AN APPLICATION OF TQFT TO MODULAR REPRESENTATION THEORY

PATRICK M. GILMER AND GREGOR MASBAUM

Abstract. For $p \geq 5$ a prime, and $g \geq 3$ an integer, we use Topological Quantum Field Theory (TQFT) to study a family of $p-1$ highest weight modules $L_p(\lambda)$ for the symplectic group $\mathrm{Sp}(2g, K)$ where K is an algebraically closed field of characteristic p. This permits explicit formulae for the dimension and the formal character of $L_p(\lambda)$ for these highest weights.

Contents

1. Introduction

Let p be an odd prime, and K be an algebraically closed field of characteristic p. For $g \geq 1$ an integer, we consider the symplectic group $\mathrm{Sp}(2g, K)$, thought of as an algebraic group of rank g. It is well-known that the classification (due to Chevalley) of rational simple $\mathrm{Sp}(2g, K)$-modules is the same as in characteristic zero (see Jantzen [J, II.2]). More precisely, for every dominant weight λ there is a simple module $L_p(\lambda)$, and these exhaust all isomorphism classes of simple modules. Here the set of dominant weights is the same as in characteristic zero: λ is dominant iff it is a linear combination of the fundamental weights ω_i $(i = 1, \ldots, g)$ with nonnegative integer coefficients.

On the other hand, while the dimensions of simple $\mathrm{Sp}(2g, \mathbb{C})$-modules can be computed from the Weyl character formula, it seems that explicit dimension formulae for the modules $L_p(\lambda)$ for $p > 0$ are quite rare, except in rather special situations. We refer to [H2] for a survey. For fundamental weights, Premet and Suprunenko [PS] gave an algorithm to compute the dimensions of $L_p(\omega_i)$ by reducing the problem to known properties of symmetric group representations. Later,

Date: April 24, 2017.
2010 *Mathematics Subject Classification.* 20C20, 20C33, 57R56.
The first author was partially supported by NSF-DMS-1311911.

Gow [Go] gave an explicit construction of $L_p(\omega_i)$ for the last $p-1$ fundamental weights (that is: ω_i where $i \geq g-p+1$) which allowed him to obtain a recursive formula for their dimensions. Even later, Foulle [F] obtained a dimension formula for all fundamental weights. As for other weights, it is known that for weights λ in the fundamental alcove the dimension of $L_p(\lambda)$ is the same as the dimension of $L_0(\lambda)$ (the corresponding simple module in characteristic zero), and can thus be computed by the Weyl character formula. But for weights outside the fundamental alcove, no general dimension formula is known. A conjectural formula by Lusztig for primes in a certain range was shown to hold for $p >> 0$ by Andersen-Jantzen-Soergel [AJS] but was recently shown not to hold for all p in the hoped-for range by Williamson [W].

In this paper, we show that Topological Quantum Field Theory (TQFT) can give new information about the dimensions of some of these simple modules. Specifically, we show that for every prime $p \geq 5$ and in every rank $g \geq 3$, there is a family of $p-1$ dominant weights λ, lying outside of the fundamental alcove except for one weight in rank $g=3$, for which we can express the dimension of $L_p(\lambda)$ by formulae similar to the Verlinde formula in TQFT. We found this family as a byproduct of Integral SO(3)-TQFT [G1, GM1], an integral refinement of the Witten-Reshetikhin-Turaev TQFT associated to SO(3). More precisely, we use Integral SO(3)-TQFT in what we call the 'equal characteristic case' which we studied in [GM5]. The family of weights λ we found together with our formulae for $\dim L_p(\lambda)$ is given in the following Theorem 1.1. We can also compute the weight space decomposition of $L_p(\lambda)$ for these weights λ; this will be given in Theorem 1.9. We follow the notation of [B, Planche III], where the fundamental weights ω_i are expressed in the usual basis $\{\varepsilon_i\}$ $(i = 1, \ldots, g)$ of weights of the maximal torus as $\omega_i = \varepsilon_1 + \ldots + \varepsilon_i$.

Theorem 1.1. *Let $p \geq 5$ be prime and put $d = (p-1)/2$. For rank $g \geq 3$, consider the following $p-1$ dominant weights for the symplectic group* $\mathrm{Sp}(2g, K)$ *:*

$$\lambda = \begin{cases} (d-1)\omega_g & & (\textit{Case } \mathrm{I}) \\ (d-c-1)\omega_g + c\,\omega_{g-1} & \textit{for } 1 \leq c \leq d-1 & (\textit{Case } \mathrm{II}) \\ (d-c-1)\omega_g + (c-1)\omega_{g-1} + \omega_{g-2} & \textit{for } 1 \leq c \leq d-1 & (\textit{Case } \mathrm{III}) \\ (d-2)\omega_g + \omega_{g-3} & & (\textit{Case } \mathrm{IV}) \end{cases}$$

Put $\varepsilon = 0$ in Case I *and* II *and $\varepsilon = 1$ in Case* III *and* IV*. Then*

$$\dim L_p(\lambda) = \frac{1}{2}\left(D_g^{(2c)}(p) + (-1)^{\varepsilon}\delta_g^{(2c)}(p)\right) \quad \textit{where} \tag{1}$$

$$D_g^{(2c)}(p) = \left(\frac{p}{4}\right)^{g-1} \sum_{j=1}^{d} \left(\sin\frac{\pi j(2c+1)}{p}\right)\left(\sin\frac{\pi j}{p}\right)^{1-2g} \tag{2}$$

$$\delta_g^{(2c)}(p) = (-1)^c \frac{4^{1-g}}{p} \sum_{j=1}^{d} \left(\sin\frac{\pi j(2c+1)}{p}\right)\left(\sin\frac{\pi j}{p}\right)\left(\cos\frac{\pi j}{p}\right)^{-2g}, \tag{3}$$

and c is the same c used in the definition of λ, except in Case I *and* IV*, where we put $c = 0$. In Case* IV *in rank $g = 3$, $\omega_{g-3} = \omega_0$ should be interpreted as zero.*

Remark 1.2. Formula (2) is an instance of the famous Verlinde formula in TQFT. Formula (3) appeared first in [GM5]. Note that the difference between the two formulae is that certain sines in (2) have become cosines in (3), and the overall prefactor is different. For fixed g, both $D_g^{(2c)}(p)$ and $\delta_g^{(2c)}(p)$ can be expressed as polynomials in p and c. See [GM5] for more information and further references. In Appendix B, we give explicit polynomial expressions for the dimensions of our $L_p(\lambda)$ in rank $g \leq 4$.

Remark 1.3. Except for the weight $\lambda = (d-2)\omega_3$ in Case IV in rank $g = 3$, all the weights in the above list lie outside of the fundamental alcove. See Section 5 for more concerning this.

Remark 1.4. When $p = 5$, the list above produces (in order) the fundamental weights $\omega_g, \omega_{g-1}, \omega_{g-2}, \omega_{g-3}$. These are exactly the weights considered by Gow [Go]. For $p > 5$, our weights are different from those of Gow. It is intriguing that both Gow's and our family of weights have $p-1$ elements.

Question 1.5. Can one find similar Verlinde-like dimension formulae for other families of dominant weights?

Remark 1.6. In [GM4], we answered this question affirmatively for the $p-1$ fundamental weights considered by Gow. But [GM4] was based on Gow's recursion formula, not on TQFT as in the present paper. On the other hand, SO(3)-TQFT is just one of the simplest TQFTs within the family of Witten-Reshetikhin-Turaev TQFTs, and it is conceivable that other Integral TQFTs (*e.g.* [ChLe]) might produce more families of weights λ where the methods of the present paper could be applied. A difficulty here is that Integral TQFT as we need it in this paper is so far not developed for other TQFTs.

Remarks 1.7. (i) The restriction that $g \geq 3$ in the theorem is only to ensure that we get $p-1$ distinct weights. The theorem also holds in rank $g = 1$ or 2 for those weights λ where it makes sense (*i.e.*, if no ω_i with $i < 0$ appears in the formula for λ) provided ω_0 is interpreted as zero.

(ii) Case I could be amalgamated with Case II in Theorem 1.1 by allowing c to be zero in Case II. We chose not to do this because Case I will require special treatment later.

Throughout the paper, we assume $p \geq 5$ and we use the notation $d = (p-1)/2$.

The construction of the modules $L_p(\lambda)$ goes as follows. For $0 \leq c \leq d-1$ and $\varepsilon \in \mathbb{Z}/2$, we construct certain simple modules which we denote by $\widetilde{F}_p(g, c, \varepsilon)$. Note that there are $p-1$ choices of pairs (c, ε). The construction of the modules $\widetilde{F}_p(g, c, \varepsilon)$ is based on results from Integral TQFT obtained in [GM5]. From the TQFT description, we shall compute the dimension and weight space decomposition of $\widetilde{F}_p(g, c, \varepsilon)$. In particular, we shall compute the highest weight occuring in $\widetilde{F}_p(g, c, \varepsilon)$, thereby identifying $\widetilde{F}_p(g, c, \varepsilon)$ with one of the $L_p(\lambda)$ in Theorem 1.1.

Here is the construction of $\widetilde{F}_p(g, c, \varepsilon)$. We give a description which can be read without any knowledge of TQFT. Consider the graph G_g depicted in Figure 1 which we call a lollipop tree. It has $2g-1$ trivalent vertices and one univalent vertex which in the figure is labelled $2c$. The 2-valent 'corner' vertex to the left of the figure should be ignored, and the two edges meeting there are to be considered a single edge. Thus, G_g has $3g-1$ edges, g of which are loop edges. The edges incident to a loop edge are called stick edges, and we refer to a loop edge together with its stick edge as a lollipop.

A p-color is an integer $\in \{0, 1, \ldots, p-2\}$. A p-coloring of G_g is an assignment of p-colors to the edges of G_g. A p-coloring is *admissible* if whenever i, j and k are

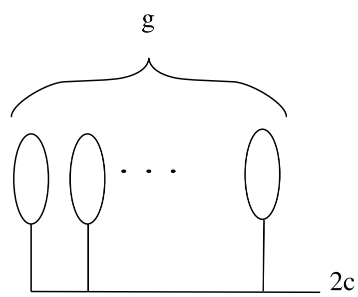

FIGURE 1. Lollipop tree G_g

the colors of edges which meet at a vertex, then

$$\begin{aligned} i+j+k &\equiv 0 \pmod 2 , \\ |i-j| \leq & \; k \leq i+j , \quad \text{and} \\ i+j+k &\leq 2p-4 . \end{aligned}$$

Admissibility at the trivalent vertex of the i-th lollipop implies that the stick edge has to receive an even color, which we denote by $2a_i$, and the loop edge has to receive a color of the form $a_i + b_i$, with $b_i \geq 0$. We denote the colors of the remaining edges by $c_1, c_2, \ldots$ as in Figure 2, and we write an admissible p-coloring as $\sigma = (a_1, \ldots, a_g, b_1, \ldots, b_g, c_1, \ldots)$.

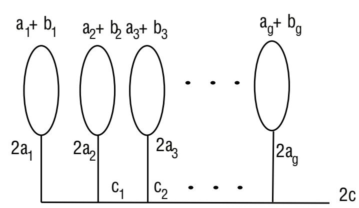

FIGURE 2. Colored Lollipop tree G_g

A p-coloring is of type (c, ε) if the color $2c$ is assigned to the edge incident with the univalent vertex and if

$$c + \sum a_i \equiv \varepsilon \pmod 2 . \tag{4}$$

A p-coloring is *small* if the colors $a_i + b_i$ of the loop edges satisfy

$$0 \leq a_i + b_i \leq d - 1 . \tag{5}$$

Let $C_p(g, c, \varepsilon)$ denote the set of small admissible p-colorings of G_g of type (c, ε). Let $\mathbb{F}_p$ denote the finite field with p elements, and let $F_p(g, c, \varepsilon)$ be the $\mathbb{F}_p$-vector space with basis $C_p(g, c, \varepsilon)$.

Theorem 1.8. *There is an irreducible representation of the finite symplectic group* $\mathrm{Sp}(2g, \mathbb{F}_p)$ *on* $F_p(g, c, \varepsilon)$.

This will be proved in Section 3.

Steinberg's restriction theorem (see *e.g.* [H2, 2.11]) implies that there is a unique simple $\mathrm{Sp}(2g, K)$-module $\widetilde{F}_p(g, c, \varepsilon)$ characterized by the following two properties:

(i) The restriction of $\widetilde{F}_p(g,c,\varepsilon)$ to the finite group $\mathrm{Sp}(2g,\mathbb{F}_p)$ is $F_p(g,c,\varepsilon)\otimes K$.

