd}}(\Sigma)$ is an irreducible subrepresentation of $F(\Sigma)$, and the quotient representation $F(\Sigma)/F^{\mathrm{odd}}(\Sigma)$ with the induced action is again irreducible.

[5] If $c \ne 0$, one should define the notion of even and odd colorings as in Definition 2.3. The definition of even and odd colorings in [6], p. 838, applies only to the case $c = 0$.

We only need to show, in the case that $F^{\mathrm{odd}}(\Sigma) \neq 0$, that $F^{\mathrm{odd}}(\Sigma)$ is the only proper non-trivial subrepresentation of $F(\Sigma)$. The argument is quite standard, but we give details for the reader's convenience. Suppose, then, that $V \subset F(\Sigma)$ is a proper non-trivial subrepresentation.

We consider first the case that $V \cap F^{\mathrm{odd}}(\Sigma) \neq 0$. Then $V \supset F^{\mathrm{odd}}(\Sigma)$ since $F^{\mathrm{odd}}(\Sigma)$ is irreducible. If V is strictly bigger than $F^{\mathrm{odd}}(\Sigma)$, then $\bar{V}$, the image of V in $F(\Sigma)/F^{\mathrm{odd}}(\Sigma)$, is non-zero. But $F(\Sigma)/F^{\mathrm{odd}}(\Sigma)$ is also irreducible. So $\bar{V} = F(\Sigma)/F^{\mathrm{odd}}(\Sigma)$ and hence $V = F(\Sigma)$ which is a contradiction. Thus $V = F^{\mathrm{odd}}(\Sigma)$ in this first case.

We consider now the second case, where $V \cap F^{\mathrm{odd}}(\Sigma) = 0$. We will see that this case cannot happen. We proceed as follows. If $V \cap F^{\mathrm{odd}}(\Sigma) = 0$, then $\bar{V}$, the image of V in $F(\Sigma)/F^{\mathrm{odd}}(\Sigma)$ is non-zero, hence equal to $F(\Sigma)/F^{\mathrm{odd}}(\Sigma)$, by irreducibility. It follows that

$$\dim V = \dim \bar{V} = \dim(F(\Sigma)/F^{\mathrm{odd}}(\Sigma)) = \dim F^{\mathrm{ev}}(\Sigma)$$

and the projection $\pi = \mathrm{Id}_{F^{\mathrm{ev}}(\Sigma)} \oplus 0_{F^{\mathrm{odd}}(\Sigma)}$ from $F(\Sigma)$ onto $F^{\mathrm{ev}}(\Sigma)$ along $F^{\mathrm{odd}}(\Sigma)$ sends V isomorphically to $F^{\mathrm{ev}}(\Sigma)$.

Now by (4) the projection π lies in the image of $\mathbb{F}_p[\Gamma_\Sigma]$. As V is stable under the action of Γ_Σ, it follows that V must be equal to $F^{\mathrm{ev}}(\Sigma)$. But $F^{\mathrm{ev}}(\Sigma)$ is not stable under the action, since $\mathrm{Image}(\mathbb{F}_p[\Gamma_\Sigma]) \supset \mathrm{Hom}_{\mathbb{F}_p}(F^{\mathrm{ev}}(\Sigma), F^{\mathrm{odd}}(\Sigma))$. This contradiction shows that the second case does not occur. □

Theorem 2.4 also implies the following corollary for the representation over the complex numbers which generalizes a result of Roberts [17] (see Remark 3.3).

Corollary 3.2. *If the surface Σ has at most one boundary component and if p is a prime, the representation of the extended mapping class group on the* SO(3)*-TQFT vector space at the p-th root of unity is irreducible over the complex numbers.*

Note that irreducibility over the complex numbers implies irreducibility over the cyclotomic field $\mathbb{Q}(\zeta_p)$.

Remark 3.3. In the case where Σ is closed, Corollary 3.2 is due to Roberts [17]. Roberts actually considered the SU(2)-TQFT-representation. But when the representation is considered over the complex numbers, his argument works also in the SO(3)-case we are considering in this paper. Roberts' argument is, however, quite different from ours.

Proof of Corollary 3.2. By hypothesis we have $\Sigma = \Sigma_g(2c)$ for some g and c, and the representation under consideration is simply $\mathcal{S}(\Sigma) \otimes \mathbb{C}$. As $1 - \zeta_p$ is a unit in $\mathbb{C}$, Theorem 2.4 shows that the group algebra $\mathbb{C}[\widetilde{\Gamma}_\Sigma^{++}]$ of the extended mapping class group maps onto $\mathrm{End}_{\mathbb{C}}(\mathcal{S}(\Sigma) \otimes \mathbb{C})$. Thus Lemma 3.1 gives the result. □

The same argument works in finite characteristic $\neq p$, as follows.

Corollary 3.4. *If I is an ideal in $\mathcal{O} = \mathbb{Z}[\zeta_p]$ so that $\mathcal{O}/I$ is a finite field of characteristic $\ell \neq p$, then the modular representation $\mathcal{S}(\Sigma)/I\mathcal{S}(\Sigma)$ in characteristic ℓ of the extended mapping class group is irreducible.*

Proof. The hypothesis implies that $1-\zeta_p$ is a unit in $\mathcal{O}/I$ and so the result follows from Theorem 2.4 as in the complex case above. □

Remark 3.5. More generally, if I is any ideal in $\mathcal{O}$ not divisible by $(1-\zeta_p)$, then $1-\zeta_p$ is a unit in the ring $R = \mathcal{O}/I$ and so the image of the extended mapping class group generates the entire endomorphism ring $\mathrm{End}_R(\mathcal{S}(\Sigma)/I\mathcal{S}(\Sigma))$. This is why we focus our attention on the ideal $(1-\zeta_p)$ in this paper.

4. Skein-theoretic definition of the integral TQFT representation

The theory of Integral SO(3)-TQFT is slightly different depending on the congruence class of the prime $p \pmod 4$. Following [6], let $\mathcal{O}_p = \mathbb{Z}[\zeta_p]$, if $p \equiv -1 \pmod 4$, and $\mathcal{O}_p = \mathbb{Z}[\zeta_{4p}]$, if $p \equiv 1 \pmod 4$. The Integral TQFT lattice $\mathcal{S}_p(\Sigma)$ defined in [6], §2, has coefficients in the ring $\mathcal{O}_p$. In the case $p \equiv 1 \pmod 4$, we defined in [6], §13, also another lattice $\mathcal{S}_p^+(\Sigma)$, with coefficients in $\mathbb{Z}[\zeta_p]$. The lattice $\mathcal{S}_p^+(\Sigma)$ lattice is again free of finite rank. It is contained (as a set) in $\mathcal{S}_p(\Sigma)$, and one has

$$\mathcal{S}_p(\Sigma) = \mathcal{S}_p^+(\Sigma) \otimes_{\mathbb{Z}[\zeta_p]} \mathbb{Z}[\zeta_{4p}] \quad (p \equiv 1 \pmod 4) \tag{10}$$

where $\zeta_{4p}^4 = \zeta_p$. The "bigger" lattice $\mathcal{S}_p(\Sigma)$ is in some sense the more natural one from the TQFT point of view. But for the purpose of studying mapping class group representations, we want the coefficient ring to be as small as possible. Therefore we take the lattice $\mathcal{S}(\Sigma)$ considered in Theorem 2.4 to be

$$\mathcal{S}(\Sigma) = \begin{cases} \mathcal{S}_p(\Sigma) & \text{if } p \equiv -1 \pmod 4, \\ \mathcal{S}_p^+(\Sigma) & \text{if } p \equiv 1 \pmod 4. \end{cases} \tag{11}$$

Thus, in both cases, $\mathcal{S}(\Sigma)$ is a free $\mathcal{O}$-module of finite rank, where $\mathcal{O} = \mathbb{Z}[\zeta_p]$. We will continue to use the notations $\mathcal{O}$ and $\mathcal{S}(\Sigma)$ whenever it is possible to make statements which are true in both cases. However, the proof of Theorem 2.4 will require some additional arguments in the case $p \equiv 1 \pmod 4$. We hope there will be no confusion from the fact that $\mathcal{O}$ is different from $\mathcal{O}_p$ in this case.

The construction of these lattices in [6] is a refinement of the skein-theoretic construction of TQFT from the Kauffman bracket in Blanchet *et al.* [4].

Notation 4.1. *Throughout the rest of the paper, we use the notations $h = 1-\zeta_p$ and $d = (p-1)/2$.*

We let Kauffman's skein variable be $A = -\zeta_p^{d+1}$; this is a primitive $2p$-th root of unity, and a square root of ζ_p. As customary in the skein-theoretic approach to TQFT, rather than considering surfaces with boundary, we think of closed surfaces equipped with colored banded points. (A banded point in a surface Σ is a small oriented closed interval embedded in Σ.) Thus, $\Sigma = \Sigma_g(2c)$ will from now on stand for a closed surface of genus g equipped with one colored banded point colored $2c$, where $0 \leq c \leq d-1$.

The TQFT-module $V_p(\Sigma)$ of [4] has coefficients in $\mathcal{O}_p[h^{-1}] = \mathcal{O}_p[p^{-1}]$.[6] This is a version of the Reshetikhin–Turaev SO(3)-TQFT module at the prime p associated to Σ. Elements of $V_p(\Sigma)$ are represented skein-theoretically as linear combinations of colored banded graphs in a handlebody H with $\partial H = \Sigma$, where the graphs should meet the boundary nicely in the colored banded point. For example, the lollipop tree $T_g^{(2c)}$ of Figure 1 (with banding parallel to the plane) and some coloring defines an element of $V_p(\Sigma)$ where $\Sigma = \Sigma_g(2c)$.

More generally, any closed connected 3-manifold M equipped with an identification of its boundary ∂M with Σ, and containing a colored banded graph which meets Σ in the banded point, defines an element $Z(M,G)$ of $V_p(\Sigma)$. Here (as is customary) we suppress the identification of ∂M with Σ from the notation, but it is important to realize that the element $Z(M,G)$ depends on this identification; indeed, the extended mapping class group $\widetilde{\Gamma}_\Sigma^{++}$ acts on the set of such (M,G) by changing how ∂M is identified with Σ, and this induces the action of $\widetilde{\Gamma}_\Sigma^{++}$ on the TQFT-module $V_p(\Sigma)$. We also downplay a technicality: in order to define $Z(M,G)$ we must fix a lagrangian in $H_1(\Sigma;\mathbb{Q})$ and equip M with an integer weight to resolve the so-called *framing anomaly*. Increasing the weight by 1 multiplies $Z(M,G)$ by an invertible scalar called κ in [6]. But lagrangians and weights will play almost no role in the present paper, and by abuse of notation, we simply write $Z(M,G)$ and $V_p(\Sigma)$.[7] This method of resolving the framing anomaly by using lagrangians and integer weights was pioneered by Walker [19] and developed by Turaev [18]. See also [8] for our take on this.[8]

The Integral TQFT lattice $\mathcal{S}_p(\Sigma)$ was originally defined as the $\mathcal{O}_p$-submodule of $V_p(\Sigma)$ spanned by all the elements $Z(M,G)$ coming from connected 3-manifolds M equipped with colored graphs G (and any integer weight) [5] and [6]. In our joint paper with van Wamelen [10], it was shown that $\mathcal{S}_p(\Sigma)$ could be also described as the $\mathcal{O}_p$-submodule spanned by certain skein elements in the handlebody H. In other words, we can use the fixed 3-manifold H if we permit our skein elements to have certain carefully controlled denominators. This is done as follows.

