Pacific Journal of Mathematics

INTEGRAL TOPOLOGICAL QUANTUM FIELD THEORY FOR A ONE-HOLED TORUS

PATRICK M. GILMER AND GREGOR MASBAUM

INTEGRAL TOPOLOGICAL QUANTUM FIELD THEORY FOR A ONE-HOLED TORUS

PATRICK M. GILMER AND GREGOR MASBAUM

We give new explicit formulas for the representations of the mapping class group of a genus-one surface with one boundary component which arise from integral TQFT. Our formulas allow the straightforward computation of the *h*-adic expansion of the TQFT-matrix associated to a mapping class. Truncating the *h*-adic expansion gives an approximation of the representation by representations into finite groups. As a special case, we study the induced representations over finite fields and identify them up to isomorphism. The key technical ingredient of the paper are new bases of the integral TQFT modules which are orthogonal with respect to the Hopf pairing. We construct these orthogonal bases in arbitrary genus, and briefly describe some other applications of them.

1. Introduction

Consider the integral topological quantum field theory (TQFT) studied in [Gilmer 2004; Gilmer and Masbaum 2007]. Associated to a compact oriented surface Σ and an odd prime p, there is a free lattice (i.e., a free finitely generated module) $\mathscr{S}_p^+(\Sigma)$ over the ring of cyclotomic integers $\mathbb{O}_p^+ = \mathbb{Z}[\zeta_p]$ formed by adjoining to $\mathbb{Z}$ a primitive p-th root of unity ζ_p. Tensoring $\mathscr{S}_p^+(\Sigma)$ with the cyclotomic field $\mathbb{Q}(\zeta_p)$ yields a version of the Reshetikhin–Turaev TQFT associated with the Lie group SO(3), and we think of $\mathscr{S}_p^+$ as an integral refinement of that theory. See [Gilmer and Masbaum 2007], henceforth abbreviated [GM2007], for more details.

There is a natural representation ρ_p of a certain central extension of Γ_Σ, the mapping class group of Σ, on the lattice $\mathscr{S}_p^+(\Sigma)$. Let $h = 1 - \zeta_p$; this is a prime in $\mathbb{O}_p^+$. For every $N \geq 0$, the representation ρ_p induces a representation $\rho_{p,N}$ on

$$\mathscr{S}_{p,N}^+(\Sigma) = \mathscr{S}_p^+(\Sigma)/h^{N+1}\mathscr{S}_p^+(\Sigma),$$

which is a free module over the quotient ring $\mathbb{O}_p^+/h^{N+1}\mathbb{O}_p^+$. Note that for $N = 0$ this ring is the finite field $\mathbb{F}_p$, so that $\rho_{p,0}$ is a representation on a finite-dimensional

$\mathbb{F}_p$-vector space. The representation $\rho_{p,0}$ factors through the mapping class group Γ_Σ [Gilmer and Masbaum 2009], but this is not the case for $\rho_{p,N}$ when $N > 0$.

Loosely speaking, we refer to the sequence of representations $\rho_{p,N}$ as the h-adic expansion[1] of the TQFT representation ρ_p. Note that each $\rho_{p,N}$ takes values in a finite group, since $\mathcal{S}^+_{p,N}(\Sigma)$ is of finite rank over $\mathbb{O}^+_p/h^{N+1}\mathbb{O}^+_p$, which itself is finite. Thus the h-adic expansion approximates the TQFT-representation ρ_p by representations into finite groups. Moreover, the natural map

$$\mathbb{O}^+_p = \mathbb{Z}[\zeta_p] \longrightarrow \varprojlim \mathbb{O}^+_p/h^{N+1}\mathbb{O}^+_p \cong \mathbb{Z}_p[\zeta_p]$$

is injective. (Here $\mathbb{Z}_p$ denotes the p-adic integers.) The last isomorphism comes from the fact that $(h^{p-1}) = (p)$ as ideals in $\mathbb{Z}[\zeta_p]$. Thus the h-adic expansion of the TQFT-representation ρ_p is complete in the sense that if a mapping class is detected by ρ_p then it is also detected by $\rho_{p,N}$ for all big enough N.

The image of ρ_p is usually infinite [Funar 1999; Masbaum 1999]. In this case, the images of $\rho_{p,N}$ are finite groups whose size must increase as $N \to \infty$.

We believe these representations into finite groups deserve further study. Unfortunately, the known formulas for ρ_p are not well suited to computing the h-adic expansion explicitly in practice, and new techniques are needed. In this paper we complete the first step in this direction. That is: we compute explicit matrices for the h-adic expansion in the case when $\Sigma = \Sigma_{1,1}$ is a genus one surface with one boundary component. Our formulas give partial information in higher genus as well, but as we don't yet have a complete answer, we won't discuss formulas for the h-adic expansion in the higher genus case in this paper.

We refer to $\Sigma_{1,1}$ as a one-holed torus. As is customary in the TQFT world, when dealing with surfaces with boundary, in practice one caps off the boundary circles by disks containing one colored banded point each in their interiors. (A banded point is a small oriented interval.) When doing this for $\Sigma_{1,1}$, we denote the resulting closed torus by $\mathcal{T}_c$, where $2c$ is the color of the banded point; here $2c$ can be any even integer satisfying $0 \le 2c \le p-3$. Mapping classes have to preserve the banded point, so that the Dehn twist t_δ about a simple closed curve δ encircling the colored banded point is non-trivial. Thus we are indeed dealing with $\Gamma_{1,1}$, the mapping class group of the one-holed torus. This group has presentation

$$(1) \qquad\qquad \Gamma_{1,1} = \langle t_\alpha, t_\beta \mid t_\alpha t_\beta t_\alpha = t_\beta t_\alpha t_\beta \rangle,$$

where t_α and t_β are Dehn twists about essential simple closed curves α and β which avoid the colored banded point and intersect exactly once. One has

---

[1]Here, we mean the h-adic expansion at a fixed p-th root of unity, not to be confused with an Ohtsuki-style expansion when p goes to infinity (hence $q = \zeta_p$ goes to 1), to be discussed in a paper in preparation by the second author.

$$(2) \qquad\qquad t_\delta = (t_\alpha t_\beta)^6.$$

We denote by t and t^* the endomorphisms of $\mathscr{S}_p^+(\mathscr{T}_c)$ given as ρ_p of certain lifts of t_α and t_β to the extended mapping class group [Gilmer and Masbaum 2009]. The notation t^* is motivated by the fact that t and t^* are adjoint with respect to a symmetric bilinear form $((\,,\,))$ called the Hopf pairing which will play a crucial role in this paper. To describe the TQFT representation ρ_p in our situation, it suffices to write down matrices for t and t^*.

In the TQFT defined over the cyclotomic *field* $\mathbb{Q}(\zeta_p)$, it is well-known how to do this, because the endomorphism t can be diagonalized over $\mathbb{Q}(\zeta_p)$ using a certain basis of "colors", and the entries of tt^*t in this basis can then be computed from an appropriate (generalized) S-matrix. However this basis in which t is diagonal is *not* an $\mathbb{O}_p^+$-basis for the lattice $\mathscr{S}_p^+(\mathscr{T}_c)$. For example, the coefficients of the matrix of t^* in this basis do not lie in $\mathbb{O}_p^+$. Hence we cannot compute the h-adic expansion of the representation ρ_p using this basis.

On the other hand, for an arbitrary surface Σ equipped with colored banded points, a $\mathbb{O}_p^+$-basis for the lattice $\mathscr{S}_p^+(\Sigma)$ was constructed explicitly in [GM2007]. In this *lollipop basis*, all mapping classes are represented by matrices with coefficients in $\mathbb{O}_p^+$. However, the explicit formulas we get from [GM2007] are still not good enough to compute the h-adic expansion in a nice way.

