Peking Mathematical Journal
https://doi.org/10.1007/s42543-020-00023-5

ORIGINAL ARTICLE

Braid Group Representations from Twisted Tensor Products of Algebras

Paul Gustafson[1] · Andrew Kimball[2] · Eric C. Rowell[2] · Qing Zhang[2]

Received: 25 July 2019 / Revised: 18 February 2020 / Accepted: 25 March 2020

Abstract
We unify and generalize several approaches to constructing braid group representations from finite groups, using iterated twisted tensor products. We provide some general characterizations and classification of these representations, focusing on the size of their images, which are typically finite groups. The well-studied Gaussian representations associated with metaplectic modular categories can be understood in this framework, and we give some new examples to illustrate their ubiquity. Our results suggest a relationship between the braiding on the G-gaugings of a pointed modular category $\mathcal{C}(A, Q)$ and that of $\mathcal{C}(A, Q)$ itself.

Keywords Braid group · Yang–Baxter operator · Twisted tensor product · Group algebra · Unitary representations · Property F

Mathematics Subject Classification 20F36 · 16S80 · 16S40

The authors gratefully acknowledge support under USA NSF Grant DMS-1664359. We also thank C. Galindo, JM Landsberg, Z. Wang and S. Witherspoon for valuable insight. ER was partially supported by a Texas A&M Presidential Impact Fellowship and a Simons Fellowship. Part of this research was carried out while ER was visiting BICMR, Peking University, and AIMR, Tohoku University—the hospitality of these institutions is gratefully acknowledged. Another part of this work was carried out while QZ and ER participated in a semester-long program at MSRI, which is partially supported by NSF Grant DMS-1440140.

✉ Eric C. Rowell
rowell@math.tamu.edu

Paul Gustafson
paul.gustafson@wright.edu

Andrew Kimball
amkimball1@math.tamu.edu

Qing Zhang
zhangqing@math.tamu.edu

1 Department of Electrical Engineering, Wright State University, Dayton, OH 45435, USA

2 Department of Mathematics, Texas A&M University, College Station, TX 77843-3368, USA

Published online: 18 May 2020

1 Introduction

Braid group representations are plentiful; for example, from any object X in a braided fusion category $\mathcal{C}$ one obtains a sequence of braid group representations $\rho^X : \mathcal{B}_n \to \mathrm{End}(X^{\otimes n})$. Braided vector spaces (R, V) [1], i.e., matrix solutions to the Yang–Baxter equation, are also a very rich source, as are families of finite dimensional quotients of braid group algebras $\mathbb{F}(\mathcal{B}_n)$, such as Hecke algebras, Temperley–Lieb algebras [27] and BMW-algebras [5, 31]. That the braided fusion category construction essentially supersedes these sources is well known (see, e.g., [41]), explicit matrices for the generators are not easy to come by—one typically needs the associativity constants (6j-symbols or F-matrices) in addition to the R-symbols, and these are only available for a few families of categories. Generally, the irreducible representations of $\mathcal{B}_n$ are only classified for dimensions at most n [14] and for $\mathcal{B}_3$ for dimensions up to 5 [40]. Braided vector spaces (R, V) are only classified for $\dim(V) = 2$ [24]. Much of the landscape of braid group representations remains to be explored, with a diversity of techniques and constructions available, see, e.g., [3, 4, 42] for some discussion of faithful representations.

In this article, we outline an approach to finding families of braid group representations from twisted tensor products of algebras. We motivate our approach with the following two "proof of principle" examples.

In [20], the following representations of the braid group $\mathcal{B}_n$ were described: set $q = \mathrm{e}^{2\pi \mathrm{i}/m}$ for m odd and let $\mathcal{A}_n(\mathbb{Z}_m)$ be the $\mathbb{C}$-algebra generated by u_i for $1 \leq i \leq n-1$ satisfying

- $u_i^m = 1$
- $u_i u_{i+1} = q^2 u_{i+1} u_i$,
- $u_i u_j = u_j u_i$ for $|i-j| \neq 1$.

The algebra $\mathcal{A}_n(\mathbb{Z}_m)$ is denoted by $ES(m, n-1)$ in [29] and by $T_n^m(q)$ in [38]. Our perspective is to regard $\mathcal{A}_n(\mathbb{Z}_m)$ as an iterated twisted tensor product of the group algebra $\mathbb{C}[\mathbb{Z}_m]$:

$$\mathcal{A}_n(\mathbb{Z}_m) = \mathbb{C}[\mathbb{Z}_m] \otimes_\vartheta \mathbb{C}[\mathbb{Z}_m] \otimes_\vartheta \cdots \otimes_\vartheta \mathbb{C}[\mathbb{Z}_m],$$

where ϑ is the twisting map corresponding to the second relation above. Defining

$$\rho_n(\sigma_i) = R_i := \frac{1}{\sqrt{m}} \sum_{j=0}^{m} q^{j^2} u_i^j,$$

we obtain a representation $\mathcal{B}_n \to \mathcal{A}_n(\mathbb{Z}_m)$. These representations are known to have finite image [18, 20], as are the images of the even m analogue. Moreover, we may obtain a matrix representation by defining $U \in \mathrm{End}(\mathbb{C}^m \otimes \mathbb{C}^m)$ by $U(\mathbf{e}_i \otimes \mathbf{e}_j) = q^{j-i} \mathbf{e}_{i+1} \otimes \mathbf{e}_{j+1}$ and assigning

$$u_i \mapsto \mathrm{Id}^{\otimes i} \otimes U \otimes \mathrm{Id}^{\otimes n-i-1}.$$

From this representation, one obtains a braided vector space as $R := \rho_2(\sigma_1)$ on $V = \mathbb{C}^m$.

Another example of braid group representations related to twisted tensor products of algebras is found in [35] (due to Jones) where the quaternion group Q_8 appears. For $1 \leq i \leq n-1$, let $\mathcal{A}_n(Q_8)$ be the algebra generated by u_i, v_i satisfying

(1) $u_i^2 = v_i^2 = -1$ for all i,
(2) $[u_i, v_j] = -1$ if $|i-j| < 2$,
(3) $[u_i, u_j] = [v_i, v_j] = 1$,
(4) $[u_i, v_j] = 1$ if $|i-j| \geq 2$.

Although $\mathcal{A}_n(Q_8)$ is, strictly speaking, a quotient of a twisted tensor product of group algebras, we nonetheless obtain braid group representations via

$$\sigma_i \mapsto (1 + u_i + v_i + u_i v_i).$$

In this article, we initiate the general problem of finding braid group representations in twisted tensor products of (group) algebras, unifying the two examples just outlined.

Our study is motivated by more than just idle curiosity. In the last section we explore some relationships between these twisted tensor products of group algebras and G-gaugings of pointed modular categories, laying the groundwork towards understanding braid group representations associated with weakly group theoretical modular categories and the property F conjecture. This conjecture [32] predicts that the braid group images obtained from any weakly integral braided fusion category $\mathcal{C}$ have finite image, i.e., $\mathcal{C}$ has property F. By taking Drinfeld centers one may reduce this conjecture to the case where $\mathcal{C}$ is a modular category. A major motivation for this conjecture is to characterize topological phases of matter in which particle exchange induces braid group representations with infinite image. This would provide a simple criterion for braiding universality for the corresponding topological quantum computation model, see [37] for a survey of this approach. For this reason, we mainly focus on unitary representations, but the general algebraic framework does not require this assumption. The property F conjecture has been verified for many classes of braided fusion categories, for example, group-theoretical categories [13], quantum group categories [16, 27, 30, 35, 38], and certain metaplectic categories [23].

The paper is organized as follows: In Sect. 2, we set down the general framework for our problem, which is explicitly described and analyzed in Sect. 3. We carry out several case studies for both abelian and non-abelian cases in Sect. 4 while the connections to categories obtained by gauging symmetries of pointed modular categories are speculated upon in Sect. 5, followed by a short section of conclusions. An appendix contains some Magma codes for some explicit examples.

2 Preliminaries

We first describe the general algebraic ingredients for the problem we are interested in.

2.1 Twisted Tensor Products

The treatment of twisted tensor products in [8] is most suitable for our purposes: let A and B be $\mathbb{F}$-algebras with multiplication maps μ_A, μ_B respectively, and a map $\vartheta : B \otimes A \to A \otimes B$, such that ϑ is $\mathbb{F}$-linear map with $\vartheta(b \otimes 1) = (1 \otimes b)$ and $\vartheta(1 \otimes a) = (a \otimes 1)$. The map $\mu_\vartheta : (A \otimes B) \otimes (A \otimes B) \to A \otimes B$ defined by

$$\mu_\vartheta = (\mu_A \otimes \mu_B)\circ(\mathrm{Id}_A \otimes \vartheta \otimes \mathrm{Id}_B)$$

defines an associative multiplication if and only if

$$\vartheta\circ(\mu_B \otimes \mu_A) = \mu_\vartheta\circ(\vartheta \otimes \vartheta)\circ(\mathrm{Id}_B \otimes \vartheta \otimes \mathrm{Id}_A). \tag{2.1}$$

The corresponding algebra, denoted $A \otimes_\vartheta B$ will be called a **twisted tensor product** of A and B, and the map ϑ will be called a unital twisting map. We shall be most interested in the case where $A = B$.

To iterate this process, we rely on the results of [26]. Given 3 algebras A, B and C and unital twisting maps $\vartheta_1 : B \otimes A \to A \otimes B$, $\vartheta_2 : C \otimes B \to B \otimes C$ and $\vartheta_3 : C \otimes A \to A \otimes C$ each of which satisfy Equation (2.1), one can define two maps $T_1 = (\mathrm{Id}_A \otimes \vartheta_2)\circ(\vartheta_3 \otimes \mathrm{Id}_B)$ on $C \otimes (A \otimes_{\vartheta_1} B)$ and $T_2 = (\vartheta_1 \otimes \mathrm{Id}_C)\circ(\mathrm{Id}_B \otimes \vartheta_3)$ on $(B \otimes_{\vartheta_2} C) \otimes A$ which are potentially unital twisting maps. [26, Theorem 2.1] shows that these are both unital twisting maps if and only if the compatibility condition

$$(\mathrm{Id}_A \otimes \vartheta_2)(\vartheta_3 \otimes \mathrm{Id}_B)(\mathrm{Id}_C \otimes \vartheta_1) = (\vartheta_1 \otimes \mathrm{Id}_C)(\mathrm{Id}_B \otimes \vartheta_3)(\vartheta_2 \otimes \mathrm{Id}_A) \tag{2.2}$$

is satisfied. Moreover, the two **iterated twisted tensor products** $(A \otimes_{\vartheta_1} B) \otimes_{T_1} C$ and $A \otimes_{T_2} (B \otimes_{\vartheta_2} C)$ constructed from these twisting maps are isomorphic algebras. One may inductively define twisted tensor products for any number of algebras A_i provided the analogous compatibility conditions are satisfied. Again, we will be especially interested in the case where $A = A_i = A_j$, and $\vartheta = \vartheta_{i,i+1} : A_{i+1} \otimes A_i \to A_i \otimes A_{i+1}$ for adjacent copies of A and $\sigma = \vartheta_{i,j} : A_j \otimes A_i \to A_i \otimes A_j$ for $|i - j| > 1$ is the usual flip map $\sigma(a \otimes b) = b \otimes a$. In fact, for all of our examples we will have $\vartheta(a \otimes b) = \tau(a, b)b \otimes a$ for some function $\tau : A \otimes A \to \mathbb{F}$. One then easily sees that (2.2) is satisfied:

$$(\mathrm{Id} \otimes \vartheta)(\sigma \otimes \mathrm{Id})(\mathrm{Id} \otimes \vartheta)(a \otimes b \otimes c) \quad \text{and} \quad (\vartheta \otimes \mathrm{Id})(\mathrm{Id} \otimes \sigma)(\vartheta \otimes \mathrm{Id})(a \otimes b \otimes c) \tag{2.3}$$

are both equal to $\tau(a, b)\tau(b, c)(c \otimes b \otimes a)$. Moreover, Condition (2.1) and unitality are equivalent to $\tau : A \otimes A \to \mathbb{F}$ being a bihomomorphism of $\mathbb{F}$-algebras:

$$\tau(a_1a_2, b_1b_2) = \tau(a_2, b_1)\tau(a_1, b_1)\tau(a_2, b_1)\tau(a_2, b_2),$$

and unitality implies $\tau(1, a) = \tau(a, 1) = 1$, while bilinearity is immediate.

