JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 29, Number 3, July 2016, Pages 857–881
http://dx.doi.org/10.1090/jams/842
Article electronically published on July 21, 2015

RANK-FINITENESS FOR MODULAR CATEGORIES

PAUL BRUILLARD, SIU-HUNG NG, ERIC C. ROWELL, AND ZHENGHAN WANG

1. Introduction

Modular categories are intricate organizing algebraic structures appearing in a variety of mathematical subjects including topological quantum field theory [52], conformal field theory [38], representation theory of quantum groups [1], von Neumann algebras [24], and vertex operator algebras [29]. They are fusion categories with additional braiding and pivotal structures [1,23,52] satisfying a non-degeneracy condition. These extra structures endow them with some "abelian-ness" which makes the theory of modular categories easier.

Besides the intrinsic mathematical aesthetics, another motivation for studying modular categories comes from their application in condensed matter physics and quantum computing [56,57]. Unitary modular categories are algebraic models of anyons in two-dimensional topological phases of matter (where simple objects model anyons). In topological quantum computation, anyons give rise to quantum computational models. Modular categories have also been used recently to construct physically realistic three-dimensional topological insulators and superconductors [8,55]. Therefore, modular categories form part of the mathematical foundations of topological quantum computation.

A modular category $\mathcal{C}$ over $\mathbb{C}$ is a non-degenerate braided spherical fusion category over $\mathbb{C}$ [1,52]. A *fusion category* $\mathcal{C}$ over $\mathbb{C}$ is an abelian $\mathbb{C}$-linear semisimple rigid monoidal category with a simple unit object $\mathbf{1}$, finite-dimensional morphism spaces, and finitely many isomorphism classes of simple objects. The label set $\Pi_{\mathcal{C}}$ of $\mathcal{C}$ is the set of isomorphism classes of simple objects of the modular category $\mathcal{C}$. The *rank* of $\mathcal{C}$ is the finite number $r = |\Pi_{\mathcal{C}}|$. Each modular category $\mathcal{C}$ leads to a $(2+1)$-dimensional topological quantum field theory and, in particular, colored oriented framed link invariants [52]. The invariant d_i for the circle colored by a label $i \in \Pi_{\mathcal{C}}$ is called the *quantum dimension* of the label i, and the global quantum dimension $D^2 = \sum_{i\in\Pi_{\mathcal{C}}} d_i^2$ is an important invariant of $\mathcal{C}$. The invariant of a Hopf link colored by labels i, j will be denoted as S_{ij}, which forms the unnormalized modular S-matrix $S = (S_{ij}), i, j \in \Pi_{\mathcal{C}}$. The invariant of the circle with a right-handed kink colored by a label i is $\theta_i \cdot d_i$ for some root of unity θ_i, which is called the *topological twist* of the label i. The topological twists are encoded

Received by the editors August 29, 2014 and, in revised form, March 13, 2015 and May 26, 2015.

2010 *Mathematics Subject Classification.* Primary 18D10; Secondary 57R56, 16T05, 81R50, 17B37.

Key words and phrases. Modular categories, Cauchy theorem, Frobenius-Schur indicator.

The first, third, and fourth authors were partially supported by NSF grant DMS1108725.

The second author was partially supported by NSF grants DMS1001566, DMS1303253, and DMS1501179.

by a diagonal modular T-matrix $T = (\delta_{ij}\theta_i), i, j \in \Pi_{\mathcal{C}}$. The modular S-matrix and modular T-matrix together lead to a projective representation of the modular group $SL(2,\mathbb{Z})$ by sending the generating matrices

$$\mathfrak{s} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \qquad \mathfrak{t} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

to S, T, respectively [1,52]. The modular group $SL(2,\mathbb{Z})$ arises here as the mapping class group of the torus. Amazingly, the kernel of this projective representation of $SL(2,\mathbb{Z})$ is always a congruence subgroup of $SL(2,\mathbb{Z})$ [43]. The S-matrix determines the fusion rules through the Verlinde formula, and the T-matrix is of finite order $\mathrm{ord}(T)$ by Vafa's theorem [1]. Together, the pair (S,T) is called the *modular data* of $\mathcal{C}$.

The abelian-ness of modular categories first manifests itself in the tensor product, via the braiding. But a deeper sense of abelian-ness is hidden in the Galois group of the number field $\mathbb{K}_{\mathcal{C}} = \mathbb{Q}[S_{ij}], i, j \in \Pi_{\mathcal{C}}$: $\mathrm{Gal}(\mathbb{K}_{\mathcal{C}}/\mathbb{Q})$ is isomorphic to an abelian subgroup [9,49] of the symmetric group $\mathfrak{S}_r$, where r is the rank of $\mathcal{C}$. This profound abelian-ness permits the application of number theory to the study of modular categories.

In 2003, the fourth author conjectured that, up to equivalence, there are only finitely many modular categories of a given rank, which we will call *the rank-finiteness conjecture* [49,58].

The first main result of the paper is a proof of this conjecture.

Theorem 3.1. *There are only finitely many modular categories of fixed rank r, up to equivalence.*

The idea of the proof is as follows. A classical result of Landau [33] is that for each n, there are only finitely many finite groups G with exactly n irreducible complex representations. Landau's result is proved by dividing the class equation $|G| = \sum_{i=1}^{n}[G : C(g_i)]$ by $|G|$ to produce the Diophantine equation $1 = \sum_{i=1}^{n} \frac{1}{x_i}$. Observing that this equation has finitely many solutions in the positive integers, one obtains a bound on $|G|$, which implies the result. Our proof follows the same strategy, with the dimension equation $D^2 = \sum_{i\in\Pi_{\mathcal{C}}} d_i^2$ playing the role of the class equation. First, Ocneanu rigidity implies that for a fixed set of fusion rules, there are only finitely many equivalence classes of modular categories [23]. Hence, the rank-finiteness conjecture is reduced to showing that there are only finitely many possible fusion rules for any given rank. Using the Verlinde formula, we can deduce the finiteness of fusion rules for a given rank from a bound of the global quantum dimension D^2. In particular, if there were only finitely possible values of D^2 in each rank, then rank-finiteness would follow [49, Proposition 6.2]. Since the $\{d_i\}$ are algebraic integers in a cyclotomic field, not necessarily in $\mathbb{Q}$, a new approach is needed.

Recall that the Frobenius-Schur exponent $\mathrm{FSexp}(\mathcal{C})$ of a spherical fusion category $\mathcal{C}$ over $\mathbb{C}$ is equal to the order of the T-matrix of its (modular) Drinfeld center $Z(\mathcal{C})$, and for a modular category, $\mathrm{FSexp}(\mathcal{C}) = \mathrm{ord}(T)$, the order of the T-matrix (cf. [44]). Our technical advance is the second main result, which is of independent interest. This is a generalization of the Cauchy theorem in group theory to the context of spherical fusion categories.

Theorem 3.9. *If $\mathcal{C}$ is a spherical fusion category over $\mathbb{C}$ with $N = \mathrm{FSexp}(\mathcal{C})$, then the set of prime ideals dividing the principal ideal generated by the global quantum dimension D^2 of $\mathcal{C}$ in the Dedekind domain $\mathbb{Z}[e^{2\pi i/N}]$ is identical to that of N.*

As a consequence, the quantum dimensions $\{d_i\}$ and D^2 of a modular category have special arithmetic properties: they are so-called $\mathcal{S}$*-units* with respect to the common set $\mathcal{S}$ of prime ideals in the factorization of the ideals generated by D^2 and $\mathrm{ord}(T)$. Then regarding $D^2 = \sum_{i\in\Pi_C} d_i^2$ as an $\mathcal{S}$-unit equation, we apply a powerful theorem of Evertse [25]: for any fixed r, there are finitely many non-degenerate solutions to $1 = \sum_{i=1}^{r} x_i$ for $\mathcal{S}$-units x_i. It follows that there are only finitely many solutions to the dimension equation $D^2 = \sum_{i\in\Pi_C} d_i^2$, which, in turn, bounds D^2 in terms of the rank. Rank-finiteness then follows.