In the present paper, we will describe a modification of the construction of [GM2007]. The crucial additional property of the bases obtained here is that they are orthogonal with respect to a Hopf-like pairing $((\,,\,))$ which generalizes the one mentioned above in the genus-one case. As we'll see, this orthogonality property is very useful as one can easily express general vectors in terms of the orthogonal basis, using the pairing. We refer to this new basis as the *orthogonal lollipop basis*. We perform its construction in the general situation of a surface Σ equipped with colored banded points, as the higher genus case presents no extra difficulty, and give two immediate applications (see Remarks 3.5 and 3.6). Moreover, [Gilmer 2009] and [Gilmer and Masbaum 2011] make use of this basis in higher genus as well.

Let us end this introduction with a brief description of how the TQFT-representation ρ_p looks like in the orthogonal lollipop basis for the one-holed torus, and discuss an application we find interesting. The lattice $\mathscr{S}_p^+(\mathscr{T}_c)$ has rank $d-c$, where $d = (p-1)/2$. The basis we'll construct is denoted by

$$Q_n'^{(c)} \ (0 \le n \le d - c - 1).$$

One of its main features is that t is upper triangular and t^* is lower triangular in this basis, as will be shown in Section 4. This fact is also the main reason why the

new basis is better than the one described in [GM2007], where only one of t and t^* would be given by triangular matrix.

The matrix coefficients of t and t^* in this basis will be denoted by $a_{m,n}^{(c)}$ and $b_{m,n}^{(c)}$, respectively, and we will give explicit formulas for them in Section 4. These formulas can be used to compute the h-adic expansion of $a_{m,n}^{(c)}$ and $b_{m,n}^{(c)}$; in particular, they make it evident that $a_{m,n}^{(c)}$ and $b_{m,n}^{(c)}$ lie in $\mathbb{Z}[\zeta_p]$.

The fact that t is upper triangular and t^* is lower triangular is reminiscent of the action of $SL(2, \mathbb{Z})$ on homogeneous polynomials in two variables. Motivated by this observation, we will show in Section 5 that the representation $\rho_{p,0}$ on the $\mathbb{F}_p$-vector space $\mathcal{S}_{p,0}^+(\mathcal{T}_c)$ factors through $SL(2, \mathbb{F}_p)$ and is, in fact, isomorphic to the representation of $SL(2, \mathbb{F}_p)$ on the space of homogeneous polynomials over $\mathbb{F}_p$ in two variables of the appropriate degree $D = d - c - 1$.

In order to put this last result into perspective, we remark that when $c = 0$, it is known [Larsen and Wang 2005; Freedman and Krushkal 2006; Gilmer 2007] that the representation ρ_p itself factors through (a finite central extension of) $SL(2, \mathbb{F}_p)$, as the situation then reduces to the classical case of the closed torus. In contrast, when $c > 0$, there is no reason to believe that the representation should factor through $SL(2, \mathbb{F}_p)$. Indeed, we conjecture that the representation ρ_p does *not* factor through any finite group, although, of course, each $\rho_{p,N}$ does, as was explained above. It would follow that the quotient group of the extended mapping class group which acts effectively under the representation $\rho_{p,N}$ must get bigger and bigger as N increases, and one of our motivations for this paper was to develop techniques to compute the representations $\rho_{p,N}$ explicitly and efficiently.

The contrast between the cases $c = 0$ and $c > 0$ are, of course, expected to be related to geometry: a closed torus is Euclidean, whereas a torus with non-empty boundary is hyperbolic. The second author has shown that for $c = d - 2$, any pseudo-Anosov mapping class φ in $\Gamma_{1,1}$ is represented by a matrix of infinite order under ρ_p if p is big enough. (See [Andersen et al. 2006] for a proof of the analogous result for the mapping class group of a four-holed sphere.) In this situation, it follows that the order of $\rho_{p,N}(\varphi)$ must go to infinity as N increases, so the conjectural picture above is correct at least in this case.

2. The orthogonal lollipop basis for a one-holed torus

Let $p \geq 5$ be a prime, and ζ_p be a primitive p-th root of unity. We denote the cyclotomic ring $\mathbb{Z}[\zeta_p]$ by $\mathbb{O}_p^+$. We also let $\mathbb{O}_p$ denote $\mathbb{O}_p^+$ if $p \equiv 3 \pmod 4$ and $\mathbb{O}_p^+[i]$ if $p \equiv 1 \pmod 4$. Throughout the paper, we use the notation $h = 1 - \zeta_p$ and $d = (p-1)/2$. When referring to quantum integers or to skein-theoretical constructions, we will often write q for ζ_p, and we put $A = -q^{d+1}$; this is a primitive $2p$-th root of unity, and a square root of $q = \zeta_p$.

Here is some more notation that we will need. For $0 \leq n < p$, let

$$\{n\} = (-A)^n - (-A)^{-n},$$
$$\{n\}^+ = (-A)^n + (-A)^{-n}.$$

(Warning: the minus signs make this different notation than commonly used.) We also let $\{n\}_q = q^n - q^{-n}$. As usual, we put $\{n\}! = \{1\}\{2\} \cdots \{n\}$, and $\{0\}! = 1$. If n is negative, let $\{n\}! = 0$. Also let $\{n\}!! = \{n\}\{n-2\} \cdots$ ending in $\{1\}$ or $\{2\}$. Interpret $\{n\}^+!$, $\{n\}^+!!$, $\{n\}_q!$ similarly.

We refer the reader to Section 2 of [GM2007] for the definitions of the TQFT-module $V_p(\Sigma)$, defined over $\mathbb{O}_p[h^{-1}]$, and the integral TQFT-module $\mathscr{S}_p(\Sigma)$, defined over $\mathbb{O}_p$. In this paper, we are mainly interested in the refined integral TQFT-module $\mathscr{S}_p^+(\Sigma)$, with coefficients in $\mathbb{O}_p^+$; it is defined in Section 13 of the same reference. Here Σ is a compact oriented surface equipped with a (possibly empty) set of colored banded points. The set of allowed colors is $\{0, 1, \ldots, p-2\}$, but the sum of the colors of all the banded points must be even. The modules $V_p(\Sigma)$ and $\mathscr{S}_p(\Sigma)$ are obtained from $\mathscr{S}_p^+(\Sigma)$ by tensoring with $\mathbb{O}_p[h^{-1}]$ and $\mathbb{O}_p$, respectively; thus, all three modules are free of the same finite rank over their respective coefficient rings, and we have natural inclusions

$$\mathscr{S}_p^+(\Sigma) \subset \mathscr{S}_p(\Sigma) \subset V_p(\Sigma)$$

coming from the inclusions

$$\mathbb{O}_p^+ \subset \mathbb{O}_p \subset \mathbb{O}_p[h^{-1}].$$

The V_p-theory is a version of the Reshetikhin–Turaev SO(3)-TQFT, the only difference being that the latter is usually considered with coefficients in the quotient field of $\mathbb{O}_p$ (or even with coefficients in $\mathbb{C}$.)

Let $\mathscr{T}_c$ be a torus with one banded point colored $2c$. If $c = 0$, we can forget the banded point, and we simply write $\mathscr{T}$ for $\mathscr{T}_0$. Elements of $V_p(\mathscr{T}_c)$ are represented skein-theoretically as linear combinations of colored banded graphs in a solid torus, which meet the boundary nicely in the colored banded point. See [Blanchet et al. 1995] for the skein-theoretical construction of TQFT we are using here.