Recall that banded knots can be also colored (= cabled) by skein elements (= linear combinations of banded links) living in a solid torus. The skein-theoretic definition of

[6] We have $\mathcal{O}_p[h^{-1}] = \mathcal{O}_p[p^{-1}]$ because $(h^{p-1}) = (p)$ as ideals in $\mathbb{Z}[\zeta_p]$.

[7] Formally, one may think that the notation M stands for a manifold equipped with an integer weight, and Σ stands for a surface equipped with a lagrangian. This is also the point of view adopted in [8].

[8] Another way to resolve the framing anomaly is to use p_1-structures as in [4].

$\mathcal{S}_p(\Sigma)$ is as the $\mathcal{O}_p$-submodule of $V_p(\Sigma)$ spanned by so-called *mixed graphs*[9] in [10] where a mixed graph is a colored banded graph G union a banded link L with each component of L colored by the following skein element v in the solid torus

$$v = h^{-1}(z+2) \tag{12}$$

(Here, z stands for the banded knot given by the core of the solid torus.) It is important to observe that the $\mathcal{O}_p$-module $\mathcal{S}_p(\Sigma)$ obtained in this way is bigger than the $\mathcal{O}_p$-submodule of $V_p(\Sigma)$ spanned by colored banded graphs in H because v has denominator h, which is a prime in $\mathcal{O}$. But it is this $\mathcal{O}_p$-module $\mathcal{S}_p(\Sigma)$ which carries a natural action of the extended mapping class group $\widetilde{\Gamma}_\Sigma^{++}$, as is most easily seen from the above description of $\mathcal{S}_p(\Sigma)$ in terms of all connected 3-manifolds M with boundary identified with Σ.

According to (10) and (11), in the case $p \equiv 1 \pmod 4$, $\mathcal{S}(\Sigma)$ is an $\mathcal{O}$-module contained in the $\mathcal{O}_p$-module $\mathcal{S}_p(\Sigma)$. We still have that $\mathcal{S}(\Sigma)$ is the $\mathcal{O}$-submodule of $V_p(\Sigma)$ spanned by all mixed graphs in H [6], §13.

We refer the reader to [6] for the definition of the basis elements $\mathfrak{b}_\sigma$ of $\mathcal{S}(\Sigma)$ discussed in the introduction. Details of this definition will not be needed in this paper, but we remark that although the $\mathfrak{b}_\sigma$ are *indexed* by colorings of the banded lollipop tree $T_g^{(2c)}$, the basis element $\mathfrak{b}_\sigma$ is not just $T_g^{(2c)}$ with coloring σ, but is a mixed graph in the sense explained above, which furthermore has been rescaled by a certain non-positive power of h. In fact, the colorings of $T_g^{(2c)}$ give the so-called *graph basis* of $V_p(\Sigma)$, and the basis $\{\mathfrak{b}_\sigma\}$ of $\mathcal{S}(\Sigma)$ is obtained from this graph basis by a triangular (but not unimodular) base change (see [6] for more details).

Let us now describe the action of the extended mapping class group on $\mathcal{S}(\Sigma)$. First we recall that, as usual in TQFT, any cobordism M from Σ to itself, equipped with some colored graph G connecting the colored point in the source surface Σ to the colored point in the target surface Σ, defines an endomorphism of $V_p(\Sigma)$ which, by abuse of notation, we denote again by $Z(M,G)$. If furthermore M is connected, then $Z(M,G)$ preserves the lattice $\mathcal{S}_p(\Sigma)$ (see [6]).[10] For example, consider $M = \Sigma \times \mathrm{I}$ with weight zero, equipped with the banded arc $pt \times \mathrm{I}$ with color $2c$ (where pt is the colored banded point in Σ). We denote this "vertical" banded arc by C, and we let $\mathrm{C}(2c)$ denote this arc colored by $2c$. Then we have that $Z(\Sigma \times \mathrm{I}, \mathrm{C}(2c))$ is the identity map of $\mathcal{S}(\Sigma)$.

Next recall that the mapping class group Γ_Σ is generated by Dehn twists about simple closed curves α which avoid the colored banded point. (We remind the reader that Γ_Σ here is the mapping class group of Σ which fixes the banded point, which is the same as the mapping class group rel. boundary of Σ with an open disk around the banded point removed; in particular, the Dehn twist about a curve encircling the banded point is non-trivial in Γ_Σ.) For a certain skein element ω_+ in the solid torus

[9] Mixed graphs were called *v-graphs* in [6].

[10] But $Z(M,G)$ does not necessarily preserve the lattice $\mathcal{S}(\Sigma) = \mathcal{S}_p^+(\Sigma)$ in the case $p \equiv 1 \pmod 4$. We will address this problem at the end of §6.

to be specified below, we denote by $\alpha_0(\omega_+)$ the skein element in $\Sigma \times \mathrm{I}$ obtained by cabling $\alpha \times \frac{1}{2}$ by ω_+, with framing zero relative to the surface $\Sigma \times \frac{1}{2}$ lying in $\Sigma \times \mathrm{I}$. Here is, then, a skein-theoretic description of the action.

Proposition 4.2. *For a certain lift $W(\alpha)$ of the Dehn twist about α to the extended mapping class group $\widetilde{\Gamma}_\Sigma^{++}$, the action of $W(\alpha)$ on $\mathcal{S}(\Sigma)$ is given by the endomorphism*

$$Z(\Sigma \times \mathrm{I}, \mathrm{C}(2c) \cup \alpha_0(\omega_+)) \,. \tag{13}$$

Statements like this are, of course, well-known in the skein-theoretic approach to TQFT. A more precise formula, taking into account the extra structure (weights and lagrangians) needed to define the central extension $\widetilde{\Gamma}_\Sigma^{++}$ and to specify the lifts $W(\alpha)$ of Dehn twists to $\widetilde{\Gamma}_\Sigma^{++}$, can be found in §11 of [8]. We don't need this more precise formula to describe the image of the group algebra $\mathcal{O}[\widetilde{\Gamma}_\Sigma^{++}]$ in $\mathrm{End}_{\mathcal{O}}(\mathcal{S}(\Sigma))$, because (1) the lifts $W(\alpha)$ generate the extended mapping class group $\widetilde{\Gamma}_\Sigma^{++}$, and (2) in the central extension

$$\mathbb{Z} \longrightarrow \widetilde{\Gamma}_\Sigma^{++} \to \Gamma_\Sigma \,,$$

any two lifts of the same mapping class to $\widetilde{\Gamma}_\Sigma^{++}$ differ by a power of the central generator, and this central generator acts on $\mathcal{S}(\Sigma)$ by κ^4 (which is a unit in $\mathcal{O}$) times the identity map.[11] Thus we have the following corollary, which will be the starting point for our proof of Theorem 2.4.

Corollary 4.3. *The image of $\mathcal{O}[\widetilde{\Gamma}_\Sigma^{++}]$ in $\mathrm{End}_{\mathcal{O}}(\mathcal{S}(\Sigma))$ is the $\mathcal{O}$-subalgebra generated by the endomorphisms $Z(\Sigma \times \mathrm{I}, \mathrm{C}(2c) \cup \alpha_0(\omega_+))$ associated to simple closed curves α on Σ avoiding the colored banded point.*

It remains to describe ω_+. Its key property (which basically implies Proposition 4.2) is described in Figure 2.

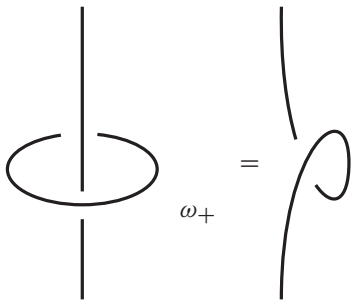


Figure 2. Encircling a strand with ω_+ has the same effect in TQFT as giving that strand a positive twist.

[11] In fact, κ is a square root of $A^{-6-p(p+1)/2}$, and since $A^2 = \zeta_p$ we have $\kappa^4 = \zeta_p^{-6}$. Notice that $\kappa^4 \equiv 1 \pmod{h}$. This is why the representation of $\widetilde{\Gamma}_\Sigma^{++}$ on $F(\Sigma) = \mathcal{S}(\Sigma)/h\mathcal{S}(\Sigma)$ factors through the ordinary mapping class group Γ_Σ.

An explicit formula for ω_+ is given in §4 of [7], based on computations of a similar skein element in Blanchet *et al.* [3]. In this paper, we only need to know the following about ω_+. Let $\mathcal{T}$ denote a closed surface of genus one (*i.e.*, a torus) viewed as the boundary of a solid torus. Since ω_+ lies in the solid torus, it defines an element of $V_p(\mathcal{T})$. By abuse of notation, we denote this element again by ω_+.

Proposition 4.4. *One has $\omega_+ \in \mathcal{S}(\mathcal{T})$. Moreover, for the usual algebra structure in $\mathcal{S}(\mathcal{T})$ coming from thinking of the solid torus as an annulus $\times$ I, the elements*

$$1, \omega_+, \omega_+^2, \ldots, \omega_+^{d-1}$$

form a basis of $\mathcal{S}(\mathcal{T})$.

(Here, 1 stands for the empty link, which is the unit element of this algebra.)

Proof. We first consider the case $p \equiv -1 \pmod 4$, where $\mathcal{S}(\mathcal{T}) = \mathcal{S}_p(\mathcal{T})$. The following proof is similar to the proof of Theorem 6.1 of [10], where the reader will find more details on some of the arguments that follow.

By its very definition, see [5] and [6], the lattice $\mathcal{S}_p(\mathcal{T})$ contains the TQFT-vectors associated to all connected manifolds with boundary $\mathcal{T}$. Since ω_+, up to multiplication by a unit, is also represented in $V_p(\mathcal{T})$ by the result of -1-framed surgery to the solid torus with boundary $\mathcal{T}$ along the core of the solid torus, we have that $\omega_+ \in \mathcal{S}_p(\mathcal{T})$. Let P be the $\mathcal{O}_p$-module spanned by the purported basis. By similar reasoning, $P \subset \mathcal{S}_p(\mathcal{T})$.

Let $\{e_0 = 1, e_1, \ldots, e_{d-1}\}$ be the standard graph basis of $V_p(\mathcal{T})$. The determinant of a matrix which expresses a basis for $\mathcal{S}_p(\mathcal{T})$ in terms of $\{e_0, e_1, \ldots, e_{d-1}\}$ is given by $h^{-d(d-1)/2}$, up to units (see [10], p. 272).

Consider the Hopf pairing

$$((\ ,\ ))\colon \mathcal{S}_p(\mathcal{T}) \times \mathcal{S}_p(\mathcal{T}) \longrightarrow \mathcal{O}_p,$$

where $((x, y))$ is given by cabling the zero-framed Hopf link with x and y and then evaluating the resulting skein element in S^3 (normalized so that the empty link evaluates to 1.) The determinant of the $d \times d$ matrix $((e_i, e_j))$ is up to units given by $h^{d(d-1)}$. This is because the e_i are an orthonormal basis for $V_p(\mathcal{T})$ with respect to the usual Hermitian TQFT form on $V_p(\mathcal{T})$ [4], and the Hopf pairing that we are considering differs from this by complex conjugation (which leaves the e_i fixed), the action of a homeomorphism (which is an isometry), and a rescaling by h^{d-1} (up to units).