All these steps can be made effective, so we have explicit bounds for the number of solutions to the dimension equation. The bound for the number of possible modular categories for a given rank that we obtained is absurdly large. For example, for rank $= 2$, there are only 8 modular categories up to equivalence, while our bound for the number of solutions to the $\mathcal{S}$-unit equation $D^2 = 1 + d_1^2$ (see Proposition 4.3) is $2^{8.15885\times 10^{41}}$. A natural question is to determine if there is a better bound for the number of modular categories of rank $= r$. Etingof observes in Remark 4.5 that the number of modular categories of rank $= r$ grows faster than any polynomial in r.

The rank-finiteness conjecture was motivated by the classification of topological phases of matter [56, 57]. Topological phases of matter are states of matter which have an energy gap in the thermodynamic limit and are stable under small yet arbitrary perturbations. Thus, they cannot be continuously deformed non-trivially inside topological states of matter. A mathematical manifestation of this rigidity of topological phases of matter should be rank-finiteness. The rank-finiteness theorem implies that, in principle, modular categories can be classified for low rank cases. Indeed, early progress in the classification program is the complete classification of unitary modular categories of rank at most 4 [49]. The authors of this paper have now pushed the classification to rank 5, which will appear in a separate publication.

The Cauchy theorem for spherical fusion categories is a generalization of [44, Theorem 8.4] for *integral* fusion categories. This question was originally asked by Etingof and Gelaki in the context of Hopf algebras [20, Question 5.1], and subsequently verified for Hopf algebras in [31]. Moreover, the Cauchy theorem provides an affirmative answer to [14, Question 6.10].

The proof of the Cauchy theorem for spherical fusion categories relies heavily upon *higher Frobenius-Schur (FS)-indicators*, which are discussed in Section 2. The theory of FS-indicators has played a key role in several recent results such as the congruence subgroup theorem [44] and Galois symmetry [14] (cf. Section 2.2.4).

For a finite group G, the nth FS-indicator of a representation V over $\mathbb{C}$ with character χ_V is given by $\nu_n(V) := \frac{1}{|G|}\sum_{g\in G}\chi_V(g^n)$. The Frobenius-Schur theorem asserts that the second FS-indicator $\nu_2(V)$ of an irreducible representation V must be -1, 0, or 1.

The second FS-indicator for a primary field of a rational conformal field theory is introduced by Bantay [2] as an expression in terms of the associated modular data. Bantay's expression provides a formula for the second FS-indicator of a simple object in a modular category. Second FS-indicators are later introduced by Fuchs, Ganchev, Szlachányi, and Vescernyés for certain $\mathbb{C}^*$-fusion categories [27],

by Linchenko and Montgomery [34] for semisimple Hopf algebras, and by Mason and Ng [37] for semisimple quasi-Hopf algebras. In each case, they are shown to satisfy an analogue of the Frobenius-Schur theorem. The less familiar higher FS-indicators ($n > 2$) are also defined for semisimple Hopf algebras in [34] and studied extensively by Kashina, Sommerhäuser, and Zhu in [31].

The second FS-indicators are first shown in [37] to be invariants of the integral fusion categories $\mathrm{Rep}(H)$, where H is a semisimple quasi-Hopf algebra over $\mathbb{C}$. This result motivates the development of higher FS-indicators ν_n for pivotal categories by Ng and Schauenburg [45], and in particular, spherical fusion categories $\mathcal{C}$ over $\mathbb{C}$ [44]. The invariance of higher FS-indicators for $\mathrm{Rep}(H)$ [42] follows from their categorical treatment. For a spherical fusion category $\mathcal{C}$, there exists a minimal positive integer $N = \mathrm{FSexp}(\mathcal{C})$, called the *$FS$-exponent* of $\mathcal{C}$, which satisfies $\nu_N(X_k) = d_k$ for all $k \in \Pi_{\mathcal{C}}, X_k \in k$ [44]. The FS-exponent of a spherical fusion category behaves, in many ways, like the exponent of a finite group. In fact, the FS-exponent of $\mathrm{Rep}(G)$ for any finite group G is equal to the exponent of G.

Inspired by the paper of Sommerhäuser and Zhu [51], Ng and Schauenburg formulate a categorical definition of generalized FS-indicators in [43] so that $SL(2,\mathbb{Z})$ acts on them in two different but compatible ways. These generalized FS-indicators reveal new arithmetic properties of modular categories, which include the congruence kernels of their projective representations of $SL(2,\mathbb{Z})$ (*loc. cit.*) and the Galois symmetry [14] conjectured by Coste and Gannon [11].

Our reduction of rank-finiteness to Evertse's theorem obscures the nature of rank-finiteness for modular categories. The key to Evertse's finiteness of $\mathcal{S}$-unit solutions is the Schmidt subspace theorem, which implies finiteness theorems for some simultaneous approximations to algebraic numbers by elements of a number field. A more direct proof of rank-finiteness might shed light on whether rank-finiteness also holds for spherical fusion categories. One potential approach is taking the Drinfeld center of spherical fusion categories and then deducing rank-finiteness for spherical fusion categories from the modular case. The key hurdle to this approach is controlling the rank of the Drinfeld center in terms of the rank of the original category. In light of [16], this appears to be difficult: even for integral fusion categories $\mathcal{C}$, the rank of the Drinfeld center $Z(\mathcal{C})$ is super-polynomial in the rank of $\mathcal{C}$.

The contents of the paper are as follows. Section 2 is a collection of necessary results on fusion and modular categories. In Section 3, we prove the Cauchy theorem for spherical fusion categories and rank-finiteness for modular categories, as well as for modularizable premodular categories. In Section 4, we conclude with a discussion of asymptotics and future directions.

2. Modular categories

In this section, we will collect some conventions and essential results on spherical fusion categories and modular categories. Most of these results can be found in [1,23,43–45,52] and the references therein. All fusion and modular categories are over the complex numbers $\mathbb{C}$ in this paper unless stated otherwise.

2.1. **Basic definitions.** A modular category is a braided spherical fusion category in which the braiding is non-degenerate. Modular categories were first axiomatized by Turaev [53], based on earlier notions in rational conformal field theory by Moore and Seiberg [38] and related foundational work of Joyal and Street [30]. Early interesting examples arose in the work of Reshetikhin and Turaev [48] on quantum

groups and their application to low-dimensional topology. In this section, we will give the precise definition and describe some further properties and consequences of the definition.

2.1.1. *Fusion categories.* Recall from [23], a *fusion category* $\mathcal{C}$ (over $\mathbb{C}$) is an abelian $\mathbb{C}$-linear semisimple rigid monoidal category with a simple unit object $\mathbf{1}$, finite-dimensional morphism spaces, and finitely many isomorphism classes of simple objects.

Here a *monoidal* category is a category $\mathcal{C}$ with

(i) a bifuntor $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$,
(ii) a natural isomorphism (associativity) $\alpha_{UVW} : (U \otimes V) \otimes W \to U \otimes (V \otimes W)$,
(iii) and a unit object $\mathbf{1}$ with natural isomorphisms $\lambda_V : \mathbf{1} \otimes V \to V$ and $\rho_V : V \otimes \mathbf{1} \to V$,

so that the associativity and the unit satisfy the pentagon and triangle compatibility axioms [36]. A monoidal functor is a pair (F, ϕ) where $F : \mathcal{C} \to \mathcal{D}$ is a functor with $F(\mathbf{1}_{\mathcal{C}}) \cong \mathbf{1}_{\mathcal{D}}$ and $\phi_{V,W} : F(V \otimes W) \to F(V) \otimes F(W)$ is a natural isomorphism which is compatible with the associator. Two monoidal categories $\mathcal{C}$ and $\mathcal{D}$ are equivalent if there is a monoidal functor (F, ϕ) from $\mathcal{C}$ to $\mathcal{D}$ so that the functor $F : \mathcal{C} \to \mathcal{D}$ is an equivalence of the underlying ordinary categories [36].

