Journal of Algebra 323 (2010) 397–418

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Monoidal Morita invariants for finite group algebras

Kenichi Shimizu [1]

Institute of Mathematics, University of Tsukuba, Tsukuba, Ibaraki 305-8571, Japan

ARTICLE INFO

Article history:
Received 11 May 2009
Available online 8 October 2009
Communicated by Nicolás Andruskiewitsch

Keywords:
Hopf algebras
Monoidal categories
Monoidal Morita theory

ABSTRACT

Two Hopf algebras are called monoidally Morita equivalent if module categories over them are equivalent as linear monoidal categories. We introduce monoidal Morita invariants for finite-dimensional Hopf algebras based on certain braid group representations arising from the Drinfeld double construction. As an application, we show, for any integer n, the number of elements of order n is a monoidal Morita invariant for finite group algebras. We also describe relations between our construction and invariants of closed 3-manifolds due to Reshetikhin and Turaev.

1. Introduction

Let H be a Hopf algebra over a field k, for example, a group algebra. As is well known, the category of H-modules, denoted by $\mathbf{Mod}(H)$, is a k-linear monoidal category. We say that two Hopf algebras H and L are *monoidally Morita equivalent* if $\mathbf{Mod}(H)$ and $\mathbf{Mod}(L)$ are equivalent as k-linear monoidal categories. In this paper, we introduce monoidal Morita invariants of finite-dimensional Hopf algebras and apply them to finite group algebras.

Following Etingof and Gelaki [1], we say that two finite groups G and G' are *k-isocategorical* if kG and kG' are monoidally Morita equivalent. In the same paper, they classify all groups $\mathbb{C}$-isocategorical to a given finite group in group-theoretical terms. Following [1], we say that a finite group G is *categorically rigid over k* if any group k-isocategorical to G is isomorphic to G. As a direct consequence of their classification, G is categorically rigid over $\mathbb{C}$ if G does not admit a normal abelian subgroup A of order 2^{2m} [1, Corollary 1.4]. In general, it is difficult to know when two finite groups are isocategorical even if we use the classification result. In this paper we show the following criterion, applying our results to finite group algebras.

E-mail address: shimizu@math.tsukuba.ac.jp.

[1] Research Fellow of the Japan Society for the Promotion of Science.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2009.08.021

Theorem 1.1. *Let k be a field. If two finite groups G and G' are k-isocategorical, then for each positive integer n, the number of elements of order n in G is equal to the number of elements of order n in G'.*

Monoidal categories arise not only from algebra but also from low-dimensional topology such as the theory of knots and braids. Our construction is based on certain braid group representations arising from the Drinfeld double $\mathcal{D}(H)$ of a finite-dimensional Hopf algebra H. Considering $\mathcal{D}(H)$ itself as a left $\mathcal{D}(H)$-module via the left multiplication, we have a series of canonical representations

$$\rho_n^{\mathcal{D}(H)} : B_n \to \mathrm{Aut}_{\mathcal{D}(H)}\big(\mathcal{D}(H)^{\otimes n}\big) \quad (n = 2, 3, \ldots)$$

of braid groups B_n. We show a monoidal Morita invariant $\tau(b; H)$ is given by $\tau(b; H) = \mathrm{Tr}(\rho_n^{\mathcal{D}(H)}(b))$, $b \in B_n$. Theorem 1.1 is actually an application of these invariants associated with certain braids; see Section 4.

When H is a finite-dimensional semisimple Hopf algebra over an algebraically closed field of characteristic zero, we can relate our construction to the Reshetikhin–Turaev invariant [2] of closed 3-manifolds. This relation gives rise to the following theorem. For groups X and Y, denote by $\mathrm{Hom}(X, Y)$ the set of group homomorphisms from X to Y.

Theorem 1.2. *Let k be a field. If finite groups G and G' are k-isocategorical, then for any oriented connected closed 3-manifold M, we have*

$$\#\,\mathrm{Hom}\big(\pi_1(M), G\big) = \#\,\mathrm{Hom}\big(\pi_1(M), G'\big)$$

where $\pi_1(M)$ is the fundamental group of M.

This paper is organized as follows. In Section 2, we introduce the notion of monoidal Morita invariance between Hopf algebras. We review Schauenburg's results [3] and prove some lemmas for latter sections. In Section 3, we define monoidal Morita invariants associated with braids and introduce some basic properties of them. In Section 4, we apply our invariants to finite group algebras and prove Theorem 1.1. In Section 5, we discuss relations between our invariants and the construction of invariants of closed 3-manifolds due to Reshetikhin and Turaev. Theorem 1.2 will be proved in this section. Section 6 is devoted to further examples and applications of our invariants.

In Appendix A, we argue similarity of permutation matrices and prove that two permutation matrices of same size are similar if and only if they are conjugate as permutations (Theorem A.1). This theorem is used in Section 4 as a part of the proof of Theorem 1.1.

Throughout this paper, the base field is denoted by k. Unless otherwise noted, vector spaces, algebras, coalgebras, etc. are over k. For vector spaces V and W, $V \otimes W$ means $V \otimes_k W$. Functors between k-linear categories are always assumed to be k-linear. We use [5] as a main reference for general theory of Hopf algebras. The comultiplication and counit of a bialgebra H are denoted by $\Delta : H \to H \otimes H$ and $\varepsilon : H \to k$, respectively. The antipode of a Hopf algebra is denoted by S. We use Sweedler's sigma notation

$$\Delta(x) = \sum x_{(1)} \otimes x_{(2)}$$

to denote the comultiplication of an element x in a coalgebra.

For an algebra A, we denote by A^{op} the opposite algebra. Similarly, for a coalgebra C, we denote by C^{cop} a coalgebra with the same underlying space with opposite comultiplication Δ^{cop} given by $\Delta^{\mathrm{cop}}(c) = \sum c_{(2)} \otimes c_{(1)}$ for all $c \in C$ (the opposite coalgebra). For a bialgebra H, bialgebras H^{op} and H^{cop} are defined in an obvious way.

2. Preliminaries

2.1. Bialgebras and monoidal categories

A *monoidal category* (or *tensor category*) is a category $\mathcal{C}$ equipped with a bifunctor $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ and an object $\mathbf{1} \in \mathcal{C}$ satisfying certain associativity and unit constraints. The bifunctor $\otimes$ is called the *tensor product* and the object $\mathbf{1}$ is called the unit object. We refer the reader to Chapter XIII of Kassel [6] for formal definitions of monoidal categories and monoidal functors.

The category of vector spaces, denoted by $\mathbf{Vec}(k)$, is a typical example of a k-linear monoidal category. A monoidal category is called *strict* if its associativity and unit isomorphisms are all identities. In this paper, we deal with mainly k-linear monoidal categories whose associativity and unit isomorphisms are "trivial" like $\mathbf{Vec}(k)$. Hence, although such categories are not strict, we treat them as if they were strict. This is valid since every monoidal category is equivalent to a strict one (see, e.g., [6, XI.5]).

Let B be a bialgebra. Given left B-modules V and W, the tensor product $V \otimes W$ is a left B-module by

$$x \cdot (v \otimes w) = \sum x_{(1)} v \otimes x_{(2)} w$$

for all $x \in B$, $v \in V$ and $w \in W$. The category of left B-modules, denoted by $\mathbf{Mod}(B)$, is a k-linear monoidal category with this tensor product. The unit object of $\mathbf{Mod}(B)$ is the trivial B-module $\mathbf{1} = k$ given by $x \cdot 1 = \varepsilon(x)1$ for all $x \in B$. The following proposition describes relations between monoidal categories $\mathbf{Mod}(B)$, $\mathbf{Mod}(B^{\mathrm{cop}})$ and $\mathbf{Mod}(B^{\mathrm{op}})$. For a monoidal category $\mathcal{C}$, we denote by $\mathcal{C}^{\mathrm{rev}}$ the monoidal category with the underlying category $\mathcal{C}$ and the reverse tensor product $\otimes^{\mathrm{rev}}$ given by $X \otimes^{\mathrm{rev}} Y = Y \otimes X$ for all $X, Y \in \mathcal{C}$.

Proposition 2.1. *Let B be a bialgebra.*

(a) $\mathbf{Mod}(B^{\mathrm{cop}})$ *is monoidally equivalent to* $\mathbf{Mod}(B)^{\mathrm{rev}}$.
(b) $\mathbf{Mod}(B^{\mathrm{op}})$ *is monoidally equivalent to* $\mathbf{Mod}(B)^{\mathrm{rev}}$ *if B has a bijective antipode.*

Proof. (a) The identity functor together with the monoidal structures

$$T_{V,W} : V \otimes^{\mathrm{rev}} W = W \otimes V \to V \otimes W, \quad T_{V,W}(w \otimes v) = v \otimes w$$

gives a monoidal equivalence between $\mathbf{Mod}(B)$ and $\mathbf{Mod}(B^{\mathrm{cop}})$.

(b) Under this assumption, the antipode gives an isomorphism $B^{\mathrm{op}} \cong B^{\mathrm{cop}}$ of Hopf algebras. This induces a monoidal equivalence between $\mathbf{Mod}(B^{\mathrm{cop}})$ and $\mathbf{Mod}(B^{\mathrm{op}})$. □

We use the sigma notation such as $\rho(v) = \sum v_{(0)} \otimes v_{(1)}$ for right comodule structures. Given right B-comodules V and W, the tensor product $V \otimes W$ is also a right B-comodule with structure map $\rho_{V\otimes W} : V \otimes W \to V \otimes W \otimes B$ given by

$$\rho_{V\otimes W}(v \otimes w) = \sum v_{(0)} \otimes w_{(0)} \otimes v_{(1)} w_{(1)}.$$

The category of right B-comodules is a monoidal category with this tensor product. We denote this monoidal category by $\mathbf{Com}(B)$. We can prove the following proposition in a similar way as Proposition 2.1.