(ii) $\widetilde{F}_p(g,c,\varepsilon)$ has p-restricted highest weight.

We recall that a dominant weight $\lambda=\sum_{i=1}^g \lambda_i\omega_i$ is *p-restricted* if, for each $1\le i\le g$, we have $0\le\lambda_i\le p-1$.

Part (i) of the following theorem says that the $\widetilde{F}_p(g,c,\varepsilon)$ are precisely the simple modules $L_p(\lambda)$ listed in Theorem 1.1. Part (ii) gives the weight space decomposition and thus determines the formal character of these modules. To state the result, let $\widetilde{W}_p(g,c,\varepsilon)$ be the multiset of weights occuring in $\widetilde{F}_p(g,c,\varepsilon)$. (By a multiset, we mean a set with multiplicities.)

Theorem 1.9. *(i) The* $\mathrm{Sp}(2g,K)$*-module* $\widetilde{F}_p(g,c,\varepsilon)$ *is isomorphic to* $L_p(\lambda)$ *where the highest weight* $\lambda=\lambda_p(g,c,\varepsilon)$ *is given by*

$$\begin{aligned}
&\lambda_p(g,0,0)=(d-1)\omega_g && && (Case\ \mathrm{I})\\
&\lambda_p(g,c,0)=(d-c-1)\omega_g+c\,\omega_{g-1}, && 1\le c\le d-1 && (Case\ \mathrm{II})\\
&\lambda_p(g,c,1)=(d-c-1)\omega_g+(c-1)\omega_{g-1}+\omega_{g-2}, && 1\le c\le d-1 && (Case\ \mathrm{III})\\
&\lambda_p(g,0,1)=(d-2)\omega_g+\omega_{g-3} && && (Case\ \mathrm{IV})
\end{aligned}$$

(ii) We have

$$\widetilde{W}_p(g,c,\varepsilon)=\{w(\sigma)\,|\,\sigma\in C_p(g,c,\varepsilon)\}\ ,$$

where the weight of a coloring $\sigma=(a_1,\dots,a_g,b_1,\dots,b_g,c_1,\dots)$ *is*

$$w(\sigma)=\sum_{i=1}^{g}(d-1-a_i-2b_i)\varepsilon_i\ . \tag{6}$$

Example 1.10. In Case I, the highest weight corresponds to the p-coloring σ_0 where all edges are colored zero. Indeed, formula (6) gives

$$w(\sigma_0)=\sum_{i=1}^{g}(d-1)\varepsilon_i=(d-1)\omega_g\ .$$

In the other cases, the coloring σ_0 is not allowed as it is not of type (c,ε) for $(c,\varepsilon)\neq(0,0)$. We shall describe the colorings corresponding to the highest weights in Case II – IV in Section 4.

Remark 1.11. The $p=5$ case of Theorem 1.9 answers affirmatively the question raised in [GM5, p. 257 (after Theorem 8.1)] (see also [GM4, p. 83 (after Corollary 3)]).

The remainder of this paper is organized as follows. In Section 2, we formulate two results (Lemma 2.1 and Lemma 2.4) about the $\mathrm{Sp}(2g,\mathbb{F}_p)$-modules $F_p(g,c,\varepsilon)$. In Section 3, we review the construction of $F_p(g,c,\varepsilon)$ and the proof of Theorem 1.8, and then prove Lemma 2.1 and Lemma 2.4 using further arguments from TQFT. In Section 4, we prove Theorems 1.1 and 1.9. The only results from TQFT that will be used in the proof of these two theorems are those stated in Section 2. Finally, in Section 5, we make a few further comments and discuss the rank 3 case as an example.

Acknowledgements. We thank Henning H. Andersen for helpful discussions. He suggested checking our results against the Jantzen Sum Formula in the rank 3 case (see Section 5) and showed us how to do it. G. M. thanks the Mathematics Department of Louisiana State University, Baton Rouge, the Centre for Quantum

Geometry of Moduli Spaces, Aarhus, Denmark, and the Max Planck Institute for Mathematics, Bonn, Germany, for hospitality while part of this paper was written. P. G. also thanks the Max Planck Institute for Mathematics for hospitality. Last but not least, we thank the referee for his insightful comments.

2. Two lemmas

We begin by fixing some notation. For k any of the rings $\mathbb{Z}$, $\mathbb{F}_p$, or K, we take $\mathrm{Sp}(2g,k)$ to be the subgroup of $\mathrm{GL}(2g,k)$ consisting of isometries of the skew symmetric form given by the matrix $J_g = \begin{bmatrix} 0 & I_g \\ -I_g & 0 \end{bmatrix}$. Let $\mathbb{T}$ be the maximal torus of $\mathrm{Sp}(2g,K)$ given by the diagonal matrices of $\mathrm{Sp}(2g,K)$. For $1 \leq i \leq g$ and $x \in K^*$, let $T_{x,i}$ denote the diagonal matrix with x on the ith diagonal entry, x^{-1} on the $(g+i)$-th diagonal entry, and 1's elsewhere on the diagonal. We have an isomorphism

$$(K^*)^g \xrightarrow{\approx} \mathbb{T}, \qquad (x_1, \dots x_g) \mapsto \prod_{i=1}^{g} T_{x_i,i} \ .$$

We denote by $\{\varepsilon_i\}_{i=1,\dots,g}$ the standard basis of the weight lattice

$$X(\mathbb{T}) = \mathrm{Hom}(\mathbb{T}, K^*) \approx \bigoplus_{i=1}^{g} \mathrm{Hom}(K^*, K^*) \approx \mathbb{Z}^g$$

where $\varepsilon_i(T_{x,i}) = x$ and $\varepsilon_i(T_{x,j}) = 1$ for $j \neq i$.

We also let $\mathcal{B}(K)$ denote the Borel subgroup of $\mathrm{Sp}(2g,K)$ which is the group of block matrices of the form

$$\begin{bmatrix} A & B \\ 0 & (A^t)^{-1} \end{bmatrix}$$

where A is an invertible upper triangular matrix and B satisfies $AB^t = BA^t$.

Recall that $F_p(g,c,\varepsilon)$ is a representation of the finite symplectic group $\mathrm{Sp}(2g,\mathbb{F}_p)$ on the $\mathbb{F}_p$-vector space with basis $C_p(g,c,\varepsilon)$. Let $\hat{\mathfrak{b}}_\sigma$ denote the basis vector correponding to the coloring $\sigma \in C_p(g,c,\varepsilon)$. Since the finite field $\mathbb{F}_p$ is a subfield of K, we may consider the actions of the finite maximal torus $\mathbb{T}(\mathbb{F}_p) = \mathbb{T} \cap \mathrm{Sp}(2g,\mathbb{F}_p)$ and of the finite Borel subgroup $\mathcal{B}(\mathbb{F}_p) = \mathcal{B}(K) \cap \mathrm{Sp}(2g,\mathbb{F}_p)$ on $F_p(g,c,\varepsilon)$. The following Lemma says that the basis vectors $\hat{\mathfrak{b}}_\sigma$ are in some sense 'weight vectors' for $\mathbb{T}(\mathbb{F}_p)$.

Lemma 2.1. *Each basis vector $\hat{\mathfrak{b}}_\sigma$ is a simultaneous eigenvector for the commuting operators $\{T_{x,i}\}_{i=1,\dots,g}$ for $x \in \mathbb{F}_p^\star$, with eigenvalues given by*

$$T_{x,i}(\hat{\mathfrak{b}}_\sigma) = x^{d-1-a_i-2b_i}\,\hat{\mathfrak{b}}_\sigma$$

where $\sigma = (a_1, \dots, a_g, b_1, \dots, b_g, c_1, \dots)$.

Note that the exponents are meaningful only modulo $p-1$, as $\mathbb{F}_p^\star$ is a cyclic group of order $p-1$. We may interpret the collection of these exponents for a given basis vector $\hat{\mathfrak{b}}_\sigma$ as specifying a reduced weight, by which we mean an element of

$$X(\mathbb{T}(\mathbb{F}_p)) = X(\mathbb{T}) \otimes \mathbb{Z}/(p-1)\mathbb{Z} \approx (\mathbb{Z}/(p-1)\mathbb{Z})^g \ .$$

Let $W_p(g,c,\varepsilon)$ be the multiset of reduced weights occuring in $F_p(g,c,\varepsilon)$. The following is an immediate corollary of Lemma 2.1.

Corollary 2.2. *We have $W_p(g,c,\varepsilon) = \{\overline{w}(\sigma) \mid \sigma \in C_p(g,c,\varepsilon)\}$, where $\overline{w}(\sigma)$ is the reduction modulo $p-1$ of $w(\sigma)$ as defined in (6).*

Remark 2.3. Note that $W_p(g,c,\varepsilon)$ is also the reduction modulo $p-1$ of $\widetilde{W}_p(g,c,\varepsilon)$. This is because the restriction of the $\mathrm{Sp}(2g,K)$-module $\widetilde{F}_p(g,c,\varepsilon)$ to the finite group $\mathrm{Sp}(2g,\mathbb{F}_p)$ is $F_p(g,c,\varepsilon)\otimes K$.

In Section 4, we shall see that this information is enough to determine $\widetilde{W}_p(g,c,\varepsilon)$, except that in Case I, we will also need to use the following Lemma.

Lemma 2.4. *Let $\sigma_0=(0,0,\dots)$ be the coloring where all edges are colored zero. Then the basis vector $\hat{\mathfrak{b}}_{\sigma_0}$ in $F_p(g,0,0)$ is fixed up to scalars by the finite Borel subgroup $\mathcal{B}(\mathbb{F}_p)$.*

The proofs of Lemma 2.1 and Lemma 2.4 will be given in Section 3.

In Section 4 we shall apply Lemma 2.4 through the following Corollary whose proof we give already here.

Corollary 2.5. *The highest weight of $\widetilde{F}_p(g,0,0)$ is congruent modulo $p-1$ to $w(\sigma_0)=(d-1)\omega_g$.*

Proof. Let v be a highest weight vector in $\widetilde{F}_p(g,0,0)$. Then v is fixed up to scalars by $\mathcal{B}(K)$ (see [H1, 31.3]). Restricting to the finite symplectic group, we can view v as a vector in $F_p(g,c,\varepsilon)\otimes K$ that is fixed up to scalars by $\mathcal{B}(\mathbb{F}_p)$. By [CaLu, Theorem 7.1], there is a unique line fixed by $\mathcal{B}(\mathbb{F}_p)$ in $F_p(g,c,\varepsilon)\otimes K$. Since $\hat{\mathfrak{b}}_{\sigma_0}$ is also contained in this line by Lemma 2.4, we conclude that v and $\hat{\mathfrak{b}}_{\sigma_0}$ are proportional. In particular, v and $\hat{\mathfrak{b}}_{\sigma_0}$ have the same reduced weight, which implies the result. □

3. Results from TQFT

In this section, we review how Integral TQFT leads to the irreducible $\mathrm{Sp}(2g,\mathbb{F}_p)$-representations $F_p(g,c,\varepsilon)$ of Theorem 1.8 which were the starting point for this paper. In particular, we show how Theorem 1.8 follows from [GM5] using a result (Lemma 3.1) originally proved in [M]. We shall provide a self-contained proof of Lemma 3.1 in Appendix A. We then prove Lemma 2.1 and Lemma 2.4.

Let $\Sigma_g(2c)$ denote a closed surface of genus g equipped with one marked framed point labelled $2c$, where c is an integer with $0\le c\le d-1$. (Recall $d=(p-1)/2$.) Integral TQFT [GM1] associates to $\Sigma_g(2c)$ a free $\mathbb{Z}[\zeta_p]$-module $\mathcal{S}_p(\Sigma_g(2c))$ of finite rank, together with a projective-linear representation of the mapping class group of $\Sigma_g(2c)$ on this module. Here $p\ge 5$ is a prime, ζ_p is a primitive p-th root of unity, and $\mathbb{Z}[\zeta_p]$ is the ring of cyclotomic integers. The mapping class group of $\Sigma_g(2c)$ can be identified with $\Gamma_{g,1}$, that is, the mapping class group of $\Sigma_{g,1}$, an oriented surface of genus g with one boundary component. (Thus $\Gamma_{g,1}$ is the group of orientation-preserving diffeomorphisms of $\Sigma_{g,1}$ that fix the boundary pointwise, modulo isotopies of such diffeomorphisms.) The projective-linear representation of $\Gamma_{g,1}$ on $\mathcal{S}_p(\Sigma_g(2c))$ can be lifted to a linear representation of a certain central extension of $\Gamma_{g,1}$. The representations of mapping class groups obtained in this way may be considered as an integral refinement of the complex unitary representations coming from Witten-Reshetikhin-Turaev TQFT associated to the Lie group SO(3). In particular, the rank of the free $\mathbb{Z}[\zeta_p]$-module $\mathcal{S}_p(\Sigma_g(2c))$ is given by the Verlinde formula (2).