In a fusion category $\mathcal{C}$ with tensor product $\otimes$ and unit object $\mathbf{1}$, the left dual of $V \in \mathcal{C}$ is a triple $(V^*, \mathrm{db}_V, \mathrm{ev}_V)$, where $\mathrm{db}_V : \mathbf{1} \to V \otimes V^*$ and $\mathrm{ev}_V : V^* \otimes V \to \mathbf{1}$ are the coevaluation and evaluation morphisms. The left duality can be extended to a monoidal functor $(-)^* : \mathcal{C} \to \mathcal{C}^{\mathrm{op}}$, and so $(-)^{**} : \mathcal{C} \to \mathcal{C}$ defines a monoidal equivalence. Moreover, we can choose $\mathbf{1}^* = \mathbf{1}$. The linear space of morphisms between objects V and W will be denoted as $\mathrm{Hom}_{\mathcal{C}}(V, W)$. Right duals are similarly defined,

Let $\Pi_{\mathcal{C}}$ be the set of isomorphism classes of simple objects of the fusion category $\mathcal{C}$. The *rank* of $\mathcal{C}$ is the finite number $r = |\Pi_{\mathcal{C}}|$, and we denote the members of $\Pi_{\mathcal{C}}$ by $\{0, \ldots, r-1\}$. We simply write V_i for an object in the isomorphism class $i \in \Pi_{\mathcal{C}}$. By convention, the isomorphism class of $\mathbf{1}$ corresponds to $0 \in \Pi_{\mathcal{C}}$. The rigidity of $\mathcal{C}$ defines an involutive permutation $i \mapsto i^*$ on $\Pi_{\mathcal{C}}$, which is given by $V_{i^*} \cong V_i^*$ for all $i \in \Pi_{\mathcal{C}}$.

2.1.2. *Braidings.* A *braiding* c of a fusion category $\mathcal{C}$ is a natural family of isomorphisms $c_{V,W} : V \otimes W \to W \otimes V$ in V and W of $\mathcal{C}$ which satisfy the hexagon axioms,

$$\begin{array}{ccc}
U \otimes (V \otimes W) & \xrightarrow{c_{U,V\otimes W}} & (V \otimes W) \otimes U \\
{\scriptstyle\alpha}\uparrow & & \downarrow{\scriptstyle\alpha} \\
(U \otimes V) \otimes W & & V \otimes (W \otimes U) \\
{\scriptstyle c\otimes\mathrm{id}}\downarrow & & \uparrow{\scriptstyle \mathrm{id}\otimes c} \\
(V \otimes U) \otimes W & \xrightarrow[\alpha]{} & V \otimes (U \otimes W),
\end{array}
\qquad
\begin{array}{ccc}
(U \otimes V) \otimes W & \xrightarrow{c_{U\otimes V,W}} & W \otimes (U \otimes V) \\
{\scriptstyle\alpha^{-1}}\uparrow & & \downarrow{\scriptstyle\alpha^{-1}} \\
U \otimes (V \otimes W) & & (W \otimes U) \otimes V \\
{\scriptstyle \mathrm{id}\otimes c}\downarrow & & \uparrow{\scriptstyle c\otimes\mathrm{id}} \\
U \otimes (W \otimes V) & \xrightarrow[\alpha^{-1}]{} & (U \otimes W) \otimes V,
\end{array}$$

for all $U, V, W \in \mathcal{C}$, where α is the associativity isomorphism of $\mathcal{C}$ (cf. [30]).

A *braided fusion category* is a pair $(\mathcal{C}, c)$ in which c is a braiding of the fusion category $\mathcal{C}$. We simply call $\mathcal{C}$ a braided fusion category if the underlying braiding c is understood.

2.1.3. *Spherical fusion categories.* A *pivotal structure* of a fusion category $\mathcal{C}$ is an isomorphism $j : \mathrm{Id}_{\mathcal{C}} \to (-)^{**}$ of monoidal functors. One can respectively define the left and the right *pivotal traces* of an endomorphism $f : V \to V$ in $\mathcal{C}$ as

$$\underline{\mathrm{ptr}}^{\ell}(f) = \left(\mathbf{1} \xrightarrow{\mathrm{db}_{V^*}} V^* \otimes V^{**} \xrightarrow{\mathrm{id}\otimes j_V^{-1}} V^* \otimes V \xrightarrow{\mathrm{id}\otimes f} V^* \otimes V \xrightarrow{\mathrm{ev}_V} \mathbf{1}\right),$$
$$\underline{\mathrm{ptr}}^{r}(f) = \left(\mathbf{1} \xrightarrow{\mathrm{db}_{V}} V \otimes V^* \xrightarrow{f\otimes\mathrm{id}} V \otimes V^* \xrightarrow{j_V\otimes\mathrm{id}} V^{**} \otimes V^* \xrightarrow{\mathrm{ev}_{V^*}} \mathbf{1}\right).$$

Note that $j_V^* = j_{V^*}^{-1}$ (cf. [50, Proposition A.1]), and so we have $\underline{\mathrm{ptr}}^{\ell}(f) = \underline{\mathrm{ptr}}^{r}(f^*)$. Since $\mathbf{1}$ is a simple object of $\mathcal{C}$, both pivotal traces $\underline{\mathrm{ptr}}^{\ell}(f)$ and $\underline{\mathrm{ptr}}^{r}(f)$ can be identified with some scalars in $\mathbb{C}$. A pivotal structure on $\mathcal{C}$ is called *spherical* if the two pivotal traces coincide for all endomorphisms f in $\mathcal{C}$. In a spherical category, the pivotal trace(s) will be denoted by $\underline{\mathrm{ptr}}(f)$.

For the purpose of this paper, a *pivotal* (resp. *spherical*) *category* $(\mathcal{C}, j)$ is a fusion category $\mathcal{C}$ equipped with a pivotal (resp. spherical) structure j. We will denote the pair $(\mathcal{C}, j)$ by $\mathcal{C}$ when there is no ambiguity. The *left* and the *right pivotal dimensions* of $V \in \mathcal{C}$ are defined as $d^{\ell}(V) = \underline{\mathrm{ptr}}^{\ell}(\mathrm{id}_V)$ and $d^{r}(V) = \underline{\mathrm{ptr}}^{r}(\mathrm{id}_V)$, respectively.

2.1.4. *Modular categories.* Following [32], a *twist* (or *ribbon structure*) of a braided fusion category $(\mathcal{C}, c)$ is an $\mathbb{C}$-linear automorphism, θ, of $\mathrm{Id}_{\mathcal{C}}$ which satisfies

$$\theta_{V\otimes W} = (\theta_V \otimes \theta_W) \circ c_{W,V} \circ c_{V,W}, \qquad \theta_V^* = \theta_{V^*}$$

for $V, W \in \mathcal{C}$. A braided fusion category equipped with a ribbon structure is called a *ribbon fusion* or *premodular* category.

Associated with the braiding c is an isomorphism of $\mathbb{C}$-linear functors $u : \mathrm{Id}_{\mathcal{C}} \to (-)^{**}$, called the *Drinfeld isomorphism*. When $\mathcal{C}$ is a strict fusion category, u_V is the composition,

$$u_V := (V \xrightarrow{\mathrm{db}\otimes\mathrm{id}} V^* \otimes V^{**} \otimes V \xrightarrow{\mathrm{id}\otimes c^{-1}} V^* \otimes V \otimes V^{**} \xrightarrow{\mathrm{ev}\otimes\mathrm{id}} V^{**} = V).$$

If u is the Drinfeld isomorphism associated with c, and θ is a ribbon structure, then

$$j = u\theta \tag{2.1}$$

is a spherical structure of $\mathcal{C}$. This equality defines a one-to-one correspondence between the spherical structures and the ribbon structures on $(\mathcal{C}, c)$. In particular, every premodular category admits a spherical structure.

A premodular category $\mathcal{C}$ is called a *modular category* if the *S-matrix* of $\mathcal{C}$, defined by

$$S_{ij} = \underline{\mathrm{ptr}}(c_{V_j,V_{i^*}} \circ c_{V_{i^*},V_j}) \qquad \text{for } i, j \in \Pi_{\mathcal{C}},$$

is non-singular. Note that S is a symmetric matrix and that $d^r(V_i) = S_{0i} = S_{i0}$ for all i.

2.2. **Further properties and basic invariants.**

2.2.1. *Grothendieck ring and dimensions.* The *Grothendieck ring* $K_0(\mathcal{C})$ of a fusion category $\mathcal{C}$ is the $\mathbb{Z}$-ring generated by $\Pi_{\mathcal{C}}$ with multiplication induced from $\otimes$. The structure coefficients of $K_0(\mathcal{C})$ are obtained from

$$V_i \otimes V_j \cong \bigoplus_{k\in\Pi_{\mathcal{C}}} N_{i,j}^k V_k,$$

where $N_{i,j}^k = \dim(\mathrm{Hom}_{\mathcal{C}}(V_k, V_i \otimes V_j))$. This family of non-negative integers $\{N_{i,j}^k\}_{i,j,k\in\Pi_{\mathcal{C}}}$ is called the *fusion rules* of $\mathcal{C}$.