The *small graph basis* (see [GM2007, Proposition 3.2]) of $V_p(\mathscr{T}_c)$ is $L_{c,n}$ (for $0 \leq n \leq d - c - 1$), where

(3) $$L_{c,n} = \underset{2c}{\overset{n+c}{\bigodot}}$$

is a lollipop graph with stick color $2c$, and color $c+n$ on the loop edge. The *Hopf pairing* is the non-degenerate bilinear form $((\ ,\ ))$ on $V_p(\mathcal{T}_c)$ defined as follows:

$$((L_{c,n}, L_{c,m})) = \left\langle \begin{array}{c} c+n \\ c+m \end{array} \ 2c \right\rangle ,$$

where $\langle\ \rangle$ denotes the evaluation of a colored banded graph in S^3 [Masbaum and Vogel 1994; Kauffman and Lins 1994]. (There is a choice of the type of clasp. We insist that the clasp be as drawn. This is just a convention; our formulas would differ slightly if we chose the other convention.) The Hopf pairing restricts to a symmetric bilinear form

$$((\ ,\ )) : \mathcal{S}_p^+(\mathcal{T}_c) \times \mathcal{S}_p^+(\mathcal{T}_c) \to \mathbb{O}_p^+.$$

If $c = 0$, the Hopf pairing is the same as the pairing $\langle\ ,\ \rangle$ studied in [Blanchet et al. 1992]. (In this case, the choice of clasp does not matter.) As shown there, an orthogonal basis for $V_p(\mathcal{T})$ with respect to this pairing is $\{Q_0, Q_1, \ldots, Q_{d-1}\}$, where $Q_0 = 1$, and

$$Q_n = \prod_{i=0}^{n-1}(z - \lambda_i).$$

Here $\lambda_i = -q^{i+1} - q^{-i-1}$, and z denotes the core of the solid torus with color 1. (In our current notation, z is $L_{0,1}$ and its framing is as drawn, i.e., the blackboard framing.) The product uses the commutative algebra structure on $V_p(\mathcal{T})$ where z^n means n parallel copies of z.

We now generalize this to the case when $c \neq 0$. Observe that $V_p(\mathcal{T}_c)$ is a module over $V_p(\mathcal{T})$. Since $V_p(\mathcal{T})$ is commutative, we may view this both as a left and as a right module structure, whatever is notationally more convenient. For example, one has

$$L_{c,n}z = zL_{c,n} = \begin{array}{c} 1 \quad n+c \\ 2c \end{array}$$

where the right side can then be expressed as a linear combination of $L_{c,n+1}$ and $L_{c,n-1}$ in the usual way [Masbaum and Vogel 1994; Kauffman and Lins 1994].

Definition 2.1. For $0 \leq n \leq d - c - 1$, we set

$$Q_n^{(c)} = L_{c,0} \prod_{i=c}^{c+n-1}(z - \lambda_i) \quad \text{and} \quad Q_n'^{(c)} = (\{n\}!)^{-1} Q_n^{(c)}.$$

Here is the main result of this section.

Theorem 2.2. $\{Q_0'^{(c)}, Q_1'^{(c)}, \ldots, Q_{d-c-1}'^{(c)}\}$ *is an orthogonal basis for* $\mathcal{S}_p^+(\mathcal{T}_c)$ *with respect to the Hopf pairing. Moreover,*

$$(4) \quad ((Q_n'^{(c)}, Q_n'^{(c)})) = q^{-c(c+1)/2} \frac{\{2c+2n+1\}!!\{2c+n+1\}^+!}{\{n\}!} \frac{(\{c\}_q!)^2}{\{1\}_q\{2c\}_q!}.$$

We use the notation $x \sim y$ to mean that $x = uy$ for some unit u in $\mathbb{O}_p$. Here x, y can be numbers, or elements of some module such as $V_p(\mathcal{T}_c)$. For $0 < n < p$, one has both $\{n\} \sim h$ and $\{n\}_q \sim h$, and (hence) $\{n\}^+ = \{n\}_q/\{n\} \sim 1$. The following corollary is easily checked.

Corollary 2.3. $\qquad\qquad\qquad ((Q_n'^{(c)}, Q_n'^{(c)})) \sim h^c.$

Proof of Theorem 2.2. First, we show that the $Q_n'^{(c)}$ are a basis for $\mathcal{S}_p^+(\mathcal{T}_c)$. The basis of $\mathcal{S}_p^+(\mathcal{T}_c)$ constructed in [GM2007] is $\{L_{c,0}v^n \mid 0 \le n \le d-c-1\}$, where $v = h^{-1}(z+2) \in \mathcal{S}_p^+(\mathcal{T})$. Note that $z - \lambda_i = (z+2) - (2+\lambda_i)$ and $2+\lambda_i \sim h^2$. Thus $h^{-1}(z-\lambda_i) = v + $ (a scalar in $\mathbb{O}_p^+$). Thus there is a triangular basis change, with ones on the diagonal, between the basis $L_{c,0}v^n$ given in [GM2007] and the vectors $h^{-n}Q_n^{(c)}$, which therefore form a basis. Since $\{n\}! \sim h^n$, it follows that the $Q_n'^{(c)}$ are also a basis for $\mathcal{S}_p^+(\mathcal{T}_c)$.

Next, we show that this basis is orthogonal with respect to the Hopf pairing. It is enough to show that the $Q_n^{(c)}$ are orthogonal. The idea of proof is the same as showing orthogonality of the Q_n in [Blanchet et al. 1992]. Each $Q_n^{(c)}$ is a linear combination of $L_{c,m}$ where $0 \le m \le n$, and the coefficient of $L_{c,n}$ is one. We have $((Q_{n+k}^{(c)}, Q_n^{(c)})) = 0$ when $k > 0$, since $Q_{n+k}^{(c)}$ contains a $z - \lambda_{c+m}$ factor for $0 \le m \le n+k-1$, which we may use to annihilate the $L_{c,m}$ terms in $Q_n^{(c)}$. See Figure 1. Since the form is symmetric, this shows that the basis is orthogonal. We remark that since $((\, , \,))$ is non-degenerate, this argument also shows that $Q_n^{(c)} = 0$ for $n \ge d - c$, which will be used in the proof of Theorem 4.8. If $k = 0$, we can eliminate all but the $L_{c,n}$ term in the expansion of one copy of $Q_n^{(c)}$ when
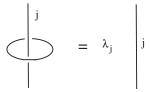

Figure 1. Encircling a strand colored j with a loop colored 1 has the same effect as multiplying by λ_j.

computing $((Q_n^{(c)}, Q_n^{(c)}))$. Thus

$$((Q_n^{(c)}, Q_n^{(c)})) = ((Q_n^{(c)}, L_{c,n})) = ((L_{c,0}, L_{c,n})) \prod_{i=c}^{c+n-1} (\lambda_{c+n} - \lambda_i).$$

But $((L_{c,0}, L_{c,n}))$ can be simplified using the first formula in the proof of [Masbaum 2003, Lemma (4.1)]. One gets

$$((L_{c,0}, L_{c,n})) = C_{c+n,c,c} \begin{vmatrix} 2c & c+n & c+n \\ n & c & c \end{vmatrix},$$

where $C_{c+n,c,c}$ is given in [Masbaum 2003, page 550], and the other symbol is a tetrahedral symbol in the notation of [Masbaum and Vogel 1994]. The formula for a tetrahedral symbol is a sum of products, but in this case there is only one term in this sum. Simplification gives

$$(5) \qquad ((Q_n^{(c)}, Q_n^{(c)})) = q^{-c(c+1)/2}\{n\}!\{2c+2n+1\}!!\{2c+n+1\}^{+}!\frac{(\{c\}_q!)^2}{\{1\}_q\{2c\}_q!}.$$

This easily implies (4) and completes the proof. $\qquad\qquad\square$

3. Orthogonal lollipop basis in higher genus

In this section, we define the Hopf pairing and construct an orthogonal basis for $\mathcal{S}_p^+(\Sigma)$ where Σ has arbitrary genus g. The reader interested only in the one-holed torus case may proceed directly to Section 4.

For the remainder of this section, we assume the reader is familiar with the concepts and notations of [GM2007, pages 820–822], where a basis of $\mathcal{S}_p(\Sigma)$ is defined in terms of certain colorings of a lollipop tree. The same construction actually yields a basis of $\mathcal{S}_p^+(\Sigma)$ [GM2007, page 837].