Recall that $1-\zeta_p$ is a prime in $\mathbb{Z}[\zeta_p]$, and $\mathbb{Z}[\zeta_p]/(1-\zeta_p)$ is the finite field $\mathbb{F}_p$. Thus we get a representation on the $\mathbb{F}_p$-vector space

$$F_p(\Sigma_g(2c))=\mathcal{S}_p(\Sigma_g(2c))/(1-\zeta_p)\mathcal{S}_p(\Sigma_g(2c))\ .$$

It is shown in [GM3, Cor. 12.4] that this induces a linear representation of $\Gamma_{g,1}$ on $F_p(\Sigma_g(2c))$ (*i.e.* the central extension is no longer needed). Furthermore, we proved in [GM5] that $F_p(\Sigma_g(2c))$ has a composition series with (at most) two irreducible factors. These irreducible factors are the $F_p(g,c,\varepsilon)$ defined in the introduction. More precisely, we have a short sequence of $\Gamma_{g,1}$-representations

$$0 \to F_p(g,c,1) \to F_p(\Sigma_g(2c)) \to F_p(g,c,0) \to 0 \ . \tag{7}$$

It remains to show that the action of $\Gamma_{g,1}$ on the irreducible factors $F_p(g,c,\varepsilon)$ factors through an action of the finite symplectic group $\mathrm{Sp}(2g,\mathbb{F}_p)$. For $g=1$, this was proved by explicit computation in [GM2]. For $g \geq 2$, we use the following lemma whose proof is deferred to Appendix A.

Lemma 3.1. *The Torelli group $\mathcal{I}_{g,1}$ acts trivially on $F_p(g,c,0)$ and $F_p(g,c,1)$.*

It follows that the action of $\Gamma_{g,1}$ on the irreducible factors $F_p(g,c,\varepsilon)$ factors through an action of the symplectic group

$$\mathrm{Sp}(2g,\mathbb{Z}) \cong \Gamma_{g,1}/\mathcal{I}_{g,1} \ .$$

To see that this descends to an action of the finite symplectic group $\mathrm{Sp}(2g,\mathbb{F}_p)$, we invoke a result of Mennicke, who proved that for $g \geq 2$, the group $\mathrm{Sp}(2g,\mathbb{F}_p)$ is the quotient of $\mathrm{Sp}(2g,\mathbb{Z})$ by the normal subgroup generated by the p-th power of a certain transvection [Me, Satz 10]. The result follows, because transvections lift to Dehn twists in $\Gamma_{g,1}$, and it is well-known that in SO(3)-TQFT at the prime p the p-th power of any Dehn twist acts trivially. This concludes the proof of Theorem 1.8.

For the proof of Lemma 2.1 and Lemma 2.4, we need to say more about the basis vectors $\hat{\mathfrak{b}}_\sigma$ associated to colorings σ. Recall the graph G_g depicted in Figure 1. A regular neighborhood in $\mathbb{R}^3$ of G_g is a 3-dimensional handlebody $\mathcal{H}_g$. We identify $\Sigma_g(2c)$ with the boundary of $\mathcal{H}_g$, in such a way that the univalent vertex labelled $2c$ in the figure meets the boundary surface in the marked point. Given this identification, there is a basis $\{\tilde{\mathfrak{b}}_\sigma\}$ of $\mathcal{S}_p(\Sigma_g(2c))$ called the orthogonal lollipop basis (see [GM2, p. 101]). The basis vectors are indexed by colorings σ in $C_p(g,c,0) \cup C_p(g,c,1)$. Reducing modulo $1-\zeta_p$, we get a basis $\{\hat{\mathfrak{b}}_\sigma\}$ of $F_p(\Sigma_g(2c))$. Notice that as an $\mathbb{F}_p$-vector space, $F_p(\Sigma_g(2c))$ is the direct sum of $F_p(g,c,0)$ and $F_p(g,c,1)$. The basis vectors $\hat{\mathfrak{b}}_\sigma$ where $\sigma \in C_p(g,c,\varepsilon)$ are a basis of $F_p(g,c,\varepsilon)$.

Remark 3.2. What we denote now by $\mathcal{S}_p$ was previously denoted by $\mathcal{S}_p^+$ in [GM2], and by $\mathcal{S}$ in [GM5]. Similarly, in [GM5], we omitted the subscript p in $F_p(\Sigma_g(2c))$. Also, we referred to ε as the parity (even or odd) of a coloring. Thus $F_p(g,c,1)$ was denoted by $F^{\,\mathrm{odd}}(\Sigma_g(2c))$ since it is spanned by the basis vectors corresponding to odd colorings ($\varepsilon = 1$). The short exact sequence (7) identifies $F_p(g,c,0)$ with the quotient representation $F_p(\Sigma_g(2c))/F^{\,\mathrm{odd}}(\Sigma_g(2c))$. As a vector space, this quotient was denoted by $F^{\,\mathrm{even}}(\Sigma_g(2c))$ in [GM5] since it is spanned by the basis vectors corresponding to even colorings ($\varepsilon = 0$).

Remark 3.3. The construction of Integral TQFT in [GM1] uses the skein-theoretic approach to TQFT of [BHMV]. In particular, the basis vectors $\tilde{\mathfrak{b}}_\sigma$ are represented by certain skein elements (that is, linear combinations of banded links or graphs) in the handlebody $\mathcal{H}_g$. If a diffeomorphism f of the surface $\Sigma_g(2c)$ extends to a diffeomorphism F of the handlebody, then the projective-linear action of f on $\mathcal{S}_p(\Sigma_g(2c))$ is determined by how F acts on skein elements in the handlebody. The details of this are irrelevant for our purposes, with one exception: In the case when $c = 0$, the basis vector $\tilde{\mathfrak{b}}_{\sigma_0}$ associated to the zero coloring σ_0 can be represented by the empty link in the handlebody $\mathcal{H}_g$. In particular, it is preserved by any diffeomorphism of the handlebody. So if f extends to a diffeomorphism of the handlebody, then the action of f on $\mathcal{S}_p(\Sigma_g(2c))$ fixes (projectively) the basis vector $\tilde{\mathfrak{b}}_{\sigma_0}$. This will be used below in the proof of Lemma 2.4.

Before giving the proof of Lemma 2.1 and Lemma 2.4, we also need to fix our conventions for the homomorphism $\Gamma_{g,1} \twoheadrightarrow \mathrm{Sp}(2g, \mathbb{Z})$. This homomorphism comes from the action of the mapping class group $\Gamma_{g,1}$ on the homology of the surface $\Sigma_g(2c)$ by isometries of the intersection form. Recall that we have identified $\Sigma_g(2c)$ with the boundary of a regular neighborhood $\mathcal{H}_g$ of the graph G_g. We identify $H_1(\Sigma_g(2c); \mathbb{Z})$ with $\mathbb{Z}^{2g}$ identifying the homology class of the positive meridian of the ith loop (oriented counterclockwise and counting from the left to right) with the ith basis vector of $\mathbb{Z}^{2g}$ and denote this element by m_i. Similarly we identify the homology class of the parallel to the ith loop to be the $(g+i)$th basis vector of $\mathbb{Z}^{2g}$. Then the intersection pairing is described by the matrix $J_g = \left[\begin{smallmatrix} 0 & I_g \\ -I_g & 0 \end{smallmatrix}\right]$.

Proof of Lemma 2.1. First, let us prove Lemma 2.1 in the special case when $g = 1$. Then $F_p(1, c, 1)$ is zero and $F_p(1, c, 0) = F(\Sigma_1(2c))$ has dimension $d - c$, as the graph G_1 is just a single lollipop, with stick color $2a_1$ equal to $2c$, so that only the color $a_1 + b_1$ of the loop edge may vary, and there are $d - a_1 = d - c$ possibilities for b_1. The representation of $\mathrm{SL}(2, \mathbb{F}_p) = \mathrm{Sp}(2, \mathbb{F}_p)$ on $F_p(1, c, 0)$ is shown in [GM2, §5] to be isomorphic to the standard representation of $\mathrm{SL}(2, \mathbb{F}_p)$ on homogeneous polynomials of degree $d - c - 1$ in two variables, say X and Y. Explicitly, this representation is given by:

$$\begin{bmatrix} \mathfrak{a} & \mathfrak{b} \\ \mathfrak{c} & \mathfrak{d} \end{bmatrix} X^{d-c-1-b} Y^b = (\mathfrak{a}X + \mathfrak{c}Y)^{d-c-1-b} (\mathfrak{b}X + \mathfrak{d}Y)^b.$$

Note that

$$\begin{bmatrix} x & 0 \\ 0 & x^{-1} \end{bmatrix} X^{d-c-1-b} Y^b = x^{d-1-c-2b} X^{d-c-1-b} Y^b.$$

Thus $X^{d-c-1-b}Y^b$, which is the b-th element in the monomial basis for the polynomials, is an eigenvector for $\left[\begin{smallmatrix} x & 0 \\ 0 & x^{-1} \end{smallmatrix}\right]$ with eigenvalue $x^{d-1-c-2b}$. One can check that the intertwiner Φ [GM2, §5] defining the isomorphism sends $X^{d-c-1-b}Y^b$ to a multiple of $\hat{\mathfrak{b}}_\sigma$ for σ the coloring which is $2c$ on the stick edge and $c + b$ on the loop edge of G_1. Thus Lemma 2.1 holds when $g = 1$.

The general case is now proved as follows. The torus $\mathbb{T}(\mathbb{F}_p)$ is contained in the subgroup of $\mathrm{Sp}(2g, \mathbb{F}_p)$ isomorphic to a product of g copies of $\mathrm{SL}(2, \mathbb{F}_p) = \mathrm{Sp}(2, \mathbb{F}_p)$ arising from the g copies of $\mathrm{SL}(2, \mathbb{Z}) = \mathrm{Sp}(2, \mathbb{Z})$ in $\mathrm{Sp}(2g, \mathbb{Z})$ corresponding to each loop of G_g. Specifically, the element $T_{x,i}$ defined in Section 2 lies in the i-th copy. Similarly, the mapping class group $\Gamma_{g,1}$ contains a subgroup isomorphic to a product of g copies of $\Gamma_{1,1}$. The i-th copy of $\Gamma_{1,1}$ is generated by the Dehn twist about the meridian and the Dehn twist about the parallel to the ith loop of G_g. Since the homomorphism $\Gamma_{g,1} \twoheadrightarrow \mathrm{Sp}(2g, \mathbb{F}_p)$ is surjective, we can lift $T_{x,i}$ (non-uniquely) to a mapping class, say ϕ, which we may assume to lie in the i-th copy of $\Gamma_{1,1}$. This copy of $\Gamma_{1,1}$ is the mapping class group of the one-holed torus which is cut off from $\Sigma_g(2c)$ by the simple closed curve γ on $\Sigma_g(2c)$ which is a meridian of the i-th stick edge of the graph G_g. Using the integral modular functor properties of [GM1, Section 11], we have an injective linear map

$$\bigoplus_{a_i=0}^{d-1} \mathcal{S}_p(\Sigma_1(2a_i)) \otimes \mathcal{S}_p(\Sigma_{g-1}(2a_i, 2c)) \longrightarrow \mathcal{S}_p(\Sigma_g(2c)) \tag{8}$$

given by gluing along γ. Here, $\Sigma_{g-1}(2a_i, 2c)$ stands for a genus $g-1$ surface with two marked points labelled $2a_i$ and $2c$, respectively. The module $\mathcal{S}_p(\Sigma_{g-1}(2a_i, 2c))$ is again a free $\mathbb{Z}[\zeta_p]$-lattice by [GM1, Theorem 4.1]. The image of the gluing map (8) is a free sublattice of $\mathcal{S}_p(\Sigma_g(2c))$ of full rank. When tensored with the quotient field of $\mathbb{Z}[\zeta_p]$, the map (8) becomes an isomorphism familiar in TQFTs defined over a field under the name of 'factorization along a separating curve'. Over the ring $\mathbb{Z}[\zeta_p]$ the gluing map (8) is, however, not surjective in general.