In a braided fusion category, $K_0(\mathcal{C})$ is a commutative ring and the fusion rules satisfy the symmetries

$$N_{i,j}^k = N_{j,i}^k = N_{i,k^*}^{j^*} = N_{i^*,j^*}^{k^*}, \qquad N_{i,j}^0 = \delta_{i,j^*}. \tag{2.2}$$

The *fusion matrix* N_i associated to V_i, defined by $(N_i)_{k,j} = N_{i,j}^k$, is an integral matrix with non-negative entries. In the braided fusion setting, these matrices are normal and mutually commuting. The largest real eigenvalue of N_i is called the *Frobenius-Perron dimension* of V_i and is denoted by $\mathrm{FPdim}(V_i)$. Moreover, FPdim can be extended to a $\mathbb{Z}$-ring homomorphism from $K_0(\mathcal{C})$ to $\mathbb{R}$ and is the unique such homomorphism that is positive (real-valued) on $\Pi_{\mathcal{C}}$ (see [23]). The *Frobenius-Perron dimension* of $\mathcal{C}$ is defined as

$$\mathrm{FPdim}(\mathcal{C}) = \sum_{i\in\Pi_{\mathcal{C}}} \mathrm{FPdim}(V_i)^2.$$

Definition 2.1. A fusion category $\mathcal{C}$ is said to be

(i) *weakly integral* if $\mathrm{FPdim}(\mathcal{C}) \in \mathbb{Z}$,
(ii) *integral* if $\mathrm{FPdim}(V_j) \in \mathbb{Z}$ for all $j \in \Pi_{\mathcal{C}}$,
(iii) *pointed* if $\mathrm{FPdim}(V_j) = 1$ for all $j \in \Pi_{\mathcal{C}}$.

Furthermore, if $\mathrm{FPdim}(V) = 1$, then V is *invertible*.

Remark 2.2. The terminology *invertible* arises from the fact that $\mathrm{FPdim}(V) = 1$ if and only if $V \otimes V^* \cong \mathbf{1}$. The set of invertible simple objects generates a full fusion subcategory $\mathcal{C}_{pt}$ called the *pointed subcategory*.

Let $\mathcal{C}$ be a pivotal category. It follows from [23, Proposition 2.9] that $d^r(V^*) = \overline{d^r(V)}$ is an algebraic integer for any $V \in \mathcal{C}$. The *global dimension* of $\mathcal{C}$ is defined by

$$D^2 = \sum_{i\in\Pi_{\mathcal{C}}} |d^r(V_i)|^2.$$

Remark 2.3. It is worth noting that the global dimension D^2 can be defined for any fusion category (cf. [23]) and does not depend on the existence, or choice, of a pivotal structure.

By [23,39], a pivotal structure of a fusion category $\mathcal{C}$ is spherical if, and only if, $d^r(V)$ is real for all $V \in \mathcal{C}$. In this case, $d^r(V) = d^\ell(V)$, and we simply write $d(V)$ to refer to the dimension of V. Furthermore for $i \in \Pi_{\mathcal{C}}$, we adopt the shorthand $d_i = d(V_i)$.

A fusion category $\mathcal{C}$ is called *pseudo-unitary* if $D^2 = \mathrm{FPdim}(\mathcal{C})$. For a pseudo-unitary fusion category $\mathcal{C}$, it has been shown in [23] that there exists a unique spherical structure of $\mathcal{C}$ such that $d(V) = \mathrm{FPdim}(V)$ for all objects $V \in \mathcal{C}$.

2.2.2. *Spherical and ribbon structures.* The set of isomorphism classes of invertible objects $G(\mathcal{C})$ in a fusion category $\mathcal{C}$ forms a group in $K_0(\mathcal{C})$ where $i^{-1} = i^*$ for $i \in G(\mathcal{C})$. For modular categories $\mathcal{C}$, the group $G(\mathcal{C})$ parameterizes pivotal structures on the underlying braided fusion category.[1]

Lemma 2.4. *Let $\mathcal{C}$ be a modular category. There is a bijective correspondence between the pivotal structures of the underlying braided fusion category $\mathcal{C}$ and the group of invertible objects $G(\mathcal{C})$. Under this correspondence, the inequivalent spherical structures of $\mathcal{C}$ map onto the maximal elementary abelian 2-subgroup, $\Omega_2 G(\mathcal{C})$, of $G(\mathcal{C})$.*

Proof. Let j_0 be the spherical structure of the modular category $\mathcal{C}$. For any pivotal structure j of $\mathcal{C}$, we have $j_0^{-1}j \in \mathrm{Aut}_\otimes(\mathrm{Id}_\mathcal{C})$, the group of automorphisms of the monoidal functor $\mathrm{Id}_\mathcal{C}$. Moreover, $j \mapsto j_0^{-1}j$ defines a bijection between the set of pivotal structures of $\mathcal{C}$ and $\mathrm{Aut}_\otimes(\mathrm{Id}_\mathcal{C})$. Note that j is spherical if, and only if, the associated dimension function is real valued, and hence for any simple V, $(j_0^{-1}j)_V = \lambda_V \mathrm{id}_V$ for some real scalar λ_V. By [28, Theorem 6.2], $\mathrm{Aut}_\otimes(\mathrm{Id}_\mathcal{C}) \cong G(\mathcal{C})$, and hence the first statement follows. In particular, $j_0^{-1}j$ has finite order. Thus, j is a spherical structure of $\mathcal{C}$ if, and only if, $(j_0^{-1}j)_V = \pm \mathrm{id}_V$ for any simple V, or $j_0^{-1}j \in \mathrm{Aut}_\otimes(\mathrm{Id}_\mathcal{C})$ is of order ≤ 2. Therefore, the second statement follows from the isomorphism $\mathrm{Aut}_\otimes(\mathrm{Id}_\mathcal{C}) \cong G(\mathcal{C})$. □

Remark 2.5. The isomorphism $\mathrm{Aut}_\otimes(\mathrm{Id}_\mathcal{C}) \cong G(\mathcal{C})$ is determined by the braiding c and the spherical structure j_0 of the modular category $(\mathcal{C}, c, j_0)$. By [39, Corollary 7.11], $(\mathcal{C}, c, j)$ is a modular category for all spherical structures j of $\mathcal{C}$, so that there are exactly $|G(\mathcal{C})|$ pivotal and $|\Omega_2 G(\mathcal{C})|$ spherical structures on the fusion category $\mathcal{C}$.

In any ribbon fusion category $\mathcal{C}$ the associated ribbon structure, θ, has finite order. This celebrated fact is part of Vafa's Theorem (see [1, 54]) in the case of modular categories. However, any ribbon category embeds in a modular category (via Drinfeld centers; see [39]) so the result holds generally. Observe that $\theta_{V_i} = \theta_i \mathrm{id}_{V_i}$ for some root of unity $\theta_i \in \mathbb{C}$. Since $\theta_\mathbf{1} = \mathrm{id}_\mathbf{1}$, $\theta_0 = 1$. The *T-matrix* of $\mathcal{C}$ is defined by $T_{ij} = \delta_{ij}\theta_j$ for $i, j \in \Pi_\mathcal{C}$. The *balancing equation*

$$\theta_i\theta_j S_{ij} = \sum_{k \in \Pi_\mathcal{C}} N_{i^*j}^k d_k \theta_k \tag{2.3}$$

is a useful algebraic consequence, holding in any premodular category. The pair (S, T) of S- and T-matrices will be called the *modular data* of a given modular category $\mathcal{C}$.

2.2.3. *Modular data and $SL(2, \mathbb{Z})$ representations.*

Definition 2.6. For a pair of matrices (S, T) for which there exists a modular category with modular data (S, T), we will say (S, T) is *realizable modular data.*

The fusion rules $\{N_{i,j}^k\}_{i,j,k \in \Pi_\mathcal{C}}$ of $\mathcal{C}$ can be written in terms of the S-matrix, via the *Verlinde formula* [1],

$$N_{i,j}^k = \frac{1}{D^2} \sum_{a \in \Pi_\mathcal{C}} \frac{S_{ia} S_{ja} S_{k^*a}}{S_{0a}} \quad \text{for all } i, j, k \in \Pi_\mathcal{C}\,. \tag{2.4}$$

[1] The second part of this result was pointed out to us by Naidu.