Suppose Σ is equipped with a set X of colored banded points. Fix a handlebody H with boundary Σ, and a banded lollipop tree G in H with boundary vertices equal to X, so that H retracts onto G. The *small graph basis* $\mathcal{G}$ of $V_p(\Sigma)$ consists of the elements $\mathfrak{g}(a, b, c)$ represented by *small colorings* of G [GM2007, Proposition 3.2]. See Figure 2, left, for an example representing the basis element

$$\mathfrak{g}\big((a_1, a_2, a_3), (b_1, b_2, b_3), (c_1, c_2, c_3, c_4)\big)$$

of $V_p(\Sigma)$, where Σ has genus 3 and $|X| = 2$, with colors c_3 and c_4 on the two banded points. The basis $\mathcal{B} = \{\mathfrak{b}(a, b, c)\}$ of $\mathcal{S}_p^+(\Sigma)$ given in [GM2007, page 822] is indexed by the same set of small colorings. It is obtained from $\mathcal{G}$ by a triangular (but not unimodular!) basis change. We will show how to modify the basis $\mathcal{B}$ to make it orthogonal with respect to the Hopf pairing which we discuss next.

In order to define the Hopf pairing in our context, assume that G and H have

been isotoped so that G is presented by a half-plane diagram with no crossings, with the banded points on the boundary of the half-plane, and one edge from each loop near the boundary of the half-plane. The graph in Figure 2, left, is already drawn in this way. One may produce a dual G' by rotating the half plane $180°$ around its boundary line and then bringing the loops together and inserting clasps (linking pairs of loops) as illustrated in Figure 2, right. Gluing G and G' along their boundary vertices produces a banded trivalent graph which we denote by GG'. Here, as in the genus-one case, we insist that all the clasps be as drawn.

As in the genus-one case, although the Hopf pairing can be defined in a basis-independent way, it is convenient to define it by its value on basis elements, as follows: $\big(\!\!\big(\mathfrak{g}(a,b,c), \mathfrak{g}(a',b',c')\big)\!\!\big)$ is the evaluation of GG' with colors (a,b,c) on the G part of GG', and colors (a',b',c') on the G' part, where we use the $180°$ rotation to transport (a',b',c') from G to G'. As before, this restricts to a symmetric bilinear form

$$(\!(\ ,\ )\!) : \mathscr{S}_p^+(\Sigma) \times \mathscr{S}_p^+(\Sigma) \to \mathbb{O}_p^+.$$

The basis $\mathcal{B}$ of $\mathscr{S}_p^+(\Sigma)$ found in [GM2007, page 822] is given as follows:

$$\mathfrak{b}(a,b,c) = h^{-\lfloor(-e+\sum_j a_j)/2\rfloor}\mathfrak{g}(a,0,c)\prod_{j=1}^{g}\frac{(2+z_j)^{b_j}}{h^{b_j}}.$$

Here $2e$ is the color of the trunk edge of G [GM2007, page 821], and z_j is a zero-framed circle colored 1 around the j-th hole. The following modification will be our orthogonal basis:

$$(6)\qquad \tilde{\mathfrak{b}}(a,b,c) = h^{-\lfloor(-e+\sum_j a_j)/2\rfloor}\mathfrak{g}(a,0,c)\prod_{j=1}^{g}\frac{\prod_{i=a_j}^{a_j+b_j-1}(z_j-\lambda_i)}{\{b_j\}!}.$$

Theorem 3.1. *The set $\widetilde{\mathcal{B}} = \{\tilde{\mathfrak{b}}(a,b,c)\}$, where (a,b,c) runs through the small colorings of G, is a basis of $\mathscr{S}_p^+(\Sigma)$ which is orthogonal with respect to the Hopf*

Figure 2. Left: lollipop graph G in good position, with some coloring. Right: GG' for the same colored graph, with colors omitted.
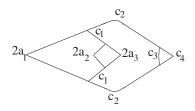
Figure 3. $DG(a, c)$ for the colored graph in Figure 2, left.

pairing. Moreover,

$$\left(\!\left(\tilde{\mathfrak{b}}(a, b, c), \tilde{\mathfrak{b}}(a, b, c)\right)\!\right) = h^{-2\lfloor(-e+\sum_i a_i)/2\rfloor} \langle DG(a, c)\rangle \prod_{i=1}^{g} \frac{(\!(Q_{b_i}^{\prime(a_i)}, Q_{b_i}^{\prime(a_i)})\!)\{1\}_q}{\{2a_i + 1\}_q},$$

where $2e$ is the color of the trunk edge, $\langle DG(a, c)\rangle$ is the evaluation of the colored banded graph $DG(a, c)$ defined below, and $(\!(Q_{b_i}^{\prime(a_i)}, Q_{b_i}^{\prime(a_i)})\!)$ is given in (4).

The proof is the same as in the one-holed torus case. To define $DG(a, c)$, assume that $G(a, b, c)$ is a colored lollipop graph in good position, as pictured in Figure 2, left, representing the small graph basis element $\mathfrak{g}(a, b, c)$. Then $DG(a, c)$ is the colored graph in the plane obtained by removing the loop edges and then adjoining a reflected copy, as in Figure 3.

Using formulas in [Masbaum and Vogel 1994], it is easy to see that $\langle DG(a, c)\rangle$ is always a unit in $\mathbb{O}_p^+$. Therefore one has the following

Corollary 3.2. $\left(\!\left(\tilde{\mathfrak{b}}(a, b, c), \tilde{\mathfrak{b}}(a, b, c)\right)\!\right) \sim \begin{cases} h^e & \text{if } \sum_j a_j \equiv e \pmod{2}, \\ h^{e+1} & \text{if } \sum_j a_j \not\equiv e \pmod{2}. \end{cases}$

Remark 3.3. The dual lattice $\mathscr{S}_p^{\sharp}(\Sigma)$ and its refined version $\mathscr{S}_p^{+\sharp}(\Sigma)$ are defined in Definition 8.1 and Section 13, respectively, of [GM2007], respectively, using certain hermitian forms. It is not hard to see that $\mathscr{S}_p^{+\sharp}(\Sigma)$ is also the lattice dual to $\mathscr{S}_p^+(\Sigma)$ with respect to the Hopf pairing:

$$\mathscr{S}_p^{+\sharp}(\Sigma) = \left\{ x \in \mathscr{S}_p^+(\Sigma) \otimes \mathbb{Q}(\zeta_p) \mid (\!(x, y)\!) \in \mathbb{O}_p^+ = \mathbb{Z}[\zeta_p] \text{ for all } y \in \mathscr{S}_p^+(\Sigma) \right\}.$$

Using orthogonality of the basis $\widetilde{\mathscr{B}}$, Corollary 3.2 easily implies that

Corollary 3.4. *The rescaling*

$$\tilde{\mathfrak{b}}^{\sharp}(a, b, c) = \begin{cases} h^{-e} \tilde{\mathfrak{b}}(a, b, c) & \text{if } \sum_j a_j \equiv e \pmod{2}, \\ h^{-e-1} \tilde{\mathfrak{b}}(a, b, c) & \text{if } \sum_j a_j \not\equiv e \pmod{2} \end{cases}$$

$$= h^{-\lceil(e+\sum_j a_j)/2\rceil} \mathfrak{g}(a, 0, c) \prod_{j=1}^{g} \frac{\prod_{i=a_j}^{a_j+b_j-1}(z_j - \lambda_i)}{\{b_j\}!}$$

is a basis $\widetilde{\mathcal{B}}^\sharp = \{\tilde{\mathfrak{b}}^\sharp(a, b, c)\}$ *of* $\mathcal{S}_p^{+\sharp}(\Sigma)$ *which is orthogonal with respect to the Hopf pairing.*

Remark 3.5. In the above, we deduced the bases $\widetilde{\mathcal{B}}$ of $\mathcal{S}_p^+(\Sigma)$ and $\widetilde{\mathcal{B}}^\sharp$ of $\mathcal{S}_p^{+\sharp}(\Sigma)$ from the basis $\mathcal{B}$ constructed in [GM2007]. Here is a sketch of a more direct proof. First, observe that both $\widetilde{\mathcal{B}}$ and $\widetilde{\mathcal{B}}^\sharp$ are bases of $V_p(\Sigma)$. Now use the 3-ball lemma and the lollipop lemma of [GM2007] to show that $\widetilde{\mathcal{B}} \subset \mathcal{S}_p^+(\Sigma)$ and $\widetilde{\mathcal{B}}^\sharp \subset \mathcal{S}_p^{+\sharp}(\Sigma)$. Then use orthogonality and Corollary 3.2 to show that

$$\left(\!\left(\tilde{\mathfrak{b}}(a, b, c), \tilde{\mathfrak{b}}^\sharp(a', b', c')\right)\!\right) \sim \delta_a^{a'} \delta_b^{b'} \delta_c^{c'},$$

and deduce that $\widetilde{\mathcal{B}}$ generates $\mathcal{S}_p^+(\Sigma)$ and $\widetilde{\mathcal{B}}^\sharp$ generates $\mathcal{S}_p^{+\sharp}(\Sigma)$. This proof avoids the index counting argument of [GM2007].