2.2 Braid Group Representations and Property *F*

Our goal is to study families of representations of the braid group $\mathcal{B}_n$. In particular, we are interested in representations that are related in the following way:

Definition 2.1 An indexed family of complex $\mathcal{B}_n$-representations (ρ_n, V_n) is a *sequence of braid representations* if there exist injective algebra homomorphisms $\iota_n : \mathbb{C}\rho_n(\mathcal{B}_n) \to \mathbb{C}\rho_{n+1}(\mathcal{B}_{n+1})$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{C}\mathcal{B}_n & \longrightarrow & \mathbb{C}\rho_n(\mathcal{B}_n) \\ \big\downarrow & & \big\downarrow \iota_n \\ \mathbb{C}\mathcal{B}_{n+1} & \longrightarrow & \mathbb{C}\rho_{n+1}(\mathcal{B}_{n+1}) \end{array}$$

where the left-hand side of the square is induced by the inclusion $\mathcal{B}_n \hookrightarrow B_{n+1}$ given by $\sigma_i \mapsto \sigma_i$.

Our examples are typically of the following form: let $1 \in \mathscr{A}_1 \subset \mathscr{A}_2 \subset \cdots \subset \mathscr{A}_n \subset \cdots$ be a tower of finite dimensional semisimple algebras, and $\rho_n : \mathbb{C}\mathcal{B}_n \to \mathscr{A}_n$ algebra homomorphisms that respect the inclusions $\mathscr{A}_n \subset \mathscr{A}_{n+1}$. Then the canonical faithful representation of $\mathscr{A}_n$ provides a sequence of representations.

For example, we obtain a sequence of $\mathcal{B}_n$-representations from any braided vector space (R, V), i.e., an invertible operator $R \in \mathrm{Aut}(V^{\otimes 2})$ that satisfies the Yang–Baxter equation

$$(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R) \in \mathrm{Aut}(V^{\otimes 3}).$$

Explicitly we have $\mathcal{B}_n \to \mathrm{Aut}(V^{\otimes n})$ via $\sigma_i \to \mathrm{Id}_V^{\otimes i-1} \otimes R \otimes \mathrm{Id}_V^{\otimes n-i-1}$.

Other standard examples come from the Temperley–Lieb, Hecke and BMW-algebras mentioned in Sect. 1.

Some conjectures on the images of such representations are found in [17, 18, 36]. For example, it is an open question whether unitary braided vector spaces have virtually abelian images, but there is strong evidence that this is so.

3 Twisted Tensor Products of Algebras and Yang–Baxter Operators

The problem that we propose to study is the following:

Problem 3.1 Find and classify braid group representations inside (iterated) twisted tensor products of (group) algebras, generalizing the well-known Gaussian solutions.

More explicitly we will first define and analyze iterated twisted tensor powers of group algebras $\mathbb{Q}(q)[G] \otimes_\vartheta \mathbb{Q}(q)[G] \otimes_\vartheta \cdots \otimes_\vartheta \mathbb{Q}(q)[G]$ following the formalism of the previous section. Then we will look for sequences of representations ρ_n of the braid group $\mathcal{B}_n$ inside these algebras where $\rho_n(\sigma_i)$ is supported in the ith tensor factor and all $\rho_n(\sigma_i)$ have the same form as elements of $\mathbb{Q}(q)[G]$.

3.1 Twisted Tensor Products of Group Algebras

First, we describe the twisted tensor products of (group) algebras we will study. Fix a finite group G and $q \in U(1)$. On the group algebra $\mathbb{Q}(q)[G]$ we would like to find a unital twisting map $\vartheta : \mathbb{Q}(q)[G] \otimes \mathbb{Q}(q)[G] \to \mathbb{Q}(q)[G] \otimes \mathbb{Q}(q)[G]$ such that $\vartheta(g \otimes h) = \tau(g,h)h \otimes g$ on basis elements where $\tau(g,h) = q^{\alpha(g,h)}$. Here α is a priori simply a function $G \times G \to \mathbb{Z}$. If ϑ is a unital twisting map then $\tau(g,h) : G \times G \to U(1)$ is a bicharacter of G, i.e., satisfies (2.3). Since $q^{\alpha(g^k,h)} = q^{k\alpha(g,h)}$ we assume that q is an mth root of unity (where $m \mid \exp(G)$), and that $\alpha : G \times G \to \mathbb{Z}_m$ is a bihomomorphism. Now define $\sigma : \mathbb{Q}(q)[G] \otimes \mathbb{Q}(q)[G] \to \mathbb{Q}(q)[G] \otimes \mathbb{Q}(q)[G]$ to be the usual flip map $g \otimes h = h \otimes g$. It is routine to check that (2.2) is satisfied by ϑ and σ.

With these verifications, we can define a finite dimensional semisimple algebra $\mathcal{A}_n(G,\tau)$ as an iterated twisted tensor product of $\mathbb{C}[G]$ follows: as a $\mathbb{Q}(q)$ vector space $\mathcal{A}_n(G,\tau) = \mathbb{Q}(q)[G]^{\otimes n-1}$. For each $1 \le i \le n-1$ and $g \in G$ we define elements $g_i = 1^{\otimes i-1} \otimes g \otimes 1^{\otimes n-i-2}$. We can then dispense with the $\otimes$ symbol altogether, and write monomials as $g_1^{(i_1)} \cdots g_{n-1}^{(i_{n-1})}$ where $g^{(i_j)} \in G$. The multiplication on $\mathcal{A}_n(G,\tau)$ has the following straightening rules on the generators g_i:

$$g_i h_j = \begin{cases} h_j g_i, & |i-j| > 1, \\ q^{\pm\alpha(g,h)} h_{i\pm1} g_i, & j = i \pm 1, \\ (gh)_i, & j = i, \end{cases}$$

where the bihomomorphism $\alpha : G \times G \to \mathbb{Z}_m$ determines τ. The following is presumably well known but can be proved directly using classical techniques, which we provide for the reader's amusement.

Proposition 3.2 *The algebra $\mathcal{A}_n(G,\tau)$ is semisimple of dimension $|G|^{n-1}$ over $\mathbb{Q}(q)$.*

Proof Notice that the set of monomials in normal form $M := \{q^\ell g_1^{(i_1)} \cdots g_{n-1}^{(i_{n-1})} : g^{(i_j)} \in G, \ell \in \mathbb{Z}_m\}$ form a basis for $\mathcal{A}_n(G,\tau)$ over $\mathbb{Q}$ since $\mathcal{A}_n(G,\tau)$ is $\mathbb{Q}(q)[G]^{\otimes n-1}$ as a vector space. To show that $\mathcal{A}_n(G,\tau)$ is semisimple, let $X \subset \mathcal{A}_n(G,\tau)$ be a submodule, and $\pi : \mathcal{A}_n(G,\tau) \to X$ any vector space projection. Note that any $\mathbf{t} \in M$ has an inverse in M, since the straightening rules allow us to write $\mathbf{t}^{-1}$ in the normal form of M. We then use the standard averaging trick to find an $\mathcal{A}_n(G,\tau)$-module projection onto X:

$$T_\pi(y) := \frac{1}{m|G|^{n-1}} \sum_{\mathbf{t} \in M} \mathbf{t}\pi(\mathbf{t}^{-1}y).$$

One can readily check that T_π is a surjective $\mathcal{A}_n(G,\tau)$-module homomorphism so that the kernel of T_π provides a direct complement to X in $\mathcal{A}_n(G,\tau)$, proving that $\mathcal{A}_n(G,\tau)$ is semisimple. □

3.1.1 Connection to Group Extensions

We also note the following alternative construction of the algebra $\mathcal{A}_n(G,\tau)$ via group extensions. In this section, we show that, as a $\mathbb{Q}$-algebra, $\mathcal{A}_n(G,\tau)$ is isomorphic to the group algebra over $\mathbb{Q}$ of a central extension of G^{n-1}.

More concretely, let G be a finite group and $m \mid \exp(G)$. Let $\alpha : G \times G \to \mathbb{Z}_m$ be a bihomomorphism. For $n \geq 2$, let $c : G^n \times G^n \to \mathbb{Z}_m$ be the bihomomorphism defined by

$$c(g,h) = -\sum_{i=1}^{n-1} \alpha(h_i, g_{i+1}).$$

Since c is a bihomomorphism, it satisfies the two-cocycle condition. We define $G^{\times_\alpha n}$ to be the central extension of G^n corresponding to the two-cocycle $c \in Z^2(G^n, \mathbb{Z}_m)$.

Proposition 3.3 *Let q be a primitive mth root of unity. There is an isomorphism of $\mathbb{Q}$-algebras*

$$\mathcal{A}_{n+1}(G,\tau) \cong \mathbb{Q}(G^{\times_\alpha n}),$$

where $\tau : \mathbb{Q}(q)[G] \otimes \mathbb{Q}(q)[G] \to \mathbb{Q}(q)[G] \otimes \mathbb{Q}(q)[G]$ is the same twisting map defined above, i.e., $\tau(g_1 \otimes h_2) = q^{\alpha(g,h)} h_2 \otimes g_1$ on basis elements.

Proof We represent $G^{\times_\alpha n}$ as the set $\mathbb{Z}_m \times G^n$ where the multiplication is given by

$$(x \times g) \cdot (y \times h) = (c(g,h) + x + y) \times gh.$$

Let $\phi : \mathcal{A}_{n+1}(G,\tau) \to \mathbb{Q}(G^{\times_\alpha n})$ be the $\mathbb{Q}$-linear bijection defined by $q^j g_1 \otimes \cdots \otimes g_n \mapsto j \times (g_1, \ldots, g_n)$. To see that ϕ is an algebra map, we need to verify that it preserves the straightening relations. If $i - j \neq 1$, we have $c(\phi(g_i), \phi(h_j)) = 1$. If $i - j = 1$, we have $c(\phi(g_i), \phi(h_j)) = \alpha(h, g^{-1})$. Thus,

$$\begin{aligned}
[\phi(g_i), \phi(h_{i+1})] &= \phi(g_i)\phi(h_{i+1})\phi(g_i^{-1})\phi(h_{i+1}^{-1}) \\
&= \phi(g_i)(\alpha(g,h) \times (e, \ldots, e, g_i^{-1}, h_{i+1}, e, \ldots, e))\phi(h_{i+1}^{-1}) \\
&= \alpha(g,h) \times e \\
&= \phi(q^{\alpha(g,h)}).
\end{aligned}$$

Thus, the straightening relations are preserved by ϕ. It follows that ϕ is an isomorphism of $\mathbb{Q}$-algebras. □

3.2 Braid Group Representations

The second part of the problem is to look for and classify the representations of the braid group inside the algebras $\mathcal{A}_n(G,\tau)$. Fix a pair (G,α) where G is a finite group and $\alpha : G\times G \to \mathbb{Z}_m$ is a bihomomorphism. We then have a corresponding twisted tensor power $\mathcal{A}_n(G,\tau)$ where $\tau(g,h)=q^{\alpha(g,h))}$ as in Sect. 3.1. We are interested in finding the invertible

$$r=\sum_{g\in G} f(g)g \in \mathbb{C}[G]$$

so that for $i=1,2$ the $r_i := \sum_{g\in G} f(g)g_i \in \mathcal{A}_3(G,\tau)\otimes_{\mathbb{Q}(q)}\mathbb{C}$ satisfy the braid relation $r_1r_2r_1=r_2r_1r_2$. We shall call such solutions r $\mathcal{A}(G,\tau)$**-Yang–Baxter operators (YBOs)**. Since the braid equation may be written as a linear combination of monomials $g_1^{(i_1)}g_2^{(i_2)}\in\mathcal{A}_3(G,\tau)$ with coefficients in $\mathbb{Q}(q)[x_1,\dots,x_{|G|}]$ where $x_i := f(g^{(i)})$, we may assume that the function f takes values in $\overline{\mathbb{Q}(q)}=\overline{\mathbb{Q}}$, i.e., the algebraic closure of $\mathbb{Q}(q)$. For the sake of notation, we will usually just consider scalars in the complex field $\mathbb{C}$.