Proposition 2.2. *Let B be a bialgebra.*

(a) $\mathbf{Com}(B^{\mathrm{op}})$ *is monoidally equivalent to* $\mathbf{Com}(B)^{\mathrm{rev}}$.
(b) $\mathbf{Com}(B^{\mathrm{cop}})$ *is monoidally equivalent to* $\mathbf{Com}(B)^{\mathrm{rev}}$ *if B has a bijective antipode.*

2.2. Monoidal Morita theory

We introduce the following definition.

Definition 2.3. Two Hopf algebras H and L are *monoidally Morita equivalent* if $\mathbf{Mod}(H)$ and $\mathbf{Mod}(L)$ are equivalent as (k-linear) monoidal categories.

Although we are interested in modules over Hopf algebras, for a while, we refer to Schauenburg's results [3] that deal with comodules over Hopf algebras. Let C be a coalgebra. The *cotensor product* $V\Box_C W$ of a right C-comodule V and a left C-comodule W is defined to be the kernel of

$$\rho_V \otimes \mathrm{id}_W - \mathrm{id}_V \otimes \lambda_W : V \otimes W \to V \otimes C \otimes W$$

where ρ_V and λ_W are the structure maps of V and W, respectively. Let D be another coalgebra. If, moreover, W is a (C, D)-bicomodule, the cotensor product $V \Box_C W$ is naturally a right D-comodule.

Let H be a Hopf algebra. For an H-comodule M, we let

$$M^{\mathrm{co}\,H} = \{m \in M \mid \rho_M(m) = m \otimes 1\}$$

denote the space of H-coinvariants. A *right H-Galois object* is a right H-comodule algebra $A \neq 0$ such that $A^{\mathrm{co}\,H} = k$ and the linear map $A \otimes A \to A \otimes H$ given by $x \otimes y \mapsto \sum xy_{(0)} \otimes y_{(1)}$ is bijective. A *left H-Galois object* is defined by replacing "right" with "left". For another Hopf algebra L, an (H, L)-bi-Galois object [3, Definition 3.4] is a left H- and right L-Galois object such that the two comodule structures make it an (H, L)-bicomodule. If A is an (H, L)-bi-Galois object, the cotensor product functor

$$F_A : \mathbf{Com}(H) \to \mathbf{Com}(L), \quad F_A(V) = V \Box_H A$$

gives a monoidal equivalence together with the monoidal structures

$$J_{V,W} : (V \Box_H A) \otimes (W \Box_H A) \to (V \otimes W) \Box_H A,$$
$$\Big(\sum v_i \otimes x_i\Big) \otimes \Big(\sum w_j \otimes y_j\Big) \mapsto \sum v_i \otimes w_j \otimes x_i y_j$$

and $\varphi : k \to k \Box_H A$, $a \mapsto a \otimes 1$.

Theorem 2.4. *(See Schauenburg [3, Corollary 5.7].) The above correspondence $A \mapsto (F_A, J, \varphi)$ gives a bijection between isomorphism classes of (H, L)-bi-Galois objects and isomorphism classes of monoidal equivalences $\mathbf{Com}(H) \to \mathbf{Com}(L)$.*

A right H-Galois object A is said to be *cleft* if there exists a convolution invertible H-colinear map $H \to A$ where we consider H as a right H-comodule via the comultiplication. Note that A is cleft if and only if A is isomorphic to H as a right H-comodule [7, Theorem 9]. The notion of *cleft left H-Galois objects* is defined similarly. If H is finite-dimensional, all left H-Galois objects and all right H-Galois objects are cleft. In the following lemma, we denote by U_H the forgetful functor $\mathbf{Com}(H) \to \mathbf{Vec}(k)$.

Lemma 2.5. *Let H and L be finite-dimensional Hopf algebras. For any monoidal equivalence $F : \mathbf{Com}(H) \to \mathbf{Com}(L)$, the followings hold.*

(a) *$F(H)$ is isomorphic to L in $\mathbf{Com}(L)$.*
(b) *$U_L \circ F$ is isomorphic to U_H as a k-linear functor.*

Proof. By Theorem 2.4, there exists an (H, L)-bi-Galois object A such that F is isomorphic to $F_A = (-)\square_H A$. Since H and L are finite-dimensional, A is cleft. In particular, A is isomorphic to H as a left H-comodule and is isomorphic to L as a right L-comodule.

(a) We have $F(H) \cong H\square_H A \cong A \cong L$ as right L-comodules.

(b) It can be proved in a similar way as in (a). □

We now return to modules over Hopf algebras. Let H be a finite-dimensional Hopf algebra. Recall that we can identify $\mathbf{Mod}(H)$ with $\mathbf{Com}(H^*)$ where H^* is the dual Hopf algebra of H. In particular, we consider a right H^*-comodule V as a left H-module by

$$x \cdot v = \sum v_{(0)} \langle v_{(1)}, x \rangle$$

for all $x \in H$ and $v \in V$. In the following lemma, we denote by $U'_H : \mathbf{Mod}(H) \to \mathbf{Vec}(k)$ the forgetful functor.

Lemma 2.6. *Let H and L be finite-dimensional Hopf algebras. For any monoidal equivalence $F : \mathbf{Mod}(H) \to \mathbf{Mod}(L)$, the followings hold.*

(a) *$F(H)$ is isomorphic to L in $\mathbf{Mod}(L)$.*
(b) *$U'_L \circ F$ is isomorphic to U'_H as a k-linear functor.*

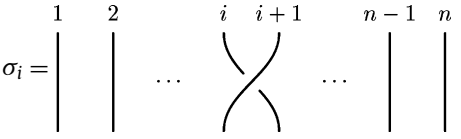
Proof. (a) Let $F : \mathbf{Mod}(H) \to \mathbf{Mod}(L)$ be an equivalence of monoidal categories. If we identify $\mathbf{Mod}(H)$ and $\mathbf{Mod}(L)$ with $\mathbf{Com}(H^*)$ and $\mathbf{Com}(L^*)$ respectively, we have an equivalence $F : \mathbf{Com}(H^*) \to \mathbf{Com}(L^*)$ of monoidal categories. By Lemma 2.5(a), $F(H^*) \cong L^*$ in $\mathbf{Com}(L^*)$. Since $H^* \in \mathbf{Com}(H^*)$ is isomorphic to H as a left H-module (see [5, Chapter 5]), we have $F(H) \cong F(H^*) \cong L^* \cong L$ as left L-modules.

(b) This is obvious by Lemma 2.5(b). □

2.3. Braiding

A *braiding* in a (strict) monoidal category $\mathcal{C}$ is a natural isomorphism $c_{X,Y} : X \otimes Y \to Y \otimes X$ ($X, Y \in \mathcal{C}$) satisfying equations $c_{X\otimes Y,Z} = (c_{X,Z} \otimes \mathrm{id}_Y)(\mathrm{id}_X \otimes c_{Y,Z})$ and $c_{X,Y\otimes Z} = (\mathrm{id}_Y \otimes c_{X,Z})(c_{X,Y} \otimes \mathrm{id}_Z)$ for $X, Y, Z \in \mathcal{C}$. A *braided monoidal category* (or *braided tensor category*) is a monoidal category equipped with a braiding (see [6, Chapter XIII]).

Let $\mathcal{C}$ be a braided monoidal category with braiding c. Each object of $\mathcal{C}$ yields a series of representations of braid groups. We denote by B_n ($n \geqslant 2$) the braid group on n strands. As is well known, B_n is generated by basic braids

$\sigma_i =$ 

$(i = 1, 2, \ldots, n-1)$

with defining relations

$$\sigma_i\sigma_j = \sigma_j\sigma_i \quad \big(\text{if } |i-j| > 1\big),$$
$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \quad (i = 1, 2, \ldots, n-2).$$

Fix an object $X \in \mathcal{C}$. Then the morphism $\sigma = c_{X,X}$ is a solution of the Yang–Baxter equation $(\sigma \otimes \mathrm{id}_X)(\mathrm{id}_X \otimes \sigma)(\sigma \otimes \mathrm{id}_X) = (\mathrm{id}_X \otimes \sigma)(\sigma \otimes \mathrm{id}_X)(\mathrm{id}_X \otimes \sigma)$ in $\mathrm{Aut}_{\mathcal{C}}(X^{\otimes 3})$, and thus we have a series of representations

$$\rho_n^X : B_n \to \mathrm{Aut}_{\mathcal{C}}\big(X^{\otimes n}\big) \quad (n = 2, 3, \ldots)$$

given by

$$\rho_n^X(\sigma_i) = \underbrace{\mathrm{id}_X \otimes \cdots \otimes \mathrm{id}_X}_{i-1} \otimes c_{X,X} \otimes \underbrace{\mathrm{id}_X \otimes \cdots \otimes \mathrm{id}_X}_{n-i-1}.$$

Remark 2.7. Let $f : X \to Y$ be a morphism in $\mathcal{C}$. Since the braiding is natural, the diagram

$$\begin{array}{ccc} X^{\otimes n} & \xrightarrow{\rho_n^X(b)} & X^{\otimes n} \\ {\scriptstyle f\otimes\cdots\otimes f}\downarrow & & \downarrow{\scriptstyle f\otimes\cdots\otimes f} \\ Y^{\otimes n} & \xrightarrow[\rho_n^Y(b)]{} & Y^{\otimes n} \end{array}$$

commutes for all $b \in B_n$. In particular, braid group representations ρ_n^X and ρ_n^Y are equivalent if X and Y are isomorphic.