The modular data (S,T) of a modular category $\mathcal{C}$ satisfy the conditions

$$(ST)^3 = p^+S^2, \qquad S^2 = p^+p^-C, \qquad CT = TC, \qquad C^2 = \mathrm{id}, \tag{2.5}$$

where $p^\pm = \sum_{i\in\Pi_\mathcal{C}} d_i^2\theta_i^{\pm 1}$ are called the *Gauss sums*, and $C = (\delta_{ij^*})_{i,j\in\Pi_\mathcal{C}}$ is called the *charge conjugation matrix* of $\mathcal{C}$. In terms of matrix entries, the first equation in (2.5) gives the *twist equation*

$$p^+S_{jk} = \theta_j\theta_k \sum_i \theta_i S_{ij}S_{ik}\,. \tag{2.6}$$

The quotient $\frac{p^+}{p^-}$, called the *anomaly* of $\mathcal{C}$, is a root of unity, and

$$p^+p^- = D^2. \tag{2.7}$$

Moreover, S satisfies

$$S_{ij} = S_{ji} \quad \text{and} \quad S_{ij^*} = S_{i^*j} \tag{2.8}$$

for all $i,j \in \Pi_\mathcal{C}$. These equations and the Verlinde formula imply that

$$S_{ij^*} = \overline{S_{ij}} \quad \text{and} \quad \frac{1}{D^2}\sum_{j\in\Pi_\mathcal{C}} S_{ij}\overline{S}_{jk} = \delta_{ik}. \tag{2.9}$$

In particular, S is projectively unitary.

A modular category $\mathcal{C}$ is called *self-dual* if $i = i^*$ for all $i \in \Pi_\mathcal{C}$. In fact, $\mathcal{C}$ is self-dual if and only if S is a real matrix.

Let D be the positive square root of D^2. The Verlinde formula can be rewritten as

$$SN_iS^{-1} = D_i \quad \text{for } i \in \Pi_\mathcal{C},$$

where $(D_i)_{ab} = \delta_{ab}\frac{S_{ia}}{S_{0a}}$. In particular, the assignments $\phi_a : i \mapsto \frac{S_{ia}}{S_{0a}}$ for $i \in \Pi_\mathcal{C}$ determine (complex) linear characters of $K_0(\mathcal{C})$. Since S is non-singular, $\{\phi_a\}_{a\in\Pi_\mathcal{C}}$ is the set of *all* the linear characters of $K_0(\mathcal{C})$. Observe that FPdim is a character of $K_0(\mathcal{C})$, so that there is some $a \in \Pi_\mathcal{C}$ such that $\mathrm{FPdim} = \phi_a$. By the unitarity of S, we have that $\mathrm{FPdim}(\mathcal{C}) = D^2/(d_a)^2$.

As an abstract group, $SL(2,\mathbb{Z}) \cong \langle \mathfrak{s},\mathfrak{t} \mid \mathfrak{s}^4 = 1, (\mathfrak{s}\mathfrak{t})^3 = \mathfrak{s}^2\rangle$. The standard choice for generators is

$$\mathfrak{s} := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad \mathfrak{t} := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Let $\eta : GL(\Pi_\mathcal{C},\mathbb{C}) \to PGL(\Pi_\mathcal{C},\mathbb{C})$ be the natural surjection. The relations (2.5) imply that

$$\overline{\rho}_\mathcal{C} \colon \mathfrak{s} \mapsto \eta(S) \quad \text{and} \quad \mathfrak{t} \mapsto \eta(T) \tag{2.10}$$

define a projective representation of $SL(2,\mathbb{Z})$. Since the modular data are an invariant of a modular category, so is the associated projective representation type of $SL(2,\mathbb{Z})$. The following arithmetic properties of this projective representation will play an important role in our discussion (cf. [43]). Let $\mathbb{Q}_N := \mathbb{Q}(\zeta_N)$, where ζ_N is a primitive Nth root of unity.

Theorem 2.7. *Let (S,T) be the modular data of the modular category $\mathcal{C}$ with $N = \mathrm{ord}\,(T)$. Then the entries of S are algebraic integers of $\mathbb{Q}_N$. Moreover, N is minimal such that the projective representation $\overline{\rho}_\mathcal{C}$ of $SL(2,\mathbb{Z})$ associated with the modular data can be factored through $\mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$. In other words, $\ker\overline{\rho}_\mathcal{C}$ is a congruence subgroup of level N.*

Definition 2.8. A *modular representation* of $\mathcal{C}$ (cf. [43]) is a representation ρ of $SL(2,\mathbb{Z})$ which satisfies the commutative diagram

$$\begin{array}{ccc} SL(2,\mathbb{Z}) & \xrightarrow{\rho} & GL(\Pi_{\mathcal{C}},\mathbb{C}) \\ & \searrow^{\overline{\rho}_{\mathcal{C}}} & \downarrow \eta \\ & & PGL(\Pi_{\mathcal{C}},\mathbb{C})\,. \end{array}$$

Let $\zeta \in \mathbb{C}$ be a fixed 6th root of the anomaly $\dfrac{p^+}{p^-}$. For any 12th root of unity x, it follows from (2.5) that the assignments

$$\rho_x^\zeta : \mathfrak{s} \mapsto \frac{\zeta^3}{x^3 p^+} S, \qquad \mathfrak{t} \mapsto \frac{x}{\zeta} T \tag{2.11}$$

define a modular representation of $\mathcal{C}$. Moreover, $\{\rho_x^\zeta \mid x^{12} = 1\}$ is the complete set of modular representations of $\mathcal{C}$ (cf. [14, Section 1.3]). Since $D^2 = p^+p^-$, we have $\zeta^3/p^+ = \gamma/D$, where $\gamma = \pm 1$. Thus, one can always find a 6th root of unity x so that $\rho_x^\zeta : \mathfrak{s} \mapsto S/D$. For the purpose of this paper, we only need to consider the modular representation ρ of $\mathcal{C}$ which assigns $\mathfrak{s} \to S/D$. Note also that $\rho_x^\zeta(\mathfrak{s})$ and $\rho_x^\zeta(\mathfrak{t})$ are matrices over a finite abelian extension of $\mathbb{Q}$. Therefore, modular representations of any modular category are defined over the abelian closure $\mathbb{Q}_{\rm ab}$ of $\mathbb{Q}$ in $\mathbb{C}$ (cf. [4]).

Let ρ be any modular representation of the modular category $\mathcal{C}$, and set

$$s = \rho(\mathfrak{s}) \quad \text{and} \quad t = \rho(\mathfrak{t})\,.$$

It is clear that a representation ρ is uniquely determined by the pair (s,t), which will be called a *normalized modular pair* of $\mathcal{C}$. In view of the preceding paragraph, there exists a root of unity y such that $(S/D, T/y)$ is a normalized modular pair of $\mathcal{C}$.

2.2.4. *Galois symmetry.* Observe that for any choice of a normalized modular pair (s,t), we have $\frac{s_{ia}}{s_{0a}} = \frac{S_{ia}}{S_{0a}} = \phi_a(i)$. For each $\sigma \in \mathrm{Aut}(\mathbb{Q}_{\rm ab})$, $\sigma(\phi_a)$ given by $\sigma(\phi_a)(i) = \sigma\left(\frac{s_{ia}}{s_{0a}}\right)$ is again a linear character of $K_0(\mathcal{C})$, and hence $\sigma(\phi_a) = \phi_{\hat{\sigma}(a)}$ for some unique $\hat{\sigma} \in \mathrm{Sym}(\Pi_{\mathcal{C}})$. That is,

$$\sigma\left(\frac{s_{ia}}{s_{0a}}\right) = \frac{s_{i\hat{\sigma}(a)}}{s_{0\hat{\sigma}(a)}} \quad \text{for all } i,a \in \Pi_{\mathcal{C}}\,. \tag{2.12}$$

Moreover, there exists a function $\epsilon_\sigma : \Pi_{\mathcal{C}} \to \{\pm 1\}$, which depends on the choice of s, such that

$$\sigma(s_{ij}) = \epsilon_\sigma(i) s_{\hat{\sigma}(i)j} = \epsilon_\sigma(j) s_{i\hat{\sigma}(j)} \quad \text{for all } i,j \in \Pi_{\mathcal{C}} \tag{2.13}$$

(cf. [4, Appendix B], [11], or [23, Appendix]). The group $\mathrm{Sym}(\Pi_{\mathcal{C}})$ will often be written as $\mathfrak{S}_r$ where $r = |\Pi_{\mathcal{C}}|$ is the rank of $\mathcal{C}$.