If we pair our purported basis with the e_i under the Hopf pairing, we get

$$((\omega_+^i, e_j)) = (-1)^j [j+1] \mu_j^i \ ,$$

where $\mu_j = (-A)^{j(j+2)} = \zeta_p^{(d+1)j(j+2)}$ are the twist eigenvalues, and the quantum integers $[j+1]$ are defined by

$$[n] = \frac{A^{2n} - A^{-2n}}{A^2 - A^{-2}} = \frac{\zeta_p^n - \zeta_p^{-n}}{\zeta_p - \zeta_p^{-1}}\,.$$

Ignoring the unit[12] factors $(-1)^j[j+1]$ which appear as multiples of the columns, this is a Vandermonde matrix. (This matrix appeared on [10], p. 272.) Up to units, its determinant is $h^{d(d-1)/2}$. It follows that the determinant of the matrix expressing ω_+^i in terms of e_j is given by $h^{-d(d-1)/2}$, up to units. As a known basis for $\mathcal{S}_p(\mathcal{T})$ has this same property, and $P \subset \mathcal{S}_p(\mathcal{T})$, it follows that $P = \mathcal{S}_p(\mathcal{T})$. This completes the proof in the case $p \equiv -1 \pmod 4$.

Now assume $p \equiv 1 \pmod 4$. Then the exact same proof as above shows that $\{1, \omega_+, \omega_+^2, \ldots, \omega_+^{d-1}\}$ is a basis of $\mathcal{S}_p(\mathcal{T})$, which now has coefficients in $\mathbb{Z}[\zeta_{4p}]$. But the explicit formula for ω_+ given in [7], §4, shows that ω_+ and its powers lie in the $\mathbb{Z}[\zeta_p]$-lattice $\mathcal{S}(\mathcal{T}) = \mathcal{S}_p^+(\mathcal{T})$. Using (10), it follows that $\{1, \omega_+, \omega_+^2, \ldots, \omega_+^{d-1}\}$ is a basis of $\mathcal{S}(\mathcal{T})$. This completes the proof in the case $p \equiv 1 \pmod 4$. □

5. v'-colored links in the product of a surface and an interval

As the material presented here has independent interest, for this section only, we work in a more general context where the coefficient ring can be any integral domain R containing an invertible element A for which $1 + A \neq 0$.

Let S be a compact oriented surface, possibly with boundary (but without colored points). Let $\mathcal{K}(S \times \mathrm{I})$ be the Kauffman bracket skein module of $S \times \mathrm{I}$ with coefficients in R. Observe that $\mathcal{K}(S \times \mathrm{I})$ has a natural product structure (given by stacking one banded link on top of another) which makes $\mathcal{K}(S \times \mathrm{I})$ into an algebra. A banded link L is called *layered* if it can be written as a product of banded knots, *i.e.,* if each component of L projects to a different subset of I. We say that a banded knot in $S \times \mathrm{I}$ is *flat* if it is (up to isotopy) entirely contained in a surface $S \times \{t\}$ for some t in the interior of I, and the banding is also flat (i.e. parallel to the layers). Equivalently, a banded knot is flat if it has a diagram on S without crossings.

Let v' be the following slight modification[13] of the element v defined in (12):

$$v' = \frac{z+2}{1+A}$$

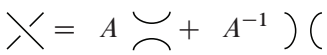
Note that v' lies in $\mathcal{K}(\text{solid torus}) \otimes R[(1+A)^{-1}]$.

[12] The fact that the quantum integers $[j+1]$ appearing here are units in $\mathbb{Z}[\zeta_p]$ is shown in Lemma 3.1(ii) of [16].

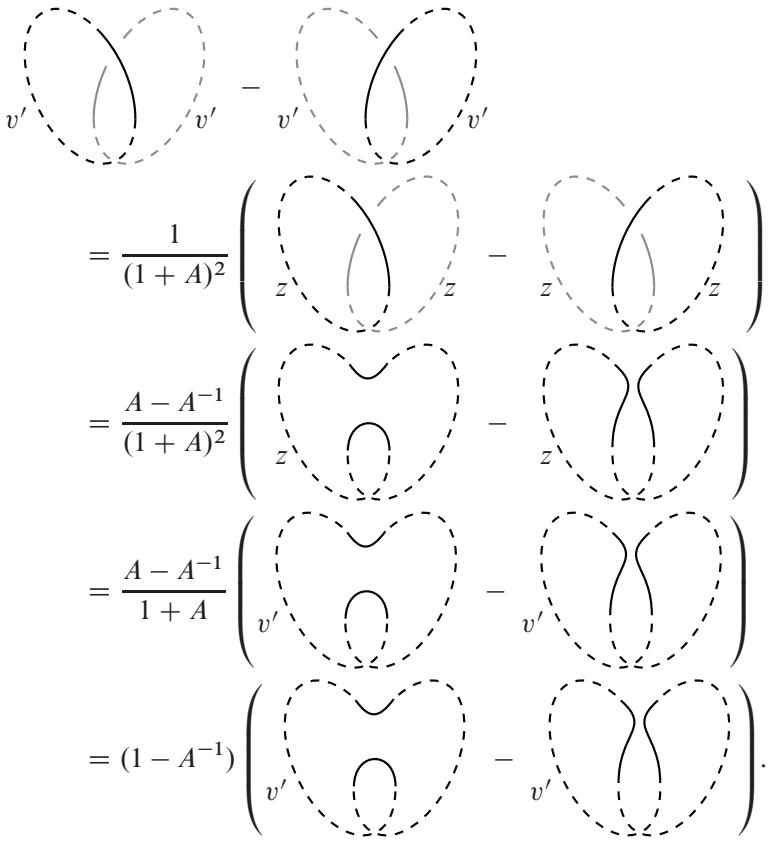
[13] Note that v' was called v in [10], but in the present paper we follow [6] and reserve the notation v for the element defined in Equation (12). We will see in (14) that v and v' are essentially equivalent when $R = \mathcal{O}$.

Lemma 5.1. *The R-submodule of $\mathcal{K}(S \times \mathrm{I}) \otimes R[(1+A)^{-1}]$ spanned by v'-colored banded links is generated, as an algebra, by v'-colored banded knots.*

Proof. We need to convert a v'-colored banded link L to an R-linear combination of banded links where the components are layered in some order one on top of the other. Recall that one of the Kauffman bracket skein relations [13] is



The following equation shows how to use this skein relation to change crossings of strands belonging to different connected components of L at the cost of introducing an R-linear combination of v'-colored banded links with fewer crossings and fewer components. The dotted lines show the connection scheme in the complement of a disc in S where the crossing occurs. This allows a proof by induction on the number of connected components of L.

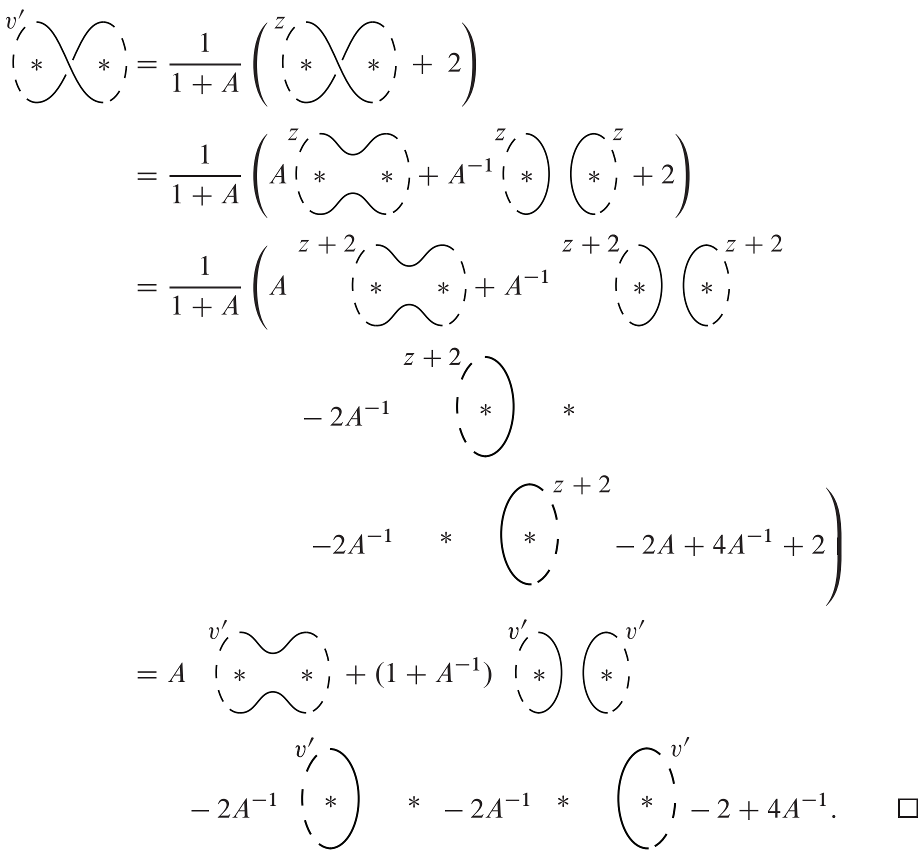


□

Proposition 5.2. *The R-submodule of $\mathcal{K}(S \times \mathrm{I}) \otimes R[(1+A)^{-1}]$ spanned by v'-colored banded links is generated, as an algebra, by v'-colored flat banded knots.*

Proof. Using the previous lemma, it is enough to see that an element given by a single v'-colored banded knot can be written as an R-linear combination of products of flat banded knots. This can be proved by induction on the number of crossings of the banded knot, using the following equation, and a similar one obtained from the same starting diagram but with the opposite crossing data. The two asterisks are meant to indicate two points on a disk in S to help locate the placement of the links with respect to these reference points. Thus the empty link could be denoted by two asterisks, but to save space, we write simply a scalar for that scalar times the empty link. The dotted lines play the same role as in the previous equation.

The following equation, then, shows that a v'-colored banded knot with n crossings can be rewritten as an R-linear combination of three v'-colored banded knots with fewer than n crossings, one v'-colored two-component banded link also with fewer than n crossings, and the empty link. By the same reasoning as in the proof of the previous lemma, this v'-colored two-component banded link may be written as a linear combination of v'-colored layered links with fewer than n crossings. So the needed result can be proved by induction on the number of crossings.



We will say a banded link in $S \times \mathrm{I}$ is a *flat layered* banded link, if it is a product of flat banded knots. In other words, each component lies in a different $S \times \{t\}$, the banding is also flat (*i.e.,* parallel to the layers), and each component is flat. We can rephrase the above result as follows.

Corollary 5.3. *The R-submodule of $\mathcal{K}(S \times \mathrm{I}) \otimes R[(1+A)^{-1}]$ spanned by v'-colored banded links is spanned (as an R-module) by flat layered v'-colored banded links.*

6. Proof of Theorem 2.4

Let us consider the results of the previous section but taking R to be $\mathcal{O}$ with $A = -\zeta_p^{d+1}$. We write $x \sim y$ (where x and y lie in some $\mathcal{O}$-module) if $x = uy$ where u is a unit of $\mathcal{O}$. Since $1 - A$ is a unit in $\mathcal{O}$, see [10], Lemma 4.1(i), we have $h = 1 - \zeta_p = 1 - A^2 \sim 1 + A$. Comparing (12) and (5), we see that

$$v \sim v' \tag{14}$$

in $\mathcal{K}(\text{solid torus}) \otimes \mathcal{O}[h^{-1}]$. Thus we have the following specialization of Corollary 5.2, where we have permissibly substituted v for v'.