This should be compared with the problem of finding Yang–Baxter operators on a vector space V. In our case, we seek invertible $r\in\mathbb{C}[G]$ so that $\rho_n(\sigma_i)=r_i$ is a homomorphism $\rho_n : \mathcal{B}_n\to\mathcal{A}_n(G,\tau)$ (suitably complexified). As $\mathcal{A}_n(G,\tau)\otimes\mathbb{C}$ is a finite-dimensional semisimple $\mathbb{C}$-algebra, one can obtain $\mathcal{B}_n$-representations by pullback on any $\mathcal{A}_n(G,\tau)\otimes\mathbb{C}$-module. For example, one might use the regular representation to get a sequence of braid group representations (ρ_n,V_n), as defined in [36]. However, one cannot, in general, turn such a homomorphism into a solution to the Yang–Baxter equation. There is one situation where one can perform such a transformation: if the sequence of braid group representations (ρ_n,V_n) is *localizable* in the sense of [36]. For example, suppose $\mathcal{A}_n(G,\tau)$ has a representation ϑ_n of the form $V^{\otimes n}$ with $\vartheta(g_i)$ acting locally:

$$\vartheta_n(g_i)(v_1\otimes\cdots\otimes v_i\otimes v_{i+1}\otimes\cdots\otimes v_n)=(v_1\otimes\cdots\otimes\vartheta(g)(v_i\otimes v_{i+1})\otimes\cdots\otimes v_n),$$

where $\vartheta : G\to \mathrm{Aut}(V^{\otimes 2})$ is a G-representation. Then $\vartheta(r)$ will be a Yang–Baxter operator, and $\vartheta_n(r_i)=(\mathrm{Id}_V)^{\otimes i-1}\otimes\vartheta(r)\otimes(\mathrm{Id}_V)^{\otimes n-i-1}$ is a localization of the corresponding braid group representation.

We may also put a $*$-structure on $\mathcal{A}_n(G,\tau)$ as follows: define $g_i^*=g_i^{-1}$ and $q^*=1/q=\overline{q}$ and then extend to an antiautomorphism on products and linearly on sums in the usual way. This makes $\mathcal{A}_n(G,\tau)$ a $*$-algebra. In this way, we can discuss unitary $\mathcal{A}(G,\tau)$-YBOs, as those r with $r^*r=1$.

3.3 Equivalence Classes of $\mathcal{A}_n(G,\tau)$

For a fixed G, different choices of τ give isomorphic algebras. We identify a few of these isomorphisms to reduce the complexity of our main goal.

One equivalence of $\mathcal{A}_n(G,\tau)$ comes from the choice of Galois conjugates of q. For $(s,m)=1$ defining $\tau^s(g,h)=q^{s\alpha(g,h)}$ obviously gives us $\mathcal{A}_n(G,\tau)\cong\mathcal{A}_n(G,\tau^s)$ by Galois conjugation.

Another equivalence comes from automorphisms of G. If $\psi \in \mathrm{Aut}(G)$ then the bicharacter $(g,h) \mapsto \alpha(\psi(g),\psi(h))$ gives us a new $\tau^{\Psi}(g,h) = \tau(\psi(g),\psi(h))$ and gives us $\mathcal{A}_n(G,\tau) \cong \mathcal{A}_n(G,\tau^{\Psi})$.

An important problem is to understand the orbits under these actions. The Galois symmetry amounts to replacing α with $s\alpha$. Now observe that since $\alpha : G \times G \to \mathbb{Z}_m$ has abelian co-domain, it is determined by its values on the abelianization $G_{ab} := G/[G,G]$. So we may assume $G = A$ is abelian for the purposes of determining the orbits. It is clear that the bicharacters $A \times A \to U(1)$ for a finite abelian group A form an abelian group under pointwise addition. In fact, this group is isomorphic to $\mathrm{Hom}(A, A^*)$ where $A^* = \mathrm{Hom}(A, U(1))$ is the group of characters. Indeed, if $\chi : A \times A \to U(1)$ is a bicharacter then define $F_\chi \in \mathrm{Hom}(A, A^*)$ by $F_\chi(a)(b) = \chi(a,b)$. Since χ is a bicharacter F_χ is a $\mathbb{Z}$-module map with values in $\mathrm{Hom}(A, U(1))$. Since $f \in \mathrm{Hom}(A, A^*)$ determines a unique bicharacter $\chi_f(a,b) = f(a)(b)$, the map $\chi \mapsto F_\chi$ is clearly a bijection, and $F_\chi + F_\eta = F_{\chi+\eta}$. As the bihomomorphisms $\alpha : A \times A \to \mathbb{Z}_m$ are in one-to-one correspondence with bicharacters, this determines all such bihomomorphisms α. For elementary abelian p-groups $A = (\mathbb{Z}_p)^k$ a bihomomorphism to $\mathbb{Z}_p$ can be represented as a $k \times k$ matrix X with i,j entry $\alpha(e_i, e_j) \in \mathbb{Z}_p$ where e_i is the generator $(0,\dots,0,1,0,\dots,0)$ of the ith factor. That is, $\alpha(g,h) = g^T X h$ where we identify $g \in A$ with column vectors. Of course an automorphism $\Psi \in \mathrm{Aut}(A) \cong \mathrm{GL}_k(\mathbb{Z}_p)$ as well, so we may sweep out orbits of α under $\mathrm{Aut}(A)$ as $\Psi^T X \Psi$ since $\alpha(\Psi(g),\Psi(h)) = g^T \Psi^T X h$. Although we will not need it in what follows, one can handle general abelian p-groups in a similar way by identifying $\mathbb{Z}_{p^a}$ with a subgroup of $\mathbb{Z}_{p^b}$ for $a \leq b$. Even more generally, bihomomorphisms on a finite abelian group can be factored by restricting to p-Sylow subgroups.

3.3.1 Forbidden Symmetries

Thus far, we have not applied *different* automorphisms of G to each factor as such an action will generally fail to produce $\mathcal{A}(G,\tau)$-YBOs r_i independent of i. Moreover, if we apply different automorphism to each tensor factor of $\mathcal{A}_n(G,\tau)$ the twisting will no longer be uniform across the iterated twisted tensor product. However, in the following special cases, uniformity is preserved.

Proposition 3.4 *Suppose $G = \mathbb{Z}_m^k$ for an odd integer m and $\tau(x,y) = q^{\alpha(x,y)}$ for a non-degenerate symmetric or skew-symmetric bihomomorphism $\alpha : G \times G \to \mathbb{Z}_p$. Then there is an isomorphism of algebras $\mathcal{A}_n(G,\tau) \cong \mathcal{A}_n(G,\chi)$, where $\chi(x,y) = q^{x^T y}$.*

Proof Observe that for $G = \mathbb{Z}_p^k$ with p odd, nondegenerate bihomomorphisms $\alpha : G \times G \to \mathbb{Z}_m$ are the same as nondegenerate bilinear forms, all of which are of the form $\alpha(x,y) = x^T S y$ for some matrix $S \in \mathrm{GL}_k(\mathbb{Z}_m)$.

First assume $\alpha(x,y) = x^T S y$ is a non-degenerate symmetric bilinear map $G \times G \to \mathbb{Z}_m$. Let $C, D \in \mathrm{GL}_k(\mathbb{Z}_m)$ be such that $I = CSD$ (the Smith normal form of S). Let $\eta(x,y) := x^T y$ be the corresponding twist. We claim that the map $\phi : G^{n-1} \to G^{n-1}$ defined by

$$\phi(g_i) = \begin{cases} ((C^T)^{-1}g)_i, & i \text{ odd,} \\ (D^{-1}g)_i, & i \text{ even} \end{cases}$$

induces an isomorphism $\mathcal{A}_n(G,\tau) \cong \mathcal{A}_n(G,\eta)$. Indeed, for $x, y \in G$, we have

$$\eta((C^T)^{-1}x, D^{-1}y) = ((C^T)^{-1}x)^T CSD(D^{-1}y) = x^T Sy.$$

On the other hand,

$$\begin{aligned} \eta(D^{-1}x, (C^T)^{-1}y) &= (D^{-1}x)^T (C^T)^{-1} y \\ &= x^T (D^{-1})^T (D^T S^T C^T)(C^T)^{-1} y \\ &= x^T Sy. \end{aligned}$$

Now since the Smith normal form of a non-degenerate symmetric matrix over $\mathbb{Z}_m$ is diagonal and we may rescale each entry by isomorphisms described above, we obtain an isomorphism with $\mathcal{A}_n(G,\chi)$ as promised.

Now suppose that k is even, and S is invertible and skew-symmetric so that we may assume $S = \begin{pmatrix} 0 & I_0 \\ -I_0 & 0 \end{pmatrix}$, where $I_0 = \mathrm{Id}_{(\mathbb{Z}_m)^{k/2}}$ and $\alpha(x,y) = x^T Sy$ the associated bihomomorphism. Notice that $S^2 = -I$ and $S^T = -S$. Letting $\eta(x,y) = -x^T y$, we define $\phi : \mathcal{A}_n(G,\tau) \to \mathcal{A}_n(G,\eta)$ by $\phi(g_i) = (S^{i-1}g)_i$. To see that ϕ is an algebra homomorphism, we compute:

$$\alpha(S^i x, S^{i+1} y) = x^T (-S)^i (S) S^{i+1} y = (-1)^i x^T S^{2i+2} y = -x^T y = \eta(x,y).$$

Since ϕ is clearly bijective, we have shown that it is an algebra isomorphism $\mathcal{A}_n(G,\tau) \cong \mathcal{A}_n(G,\eta)$. Since η is symmetric, we may use the above to obtain an isomorphism $\mathcal{A}_n(G,\tau) \cong \mathcal{A}_n(G,\chi)$ as promised. □

3.4 Symmetries of $(\mathcal{A}_n(G,\tau), r)$

For a fixed G and τ, the set R of $\mathcal{A}(G,\tau)$-YBOs could be quite large: they are determined by the functions $f : G \to \mathbb{C}$ with $r = \sum_{g\in G} f(g)g \in R$. To reduce the search space we can make use of various symmetries, identifying function f in the same orbit. Informally we will say that two $\mathcal{A}_n(G,\tau)$-YBOs r and s are equivalent if $\rho^r, \rho^s : \mathcal{B}_n \to \mathcal{A}_n(G,\tau)$ have the same image, projectively.

One obvious symmetry comes from the homogeneity of the braid equation $r_1r_2r_1 = r_2r_1r_2$: we can rescale any solution by $z \in \mathbb{C}^\times$ and if our solution is unitary, then we can rescale by $z \in U(1)$. This corresponds to identifying f and zf since the $\mathcal{B}_n$ images are projectively equivalent.

We also have rescaling symmetries of the form $g_i \mapsto q^{s(g_i)} g_i$ for some homomorphism $s : G \to \mathbb{Z}_m$. Since the straightening relations in $\mathcal{A}_n(G,\tau)$ are homogeneous, it is only necessary to check that the map $\chi : G \to U(1)$ given by $\chi(g) = q^{s(g)}$ is a linear character. This automorphism of $\mathbb{C}[G]$ lifts to an automorphism of $\mathcal{A}_n(G,\tau)$, which carries $r_i = \sum_{g\in G} f(g) g_i$ to $r_i^\chi := \sum_{g\in G} f(g) q^{s(g)} g_i$ and hence the images are isomorphic. Therefore, we can identify the solutions that are in the orbit of f under $f \mapsto q^{s(g)}f$.

Denote by $\mathrm{Aut}(G, \alpha)$ the group of automorphisms $\psi \in \mathrm{Aut}(G)$ such that $\alpha\circ(\psi \times \psi) = \alpha$. Any $\psi \in \mathrm{Aut}(G, \alpha)$ lifts to an automorphism of $\mathcal{A}_n(G, \tau)$. For such $\psi \in \mathrm{Aut}(G, \alpha)$, the $\psi(r_i) = \sum_{g\in G} f(g)\psi(g)_i$ for $i = 1, 2$ will satisfy the braid relation, and hence $\psi^{-1}(r) = \sum_{g\in G} f(\psi^{-1}(g))g$ will also be an $\mathcal{A}(G, \tau)$-YBO. Moreover, this obviously induces an isomorphism between $\rho^r(\mathcal{B}_n)$ and $\rho^{\psi(r)}(\mathcal{B}_n)$, so we will thus identify all solutions in the orbit of f under this symmetry $f \mapsto \psi^* f$ for $\psi \in \mathrm{Aut}(G, \alpha)$.

3.4.1 Symmetry Induced by Inversion

An important special case of symmetry induced by automorphisms is the following: if G is *abelian*, the inversion automorphism $\imath : g \mapsto g^{-1}$ on G lifts to an automorphism of $\mathcal{A}_n(G, \tau)$ by defining $\imath(q) = q$, and $\imath(g_i h_j) = \imath(g_i)\imath(h_j) = g_i^{-1}h_j^{-1}$ on products and extending linearly. We will carefully check the defining relations are preserved. First,

$$\imath(g_i)\imath(h_{i+1}) = g_i^{-1}h_{i+1}^{-1} = (h_{i+1}g_i)^{-1} = (q^{-\alpha(g,h)}g_i h_{i+1})^{-1} = q^{\alpha(g,h)}\imath(h_{i+1})\imath(g_i)$$

so that $\imath(g_i h_{i+1}) = q^{\alpha(\imath(g),\imath(h))}\imath(h_{i+1}g_i)$. Second, since G is abelian,

$$\imath((gh)_i) = \imath(g_i h_i) = g_i^{-1}h_i^{-1} = (g^{-1})_i(h^{-1})_i = (g^{-1}h^{-1})_i \stackrel{\star}{=} ((gh)^{-1})_i = (\imath(gh))_i,$$

where the equality denoted $\stackrel{\star}{=}$ uses the G abelian assumption. Finally, note that if g_i and h_j commute then so do $\imath(g_i)$ and $\imath(h_j)$. If $r = \sum_{g\in G} f(g)g$ is an $\mathcal{A}(G, \tau)$-YBO then so is $\imath(r) = \sum_{g\in G} f(g)g^{-1}$; hence, $r'' = \sum_{g\in G} f(g^{-1})g$ is as well.