On the sublattice of $\mathcal{S}_p(\Sigma_g(2c))$ given by the image of the map (8), the mapping class ϕ preserves the direct sum decomposition and in each summand, ϕ acts only on the first tensor factor $\mathcal{S}_p(\Sigma_1(2a_i))$. When reduced modulo $1-\zeta_p$, the action induced by ϕ on $F_p(\Sigma_1(2a_i))$ is as described in the genus one case. In particular, the lollipop with stick color $2a_i$ and loop color $a_i + b_i$ indexes an eigenvector for the induced action of ϕ on $F_p(\Sigma_1(2a_i))$ with eigenvalue $x^{d-1-a_i-2b_i}$. If the map (8) were an isomorphism of $\mathbb{Z}[\zeta_p]$-modules, this would prove the lemma by familiar TQFT arguments, since it would then also induce an isomorphism when reduced modulo $1-\zeta_p$.

Although (8) is not an isomorphism of $\mathbb{Z}[\zeta_p]$-modules, we are saved by the following fact (see [GM1, Theorem 11.1]). Pick a basis $\{\mathfrak{b}_\nu^{(a_i)}\}$ of the lattice $\mathcal{S}_p(\Sigma_{g-1}(2a_i, 2c))$ associated to a lollipop tree as in [GM1, Theorem 4.1]. Then the image under the map (8) of the direct summand $\mathcal{S}_p(\Sigma_1(2a_i)) \otimes \mathfrak{b}_\nu^{(a_i)}$ of the L.H.S. of (8) is a certain power of $1-\zeta_p$ times a direct summand of the R.H.S. of (8), that is, of $\mathcal{S}_p(\Sigma_g(2c))$. (The power of $1-\zeta_p$ may depend on the summand.) Thus the action of ϕ on this direct summand, and hence the action of $T_{x,i}$ on the reduction modulo $1-\zeta_p$ of this direct summand, can be computed from the action of ϕ on $\mathcal{S}_p(\Sigma_1(2a_i)) \otimes \mathfrak{b}_\nu^{(a_i)} \simeq \mathcal{S}_p(\Sigma_1(2a_i))$. Since this action is given by the genus one case, where the lemma is already proved, it follows that for a coloring $\sigma = (a_1, \ldots, a_g, b_1, \ldots, b_g, c_1, \ldots)$, the basis vector $\hat{\mathfrak{b}}_\sigma$ is an eigenvector of $T_{x,i}$ with eigenvalue $x^{d-1-a_i-2b_i}$. This completes the proof. □

Remark 3.4. As a word of caution, we mention that a basis $\{\mathfrak{b}_\nu^{(a_i)}\}$ of the lattice $\mathcal{S}_p(\Sigma_{g-1}(2a_i, 2c))$ as needed in the proof above cannot be obtained from colorings of the graph obtained from G_g by cutting G_g at the mid-point of the stick edge of the i-th lollipop and removing the connected component containing the loop edge of the lollipop, as one would do when working with TQFTs defined over a field. This is because the remaining graph would not be a lollipop tree. See [GM1, Section 10].

We now prepare the way for the proof of Lemma 2.4. Let $\mathfrak{L}$ be the span of the homology classes of the meridians $m_1, m_2, \ldots, m_g$ in $H_1(\Sigma_g) = \mathbb{Z}^{2g}$. Note that $\mathfrak{L}$ is a lagrangian subspace with respect to the form J_g. Let $\mathcal{L}(\mathbb{Z})$ be the subgroup of $\mathrm{Sp}(2g, \mathbb{Z})$ consisting of the matrices which preserve $\mathfrak{L}$. One has that $\mathcal{L}(\mathbb{Z})$ is the set of matrices of the form $\begin{bmatrix} A & B \\ 0 & (A^t)^{-1} \end{bmatrix}$ where $A \in \mathrm{GL}(g, \mathbb{Z})$, and B satisfies $AB^t = BA^t$. We call this subgroup the lagrangian subgroup.

Let Γ_g be the mapping class group of the closed surface Σ_g of genus g, viewed as the boundary of the handlebody $\mathcal{H}_g$. Note that $\mathfrak{L}$ is the kernel of the map $H_1(\Sigma_g) \to H_1(\mathcal{H}_g)$. If $f \in \Gamma_g$, and f extends to a diffeomorphism $F : \mathcal{H}_g \to \mathcal{H}_g$ then $f_* \in \mathcal{L}(\mathbb{Z})$. We have a converse:

Proposition 3.5. *If $f \in \mathcal{L}(\mathbb{Z})$, then f is induced by an element of Γ_g which extends to a diffeomorphism $F : \mathcal{H}_g \to \mathcal{H}_g$.*

Proof. Consider the special case when $f \in \mathcal{L}(\mathbb{Z})$ has the form $\begin{bmatrix} I_g & B \\ 0 & I_g \end{bmatrix}$. It follows that $B = B^t$. Consider the building blocks $\begin{bmatrix} I_g & E(i,j) \\ 0 & I_g \end{bmatrix}$ where $E(i,i)$ has zero entries everywhere except for the (i,i) location where it has a 1, and $E(i,j)$ (for $i \neq j$) has zero entries everywhere except for the (i,j) location and the (j,i) location where it has 1's. These $E(i,j)$ are realized by Dehn twists along m_i in the case $i = j$, and along a curve representing $m_i + m_j$ when $i \neq j$. These curves may be chosen so that they bound disks in $\mathcal{H}_g$. Thus these Dehn twists extend over $\mathcal{H}_g$. Products of such Dehn twists realize any symmetric matrix B. See [GL, p 312-313].

We can reduce the general case to the above case, using another special case: $f \in \mathcal{L}(\mathbb{Z})$ has the form $\left[\begin{smallmatrix} A & 0 \\ 0 & D \end{smallmatrix}\right]$. We note that this is the case when $A = (D^t)^{-1}$, where $D \in \mathrm{GL}(g, \mathbb{Z})$. An elementary matrix in $\mathrm{SL}(g, \mathbb{Z})$ can be realized, as D, by sliding one 1-handle in $\mathcal{H}_g$ over another. Permuting two handles realizes, as D, a transposition matrix. Any $D \in \mathrm{GL}(g, \mathbb{Z})$ is a product of elementary matrices and perhaps a transposition matrix. Thus $\begin{bmatrix} (D^t)^{-1} & 0 \\ 0 & D \end{bmatrix}$ for any $D \in \mathrm{GL}(g, \mathbb{Z})$ can be realized by a diffeomorphism which extends over $\mathcal{H}_g$. □

We let $U(\mathbb{F}_p)$ denote the unipotent radical of the finite Borel subgroup $\mathcal{B}(\mathbb{F}_p)$.

Proposition 3.6. *The image of $\mathcal{L}(\mathbb{Z})$ under the quotient map $\pi : \mathrm{Sp}(2g, \mathbb{Z}) \twoheadrightarrow \mathrm{Sp}(2g, \mathbb{F}_p)$ contains $U(\mathbb{F}_p)$.*

Proof. We have that $U(\mathbb{F}_p)$ is the group of block matrices over $\mathbb{F}_p$ of the form $\begin{bmatrix} V & B \\ 0 & (V^t)^{-1} \end{bmatrix}$ where V is an invertible upper triangular matrix with 1's on the diagonal and B satisfies $VB^t = BV^t$. Each such matrix may be factored $\begin{bmatrix} I_g & BV^t \\ 0 & I_g \end{bmatrix} \begin{bmatrix} V & 0 \\ 0 & (V^t)^{-1} \end{bmatrix}$, and BV^t will equal its transpose. As above, we note that $\begin{bmatrix} I_g & BV^t \\ 0 & I_g \end{bmatrix}$ can be written as a product of $\begin{bmatrix} I_g & E(i,j) \\ 0 & I_g \end{bmatrix}$ matrices. Thus any matrix of the form $\begin{bmatrix} I_g & BV^t \\ 0 & I_g \end{bmatrix}$ has lifts under the quotient map $\pi : \mathrm{Sp}(2g, \mathbb{Z}) \twoheadrightarrow \mathrm{Sp}(2g, \mathbb{F}_p)$ that lie in $\mathcal{L}(\mathbb{Z})$. Also any matrix of the form $\begin{bmatrix} V & 0 \\ 0 & (V^t)^{-1} \end{bmatrix}$ has such a lift. It follows that any element of $U(\mathbb{F}_p)$ lifts to an element of $\mathcal{L}(\mathbb{Z})$. □

Proof of Lemma 2.4. Recall that $\sigma_0 = (0, 0, \dots)$ denotes the coloring where all edges are colored zero. We are to show that the basis vector $\hat{\mathfrak{b}}_{\sigma_0}$ in $F_p(g, 0, 0)$ is fixed up to scalars by $\mathcal{B}(\mathbb{F}_p)$. It will suffice to show that $\hat{\mathfrak{b}}_{\sigma_0}$ is fixed by $U(\mathbb{F}_p)$. Note that $\hat{\mathfrak{b}}_{\sigma_0}$ is the reduction modulo $1 - \zeta_p$ of the basis vector $\tilde{\mathfrak{b}}_{\sigma_0}$ of $\mathcal{S}_p(\Sigma_g(0))$ which is represented by the empty skein, and is thus fixed by any element of Γ_g which extends to a diffeomorphism of $\mathcal{H}_g$, as observed in Remark 3.3. By Proposition 3.6, any element of $U(\mathbb{F}_p)$ lifts to an element of $\mathcal{L}(\mathbb{Z})$, and by Proposition 3.5, any element of $\mathcal{L}(\mathbb{Z})$ is induced by an element of Γ_g which extends to a diffeomorphism of $\mathcal{H}_g$. This implies the result. □

4. Proof of Theorems 1.1 and 1.9

Theorem 1.1 follows easily from Theorem 1.9 and the dimension formulae of [GM5, p. 229], where we computed the cardinality of the sets $C_p(g,c,\varepsilon)$ in the various cases in terms of the Verlinde formula (2) and its cousin (3).

In the proof of Theorem 1.9, we shall need one more result from modular representation theory. Recall that the set of simple positive roots for the symplectic Lie algebra consists of $\alpha_1 = \varepsilon_1 - \varepsilon_2, \ldots, \alpha_{g-1} = \varepsilon_{g-1} - \varepsilon_g$, and $\alpha_g = 2\varepsilon_g$ [B, Planche III].

Lemma 4.1. *Let $p > 2$ and suppose λ is a p-restricted dominant weight for $\mathrm{Sp}(2g,K)$. Let $\Pi(\lambda)$ be the set (without multiplicities) of weights occuring in the simple module $L_p(\lambda)$.*

(i) *If $\mu \in \Pi(\lambda)$ is such that $\mu + \alpha_i \notin \Pi(\lambda)$ for all $i = 1,\ldots,g$, then $\mu = \lambda$.*
(ii) *If $\lambda = \sum \eta_i\omega_i$ and $\eta_i > 0$ for some $i = 1,\ldots,g$, then $\lambda - \alpha_i \in \Pi(\lambda)$.*

Proof. This is true for the sets of weights of simple $\mathrm{Sp}(2g,\mathbb{C})$-modules. By a result of Premet [P] (see also the discussion in [H2, §3.2]), $\Pi(\lambda)$ is the same when working over K or $\mathbb{C}$ as long as λ is p-restricted and the characteristic $p > 2$. The result follows. □

Let us now prove Theorem 1.9. Recall that we must determine $\widetilde{W}_p(g,c,\varepsilon)$ (= the multiset of weights occuring in $\widetilde{F}_p(g,c,\varepsilon)$), and we must determine which of the weights in $\widetilde{W}_p(g,c,\varepsilon)$ is the highest weight, which we denote by $\lambda_p(g,c,\varepsilon)$. As the details of this are somewhat involved, let us first outline the strategy of the proof. The proof proceeds in four steps, as follows.

Step 1. The first step is to compute $\widetilde{W}_p(g,c,\varepsilon)$ modulo $p-1$. As observed in Remark 2.3, we already know the answer: it is the multiset $W_p(g,c,\varepsilon)$ which was determined in Corollary 2.2. Recall that the elements of $W_p(g,c,\varepsilon)$ are reduced weights, and that every coloring in $C_p(g,c,\varepsilon)$ determines a reduced weight in $W_p(g,c,\varepsilon)$.