Proposition 6.1. *The $\mathcal{O}$-submodule of $\mathcal{K}(S \times \mathrm{I}) \otimes \mathcal{O}[h^{-1}]$ spanned by v-colored banded links is spanned by flat layered v-colored banded links.*

We now return to $\Sigma = \Sigma_g(2c)$. In order to prove Theorem 2.4, we must compute the image of $\mathcal{O}[\widetilde{\Gamma}_\Sigma^{++}]$ in $\mathrm{End}_{\mathcal{O}}(\mathcal{S}(\Sigma))$. We proceed in three steps. The first step is to apply the previous Proposition 6.1 with S equal to Σ with a disk around the colored banded point removed. Thus $S \times \mathrm{I}$ is $\Sigma \times \mathrm{I}$ minus a tubular neighborhood of the vertical arc $\mathrm{C} = pt \times \mathrm{I}$.

Lemma 6.2. *The image of $\mathcal{O}[\widetilde{\Gamma}_\Sigma^{++}]$ in $\mathrm{End}_{\mathcal{O}}(\mathcal{S}(\Sigma))$ is equal to the $\mathcal{O}$-submodule of $\mathrm{End}_{\mathcal{O}}(\mathcal{S}(\Sigma))$ spanned by elements of the form $Z(\Sigma \times \mathrm{I}, \mathrm{C}(2c) \cup s)$, where s is some v-colored banded link in $(\Sigma \times \mathrm{I}) \setminus \mathrm{C}$.*

Proof. Let $\mathcal{E}$ be the image of $\mathcal{O}[\widetilde{\Gamma}_\Sigma^{++}]$ in $\mathrm{End}_{\mathcal{O}}(\mathcal{S}(\Sigma))$, and let $\mathcal{E}'$ be the $\mathcal{O}$-submodule of $\mathrm{End}_{\mathcal{O}}(\mathcal{S}(\Sigma))$ described in the lemma. Note that both $\mathcal{E}$ and $\mathcal{E}'$ are sub-algebras of $\mathrm{End}_{\mathcal{O}}(\mathcal{S}(\Sigma))$. We must show that $\mathcal{E} = \mathcal{E}'$.

The inclusion $\mathcal{E} \subset \mathcal{E}'$ is easy: by Corollary 4.3, we know that $\mathcal{E}$ is the $\mathcal{O}$-subalgebra generated by the endomorphisms $Z(\Sigma \times \mathrm{I}, \mathrm{C}(2c) \cup \alpha_0(\omega_+))$ associated to simple closed curves α on Σ avoiding the colored banded point. Notice that α_0 is a flat banded knot, so that $\mathcal{E}$ is the subalgebra generated by the endomorphisms coming from flat ω_+-colored banded knots. As $\omega_+ \in S(\mathcal{T})$, and $S(\mathcal{T})$ is spanned by v-colored banded links in the solid torus, we see that $\mathcal{E} \subset \mathcal{E}'$.

For the opposite inclusion, we must show that every v-colored banded link s in $(\Sigma \times \mathrm{I}) \setminus \mathrm{C}$ can be rewritten as an $\mathcal{O}$-linear combination of products of flat ω_+-colored banded knots. We proceed as follows. First, Proposition 6.1 tells us that s can be rewritten as an $\mathcal{O}$-linear combination of flat layered v-colored banded links, *i.e.,* products of flat v-colored banded knots. Thus, it is enough to show that a flat v-colored banded knot can be rewritten as an $\mathcal{O}$-linear combination of products of flat ω_+-colored banded knots. But this follows from Proposition 4.4. This completes the proof. □

In the next step of the proof of Theorem 2.4, we wish to replace $\Sigma \times \mathrm{I}$ by another cobordism from Σ to itself. For this we use the following general fact about Integral TQFT.

Lemma 6.3. *Let M be a compact connected oriented 3-manifold with $\partial M = -\Sigma \sqcup \Sigma$, and let $G \subset M$ be a colored banded graph which meets the boundary at the colored points of $-\Sigma$ and Σ. Let (M', G') be obtained from (M, G) by surgery on some framed link in $M \setminus G$. Then the set of endomorphisms*

$$\{Z(M, G \cup s) \colon s \text{ is a } v\text{-colored banded link in } M \setminus G\}$$

spans the same $\mathcal{O}_p$-submodule of $\mathrm{End}_{\mathcal{O}_p}(\mathcal{S}_p(\Sigma))$ *as the set of endomorphisms*

$$\{Z(M', G' \cup s) \colon s \text{ is a } v\text{-colored banded link in } M' \setminus G'\}\,.$$

Proof. This is similar to [4], Proposition 1.9, in the skein-theoretic construction of TQFT over a field. The proof is based on the surgery axiom (see *e.g.* [8], Lemma 11.1) which says that the effect of performing surgery along a framed curve in M is the same as the effect of cabling that curve with a certain skein element ω. Given the fact that ω lies in $S_p(\mathcal{T})$ and can therefore be expressed as a $\mathcal{O}_p$-linear combination of v-colored links in a solid torus, and the fact that surgery is reversible (we can also perform surgery M' in the complement of G' to recover M), the result follows. □

Notice that we have formulated the above Lemma 6.3 for the lattice $\mathcal{S}_p(\Sigma)$. In the case $p \equiv 1 \pmod 4$ (where $\mathcal{O} \subsetneq \mathcal{O}_p$ and $\mathcal{S}(\Sigma) \subsetneq \mathcal{S}_p(\Sigma)$), the lemma as stated does not hold for $\mathcal{S}(\Sigma)$. This is not really a problem, as there is also a version of Lemma 6.3 for the lattice $\mathcal{S}(\Sigma)$. But we defer the discussion of how to deal with this issue to the end of this section. Therefore, in what follows, we will work with the lattice $\mathcal{S}_p(\Sigma)$. We will thus obtain a proof of Theorem 2.4 for $\mathcal{S}_p(\Sigma)$ in place of $\mathcal{S}(\Sigma)$. This will already constitute a proof of Theorem 2.4 in the case $p \equiv -1 \pmod 4$. Once this is done, we will then explain the extra arguments needed in the case $p \equiv 1 \pmod 4$ to conclude the proof.

In the second step of the proof of Theorem 2.4, we use Lemma 6.3 to replace $\Sigma \times \mathrm{I}$ with the interior connected sum of two handlebodies, $H_1 \# H_2$, where H_2 is a genus g handlebody with boundary Σ, and H_1 is H_2 with the reversed orientation. Note that $H_1 \# H_2$ is a cobordism from Σ to itself.

We will need an explicit description of this construction. To this end, we identify $\Sigma \times \mathrm{I}$ with the complement of a neighborhood of two linked graphs $G_1, G_2 \subset S^3$, as drawn in Figure 3. In this figure, the vertical arc C is drawn as a thickened line. Note that C is not part of G_1 nor of G_2, as C lies in $\Sigma \times \mathrm{I}$.

Also we identify $H_1 \# H_2$ with the complement of a neighborhood of the disjoint union of two graphs $G_1' \sqcup G_2' \subset S^3$. One may pass from $\Sigma \times \mathrm{I}$ to $H_1 \# H_2$ by doing $+1$ framed surgery along g curves which encircle each of the clasps between G_1 and G_2. The thickened line labelled C$'$ in Figure 3 represents the image of C after the surgery. Again we remark that C$'$ lies in $H_1 \# H_2$ and is not part of G_1' nor of G_2'. Note that C$'$ meets the 2-sphere along which the connected sum occurs in a single point.

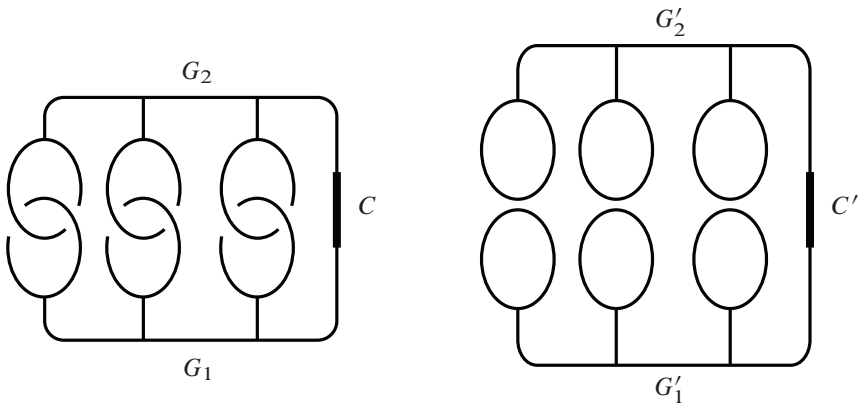


Figure 3. $\Sigma \times \mathrm{I}$ can be surgered to obtain $H_1 \# H_2$.

By lemmas 6.2 and 6.3 we obtain the following result.

Lemma 6.4. *The image of* $\mathcal{O}_p[\widetilde{\Gamma}_\Sigma^{++}]$ *in* $\mathrm{End}(\mathcal{S}_p(\Sigma))$ *is the* $\mathcal{O}_p$*-submodule spanned by the endomorphisms* $Z(H_1 \# H_2, \mathrm{C}'(2c) \cup s)$, *where* s *is any* v*-colored banded link in* $H_1 \# H_2 \setminus \mathrm{C}'$.

We can describe this submodule as follows. First, note that G_1' and G_2' are lollipop trees for two handlebodies $\mathcal{H}_1$ and $\mathcal{H}_2$ (not to be confused with H_1 and H_2) whose boundaries are copies of Σ (and each G_i' meeting the boundary of $\mathcal{H}_i$ in the colored point). Thus the second figure in Figure 3 describes a decomposition of S^3 into three pieces: the cobordism $H_1 \# H_2$ and the handlebodies $\mathcal{H}_1$ and $\mathcal{H}_2$. Now let $\nu(\mathrm{C}') \subset H_1 \# H_2$ be a tubular neighborhood of C$'$ which meets the handlebodies $\mathcal{H}_1$ and $\mathcal{H}_2$ along 2-disks. The complement of $\mathcal{H}_1 \sqcup \mathcal{H}_2 \cup \nu(\mathrm{C}')$ in S^3 (which is the same as the complement of $\nu(\mathrm{C}')$ in $H_1 \# H_2$) is a genus $2g$ handlebody H. A lollipop tree T for H is drawn in Figure 4.

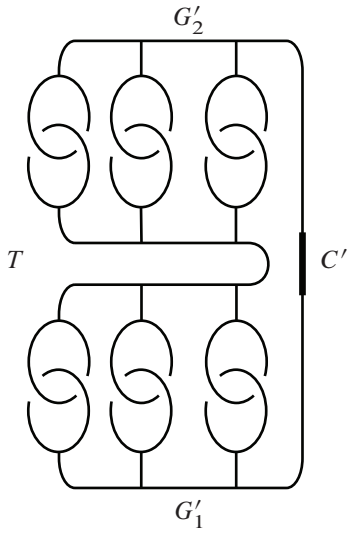


Figure 4. A lollipop tree T for the handlebody H of genus $2g$ which is the complement in S^3 of the union of neighborhoods of G_1' and G_2' and a neighborhood of C'.