If G is abelian there is an additional symmetry of the braid relation $r_1r_2r_1 = r_2r_1r_2$ that we may use to show that $r = \sum_{g\in G} f(g)g$ and $r' := \sum_{g\in G} \overline{f(g)}g$ have isomorphic images. The map σ on $\mathcal{A}_3(G, \tau)$ given by $\sigma(g_1) = g_2$ and $\sigma(xy) = \sigma(y)\sigma(x)$ for $x, y \in \mathcal{A}_3(G, \tau)$ and $\sigma(q) = q^{-1} = \overline{q}$ is an anti-automorphism of $\mathcal{A}_3(G, \tau)$ since

$$\sigma(g_1h_2) = h_1g_2 = q^{\alpha(h,g)}g_2h_1 = \sigma(q^{\alpha(g,h)}h_2g_1)$$

and $\sigma((gh)_1) = (gh)_2 = g_2h_2 = h_2g_2 = \sigma(h_1)\sigma(g_1) = \sigma(g_1h_1)$. This implies that r' is an $\mathcal{A}(G, \tau)$-YBO since

$$r_2'r_1'r_2' = \sigma(r_1r_2r_1) = \sigma(r_2r_1r_2) = r_1'r_2'r_1'.$$

4 Case Studies

In practice, we take the following approach, using symbolic computation software such as Magma and Maple.

(1) Fix G and α, and present the corresponding finitely generated algebra $\mathcal{A}_3(G,\tau)\times\mathbb{Q}(q)[x_g : g\in G]$, using generators and relations, with the x_g being commuting variables.
(2) Define $r_i=\sum_{g\in G}x_g g_i$ for $i=1,2$, and use non-commutative Gröbner bases to write $r_1r_2r_1-r_2r_1r_2$ in its normal form, i.e., as a polynomial in the $g_1^{(i_1)}g_2^{(i_2)}$ with coefficients in $\mathbb{Q}(q)[x_g : g\in G]$.
(3) Compute a commutative Gröbner basis for the ideal generated by the the coefficients using pure lexicographic order to find the ideal of solutions.
(4) Use symmetries to describe families of related solutions.

Often we find that there are finitely many solutions, so that we can give a complete description of them.

4.1 Abelian Groups

4.1.1 Prime Cyclic Groups $G=\mathbb{Z}_p$

We first apply our approach to a well-known case both as a proof of principle and a template for further study.

Let $p\geq 3$ be prime and fix q a primitive pth root of unity. A nontrivial bicharacter $\mathbb{Z}_p\times\mathbb{Z}_p\to U(1)$ must take values in $\mu_p=\{q^j : 0\leq j\leq p-1\}$, so any bicharacter corresponds to a bihomomorphism $\alpha\in\mathrm{Hom}(\mathbb{Z}_p\times\mathbb{Z}_p,\mathbb{Z}_p)$, which is determined by $\alpha(1,1)$. Define a bihomomorphism $\alpha:\mathbb{Z}_p\times\mathbb{Z}_p\to\mathbb{Z}_p$ by $\alpha(1,1)=2$. The orbit of α under automorphisms of $\mathbb{Z}_p$ gives half of all non-trivial bihomomorphisms since $\alpha(\varphi_k(1),\varphi_k(1))=2k^2$ for $k\in\mathbb{Z}_p^\times$ is a square modulo p if and only if 2 is. Galois symmetry $\psi(q)=q^s$ maps the bicharacter $\tau(x,y)=q^{\alpha(x,y)}$ to $\tau^\psi(x,y)=q^{s\alpha(x,y)}$. Thus, we may assume that our bicharacter is associated with the bihomomorphism $\alpha(x,y)=2xy$. The reader may wonder why we do not choose $\alpha'(x,y)=xy$ instead—we will see later that this simplifies the form of our $\mathcal{A}_n(\mathbb{Z}_p,\tau)$-YBOs. Indeed, this choice of α recovers the $\mathbb{Q}(q)$-algebra $\mathcal{A}_n(\mathbb{Z}_p)$ described in the Sect. 1, with generators $u_1,\dots,u_{n-1}$ satisfying $u_iu_{i+1}=q^2u_{i+1}u_i$ and $u_iu_j=u_ju_i$ for $|i-j|>1$ and $u_i^p=1$. The goal now is to find invertible $\mathcal{A}(\mathbb{Z}_p)$-YBOs $r=\gamma\sum_{j=0}^{p-1}f(j)u^j\in\mathbb{C}[\mathbb{Z}_p]$.

To reduce redundancy we will normalize $f(0)=1$ (the solutions where $f(0)=0$ do not seem to be interesting). The symmetries of these solutions again come in several forms. First, since each automorphism of $\mathbb{Z}_p$ that leaves α invariant leads to an automorphism of $\mathcal{A}_n(\mathbb{Z}_p)$ we may identify the corresponding solutions. For $\alpha(x,y)=2xy$ only inversion $x\to -x$ leaves α invariant, which means we may freely identify f and $f'(j)=f(-j)$. We have an additional symmetry in $\mathcal{A}_n(\mathbb{Z}_p)$ given by $u_i\to q^su_i$ since the first two defining relations are homogeneous and $(q^su_i)^p=u_i^p=1$. This corresponds to identifying f with $f^s(j):=f(j)q^{js}$. Finally, complex conjugation is a symmetry of the braid equation $r_1r_2r_1=r_2r_1r_2$, so that we may identify f and its complex conjugate $\overline{f}$.

4.1.2 The Gaussian Solution

One unitary $\mathcal{A}(\mathbb{Z}_p)$-YBO is the Gaussian solution $r = \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} q^{j^2} u$, i.e., $f(j) = q^{j^2}$ [18, 20, 29] and $\gamma = \frac{1}{\sqrt{p}}$. Complex conjugation gives us the solution $\bar{f}(j) = q^{-j^2}$ and the rescaling symmetry gives us $f^s(j) = q^{j^2+sj}$, giving $2p$ distinct solutions.

In [18], it is shown that the braid group representation $\rho_n : \mathcal{B}_n \to \mathcal{A}_n(\mathbb{Z}_p)$ given by $\sigma_i \to r_i$ has finite image. In fact, one has

$$r_i u_{i+1} r_i^{-1} = q u_i^{-1} u_{i+1},$$
$$r_i u_{i-1} r_i^{-1} = q^{-1} u_{i-1} u_i,$$

so that the conjugation action on $\mathcal{A}_n(\mathbb{Z}_p)$ provides a homomorphism of $\rho_n(\mathcal{B}_n)$ into monomial matrices, with kernel a subgroup of the center of $\mathcal{A}_n(\mathbb{Z}_p)$. For n odd, the normal form for $\mathcal{A}_n(\mathbb{Z}_p)$ allows one to show that the center consists of scalars, and since any $\rho_n(\beta)$ in the center of $\mathcal{A}_n(\mathbb{Z}_p)$ has determinant a root of unity (under the regular representation of $\mathcal{A}_n(\mathbb{Z}_p)$) the kernel of the conjugation action above is finite, for n odd. Since $\rho_n(\mathcal{B}_n) \subset \rho_{n+1}(\mathcal{B}_n)$, this is sufficient.

The algebras $\mathcal{A}_n(\mathbb{Z}_p)$ have a *local* representation (see [36]). Let $V = \mathbb{C}^p$ and define an operator on $V^{\otimes 2}$ by $U(\mathbf{e}_i \otimes \mathbf{e}_j) = q^{j-i} \mathbf{e}_{i+1} \otimes \mathbf{e}_{j+1}$ where $\{\mathbf{e}_i\}_{i=0}^{p-1}$ is a basis for V with indices taken modulo p. Then $\Phi_n : u_i \to (\mathrm{Id}_V)^{\otimes i-1} \otimes U \otimes (\mathrm{Id}_V)^{\otimes n-i-1}$ defines a representation $\mathcal{A}_n(\mathbb{Z}_p) \to \mathrm{End}(V^{\otimes n})$. In particular, $\Phi_2(r)$ is an honest $p^2 \times p^2$ YBO.

Example 4.1 We use Magma [7] to work two explicit examples. First consider the case $G = \mathbb{Z}_3$, and suppose $r = 1 + au + bu^2$ is an $\mathcal{A}(\mathbb{Z}_3)$-YBO. All solutions satisfy $a^3 = b^3 = 1$ and $a^2 \neq b$, so that there are exactly 6 distinct solutions (as elements of the algebra, up to rescaling) all of which are obtained from the Gaussian solution via the symmetries described above, hence are equivalent in our sense. In particular, the solutions are all unitary when appropriately normalized.

Similarly for $p = 5$, under the additional assumption that a, b, c, d are 5th roots of unity, we find that there are exactly 10 non-trivial solutions $r = 1 + au + bu^2 + cu^3 + du^4$ (up to rescaling), all of which are obtained from the Gaussian solution via the above symmetries. These solutions are unitary when appropriately normalized. There are ten other non-trivial solutions; however, none of them are (projectively) unitary.

4.2 $G = \mathbb{Z}_p \times \mathbb{Z}_p$

Let p be an odd prime, and let $G = \mathbb{Z}_p \times \mathbb{Z}_p$. To classify $\mathcal{A}_n((\mathbb{Z}_p)^2, \tau)$ we first look at orbits of bihomomorphisms $\alpha : (\mathbb{Z}_p)^2 \to \mathbb{Z}_p$. Such bihomomorphisms are determined by the values on pairs of generators (1, 0), (0, 1) of $\mathbb{Z}_p \times \mathbb{Z}_p$, encoded in a matrix $A_\alpha := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_p)$, so that $\alpha(x, y) = x^T A_\alpha y$. Under automorphisms $X \in \mathrm{GL}_2(\mathbb{Z}_p)$ of $(\mathbb{Z}_p)^2$ the orbit of α is represented by the matrices $\{X^T A_\alpha X : X \in \mathrm{GL}_2(\mathbb{Z}_p)\}$. From [43], we know that there are $p + 7$ orbits.

Example 4.2 The case of $p = 3$ can be completely analyzed computationally as follows: from a representative of each of the 10 orbits of bihomomorphisms $\mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_3$ we use Magma [7] to search for *non-degenerate, unitary* solutions $r = \gamma \sum_{i,j} f(i,j) u^i v^j$ to the corresponding $\mathcal{A}(\mathbb{Z}_3 \times \mathbb{Z}_3, \tau)$-YBE. Here by *non-degenerate* we mean that it does not degenerate to the $\mathbb{Z}_3$-case. The results of these computations are:

- Non-degenerate unitary solutions only exist for the classes represented by $A_1 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, $A_2 = \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix}$ and $A_3 = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$.
- In all cases, after applying an appropriate symmetry of $(\mathcal{A}_n(\mathbb{Z}_3 \times \mathbb{Z}_3, \tau), r)$, the non-degenerate unitary solutions factor as a product of Gaussian $\mathcal{A}_n(\mathbb{Z}_3)$-YBOs, and hence have finite images.

From this example, we expect that the most interesting ones correspond to non-degenerate symmetric or skew-symmetric bilinear forms on $\mathbb{Z}_p^2$. We also allow ourselves to rescale α by a constant. Thus, we focus on $A_1 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, $A_2 = \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix}$ and $A_3 = \begin{pmatrix} 2 & 0 \\ 0 & 2x \end{pmatrix}$ where x is a non-square modulo p. The appearance of the scalar 2 is simply for convenience when we make contact with the Gaussian solution.