Remark 2.8. Let $\mathcal{D}$ be another braided monoidal category and $F : \mathcal{C} \to \mathcal{D}$ be a braided monoidal functor. If we fix an object $X \in \mathcal{C}$, we have representations

$$\rho_n' : B_n \to \mathrm{Aut}_{\mathcal{D}}\big(F(X)^{\otimes n}\big), \quad \rho_n'(b) = \rho_n^{F(X)}(b)$$

and

$$\rho_n'' : B_n \to \mathrm{Aut}_{\mathcal{D}}\big(F\big(X^{\otimes n}\big)\big), \quad \rho_n''(b) = F\big(\rho_n^X(b)\big).$$

These representations are equivalent. In fact, the canonical isomorphism $F(X)^{\otimes n} \cong F(X^{\otimes n})$ given by the monoidal structures of F gives an intertwiner.

2.4. Quasitriangular Hopf algebras

We argue braidings in the category of modules over a Hopf algebra. If $R = \sum s_i \otimes t_i \in A^{\otimes 2}$ is a universal R-matrix [6, Definition VIII.2.2] of A, **Mod**(A) is a braided monoidal category with braiding $c_{V,W}^R : V \otimes W \to W \otimes V$ given by

$$c_{V,W}^R(v \otimes w) = \sum t_i w \otimes s_i v$$

for $v \in V$ and $w \in W$. It is known that this gives a one-to-one correspondence between braidings of **Mod**(A) and universal R-matrices of A. We denote this braided monoidal category by **Mod**(A, R). We often omit R and denote **Mod**(A, R) by **Mod**(A) if R is obvious.

A *quasitriangular Hopf algebra* is a pair (A, R) of a Hopf algebra A and a universal R-matrix of A. We list basic properties of quasitriangular Hopf algebras.

Proposition 2.9. *(See [8, §2], [6, Chapter VIII].) Let (A, R) be a quasitriangular Hopf algebra. Set $u = \sum S(t_i)s_i$ where $\sum s_i \otimes t_i = R$. Then the followings hold.*

(a) *u is invertible with inverse $u^{-1} = \sum t_i S^2(s_i)$.*
(b) *The antipode S is bijective and we have $S^2(x) = uxu^{-1}$ for all $x \in A$.*
(c) $(\varepsilon \otimes \mathrm{id}_A)(R) = 1 = (\mathrm{id}_A \otimes \varepsilon)(R)$.
(d) $(S \otimes \mathrm{id}_A)(R) = R^{-1} = (\mathrm{id}_A \otimes S^{-1})(R)$ *and* $(S \otimes S)(R) = R$.

The element u above is called the *Drinfeld element* of (A, R). Note that A is *involutive*, i.e., $S^2 = \mathrm{id}_A$ if and only if u is central.

Let $\mathcal{C}$ be a braided monoidal category with braiding c. Then the reverse monoidal category $\mathcal{C}^{\mathrm{rev}}$ is also a braided monoidal category with braiding $c^{\mathrm{rev}}_{X,Y} = c_{Y,X} : X \otimes^{\mathrm{rev}} Y \to Y \otimes^{\mathrm{rev}} X$. $\mathcal{C}^{\mathrm{rev}}$ is equivalent to $\mathcal{C}$ as a braided monoidal category. In fact, the identity functor together with monoidal structure $\varphi_{V,W} = c_{W,V} : V \otimes^{\mathrm{rev}} W \to V \otimes W$ gives an equivalence.

Proposition 2.10. *Let (A, R) be a quasitriangular Hopf algebra.*

(a) *$(A^{\mathrm{cop}}, R_{21})$ is isomorphic to $(A^{\mathrm{op}}, R_{21})$ as a quasitriangular Hopf algebra.*
(b) **Mod**(A, R), **Mod**$(A^{\mathrm{cop}}, R_{21})$ *and* **Mod**$(A^{\mathrm{op}}, R_{21})$ *are equivalent as braided monoidal categories.*

Proof. (a) The antipode $S : A^{\mathrm{cop}} \to A^{\mathrm{op}}$ gives an isomorphism of Hopf algebras. This preserves the universal R-matrix since $(S \otimes S)(R) = R$.

(b) The equivalence given in the proof of Proposition 2.1 induces an equivalence between braided monoidal categories **Mod**$(A^{\mathrm{cop}}, R_{21})$ and **Mod**$(A, R)^{\mathrm{rev}}$. The latter is equivalent to **Mod**(A, R) as we remarked above. □

Lemma 2.11. *Let (A, R) and (A', R') be finite-dimensional quasitriangular Hopf algebras. If* **Mod**(A, R) *and* **Mod**(A', R') *are equivalent as braided monoidal categories, braid group representations ρ_n^A and $\rho_n^{A'}$ are equivalent for each $n \geqslant 2$.*

Proof. Let $F :$ **Mod**$(A, R) \to$ **Mod**(A', R') be an equivalence of braided monoidal categories. By Lemma 2.6, Remark 2.7 and Remark 2.8, we have isomorphisms $\eta_n : A^{\otimes n} \to F(A^{\otimes n})$, $\eta'_n : F(A^{\otimes n}) \to F(A)^{\otimes n}$ and $\eta''_n : F(A)^{\otimes n} \to A'^{\otimes n}$ such that the diagram in **Vec**(k)

$$\begin{array}{ccccccc}
A^{\otimes n} & \xrightarrow{\eta_n} & F(A^{\otimes n}) & \xrightarrow{\eta'_n} & F(A)^{\otimes n} & \xrightarrow{\eta''_n} & A'^{\otimes n} \\
{\scriptstyle \rho_n^A(b)}\downarrow & & {\scriptstyle F(\rho_n^A(b))}\downarrow & & \downarrow{\scriptstyle \rho_n^{F(A)}(b)} & & \downarrow{\scriptstyle \rho_n^{A'}(b)} \\
A^{\otimes n} & \xrightarrow[\eta_n]{} & F(A^{\otimes n}) & \xrightarrow[\eta'_n]{} & F(A)^{\otimes n} & \xrightarrow[\eta''_n]{} & A'^{\otimes n}
\end{array}$$

commutes for all $b \in B_n$. □

3. Invariants associated with braids

In this section, we define monoidal Morita invariants of finite-dimensional Hopf algebras associated with braids. Our construction is based on braid group representations arising from quasitriangular structures. A Hopf algebra does not always have universal R-matrices. We recall the Drinfeld double construction [6, Chapter IX] which admits the canonical quasitriangular structure.

For a finite-dimensional Hopf algebra H, let $\mathcal{D}(H)$ be the Drinfeld double of H. Recall that $\mathcal{D}(H) = H^{*\mathrm{cop}} \otimes H$ as a coalgebra. To avoid confusion, we denote $f \otimes x \in \mathcal{D}(H)$ by $f \bowtie x$. $\mathcal{D}(H)$ has a universal R-matrix

$$\mathcal{R}(H) = \sum_{i=1}^{n} \varepsilon \bowtie h_i \otimes h_i^* \bowtie 1 \in \mathcal{D}(H) \otimes \mathcal{D}(H)$$

where $\{h_1, \ldots, h_n\}$ is a basis of H and $\{h_1^*, \ldots, h_n^*\}$ is the dual basis. $\mathcal{R}(H)$ is denoted by $\mathcal{R}$ if H is obvious. Note that the braided monoidal category **Mod**$(\mathcal{D}(H), \mathcal{R})$ is characterized as the *center*, denoted by $\mathcal{Z}($**Mod**$(H))$, of the monoidal category **Mod**(H) [6, XIII.5]. If finite-dimensional Hopf algebras H and L are monoidally Morita equivalent, we have equivalences

$$\mathbf{Mod}\big(\mathcal{D}(H),\mathcal{R}\big)\approx\mathcal{Z}\big(\mathbf{Mod}(H)\big)\approx\mathcal{Z}\big(\mathbf{Mod}(L)\big)\approx\mathbf{Mod}\big(\mathcal{D}(L),\mathcal{R}\big)$$

of braided monoidal categories. Applying Lemma 2.11, we have the following theorem.

Theorem 3.1. *Let H and L be finite-dimensional Hopf algebras. If H and L are monoidally Morita equivalent, then, for any integers $n\geqslant 2$, braid group representations*

$$\rho_n^{\mathcal{D}(H)}:B_n\to\mathrm{Aut}\big(\mathcal{D}(H)^{\otimes n}\big)\quad\text{and}\quad\rho_n^{\mathcal{D}(L)}:B_n\to\mathrm{Aut}\big(\mathcal{D}(L)^{\otimes n}\big)$$

are equivalent.

Remark 3.2. The above theorem gives us various monoidal Morita invariants. For instance, the exponent of finite-dimensional Hopf algebra H, which is defined to be the smallest integer $n\geqslant 1$ such that the equation

$$\sum x_{(1)}S^{-2}(x_{(2)})\cdots S^{-2n+2}(x_{(n)})=\varepsilon(x)1_H$$

holds for all $x\in H$, is equal to the order of $\rho_n^{\mathcal{D}(H)}(\sigma_1^2)$ (see [9, Theorem 2.5]).

We study the following type of invariants.

Definition 3.3. Let $b\in B_n$ be a braid. We define a *monoidal Morita invariant $\tau(b;H)$ associated with b and a finite-dimensional Hopf algebra H* by

$$\tau(b;H)=\mathrm{Tr}\big(\rho_n^{\mathcal{D}(H)}(b)\big).$$

Let us list some elementary properties of $\tau(b;H)$. For braids $b_1\in B_n$ and $b_2\in B_m$, we denote by $b_1\otimes b_2\in B_{n+m}$ the braid on $n+m$ strands which is obtained by arranging b_2 to the right of b_1.

Proposition 3.4. *Let H be a finite-dimensional Hopf algebra. Then*:

(a) $\tau(1_n;H)=\dim(H)^{2n}$ *where 1_n is the identity of B_n.*
(b) $\tau(b_1b_2;H)=\tau(b_2b_1;H)$ *for all $b_1,b_2\in B_n$.*
(c) $\tau(b_1\otimes b_2;H)=\tau(b_1;H)\tau(b_2;H)$ *for all $b_1\in B_n$ and $b_2\in B_m$.*
(d) *If K/k is a field extension, $\tau(b;K\otimes_k H)=\tau(b;H)$.*

Proof. Proofs are obvious from properties of trace. □

Our invariants cannot distinguish a finite-dimensional Hopf algebra and its dual since the construction is based on the Drinfeld double.