Step 2. The second step is to identify $\overline{\lambda}_p(g,c,\varepsilon)$, that is, the reduced weight in $W_p(g,c,\varepsilon)$ which is the reduction modulo $p-1$ of the highest weight. In Case I, this is the reduced weight associated to the zero coloring, as proved in Corollary 2.5. In the three other cases, we will show that $\overline{\lambda}_p(g,c,\varepsilon)$ is the reduced weight associated to a coloring illustrated in Figure 3.

This will be proved by showing that these colorings satisfy the hypothesis of the following Lemma. We let $\overline{\alpha}_i$ denote the reduction modulo $p-1$ of the root α_i.

Lemma 4.2. *Let σ be a coloring in $C_p(g,c,\varepsilon)$ and let $\overline{w}(\sigma)$ be its associated reduced weight. If $\overline{w}(\sigma) + \overline{\alpha}_i \notin W_p(g,c,\varepsilon)$ for all $i = 1,\ldots,g$, then $\overline{w}(\sigma) = \overline{\lambda}_p(g,c,\varepsilon)$.*

Proof. Let μ be any lift of $\overline{w}(\sigma)$ to $\widetilde{W}_p(g,c,\varepsilon)$. The hypothesis implies that for all $i = 1,\ldots,g$, the weight $\mu + \alpha_i$ does not occur in $\widetilde{W}_p(g,c,\varepsilon)$. By the construction of the module $\widetilde{F}_p(g,c,\varepsilon)$, we know that its highest weight is p-restricted, so that we can apply Lemma 4.1(i). It follows that μ is the highest weight, and so $\overline{w}(\sigma)$ is the reduction modulo $p-1$ of the highest weight, as claimed. □

Step 3. Once $\overline{\lambda}_p(g,c,\varepsilon)$ is known, the third step will be to determine $\lambda_p(g,c,\varepsilon)$. Write $\lambda_p(g,c,\varepsilon) = \sum \eta_i\omega_i$ with $0 \le \eta_i \le p-1$ (since $\lambda_p(g,c,\varepsilon)$ is p-restricted). The

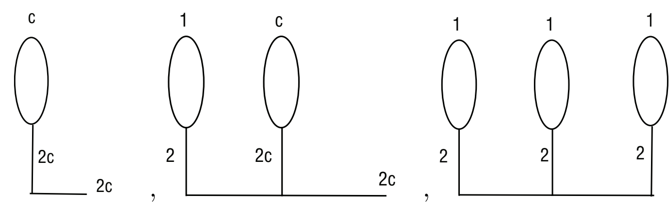

FIGURE 3. The colorings associated to the highest weights in Case II, Case III, and Case IV. The leftmost part of G_g is not drawn as it is colored zero. For the same reason the rightmost edge is not drawn in Case IV as c is zero. These graphs could be guessed by taking the smallest coloring which is rightmost on the graph and has the given type.

coefficient η_i is determined by its reduction $\overline{\eta}_i$ modulo $p-1$ provided $\overline{\eta}_i \neq 0$. But if $\overline{\eta}_i = 0$, then η_i can be either 0 or $p-1$. We shall show that $\eta_i = 0$ whenever $\overline{\eta}_i = 0$ in all our cases by means of the following Lemma.

Lemma 4.3. *Let $\lambda_p(g,c,\varepsilon) = \sum \eta_i\omega_i$ be the highest weight in $\widetilde{W}_p(g,c,\varepsilon)$. If $\overline{\lambda}_p(g,c,\varepsilon) - \overline{\alpha}_i \notin W_p(g,c,\varepsilon)$, then $\eta_i = 0$.*

Proof. This follows immediately from Lemma 4.1(ii). □

Step 4. Once Step 3 is completed, it only remains to prove that $\widetilde{W}_p(g,c,\varepsilon)$ is as claimed in the theorem. This is now easy. Recall the notation $d = (p-1)/2$. We simply note that all weights in $\widetilde{W}_p(g,c,\varepsilon)$ must lie in $[1-d, d-1]^g$ as they must lie in the convex hull of the orbit under the Weyl group of the highest weight, and in each case this highest weight has been shown in Step 3 to lie in $[0, d-1]^g$. But no two distinct integer points in $[1-d, d-1]^g$ agree modulo $p-1 = 2d$ in each coordinate. Thus $\widetilde{W}_p(g,c,\varepsilon)$ is determined by its reduction modulo $p-1$, and we are done.

In the rest of this section, we shall now carry out Steps 2 and 3 in the various cases. Having done this, the proof will be complete. To simplify notation, we shall denote the highest weight $\lambda_p(g,c,\varepsilon)$ simply by λ. Also, from now on when we say coloring, we mean a small admissible p-coloring.

Recall that a coloring $\sigma = (a_1, \ldots, a_g, b_1, \ldots, b_g, c_1, \ldots)$ assigns the color $2a_i$ to the ith stick edge and the color $a_i + b_i$ to the ith loop edge (see Figure 2). Recall also that $a_i \geq 0$, $b_i \geq 0$ satisfy the smallness condition $a_i + b_i \leq d-1$, and the coefficient of ε_i in the weight $w(\sigma)$ is $d - 1 - a_i - 2b_i$ (see (6)).

Before we begin with the cases, we state two lemmas. Both are an easy consequence of Corollary 2.2 and the smallness condition. Recall $2d = p-1$.

Lemma 4.4. *If $n_i \equiv d \pmod{2d}$ for some $1 \leq i \leq g$, then $\sum_{i=1}^g n_i\overline{\varepsilon}_i \notin W_p(g,c,\varepsilon)$,*

Lemma 4.5. *Suppose $\sigma = (a_1, \ldots, a_g, b_1, \ldots, b_g, c_1, \ldots)$, and $\overline{w}(\sigma) = \sum_{i=1}^g n_i\overline{\varepsilon}_i$. If $n_i \equiv d-1 \pmod{2d}$ for some $1 \leq i \leq g$, then $a_i = b_i = 0$.*

Case I. Recall σ_0 is the coloring which is zero on every edge. Step 2 was already taken in Corollary 2.5 and so we know that $\overline{\lambda} = \overline{w}(\sigma_0) = (d-1)\overline{\omega}_g$. In Step 3, we must show that $\lambda = (d-1)\omega_g$. By Lemma 4.3, it is enough to show that

$\overline{\lambda} - \overline{\alpha}_j \notin W_p(g,0,0)$ for $1 \le j \le g-1$, which follows easily from Lemma 4.4. This completes the proof in Case I.

Remark 4.6. One cannot accomplish Step 2 in Case I in the same way as we do below in Cases II, III, and IV, as σ_0 does not satisfy the hypotheses of Lemma 4.2. This is because $\overline{w}(\sigma_0) + \overline{\alpha}_g = (d-1)\overline{\omega}_{g-1} + (d+1)\overline{\varepsilon}_g = \overline{w}(\sigma') \in W_p(g,0,0)$, where σ' denotes the coloring with all a_i's, b_i's and c_i's zero except for $b_g = d-1$.

Case II. Let σ be the coloring on the left of Figure 3, then

$$\overline{w}(\sigma) = (d-1)\sum_{i=1}^{g-1} \overline{\varepsilon}_i + (d-c-1)\overline{\varepsilon}_g = (d-c-1)\overline{\omega}_g + c\,\overline{\omega}_{g-1}.$$

We shall show that $\lambda = w(\sigma) = (d-c-1)\omega_g + c\,\omega_{g-1}$.

As explained above, Step 2 in the proof is based on Lemma 4.2. We must show that $\overline{w}(\sigma) + \overline{\alpha}_i \notin W_p(g,c,0)$ for all $1 \le i \le g$. For $i \ne g$ this follows from Lemma 4.4. For $i = g$, it is proved by contradiction, as follows. Assume that $\overline{w}(\sigma) + \overline{\alpha}_g \in W_p(g,c,0)$. Then there is a coloring $\sigma' = (a'_1, \ldots, b'_1, \ldots, c'_1, \ldots)$ of type $(c,0)$ with

$$\overline{w}(\sigma') = \overline{w}(\sigma) + \overline{\alpha}_g = (d-1)\sum_{i=1}^{g-1} \overline{\varepsilon}_i + (d-c+1)\overline{\varepsilon}_g \ .$$

We will see such a coloring is impossible. By Lemma 4.5, $a'_i = b'_i = 0$ for $i \ne g$. In other words, σ' must color all but the rightmost lollipop by zero. By admissibility, it follows that $a'_g = c$. On the other hand, since the coefficient of $\overline{\varepsilon}_g$ in $\overline{w}(\sigma')$ is $d-1-a'_g-2b'_g \pmod{2d}$, we have

$$d-c+1 \equiv d-1-a'_g-2b'_g = d-1-c-2b'_g \pmod{2d}\ , \tag{9}$$

so $b'_g \equiv -1 \pmod d$, so $b'_g = d-1$ by smallness and hence $a'_g = 0$ again by smallness (see (5)). This contradicts $a'_g = c > 0$. Thus σ' does not exist and hence $\overline{w}(\sigma) + \overline{\alpha}_g \notin W_p(g,c,0)$.

This completes Step 2, and we now know that $\overline{\lambda} = \overline{w}(\sigma) = (d-c-1)\overline{\omega}_g + c\,\overline{\omega}_{g-1}$.

Next, Step 3 in the proof is based on Lemma 4.3. We must show that $\overline{\lambda} - \overline{\alpha}_i \notin W_p(g,c,0)$ whenever the coefficient of $\overline{\omega}_i$ in $\overline{\lambda}$ is zero. For $1 \le j \le g-2$, this follows from Lemma 4.4. Then if $1 \le c \le d-2$, Step 3 is already complete, as the coefficient of $\overline{\omega}_g$ and of $\overline{\omega}_{g-1}$ in $\overline{\lambda}$ is non-zero. But if $c = d-1$, the coefficient of $\overline{\omega}_g$ in $\overline{\lambda}$ is zero and we therefore also need to show that $\overline{\lambda} - \overline{\alpha}_g \notin W_p(g,d-1,0)$. This is again proved by contradiction. Assume that $\overline{\lambda} - \overline{\alpha}_g \in W_p(g,d-1,0)$. Then there is a coloring σ'' of type $(d-1,0)$ with

$$\overline{w}(\sigma'') = \overline{\lambda} - \overline{\alpha}_g = (d-1)\sum_{i=1}^{g-1} \overline{\varepsilon}_i - 2\,\overline{\varepsilon}_g \ . \tag{10}$$

As before when we ruled out the coloring σ' in Step 2, it follows from Lemma 4.5 that σ'' must color all but the rightmost lollipop by zero. By admissibility, it follows that $a''_g = c = d-1$ and so $b''_g = 0$ by smallness. But then the coefficient of $\overline{\varepsilon}_g$ in $\overline{w}(\sigma'')$ must be $d-1-a''_g-2b''_g = 0 \pmod{2d}$, which contradicts (10) where this coefficient is $-2 \pmod{2d}$. This contradiction shows that σ'' does not exist. This completes the proof in Case II.

In Case III and IV, we will also need the following Lemma which says that odd colorings must assign nonzero colors to at least two lollipop sticks, and to at least three lollipop sticks if $c = 0$.

Lemma 4.7. *Suppose $\sigma = (a_1, \ldots, a_g, b_1, \ldots, b_g, c_1, \ldots)$ is a small admissible p-coloring of type $(c, 1)$.*

(i) *There are at least two distinct $i \in \{1, \ldots, g\}$ with $a_i > 0$.*
(ii) *If moreover $c = 0$, then there are at least three distinct $i \in \{1, \ldots, g\}$ with $a_i > 0$.*

Proof. (i) If only one of the a_i is non-zero, say a_{i_0}, then admissibility implies that $a_{i_0} = c$ and so condition (4) in the definition of colorings of type $(c, 1)$ is violated.

(ii) If moreover $c = 0$, and only two of the a_i are non-zero, say a_{i_0} and a_{i_1}, then admissibility implies that $a_{i_0} = a_{i_1}$ and so condition (4) is again violated. □

Case III. Let σ be the coloring in the middle of Figure 3, then

$$\overline{w}(\sigma) = (d-1)\sum_{i=1}^{g-2} \overline{\varepsilon}_i + (d-2)\overline{\varepsilon}_{g-1} + (d-c-1)\overline{\varepsilon}_g = (d-c-1)\overline{\omega}_g + (c-1)\overline{\omega}_{g-1} + \overline{\omega}_{g-2}.$$

We shall show that $\lambda = w(\sigma) = (d - c - 1)\omega_g + (c - 1)\omega_{g-1} + \omega_{g-2}$.