Remark 3.6. Let $\mathcal{J}_p^+(N)$ denote the Frohman–Kania-Bartoszyńska ideal [2001] (see also [GM2007, Gilmer 2006]) of a compact connected oriented 3-manifold N with connected boundary Σ. Using our orthogonal basis, we can give generators for this ideal as follows. The TQFT associates to N a vector $[N] \in \mathcal{S}_p^+(\Sigma)$ which is well defined up to multiplication by a root of unity. Write

$$[N] = \sum_{(a,b,c)} x_{(a,b,c)} \tilde{\mathfrak{b}}(a, b, c),$$

where the coefficients $x_{(a,b,c)}$ lie in $\mathbb{O}_p^+$, and the sum is over small admissible colorings of a lollipop graph in a handlebody with boundary Σ. Then by Theorem 3.1 and Corollary 3.2, together with [GM2007, Theorem 16.5], $\mathcal{J}_p^+(N)$ is the $\mathbb{O}_p^+$-ideal generated by the numbers $h^{\varepsilon(a)} x_{(a,b,c)}$ where $\varepsilon(a)$ is zero or one accordingly as $\sum_j a_j$ is even or odd.

4. Matrices for t and t^*

Recall that elements of $V_p(\mathcal{T}_c)$ are represented skein-theoretically as linear combinations of colored banded graphs in a solid torus which meet the boundary nicely in the colored banded point. We refer to such linear combinations as skein elements.

Definition 4.1. We let t be the endomorphism of $V_p(\mathcal{T}_c)$ induced by a full positive twist of the solid torus. It follows from [GM2007] that t preserves the lattice $\mathcal{S}_p^+(\mathcal{T}_c)$.

In the basis (3) of $V_p(\mathcal{T}_c)$, t is diagonal:

$$(7) \qquad\qquad\qquad t(L_{c,n}) = \mu_{c+n} L_{c,n},$$

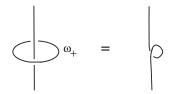where $\mu_k = (-1)^k A^{k(k+2)}$ is the twist eigenvalue [Blanchet et al. 1992].

Figure 4. Encircling a strand with ω_+ has the same effect in TQFT as giving that strand a positive twist.

Let $\omega_+ \in V_p(\mathcal{T})$ be defined as

$$(8) \qquad \omega_+ = \sum_{m=0}^{d-1} \gamma_m \frac{Q_m}{\{m\}!}, \quad \text{where } \gamma_m = \frac{(-A)^{(m^2+5m)/2}}{\prod_{k=1}^m (A^{2k+1} - 1)} \sim 1.$$

(To see that $\gamma_m \sim 1$ one uses that $1 - A$ is a unit in $\mathbb{O}_p^+$, see [Gilmer et al. 2004, Lemma 4.1(i)].) It follows from Theorem 2.2 (for $c = 0$) that $\omega_+ \in \mathcal{S}_p^+(\mathcal{T})$.

Theorem 4.2. *If $x \in V_p(\mathcal{T}_c)$ is represented by a skein element (which we also denote by x), then $t(x)$ is represented by the union of x with a zero-framed ω_+ placed on a meridian of the solid torus pushed slightly into the interior.* (See Figure 4.)

Proof. The existence of an ω_+ with this property is well-known in TQFT [Blanchet et al. 1995]. The expression (8) for it can be deduced from [Blanchet et al. 1992] as follows. Let ω_{BHMV1} be the skein element of [Blanchet et al. 1992].[2] By [Blanchet et al. 1992, 4.3(2)], encircling with $t(\omega_{\mathrm{BHMV1}})$ produces a *negative* twist, and

$$t(\omega_{\mathrm{BHMV1}}) = \sum_{m=0}^{d-1} \frac{(-1)^m A^{-2m}}{\prod_{j=2}^{2m+1}(A^j - 1)} \mu_m Q_m = \sum_{m=0}^{d-1} \frac{A^{m^2}}{\prod_{j=2}^{2m+1}(A^j - 1)} Q_m.$$

A skein expression for ω_+ can now be obtained from this formula for $t(\omega_{\mathrm{BHMV1}})$ by taking mirror images of the skein elements and conjugating the scalars (using $\overline{A} = A^{-1}$). (Note that this operation leaves Q_m invariant.) Formula (8) follows. $\square$

Definition 4.3. We let t^* be the endomorphism of $V_p(\mathcal{T}_c)$ given by

$$t^*(x) = x\omega_+.$$

It follows from [GM2007] that t^* preserves $\mathcal{S}_p^+(\mathcal{T}_c)$, since $\omega_+ \in \mathcal{S}_p^+(\mathcal{T})$.

Here the multiplication on the right-hand side is the module structure discussed in Section 2. Observe that $t^*(x)$ is represented by the union of x with a zero-framed ω_+ placed on the standard longitude of the solid torus pushed slightly into the interior. (See the last figure in Section 2.)

---

[2]Warning: the ω of [Blanchet et al. 1992] is not the same as that of [Blanchet et al. 1995].

Recall that the mapping class group $\Gamma_{1,1}$ is generated by the two Dehn twists about the meridian and the longitude of the torus. It follows from standard results in the skein-theoretical construction of the TQFT-representation ρ_p [Blanchet et al. 1995] that t and t^* are ρ_p of certain lifts of these twists to the extended mapping class group. Thus we have:

Theorem 4.4. *The endomorphisms t and t^* describe the TQFT representation ρ_p of the extended mapping class group on $\mathcal{S}_p^+(\mathcal{T}_c)$.*

Remark 4.5. The lifts chosen here are the "geometric" lifts as discussed in [Masbaum and Roberts 1995]. Choosing different lifts would multiply t and t^* by well-known scalar factors. Adapting the techniques of [Masbaum and Roberts 1995], one can show that $tt^*t = t^*tt^*$ and

$$(9) \qquad\qquad (tt^*t)^4 = q^{-6+2c(c+1)-p(p+1)/2}.$$

We will discuss our method to do computations like these in a more general context in [Gilmer and Masbaum 2009].

We now set out to compute matrix coefficients for t and t^*. The following proposition tells us that it will be good to use the basis constructed in Section 2 which is orthogonal for the Hopf pairing.