Proposition 3.5. *Let H be a finite-dimensional Hopf algebra.* $\mathbf{Mod}(\mathcal{D}(H),\mathcal{R})$ *and* $\mathbf{Mod}(\mathcal{D}(H^*),\mathcal{R})$ *are equivalent as braided monoidal categories.*

Proof. Recall that $\mathcal{D}(H)=H^*\otimes H$ as a vector space. Under the canonical identification $H^{**}\cong H$, a linear map $T:H^*\otimes H\to H\otimes H^*$ given by $T(f\otimes x)=x\otimes f$ induces an isomorphism

$$T:\big(\mathcal{D}(H),\mathcal{R}(H)\big)\to\big(\mathcal{D}\big(H^{\mathrm{op\,cop}\,*}\big)^{\mathrm{op}},\mathcal{R}\big(H^{\mathrm{op\,cop}\,*}\big)_{21}\big)$$

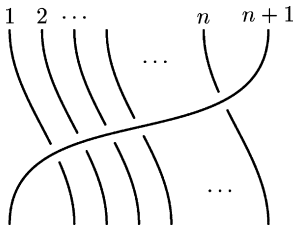


Fig. 1. The braid $b_n \in B_{n+1}$.

of quasitriangular Hopf algebras [10, Theorem 3]. Since H is finite-dimensional, H and $H^{\mathrm{op}\,\mathrm{cop}}$ are isomorphic as Hopf algebras via the antipode. Therefore, we have an isomorphism $(\mathcal{D}(H^*), \mathcal{R}(H^*)) \cong (\mathcal{D}(H)^{\mathrm{op}}, \mathcal{R}(H)_{21})$ of quasitriangular Hopf algebras. Applying Proposition 2.10 completes the proof. □

Corollary 3.6. *For each $n \geqslant 2$, braid group representations $\rho_n^{\mathcal{D}(H)}$ and $\rho_n^{\mathcal{D}(H^*)}$ are equivalent. In particular, $\tau(b; H^*) = \tau(b; H)$ for any braid b.*

4. Application to group algebras

Our aim in this section is to prove Theorem 1.1. This will be done by calculating the monoidal Morita invariant associated with braid

$$b_n = \sigma_n \sigma_{n-1} \cdots \sigma_1 \in B_{n+1} \quad (n = 1, 2, \ldots)$$

which is illustrated as Fig. 1.

4.1. Reduction to characteristic zero

Let G be a finite group. As we prove later in Lemma 4.7, we have

$$\tau(b_n; kG) = |G| \cdot \#\left\{g \in G \mid g^n = 1\right\}$$

for each n. This equation holds in any characteristic. In characteristic zero, Theorem 1.1 follows easily from it. The first step of the proof of Theorem 1.1 is to reduce the problem to the case when the characteristic of k is zero. We have the following theorem.

Theorem 4.1.

(a) *Let G be a finite group. Then, $\tau(b; \mathbb{C}G)$ is a non-negative integer for any braid $b \in B_n$. For an arbitrary field k, we have $\tau(b; \mathbb{C}G) = \tau(b; kG)$ in k.*
(b) *Let k be an arbitrary field. If two finite groups G and G' are k-isocategorical, we have $\tau(b; \mathbb{C}G) = \tau(b; \mathbb{C}G')$ for any braid $b \in B_n$.*

In fact, the field $\mathbb{C}$ in Theorem 4.1(b) can be replaced by any field. There are two reasons why we use $\mathbb{C}$. First, $\mathbb{C}$ is an algebraically closed field of characteristic zero. Second, we desire to relate our monoidal Morita invariants to certain theories of closed 3-manifolds; see Section 5.

We recall the structure of $\mathcal{D}(kG)$. For each $g \in G$, define $e_g \in (kG)^*$ by $\langle e_g, x\rangle = \delta_{x,g}$ for all $x \in G$ where δ is the Kronecker delta. Then, the set $\{e_g \bowtie x\}_{g,x\in G}$ is a basis of $\mathcal{D}(kG)$. The multiplication of $\mathcal{D}(kG)$ is given by

$$(e_g \bowtie x)(e_h \bowtie y) = \delta_{g,xhx^{-1}} e_g \bowtie (xy)$$

for all $g, h, x, y \in G$. The comultiplication Δ is given by

$$\Delta(e_g \bowtie x) = \sum_{h \in G} (e_{hg} \bowtie x) \otimes (e_{gh^{-1}} \bowtie x)$$

for all $g, x \in G$. Set $1^* = \sum_{g \in G} e_g$ (this is the counit of kG). Then, the universal R-matrix of $\mathcal{D}(kG)$ is given by

$$\mathcal{R}(kG) = \sum_{g \in G} (1^* \bowtie g) \otimes (e_g \bowtie 1).$$

The Drinfeld element u and its inverse are given respectively by

$$u = \sum_{g \in G} e_g \bowtie g^{-1} \quad \text{and} \quad u^{-1} = \sum_{g \in G} e_g \bowtie g.$$

The proof of Theorem 4.1 is based on the following observation: For all braid $b \in B_n$, $\rho_n^{\mathcal{D}(kG)}(b)$ is represented by a permutation matrix in basis

$$e_{g_1} \bowtie x_1 \otimes \cdots \otimes e_{g_n} \bowtie x_n \quad (g_i, x_i \in G).$$

Note that this permutation is independent from the base field k. For a permutation matrix P, we denote by $\mathrm{Fix}(P)$ the number of fixed points of the corresponding permutation. The following lemma is a direct consequence of Theorem A.1 in Appendix A.

Lemma 4.2. *Let P and Q be permutation matrices of the same size. If P and Q are similar over k, we have* $\mathrm{Fix}(P) = \mathrm{Fix}(Q)$.

If the characteristic of the base field k is zero, the proof is obvious since $\mathrm{Tr}(P) = \mathrm{Fix}(P)$ in k. Lemma 4.2 allows us to define $\mathrm{Fix}(P)$ for an automorphism P on a finite-dimensional vector space which is represented by a permutation matrix in some basis. Now we can prove Theorem 4.1.

Proof of Theorem 4.1. (a) Let $b \in B_n$ be a braid. $\tau(b; \mathbb{C}G)$ is a non-negative integer as the trace of a permutation matrix. Since, as we remarked above, a permutation induced by $\rho_n^{\mathcal{D}(kG)}(b)$ is independent from the choice of the base field k, we have

$$\mathrm{Fix}\big(\rho_n^{\mathcal{D}(kG)}(b)\big) = \mathrm{Fix}\big(\rho_n^{\mathcal{D}(\mathbb{C}G)}(b)\big) = \mathrm{Tr}\big(\rho_n^{\mathcal{D}(\mathbb{C}G)}(b)\big) = \tau(b; \mathbb{C}G).$$

Thus, we have $\tau(b; kG) = \tau(b; \mathbb{C}G)$ in k.

(b) Assume that finite groups G and G' are k-isocategorical. Theorem 3.4 yields

$$\mathrm{Fix}\big(\rho_n^{\mathcal{D}(kG)}(b)\big) = \mathrm{Fix}\big(\rho_n^{\mathcal{D}(kG')}(b)\big)$$

for all $b \in B_n$. Thus, we have $\tau(b; \mathbb{C}G) = \tau(b; \mathbb{C}G')$. □

4.2. The number of elements of order n

Let (A, R) be a quasitriangular Hopf algebra and V be a finite-dimensional left A-module. Write $R = \sum_i s_i \otimes t_i$. By the definition of ρ^V_{n+1}, we have

$$\rho^V_{n+1}(b_n)(v_0 \otimes \cdots \otimes v_n) = \sum_{i_1,\dots,i_n} t_{i_1} v_1 \otimes \cdots \otimes t_{i_n} v_n \otimes s_{i_n} \cdots s_{i_1} v_0$$

for all $v_0, \dots, v_n \in V$. First, we give a description of the trace of $\rho^V_{n+1}(b_n)$ in terms of R and the Drinfeld element u. For $a \in A$, we denote by $\mathrm{Tr}_V(a)$ the trace of the linear endomorphism on V given by $v \mapsto a \cdot v$ $(v \in V)$.

Lemma 4.3. *Notations are as above.*

(a) *For each $n \geqslant 1$, we have*

$$\mathrm{Tr}\big(\rho^V_{n+1}(b_n)\big) = \sum_{i_1,\dots,i_n} \mathrm{Tr}_V(s_{i_1} \cdots s_{i_n} t_{i_n} \cdots t_{i_1}).$$

(b) *If A is involutive, $\mathrm{Tr}(\rho^V_{n+1}(b_n)) = \mathrm{Tr}_V(u^{-n})$.*

Proof. (a) Let $f_0, \dots, f_n \in \mathrm{End}(V)$ be linear endomorphisms on V. Define a linear map $f : V^{\otimes(n+1)} \to V^{\otimes(n+1)}$ by

$$f(v_0 \otimes \cdots \otimes v_n) = f_1(v_1) \otimes \cdots \otimes f_n(v_n) \otimes f_0(v_0)$$

for all $v_0, \dots, v_n \in V$. Then we have $\mathrm{Tr}(f) = \mathrm{Tr}(f_1 \circ \cdots \circ f_n \circ f_0)$ by direct calculation. Applying this formula to $\rho^V_{n+1}(b_n)$ the assertion follows.

(b) Since A is involutive, u is central in A and its inverse is given by $u^{-1} = \sum_i t_i s_i$ (see Proposition 2.9). Thus we have

$$\sum_{i_1,\dots,i_n} t_{i_1} \cdots t_{i_n} s_{i_n} \cdots s_{i_1} = u^{-n}.$$

This implies $\mathrm{Tr}(\rho^V_{n+1}(b_n)) = \mathrm{Tr}_V(u^{-n})$. □

Remark 4.4. We can avoid the large part of the calculation. The proof will be much easier if we use Kauffman's beads arguments [11] with suitable modification.