In Step 2, we must show that $\overline{w}(\sigma) + \overline{\alpha}_i \notin W_p(g, c, 1)$ for all $1 \le i \le g$. For $i \le g-2$ this follows from Lemma 4.4. For $i \in \{g-1, g\}$ it is proved by contradiction, as follows.

(Case $i = g - 1$.) Assume that $\overline{w}(\sigma) + \overline{\alpha}_{g-1} \in W_p(g, c, 1)$. Then there is a coloring σ' of type $(c, 1)$ with

$$\overline{w}(\sigma') = \overline{w}(\sigma) + \overline{\alpha}_{g-1} = (d-1)\sum_{i=1}^{g-1} \overline{\varepsilon}_i + (d - c - 2)\overline{\varepsilon}_g \ .$$

Note σ' must color all but the rightmost lollipop with zeros by Lemma 4.5, and so σ' contradicts Lemma 4.7(i).

(Case $i = g$.) Assume that $\overline{w}(\sigma) + \overline{\alpha}_g \in W_p(g, c, 1)$. Then there is a coloring σ'' of type $(c, 1)$ with

$$\overline{w}(\sigma'') = \overline{w}(\sigma) + \overline{\alpha}_g = (d-1)\sum_{i=1}^{g-2} \overline{\varepsilon}_i + (d-2)\overline{\varepsilon}_{g-1} + (d - c + 1)\overline{\varepsilon}_g \ .$$

By Lemma 4.5 we have $a''_i = 0$ for $1 \le i \le g - 2$. By admissibility, it follows that the three colors meeting at the trivalent vertex at the bottom of the rightmost stick are $2a''_{g-1}, 2a''_g$, and $2c$. Computing the coefficient of $\overline{\varepsilon}_{g-1}$, we have

$$d - 2 \equiv d - 1 - a''_{g-1} - 2b''_{g-1} \pmod{2d}$$

or $a''_{g-1} + 2b''_{g-1} \equiv 1 \pmod{2d}$. By smallness, it follows that $a''_{g-1} = 1$. This implies two things. First, since $\varepsilon = 1$ (*i.e.*, the coloring is odd), it follows that $a''_g \equiv c \pmod 2$. Second, by the triangle inequality in the admissibility condition at the trivalent vertex at the bottom of the rightmost stick, it follows that $c - 1 \le a''_g \le c + 1$. One concludes that $a''_g = c$. The rest of the proof is now the same as in Case II Step 2. Computing the coefficient of $\overline{\varepsilon}_g$ exactly as was done there (see (9)), we deduce $b''_g \equiv -1 \pmod d$, hence $b''_g = d - 1$ and so $a''_g = 0$ by smallness. This contradicts $a''_g = c > 0$.

Thus Step 2 is complete, and we now know that $\overline{\lambda} = \overline{w}(\sigma) = (d-c-1)\overline{\omega}_g + (c-1)\overline{\omega}_{g-1} + \overline{\omega}_{g-2}$.

For Step 3, we must show that $\overline{\lambda} - \overline{\alpha}_i \notin W_p(g, c, 0)$ whenever the coefficient of $\overline{\omega}_i$ in $\overline{\lambda}$ is zero. For $1 \le i \le g-3$, this follows from Lemma 4.4. Then if $2 \le c \le d-2$, Step 3 is already complete, as the coefficient of $\overline{\omega}_g$, $\overline{\omega}_{g-1}$, and $\overline{\omega}_{g-2}$ in $\overline{\lambda}$ is non-zero. But if $c = 1$, then we also need to show that $\overline{\lambda} - \overline{\alpha}_{g-1} \notin W_p(g, 1, 1)$, and if $c = d-1$, then we also need to show that $\overline{\lambda} - \overline{\alpha}_g \notin W_p(g, d-1, 1)$. The arguments in these two cases will be given below. Note that for $d = 2$ (which corresponds to $p = 5$) we have both $c = 1$ and $c = d-1$, so that we need to use both arguments.

(Case $c = 1$.) Assume for a contradiction that $\overline{\lambda} - \overline{\alpha}_{g-1} \in W_p(g, 1, 1)$. Then there is a coloring σ''' of type $(1, 1)$ with

$$\overline{w}(\sigma''') = \overline{\lambda} - \overline{\alpha}_{g-1} = (d-1)\sum_{i=1}^{g-2} \overline{\varepsilon}_i + (d-3)\overline{\varepsilon}_{g-1} + (d-1)\overline{\varepsilon}_g \ .$$

By Lemma 4.5 σ''' must color all but the $(g-1)$st lollipop by zero, which violates Lemma 4.7(i). This shows that $\overline{\lambda} - \overline{\alpha}_{g-1} \notin W_p(g, 1, 1)$.

(Case $c = d-1$.) Assume for a contradiction that $\overline{\lambda} - \overline{\alpha}_g \in W_p(g, d-1, 1)$. Then there is a coloring $\tilde{\sigma}$ of type $(d-1, 1)$ with

$$\overline{w}(\tilde{\sigma}) = \overline{\lambda} - \overline{\alpha}_g = (d-1)\sum_{i=1}^{g-2} \overline{\varepsilon}_i + (d-2)\overline{\varepsilon}_{g-1} - 2\overline{\varepsilon}_g \ . \tag{11}$$

By the exact same reasoning as when showing that $a''_g = c$ for the coloring σ'' in Step 2 (Case $i = g$), we have $\tilde{a}_g = c$. Hence $\tilde{a}_g = d-1$ (since we assume $c = d-1$) and so $\tilde{b}_g = 0$ by smallness. But then the coefficient of $\overline{\varepsilon}_g$ in $\overline{w}(\tilde{\sigma})$ must be $d - 1 - \tilde{a}_g - 2\tilde{b}_g = 0 \pmod{2d}$ which contradicts (11). This shows that $\overline{\lambda} - \overline{\alpha}_g \notin W_p(g, d-1, 1)$.

The proof in Case III is now complete.

Case IV**.** Let σ be the coloring on the right of Figure 3, then

$$\overline{w}(\sigma) = (d-1)\sum_{i=1}^{g-3} \overline{\varepsilon}_i + (d-2)\sum_{i=g-2}^{g} \overline{\varepsilon}_i = (d-2)\overline{\omega}_g + \overline{\omega}_{g-3}.$$

We shall show that $\lambda = w(\sigma) = (d-2)\omega_g + \omega_{g-3}$.

In Step 2, we must show that $\overline{w}(\sigma) + \overline{\alpha}_i \notin W_p(g, c, 0)$ for all $1 \le i \le g$. For $i \le g-3$ and also for $i = g$, this follows from Lemma 4.4. For $i = g-2$, it is proved by contradiction, as follows. Assume that $\overline{w}(\sigma) + \overline{\alpha}_{g-2} \in W_p(g, 0, 1)$. Then there is a coloring σ' of type $(0, 1)$ with

$$\overline{w}(\sigma') = \overline{w}(\sigma) + \overline{\alpha}_{g-2} = (d-1)\sum_{i=1}^{g-2} \overline{\varepsilon}_i + (d-3)\overline{\varepsilon}_{g-1} + (d-2)\overline{\varepsilon}_g \ .$$

Note that σ' must color all but two of the lollipops with zeros by Lemma 4.5 and so σ' contradicts Lemma 4.7(ii). This shows that $\overline{w}(\sigma) + \overline{\alpha}_{g-2} \notin W_p(g, 0, 1)$. We refer to this argument as the "two lollipop argument".

For $i = g-1$, the proof is similar: We have that

$$\overline{w}(\sigma) + \overline{\alpha}_{g-1} = (d-1)\sum_{i=1}^{g-3} \overline{\varepsilon}_i + (d-2)\overline{\varepsilon}_{g-2} + (d-1)\overline{\varepsilon}_{g-1} + (d-3)\overline{\varepsilon}_g$$

and the two lollipop argument shows that $\overline{w}(\sigma) + \overline{\alpha}_{g-1} \notin W_p(g,0,1)$.

Thus Step 2 is complete, and we now know that $\overline{\lambda} = \overline{w}(\sigma) = (d-2)\overline{\omega}_g + \overline{\omega}_{g-3}$.

Concerning Step 3, we have that $\overline{\lambda} - \overline{\alpha}_i \notin W_p(g,0,1)$ for $i \leq g-4$ by Lemma 4.4, and for $i = g-2$ or $g-1$ by the two lollipop argument. Thus Step 3 is complete, except if $d = 2$ (hence $p = 5$) in which case we also need to show that $\overline{\lambda} - \overline{\alpha}_g \notin W_5(g,0,1)$, which is easy and left to the reader.

This completes the proof in Case IV.

5. Further Comments

We elaborate on Remark 1.3. Let $\overline{C}_0$ denote the closure of the fundamental alcove. (See *e.g.* [H2, 3.5].) A dominant weight λ lies in $\overline{C}_0$ iff

$$\langle \lambda + \rho, \beta^\vee \rangle \leq p \ ,$$

where ρ is sum of the fundamental weights, and β is the highest short root (thus $\beta^\vee$ is the highest root of the dual root system). By [B, Planche II], we have

$$\beta^\vee = \alpha_1^\vee + 2\alpha_2^\vee + \ldots + 2\alpha_g^\vee \ .$$

Using $\langle \omega_i, \alpha_j^\vee \rangle = \delta_{ij}$, one can check that all the weights λ arising in Theorem 1.1 lie outside of $\overline{C}_0$ (*i.e.*, one has $\langle \lambda + \rho, \beta^\vee \rangle > p$) except for the weight $\lambda = (d-2)\omega_3$ in rank $g = 3$ (for which $\langle \lambda + \rho, \beta^\vee \rangle = p$). In fact, as soon as the rank $g \geq 5$, one uniformly has

$$\langle \lambda + \rho, \beta^\vee \rangle = p + 2g - 4$$

for all the weights in our list. Thus the distance of our weights to the fundamental alcove grows linearly with the rank g.

On the other hand, Theorem 1.1 also holds in rank $g = 2$ for those weights where it makes sense (*cf.* Remark 1.7(i)). It turns out that those weights λ in rank $g = 2$ all lie in $\overline{C}_0$. Hence the dimension of $L_p(\lambda)$ is given by the Weyl character formula, as it is a well-known consequence of the linkage principle that for dominant weights λ in $\overline{C}_0$, the simple module $L_p(\lambda)$ is isomorphic to the Weyl module $\Delta_p(\lambda)$ (see *e.g.* [H2, 3.6]). We have checked that indeed for $g = 2$ our dimension formulae (see Appendix B.2) agree with the Weyl character formula.

A further consistency check is possible in rank $g = 3$. In this case, although our weights (with one exception) lie outside of $\overline{C}_0$, the distance to $\overline{C}_0$ is not too big (one has $\langle \lambda + \rho, \beta^\vee \rangle \leq p + 2$) and one can use the Jantzen Sum Formula to compute the formal character of $L_p(\lambda)$. (See [J, II.8] and references therein. See also the summary in [H2, 3.9].) Here is the answer in the case $\varepsilon = 0$. We have

$$\lambda = \lambda_p(3,c,0) = c\,\omega_2 + (d-1-c)\omega_3 \ .$$

One finds that $L_p(\lambda)$ is equal to the Weyl module $\Delta_p(\lambda)$ if $c \in \{0,1\}$, but for $c \geq 2$ there is a short exact sequence

$$0 \to \Delta_p(\mu) \to \Delta_p(\lambda) \to L_p(\lambda) \to 0$$

where

$$\mu = \lambda - 2\omega_2 = (c-2)\omega_2 + (d-1-c)\omega_3 \ .$$

In particular $\dim L_p(\lambda)$ can be computed from the Weyl character formula as

$$\dim L_p(\lambda) = \dim \Delta_p(\lambda) - \dim \Delta_p(\mu)$$

and we have checked that our dimension formulae (see Appendix B.3) agree with this.

In rank $g \geq 4$, we have not attempted to compute $L_p(\lambda)$ with the Jantzen Sum Formula. Note that it is easy to see that $L_p(\lambda)$ can only very rarely be equal to the Weyl module $\Delta_p(\lambda)$ for a weight λ that arises in Theorem 1.1, because of the following observations (the first two of which imply the third).