Now observe that any v-colored banded link in $H_1\#H_2 \setminus \mathrm{C}'$ may be isotoped to lie in H, and the collection of such links then span the lattice $\mathcal{S}(\partial H)$. The set

$$\{\mathfrak{b}_\sigma : \sigma \text{ is a coloring of } T\}$$

(recall that all colorings are assumed small and admissible) is a basis for $\mathcal{S}(\partial H)$ and hence also for $\mathcal{S}_p(\partial H)$. Thus Lemma 6.4 can be restated more explicitly as follows.

Lemma 6.5. *The image of* $\mathcal{O}_p[\widetilde{\Gamma}_\Sigma^{++}]$ *in* $\mathrm{End}(\mathcal{S}_p(\Sigma))$ *is the* $\mathcal{O}_p$*-submodule spanned by the endomorphisms*

$$Z(H_1\#H_2, \mathrm{C}'(2c) \cup \mathfrak{b}_\sigma)\ ,$$

where σ *runs through the colorings of* T.

This completes the second step of the proof of Theorem 2.4. For the third and last step, we must first recall the orthogonal lollipop bases for the integral TQFT modules which we constructed in [7]. The following discussion is valid for the lattices $\mathcal{S}(\Sigma)$ as defined in (11). The elements of an orthogonal lollipop basis are denoted by $\{\tilde{\mathfrak{b}}_\sigma\}$, and are again indexed by (small admissible) colorings σ of a lollipop tree for a handlebody with boundary the given surface. Of course, for a given surface this basis (as well as the original basis $\{\mathfrak{b}_\sigma\}$ defined in [6]) depends on a choice of handlebody and lollipop tree with it. The fact that our notation in what follows does not indicate this should cause no confusion. Also we note that, in the proof we present, besides our original surface Σ of genus g with one banded point colored $2c$, we also need

to consider ∂H, which is a surface of genus $2g$ with no colored points, and the basis of $\mathcal{S}(\partial H)$ associated to the lollipop tree T (see Figure 4). For this reason, in the following discussion of bases, we use the letter $2e$ to denote the color of the colored banded point and thus of the trunk edge (see formulas (15) and (16) below). In one case, this trunk color is $2c$ and in the other case it is zero. The discussion in §2 of bases, when modified in this way, applies as well to $\mathcal{S}(\partial H)$.

The important property of the orthogonal lollipop basis for us is that $\{\tilde{\mathfrak{b}}_\sigma\}$ is orthogonal with respect to the Hopf pairing

$$((\ ,\ ))\colon \mathcal{S}(\Sigma)\times\mathcal{S}(\Sigma)\longrightarrow\mathcal{O}$$

which is based on placing skeins in neighborhoods of linked lollipop trees and evaluating. See §3 of [7] for more details about this pairing. The linked lollipop trees defining the Hopf pairing are as in the left part of Figure 3 in the case where the surface is $\Sigma_g(2c)$, and as in Figure 4 in the case where the surface is ∂H.

In [7], there is also defined a basis $\{\tilde{\mathfrak{b}}^\#_\sigma\}$ for the dual lattice

$$\mathcal{S}^\#(\Sigma)=\{x\in V(\Sigma)\colon ((x,y))\in\mathcal{O}\ \ \forall y\in\mathcal{S}(\Sigma)\}$$

so that [7], Remark 3.5,

$$((\tilde{\mathfrak{b}}_\sigma,\tilde{\mathfrak{b}}^\#_{\sigma'}))\sim\delta^\sigma_{\sigma'}\ .$$

Moreover, $\tilde{\mathfrak{b}}^\#_\sigma$ is a power of h^{-1} times $\tilde{\mathfrak{b}}_\sigma$. For our computation below, it will be convenient to express this rescaling by a power of h^{-1} as follows. Given a coloring σ of a lollipop tree, let $A(\sigma)=\sum a_i$ denote the sum of the half-colors at the stick edges (see Figure 1). Then for a certain skein element x_σ (see [7], eq. (6), Corollary 3.4) we have

$$\tilde{\mathfrak{b}}_\sigma=h^{-\lfloor(A(\sigma)-e)/2\rfloor}x_\sigma \tag{15}$$

and

$$\tilde{\mathfrak{b}}^\#_\sigma=h^{-\lceil(A(\sigma)+e)/2\rceil}x_\sigma \tag{16}$$

where $\lfloor x\rfloor$ is the greatest integer $\le x$, and $\lceil x\rceil$ is the smallest integer $\ge x$.

We are now ready for the final step in the proof of Theorem 2.4. Recall the lollipop tree T in the genus $2g$ handlebody H. If σ is a coloring of T, let

$$Z(\sigma)=Z(H_1\#H_2,\mathrm{C}'(2c)\cup\tilde{\mathfrak{b}}_\sigma)\ .$$

The endomorphisms $Z(\sigma)$ span the image of $\mathcal{O}_p[\widetilde{\Gamma}^{++}_\Sigma]$ in $\mathrm{End}(\mathcal{S}_p(\Sigma))$ by Lemma 6.5. We shall compute the matrix of $Z(\sigma)$ with respect to the orthogonal lollipop basis of $\mathcal{S}_p(\Sigma)$. We shall find that the matrix of $Z(\sigma)$ is either zero or a scalar multiple of an elementary matrix.

To carry out this computation, we need to fix some notation. Recall that the orthogonal lollipop basis of $\mathcal{S}_p(\Sigma)$ consists of the $\tilde{\mathfrak{b}}_\sigma$ where σ runs through the colorings of G_1 with trunk color $2c$. For two such colorings σ_1 and σ_2, let E_{σ_2,σ_1} be

the elementary matrix with (σ_2, σ_1) entry equal to one, and all other entries equal to zero. (Thus, the corresponding endomorphism sends $\tilde{\mathfrak{b}}_{\sigma_1}$ to $\tilde{\mathfrak{b}}_{\sigma_2}$, and all other basis vectors to zero.) Next, as G_i' is simply G_i in a different position, we will identify colorings of G_i with those of G_i'. There is also a graph isomorphism $r\colon G_2 \to G_1$ that is given by reflection across a horizontal axis. If σ is a coloring of G_1, then r induces a coloring $\sigma \circ r$ of G_2, which we denote by $r(\sigma)$. Let T' denote the graph $G_1' \cup \mathrm{C}' \cup G_2'$. Given two colorings σ_2, σ_1 of G_1 which are colored $2c$ on the trunk edge, let $\sigma_1 \#_c \sigma_2$ denote the coloring of T' obtained by coloring G_1' by σ_1, G_2' by $r(\sigma_2)$, and C' by $2c$. Finally, we call $o\colon T \to T'$ the graph isomorphism that sends a loop to the loop that clasps it.

Lemma 6.6. *Let σ be a coloring of T. Then $Z(\sigma) = 0$ unless $\sigma = o(\sigma_1 \#_c \sigma_2)$ for some colorings σ_1 and σ_2 of G_1 with trunk edge colored by $2c$. Conversely, if $\sigma = o(\sigma_1 \#_c \sigma_2)$, then the matrix of $Z(\sigma)$ is a scalar multiple of the elementary matrix E_{σ_2,σ_1}. The scalar multiple is h times a unit in $\mathcal{O}_p$ if σ_1 is odd and σ_2 is even. (See Definition 2.3 for the definition of odd and even colorings.) In all other cases, the scalar multiple is a unit.*

Proof. The matrix entry $Z(\sigma)_{\sigma_2,\sigma_1}$ is, up to units, the evaluation of the skein in S^3 given by placing $\tilde{\mathfrak{b}}_\sigma$ in H, $\tilde{\mathfrak{b}}_{\sigma_1}$ in $\mathcal{H}_1$, and $\tilde{\mathfrak{b}}^{\#}_{r(\sigma_2)}$ in $\mathcal{H}_2$, with the last two connected by C' colored $2c$, and thus determining a coloring of the graph T'. Note that every coloring σ of T is of the form $o(\sigma_1' \#_{c'} \sigma_2')$ for some σ_1', c', and σ_2'. Using orthogonality for ∂H, we see that $Z(\sigma)_{\sigma_2,\sigma_1}$ is zero unless $\sigma_1' = \sigma_1$, $c' = c$, and $\sigma_2' = \sigma_2$. This shows that $Z(\sigma)$ is either zero (if $c' \neq c$) or a scalar multiple of the elementary matrix E_{σ_2,σ_1} (if $c' = c$ and $\sigma = o(\sigma_1 \#_c \sigma_2)$). Assume we are in the latter case. Then the scalar multiple can be computed as follows. Using (15) and (16), and $A(\sigma_1 \#_c \sigma_2) = A(\sigma_1) + A(\sigma_2)$, we have that

$$\begin{aligned} Z(\sigma)_{\sigma_2,\sigma_1} &= h^{-\lfloor (A(\sigma_1)-c)/2 \rfloor} h^{-\lceil (A(\sigma_2)+c)/2 \rceil}((\tilde{\mathfrak{b}}_{\sigma_1 \#_c \sigma_2}, x_{\sigma_1 \#_c \sigma_2})) \\ &= h^{-\lfloor (A(\sigma_1)-c)/2 \rfloor} h^{-\lceil (A(\sigma_2)+c)/2 \rceil} h^{\lceil A(\sigma_1 \#_c \sigma_2)/2 \rceil}((\tilde{\mathfrak{b}}_{\sigma_1 \#_c \sigma_2}, \tilde{\mathfrak{b}}^{\#}_{\sigma_1 \#_c \sigma_2})) \\ &\sim h^{-\lfloor (A(\sigma_1)-c)/2 \rfloor - \lceil (A(\sigma_2)+c)/2 \rceil + \lceil (A(\sigma_1)+A(\sigma_2))/2 \rceil} \\ &= \begin{cases} h & \text{if } \sigma_1 \text{ is odd and } \sigma_2 \text{ is even,} \\ 1 & \text{otherwise.} \end{cases} \end{aligned}$$

This completes the proof of Lemma 6.6. □

The proof of Theorem 2.4 in the case $p \equiv -1 \pmod 4$ (where $\mathcal{S}(\Sigma) = \mathcal{S}_p(\Sigma)$) is now completed as follows. The statement to be proved is that the image of the group algebra $\mathcal{O}_p[\tilde{\Gamma}_\Sigma^{++}]$ in $\mathrm{End}(\mathcal{S}_p(\Sigma))$ is

$$\left[\begin{array}{c|c} \mathrm{End}(\mathcal{S}_p^{\mathrm{ev}}(\Sigma)) & h\,\mathrm{Hom}(\mathcal{S}_p^{\mathrm{odd}}(\Sigma), \mathcal{S}_p^{\mathrm{ev}}(\Sigma)) \\ \hline \mathrm{Hom}(\mathcal{S}_p^{\mathrm{ev}}(\Sigma), \mathcal{S}_p^{\mathrm{odd}}(\Sigma)) & \mathrm{End}(\mathcal{S}_p^{\mathrm{odd}}(\Sigma)) \end{array}\right]$$

This is very similar to what Lemma 6.6 says, except that Lemma 6.6 expresses $Z(\sigma)$ in the orthogonal lollipop basis $\{\tilde{\mathfrak{b}}_\sigma\}$ of $\mathcal{S}_p(\Sigma)$, whereas the definition of $\mathcal{S}_p^{\mathrm{ev}}(\Sigma)$ and $\mathcal{S}_p^{\mathrm{odd}}(\Sigma)$ was in terms of the original lollipop basis $\{\mathfrak{b}_\sigma\}$. But the submodules $\mathcal{S}_p^{\mathrm{ev}}(\Sigma)$ and $\mathcal{S}_p^{\mathrm{odd}}(\Sigma)$ are the same no matter whether we use the original lollipop basis or the orthogonal lollipop basis. This is because [7], §2, there is a triangular basis change between the two bases which respects the block summands given by specifying the stick colors $2a_i$. Thus, Lemma 6.5 together with Lemma 6.6 imply Theorem 2.4 in the case $p \equiv -1 \pmod 4$.