The order of the antipode of a finite-dimensional Hopf algebra H equals to the order of the antipode of $\mathcal{D}(H)$. The following description of $\tau(b_n; H)$ is a direct consequence of Lemma 4.3.

Lemma 4.5. *For a finite-dimensional involutive Hopf algebra H, we have*

$$\tau(b_n; H) = \mathrm{Tr}_{\mathcal{D}(H)}\big(u^{-n}\big)$$

where u is the Drinfeld element of the Drinfeld double $\mathcal{D}(H)$.

Remark 4.6. Similarly, we have $\tau(b_n^{-1}; H) = \mathrm{Tr}_{\mathcal{D}(H)}(u^n)$ under the same assumption as the above lemma. If the characteristic of k is zero, $\dim(H)^{-1}\tau(b_n^{-1}; H)$ equals to $\nu_n(\mathrm{Tr}_H)$ where ν_n is the n-th Frobenius–Schur indicator [12]. The following lemma is only a well-known property of higher Frobenius–Schur indicators.

Lemma 4.7. *Let G be a finite group. For each positive number n, we have*

$$\tau(b_n; kG) = |G| \cdot \#\{g \in G \mid g^n = 1\}.$$

Proof. Let u be the Drinfeld element of $\mathcal{D}(kG)$. We calculate $\mathrm{Tr}_{\mathcal{D}(kG)}(u^{-n})$ in view of Lemma 4.5. We have $u^{-n} = \sum_{g\in G} e_g \bowtie g^n$ by induction on n. By the definition of the multiplication, we have

$$\mathrm{Tr}_{\mathcal{D}(kG)}(e_x \bowtie g) = \delta_{g,1}|G|$$

for all $x, g \in G$. Thus, we have

$$\tau(b_n; kG) = \mathrm{Tr}_{\mathcal{D}(kG)}\big(u^{-n}\big) = |G| \cdot \#\{g \in G \mid g^n = 1\}. \qquad \square$$

Proof of Theorem 1.1. Let $o_n(G)$ be the number of elements of order n in G. By Lemma 4.7, we have

$$\frac{1}{|G|}\tau(b_n; \mathbb{C}G) = \sum_{d|n} o_d(G)$$

where the sum is taken over all positive integer d that divides n. Applying the Möbius inversion formula to this equation, we have

$$o_n(G) = \frac{1}{|G|}\sum_{d|n} \mu\left(\frac{n}{d}\right)\tau(b_d; \mathbb{C}G)$$

where μ is the Möbius function. If G and G' are k-isocategorical finite groups, then $\tau(b_d; \mathbb{C}G) = \tau(b_d; \mathbb{C}G')$ by Theorem 4.1(b). Hence we have $o_n(G) = o_n(G')$. $\square$

Finally, we give some remarks on monoidal Morita invariants $\tau(b_n; -)$ and $\tau(b_n^{-1}; -)$. Until the end of this section, the base field k is assumed to be an algebraically closed field of characteristic zero. For a finite-dimensional semisimple Hopf algebra H and an integer n, we set

$$\omega_n(H) = \frac{1}{\dim(H)}\mathrm{Tr}_{\mathcal{D}(H)}\big(u^n\big)$$

where u is the Drinfeld element of the Drinfeld double $(\mathcal{D}(H), \mathcal{R})$. This is a monoidal Morita invariant by Lemma 4.5 and Remark 4.6.

Let V be a finite-dimensional H-module with character χ. For a positive integer n, the *n-th Frobenius–Schur indicator* of χ is the number

$$\nu_n(\chi) := \sum \chi(\Lambda_{(1)}\Lambda_{(2)}\cdots\Lambda_{(n)})$$

where $\Lambda \in H$ is the integral such that $\varepsilon(\Lambda) = 1$. If $\widetilde{\chi}$ is the character of the induced module $\mathcal{D}(H)\otimes_H V$, $\nu_n(\chi) = \dim(H)^{-1}\widetilde{\chi}(u^n)$ [12]. In particular, $\omega_n(H) = \nu_n(\chi_H)$ where χ_H is the character of the regular representation H. The following lemma is essentially given in [12].

Lemma 4.8. $\omega_r(H) = 1$ *if* r *is coprime to* $\dim(H)$. *In particular,* $\omega_{\pm 1}(H) = 1$.

Proof. We first prove the case when $r = 1$. Let $\lambda \in H^*$ be the integral on H such that $\langle \lambda, \Lambda \rangle = 1$. Then we have $\langle \lambda, 1 \rangle = \dim(H)$, and hence $\chi_H = \lambda$ (see [5, Chapter 7]). Therefore, $\omega_1(H) = \nu_1(\chi_H) = \langle \lambda, \Lambda \rangle = 1$.

Next, we prove the general case. Since H is semisimple, $u^{\dim(H)^3} = 1$ [9, Theorem 4]. Let $\{V_i\}_{i \in I}$ be representatives of isomorphism classes of simple $\mathcal{D}(H)$-modules. We denote $\dim(V_i)$ by d_i. Since u is central, u acts on V_i as scalar. We denote this scalar by u_i. u_i's are $\dim(H)^3$-th root of unity. By Artin–Wedderburn theorem, we have an isomorphism $\mathcal{D}(H) \cong \oplus_{i \in I} V_i^{\oplus d_i}$ of left $\mathcal{D}(H)$-modules. This decomposition yields

$$\mathrm{Tr}_{\mathcal{D}(H)}\big(u^n\big) = \sum_{i \in I} u_i^n d_i^2$$

for any integer n.

Let ζ be a primitive $\dim(H)^3$-th root of unity. Since r is coprime to $\dim(H)$, there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ such that $\sigma(\zeta) = \zeta^r$. Then, $\sigma(u_i) = u_i^r$ for all $i \in I$. Thus,

$$\mathrm{Tr}_{\mathcal{D}(H)}\big(u^r\big) = \sum_{i \in I} u_i^r d_i^2 = \sum_{i \in I} \sigma(u_i) d_i^2 = \sigma\big(\dim(H)\big) = \dim(H).$$

This implies $\omega_r(H) = 1$. □

5. Relations to low-dimensional topology

We discuss relations between our invariants and the construction of invariants of closed 3-manifolds due to Reshetikhin and Turaev. Throughout this section, the base field k is assumed to be algebraically closed of characteristic zero.

5.1. Ribbon categories

A *ribbon category* is a braided monoidal category with left duality and balancing isomorphism (see [2, Chapter I] and [6, Chapter XIV]). The balancing isomorphism is denoted by $\theta_V : V \to V$. In this section, we use the *graphical calculus* ([2, I.1.6], [6, Chapter XIV]) which is a pictorial technique to represent morphisms in ribbon categories.

Let $\mathcal{C}$ be a ribbon category. We say that an oriented framed link is $\mathcal{C}$-colored if each of its component is labeled with an object of $\mathcal{C}$. Every $\mathcal{C}$-colored oriented framed link L defines a morphism $\mathbf{1} \to \mathbf{1}$ in $\mathcal{C}$ (see [2, Chapter I]). This morphism is called the *operator valued invariant* of L.

Let (A, R) be a quasitriangular Hopf algebra. A central invertible element $\theta \in A$ is called a *ribbon element* if we have $S(\theta) = \theta$ and $\Delta(\theta) = (R_{21}R)(\theta \otimes \theta)$. A *ribbon Hopf algebra* is a quasitriangular Hopf algebra equipped with a ribbon element. If (A, R, θ) is a ribbon Hopf algebra, finite-dimensional left A-modules form a ribbon category with braiding c^R and a balancing isomorphism given by $\theta_V : V \to V$, $v \mapsto \theta \cdot v$ $(v \in V)$. We denote this ribbon category by $\mathbf{mod}(A, R, \theta)$, or simply by $\mathbf{mod}(A)$ if R and θ are obvious.

The quantum trace [2, I.1.5] of an endomorphism $f : V \to V$ in a ribbon category is denoted by $\mathrm{tr}_q(f)$. For an object V of a ribbon category, the quantum dimension $\dim_q(V)$ is defined by $\dim_q(V) = \mathrm{tr}_q(\mathrm{id}_V)$. We argue some properties of the quantum trace in $\mathbf{mod}(A)$.

Lemma 5.1. *Notations are as above.*

(a) *Let* $f : V \to V$ *be a morphism in* $\mathbf{mod}(A)$. *Then, we have*

$$\mathrm{tr}_q(f) = \mathrm{Tr}\big(v \mapsto u\theta \cdot f(v)\big)$$

where u is the Drinfeld element of (A, R). Here, Tr *means the usual trace of linear endomorphisms.*

(b) *Consider the commutative diagram of morphisms in* $\mathbf{mod}(A)$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V' & \xrightarrow{i} & V & \xrightarrow{p} & V'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & V' & \xrightarrow[i]{} & V & \xrightarrow[p]{} & V'' & \longrightarrow & 0 \end{array}$$

with exact rows. We have $\mathrm{tr}_q(f) = \mathrm{tr}_q(f') + \mathrm{tr}_q(f'')$.

Proof. (a) is well known, see for example [6, Proposition XIV.6.4]. (b) is obvious by (a) and usual properties of the trace. □

Let $\mathcal{C}$ be a ribbon category, L an oriented framed link with components $L_1, \dots, L_m$. If we color each component L_i with an object $V_i \in \mathcal{C}$, we obtain an element $\mathrm{End}_{\mathcal{C}}(\mathbf{1})$ via the operator-valued invariant. We denote this element by $\langle L; V_1, \dots, V_m\rangle$.