The following theorem will be used in the sequel.

Theorem 2.9. *Let $\mathcal{C}$ be a modular category of rank r, with T-matrix of order N. Suppose (s,t) is a normalized modular pair of $\mathcal{C}$. Set $t = (\delta_{ij}t_i)$ and $n = \mathrm{ord}(t)$. Then*

(a) $N \mid n \mid 12N$ and $s,t \in \mathrm{GL}_r(\mathbb{Q}_n)$. Moreover,
(b) (Galois symmetry) for $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$, $\sigma^2(t_i) = t_{\hat{\sigma}(i)}$.

Part (a) of Theorem 2.9 is proved in [43], whereas part (b) is proved in [14, Theorem II(iii)].

In the sequel, we will simply denote by $\mathbb{F}_A$ the field extension over $\mathbb{Q}$ generated by the entries of a complex matrix A. If $\mathbb{F}_A/\mathbb{Q}$ is Galois, then we simply write $\mathrm{Gal}(A)$ for the Galois group $\mathrm{Gal}(\mathbb{F}_A/\mathbb{Q})$.

In this notation, if (S,T) is the modular data of $\mathcal{C}$, then $\mathbb{F}_T = \mathbb{Q}_N$, where $N = \mathrm{ord}\,(T)$, and we have $\mathbb{F}_S \subseteq \mathbb{F}_T$ by Theorem 2.7. In particular, $\mathbb{F}_S$ is an abelian Galois extension over $\mathbb{Q}$.

For any normalized modular pair (s,t) of $\mathcal{C}$ we have $\mathbb{F}_t = \mathbb{Q}_n$, where $n = \mathrm{ord}\,(t)$. Moreover, by Theorem 2.9, $\mathbb{F}_S \subseteq \mathbb{F}_s \subseteq \mathbb{F}_t$. In particular, the field extension $\mathbb{F}_s/\mathbb{Q}$ is also Galois. The kernel of the restriction map $\mathrm{res} : \mathrm{Gal}(t) \to \mathrm{Gal}(S)$ is isomorphic to $\mathrm{Gal}(\mathbb{F}_t/\mathbb{F}_S)$.

The following important lemma is proved in [14, Proposition 6.5].

Lemma 2.10. *Let $\mathcal{C}$ be a modular category with modular data (S,T). For any normalized modular pair (s,t) of $\mathcal{C}$, $\mathrm{Gal}(\mathbb{F}_t/\mathbb{F}_S)$ is an elementary 2-group.*

2.2.5. *Frobenius-Schur indicators.* A *strict pivotal* category is a pivotal category in which the associativity isomorphisms are identities, the pivotal structure $j : \mathrm{Id}_{\mathcal{C}} \to (-)^{**}$ is the identity, and the associated natural isomorphisms $\xi_{U,V} : U^* \otimes V^* \to (V \otimes U)^*$ are also identities. Moreover, we have the following theorem (cf. [45]).

Theorem 2.11. *Every pivotal category is pivotally equivalent to a strict pivotal category.*

Frobenius-Schur indicators are indispensable invariants of spherical categories introduced in [45]. They are defined for each object in a pivotal category. Here, we only provide the definitions of these indicators in a *strict* spherical category. Let n be a positive integer and V an object of a strict spherical category $\mathcal{C}$. We denote by $V^{\otimes n}$ the n-fold tensor power of V. One can define a $\mathbb{C}$-linear operator $E_V^{(n)} : \mathrm{Hom}_{\mathcal{C}}\,(\mathbf{1}, V^{\otimes n}) \to \mathrm{Hom}_{\mathcal{C}}\,(\mathbf{1}, V^{\otimes n})$ given by

$$E_V^{(n)}(f) = \left(\mathbf{1} \xrightarrow{\mathrm{db}} V^* \otimes V \xrightarrow{\mathrm{id}_{V^*} \otimes f \otimes \mathrm{id}_V} V^* \otimes V^{\otimes n+1} \xrightarrow{\mathrm{ev} \otimes \mathrm{id}_V^{\otimes n}} V^{\otimes n}\right).$$

The nth Frobenius-Schur indicator of V is defined as

$$\nu_n(V) = \mathrm{Tr}(E_V^{(n)})\,.$$

It follows directly from graphical calculus that $\left(E_V^{(n)}\right)^n = \mathrm{id}$, and so $\nu_n(V)$ is an algebraic integer in the nth cyclotomic field $\mathbb{Q}_n = \mathbb{Q}(e^{\frac{2\pi i}{n}})$.

The first indicator $\nu_1(V_i)$ is the Kronecker delta function δ_{0i} on $\Pi_{\mathcal{C}}$, i.e. $\nu_1(V) = 1$ if $V \cong \mathbf{1}$ and 0 otherwise. The second indicator is consistent with the classical Frobenius-Schur indicator of an irreducible representation of a group, namely $\nu_2(V) = \pm 1$ if $V \cong V^*$ and 0 otherwise for any simple object V of $\mathcal{C}$. The higher indicators are more obscure in nature, but they are all additive complex valued functions of the Grothendieck ring $K_0(\mathcal{C})$ of $\mathcal{C}$.

The classical definition of exponent of a finite group can be generalized to a spherical category via the following theorem [44].

Theorem 2.12. *Let $\mathcal{C}$ be a spherical category. There exists a positive integer n such that $\nu_n(V) = d\,(V)$ for all $V \in \mathcal{C}$. If N is minimal among such n, then $d\,(V)$ are algebraic integers in $\mathbb{Q}_N$.*

The minimal integer $\mathrm{FSexp}(\mathcal{C}) := N$ above is called the *Frobenius-Schur exponent*. If $\mathcal{C}$ is the category of complex representations of a finite group G, then $\mathrm{FSexp}(\mathcal{C}) = \exp(G)$. For modular categories the Frobenius-Schur indicators $\nu_n(V)$ are completely determined by the modular data of $\mathcal{C}$, explicitly given in [44] (generalizing the second indicator formula in [2]).

Theorem 2.13. *Let $\mathcal{C}$ be a modular category with the T-matrix given by $[\delta_{ij}\theta_i]_{i,j\in\Pi_{\mathcal{C}}}$. Then* $\mathrm{ord}\,(T) = \mathrm{FSexp}(\mathcal{C})$*, and*

$$\nu_n(V_k) = \frac{1}{D^2} \sum_{i,j\in\Pi_{\mathcal{C}}} N_{i,j}^k \, d_i d_j \left(\frac{\theta_i}{\theta_j}\right)^n \tag{2.14}$$

for all $k \in \Pi_{\mathcal{C}}$ and positive integers n.

2.2.6. *Modular data.*

Definition 2.14. Let $S, T \in \mathrm{GL}_r(\mathbb{C})$ and define constants $d_j := S_{0j}$, $\theta_j := T_{jj}$, $D^2 := \sum_j d_j^2$, and $p_\pm = \sum_{k=0}^{r-1} (S_{0,k})^2 \theta_k^{\pm 1}$. The pair (S, T) is an *admissible modular data* of rank r if they satisfy the following conditions:

(i) $d_j \in \mathbb{R}$ and $S = S^t$ with $S\overline{S}^t = D^2\,\mathrm{Id}$. $T_{i,j} = \delta_{i,j}\theta_i$ with $N := \mathrm{ord}(T) < \infty$.
(ii) $(ST)^3 = p^+ S^2$, $p_+ p_- = D^2$, and $\frac{p_+}{p_-}$ is a root of unity.
(iii) $N_{i,j}^k := \frac{1}{D^2} \sum_{a=0}^{r-1} \frac{S_{ia} S_{ja} \overline{S_{ka}}}{S_{0a}} \in \mathbb{N}$ for all $0 \le i, j, k \le (r-1)$.
(iv) $\theta_i\theta_j S_{ij} = \sum_{k=0}^{r-1} N_{i^* j}^k d_k \theta_k$ where i^* is the unique label such that $N_{i,i^*}^0 = 1$.
(v) Define $\nu_n(k) := \frac{1}{D^2} \sum_{i,j=0}^{r-1} N_{i,j}^k \, d_i d_j \left(\frac{\theta_i}{\theta_j}\right)^n$. Then $\nu_2(k) = 0$ if $k \neq k^*$ and $\nu_2(k) = \pm 1$ if $k = k^*$. Moreover, $\nu_n(k) \in \mathbb{Z}[e^{2\pi i/N}]$ for all n, k.
(vi) $\mathbb{F}_S \subset \mathbb{F}_T = \mathbb{Q}_N$, $\mathrm{Gal}(\mathbb{F}_S/\mathbb{Q})$ is isomorphic to an abelian subgroup of $\mathfrak{S}_r$ and $\mathrm{Gal}(\mathbb{F}_T/\mathbb{F}_S) \cong (\mathbb{Z}/2\mathbb{Z})^\ell$ for some integer ℓ.
(vii) The prime divisors of D^2 and N coincide in $\mathbb{Z}[e^{2\pi i/N}]$.[2]

Theorem 2.15. *Let (S, T) be realizable modular data. Then*
(a) (S, T) is admissible, and
(b) for all $\sigma \in \mathrm{Aut}(\mathbb{Q}_{\mathrm{ab}})$, $(\sigma(S), \sigma(T))$ is realizable.