We consider each of these cases in turn. We will distinguish the symmetric cases A_1, A_3 by noting that A_1 corresponds to an elliptic form, while A_3 corresponds to a hyperbolic form. For $A_\alpha = A_i$, the corresponding algebras $\mathcal{A}_n(\mathbb{Z}_p \times \mathbb{Z}_p, \tau_i)$ have generators $u_1, v_1, \dots, u_{n-1}, v_{n-1}$ with the multiplicative group $\langle u_i, v_i \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$. All generators commute except for:

(1) For A_1: $u_i u_{i\pm1} = q^{\pm2} u_{i\pm1} u_i$ and $v_i v_{i\pm1} = q^{\pm2} v_{i\pm1} v_i$.
(2) For A_2: $u_i v_{i\pm1} = q^{\pm2} v_{i\pm1} u_i$ and $v_i u_{i\pm1} = q^{\mp2} v_{i\pm1} u_i$.
(3) For A_3: $u_i u_{i\pm1} = q^{\pm2} u_{i\pm1} u_i$ and $v_i v_{i\pm1} = q^{\pm2x} v_{i\pm1} v_i$.

We pause to describe the structure of the algebras $\mathcal{A}_n(\mathbb{Z}_m \times \mathbb{Z}_m, \tau_i)$ for arbitrary odd m. Since the monomials in the u_i, v_i form a basis, we see that $\dim_{\mathbb{Q}(q)} \mathcal{A}_n(\mathbb{Z}_m \times \mathbb{Z}_m, \tau_i) = m^{2n-2}$.

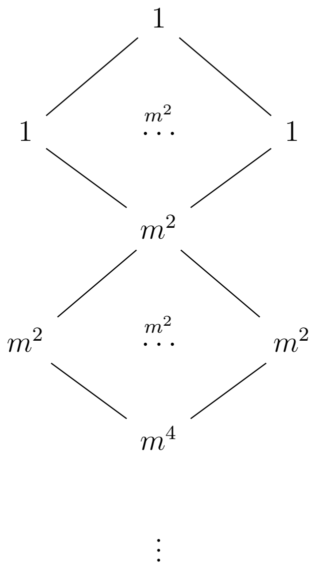

Fig. 1 Bratteli diagram for $\mathcal{A}_n(\mathbb{Z}_m \times \mathbb{Z}_m, \tau_i)$ for m odd

The following proposition explores the structure of $A_n(\mathbb{Z}_m \times \mathbb{Z}_m, \tau_i)$ and the subalgebra of fixed points under the automorphism $\imath$ described in Sect. 3.4.1 given by lifting $u_i \mapsto u_i^{-1}, v_i \mapsto v_i^{-1}$ to $\mathcal{A}_n(G, \tau_i)$. We describe inclusions of algebras in terms of Bratteli diagrams (see [21]): generally, to a tower of multi-matrix algebras with common unit $1 \in A_1 \subset \cdots A_n \subset A_{n+1} \subset \cdots$, we associate a graph with vertices labeled by simple A_k-modules $M_{k,i}$ with $d_{k-1,i,j}$ edges between $M_{k,i}$ and $M_{k-1,j}$ if the restriction of $M_{k,i}$ to A_{k-1} contains $M_{k-1,j}$ with multiplicity $d_{k-1,i,j}$.

Proposition 4.3 *Let m be odd and $G = \mathbb{Z}_m \times \mathbb{Z}_m$. Consider the algebra $\mathcal{A}_n(G, \tau_i)$ with the twists τ_i given by $A_i, 1 \le i \le 3$. Then*

(1) *The center of $\mathcal{A}_n(G, \tau_i)$ is 1 dimensional if n is odd and is m^2 dimensional if n is even. Moreover, when n is odd $\mathcal{A}_n(G, \tau_i) \cong M_{m^{n-1}}(\mathbb{Q}(q))$ is simple while for n even $\mathcal{A}_n(G, \tau_i)$ decomposes as a direct sum of m^2 simple algebras of dimension m^{2n-4}. Moreover, the Bratteli diagram of $\cdots \subset \mathcal{A}_n(G, \tau_i) \subset \cdots$ is given in Fig. 1.*

(2) *Consider the fixed point subalgebra $\mathcal{C}_n(G, \tau_i)$ for the automorphism $\imath$ induced by inversion on $\mathcal{A}_n(G, \tau_i)$. Then for $n \ge 3$ odd, $\mathcal{C}_n(G, \tau_i)$ is a direct sum of two matrix algebras of dimensions $\left(\frac{m^{n-1} \pm 1}{2}\right)^2$. For $n \ge 4$ and even, $\mathcal{C}_n(G, \tau_i)$ has $\frac{m^2+3}{2}$ simple summands: $\frac{m^2-1}{2}$ of dimension m^{2n-4} and two others of dimensions $\left(\frac{m^{n-2} \pm 1}{2}\right)^2$. Moreover, the Bratteli diagram for $\cdots \subset \mathcal{C}_n(G, \tau_i) \subset \mathcal{C}_{n+1}(G, \tau_i) \subset \cdots$ is given by Fig. 2, where the nodes are labelled by the dimensions of the distinct simple modules.*

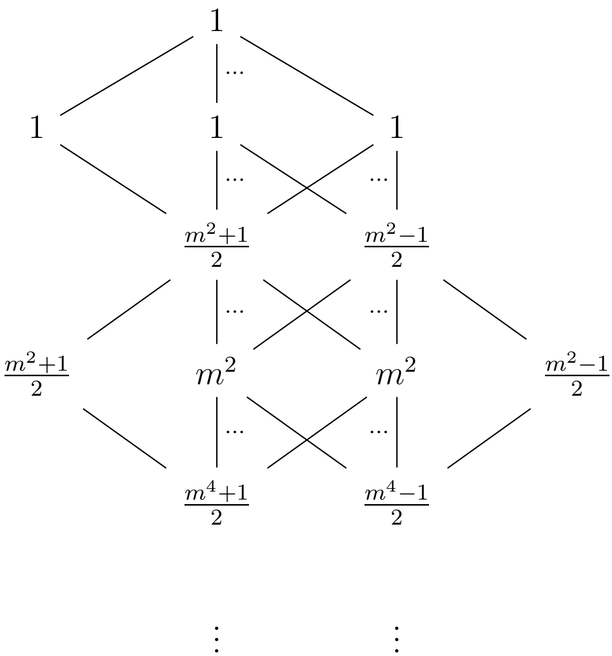

Fig. 2 Bratteli diagram for $\mathcal{C}_n(\mathbb{Z}_m \times \mathbb{Z}_m, \tau_i)$ for m odd

Proof Similar results are found, for example, in [28, 29], so we are content to provide a sketch.

We first note that, by its construction, the isomorphism $\mathcal{A}_n(G,\tau) \cong \mathcal{A}_n(G,\chi)$ of Proposition 3.4 restricts to a bijection on the subalgebras $\langle u_j, v_j \rangle$ for each j, and respect inclusions. It follows that it restricts to an isomorphism $\mathcal{C}_n(G,\tau) \cong \mathcal{C}_n(G,\chi)$. Thus, it suffices to prove the proposition for $\tau(x,y) = \chi(x,y) := q^{x^T y}$, in which the u_i and v_j commute. Now one could derive the stated result directly from [28] without too much trouble, but since some details are left out we will give some idea of how to proceed.

Since the monomials in in normal form $u_1^{a_1} \cdots u_{n-1}^{a_{n-1}} v_1^{b_1} \cdots v_{n-1}^{b_{n-1}}$ in $\mathcal{A}_n(\mathbb{Z}_m \times \mathbb{Z}_m), \chi)$ form a basis over $\mathbb{Q}(q)$, a routine calculation gives a basis for the center to be 1 for n odd and $\{\prod_i u_i^a v_i^b : 0 \le a, b \le m-1\}$ for n even. For later use, we note that for n even, $\{X_{a,b} = u_1^a v_1^b \cdots u_{n-1}^a v_{n-1}^b : 0 \le a, b \le m-1\}$ forms an abelian group isomorphic to G, and the m^2 elements $\Xi_{x,y} := \frac{1}{m^2} \sum_{a,b} q^{xa+yb} X_{a,b} \in \mathcal{A}_n(G,\chi)$ are minimal set of orthogonal idempotents, and one obviously has the Bratteli diagram given in Fig. 1.

Now let us consider the fixed point subalgebra $\mathbb{C}_n(G,\chi)$ of the automorphism ι. Recall that $\mathcal{A}_n(G,\chi)$ has dimension $d(n)^2$ where $d(n) = m^{n-1}$, and is spanned by monomials. Since $\iota(u_1^{a_1} \cdots v_{n-1}^{b_{n-1}}) = u_1^{-a_1} \cdots v_{n-1}^{-b_{n-1}}$ one computes that the subspaces with $\iota(x) = \pm x$ have dimensions $\frac{d(n)^2 \pm 1}{2}$, respectively.

First, suppose n is odd—we will compute the ± 1 eigenspaces for ι in another way. In this case, $\mathbb{C}_n(G,\chi)$ is simple, so that ι is an inner automorphism, i.e., $\iota(x) = JxJ$ for some $d(n) \times d(n)$ matrix with $J^2 = \kappa$ a constant. After rescaling J, we may assume that J is diagonal, $J^2 = I$, and J has eigenvalue 1 with multiplicity k and eigenvalue -1 with multiplicity $d(n) - k < k$. Writing an arbitrary x as a $k, d(n) - k$ block matrix, we find that the subspaces $E_\pm = \{x : JxJ = \pm x\}$ have dimensions $k^2 + (d(n) - k)^2$ and $2k(d(n) - k)$, respectively. Subtracting dimension and comparing to the above we obtain $1 = (2k - d(n))^2$; hence, $k = \frac{d(n)+1}{2}$. Now a double commutant argument shows that $\mathcal{C}_n(G,\chi)$ is a direct sum of two simple algebras of dimension k^2 and $(d(n) - k)^2$ as required.

For the n even case, we observe that on each simple constituent ι either gives an isomorphism to another simple constituent or is an automorphism. Since the simple $(d(n)/m)^2$-dimensional) constituents are $\mathcal{A}_n(x,y) := \Xi_{x,y}\mathcal{A}_n(G,\chi)\Xi_{x,y}$, we observe that $\iota(\Xi_{x,y}) = \Xi_{-x,-y}$, so that ι induces an automorphism on $\mathcal{A}_n(0,0)$ and permutes the other $m^2 - 1$ simple constituents in pairs. Thus, an argument similar to the odd case above shows that $\mathcal{A}_n(0,0)$ splits into two components of dimension $\left(\frac{m^{n-2}\pm 1}{2}\right)^2$ and the remaining $\frac{m^2-1}{2}$ pairs interchanged by ι each yield a single simple m^{2n-4}-dimensional algebra.

Dimension counting finishes the calculation of the Bratteli diagram as stated. □

We now return to the problem of finding solutions

$$r = \gamma \sum_{0 \le j,k \le p-1} f(j,k) u^j v^k$$

to the $\mathcal{A}(\mathbb{Z}_p \times \mathbb{Z}_p, \tau_i)$-YBE for $i = 1, 2$ and 3.

We could not find any non-trivial unitary solutions that do not factor as $f(j,k) = f_u(j) f_v(k)$ after applying the symmetries of Sect. 3.4, and can verify computationally that all solutions factor as products of Gaussian-type solutions in the case for $p = 3$. Thus we focus on such solutions. All of the solutions that follow will have finite braid group image when properly normalized to be unitary, which can be easily verified using the finiteness of the Gaussian representation images. The eigenvalues of $r = \sum_{0 \le j,k \le p-1} q^{j^2 \epsilon x k^2} u^j v^k$ for $q = \mathrm{e}^{2\pi \mathrm{i}/p}$ and $\epsilon = \pm 1$ in any faithful representation of $\mathcal{A}_2(G, \tau_i)$ are

$$\lambda_{\epsilon,x}(s,t) = \left(\sum_j q^{j^2+sj}\right)\left(\sum_k q^{\epsilon x k^2 + tk}\right).$$

Up to an overall normalization factor, the eigenvalues and their multiplicities can be computed using standard Gaussian quadratic form techniques, and only depend on the sign $\pm$ and whether -1 and x are squares or non-squares modulo p. We have that the multi-set $[\lambda_{\epsilon,x}(s,t)]$ has

(1) 1 with multiplicity 1 and $\mathrm{e}^{2\pi \mathrm{i} j/p}$ with multiplicity $p + 1$ for each $1 \le j \le p - 1$ when $(\epsilon, \left(\frac{-1}{p}\right), \left(\frac{x}{p}\right)) \in \{(1,-1,1),\ (-1,-1,-1), (1,1,-1),\ (-1,1,-1)\}$ and

(2) 1 with multiplicity $2p-1$ and $e^{2\pi i j/p}$ with multiplicity $p-1$ for each $1 \le j \le p-1$ when $(\varepsilon, (\frac{-1}{p}), (\frac{x}{p})) \in \{(1,-1,-1),(-1,-1,1),(1,1,1),(-1,1,1)\}$.