Lemma 5.2. *Let L be an oriented framed link with m-components. $\langle L; -, \dots, -\rangle$ is multiadditive in the following sense*: *Let $V_1, \dots, V_m \in \mathbf{mod}(A)$. If there exists an exact sequence*

$$0 \longrightarrow V_i' \longrightarrow V_i \longrightarrow V_i'' \longrightarrow 0$$

in $\mathbf{mod}(A)$ *for some i, we have*

$$\begin{aligned} \langle L; V_1, \dots, V_m\rangle = {} & \langle L; V_1, \dots, V_{i-1}, V_i', V_{i+1}, \dots, V_m\rangle \\ & + \langle L; V_1, \dots, V_{i-1}, V_i'', V_{i+1}, \dots, V_m\rangle. \end{aligned}$$

Proof. First, color each component L_j with V_j except for the i-th one. Then cut the i-th component of L and form a partially colored ribbon graph T so that we can obtain L by closing T. For each $V \in \mathbf{mod}(A)$, we obtain a morphism $\eta_V : V \to V$ in $\mathbf{mod}(A)$ by coloring the uncolored component with V. By graphical calculus, we have

$$\mathrm{tr}_q(\eta_V) = \langle L; V_1, \dots, V_{i-1}, V, V_{i+1}, \dots, V_m\rangle.$$

The family η is a natural morphism in $\mathbf{mod}(A)$. Thus, we have

$$\mathrm{tr}_q(\eta_{V_i}) = \mathrm{tr}_q(\eta_{V_i'}) + \mathrm{tr}_q(\eta_{V_i''})$$

by Lemma 5.1(b). This completes the proof. □

The following lemma is due to Etingof and Gelaki [13].

Lemma 5.3. *Let (A, R) be a quasitriangular Hopf algebra with u the Drinfeld element. If A is finite-dimensional semisimple and cosemisimple, u^{-1} is a ribbon element of (A, R).*

In the ribbon category $\mathbf{mod}(A, R, u^{-1})$, the quantum trace and the quantum dimension reduce to the usual trace and the dimension by Lemma 5.1(a).

5.2. Reshetikhin–Turaev invariant of closed 3-manifolds

By a "manifold" we mean an oriented connected topological manifold. A *modular category* [4, Definition 3.1.1] is a semisimple ribbon category with a finite number of simple objects satisfying a certain non-degeneracy condition. Reshetikhin and Turaev [14] introduced a method of constructing an invariant of closed 3-manifold using a modular category. Let us briefly describe their construction following [2] and [4].

Let $\mathcal{C}$ be a modular category with $\{V_i\}_{i\in I}$ representatives of isomorphism classes of simple objects of $\mathcal{C}$. We denote by d_i the quantum dimension of V_i. Since $\mathrm{End}_{\mathcal{C}}(V_i) = k$ by definition, we can define $\theta_i \in k$ by $\theta_{V_i} = \theta_i \cdot \mathrm{id}_{V_i}$ for each $i \in I$. Set $p^{\pm} = \sum_{i\in I} \theta_i^{\pm 1} d_i^2$ and $D = \sqrt{p^+ p^-}$. Then the numbers $p^{\pm}$ and D are nonzero [4, Theorem 3.1.7].

For a framed link L with components $L_1, \dots, L_m$, we fix an arbitrary orientation of L and set

$$\{L\} = \sum_{i_1,\dots,i_m \in I} \langle L; V_{i_1}, \dots, V_{i_m}\rangle\, d_{i_1} \cdots d_{i_m}.$$

The right-hand side does not depend on the numbering of components and the choice of orientation of L.

Now we describe the *Reshetikhin–Turaev invariant* $\mathbf{RT}_{\mathcal{C}}$ of a closed 3-manifold associated with $\mathcal{C}$. Let M be a closed 3-manifold. By a classical result, any closed 3-manifold can be obtained by the so-called *Dehn surgery* on S^3 along a certain framed link. Fix a framed link L yielding M. Then, $\mathbf{RT}_{\mathcal{C}}(M)$ is given by

$$\mathbf{RT}_{\mathcal{C}}(M) = D^{-|L|-1}\left(\frac{p^+}{p^-}\right)^{\frac{1}{2}\sigma(L)} \{L\}$$

where $|L|$ is the number of components of L and $\sigma(L)$ is the so-called *wreath number* of L (see [2, II.2.1] for its definition). The right-hand side does not depend on the choice of L and thus $\mathbf{RT}_{\mathcal{C}}(M)$ is an invariant of the closed 3-manifold M.

Remark 5.4. We defined D to be $\sqrt{p^+ p^-}$. This exists since we work over an algebraically closed field of characteristic zero. The definition of $\mathbf{RT}_{\mathcal{C}}$ depends on the choice of D, that is, the choice of square roots of $p^+ p^-$. Therefore, we need to fix D to define $\mathbf{RT}_{\mathcal{C}}$.

5.3. Modular categories arising from Hopf algebras

Let H be a finite-dimensional semisimple Hopf algebra and u the Drinfeld element for the Drinfeld double $\mathcal{D}(H)$. Then $\mathbf{mod}(\mathcal{D}(H), \mathcal{R}, u^{-1})$ is a modular category [13, Lemma 1.1]. We denote by $\mathbf{RT}_{\mathcal{D}(H)}$ the Reshetikhin–Turaev invariant associated to this modular category.

Let us describe the invariant $\mathbf{RT}_{\mathcal{D}(H)}$. First, we compute numbers $p^{\pm}$ and D. Let $\{V_i\}_{i\in I}$ be representatives of isomorphism classes of irreducible $\mathcal{D}(H)$-modules. By Artin–Wedderburn theorem, we have an isomorphism $\mathcal{D}(H) \cong \bigoplus_{i\in I} V_i^{\oplus d_i}$ of left $\mathcal{D}(H)$-modules. Note that θ_i is the unique eigenvalue of the action of central element u^{-1} on V_i. By Lemma 4.8, we have

$$p^{\pm} = \sum_{i\in I} \theta_i^{\pm 1} d_i^2 = \mathrm{Tr}_{\mathcal{D}(H)}\left(u^{\mp 1}\right) = \dim(H).$$

This allows us to choose $D = \sqrt{p^+ p^-}$ to be $\dim(H)$.

Remark 5.5. $\zeta = (p^+/p^-)^{1/6}$ is known to be a root of unity in general. When the base field is $\mathbb{C}$, we can write $\zeta = \exp(2\pi c\sqrt{-1}/24)$ for some c. c is called the *central charge* for the theory [4, Remark 3.1.20]. In our cases, we have $p^{\pm} = \dim(H)$ as described above. This implies that the central charge of $\mathbf{mod}(\mathcal{D}(H))$ is zero.

Next, we argue $\{L\}$ where L is a framed link with m components. Note that every d_i is a positive integer. By Lemma 5.2,

$$\{L\} = \sum_{i_1,\dots,i_m} \langle L; V_{i_1}^{\oplus d_{i_1}}, \dots, V_{i_m}^{\oplus d_{i_m}} \rangle = \langle L; \mathcal{D}(H), \dots, \mathcal{D}(H) \rangle.$$

Summarizing, we have the following theorem.

Theorem 5.6. *The Reshetikhin–Turaev invariant* $\mathbf{RT}_{\mathcal{D}(H)}$ *is given as follows*: *If a closed* 3*-manifold* M *is obtained by surgery on* S^3 *along a framed link* L*,*

$$\mathbf{RT}_{\mathcal{D}(H)}(M) = \dim(H)^{-|L|-1} \langle L; \mathcal{D}(H), \dots, \mathcal{D}(H) \rangle.$$

For a braid $b \in B_n$, we denote by $\widehat{b}$ the framed link obtained by closing b. A graphical calculus gives the equation

$$\operatorname{Tr}\big(\rho_n^{\mathcal{D}(H)}(b)\big) = \langle \widehat{b}; \mathcal{D}(H), \dots, \mathcal{D}(H) \rangle.$$

Thus, if a closed 3-manifold M is obtained by surgery along $\widehat{b}$, we have

$$\mathbf{RT}_{\mathcal{D}(H)}(M) = \dim(H)^{-|\widehat{b}|-1} \tau(b; H).$$

Note that any framed link can be obtained by closing a certain braid (for ordinary links, this fact is known as Alexander's theorem). Thus, any closed 3-manifold can be obtained by surgery along $\widehat{b}$ for some braid b. Let H and L be finite-dimensional semisimple Hopf algebras. If H and L are monoidally Morita equivalent, we have $\dim(H) = \dim(L)$ by Lemma 2.6. Summarizing, we have the following theorem.

Theorem 5.7. *H and L are as above. Then we have* $\mathbf{RT}_{\mathcal{D}(H)} = \mathbf{RT}_{\mathcal{D}(L)}$.

Let G be a finite group and $\omega : G \times G \times G \to \mathbb{C}^{\times}$ a normalized 3-cocycle. Dijkgraaf and Witten [15] introduced a method of constructing an invariant of closed 3-manifolds using a pair (G, ω) (see also [16]). Let us denote this invariant by $Z_{G,\omega}$. When ω is the trivial 3-cocycle, by definition, we have

$$Z_{G,1}(M) = \frac{1}{|G|} \#\operatorname{Hom}\big(\pi_1(M), G\big)$$

where $\pi_1(M)$ is the fundamental group of M.

On the other hand, Altsüler and Coste [17] introduced a method of constructing an invariant of 3-manifolds using the modular category of finite-dimensional modules over the quasi-Hopf algebra $\mathcal{D}^{\omega}(G)$, which is defined to be a certain deformation of $\mathcal{D}(\mathbb{C}G)$. When ω is the trivial 3-cocycle, this invariant is equal to $\mathbf{RT}_{\mathcal{D}(\mathbb{C}G)}$. Altsüler and Coste conjectured in [17] and Sato and Wakui proved in [18, Corollary 5.5] that Altsüler-Coste invariant is equal to the Dijkgraaf–Witten invariant $Z_{G,\omega}$. Thus we have

$$\mathbf{RT}_{\mathcal{D}(\mathbb{C}G)}(M) = Z_{G,1}(M) = \frac{1}{|G|}\#\operatorname{Hom}\bigl(\pi_1(M), G\bigr)$$

for all closed 3-manifold M. This gives rise to the following theorem.