We now consider the case $p \equiv 1 \pmod 4$. In this case, we need to be more precise about the integer weights which we put on cobordisms to resolve the framing anomaly. As mentioned in §4, changing the weight of a cobordism (M, G) multiplies the induced endomorphism $Z(M, G)$ by κ, where κ is a unit in $\mathcal{O}_p$. Thus, as long as we were working with coefficients in $\mathcal{O}_p$, we could (and did) ignore weights in the above proof. The problem in the case $p \equiv 1 \pmod 4$ is that only κ^2 lies in $\mathcal{O} = \mathbb{Z}[\zeta_p]$, but not κ itself.[14] Thus $Z(M, G)$ preserves the lattice $\mathcal{S}(\Sigma)$ if and only if the weight of M satisfies a parity condition. This condition is best formulated by saying that M together with its weight should lie in the *even cobordism category* defined in Gilmer [5]. If this is the case, we say that the weight of M is of the correct parity. We will not need the precise formulation of this condition, which is non-trivial to state. (It is *not* simply to require all weights to be even.) It will be enough for us to know that for every cobordism M and integer n, exactly one of n or $n + 1$ is a weight of the correct parity for M. Also, for the cobordisms (13) describing the representation of the extended mapping class group $\widetilde{\Gamma}_\Sigma^{++}$ at the beginning of our proof, it is alright to take the weight to be zero.

Here is, then, how to modify the above proof of Theorem 2.4 in the case $p \equiv 1 \pmod 4$ so that it holds for the lattice $\mathcal{S}(\Sigma)$ and not just for the lattice $\mathcal{S}_p(\Sigma)$. At the beginning of the proof, we equip the cobordisms (13) with weight zero. In Lemma 6.3, we add the hypothesis that both M and M' are equipped with a weight of the correct parity, then the statement holds true for $\mathcal{S}(\Sigma)$ in place of $\mathcal{S}_p(\Sigma)$. In Lemmas 6.4 and 6.5, we equip the cobordism $H_1 \# H_2$ from Σ to itself with a weight of the correct parity, then both Lemmas hold true for the image of $\mathcal{O}[\widetilde{\Gamma}_\Sigma^{++}]$ in $\mathrm{End}_{\mathcal{O}}(\mathcal{S}(\Sigma))$. We do not change anything in the computation in Lemma 6.6, but notice that $Z(\sigma)$ is now defined more precisely (by the requirement on the weight of the cobordism $H_1 \# H_2$ to be of the correct parity). Lemma 6.6 shows that the matrix of $Z(\sigma)$ is either zero or a scalar multiple of an elementary matrix E_{σ_2,σ_1}, and it also computes this scalar multiple up to a unit in $\mathcal{O}_p = \mathbb{Z}[\zeta_{4p}]$. But since we know that the matrix of $Z(\sigma)$ has coefficients in $\mathcal{O} = \mathbb{Z}[\zeta_p]$, this actually computes the scalar multiple up to a unit in $\mathcal{O}$. The remaining arguments in the proof are the same as before. This completes the proof of Theorem 2.4.

[14] As already mentioned, κ is a square root of $A^{-6-p(p+1)/2}$, so that $\kappa \in \mathbb{Z}[\zeta_p]$ if and only if $p \equiv -1 \pmod 4$. This is why $\mathcal{O}_p = \mathbb{Z}[\zeta_{4p}]$ if $p \equiv 1 \pmod 4$. In both cases, $\mathcal{O}_p$ is the minimal ring containing ζ_p and κ.

7. Proof of Theorem 2.7, Theorem 2.8, and Corollary 2.9

7.1. Recursion formulas for $\mathfrak{o}_g^{(2c)}$ and $\mathfrak{e}_g^{(2c)}$. Recall that

$$\mathfrak{o}_g^{(2c)} = \dim_{\mathbb{F}_p}(F^{\text{odd}}(\Sigma)) \quad \text{and} \quad \mathfrak{e}_g^{(2c)} = \dim_{\mathbb{F}_p}(F(\Sigma)/F^{\text{odd}}(\Sigma))$$

(where $\Sigma = \Sigma_g(2c)$) are given by the number of odd or even colorings of the lollipop tree $T_g^{(2c)}$ shown in Figure 1. In a coloring of a lollipop tree, all the colors except the loop colors must be even numbers $2a$ with $0 \leq a \leq d-1$. Recall [6] that a stick edge is an edge which meets a loop. We will call a trivalent vertex at the opposite end of a stick edge from the loop a stick vertex. We say a coloring is *balanced* at a stick vertex if the three edges which meet at the stick vertex are colored $2a$, $2b$, and $2c$ with $a+b+c \equiv 0 \pmod 2$. Otherwise the coloring is called *unbalanced* at the stick vertex. It is easy to see from Definition 2.3 that a coloring is even if and only if the number of stick vertices where the coloring is unbalanced is even.

As a building block, we consider first the lollipop tree $T_1^{(2c_1,2c_2)}$ associated to a surface of genus one with two colored points colored $2c_1$ and $2c_2$ shown in Figure 5. Note that colorings of $T_1^{(0,2c)}$ are the same as colorings of $T_1^{(2c)}$, as an arc which is colored zero can be erased. Let $\beta(c_1,c_2)$ denote the number of colorings of $T_1^{(2c_1,2c_2)}$ that are balanced at the stick vertex and $\eta(c_1,c_2)$ denote the number of colorings of $T_1^{(2c_1,2c_2)}$ that are unbalanced at the stick vertex.

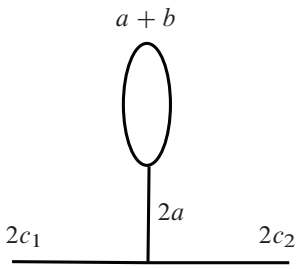


Figure 5

Lemma 7.1. *If $c_1 \geq c_2$, then*

$$\beta(c_1,c_2) = (c_2+1)(d-c_1)$$

and

$$\eta(c_1,c_2) = c_2(d-c_1).$$

Proof. Small admissibility at the top of the stick edge says simply that $0 \leq b \leq d-a-1$. Admissibility at the bottom of the stick edge says

$$c_1 - c_2 \leq a \leq \min\{c_1+c_2, 2d-1-c_1-c_2\}\,.$$

Thus $\beta(c_1, c_2)$ is either

$$\sum_{\substack{c_1-c_2\le a\le c_1+c_2\\ a\equiv c_1-c_2 \pmod 2}} (d-a) \quad \text{or} \quad \sum_{\substack{c_1-c_2\le a\le 2d-1-c_1-c_2\\ a\equiv c_1-c_2 \pmod 2}} (d-a)$$

depending on which upper limit for a is smaller. But it turns out that both these sums sum to $(c_2+1)(d-c_1)$. The unbalanced case is done similarly. □

Proposition 7.2. *The numbers $\mathfrak{e}_g^{(2c)}$ and $\mathfrak{o}_g^{(2c)}$ satisfy the recursion formulas*

$$\mathfrak{e}_1^{(2c)} = \delta_1^{(2c)} = D_1^{(2c)} = d-c \quad \text{and} \quad \mathfrak{o}_1^{(2c)} = 0, \tag{17}$$

$$\mathfrak{e}_{g+1}^{(2c)} = \sum_{a=0}^{d-1} (\mathfrak{e}_g^{(2a)}\beta(a,c) + \mathfrak{o}_g^{(2a)}\eta(a,c)), \tag{18}$$

$$\mathfrak{o}_{g+1}^{(2c)} = \sum_{a=0}^{d-1} (\mathfrak{o}_g^{(2a)}\beta(a,c) + \mathfrak{e}_g^{(2a)}\eta(a,c)). \tag{19}$$

Proof. This follows from the discussion preceding Lemma 7.1. □

Of course the numbers $D_g^{(2c)} = \mathfrak{e}_g^{(2c)} + \mathfrak{o}_g^{(2c)}$ and $\delta_g^{(2c)} = \mathfrak{e}_g^{(2c)} - \mathfrak{o}_g^{(2c)}$ can also be computed recursively from (17)–(19). For later use, we remark that

$$\delta_{g+1}^{(2c)} = \sum_{a=0}^{d-1} (\beta(a,c) - \eta(a,c))\, \delta_g^{(2a)} = \sum_{a=0}^{d-1} (d - \max\{a,c\})\, \delta_g^{(2a)}\,. \tag{20}$$

It is not hard to get explicit formulas for low genus in this way, such as

$$\mathfrak{e}_2^{(2c)} = ((c+1)p^3 - (3c^2+3c)p^2 + (2c^3-3c-1)p + 2c^3 + 3c^2 + c)/24, \tag{21}$$

$$\mathfrak{o}_2^{(2c)} = (cp^3 - (3c^2+3c)p^2 + (2c^3+6c^2+3c)p - (2c^3+3c^2+c))/24, \tag{22}$$

$$\delta_2^{(2c)} = (p^3 - (6c^2+6c+1)p + 4c^3 + 6c^2 + 2c)/24, \tag{23}$$

$$\mathfrak{o}_3 = (p-3)(p-2)(p-1)^2 p(p+1)/2880, \tag{24}$$

$$\mathfrak{e}_3 = (p-1)p(p+1)^2(p+2)(p+3)/2880, \tag{25}$$

$$\delta_3 = (p-1)p(p+1)(p^2+1)/240, \tag{26}$$

$$\delta_4 = (p-1)p(p+1)(17p^4+31p^2+24)/40320, \tag{27}$$

$$\delta_5 = (p-1)p(p+1)(31p^6+82p^4+103p^2+72)/725760. \tag{28}$$

7.2. Proof of Theorem 2.7. We must prove formula (5) for $\delta_g^{(2c)}$. To this end, let us reformulate the recursion relation (20) in terms of the Verlinde algebra, as follows. The Verlinde algebra V_p for the SO(3)-TQFT at the p-th root of unity (where $p = 2d+1$) is the quotient algebra

$$V_p = K[z]/(e_d - e_{d-1})$$

where $K = \mathbb{Q}(\zeta_p)$ is the cyclotomic field and where $e_i = e_i(z)$ is the Chebyshev polynomial of the second kind defined recursively by $e_0 = 1, e_1(z) = z$, and $e_{n+1}(z) = ze_n(z) - e_{n-1}(z)$ (see Blanchet *et al.* [3] and [4].) In V_p, one has

$$e_{d+i} = e_{d-1-i} \ , \tag{29}$$

so that the linear basis $\{e_0, e_1, \ldots, e_{d-1}\}$ of V_p is the same, up to reordering, as the basis $\{e_0, e_2, \ldots, e_{2d-2}\}$. If $x \in V_p$, we denote by $M(x) = (M(x)_{ji})$ the $d \times d$ matrix describing multiplication by x in the basis $\{e_0, e_2, \ldots, e_{2d-2}\}$. Here, we index the matrix entries from 0 to $d-1$ so that

$$x\, e_{2i} = \sum_{j=0}^{d-1} M(x)_{ji} e_{2j} \ .$$

The following result identifies $(-1)^c \delta_g^{(2c)}$ as a matrix coefficient.