- By [GM5, Corollary 2.10], $\dim L_p(\lambda_p(g, c, \varepsilon))$, with $g \geq 3$, c, and ε held fixed and viewed as a function of p is polynomial of degree $3g - 3$.
- By the Weyl character formula [FH, 24.20], $\dim \Delta_p(\lambda_p(g, c, \varepsilon))$, with $g \geq 1$, c, and ε held fixed and viewed as a function of p is polynomial of degree $g(g + 1)/2$.
- For each $g \geq 4$, c, and ε, there is a integer $N(g, c, \varepsilon)$ such that for all $p \geq N(g, c, \varepsilon)$, $\dim L_p(\lambda_p(g, c, \varepsilon)) < \dim \Delta_p(\lambda_p(g, c, \varepsilon))$.

Appendix A. Proof of Lemma 3.1

In this appendix, we assume some familiarity with Integral TQFT, in particular with the results of [GM2, §3] and [GM5]. See Remark 3.2 above for the correspondence between our present notations and those in [GM2] and [GM5]. It is shown in [GM5, Cor. 2.5] that every mapping class $f \in \Gamma_{g,1}$ is represented on $F_p(\Sigma_g(2c))$ by a matrix of the form

$$\begin{pmatrix} \star & 0 \\ \star & \star \end{pmatrix}$$

with respect to the direct sum decomposition (as vector spaces)

$$F_p(\Sigma_g(2c)) = F_p(g, c, 0) \oplus F_p(g, c, 1) \ .$$

(Here, the top left $\star$ stands for an element of $\mathrm{End}_{\mathbb{F}_p}(F_p(g, c, 0))$, and similarly for the two other $\star$s.) Lemma 3.1 is equivalent to the following

Lemma A.1. *Any f in the Torelli group $\mathcal{I}_{g,1}$ is represented by a matrix of the form*

$$\begin{pmatrix} 1 & 0 \\ \star & 1 \end{pmatrix}$$

To prove this, let us review how the coefficients of this matrix can be computed. Throughout this appendix we put $h = 1 - \zeta_p$. Recall that $\mathbb{Z}[\zeta_p]/(h) = \mathbb{F}_p$. We use the basis $\{\hat{b}_\sigma\}$ of $F_p(\Sigma_g(2c))$; it is the reduction modulo h of the orthogonal lollipop basis $\{\tilde{b}_\sigma\}$ of $\mathcal{S}_p(\Sigma_g(2c))$ constructed in [GM2]. The basis $\{\tilde{b}_\sigma\}$ is orthogonal with respect to the Hopf pairing $((\ ,\ ))$ defined in [GM2, §3], and we can therefore compute matrix coefficients by pairing with the dual basis $\{\tilde{b}^\star_\sigma\}$ satisfying

$$((\tilde{b}_\sigma, \tilde{b}^\star_{\sigma'})) = \delta_{\sigma,\sigma'} \ .$$

Here $\tilde{b}^\star_\sigma$ lies in the dual lattice $\mathcal{S}^\sharp_p(\Sigma_g(2c)) \subset \mathcal{S}_p(\Sigma_g(2c)) \otimes \mathbb{Q}(\zeta_p)$. We will use that

$$\tilde{b}^\star_\sigma \sim \tilde{b}^\sharp_\sigma \ , \tag{12}$$

where $\tilde{b}^\sharp_\sigma$ is defined in [GM2, Cor. 3.4] to be a certain power of h times $\tilde{b}_\sigma$, and $\sim$ means equality up to multiplication by a unit in $\mathbb{Z}[\zeta_p]$. (The power of h depends on σ.)

The Hopf pairing is a symmetric $\mathbb{Z}[\zeta_p]$-valued form on $\mathcal{S}_p(\Sigma_g(2c))$ which depends on a choice of Heegaard splitting of S^3. Given $x, y \in \mathcal{S}_p(\Sigma_g(2c))$, their Hopf pairing is computed skein-theoretically as follows. Think of x and y as represented by skein elements in the handlebody $\mathcal{H}_g$. Pick a complementary handlebody $\mathcal{H}'_g$ such that

$$\mathcal{H}_g \cup_{\Sigma_g} \mathcal{H}'_g = S^3 .$$

Then

$$((x, y)) = \langle x \cup r(y) \rangle \ , \tag{13}$$

where the right hand side of (13) is the Kauffman bracket evaluation (at a certain square root of ζ_p) of the skein element in S^3 obtained as the union of x in $\mathcal{H}_g$ and $r(y)$ in $\mathcal{H}'_g$ where r is a certain identification of $\mathcal{H}_g$ with $\mathcal{H}'_g$ (see [GM2, §3] for a more precise definition).

Given now a mapping class f, the (σ, σ') matrix coefficient of f acting on $\mathcal{S}_p(\Sigma_g(2c))$ is computed skein-theoretically as the evaluation

$$\langle \tilde{b}_\sigma \cup s \cup r(\tilde{b}^\star_{\sigma'}) \rangle \tag{14}$$

in

$$S^3 = \mathcal{H}_g \cup_{\Sigma_g} (\Sigma_g \times \mathrm{I}) \cup_{\Sigma_g} \mathcal{H}'_g \ ,$$

where s is a certain skein element in $\Sigma_g(2c) \times \mathrm{I}$ obtained from f in the usual way: there is a banded link L in $\Sigma_{g,1} \times \mathrm{I}$ so that surgery on L gives the mapping cylinder of f; one then obtains s by replacing each component of L by a certain skein element ω_p (see [BHMV, p. 898]) and placing the resulting skein element in $\Sigma_{g,1} \times \mathrm{I}$ into $\Sigma_g(2c) \times \mathrm{I}$ in the standard way. Here L and s are not uniquely determined by f, but it is shown in [BHMV] that this procedure is well-defined, and gives the correct answer. (More precisely, it gives the correct answer up to multiplication by a global projective factor which is a power of ζ_p. Here, we can safely ignore this projective ambiguity as we are eventually interested in the matrix of f modulo $h = 1 - \zeta_p$ only.)

We are now ready to prove Lemma A.1. The main idea is that if f lies in the Torelli group $\mathcal{I}_{g,1}$, then L and hence s are very special, because the mapping cylinder of f can be obtained by Y_1-surgery on $\Sigma_{g,1} \times \mathrm{I}$ [Ha, MM, HM]. The notion of Y_1-surgery goes back to Matveev [Mat] (who called it Borromean surgery), and then Goussarov [Gou] and Habiro [Ha] (who called it clasper surgery). We refer the reader to §5 of the survey [HM] for a good introduction to Y_1-surgery and also for more references to the original papers.

The result we need is stated in [HM, Prop. 5.5] and can be formulated as follows. There is a certain 6-component banded link Y in a genus 3 handlebody with the following property. For every $f \in \mathcal{I}_{g,1}$, there exists an embedding of a finite disjoint union of, say, n copies of the pair $(\mathcal{H}_3, Y)$ into $\Sigma_{g,1} \times \mathrm{I}$, giving rise to a $6n$-component banded link L in $\Sigma_{g,1} \times \mathrm{I}$ such that the mapping cylinder of f is obtained by surgery on this banded link L.

Cabling each component of Y by ω_p gives rise to a skein element $\mathcal{Y}_p$ in $\mathcal{H}_3$, and the skein element s appearing in our computation of matrix coefficients (see (14)) is obtained by placing n copies of $\mathcal{Y}_p$ into $\Sigma_g(2c) \times \mathrm{I}$.

We can view $\mathcal{Y}_p$ as an element of the free $\mathbb{Z}[\zeta_p]$-module $\mathcal{S}_p(\Sigma_3)$. The orthogonal lollipop basis $\{\tilde{b}_\sigma\}$ of $\mathcal{S}_p(\Sigma_3)$ is indexed by colorings of the form $\sigma = (a_1, a_2, a_3, b_1, b_2, b_3)$. As before, let σ_0 denote the zero coloring. The following lemma is the key to proving Lemma A.1, as it shows that all but two coefficients of $\mathcal{Y}_p$ in the $\{\tilde{b}_\sigma\}$ basis are divisible by h.

Lemma A.2. $\mathcal{Y}_p - \tilde{b}_{\sigma_0} = \alpha\, \tilde{b}_{(1,1,1,0,0,0)} \pmod h$ *for some* $\alpha \in \mathbb{Z}[\zeta_p]$.

Proof of Lemma A.1 from Lemma A.2. We have that $\tilde{b}_{\sigma_0}$ is represented by the empty link and $\tilde{b}_{(1,1,1,0,0,0)}$ is h^{-1} times the elementary tripod (see [GM1, Fig. 2 on p. 824]). Thus

$$s = \sum_{k=0}^{n} h^{-k} s_k \ ,$$

where s_k is the disjoint union of k elementary tripods embedded in $\Sigma_g(2c) \times \mathrm{I}$. The contribution of $h^{-k} s_k$ to the (σ, σ') matrix coefficient of f is

$$h^{-k} \langle \tilde{b}_\sigma \cup s_k \cup r(\tilde{b}^\star_{\sigma'}) \rangle \ . \tag{15}$$

For $k = 0$ this is $\delta_{\sigma,\sigma'}$, as s_0 is the empty link. For $k > 0$, a straightforward application of the lollipop lemma [GM1, Thm. 7.1] shows that if σ and σ' have the same parity, then (15) is divisible by h (since a tripod has 3 elementary lollipops). This proves Lemma A.1. □

Proof of Lemma A.2. The 6-component banded link Y in $\mathcal{H}_3$ can be described as follows (see [HM, Fig. 5]). We can number the components of Y as $Y_1, Y_2, Y_3, Y'_1, Y'_2, Y'_3$ such that the following holds. The components (Y_1, Y_2, Y_3) lie in a ball $B \subset \mathcal{H}_3$ and form zero-framed Borromean rings. For $i = 1, 2, 3$, the component Y'_i is a zero-framed unknot going once around the ith 'hole' of $\mathcal{H}_3$; moreover Y'_i is linked exactly once with Y_i, and unlinked with the two other Y_js.

Recall that $\mathcal{Y}_p$ is obtained by cabling each of these 6 components by ω_p. For the lemma, we need to compute the coefficients of the basis vectors $\tilde{b}_{(a_1,a_2,a_3,b_1,b_2,b_3)}$ in $\mathcal{Y}_p$. (In fact, except for the zero coloring, we only need these coefficients modulo h.) Such a coefficient is given by the Hopf pairing

$$((\mathcal{Y}_p, \tilde{b}^\star_{(a_1,a_2,a_3,b_1,b_2,b_3)})) \ .$$

As explained above, this is computed as the Kauffman bracket of a certain skein element in S^3. Using now the handle slide property of ω_p (which is at the basis of the skein-theoretic construction of TQFT [BHMV]), we can compute this by performing surgery on Y, which gives back S^3, but transforms the standard embedding of $\mathcal{H}'_3$ in S^3 into an embedding φ of $\mathcal{H}'_3$ in S^3 where the three handles of $\varphi(\mathcal{H}'_3)$ are linked as in the Borromean rings. Thus the coefficient of $\tilde{b}_{(a_1,a_2,a_3,b_1,b_2,b_3)}$ in $\mathcal{Y}_p$ is the Kauffman bracket evaluation

$$\langle \varphi(r(\tilde{b}^\star_{(a_1,a_2,a_3,b_1,b_2,b_3)})) \rangle \ . \tag{16}$$

For the zero coloring, the basis vector $\tilde{b}^\star_{\sigma_0}$ is represented by the empty link, and so (16) evaluates to 1, as asserted. The following Lemma A.3 shows that (16) is divisible by h as soon as $\max(b_i) > 0$ or $\max(a_i) > 1$. Thus it only remains to compute (16) for the colorings with $\max(a_i) = 1$ and all $b_j = 0$. Assume all $b_j = 0$. For $a_1 = a_2 = a_3 = 1$, there is nothing to prove, while if one of the a_i is zero, then

(16) evaluates to zero (as the two remaining handles are unlinked). This proves the lemma. □

For $r \in \mathbb{Q}$, we define its floor $\lfloor r \rfloor$ to be the largest integer $\leq r$, and its roof $\lceil r \rceil$ to be the smallest integer $\geq r$.

Lemma A.3. *We have that (16) is divisible by*

$$h^{\lfloor (E_1+E_2-E_3)/2 \rfloor}$$

where $E_i = a_i + 2b_i$ $(i = 1, 2, 3)$, and w. l. o. g. we may assume $E_1 \geq E_2 \geq E_3$.