Theorem 5.8. *Let b be a braid, m the number of components of $\widehat{b}$ and M the closed 3-manifold obtained by surgery along $\widehat{b}$. Then we have*

$$\tau(b; \mathbb{C}G) = |G|^m \#\operatorname{Hom}\bigl(\pi_1(M), G\bigr).$$

Combining Theorem 4.1 and this theorem, we have Theorem 1.2. Note that Lemma 4.7 is a special case of the above theorem when M is the lens space $L(n,1)$ whose fundamental group is the cyclic group of order n. In fact, it is well known in the theory of surgery that framed link $\widehat{b}_n$ yields $L(n,1)$. ($\widehat{b}_n$ is isotopic to the trivial knot with the framing $+n$.)

6. Examples

6.1. Numbers of homomorphisms from quaternion groups

For an integer $m \geqslant 2$, set $Q_{4m} = \langle x, y \mid x^{2m} = 1,\ \ y^2 = x^m,\ \ yxy^{-1} = x^{-1}\rangle$. Q_8 is the quaternion group. In general, Q_{4m} is called the generalized quaternion group of order $4m$. The following theorem is an example of our monoidal Morita invariants.

Theorem 6.1. *Set $b = \sigma_1^4 \in B_2$. Then, for any finite group G, we have*

$$\tau(b; \mathbb{C}G) = |G|^2 \#\operatorname{Hom}(Q_8, G).$$

Proof. For simplicity, we write $\mathcal{D}(\mathbb{C}G)$ by $\mathcal{D}(G)$. Let $\mathcal{R}$ be the universal R-matrix of $\mathcal{D}(G)$. Then, in a similar way to the proof of Lemma 4.7, we have

$$\begin{aligned}
\tau(b; \mathbb{C}G) &= \operatorname{Tr}_{\mathcal{D}(G)\otimes\mathcal{D}(G)}\bigl((\mathcal{R}_{21}\mathcal{R})^2\bigr) \\
&= \sum_{g,h\in G} \operatorname{Tr}_{\mathcal{D}(G)}\bigl(e_g \bowtie g^{-1}hgh\bigr) \operatorname{Tr}_{\mathcal{D}(G)}\bigl(e_{ghg^{-1}} \bowtie gh^{-1}gh\bigr) \\
&= |G|^2 \#\bigl\{(g,h) \in G\times G \mid g^{-1}hgh = 1,\, gh^{-1}gh = 1\bigr\} \\
&= |G|^2 \#\operatorname{Hom}(Q, G)
\end{aligned}$$

where Q is the group defined by generators g and h with relations $g^{-1}hgh = gh^{-1}gh = 1$. Q is isomorphic to Q_8 via a map $Q_8 \to Q$ given by $x \mapsto g$, $y \mapsto h$. □

Remark 6.2. The list of all finite subgroups of $SO(4)$ which can act freely on S^3 is known (see, e.g., [19, §6]) and contains Q_{4m} for all $m \geqslant 2$. If Γ is such a finite group, the quotient space S^3/Γ is an orientable closed 3-manifold with fundamental group Γ (spherical manifolds). Thus, in view of Theorem 5.8, there exists a braid b such that $\tau(b; \mathbb{C}G) = |G|^m \#\operatorname{Hom}(\Gamma, G)$ where m is the number of components of $\widehat{b}$. The above theorem may be considered as a special case of this fact. However, the author does not know whether the closed 3-manifold S^3/Q_8 is obtained by surgery along $\widehat{b}$ with $b = \sigma_1^4$.

6.2. Categorical rigidity of finite groups of small order

In this subsection, we argue categorical rigidity of finite groups of small order and prove the following theorem.

Theorem 6.3. *All finite groups of orders less than* 32 *are categorically rigid.*

Proof. We first note that all finite abelian groups are categorically rigid over an arbitrary field. In fact, if H is a finite-dimensional commutative Hopf algebra, every finite-dimensional Hopf algebra which is monoidally Morita equivalent to H is isomorphic to H (see [3, Remark 3.8]). Therefore, we consider non-abelian finite groups.

By using Theorem 1.1 and the above-mentioned fact, we can conclude that all finite groups of orders less than 32 except for 16 are categorically rigid over an arbitrary field. However, this theorem is not sufficient to give the complete classification of groups of order 16.

Let us argue categorical rigidity of groups of order 16. As is well known, there are exactly nine non-abelian groups of order 16 up to isomorphism. Using Theorem 1.1, we conclude that five of them are categorically rigid over an arbitrary field. The rest of them consists of two pairs for which Theorem 1.1 fails to work. The first pair consists of

$$G_1 = Q_8 \times \mathbb{Z}_2 \quad \text{and} \quad G_2 = \langle x, y \mid x^4 = y^4 = 1,\ yxy^{-1} = x^{-1} \rangle.$$

They are not isomorphic, but, for each positive integer n, the number of elements of order n in them are equal. We conclude that G_1 and G_2 are not isocategorical by using Theorem 6.1. In fact, we have

$$\#\operatorname{Hom}(Q_8, G_1) = 112 \quad \text{and} \quad \#\operatorname{Hom}(Q_8, G_2) = 16.$$

The second pair (F_1, F_2) is given as follows. Set

$$F = \langle x, y \mid x^4 = y^2 = 1,\ xy = yx \rangle \quad \text{and} \quad C_2 = \langle s \mid s^2 = 1 \rangle,$$

and define automorphisms f_1 and f_2 on F respectively by

$$f_1(x) = x, \qquad f_1(y) = x^2 y \quad \text{and} \quad f_2(x) = xy, \qquad f_2(y) = y.$$

F_1 and F_2 are semidirect products $F \rtimes C_2$ where $s \in C_2$ acts on F respectively by f_1 and f_2. They are not isomorphic since their abelianizations are different:

$$F_1^{\mathrm{ab}} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \quad \text{and} \quad F_2^{\mathrm{ab}} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4.$$

This pair is an example for which both Theorem 1.1 and Theorem 6.1 fail to work. In fact, they have an equal number of elements of order n for each positive integer n, and, moreover,

$$\#\operatorname{Hom}(Q_8, F_1) = \#\operatorname{Hom}(Q_8, F_2) = 64.$$

If k is an algebraically closed field of $\operatorname{char}(k) \neq 2$, F_1 and F_2 are not k-isocategorical since their Grothendieck rings are different. If $\operatorname{char}(k) = 2$, kF_1 and kF_2 are not even Morita equivalent. This can be proved as follows. First, we note that every irreducible representation of a finite p-group in characteristic p is isomorphic to the trivial one. Therefore, if they are Morita equivalent, there is an isomorphism

$$\operatorname{Ext}^1_{kF_1}(k, k) \cong \operatorname{Ext}^1_{kF_2}(k, k).$$

Now we recall that there is an isomorphism $\mathrm{Ext}^1_{kG}(k,k) \cong \mathrm{Hom}(G^{\mathrm{ab}}, k)$ for every group G. We have

$$\mathrm{Ext}^1_{kF_1}(k,k) \cong k^3 \quad \text{and} \quad \mathrm{Ext}^1_{kF_2}(k,k) \cong k^2.$$

This is a contradiction. Therefore, all finite groups of order 16 are categorically rigid over an arbitrary field. □

Acknowledgment

The author is grateful to Professor Mitsuhiro Takeuchi for his valuable comments on a draft of this paper. This work is supported by Grant-in-Aid for JSPS Fellows.

Appendix A. Similarity between permutation matrices

We denote by $\mathfrak{S}_n$ the symmetric group of degree n. For $\sigma \in \mathfrak{S}_n$, we denote by P_σ the $n \times n$ matrix whose (i,j)-entry is $\delta_{\sigma(i),j}$ where δ is Kronecker's delta. We prove the following theorem.

Theorem A.1. *P_σ and P_τ are similar if and only if σ and τ are conjugate.*

The "if" part is clear since the map $\sigma \mapsto P_\sigma$ is a group homomorphism. Let us prove the "only if" part. As a first step, we characterize linear automorphisms of a finite-dimensional vector space which are represented by permutation matrices in some basis. Let $A = k[X, X^{-1}]$ be the Laurent polynomial ring with an indeterminate X. For a vector space V and a linear automorphism P on V, we denote by ${}_PV$ the A-module with the underlying space V and the action given by $X \cdot v = P(v)$ for $v \in V$. Set

$$M(n) = k\big[X, X^{-1}\big]/\big(X^n - 1\big) \quad (n = 1, 2, \ldots).$$

Lemma A.2. *Let V be a finite-dimensional vector space and P be a linear automorphism on V. P is represented by a permutation matrix in some basis if and only if the A-module ${}_PV$ is isomorphic to a direct sum of $M(i)$'s.*

Proof. The "if" part is clear since the action of X on $M(i)$ is represented by a permutation matrix in basis $\{1, X, \ldots, X^{i-1}\}$. We prove the "only if" part. Set $n = \dim(V)$. Assume that P is represented by the permutation matrix P_σ for some $\sigma \in \mathfrak{S}_n$ in basis $\{e_1, \ldots, e_n\}$. Let

$$\{1, 2, \ldots, n\} = \mathcal{O}_1 \sqcup \cdots \sqcup \mathcal{O}_r \tag{A.1}$$

be the σ-orbit decomposition. $V_i = \mathrm{span}_k\{e_s \mid s \in \mathcal{O}_i\}$ is an A-submodule of ${}_PV$ isomorphic to $M(\#\mathcal{O}_i)$. Thus, we have an isomorphism

$$V = V_1 \oplus \cdots \oplus V_r \cong M(\#\mathcal{O}_1) \oplus \cdots \oplus M(\#\mathcal{O}_r)$$

of A-modules. □

Actually, the σ-orbit decomposition (A.1) gives a cycle decomposition of the permutation σ. We say that a finite-dimensional A-module M *admits a cycle decomposition* if M is isomorphic to a direct sum of $M(i)$'s.