4.2.1 Elliptic Symmetric Case

First, consider the case A_1. We can deduce some solutions

$$t(u,v) = \sum_{0\le j,k\le p-1} F(j,k)u^j v^k$$

to the $\mathcal{A}_n(\mathbb{Z}_p \times \mathbb{Z}_p, \tau_i)$-YBE from the Gaussian solutions. Indeed, if $f, h : \mathbb{Z}_p \to \mathbb{C}$ and are such that $r(u) = \sum_{j=0}^{p-1} f(j)u^j$ and $s(v) = \sum_{j=0}^{p-1} h(j)v^j$ are solutions to the $\mathcal{A}_n(\mathbb{Z}_p)$-YBE, then setting $t(u,v) = r(u)s(v)$ we can easily verify

$$t_1t_2t_1 = (r_1s_1)(r_2s_2)(r_1s_1) = (r_1r_2r_1)(s_1s_2s_1) = t_2t_1t_2$$

since $r_i := r(u_i)$ commutes with $s_i := s(v_j)$. If both f and h correspond to Gaussian solutions, we may rescale u and v independently followed by complex conjugation to assume that $f(j) = q^{j^2}$ and $h(k) = q^{\pm k^2}$. The choice of sign indeed gives two distinct solutions. The additional symmetry that we have not used comes from the group of τ_1-invariant G-automorphism, i.e., $\{X \in \mathrm{GL}_2(\mathbb{Z}_p) : X^T A_1 X = A_1\}$, which is a group of order $2(p-1)$ in this case.

4.2.2 Skew-Symmetric Case

Next we consider the case A_2. Suppose that our solution

$$t(u,v) = \sum_{0\le j,k\le p-1} F(j,k)u^j v^k$$

factors as $t(u,v) = r(u)s(v)$ where $r(u) = \sum_{j=0}^{p-1} f(j)u^j$ and $s(v) = \sum_{j=0}^{p-1} h(j)v^j$ are solutions to the $\mathcal{A}_n(\mathbb{Z}_p)$-YBE. Again, setting $r_i = r(u_i)$ and $s_i = s(v_i)$ we observe that $[r_1, r_2] = 1$ and $[s_1, s_2] = 1$, so that $t_1t_2t_1 = r_1s_1r_2s_2r_1s_1 = (s_1r_2s_1)(r_1s_2r_1)$. From this we deduce that we should take $r(u) = s(u)$ and $r(v) = s(v)$, i.e., $h = f$ so that $t(u,v) = r(u)r(v)$. Now we can use symmetry to choose $f(j) = h(j) = q^{j^2}$. In this case, the group of automorphisms of $\mathbb{Z}_p \times \mathbb{Z}_p$ that preserve α_2 is $\mathrm{SL}_2(\mathbb{Z}_p)$, a group of order $(p^2 - p)(p+1)$.

4.2.3 Hyperbolic Symmetric Case

As the details are similar to the elliptic symmetric case, we are content to provide the factored solution

$$t(u,v) = \sum_{0\le j,k\le p-1} q^{j^2 \pm xk^2} u^j v^k.$$

It is an easy exercise to show that this is the unique factorizable solution up to symmetries. The group of automorphisms of $\mathcal{A}(G, \tau_3)$ that preserve α_3 has order $2(p+1)$.

4.3 Non-commutative Cases

To illustrate our methods for non-abelian groups, we first apply them to the case of the symmetric group S_3 and the algebra $\mathcal{A}_n(Q_8)$ from the introduction.

4.3.1 Symmetric Group S_3

For S_3, the bihomomorphisms $\alpha : S_3 \times S_3 \to \mathbb{Z}_m$ are determined by the abelianization $\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_m$ so that we may take $m = 2$. In particular, we have the following description of $\mathcal{A}_n(S_3, \tau)$ for the non-trivial choice $\alpha((1\ 2), (1\ 2)) = 1$. We take generators $u = (1\ 2)$ and $v = (1\ 2\ 3)$ for S_3 and corresponding generators of $\mathcal{A}_n(S_3, \tau)$ $u_1, v_1, \dots, u_{n-1}, v_{n-1}$ with relations:

- $u_i v_i = v_i^2 u_i$ and $u_i^2 = v_i^3 = 1$ (S_3 relations) and
- $u_i u_{i+1} = -u_{i+1} u_i$ and $v_i v_j = v_j v_i$ for all i, j, and
- $u_i v_j = v_j u_i$ for $i \neq j$.

We seek (invertible) solutions $r = \gamma(1 + au + bv + cv^2 + duv + euv^2) \in \mathbb{C}[S_3]$ to the $\mathcal{A}(S_3, \tau)$-YBE, where γ is a normalization factor chosen to give r finite order. Appendix contains the details of the computation, the upshot of which is that $b = c = 0$ is a consequence of invertibility and to have solutions r that are unitary with respect to the standard $*$-operation we should take $\gamma = \frac{1}{1+\mathrm{i}}$ and $(a, d, e) = (\mathrm{i}x, \mathrm{i}y, \mathrm{i}z)$ with $(x, y, z) \in \mathbb{R}^3$ on the intersection of the surface given by $xy + xz + yz = 0$ with the unit sphere $x^2 + y^2 + z^2 = 1$. Since $(x + y + z)^2 = 1$ modulo the ideal generated by these two polynomials we conclude that the solutions are the points on the intersection of the two planes $(x + y + z) = \pm 1$ with the unit sphere.

In all cases, we find that $r^4 = 1$, with eigenvalues $1, -\mathrm{i}$. This suggests that this representation is related to the Ising theory, see [15].

4.3.2 Quaternionic Algebra $\mathcal{A}_n(Q_8)$

Recall the algebra $\mathcal{A}_n(Q_8)$ described in the introduction, generated by u_i, v_i satisfying

(1) $u_i^2 = v_i^2 = -1$ for all i,
(2) $[u_i, v_j] = -1$ if $|i - j| < 2$,
(3) $[u_i, u_j] = [v_i, v_j] = 1$,
(4) $[u_i, v_j] = 1$ if $|i - j| \geq 2$.

From the relations, one deduces that for each i the pair u_i, v_i generates a group isomorphic to Q_8. Notice, however, that $\langle u_i, v_i \rangle \cap \langle u_i, v_i \rangle = \{\pm 1\}$ so that $\mathcal{A}_n(Q_8)$ is not a twisted tensor product of group algebras; indeed, it is not $\mathbb{C}[Q_8]^{\otimes n-1}$ as a vector space. The algebra is closely related to group algebras, in at least two ways. First, suppose that $Q_8 = \langle u, v \rangle$, where $uv = zvu$ with $u^2 = v^2 = z$ central of order 2. Then we may define the quotient $\mathcal{T} = \mathbb{C}[Q_8]/\langle z+1\rangle$ and then $\mathcal{A}(Q_8)$ above is a twisted tensor product of $n-1$ copies of $\mathcal{T}$ with the tensor product twist given as above, determined by $\tau(u,v) = -1$ and $\tau(u,u) = \tau(v,v) = 1$ since $u_i v_{i+1} = -1 v_{i+1} u_i$.

Alternatively, we can consider the twisted group algebra $\mathbb{C}^\nu[\mathbb{Z}_2 \times \mathbb{Z}_2]$ associated with the cocycle $\nu \in Z^2(\mathbb{Z}_2 \times \mathbb{Z}_2, U(1))$ defined by

- $\nu((1,0),(0,1)) = -\nu((0,1),(1,0)) = 1$,
- $\nu((1,0),(1,0)) = \nu((0,1),(0,1)) = -1$

with multiplication in $\mathbb{C}^\nu[\mathbb{Z}_2 \times \mathbb{Z}_2]$ given by $g \star_\nu h = \nu(g,h)gh$ for $g,h \in \mathbb{Z}_2 \times \mathbb{Z}_2$. Then

$$\mathcal{A}_n(Q_8) = \mathbb{C}^\nu[\mathbb{Z}_2 \times \mathbb{Z}_2] \otimes_\tau \mathbb{C}^\nu[\mathbb{Z}_2 \times \mathbb{Z}_2] \otimes_\tau \cdots \otimes_\tau \mathbb{C}^\nu[\mathbb{Z}_2 \times \mathbb{Z}_2],$$

where τ is the twisting corresponding to the relations above.

We look for $\mathcal{A}(Q_8)$-YBOs of the form $r = 1 + au + bv + cuv$. We find 8 non-trivial solutions namely $a,b,c \in \{\pm\frac{1}{2}\}$, normalized to a unitary solution. These are all related by symmetry since we may rescale $a \to -a$ and $b \to -b$ independently, permute the a, b, c freely using the fact that τ is invariant under permuting u, v, uv and inversion corresponds to simultaneously changing all signs. The Magma code is found in Appendix.

5 Categorical Connections

The class of weakly integral modular categories, i.e., those for which $\mathrm{FPdim}(\mathcal{C}) \in \mathbb{Z}$ is not well understood. However, a long-standing question [12, Question 2] asks if the class of weakly integral fusion categories coincides with the class of weakly group-theoretical fusion categories, i.e., those that are Morita equivalent to a nilpotent fusion category. Recently Natale [33] proved that any weakly group-theoretical modular category is a G-gauging of either a pointed modular category (all simple objects are invertible) or a Deligne product of a pointed modular category and an Ising-type modular category [10, Appendix B]. These latter categories are well known to have property F, which reduces the verification of the property F conjecture for weakly integral braided fusion categories to verifying that G-gauging preserves property F and that weak integrality is equivalent to weak group-theoreticity. In fact, after this article was submitted, the preprint [22] appeared, which proves that weakly group-theoretical braided fusion categories has property F. Nonetheless, understanding the precise connection between the braid group representations associated with a category $\mathcal{C}$ and its G-gaugings is an interesting problem.

The difficulty with verifying property F for a given category is that one rarely has a sufficiently explicit description of the braid group representations ρ_X associated with an object $X \in \mathcal{C}$. The braiding $c_{X,X}$ on $X \otimes X$ provides a map $\mathbb{C}\mathcal{B}_n \to \mathrm{End}(X^{\otimes n})$ which then acts on each $\mathrm{Hom}(Y, X^{\otimes n})$ for simple objects Y by composition, but an explicit basis for $\mathrm{Hom}(Y, X^{\otimes n})$ is lacking. In all cases where the property F

conjecture has been verified for a weakly integral braided fusion category [13, 16, 27, 32, 36], the first step is a concrete description of the centralizer algebras $\mathrm{End}(X^{\otimes n})$, and the corresponding modules $\mathrm{Hom}(Y, X^{\otimes n})$ which are obtained by studying a specific realization of $\mathcal{C}$, as a subquotient category of representations of a quantum group, for example. From this description, one extracts a sufficiently explicit $\mathcal{B}_n$ representation to facilitate the verification of property F.

One approach to a uniform proof of (one direction of) the property F conjecture is to understand the connection between the centralizer algebras of pointed modular categories and those of its G-gaugings. Pointed modular categories are in one to one correspondence with metric groups, i.e., pairs (A, Q), where A is a finite abelian group and Q is a non-degenerate quadratic form on A. We denote by $\mathcal{C}(A, Q)$ the corresponding modular category. Pointed modular categories and their products with Ising-type categories are well known to have property F [32]. Thus, if we could prove G-gauging preserves property F, then this direction of the property F conjecture would reduce to [12, Question 2].

For a general mathematical reference on G-gaugings, see [9], the notation of which we will adopt here. Let A be an abelian group, and Q a non-degenerate quadratic form on A, and $\mathcal{C}(A, Q)$ the corresponding pointed modular category, with twists given by $\theta_a = Q(a)$ and braiding by $c_{a,b} = \beta(a, b)\sigma$, where σ is the usual flip map and $\beta(a, b) := Q(a + b) - Q(a) - Q(b)$. A G symmetry of $\mathcal{C}(A, Q)$ is a group homomorphism $\rho : G \to \mathrm{Aut}^{\mathrm{br}}_{\otimes}(\mathcal{C}(A, Q)) \cong O(A, Q)$. Provided certain cohomological obstructions vanish one may construct (potentially several) modular categories by *gauging* the G symmetry. In the case of an elementary abelian p-group for p an odd prime all of the obstructions vanish by [11, Theorem 6.1].