Proof. (a) follows from the definition of admissible modular data, while (b) follows from [23, Section 2.7] (see also [12]). □

Remark 2.16. We expect a converse of Theorem 2.15 to be true: that is, if (S, T) is admissible, then it is realizable. Indeed, a satisfactory definition of admissible would be a minimal set of conditions that guarantee realizability.

3. Rank-finiteness and the Cauchy theorem

The main goal of this section is to prove the following theorem, conjectured by the fourth author in 2003 (see [58]).

Theorem 3.1 (Rank-finiteness theorem)**.** *There are only finitely many modular categories of fixed rank r, up to equivalence.*

[2] See Section 3.1.

Prior to this work this conjecture had been resolved only in certain restricted cases; for instance, it was shown [23, Proposition 8.38] that there are finitely many *weakly integral fusion* categories of a given fixed rank through a number theoretic argument similar to that of Landau [33].

The proof of the rank-finiteness theorem relies upon several well-known reductions, a new result known as the Cauchy theorem (for spherical fusion categories 3.9) and some results in analytic number theory due to Evertse [25].

In Section 3.1, the Cauchy theorem for spherical fusion categories is proved, and in Section 3.2 we prove Theorem 3.1. We discuss asymptotics related to Theorem 3.1 in Section 4.

3.1. **The Cauchy theorem.** Let $\mathbb{A}$ be the ring of algebraic integers in $\mathbb{C}$. For $a, b, c \in \mathbb{A}$ with $a \neq 0$, $b \equiv c \bmod a$ means that $(b-c)/a \in \mathbb{A}$.

Suppose $\mathcal{C}$ is a modular category with $N = \mathrm{FSexp}(\mathcal{C})$ and q is prime with $(q, N) = 1$. We begin with a simple lemma, which is essentially proved in [59, Lemma 1.8] and [31, Section 3.4].

Lemma 3.2. *Let W be a finite-dimensional $\mathbb{C}$-linear space. If E is a $\mathbb{C}$-linear operator on W such that $E^q = \mathrm{id}_W$ for some prime number q, then*

$$\mathrm{Tr}(E)^q \equiv \dim_{\mathbb{C}} W \bmod q\,.$$

In particular, if $\mathrm{Tr}(E) \in \mathbb{Z}$, then $\mathrm{Tr}(E) \equiv \dim_{\mathbb{C}} W \bmod q$.

Proof. Let $\zeta_q \in \mathbb{C}$ denote a primitive qth root of unity. Then $\mathrm{Tr}(E) = \sum_{i=0}^{q-1} m_i \zeta_q^i$, where m_i is the multiplicity of the eigenvalue ζ_q^i. Thus,

$$\mathrm{Tr}(E)^q \equiv \sum_{i=0}^{q-1} m_i^q \equiv \sum_{i=0}^{q-1} m_i = \dim_{\mathbb{C}} W \bmod q\,.$$

In particular, if $\mathrm{Tr}(E) \in \mathbb{Z}$, the second statement follows from Fermat's little theorem. □

Recall that the nth Frobenius-Schur indicator $\nu_n(V)$ for $V \in \mathcal{C}$ is defined as the trace of a $\mathbb{C}$-linear operator $E_V^{(n)} : \mathrm{Hom}_{\mathcal{C}}(\mathbf{1}, V^{\otimes n}) \to \mathrm{Hom}_{\mathcal{C}}(\mathbf{1}, V^{\otimes n})$. This operator $E_V^{(n)}$ satisfies

$$\left(E_V^{(n)}\right)^n = \mathrm{id}\,.$$

Moreover, $\nu_n(V)$ is an algebraic integer in $\mathbb{Q}_n \cap \mathbb{Q}_N$. Since q and N are relatively prime, we have

$$\nu_q(V) \in \mathbb{Q}_N \cap \mathbb{Q}_q = \mathbb{Q}\,.$$

Thus $\nu_q(V) \in \mathbb{Z}$. By the preceding lemma, we have proved Lemma 3.3.

Lemma 3.3. *For any $V \in \mathcal{C}$, $\nu_q(V) \in \mathbb{Z}$, and we have*

$$\nu_q(V) \equiv \dim_{\mathbb{C}} \mathrm{Hom}_{\mathcal{C}}\left(\mathbf{1}, V^{\otimes q}\right) \bmod q\,.$$

Let $\mathcal{O}_N$ be the ring of algebraic integers of $\mathbb{Q}_N$. It is well known that $\mathcal{O}_N = \mathbb{Z}[\zeta_N]$, where ζ_N is a primitive Nth root of unity in $\mathbb{C}$. Set $K_N(\mathcal{C}) = K_0(\mathcal{C}) \otimes_{\mathbb{Z}} \mathcal{O}_N$. Then $K_N(\mathcal{C})$ is an $\mathcal{O}_N$-algebra. For any non-zero element $a \in \mathcal{O}_N$ and $\alpha, \beta \in K_N(\mathcal{C})$, we write $\alpha \equiv \beta \bmod a$ if $\alpha - \beta = a\gamma$ for some $\gamma \in K_N(\mathcal{C})$.

By [44], $\nu_q : K_0(\mathcal{C}) \to \mathbb{Z}$ is a group homomorphism; however, the assignment $V \mapsto \dim_{\mathbb{C}} \mathrm{Hom}_{\mathcal{C}}(\mathbf{1}, V^{\otimes q})$ is not. We can extend the ν_q to an $\mathcal{O}_N$-linear map from $K_N(\mathcal{C})$ to $\mathcal{O}_N$, and we continue to denote such an extension by ν_q. Similarly, we can

extend the dimension function $d : K_0(\mathcal{C}) \to \mathcal{O}_N$ to an $\mathcal{O}_N$-linear map from $K_N(\mathcal{C})$ to $\mathcal{O}_N$. However, it is important to note that this extension is an $\mathcal{O}_N$-*algebra* homomorphism.

Note that $K_N(\mathcal{C})$ is a free $\mathcal{O}_N$-module with $\Pi_{\mathcal{C}}$ as a basis. For $\alpha = \sum_{i\in\Pi_{\mathcal{C}}} \alpha_i i \in K_N(\mathcal{C})$, we define $\delta(\alpha) = \alpha_0$. Obviously, $\delta : K_N(\mathcal{C}) \to \mathcal{O}_N$ is $\mathcal{O}_N$-linear. Although $\delta(\alpha^q)$ is not $\mathcal{O}_N$-linear in α, it is $\mathbb{Z}$-linear modulo q.

Lemma 3.4. *For $\alpha \in K_N(\mathcal{C})$, we have*

$$\delta(\alpha^q) \equiv \sigma_q(\nu_q(\alpha)) \bmod q,$$

where $\sigma_q \in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$ is defined by $\sigma_q(\zeta_N) = \zeta_N^q$.