Set $V = k^n$. Note that two invertible $n \times n$-matrices P and Q are similar if and only if ${}_PV$ and ${}_QV$ are isomorphic as A-modules. As we observed above, if $P = P_\sigma$ ($\sigma \in \mathfrak{S}_n$) is a permutation matrix, ${}_PV$ admits a cycle decomposition

$${}_PV \cong M(1)^{\oplus c_1(\sigma)} \oplus \cdots \oplus M(n)^{\oplus c_n(\sigma)}$$

where $c_r(\sigma)$ is the number of cyclic permutations of length r which appear in the cyclic decomposition of σ. If another permutation matrix $Q = P_\tau$ ($\tau \in \mathfrak{S}_n$) is similar to P, ${}_PV$ admits another cycle decomposition

$$ {}_PV \cong M(1)^{\oplus c_1(\tau)} \oplus \cdots \oplus M(n)^{\oplus c_n(\tau)}. $$

Recall that σ and τ are conjugate if and only if their cycle shape are same, i.e., $c_r(\sigma) = c_r(\tau)$ for all r. Theorem A.1 turns into the following statement: If

$$ M(1)^{\oplus d_1} \oplus \cdots \oplus M(n)^{\oplus d_n} \cong M(1)^{\oplus e_1} \oplus \cdots \oplus M(n)^{\oplus e_n} $$

as A-modules, then $d_i = e_i$ for all i.

Note that A has a Hopf algebra structure as a group algebra of an infinite cyclic group generated by $X \in A$. Thus, we can consider tensor products and dual modules of A-modules.

Lemma A.3.

(a) *$M(n) \otimes M(m) \cong M(mn/d)^{\oplus d}$ as an A-module where $d = \gcd(n, m)$ is the greatest common divisor of n and m.*
(b) *$M(n)^* \cong M(n)$ as an A-module.*

Proof. (a) The action of X permutes $\{X^i \otimes X^j\} \subset M(n) \otimes M(m)$. Easy combinatorial arguments completes the proof.

(b) Define $X_i^* \in M(n)^*$ by $X_i^*(X^j) = \delta_{i,n-j}$. Then the linear map $M(n) \to M(n)^*$ given by $X^i \mapsto X_i^*$ gives an isomorphism of A-modules. □

Lemma A.4. $\dim \mathrm{Hom}_A(M(n), M(m)) = \gcd(n, m)$.

Proof. First, we prove the case when $n = 1$. Let $f : M(1) \to M(m)$ be an A-linear map. If $f(1) = \sum_{i=0}^{m-1} c_i X^i$ ($c_i \in k$), we have $c_0 = \cdots = c_{m-1}$ by A-linearity of f. Thus, we have $\dim \mathrm{Hom}_A(M(1), M(m)) = 1$.

Now we prove the general case. By Lemma A.3, we have isomorphisms

$$ \begin{aligned} \mathrm{Hom}_A\big(M(n), M(m)\big) &\cong \mathrm{Hom}_A\big(M(1), M(m) \otimes M(n)^*\big) \\ &\cong \mathrm{Hom}_A\big(M(1), M(l)\big)^{\oplus d} \end{aligned} $$

where $d = \gcd(n, m)$ and $l = mn/d$. Therefore, we have

$$ \dim \mathrm{Hom}_A\big(M(n), M(m)\big) = d \cdot \dim \mathrm{Hom}_A\big(M(1), M(l)\big) = d. \qquad \square $$

Proof of Theorem A.1. Suppose that

$$ V := M(1)^{\oplus e_1} \oplus \cdots \oplus M(n)^{\oplus e_n} \cong M(1)^{\oplus f_1} \oplus \cdots \oplus M(n)^{\oplus f_n} $$

as A-modules. Our aim is to prove $e_i = f_i$ for each i. Set $d_i = \dim \mathrm{Hom}_A(M(i), V)$. By Lemma A.4, we have equations

$$ d_i = \sum_{j=1}^{m} \gcd(i, j) e_j \quad \text{and} \quad d_i = \sum_{j=1}^{m} \gcd(i, j) f_j. $$

Thus, we have a linear equation

$$\Phi_m \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \Phi_m \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}$$

where Φ_m is an $m \times m$ matrix whose (i, j)-entry is $\gcd(i, j)$. The determinant of Φ_m, which is known as Smith's determinant (see, e.g., [20]), equals $\varphi(1) \cdots \varphi(n)$ where φ is Euler's totient function. In particular, Φ_m is invertible, and thus we have $e_i = f_i$ for each i. □

Notes added in proof

After this paper was accepted for publication, I received from Ng the following comments which show that Theorem 1.1 follows from his results joint with Schauenburg under the assumption that the base field k is an algebraically closed field of characteristic zero. I thank Ng for his valuable comments.

In [21], Ng and Schauenburg defined higher Frobenius–Schur indicators for pivotal monoidal categories and proved that these indicators are invariants under equivalences of such categories. Let H and L be finite-dimensional semisimple quasi-Hopf algebras. If $F : \mathbf{Mod}(H) \to \mathbf{Mod}(L)$ is an equivalence of monoidal categories, by [22, Proposition 3.2], we have $\nu_m(V) = \nu_m(F(V))$ for every finite-dimensional H-module V. In particular, $\nu_m(H) = \nu_m(F(H)) = \nu_m(L)$. On the other hand, if $H = kG$ for some finite group G, we have

$$\nu_m(kG) = \#\{g \in G \mid g^m = 1\}.$$

This completes the proof.

References

[1] P. Etingof, S. Gelaki, Isocategorical groups, Int. Math. Res. Not. IMRN (2) (2001) 59–76.
[2] V.G. Turaev, Quantum Invariants of Knots and 3-Manifolds, de Gruyter Stud. Math., vol. 18, Walter de Gruyter & Co., Berlin, 1994.
[3] P. Schauenburg, Hopf bi-Galois extensions, Comm. Algebra 24 (12) (1996) 3797–3825.
[4] B. Bakalov, A. Kirillov Jr., Lectures on Tensor Categories and Modular Functors, Univ. Lecture Ser., vol. 21, American Mathematical Society, Providence, RI, 2001.
[5] S. Dăscălescu, C. Năstăsescu, Ş. Raianu, Hopf Algebras, Monographs and Textbooks in Pure and Applied Mathematics, vol. 235, Marcel Dekker Inc., New York, 2001, an introduction.
[6] C. Kassel, Quantum Groups, Grad. Texts in Math., vol. 155, Springer-Verlag, New York, 1995.
[7] Y. Doi, M. Takeuchi, Cleft comodule algebras for a bialgebra, Comm. Algebra 14 (5) (1986) 801–817.
[8] V.G. Drinfeld, Almost cocommutative Hopf algebras, Algebra i Analiz 1 (2) (1989) 30–46.
[9] P. Etingof, S. Gelaki, On the exponent of finite-dimensional Hopf algebras, Math. Res. Lett. 6 (2) (1999) 131–140.
[10] D.E. Radford, Minimal quasitriangular Hopf algebras, J. Algebra 157 (2) (1993) 285–315.
[11] L.H. Kauffman, Right integrals and invariants of three-manifolds, in: Proceedings of the Kirbyfest, Berkeley, CA, 1998, in: Geom. Topol. Monogr., vol. 2, Geom. Topol. Publ., Coventry, 1999, pp. 215–232 (electronic).
[12] Y. Kashina, Y. Sommerhäuser, Y. Zhu, On higher Frobenius–Schur indicators, Mem. Amer. Math. Soc. 181 (855) (2006) viii+65.
[13] P. Etingof, S. Gelaki, Some properties of finite-dimensional semisimple Hopf algebras, Math. Res. Lett. 5 (1–2) (1998) 191–197.
[14] N.Y. Reshetikhin, V.G. Turaev, Ribbon graphs and their invariants derived from quantum groups, Comm. Math. Phys. 127 (1) (1990) 1–26.
[15] R. Dijkgraaf, E. Witten, Topological gauge theories and group cohomology, Comm. Math. Phys. 129 (2) (1990) 393–429.
[16] M. Wakui, On Dijkgraaf–Witten invariant for 3-manifolds, Osaka J. Math. 29 (4) (1992) 675–696.
[17] D. Altschüler, A. Coste, Quasi-quantum groups, knots, three-manifolds, and topological field theory, Comm. Math. Phys. 150 (1) (1992) 83–107.
[18] N. Sato, M. Wakui, $(2+1)$-dimensional topological quantum field theory with a Verlinde basis and Turaev–Viro–Ocneanu invariants of 3-manifolds, in: Invariants of Knots and 3-Manifolds, Kyoto, 2001, in: Geom. Topol. Monogr., vol. 4, Geom. Topol. Publ., Coventry, 2002, pp. 281–294 (electronic).
[19] P. Orlik, Seifert Manifolds, Lecture Notes in Math., vol. 291, Springer-Verlag, Berlin, 1972.
[20] P. Haukkanen, J. Wang, J. Sillanpää, On Smith's determinant, Linear Algebra Appl. 258 (1997) 251–269.

[21] Siu-Hung Ng, Peter Schauenburg, Higher Frobenius–Schur indicators for pivotal categories, in: Hopf Algebras and Generalizations, in: Contemp. Math., vol. 441, Amer. Math. Soc., Providence, RI, 2007, pp. 63–90.
[22] Siu-Hung Ng, Peter Schauenburg, Central invariants and higher indicators for semisimple quasi-Hopf algebras, Trans. Amer. Math. Soc. 360 (4) (2008) 1839–1860.