Proposition 7.3. *Define* $\widehat{\mathcal{K}} \in V_p$ *by*

$$\widehat{\mathcal{K}} = \sum_{n=0}^{d-1} (-1)^n (d-n) e_{2n} \ .$$

Then for $0 \le c \le d-1$, *we have*

$$(-1)^c \delta_g^{(2c)} = M(\widehat{\mathcal{K}}^g)_{c,0} \ .$$

Proof. Since e_0 is the identity element of the algebra V_p, we have $\widehat{\mathcal{K}}^g e_0 = \widehat{\mathcal{K}}^g$ and it is enough to show that

$$\widehat{\mathcal{K}}^g = \sum_{c=0}^{d-1} (-1)^c \delta_g^{(2c)} e_{2c} \ . \tag{30}$$

We prove (30) by induction on g. The formula certainly holds for $g = 0, 1$ since $\delta_0^{(0)} = 1$, $\delta_0^{(2c)} = 0$ $(c \neq 0)$ and $\delta_1^{(2c)} = \mathfrak{e}_1^{(2c)} = d - c$. The induction step follows from our recursion formula (20), since the matrix coefficients of $M(\widehat{\mathcal{K}})$ are given by

$$M(\widehat{\mathcal{K}})_{ji} = (-1)^{i+j} (d - \max\{i, j\}) \ ,$$

as is easily checked using the fact that the structure constants of the Verlinde algebra in the basis $\{e_0, e_2, \ldots, e_{2d-2}\}$ encode the admissibility conditions at the trivalent vertices of a colored graph. □

The original Verlinde numbers $D_g^{(2c)}$ can also be described as matrix coefficients: put

$$\mathcal{K} = \sum_{n=0}^{d-1}(d-n)e_{2n} = \sum_{n=0}^{d-1} e_{2n}^2 ,$$

then

$$D_g^{(2c)} = M(\mathcal{K}^g)_{c,0} . \tag{31}$$

Moreover, it is well-known how to diagonalize the matrix $M(\mathcal{K})$ using the so-called S-matrix, and this diagonalization gives a proof of the Verlinde formula (6) (see Remark 7.6 below). We now apply the same method to the matrix $M(\widehat{\mathcal{K}})$.

Here is a formulation of the basic diagonalization result. Let us write $q = \zeta_p$. Let $S = (S_{ij})$ be the $d \times d$ matrix defined by

$$S_{ij} = q^{(2i+1)(2j+1)} - q^{-(2i+1)(2j+1)} \qquad (i, j = 0, 1, \ldots, d-1) .$$

This matrix is $q - q^{-1}$ times the S-matrix of the $SO(3)$-TQFT, and one has

$$S^{-1} = -\tfrac{1}{p}S$$

(this last statement can also be checked by direct computation).

Lemma 7.4. *Let* $Q = \mathrm{diag}(-q^{2j+1} - q^{-2j-1})_{j=0,1,\ldots,d-1}$. *Then*

$$M(z) = SQS^{-1} = -\tfrac{1}{p}SQS \tag{32}$$

Proof. This statement can also be checked by a direct computation (which is given in our paper [9]). Here is how to deduce it from results in Blanchet *et al.* [4]. On page 913 of that paper, one finds elements $v_j \in V_p$ which are eigenvectors for the multiplication by z:

$$zv_j = -(q^{j+1} + q^{-j-1})v_j .$$

It is observed there that $v_0, v_1, \ldots v_{d-1}$ form a basis of V_p, but using (29), one sees that this is the same, up to reordering, as $v_0, v_2, \ldots v_{2d-2}$, which is therefore also a basis. The matrix Q is the matrix of multiplication by z in this latter basis. Moreover, using (29) again, one can check that in our notation v_{2j} is given by

$$v_{2j} = \frac{1}{q - q^{-1}} \sum_{i=0}^{d-1} S_{ij} e_{2i} .$$

This proves the lemma. □

Let G_j denote the Galois automorphism of the cyclotomic field $Q(q)$ (recall $q = \zeta_p$ is a primitive p-th root of unity) defined by $G_j(q) = q^j$ $(j = 1, \ldots, p-1)$. Thinking of $\widehat{\mathcal{K}}$ as a polynomial in z, we see from (32) that the eigenvalues of $M(\widehat{\mathcal{K}})$ are given by $G_{2j+1}(\Lambda)$ $(j = 0, \ldots, d-1)$, where

$$\Lambda = \widehat{\mathcal{K}}(z)\Big|_{z=-q-q^{-1}} = \sum_{n=0}^{d-1}(-1)^n(d-n)\frac{q^{2n+1}-q^{-2n-1}}{q-q^{-1}} = \frac{1}{(q+q^{-1})^2}.$$

(To see the last equality, multiply both sides by $(q-q^{-1})(q+q^{-1})^2$ and compare the coefficients of the resulting polynomials.)

Thus (32) gives

$$\begin{aligned} M(\widehat{\mathcal{K}}^g)_{c,0} &= -\frac{1}{p}\sum_{j=0}^{d-1} S_{cj}G_{2j+1}(\Lambda^g)S_{j0} \\ &= -\frac{1}{p}\sum_{j=0}^{d-1} G_{2j+1}((q^{2c+1}-q^{-2c-1})(q-q^{-1})\Lambda^g) \\ &= -\frac{1}{p}\sum_{j=1}^{d} G_j((q^{2c+1}-q^{-2c-1})(q-q^{-1})\Lambda^g). \end{aligned}$$

The last equality is justified by the fact that both $(q^{2c+1}-q^{-2c-1})(q-q^{-1})$ and Λ lie in the real subfield $\mathbb{Q}(q+q^{-1})$ of the cyclotomic field $\mathbb{Q}(q)$.

Substituting now $q = -e^{\pi i/p}$ (which is a primitive p-th root of unity), and using Proposition 7.3, we get (5) for $\delta_g^{(2c)}$ in Theorem 2.7.

Remark 7.5. In [9], eq. (5), we wrote down a different formula for $\delta_g^{(2c)}$ which was based on the following expression for Λ as a polynomial in $q = \zeta_p$:

$$\Lambda = \lceil d/2 \rceil + \sum_{k=1}^{d-1}(-1)^k \lceil (d-k)/2 \rceil (q^{2k}+q^{-2k}) \, .$$

We thank Don Zagier for pointing out that this is equal to $1/(q+q^{-1})^2$, which leads to the simpler formula for $\delta_g^{(2c)}$ given in Theorem 2.7.

Remark 7.6. In the same way, one gets a proof of the Verlinde formula (6) by expressing $D_g^{(2c)}$ as a coefficient of the matrix $M(\mathcal{K})$ as in (31) and computing the eigenvalues of this matrix. The computation is exactly the same, except that Λ must be replaced with

$$\mathcal{K}(z)\Big|_{z=-q-q^{-1}} = \frac{-p}{(q-q^{-1})^2}$$

(see [4], p. 913).

7.3. Proof of Theorem 2.8. Observe that $\delta_1^{(2c)} = d - c$ is a polynomial in $p = 2d + 1$ and c of total degree one, and

$$\delta_{g+1}^{(2c)} = \sum_{a=0}^{d-1} (d-a)\, \delta_g^{(2a)} + \sum_{a=0}^{c-1} (a-c)\, \delta_g^{(2a)} , \tag{33}$$

as follows easily from (20). Using the well-known formula

$$\sum_{n=0}^{N-1} n^k = \frac{N^{k+1}}{k+1} + O(N^k) \tag{34}$$

(where $O(N^k)$ is a polynomial in N of degree at most k), one sees by induction on g that $\delta_g^{(2c)}$ is a polynomial of total degree at most $2g-1$ in p and c. Let L_g the homogeneous part of degree $2g-1$ in $\delta_g^{(2c)}$. We must show that

$$L_g = (-1)^{g-1} \sum_{k=1}^{2g} 2(2^k - 1)\, \frac{B_k}{k!}\, \frac{c^{2g-k}}{(2g-k)!}\, p^{k-1} . \tag{35}$$

This will also be proved by induction. It is certainly true for $g = 1$. To perform the induction step, assume it is true for g. Using (33) and (34), it is easy to see that a monomial $c^{2g-k} p^{k-1}$ in L_g gives rise to a term

$$\frac{-c^{2g+2-k} p^{k-1} + 2^{k-2g-2} p^{2g+1}}{(2g-k+1)(2g-k+2)} \tag{36}$$

in L_{g+1}. We must show that the coefficient of $c^{2g+2-k} p^{k-1}$ in L_{g+1} is given by (35) with $g+1$ in place of g. This is immediate from (36) for $k < 2g+2$, while for $k = 2g+2$ it follows from the identity

$$\sum_{k=0}^{2g+2} 2^k (2^k - 1) \binom{2g+2}{k} B_k = 0 . \tag{37}$$

Identity (37) follows from Exercises 12, 17, 19, 21, and 22, in [12], Chapter 15.[15]

7.4. A residue formula for $D_g^{(2c)}$. For the proof of Corollary 2.9, we need the following expression for the Verlinde formula (6) which is computed using the residue theorem. This computation is well-known in the case $c = 0$ (see the references in [4].) If $c \neq 0$, however, an additional binomial coefficient appears in the formula, which we have not seen in the literature. Therefore we sketch the computation here. We use the notation

$$\mathrm{s}(t) = \frac{\sinh(t)}{t} = \sum_{k=0}^{\infty} \frac{t^{2k}}{(2k+1)!} . \tag{38}$$

[15] Warning: there is a factor 2^{n-1} (resp. a^{n-1}) missing in the statements of Exercises 21 (resp. 22).

Proposition 7.7 (residue formula for $D_g^{(2c)}$). *For $g \geq 1$, one has*

$$D_g^{(2c)} = \frac{(-p)^g}{2}\Big(4^{1-g}\frac{2c+1}{p}\,\mathrm{res}_{t=0}\Big(\frac{2pt}{e^{2pt}-1}\frac{\mathrm{s}((2c+1)t)}{\mathrm{s}(t)^{2g-1}}\frac{dt}{t^{2g-1}}\Big) - \binom{c+g-1}{2g-2}\Big). \tag{39}$$

Proof (*cf.* [4], *p. 914*). We apply the residue theorem to the meromorphic 1-form

$$\frac{(z^{2c+1}-z^{-2c-1})dz}{z(z^p-1)(z-z^{-1})^{2g-1}}.$$

This form has simple poles at all non-trivial p-th roots of unity, and the sum of the residues at these poles is $-2D_g^{(2c)}/(-p)^g$ by the Verlinde formula (6). The poles at $z = \pm 1$ give rise to the residue term in (39), and the pole at $z = 0$ gives rise to the binomial coefficient in (39). (This term would be absent in the case $c = 0$.) There are no other poles. Thus the result follows from the residue theorem. □

Using the power series expansions for $t/(e^t-1)$ in (7), and for $\mathrm{s}(t)$ in (38), it is easy to see from (39) that for $g \geq 2$, $D_g^{(2c)}$ is a polynomial of total degree $3g-2$ in p and c. Moreover, it is easy to get an explicit formula for the leading order terms. One finds that for $g \geq 2$, and in degrees $\geq 3g-3$, the polynomial $D_g^{(2c)}/2$ is given by the expression appearing on the right hand side of Eq. (9) in Corollary 2.9.