We expect there to be a connection between the algebras $\mathcal{A}_n(G, \tau)$ described above and the H-gaugings of pointed modular categories, i.e., categories $\mathcal{C}(G, Q)^{\times, H}_{H}$, where $H \subset \mathrm{Aut}^{\mathrm{br}}_{\otimes}(\mathcal{C}(G, Q))$. Indeed, in the case $G = \mathbb{Z}_p$ and $H = \mathbb{Z}_2$ acting by inversion, these categories are called *p-metaplectic* and we have the following, using results of [2, 23, 28, 38] and some careful adjustment of parameters:

Theorem 5.1 *Let $\mathbb{Z}_2$ act on $\mathcal{C} := \mathcal{C}(\mathbb{Z}_p, Q)$ by inversion, and let $\mathcal{D} = \mathcal{C}^{\times, \mathbb{Z}_2}_{\mathbb{Z}_2}$ be any of the corresponding gaugings, and X a simple object of dimension $\sqrt{p}$. Then*

$$\mathrm{End}(X^{\otimes n}) \cong \langle u_1 + u_1^{-1}, \dots, u_{n-1} + u_{n-1}^{-1} \rangle \subset \mathcal{A}_n(\mathbb{Z}_p).$$

In fact, this result is key to verifying the property F conjecture for p-metaplectic categories.

A similar relationship exists between a $\mathbb{Z}_3$-gauging of the so-called *three fermion* theory $\mathcal{C}(\mathbb{Z}_2 \times \mathbb{Z}_2, Q)$ where $Q(x) = -1$ for $x \neq (0, 0)$ and the algebra $\mathcal{A}_n(Q_8)$ described above. In this case, $\mathcal{C}(\mathbb{Z}_2 \times \mathbb{Z}_2, Q)^{\times, \mathbb{Z}_3}_{\mathbb{Z}_3} \cong \mathrm{SU}(3)_3$ for one choice of $\mathbb{Z}_3$-gauging, where the action of $\mathbb{Z}_3$ at the level of object is given by cyclic permutation of the three non-trivial simple objects (see [9]). Now for a generating 2-dimensional object X it is shown in [35] that the subalgebra $\mathcal{C}_n(Q_8)$ of $\mathcal{A}_n(Q_8)$ generated by $(u_i + v_i + u_i v_i)$ for $1 \leq i \leq n - 1$ is isomorphic to $\mathrm{End}(X^{\otimes n})$, which is also isomorphic to a quotient of the Hecke algebra specialization $\mathcal{H}_n(3, 6)$. The reader will also notice that the $\mathbb{Z}_3$-action on Q_8 given by cyclic permutation of u, v

and uv lifts to an automorphism of $\mathcal{A}_n(Q_8)$ and $\mathcal{C}_n(Q_8)$ is the fixed point subalgebra. Finally, we remark that the image of the braid group representation on $\mathrm{End}(X^{\otimes n})$ is finite—it factors through the representations found above: $\sigma_i \mapsto (1 + u_i + v_i + u_i v_i)$.

This inspires the following:

Principle 5.2 If $G \subset \mathrm{Aut}_{\otimes}^{\mathrm{br}}(\mathcal{C}(A, Q))$ is a gaugeable action on $\mathcal{C}(A, Q)$ then there is a (quotient of an) iterated twisted tensor product $\mathcal{A}_n(A, \tau)$ of $\mathbb{C}[A]$ and an object $X \in \mathcal{C}(A, Q)_G^{\times, G}$ so that $\mathrm{End}(X^{\otimes n})$ is isomorphic to the fixed point subalgebra $\mathcal{C}_n(A, \tau)$ of the automorphism induced by the action of G on A. Moreover there is an $\mathcal{A}(A, \tau)$-YBO r supported in $\mathcal{C}_n(A, \tau)$ such that the $\mathcal{B}_n$ representation on $\mathrm{End}(X^{\otimes n})$ factors through the $\mathcal{B}_n$ representation defined by r.

We do not have a general proof of this principle for all groups. In the case of $\mathbb{Z}_p \times \mathbb{Z}_p$ with $\mathbb{Z}_2$ acting by inversion, we give some compelling evidence for this principle.

Now suppose that $|A| = m = 2k + 1$ is odd and $\rho : \mathbb{Z}_2 \to \mathrm{Aut}_{\otimes}^{\mathrm{br}}(\mathcal{C}(A, Q))$ is the action by inversion. The $\mathbb{Z}_2$-extensions are Tambara–Yamagami categories $TY(A, \chi, \pm)$ [39], and their equivariantizations are found in [19] (see also [25]). There are two distinct $\mathbb{Z}_2$-gaugings $\mathcal{D}_\pm := \mathcal{C}(A, Q)_{\mathbb{Z}_2}^{\times, \mathbb{Z}_2}$ of the inversion action ρ. Each modular category $\mathcal{D}_\pm$ has dimension $4|A|$. It has the following simple objects:

- two invertible objects, $\mathbf{1} = X_+$ and X_-,
- $\frac{m-1}{2}$ two-dimensional objects Y_a, $a \in A - \{0\}$ (with $Y_{-a} = Y_a$),
- two $\sqrt{m}$-dimensional objects Z_l, $l \in \mathbb{Z}_2$.

The fusion rules of $\mathcal{D}_\pm$ are given by

$$\begin{aligned}
&X_- \otimes X_- = X_+, && X_\pm \otimes Y_a = Y_a, && X_+ \otimes Z_l = Z_l,\\
&X_- \otimes Z_l = Z_{l+1}, && Y_a \otimes Y_b = Y_{a+b} \oplus Y_{a-b}, && Y_a \otimes Y_a = X_+ \oplus X_- \oplus Y_{2a},\\
&Y_a \otimes Z_l = Z_0 \oplus Z_1, && Z_l \otimes Z_l = X_+ \oplus \left(\bigoplus_a Y_a \right), && Z_l \otimes Z_{l+1} = X_- \oplus \left(\bigoplus_a Y_a \right),
\end{aligned}$$

where $a, b \in A$ $(a \neq b)$ and $l \in \mathbb{Z}_2$. All objects of $\mathcal{D}_\pm$ are self-dual. Here the addition $a + b$ takes place in A. We see that X_- must be a boson, in the sense that the subcategory $\langle X_- \rangle \cong \mathrm{Rep}(\mathbb{Z}_2)$ as a braided fusion category. Indeed, as $\mathcal{D}_\pm$ is a non-degenerate braided fusion category it is faithfully $\mathbb{Z}_2$-graded with the trivial component having the $\frac{m+1}{2}$ simple objects $Y_a, X_\pm$, and non-trivial component having the two simple objects Z_l.

In particular, the algebras $\mathrm{End}(Z_0^{\otimes n}) \subset \mathrm{End}(Z_0^{\otimes n+1})$ have the Bratteli diagram of Fig. 3, where we have labeled the objects Y_a by an arbitrary choice Y_i for $1 \leq i \leq k$.

The categories $\mathcal{D}_\pm$ described above for the group $G = \mathbb{Z}_p \times \mathbb{Z}_p$ were explored in [19], and found to be non-group-theoretical in one case and group-theoretical in the other. For the case $p = 3$, the group-theoretical cases are equivalent to $\mathrm{Rep}(D^\omega S_3)$ where ω is a 3-cocycle on S_3. Up to equivalence there is one non-trivial choice for ω.

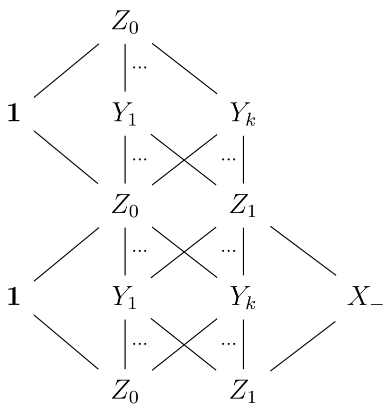

Fig. 3 Bratteli diagram for $\mathcal{C}(A,Q)_{\mathbb{Z}_2}^{\times,\mathbb{Z}_2}$ for $|A|$ odd

We expect that:

(1) $\mathrm{End}(Z^{\otimes n}) \cong \mathcal{C}_n(\mathbb{Z}_p \times \mathbb{Z}_p, \tau)$ for some choice of τ.
(2) Under the above isomorphisms the image of the braid group generators are described by the $\mathcal{A}(\mathbb{Z}_p \times \mathbb{Z}_p, \tau)$-YBOs determined above.

The two pieces of evidence are as follows:

(1) The Bratteli diagrams for $\mathrm{End}(Z_0^{\otimes n})$ and $\mathcal{C}_n(\mathbb{Z}_p \times \mathbb{Z}_p, \tau_i)$ coincide and
(2) The eigenvalue profile of c_{Z_0,Z_0} and $\sum_{j,k} q^{j^2 \pm xk^2} u^j v^k$ coincide, for some choice of $\pm x$ where x is either 1 or any non-square modulo p.

The S and T matrices of all 4 of these categories are given in [19], as they are equivalent to $\mathbb{Z}_2$-equivariantizations of Tambara–Yamagami categories. From [6, Prop. 2.3] we may deduce the eigenvalues of the braiding for the object Z_0 of dimension p.

5.1 A Special Case: $p = 3$

Let $q = e^{2\pi i/3}$. The two group-theoretical categories $\mathrm{Rep}(D^\omega S_3)$ can be obtained by gauging the $\mathbb{Z}_2$ inversion symmetry on $\mathcal{C}(\mathbb{Z}_3 \times \mathbb{Z}_3, Q_1)$ where $Q_2(x,y) = q^{x^2-y^2}$ is hyperbolic. For the elliptic quadratic form $Q_2(x,y) = q^{x^2+y^2}$, the two inequivalent $\mathbb{Z}_2$-gaugings are non-group-theoretical. Each of these categories can be tensor generated by a simple object Z of dimension 3. The two group theoretical-categories $\mathrm{Rep}(D^\omega G)$ have property F [13], but it is currently open whether the non-group-theoretical cases have property F.

On the other hand, we can completely determine all unitary solutions to the $\mathcal{A}(\mathbb{Z}_3 \times \mathbb{Z}_3, \tau)$-YBE for the bicharacters τ associated with the 3 matrices A_1, A_2 and A_3, up to the usual symmetries in Example 4.2.

One more piece of circumstantial evidence is that the results of [23] show that the braid group representations associated with a modular category only nominally depend on the finer structures such as the associativity constraints: for odd primes p, the images of the braid group representations for p-metaplectic modular categories are projectively equivalent. Since the property F conjecture depends only on the dimensions of objects, which are determined by fusion rules, it would perhaps not be so surprising if the fusion rules essentially determine the braid group images. A related result in [34] implies that the images of the braid group representations associated with different modular categories with the same underlying fusion category are either all finite or all infinite.

6 Conclusions

In this paper, we have unified some explicit constructions of braid group representations that come from finite groups in a fairly direct way. We have also provided strong evidence that twisted tensor products of group algebras simplify the analysis of gaugings of pointed modular categories. In particular, the data describing $\mathcal{A}(A,\tau)$-YBOs, simply a function on A, is much simpler than the construction of the R-matrices of a gauged modular tensor category. However, beyond the Gaussian case, the connection between the two braid group representations remains at the level of Bratteli diagrams and eigenvalues.

It would be of great interest to formulate precise intertwining operators between braid group representations in centralizer algebras of gaugings of pointed modular tensor categories and those from $\mathcal{A}(A,\tau)$-YBOs. This was accomplished with great difficulty in the Gaussian case [36]. Ideally, we would like to find a uniform framework generalizing this construction to all gaugings of pointed modular tensor categories.

Appendix: Computations for $G = S_3$ and $\mathcal{A}_n(Q_8)$

In what follows we provide some details classifying solutions to the $\mathcal{A}(S_3,\tau)$ and $\mathcal{A}(Q_8)$-YBE.

Symmetric Group S_3

We let u, v be the generators for S_3 with $u^2 = v^3 = 1$ and $uvu = v^2$. For example, we could take $u = (1\ 2)$ and $v = (1\ 2\ 3)$. By the theory above, we initialize with the following Magma code to find conditions on $a, b, c, d, e \in \mathbb{C}$ so that $r = 1 + au + bv + cv^2 + duv + euv^2$ is an $\mathcal{A}(S_3,\tau)$-YBO.

```
F<w>:=CyclotomicField(4);
R<u1,v1,v2,u2,a,b,c,d,e>:=FreeAlgebra(F,9);
f:=function(x,y,z)
return x*y-z*y*x;
end function;
X:=[u1,v1,u2,v2,a,b,c,d,e];
B:=[u1^2-1,v1^3-1,u2^2-1,v2^3-1,u1*v1-v1^2*u1,u2*v2-v2^2*u2] cat
[f(u1,u2,-1),f(v1,v2,1),f(u1,v2,1),f(u2,v1,1)] cat
[f(a,x,1): x in X] cat
[f(c,x,1): x in X] cat
[f(b,x,1): x in X] cat
[f(e,x,1): x in X] cat
[f(d,x,1): x in X];
I:=ideal<R|B>;
R1:=1+a*u1+b*v1+c*v1^2+d*u1*v1+e*u1*v1^2;
R2:=1+a*u2+b*v2+c*v2^2+d*u2*v2+e*u2*v2^2;
NormalForm(R1*R2*R1-R2*R1*R2,I);
```

The ideal of solutions is generated by the coefficients of the monomials in u_i, v_j. We enforce invertibility of r by assuming the determinant of the image of r under the faithful S_3 representation on $\mathbb{C}^3$ is non-zero. The output of the Gröbner basis is the following set of polynomials:

$$\{c, b, e(a^2 + d^2 + e^2 + 1), ad + ae + de, a^3 + a^2e + 2ae^2 + de^2 + e^3 + a + e,$$
$$- a^2e + ae^2 + d^3 + 2de^2 + d\}.$$

Notice that $c = b = 0$, in all cases. If $e = 0$ then $ad = 0$, and $a^3 + a = d^3 + d = 0$, which are degenerate solutions of the form $1 + xu$ that can be obtained from $\mathbb{Z}_2$ (see [15]).