Proposition 4.6. *The endomorphisms t and t^* are adjoint for the Hopf pairing*:

$$((t(x), y)) = ((x, t^\star(y))).$$

Proof. We need to show that

$$((x \cup \omega_+(\text{along the meridian}), y)) = ((x, y \cup \omega_+(\text{along the longitude}))).$$

But this is clear, since in the standard decomposition of S^3 into two solid tori, the meridian of one solid torus is the longitude of the other. □

Let $a_{m,n}^{(c)}$ and $b_{n,m}^{(c)}$ denote the matrix coefficients for t and t^*, respectively:

$$t(Q_n'^{(c)}) = \sum_{m=0}^{d-1-c} a_{m,n}^{(c)} Q_m'^{(c)}, \quad t^\star(Q_m'^{(c)}) = \sum_{n=0}^{d-1-c} b_{n,m}^{(c)} Q_n'^{(c)}.$$

It follows from Proposition 4.6 that

$$a_{m,n}^{(c)}((Q_m'^{(c)}, Q_m'^{(c)})) = ((t(Q_n'^{(c)}), Q_m'^{(c)})) = ((Q_n'^{(c)}, t^\star(Q_m'^{(c)}))) = b_{n,m}^{(c)}((Q_n'^{(c)}, Q_n'^{(c)})).$$

Hence

$$(10) \qquad\qquad a_{m,n}^{(c)} = \frac{((Q_n'^{(c)}, Q_n'^{(c)}))}{((Q_m'^{(c)}, Q_m'^{(c)}))} b_{n,m}^{(c)} = R_{n,m}^{(c)} b_{n,m}^{(c)},$$

where

$$(11) \qquad R_{n,m}^{(c)} = \frac{\{m\}!\{2c+2n+1\}!!\{2c+n+1\}^+!}{\{n\}!\{2c+2m+1\}!!\{2c+m+1\}^+!} \sim 1.$$

That $R_{n,m}^{(c)} \sim 1$ follows easily from the remarks before Corollary 2.3. These same remarks and (8) justify the $\sim$'s appearing in (13) and Theorem 4.8 below.

Thus we are reduced to compute the $b_{n,m}^{(c)}$. To do so, we need the coefficients defined in the following proposition, which describes the module structure of $V_p(\mathcal{T}_c)$ over the algebra $V_p(\mathcal{T})$ in terms of the Q-bases.

Proposition 4.7. *We have*

$$(12) \qquad Q_m Q_n^{(c)} = \sum_{l=0}^{\min\{m,n+c\}} C_{m,n+c}^l Q_{m+n-l}^{(c)},$$

where

$$(13) \qquad C_{m,n}^l = (-1)^l \frac{\{m\}!\{n\}!\{m+n+1\}!}{\{m-l\}!\{n-l\}!\{m+n+1-l\}!\{l\}!} \sim h^{2l}.$$

We defer the proof to the end of this section. We are now ready to state the main result of this section.

Theorem 4.8. *The matrix for t^* is lower triangular, and the matrix for t is upper triangular:*

$$b_{n,m}^{(c)} = a_{m,n}^{(c)} = 0 \quad if \ m > n.$$

Moreover, if $m \leq n$, then

$$b_{n,m}^{(c)} = \sum_{l=0}^{m+c} b_{n,m,l}^{(c)}, \quad a_{m,n}^{(c)} = \sum_{l=0}^{m+c} a_{m,n,l}^{(c)},$$

where

$$b_{n,m,l}^{(c)} = C_{l+n-m,m+c}^l \frac{\gamma_{l+n-m}}{\{l+n-m\}!} \frac{\{n\}!}{\{m\}!} \sim h^l,$$

$$a_{m,n,l}^{(c)} = C_{l+n-m,m+c}^l \frac{\gamma_{l+n-m}}{\{l+n-m\}!} \frac{\{n\}!}{\{m\}!} R_{n,m}^{(c)} \sim h^l.$$

Proof. We compute

$$t^\star(Q_m'^{(c)}) = \omega_+ Q_m'^{(c)} = \sum_{k=0}^{d-1} \gamma_k \frac{Q_k}{\{k\}!} \frac{Q_m^{(c)}}{\{m\}!} = \sum_{k=0}^{d-1} \frac{\gamma_k}{\{k\}!\{m\}!} \sum_{l=0}^{\min\{k,m+c\}} C_{k,m+c}^l Q_{k+m-l}^{(c)}$$

$$= \sum_{l=0}^{m+c} \sum_{k=l}^{d-1} \frac{\gamma_k}{\{k\}!\{m\}!} C_{k,m+c}^l Q_{k+m-l}^{(c)} \text{ (changing the order of summation)}$$

$$= \sum_{l=0}^{m+c} \sum_{n=m}^{d-1+m-l} \frac{\gamma_{l+n-m}}{\{l+n-m\}!\{m\}!} C_{l+n-m,m+c}^l Q_n^{(c)} \text{ (letting } n=k+m-l)$$

$$= \sum_{l=0}^{m+c} \sum_{n=m}^{d-1-c} \frac{\gamma_{l+n-m}\{n\}!}{\{l+n-m\}!\{m\}!} C_{l+n-m,m+c}^l Q_n'^{(c)} \text{ (as } Q_n^{(c)}=0 \text{ for } n \geq d-c)$$

$$= \sum_{n=m}^{d-1-c} \sum_{l=0}^{m+c} b_{n,m,l}^{(c)} Q_n'^{(c)},$$

where $b_{n,m,l}^{(c)}$ is as in the statement of the theorem. This proves the result for the matrix coefficients $b_{n,m}^{(c)}$ of $t^\star$. To get the matrix coefficients for t, it now suffices to apply (10). $\square$

Proof of Proposition 4.7. Let us first consider the case $c=0$. It is easy to see that

$$(14) \qquad\qquad Q_m Q_n = \sum_{l=0}^{\min\{m,n\}} C_{m,n}^l Q_{m+n-l},$$

for some coefficients $C_{m,n}^l$ in the range $0 \leq l \leq \min\{m,n\}$. We must show that $C_{m,n}^l$ satisfies (13). Observe that if (13) holds for $n \leq m$, then it holds in general, by symmetry. So we may assume $n \leq m$. We now fix m, and prove the formula by induction on n, for all $0 \leq l \leq n$ at once. If $n = 0$, $C_{m,0}^0 = 1$, and formula (13) agrees. Assume inductively the formula is proven for n, and consider it for $n + 1$. Again, we may assume that $n + 1 \leq m$.

To perform the inductive step, let $\beta_{m,n} = \lambda_m - \lambda_n = \{n - m\}\{m + n + 2\}$. Since $Q_{n+1} = (z - \lambda_n) Q_n$, after multiplying (14) by $z - \lambda_n$ we get the following recursive relation:

$$C_{m,n+1}^l = \begin{cases} C_{m,n}^0 & \text{if } l = 0, \\ C_{m,n}^l + \beta_{m+n-l+1,n} C_{m,n}^{l-1} & \text{if } 1 \leq l \leq n, \\ \beta_{m,n} C_{m,n}^n & \text{if } l = n+1. \end{cases}$$

It is not hard to check that formula (13) satisfies these recursion relations. Thus, the $c = 0$ case of Proposition 4.7 is proved.

For the general case, let

$$Q_{n,c} = \prod_{i=c}^{c+n-1} (z - \lambda_i) = \frac{Q_{n+c}}{Q_c},$$

so that $Q_n^{(c)} = Q_{n,c} L_{c,0}$. We have

$$Q_m Q_{n,c} = \sum_{l=0}^{\min\{m,n+c\}} C_{m,n+c}^l Q_{m+n-l,c},$$

as follows from applying (14) with $n + c$ in place of n, and dividing by Q_c. Multiplying both sides of this equation by $L_{c,0}$, we get (12), completing the proof. □

We remark that Proposition 4.7 and its proof also work in the context of the Kauffman Bracket skein module of a solid torus (relative to a $2c$-colored banded point on its boundary if $c > 0$) over the Laurent polynomial ring $\mathbb{Z}[A^{\pm 1}]$ where A is generic (i.e., not necessarily a root of unity).