Corollary 2.9 follows from this by observing that both $\mathfrak{e}_g^{(2c)}$ and $\mathfrak{o}_g^{(2c)}$ coincide with $D_g^{(2c)}/2$ up to addition of some polynomial of degree $2g-1$, by Theorem 2.8.

7.5. A residue formula for $\delta_g^{(2c)}$. Here is an analog of Proposition 7.7 for $\delta_g^{(2c)}$.

Proposition 7.8 (residue formula for $\delta_g^{(2c)}$). *For $g \geq 1$, one has*

$$\delta_g^{(2c)} = \frac{(-1)^g}{2}\Big(\frac{4^{1-g}}{p}\,\mathrm{res}_{t=0}\Big(\frac{2pt}{e^{2pt}+1}\frac{\cosh((2c+1)t)\cosh(t)}{\mathrm{s}(t)^{2g}}\frac{dt}{t^{2g+1}}\Big) + \frac{2c+1}{2g-1}\binom{c+g-1}{2g-2}\Big). \tag{40}$$

Proof. Consider the meromorphic 1-form

$$\frac{(z^{2c+1}-z^{-2c-1})(z-z^{-1})dz}{z(z^p-1)(z+z^{-1})^{2g}}.$$

This form has simple poles at all non-trivial p-th roots of unity, and the sum of the residues at these poles is $(-1)^{c+1}2\delta_g^{(2c)}$ by formula (5). The poles at $z = \pm i$ give rise to the residue term in (40), and the pole at $z = 0$ gives rise to the binomial coefficient term in (40). There are no other poles. Thus the result follows, as before, from the residue theorem. □

Remark 7.9. Formula (40) shows again that $\delta_g^{(2c)}$ is a polynomial in c and p of total degree $2g-1$. Using

$$\frac{t}{e^t+1} = \sum_{n=1}^{\infty}(1-2^n)B_n\frac{t^n}{n!} \tag{41}$$

(as follows easily from (7)), one can write down an explicit formula for this polynomial in terms of Bernoulli numbers. This could be used to give another proof of Theorem 2.8. Below, we make two more remarks about this polynomial.

First, the contribution to $\delta_g^{(2c)}$ coming from the residue term in (40) is of the form p times a polynomial in $(2c+1)^2$ and p^2. (This is because both $\cosh(t)$ and $\mathrm{s}(t)$ are even functions of t; note also that there is no constant term in (41).) Thus, any monomial $c^n p^m$ appearing in $\delta_g^{(2c)}$ has m odd or zero. (See for example (23).)

Second, the contribution to $\delta_g^{(2c)}$ coming from the binomial coefficient is zero for $c < g-1$. In particular, for $g \geq 2$, the one-variable polynomial δ_g obtained by putting $c=0$ in $\delta_g^{(2c)}$ is an odd polynomial in p. We claim that for $g \geq 2$ this polynomial δ_g is always divisible by

$$\delta_2 = \mathfrak{e}_2 = D_2 = p(p^2-1)/24\,.$$

(See for example formulas (26)–(28)). This can be seen as follows. First, divisibility by p is clear since δ_g is an odd polynomial in p. Next, running the residue computation in the proof of Proposition 7.8 backwards in the special case $c=0$, $p=1$, one finds that the right hand side of (40) is zero in this case. Thus the polynomial δ_g is divisible by $p-1$. But since δ_g is odd, it must then also be divisible by $p+1$. This proves the claim.

As mentioned in the introduction, we believe that the polynomial $\delta_g^{(2c)}$ and its specialization δ_g should have an algebro-geometric interpretation. If so, there should probably be a geometric reason behind the above-mentioned properties of these polynomials.

8. Further Comments

For $g \geq p-1$, Gow [11] has constructed $p-1$ irreducible modular K-representations of the symplectic group $\mathrm{Sp}(2g,K)$, where K is a field of characteristic p. Gow denotes these representations by

$$V(g,k) \qquad (g-p+2 \leq k \leq g)\,.$$

The representation $V(g,k)$ is a subquotient of $\Lambda^k V$ where $V \simeq K^{2g}$ is the standard representation of $\mathrm{Sp}(2g,K)$. If K is algebraically closed, then $V(g,k)$ is the fundamental module with highest weight ω_k; see [11], Corollary 2.4.

The dimensions of these representations of $\mathrm{Sp}(2g,K)$ depend only on the characteristic p of the field K. It turns out that for $p=5$, the dimensions of the four

representations constructed by Gow coincide with the dimensions of our irreducible factors $F^{\mathrm{odd}}(\Sigma_g(2c))$ and $F(\Sigma_g(2c))/F^{\mathrm{odd}}(\Sigma_g(2c))$.

Theorem 8.1. *For $p = 5$ and $g \geq 4$, we have*

$$(\dim V(g, g+1-n))_{n=1,2,3,4} = (\mathfrak{e}_g^{(0)}(5), \mathfrak{e}_g^{(2)}(5), \mathfrak{o}_g^{(2)}(5), \mathfrak{o}_g^{(0)}(5)) \,.$$

This is proved in [9]. It would be interesting to know whether these equalities of dimensions come from isomorphisms of the corresponding $\mathrm{Sp}(2g, \mathbb{F}_p)$-representations. In [9], we give an explicit formula for the dimensions of the $V(g,k)$ analogous to formulas (5) and (6) for $\delta_g^{(2c)}$ and $D_g^{(2c)}$. We remark that for every prime $p \geq 5$ we have *a priori* as many irreducible representations of $\mathrm{Sp}(2g, \mathbb{F}_p)$ as Gow.[16] But it appears that for $p > 5$ the dimensions of the $V(g,k)$ and the dimensions of our irreducible factors are different.

References

[1] J. E. Andersen, Mapping class groups do not have Kazhdan's property (T). Preprint 2007. arXiv:0706.2184

[2] J. E. Andersen and G. Masbaum, Involutions on moduli spaces and refinements of the Verlinde formula. *Math. Ann.* **314** (1999), 291–326. MR 1697447 Zbl 0943.14016

[3] C. Blanchet, N. Habegger, G. Masbaum, and P. Vogel, Three-manifold invariants derived from the Kauffman bracket. *Topology* **31** (1992), 685–699. MR 1191373 Zbl 0771.57004

[4] C. Blanchet, N. Habegger, G. Masbaum, and P. Vogel, Topological quantum field theories derived from the Kauffman bracket. *Topology* **34** (1995), 883–927. MR 1362791 Zbl 0887.57009

[5] P. M. Gilmer, Integrality for TQFTs. *Duke Math J.* **125** (2004), 389–413. MR 2096678 Zbl 1107.57020

[6] P. M. Gilmer and G. Masbaum, Integral lattices in TQFT. *Ann. Sci. École Norm. Sup.* (4) **40** (2007), 815–844. MR 2382862 Zbl 1178.57023

[7] P. M. Gilmer and G. Masbaum, Integral topological quantum field theory for a one-holed torus. *Pacific J. Math.* **252** (2011), 93–112. MR 2862143 Zbl 1232.57023

[8] P. M. Gilmer and G. Masbaum, Maslov index, Lagrangians, mapping class groups and TQFT. *Forum Math.* **25** (2013), 1067–1106. MR 3100961 Zbl 06220101

[9] P. M. Gilmer and G. Masbaum, Dimension formulas for some modular representations of the symplectic group in the natural characteristic. *J. Pure Appl. Algebra* **217** (2013), 82–86. MR 2965906 Zbl 1268.20047

[10] P. M. Gilmer, G. Masbaum, and P. van Wamelen, Integral bases for TQFT modules and unimodular representations of mapping class groups. *Comment. Math. Helv.* **79** (2004), 260–284. MR 2059432 Zbl 1055.57026

[16] *A priori,* we have $p-1$ irreducible representations of $\mathrm{Sp}(2g, \mathbb{F}_p)$, since we have two of them for each $0 \leq c \leq (p-3)/2$). For $g \geq 3$, these representations are all non-trivial, but in principle some of them could be isomorphic, although we don't expect this to happen.

[11] R. Gow, Construction of $p-1$ irreducible modules with fundamental highest weight for the symplectic group in characteristic p. *J. London Math. Soc.* (2) **58** (1998) 619–632. MR 1678154 Zbl 0974.20032

[12] K. Ireland and M. Rosen, *A classical introduction to modern number theory.* Second ed. Graduate texts in mathematics 84. Springer Verlag, New York etc., 1990. MR 1070716 Zbl 0712.11001

[13] L. H. Kauffman, State models and the Jones polynomial. *Topology* **26** (1987), 395–407. MR 0899057 Zbl 0622.57004

[14] G. Masbaum, in preparation.

[15] G. Masbaum and A. W. Reid, All finite groups are involved in the mapping class group. *Geom. Topol.* **16** (2012), 1393–1411. MR 2967055 Zbl 1254.57018

[16] G. Masbaum and J. D. Roberts, A simple proof of integrality of quantum invariants at prime roots of unity. *Math. Proc. Cambridge Philos. Soc.* **121** (1997), 443–454. MR 1434653 Zbl 0882.57010

[17] J. D. Roberts, Irreducibility of some quantum representations of mapping class groups. *J. Knot Theory Ramifications* **10** (2001), 763–767. MR 1839700 Zbl 1001.57036

[18] V. G. Turaev, *Quantum invariants of knots and 3-manifolds.* de Gruyter Studies in Mathematics 18. Walter de Gruyter, Berlin, 1994. Second revised ed., Walter de Gruyter, Berlin, 2010. MR 1292673 MR 2654259 (second ed.) Zbl 0812.57003 Zbl 1213.57002 (second ed.)

[19] K. Walker, *On Witten's 3-manifold invariants.* Preprint 1991. http://canyon23.net/math/

[20] E. Witten, On quantum gauge theories in two dimensions. *Comm. Math. Phys.* **141** (1991), 153–209. MR 1133264 Zbl 0762.53063

[21] D. Zagier, Elementary aspects of the Verlinde formula and the Harder–Narasimhan–Atiyah–Bott formula. In M. Teicher (ed.), *Proceedings of the Hirzebruch 65 Conference on Algebraic Geometry.* Held at Bar-Ilan University, Ramat Gan, May 2–7, 1993. Israel Mathematical Conference Proceedings 9. Bar-Ilan University, Gelbart Research Institute for Mathematical Sciences, Ramat Gan; distributed by the American Mathematical Society, Providence, RI, 1996, 445–462 MR 1360519 MR 1360492 (collection) Zbl 0854.14020 Zbl 0828.00035 (collection)

Received January 24, 2012

Patrick M. Gilmer, Department of Mathematics, Louisiana State University, Baton Rouge, U.S.A.

E-mail: gilmer@math.lsu.edu

Gregor Masbaum, Institut de Mathématiques de Jussieu (UMR 7586 du CNRS), Paris, France

E-mail: masbaum@math.jussieu.fr