Proof. Put

$$B_{(a_1,a_2,a_3,b_1,b_2,b_3)} = h^{\lceil (E_1+E_2+E_3)/2 \rceil}\, \tilde{b}^{\star}_{(a_1,a_2,a_3,b_1,b_2,b_3)} \ .$$

Then $B_{(a_1,a_2,a_3,b_1,b_2,b_3)}$ is represented by a linear combination of skein elements in $\mathcal{H}_3$ with coefficients in $\mathbb{Z}[\zeta_p]$. (This follows from (12) and the definition of $\{\tilde{b}^{\sharp}_{\sigma}\}$ in [GM2, §3].) Below, we say that such a skein element has no denominators. Let β denote the result of evaluating (16) with $B_{(a_1,a_2,a_3,b_1,b_2,b_3)}$ in place of $\tilde{b}^{\star}_{(a_1,a_2,a_3,b_1,b_2,b_3)}$. Since the three lollipops are linked as in the Borromean rings, we can pull the first two of them apart and consider the third as just some skein element in the complement of the first two. In other words, by cutting $B_{(a_1,a_2,a_3,b_1,b_2,b_3)}$ at the midpoint of the edge labelled $2a_3$, we can write β as the genus two Hopf pairing of two skein elements, say $\mathfrak{s}$ and $\mathfrak{s}'$, in a genus 2 handlebody with one banded point labelled $2a_3$. Moreover, one of these two skein elements, say $\mathfrak{s}$ (namely the one containing the first two lollipops), is a power of h times the basis element $\tilde{b}^{\star}_{(a_1,a_2,b_1,b_2,2a_3)}$ of the orthogonal lollipop basis of $\mathcal{S}_p(\Sigma_2(2a_3))$. Rewriting $\mathfrak{s}'$ also in this basis and using the formulae in [GM2, §3] for the Hopf pairing in the orthogonal lollipop basis, one finds that β is divisible by $h^{E_1+E_2}$. (Here it is important to observe that both $\mathfrak{s}$ and $\mathfrak{s}'$ are skein elements without denominators.) Thus (16) is divisible by

$$h^{-\lceil (E_1+E_2+E_3)/2 \rceil + E_1 + E_2} = h^{\lfloor (E_1+E_2-E_3)/2 \rfloor} \ .$$

This completes the proof. □

Remark A.4. Other applications of Lemma A.3 include a skein-theoretic construction of Ohtsuki's power series invariant for integral homology 3-spheres, and a Torelli group representation inducing this invariant [M].

Appendix B. Some polynomial formulae for dimensions

In [GM5, Prop. 7.7, Prop. 7.8] we gave residue formulae for $D_g^{(2c)}(p)$ and $\delta_g^{(2c)}(p)$ valid for $g \geq 1$. Using Equation (1), one can then express $\dim L_p(\lambda)$, for the λ that arise in Theorem 1.1, for specified g as polynomials in p and c using mathematical software. Below we write down these polynomials in rank $g = 2$, 3, and 4. These formulae hold for $p \geq 5$ and $1 \leq c \leq d-1$ where $d = (p-1)/2$. The first polynomial in each rank is the second polynomial with c set to zero. Similarly the fourth polynomial in each rank (except rank 2) is the third polynomial with c set to zero. As noted in Section 5, our formulae in rank $g = 2$ and also the first one in rank $g = 3$ agree with Weyl's character formula. The second formula in rank $g = 3$ agrees with Weyl's character formula for $c = 1$, but not for $c > 1$.

B.2. **Rank** $g = 2$.

$$\dim L_p\big((d-1)\omega_2\big) = \frac{1}{24}(p-1)p(p+1)$$

$$\dim L_p\big((d-c-1)\omega_2 + c\,\omega_1\big) = \frac{1}{24}(c+1)(p+1)(p-2c-1)(p-c)$$

$$\dim L_p\big((d-c-1)\omega_2 + (c-1)\omega_1\big) = \frac{1}{24}c(p-1)(p-2c-1)(p-c-1)$$

B.3. **Rank** $g = 3$.

$$\dim L_p\big((d-1)\omega_3\big) = \frac{1}{2880}(p-1)p(p+1)^2(p+2)(p+3)$$

$$\begin{aligned}\dim L_p\big((d-c-1)\omega_3 + c\,\omega_2\big) = \frac{1}{2880}(p-2c-1)\Big(&p^5(2c+1) + p^4(4c^2+4c+7)+\\ &p^3(-12c^3-18c^2+28c+17) + p^2(6c^4+12c^3-22c^2-28c+17)+\\ &6p(-2c^3-3c^2+c+1) + 6c(c^3+2c^2-c-2)\Big)\end{aligned}$$

$$\begin{aligned}\dim L_p\big((d-c-1)\omega_3 + (c-1)\omega_2 + \omega_1\big) = \frac{1}{2880}(p-1)(p+1)(p-2c-1)\Big(&p^3(2c+1)+\\ &p^2(4c^2+4c-5) + 6p(-2c^3-3c^2+c+1) + 6c(c^3+2c^2-c-2)\Big)\end{aligned}$$

$$\dim L_p\big((d-2)\omega_3\big) = \frac{1}{2880}(p-3)(p-2)(p-1)^2p(p+1)$$

B.4. **Rank** $g = 4$.

$$\dim L_p\big((d-1)\omega_4\big) = \frac{1}{120960}(p-1)p(p+1)\left(p^6+37p^4+142p^2+36\right)$$

$$\begin{aligned}\dim L_p\big((d-c-1)\omega_4 + c\,\omega_3\big) = \frac{1}{120960}(p+1)(p-2c-1)\Big(&p^7(2c+1) + 2p^6c(2c+1)+\\ &p^5(-6c^3-13c^2+18c+37) + 2p^4c(-6c^3-9c^2+22c+38)+\\ &p^3(18c^5+57c^4-84c^3-266c^2+22c+142) - 6p^2c(c^5+6c^4+c^3-28c^2-12c+24)+\\ &3p(2c^6+12c^5+5c^4-50c^3-37c^2+32c+12) - 6c(c^5+3c^4-5c^3-15c^2+4c+12)\Big)\end{aligned}$$

$$\begin{aligned}\dim L_p\big((d-c-1)\omega_4 + (c-1)\omega_3 + \omega_2\big) = \frac{1}{120960}(p-1)(p-2c-1)\Big(&p^7(2c+1)+\\ &p^6(4c^2+6c+2) + p^5(-6c^3-5c^2+26c-12) - 2p^4(6c^4+15c^3-13c^2-9c+13)+\\ &p^3(18c^5+33c^4-132c^3-148c^2+164c+23) - 6p^2(c^6-14c^4-8c^3+33c^2+16c-12)+\\ &p(-6c^6+75c^4+30c^3-159c^2-48c+36) - 6c(c^5+3c^4-5c^3-15c^2+4c+12)\Big)\end{aligned}$$

$$\dim L_p\big((d-2)\omega_4 + \omega_1\big) = \frac{1}{120960}(p-3)(p-2)(p-1)^2p(p+1)^2(p+2)(p+3)$$

References

[AJS] H. H. Andersen, J. C. Jantzen, W. Soergel. Representations of quantum groups at a p-th root of unity and of semisimple groups in characteristic p: independence of p. *Astérisque* **220** (1994)

[B] N. Bourbaki. Groupes et Algèbres de Lie. Chapters 4-6, Hermann, Paris, 1968. 2nd ed. Masson, Paris 1981.

[BHMV] C. Blanchet, N. Habegger, G. Masbaum, P. Vogel. Topological quantum field theories derived from the Kauffman bracket, *Topology* **34** (1995), 883-927

[CaLu] R. W. Carter, G. Lusztig. Modular representations of finite groups of Lie typ. *Proc. London Math. Soc.* (3) 32 (1976), no. 2, 347-384

[ChLe] Q. Chen, T. T. Q. Le. Almost integral TQFTs from simple Lie algebras. *Algebr. Geom. Topol.* **5** (2005), 1291–1314.

[F] S. Foulle. Characters of the irreducible representations with fundamental highest weight for the symplectic group in characteristic p. `arXiv:math/0512312`

[FH] W. Fulton, J. Harris. *Representation theory. A first course.* Graduate Texts in Mathematics, 129. Readings in Mathematics. Springer-Verlag, New York, 1991.

[GL] S. Garoufalidis, J. Levine, Finite type 3-manifold invariants, the mapping class group and blinks. J. Diff. Geom. 47 (1997), no. 2, 257 - 320.

[G1] P. M. Gilmer. Integrality for TQFTs, *Duke Math J*, **125** (2004), no. 2, 389–413

[G2] P. M. Gilmer. Integral TQFT and Modular representations (joint with Gregor Masbaum). *Oberwolfach Reports* No 30, 2015, pp.1713

[GM1] P. M. Gilmer, G. Masbaum. Integral lattices in TQFT. *Ann. Scient. Ec. Norm. Sup.* 40, (2007), 815–844

[GM2] P. M. Gilmer, G. Masbaum. Integral TQFT for a one-holed torus, Pac. J. Math. 252 No 1 (2011), 93–112.

[GM3] P. M. Gilmer, G. Masbaum. Maslov index, Lagrangians, Mapping Class Groups and TQFT, Forum Mathematicum Volume 25, Issue 5 (2011) 1067-1106

[GM4] P. M. Gilmer, G. Masbaum. Dimension formulas for some modular representations of the symplectic group in the natural characteristic. J. Pure Appl. Algebra 217 (2013), no. 1, 82 - 86.

[GM5] P. M. Gilmer, G. Masbaum. Irreducible factors of modular representations of mapping class groups arising in Integral TQFT, Quantum Topology, 5, Issue 2, 2014, pp. 225-258

[Go] R. Gow. Construction of $p-1$ irreducible modules with fundamental highest weight for the symplectic group in characteristic p, J. Lond. Math. Soc. 58 (1998) 619632.

[Gou] M. N. Goussarov. Variations of knotted graphs. The geometric technique of n- equivalence. In Russian: Algebra i Analiz 12 (2000), no. 4, 79 - 125. English translation: St. Petersburg Math. J. 12 (2001), no. 4, 569 - 604.

[Ha] K. Habiro. Claspers and finite type invariants of links. *Geom. Topol.* **4** (2000), 183.

[HM] K. Habiro, G. Massuyeau. From mapping class groups to monoids of homology cobordisms: a survey. Handbook of Teichmüller theory. Volume III, 465 - 529, IRMA Lect. Math. Theor. Phys., 17, Eur. Math. Soc., Zürich, 2012. `arXiv.1003.2512`

[H1] J. E. Humphreys. Linear algebraic groups. Graduate Texts in Mathematics, No. 21. Springer-Verlag, New York-Heidelberg, 1975.

[H2] J. E. Humphreys. Modular Representations of Finite Groups of Lie Type, London Math. Soc. Lecture Note Series, 326, Cambridge Univ. Press, (2006).

[J] J. C. Jantzen. Representations of Algebraic Groups (2nd ed.) Math. Surveys Monographs, Vol. **107**. Amer. Math. Soc. Providence RI (2003)

[M] G. Masbaum. Skein theory and the Ohtsuki series. (In preparation.)

[MM] G. Massuyeau, J.-B. Meilhan. Characterization of Y 2 -equivalence for homology cylinders. *J. Knot Theory Ramifications* 12 (2003), 493 - 522.

[Mat] S. V. Matveev. Generalized surgeries of three-dimensional manifolds and representations of homology spheres. In Russian: Mat. Zametki 42 (1987), no. 2, 268 - 278, 345. English translation: Math. Notes 42 (1987), no. 1-2, 651 - 656.

[Me] J. Mennicke. Zur Theorie der Siegelschen Modulgruppe. *Math. Ann.* **159** (1965) 115-129.

[P] A. A. Premet. Weights of Infinitesimally Irreducible Representations of Chevalley Groups Over a Field of Prime Characteristic. *Mat. Sb.* **133** (1987) 167-183; transl. *Math. USSR-Sb.* **61** (1988), 167-183

[PS] A. A. Premet, I. D. Suprunenko. The Weyl mdules and irreducible representations of the symplectic group with fundamental highest weights. *Comm. Algebra* **11** (1983) 1309-1342

[W] G. Williamson. Schubert calculus and torsion explosion. To appear in *Journal of the AMS.* arXiv:1309.5055

Department of Mathematics, Louisiana State University, Baton Rouge, LA 70803, USA

E-mail address: gilmer@math.lsu.edu

URL: www.math.lsu.edu/~gilmer/

Institut de Mathématiques de Jussieu (UMR 7586 du CNRS), Case 247, 4 pl. Jussieu, 75252 Paris Cedex 5, FRANCE

E-mail address: gregor.masbaum@imj-prg.fr

URL: webusers.imj-prg.fr/~gregor.masbaum