5. Irreducibility of the representation over $\mathbb{F}_p$

Recall that $\mathbb{Z}[\zeta_p]/(h)$ is the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The TQFT-representation ρ_p on $\mathscr{S}_p^+(\mathscr{T}_c)$ induces a representation $\rho_{p,0}$ on

$$\mathscr{S}_{p,0}^+(\mathscr{T}_c) = \mathscr{S}_p^+(\mathscr{T}_c)/h\mathscr{S}_p^+(\mathscr{T}_c),$$

which is an $\mathbb{F}_p$-vector space of dimension $d - c$. (Recall $d = (p-1)/2$.) This representation is generated by the two matrices t and t^* considered modulo h. Recall from Remark 4.5 that $tt^*t = t^*tt^*$ and $(tt^*t)^4 \equiv 1 \pmod{h}$. Thus $\rho_{p,0}$ factors through a representation of

$$(15) \qquad \mathrm{SL}(2, \mathbb{Z}) = \langle T, T^* \mid TT^*T = T^*TT^*, \ (TT^*T)^4 = 1 \rangle,$$

$$\text{where } T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \text{and} \quad T^* = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}.$$

Note that T and T^* are respectively the matrices for the action of a meridional and a longitudinal Dehn twist on the homology of the torus $\mathscr{T}$ with respect to the meridian-longitude basis.

We now come to the main result of this section.

Theorem 5.1. *For every $0 \le c \le d - 1$, the representation $\rho_{p,0}$ factors through* $\mathrm{SL}(2, \mathbb{F}_p)$. *Moreover, the induced representation of* $\mathrm{SL}(2, \mathbb{F}_p)$ *is isomorphic to the representation of* $\mathrm{SL}(2, \mathbb{F}_p)$ *on the vector space $H_{p,D}$ of homogeneous polynomials in two variables over $\mathbb{F}_p$ of total degree D, where $D + 1 = d - c$.*

Here we consider the left action of $\mathrm{SL}_2(\mathbb{F}_p)$ on polynomials in variables x and y over $\mathbb{F}_p$ given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} x^m y^n = (ax + cy)^m (bx + dy)^n.$$

This restricts to a representation $r_{p,D}$ of $\mathrm{SL}_2(\mathbb{F}_p)$ on the vector space $H_{p,D}$ of homogeneous polynomials of a given degree D. The dimension of this representation is $D + 1$. It is irreducible if and only if $0 \leq D \leq p - 1$ [Humphreys 1975, pages 31–32]. These are the only irreducible representations of $\mathrm{SL}_2(\mathbb{F}_p)$ over $\mathbb{F}_p$.

Corollary 5.2. *The representation $\rho_{p,0}$ on the $\mathbb{F}_p$-vector space $\mathscr{S}_{p,0}^+(\mathcal{T}_c)$ is irreducible for all $0 \leq c \leq d - 1$.*

Remark 5.3. The matrices t and t^* have order p, as follows from (7). But this is not enough to ensure that $\rho_{p,0}$ factors through $\mathrm{SL}(2, \mathbb{F}_p)$, because adding the relation $T^p = (T^*)^p = 1$ to the presentation (15) defines still an infinite group if $p \geq 7$ (it is a double cover of the $(2, 3, p)$ triangle group).

Remark 5.4. The reader may wonder whether $\mathscr{S}_{p,0}^+(\Sigma)$ is an irreducible representation of the mapping class group for general surfaces Σ. In fact, if the genus of Σ is at least 3, $\mathscr{S}_{p,0}^+(\Sigma)$ is not irreducible, as already observed in [GM2007, Section 14]. The situation can be understood completely using the orthogonal lollipop basis: one finds that $\mathscr{S}_{p,0}^+(\Sigma)$ has a composition series with at most two irreducible pieces (at least when Σ has at most one colored point). Details will be given in [Gilmer and Masbaum 2011].

We remark that over the complex numbers, the representation $\mathscr{S}_p^+(\Sigma) \otimes \mathbb{C}$ is always irreducible when p is prime and when Σ has at most one colored point [Gilmer and Masbaum 2011]. If Σ has no colored points, this result can be obtained by adapting Robert's proof of the analogous result for the $\mathrm{SU}(2)$-TQFT (where A is a primitive $4p$-th root of unity) [2001]. Irreducibility over the complex numbers implies irreducibility over the cyclotomic field $\mathbb{Q}(\zeta_p)$, but does not, of course, imply irreducibility over the finite field $\mathbb{F}_p$. Also, Roberts' argument does not apply over $\mathbb{F}_p$, because it uses the fact that the twist eigenvalues

$$\mu_k = (-A)^{k(k+2)} = \zeta_p^{(d+1)k(k+2)}, \quad \text{for } 0 \leq k \leq d - 1,$$

are all distinct. But these eigenvalues become equal to 1 in $\mathbb{F}_p$ (since $\zeta_p = 1$ in $\mathbb{F}_p$).

Proof of Theorem 5.1. Consider the basis $(x^{D-n}y^n)_{n=0,1,\dots,D}$ of $H_{p,D}$. In this basis, T is upper triangular, T^* is lower triangular, and the matrix coefficients of T and T^* are given by

$$T(x^{D-n}y^n) = \sum_{m=0}^{n} \alpha_{m,n}^{(D)} x^{D-m} y^m, \quad \text{where } \alpha_{m,n}^{(D)} = \binom{n}{m},$$

$$T^{\star}(x^{D-n}y^n) = \sum_{m=n}^{D} \beta_{m,n}^{(D)} x^{D-m} y^m, \quad \text{where } \beta_{m,n}^{(D)} = (-1)^{m-n} \binom{D-n}{m-n}.$$

The matrix coefficients of t and t^* acting on $\mathscr{S}^+_{p,0}(\mathscr{T}_c)$ are given by $a^{(c)}_{m,n}$ and $b^{(c)}_{m,n}$ (mod h), which we denote by $\hat{a}^{(c)}_{m,n}$ and $\hat{b}^{(c)}_{m,n}$. Recall that they lie in the finite field $\mathbb{F}_p$.

Lemma 5.5. $\quad \hat{a}^{(c)}_{m,n} = \dfrac{(-1)^{n-m}(2c+2n+1)!!}{(n-m)!(2c+2m+1)!!} \quad$ and $\quad \hat{b}^{(c)}_{m,n} = (-2)^{n-m}\dbinom{m}{n}.$

Proof. This follows from Theorem 4.8, using that $q \equiv 1 \pmod{h}$, $A \equiv -1 \pmod{h}$, $\gamma_m \equiv (-1)^m 2^{-m} \pmod{h}$, $\{n\}^+ \equiv 2 \pmod{h}$, and $\{n\}/\{1\} \equiv n \pmod{h}$. $\qquad\square$

Now assume $D = d - c - 1$ and define a vector space isomorphism:

$$\Phi : H_{p,D} \to \mathscr{S}^+_{p,0}(\mathscr{T}_c) \quad \text{by } \Phi(x^{D-n}y^n) = (-1)^n \frac{n!}{(2c+2n+1)!!} Q'^{(c)}_n.$$

We claim that Φ intertwines the representations $r_{p,D}$ on $H_{p,D}$ and $\rho_{p,0}$ on $\mathscr{S}^+_{p,0}(\mathscr{T}_c)$. To see this, it suffices to check that (in $\mathbb{F}_p$) one has

$$(-1)^m \frac{m!}{(2c+2m+1)!!} \alpha^{(d-c-1)}_{m,n} = (-1)^n \frac{n!}{(2c+2n+1)!!} \hat{a}^{(c)}_{m,n},$$

$$(-1)^m \frac{m!}{(2c+2m+1)!!} \beta^{(d-c-1)}_{m,n} = (-1)^n \frac{n!}{(2c+2n+1)!!} \hat{b}^{(c)}_{m,n}.$$

The first is immediate. The second reduces to

$$(-2)^{-n}(d-c-1-n)!(2c+2n+1)!! = (-2)^{-m}(d-c-1-m)!(2c+2m+1)!!,$$

which is true due to the following lemma.