If $e \neq 0$, we find that e is a free parameter, and the following code shows that we may normalize to get $r^4 = 1$. There is a 1-parameter family of solutions for (a, d, e). Moreover, one sees that if we require a unitary solution each of a, d, e should be pure imaginary, and consequently the equation $a^2 + d^2 + e^2 + 1 = 0$ implies that $(a/\mathrm{i}, d/\mathrm{i}, e/\mathrm{i})$ is a point on the unit sphere. Geometrically, this is the intersection of the unit sphere with the surface given by $xy + xz + yz = 0$.

```
F<w>:=CyclotomicField(4);
R<u1,v1,v2,u2,a,d,e>:=FreeAlgebra(F,7);
f:=function(x,y,z)
return x*y-z*y*x;
end function;
X:=[u1,v1,u2,v2,a,d,e];
B:=[u1^2-1,v1^3-1,u2^2-1,v2^3-1,u1*v1-v1^2*u1,u2*v2-v^2*u2] cat
[f(u1,u2,-1),f(v1,v2,1),f(u1,v2,1),f(u2,v1,1)] cat
[f(a,x,1): x in X] cat
[f(e,x,1): x in X] cat
[f(d,x,1): x in X] cat [a^4+2*a^3*e+3*a^2*e^2+2*a*e^3+e^4+a^2+2*a*e+e^2,
a^3+a^2*d+2*a^2*e+a*e^2+e^3+a+e, a*d+a*e+d*e, (a^2+d^2+e^2+1)];
```

```
I:=ideal<R|B>;
R1:=(1+a*u1+d*u1*v1+e*u1*v1^2)/(1+w);
R1i:=(1-(a*u1+d*u1*v1+e*u1*v1^2))/(1-w);
R2:=(1+a*u2+d*u2*v2+e*u2*v2^2)/(1+w);
NormalForm(R1*R2*R1-R2*R1*R2,I);
NormalForm(R1^4,I);
NormalForm(R1i*R1,I);
```

Quaterionic Algebra $\mathcal{A}_n(Q_8)$

For the case of the algebra $\mathcal{A}_n(Q_8)$, we use Magma to classify $\mathcal{A}(Q_8)$-YBOs. The following is the final code, where the last polynomial relations are the coefficients obtained from an initial run of the normal form command on an initial run (i.e., without the last set of relations). One finds that the non-trivial solutions for (a, b, c) are all ± 1, so that if we want unitary solutions, the inverse of R1 is of the form given as R1i since $u^* = u^{-1} = -u$, etc. We conclude that all unitary solutions are equivalent to the choice $(a, b, c) = (1, 1, 1)$.

```
F<w>:=CyclotomicField(12);
R<u1,v1,v2,u2,a,b,c>:=FreeAlgebra(F,7);
f:=function(x,y,z)
return x*y-z*y*x;
end function;
g:=function(a)
return a^2+1;
end function;
X:=[u1,v1,v2,u2,a,b,c];
Y:=[u1,v1,v2,u2];
B:=[g(x):x in Y] cat
[f(u1,v1,-1),f(u2,v2,-1)] cat
[f(u1,u2,1),f(v1,v2,1),f(u1,v2,-1),f(u2,v1,-1)]
cat [f(a,x,1): x in X]
cat [f(b,x,1): x in X]
cat [f(c,x,1): x in X]
cat [-2*b*a^2+ 2*c^2*b,2*b^2*a-2*c^2*a,
c*a^2+c*b^2-c^3-c,4*c*b^2- 2*c^3-2*c,
a^3-2*c^2*a+a,b^3-2*c^2*b+b];
I:=ideal<R|B>;
R1:=(1+a*u1+b*v1+c*u1*v1)/2;
R2:=(1+a*u2+b*v2+c*u2*v2)/2;
R1i:=1/2-(a*u1+b*v1+c*u1*v1)/2;
NormalForm(R1*R2*R1-R2*R1*R2,I);
NormalForm(R1*R1i,I);
```

References

1. Andruskiewitsch, N., Schneider, H.-J.: Pointed Hopf algebras. In: New Directions in Hopf Algebras, Math. Sci. Res. Inst. Publ., vol. 43, pp. 1–68. Cambridge University Press, Cambridge (2002)

2. Ardonne, E., Cheng, M., Rowell, E.C., Wang, Z.: Classification of metaplectic modular categories. J. Algebra **466**, 141–146 (2016)
3. Bardakov, V.G., Bellingeri, P.: On representations of braids as automorphisms of free groups and corresponding linear representations. In: Knot Theory and Its Applications, Contemp. Math., vol. 670, pp. 285–298. American Mathematical Society, Providence (2016)
4. Bigelow, S.: Braid groups are linear. J. Am. Math. Soc. **14**(2), 471–486 (2001)
5. Birman, J.S., Wenzl, H.: Braids, link polynomials and a new algebra. Trans. Am. Math. Soc. **313**(1), 249–273 (1989)
6. Bonderson, P., Delaney, C., Galindo, C., Rowell, E.C., Tran, A., Wang, Z.: On invariants of modular categories beyond modular data. J. Pure Appl. Algebra **223**(9), 4065–4088 (2019)
7. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. Computational Algebra and Number Theory (London, 1993). J. Symb. Comput. **24**(3–4), 235–265 (1997)
8. Cap, A., Schichl, H., Vanžura, J.: On twisted tensor products of algebras. Commun. Algebra **23**(12), 4701–4735 (1995)
9. Cui, S.X., Galindo, C., Plavnik, J.Y., Wang, Z.: On gauging symmetry of modular categories. Commun. Math. Phys. **348**(3), 1043–1064 (2016)
10. Drinfeld, V., Gelaki, S., Nikshych, D., Ostrik, V.: On braided fusion categories. I. Selecta Math. (N.S.) **16**(1), 1–119 (2010)
11. Etingof, P., Galindo, C.: Reflection fusion categories. J. Algebra **516**, 172–196 (2018)
12. Etingof, P., Nikshych, D., Ostrik, V.: Weakly group-theoretical and solvable fusion categories. Adv. Math. **226**(1), 176–205 (2011)
13. Etingof, P., Rowell, E., Witherspoon, S.: Braid group representations from twisted quantum doubles of finite groups. Pac. J. Math. **234**(1), 33–41 (2008)
14. Formanek, E., Lee, W., Sysoeva, I., Vazirani, M.: The irreducible complex representations of the braid group on n strings of degree $\leq n$. J. Algebra Appl. **2**(3), 317–333 (2003)
15. Franko, J.M., Rowell, E.C., Wang, Z.: Extraspecial 2-groups and images of braid group representations. J. Knot Theory Ramif. **15**(4), 413–427 (2006)
16. Freedman, M.H., Larsen, M., Wang, Z.: A modular functor which is universal for quantum computation. Commun. Math. Phys. **227**(3), 605–622 (2002)
17. Galindo, C., Hong, S.-M., Rowell, E.C.: Generalized and quasi-localizations of braid group representations. Int. Math. Res. Not. IMRN **2013**(3), 693–731 (2013)
18. Galindo, C., Rowell, E.C.: Braid representations from unitary braided vector spaces. J. Math. Phys. **55**(6), 061702 (2014). https://doi.org/10.1063/1.4880196
19. Gelaki, S., Naidu, D., Nikshych, D.: Centers of graded fusion categories. Algebra Number Theory **3**(8), 959–990 (2009)
20. Goldschmidt, D.M., Jones, V.F.R.: Metaplectic link invariants. Geom. Dedicata **31**(2), 165–191 (1989)
21. Goodman, F.M., de la Harpe, P., Jones, V.F.R.: Coxeter Graphs and Towers of Algebras. Mathematical Sciences Research Institute Publications, vol. 14. Springer, New York (1989). https://doi.org/10.1007/978-1-4613-9641-3
22. Green, J., Nikshych, D.: On the braid group representations coming from weakly group-theoretical fusion categories, preprint. arXiv:1911.02633
23. Gustafson, P., Rowell, E., Ruan, Y.: Metaplectic categories, gauging and property F. Tohoku Math. J. **(to appear)**. arXiv:1808.00698
24. Hietarinta, J.: All solutions to the constant quantum Yang–Baxter equation in two dimensions. Phys. Lett. A **165**(3), 245–251 (1992)
25. Izumi, M.: The structure of sectors associated with Longo–Rehren inclusions. II: Examples. Rev. Math. Phys. **13**(5), 603–674 (2001)
26. Jara Martínez, P., López Peña, J., Panaite, F., van Oystaeyen, F.: On iterated twisted tensor products of algebras. Int. J. Math. **19**(9), 1053–1101 (2008)
27. Jones, V.F.R.: Braid groups, Hecke algebras and type II_1 factors. In: Geometric Methods in Operator Algebras (Kyoto, 1983), Pitman Res. Notes Math. Ser., vol. 123, pp. 242–273. Longman Sci. Tech., Harlow (1986)
28. Jones, V.F.R.: Notes on subfactors and statistical mechanics. In: Braid Group, Knot Theory and Statistical Mechanics, Adv. Ser. Math. Phys., vol. 9, pp. 1–25. World Sci. Publ., Teaneck (1989)
29. Jones, V.F.R.: On knot invariants related to some statistical mechanical models. Pac. J. Math. **137**(2), 311–334 (1989)
30. Larsen, M.J., Rowell, E.C.: An algebra-level version of a link-polynomial identity of Lickorish. Math. Proc. Camb. Philos. Soc. **144**(3), 623–638 (2008)

31. Murakami, J.: The Kauffman polynomial of links and representation theory. Osaka J. Math. **24**(4), 745–758 (1987)
32. Naidu, D., Rowell, E.C.: A finiteness property for braided fusion categories. Algebr. Represent. Theory **14**(5), 837–855 (2011)
33. Natale, S.: The core of a weakly group-theoretical braided fusion category. Int. J. Math. **29**(2), 1850012, 23 pp. (2018)
34. Nikshych, D.: Classifying braidings on fusion categories. In: Tensor Categories and Hopf Algebras, Contemp. Math., vol. 728, pp. 155–167. American Mathematical Society, Providence (2019)
35. Rowell, E.C.: A quaternionic braid representation (after Goldschmidt and Jones). Quantum Topol. **2**(2), 173–182 (2011)
36. Rowell, E.C., Wang, Z.: Localization of unitary braid group representations. Commun. Math. Phys. **311**(3), 595–615 (2012)
37. Rowell, E.C., Wang, Z.: Mathematics of topological quantum computing. Bull. Am. Math. Soc. (N.S.) **55**(2), 183–238 (2018)
38. Rowell, E.C., Wenzl, H.: $SO(N)_2$ braid group representations are Gaussian. Quantum Topol. **8**(1), 1–33 (2017)
39. Tambara, D., Yamagami, S.: Tensor categories with fusion rules of self-duality for finite abelian groups. J. Algebra **209**(2), 692–707 (1998)
40. Tuba, I., Wenzl, H.: Representations of the braid group B_3 and of $SL(2, Z)$. Pac. J. Math. **197**(2), 491–510 (2001)
41. Turaev, V., Wenzl, H.: Quantum invariants of 3-manifolds associated with classical simple Lie algebras. Int. J. Math. **4**(2), 323–358 (1993)
42. Turaev, V.: Faithful linear representations of the braid groups. Séminaire Bourbaki, vol. 1999/2000. Astérisque (276), 389–409 (2002)
43. Waterhouse, W.C.: The number of congruence classes in $M_n(\mathbf{F}_q)$. Finite Fields Appl. **1**(1), 57–63 (1995)