Lemma 5.6. *For* $0 \le k \le d-1$,

$$(-2)^{-k}(d-k-1)!(2k+1)!! = (d-1)! \pmod{p}.$$

Proof. We prove by induction on k. Let u_k be the expression on the left side. We have $u_0 = (d-1)!$, and also $u_{k+1} = (2k+3)u_k/(-2)(d-k-1) = u_k \in \mathbb{F}_p$, as $(-2)(d-k-1) = 2k+3 \in \mathbb{F}_p$. $\qquad\square$

This completes the proof of Theorem 5.1. $\qquad\square$

Remark 5.7. With van Wamelen [Gilmer et al. 2004, page 264], we gave a formula for the action of t on v^n in the Kauffman bracket skein module of $S^1 \times D^2$. This formula gives an expression for the matrix coefficients $\hat{a}^{(0)}_{m,n}$ which looks quite different (and more complicated) than the $c = 0$ case of the expression in Lemma 5.5. Comparing the two expressions leads to a proof of the following identity:

For integers n, m, and i with $n \ge m \ge 1$, and $i \ge 0$,

$$\sum_{k=m}^{n}(-1)^{k+n}\frac{k}{n}\binom{k^2-1}{n-m-i}\binom{2n}{n-k}\binom{k+m-1}{k-m} = \begin{cases} \dfrac{(2n-1)!}{(n-m)!(2m-1)!} & \text{if } i = 0, \\ 0 & \text{if } i > 0. \end{cases}$$

Conversely, if one has an independent proof of this identity for $i = 0$, then one can deduce the formula for $\hat{a}_{m,n}^{(0)}$ in Lemma 5.5 from the formula for $t(v^n)$ in [Gilmer et al. 2004].

We thank C. Krattenthaler (private communication, 2009) for providing an independent proof of this identity. Although the sum is not hypergeometric (due to the k^2 in the binomial coefficient), Krattenthaler was able to reduce the proof to applications of Dixon's identity [Slater 1966, (2.3.3.6) and Appendix (III.9)].

References

[Andersen et al. 2006] J. E. Andersen, G. Masbaum, and K. Ueno, "Topological quantum field theory and the Nielsen–Thurston classification of $M(0,4)$", *Math. Proc. Cambridge Philos. Soc.* **141**:3 (2006), 477–488. MR 2007k:57059 Zbl 1110.57009

[Blanchet et al. 1992] C. Blanchet, N. Habegger, G. Masbaum, and P. Vogel, "Three-manifold invariants derived from the Kauffman bracket", *Topology* **31**:4 (1992), 685–699. MR 94a:57010 Zbl 0771.57004

[Blanchet et al. 1995] C. Blanchet, N. Habegger, G. Masbaum, and P. Vogel, "Topological quantum field theories derived from the Kauffman bracket", *Topology* **34**:4 (1995), 883–927. MR 96i:57015 Zbl 0887.57009

[Freedman and Krushkal 2006] M. Freedman and V. Krushkal, "On the asymptotics of quantum SU(2) representations of mapping class groups", *Forum Math.* **18**:2 (2006), 293–304. MR 2007b:57056 Zbl 1120.57014

[Frohman and Kania-Bartoszyńska 2001] C. Frohman and J. Kania-Bartoszyńska, "A quantum obstruction to embedding", *Math. Proc. Cambridge Philos. Soc.* **131**:2 (2001), 279–293. MR 2002f:57023 Zbl 0991.57023

[Funar 1999] L. Funar, "On the TQFT representations of the mapping class groups", *Pacific J. Math.* **188**:2 (1999), 251–274. MR 2000d:57026 Zbl 0948.57024

[Gilmer 2004] P. M. Gilmer, "Integrality for TQFTs", *Duke Math. J.* **125**:2 (2004), 389–413. MR 2005m:57042 Zbl 1107.57020

[Gilmer 2006] P. M. Gilmer, "On the Frohman Kania-Bartoszynska ideal", *Math. Proc. Cambridge Philos. Soc.* **141**:2 (2006), 265–271. MR 2007i:57008 Zbl 1181.57013

[Gilmer 2007] P. M. Gilmer, "Congruence and quantum invariants of 3-manifolds", *Algebr. Geom. Topol.* **7** (2007), 1767–1790. MR 2008k:57039 Zbl 1161.57003

[Gilmer 2009] P. M. Gilmer, "Heegaard genus, cut number, weak p-congruence, and quantum invariants", *J. Knot Theory Ramifications* **18**:10 (2009), 1359–1368. MR 2011d:57031 Zbl 1181.57014

[Gilmer and Masbaum 2007] P. M. Gilmer and G. Masbaum, "Integral lattices in TQFT", *Ann. Sci. École Norm. Sup.* (4) **40**:5 (2007), 815–844. MR 2009m:57049 Zbl 1178.57023

[Gilmer and Masbaum 2009] P. M. Gilmer and G. Masbaum, "Maslov index, lagrangians, mapping class groups and TQFT", preprint, 2009. To appear in *Forum Math.* arXiv 0912.4706

[Gilmer and Masbaum 2011] P. M. Gilmer and G. Masbaum, "Irreducible factors of modular representations of mapping class groups arising in integral TQFT", preprint, 2011.

[Gilmer et al. 2004] 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**:2 (2004), 260–284. MR 2005i:57042 Zbl 1055.57026

[Humphreys 1975] J. E. Humphreys, "Representations of SL(2, p)", *Amer. Math. Monthly* **82** (1975), 21–39. MR 51 #732 Zbl 0296.20020

[Kauffman and Lins 1994] L. H. Kauffman and S. L. Lins, *Temperley–Lieb recoupling theory and invariants of 3-manifolds*, Annals of Mathematics Studies **134**, Princeton University Press, 1994. MR 95c:57027 Zbl 0821.57003

[Krattenthaler ≥ 2011] C. Krattenthaler, private communication.

[Larsen and Wang 2005] M. Larsen and Z. Wang, "Density of the SO(3) TQFT representation of mapping class groups", *Comm. Math. Phys.* **260**:3 (2005), 641–658. MR 2007b:57058 Zbl 1114.57012

[Masbaum 1999] G. Masbaum, "An element of infinite order in TQFT-representations of mapping class groups", pp. 137–139 in *Low-dimensional topology* (Funchal, 1998), edited by H. Nencka, Contemp. Math. **233**, Amer. Math. Soc., Providence, RI, 1999. MR 2000h:57053 Zbl 0929.57006

[Masbaum 2003] G. Masbaum, "Skein-theoretical derivation of some formulas of Habiro", *Algebr. Geom. Topol.* **3** (2003), 537–556. MR 2004f:57013 Zbl 1042.57005

[Masbaum and Roberts 1995] G. Masbaum and J. D. Roberts, "On central extensions of mapping class groups", *Math. Ann.* **302**:1 (1995), 131–150. MR 96i:57013 Zbl 0823.57010

[Masbaum and Vogel 1994] G. Masbaum and P. Vogel, "3-valent graphs and the Kauffman bracket", *Pacific J. Math.* **164**:2 (1994), 361–381. MR 95e:57003 Zbl 0838.57007

[Roberts 2001] J. Roberts, "Irreducibility of some quantum representations of mapping class groups", *J. Knot Theory Ramifications* **10**:5 (2001), 763–767. MR 2002f:57065 Zbl 1001.57036

[Slater 1966] L. J. Slater, *Generalized hypergeometric functions*, Cambridge University Press, 1966. MR 34 #1570 Zbl 0135.28101

PATRICK M. GILMER
DEPARTMENT OF MATHEMATICS
LOUISIANA STATE UNIVERSITY
BATON ROUGE, LOUISIANA 70803
UNITED STATES

gilmer@math.lsu.edu
http://www.math.lsu.edu/~gilmer/

GREGOR MASBAUM
EQUIPE TOPOLOGIE ET GÉOMÉTRIE ALGÉBRIQUES
INSTITUT DE MATHÉMATIQUES DE JUSSIEU (UMR 7586 DU CNRS)
CASE 247
4 PL. JUSSIEU
75252 CEDEX 5 PARIS
FRANCE

masbaum@math.jussieu.fr
http://www.math.jussieu.fr/~masbaum/

PACIFIC JOURNAL OF MATHEMATICS

http://www.pjmath.org