Proof. Let $\alpha = \sum_{i\in\Pi_{\mathcal{C}}} \alpha_i i$. Then $\alpha^q \equiv \sum_{i\in\Pi_{\mathcal{C}}} \alpha_i^q i^q \bmod q$. Since δ is $\mathcal{O}_N$-linear, we have

$$\delta(\alpha^q) \equiv \delta\Big(\sum_{i\in\Pi_{\mathcal{C}}} \alpha_i^q i^q\Big) = \sum_{i\in\Pi_{\mathcal{C}}} \alpha_i^q \delta(i^q) \bmod q\,.$$

Since $\delta(i^q) = \dim_{\mathbb{C}} \mathrm{Hom}_{\mathcal{C}}(\mathbf{1}, V_i^{\otimes q})$, it follows from Lemma 3.3 that

$$\delta(i^q) \equiv \nu_q(V) \bmod q\,.$$

Thus, we find

$$\delta(\alpha^q) \equiv \sum_{i\in\Pi_{\mathcal{C}}} \alpha_i^q \nu_q(V_i) \bmod q\,.$$

Note that for $a \in \mathcal{O}_N$, $a = \sum_j a_j \zeta_N^j$ where $a_j \in \mathbb{Z}$. Therefore,

$$a^q \equiv \sum_j a_j^q \zeta_N^{qj} \equiv \sum_j a_j \sigma_q(\zeta_N^j) = \sigma_q(a) \bmod q\,.$$

Hence, we have

$$\delta(\alpha^q) \equiv \sum_{i\in\Pi_{\mathcal{C}}} \sigma_q(\alpha_i)\nu_q(V_i) = \sigma_q(\nu_q(\alpha)) \bmod q\,.$$

The last equality follows from the $\mathcal{O}_N$-linearity of ν_q, and $\nu_q(V_i) \in \mathbb{Z}$ for all $i \in \Pi_{\mathcal{C}}$. □

By [44], $d_i \in \mathcal{O}_N$ for $i \in \Pi_{\mathcal{C}}$. Therefore, $R = \sum_{i\in\Pi_{\mathcal{C}}} d_i i$ is an element of $K_N(\mathcal{C})$.

Notice that R defines a rank 1 ideal of $K_N(\mathcal{C})$ as $iR = d_i R$ for all $i \in \Pi_{\mathcal{C}}$. Thus, for $\alpha \in K_N(\mathcal{C})$, $\alpha R = d(\alpha)R$, where $d : K_N(\mathcal{C}) \to \mathcal{O}_N$ is the extended dimension function. Therefore,

$$R^n = R^{n-1}R = d(R^{n-1})R = D^{2(n-1)}R\,.$$

Now, we can write our first proposition for the indicators of the *virtual* object R.

Proposition 3.5. *Let $R = \sum_{i\in\Pi_{\mathcal{C}}} d_i i \in K_N(\mathcal{C})$, and q a prime number not dividing N. Then we have*

$$\sigma_q\left(\nu_q(R)\right) \equiv D^{2(q-1)} \bmod q\,.$$

Proof. By the preceding discussion, we have $R^q = D^{2(q-1)}R$. Since $\delta(R) = d_0 = 1$, we have $\delta(R^q) = D^{2(q-1)}$. By Lemma 3.4,

$$\sigma_q(\nu_q(R)) \equiv D^{2(q-1)} \bmod q\,.$$ □

Proposition 3.6. *For any $\sigma \in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$, $d_{\hat{\sigma}(0)}$ is a unit of $\mathcal{O}_N$.*

Proof. Without loss of generality, we may assume $\hat{\sigma}(0) = 1$. Then

$$\sigma(\frac{1}{D^2}) = d_1^2/D^2 \quad \text{or} \quad d_1^2 = D^2/\sigma(D^2).$$

Obviously, the norm of $D^2/\sigma(D^2)$ is 1, and so is d_1^2. Therefore d_1 is a unit in $\mathcal{O}_N$. □

Remark 3.7. The preceding is another proof of the fact proved in [46] that D^2 is a d-number.

Proposition 3.8. $\nu_q(R) = d^2_{\hat{\sigma}_q^{-1}(0)}$.

Proof. Note that

$$\nu_q(R) = \sum_k d_k \nu_q(V_k) = \frac{1}{D^2} \sum_{i,j,k} d_k N_{ij}^k d_i d_j \frac{\theta_i^q}{\theta_j^q} = \frac{1}{D^2} \left(\sum_i d_i^2 \theta_i^q \right) \left(\sum_j d_j^2 \theta_j^{-q} \right) .$$

Choose y so that $s = S/D$ and $t = T/y$ give a modular representation. Reexpressing Equation (2.7), we find that

$$s_{00}^2 = \frac{1}{D^2} = \left(\sum_i s_{0i}^2 \theta_i \right) \left(\sum_j s_{0j}^2 \theta_j^{-1} \right) .$$

Let $\tau \in \mathrm{Aut}(\mathbb{Q}_{\mathrm{ab}})$ such that $\tau|_{\mathbb{Q}_N} = \sigma_q^{-1}$. Applying τ to this equation and applying (2.13), we find

$$s_{\hat{\tau}(0)0}^2 = d_{\hat{\tau}(0)}^2 s_{00}^2 = \left(\sum_i s_{0\hat{\tau}(i)}^2 \tau(\theta_i) \right) \left(\sum_j s_{0\hat{\tau}(j)}^2 \tau(\theta_j)^{-1} \right) .$$

By Galois symmetry, Theorem 2.9, we have

$$\tau(t_i) = \tau^{-1}\tau^2(t_i) = \tau^{-1}\left(t_{\hat{\tau}(i)}\right) = \frac{\theta^q_{\hat{\tau}(i)}}{\tau^{-1}(y)}$$

since $\tau^{-1}|_{\mathbb{Q}_N} = \sigma_q$. Therefore, in terms of $\theta_i = yt_i$, we get $\tau(\theta_i^{\pm 1}) = \theta^{\pm q}_{\hat{\tau}(i)} K^{\pm 1}$ for some constant K independent of i, which yields

$$d_{\hat{\tau}(0)}^2 s_{00}^2 = \left(\sum_i s_{0\hat{\tau}(i)}^2 \theta^q_{\hat{\tau}(i)} \right) \left(\sum_j s_{0\hat{\tau}(j)}^2 \theta^{-q}_{\hat{\tau}(j)} \right) .$$

Thus,

$$d_{\hat{\tau}(0)}^2 = \frac{1}{D^2} \left(\sum_i d_i^2 \theta_i^q \right) \left(\sum_j d_j^2 \theta_j^{-q} \right) = \nu_q(R) . \qquad \square$$

Theorem 3.9 (Cauchy theorem for spherical fusion categories)**.** *Let $\mathcal{C}$ be a spherical fusion category. Then the set of prime ideals dividing the principal ideal generated by D^2 is identical to that of $N = \mathrm{FSexp}(\mathcal{C})$ in $\mathcal{O}_N = \mathbb{Z}[e^{2\pi i/N}]$.*

Proof. We first consider the case when $\mathcal{C}$ is a modular category. Since $N \mid D^6$ [17], every prime ideal factor of N in $\mathcal{O}_N$ is a factor of D^2. Suppose $\mathfrak{p}$ is a prime ideal factor of D^2. By Propositions 3.5 and 3.8, we find the congruence

$$\sigma_q(d_i^2) \equiv D^{2(q-1)} \bmod q$$

for any prime $q \nmid N$ where $i = \hat{\sigma}_q^{-1}(0)$. By Proposition 3.6, d_i is a unit of $\mathcal{O}_N$. Therefore, we have the equality of ideals $\mathcal{O}_N = (D^2) + (q)$. This implies that $q \notin \mathfrak{p}$. Therefore, $\mathfrak{p} \cap \mathbb{Z} = (p)$ for some prime $p \mid N$. Hence, $\mathfrak{p}$ is a prime factor of N in $\mathcal{O}_N$.

Now, we assume $\mathcal{C}$ is a general spherical fusion category. Then its Drinfeld center $Z(\mathcal{C})$ is modular and $\dim Z(\mathcal{C}) = (\dim \mathcal{C})^2$ by [39]. Since $N = \mathrm{FSexp}(\mathcal{C}) = \mathrm{FSexp}(Z(\mathcal{C}))$ by [43], the theorem follows from the modular case, i.e. N and $(\dim \mathcal{C})^2$ have the same set of prime ideal factors in $\mathcal{O}_N$. □

Remark 3.10. If $\mathcal{C}$ is the category of representations of a finite group G, then $\mathrm{FSexp}(\mathcal{C}) = \exp(G)$ and $\dim \mathcal{C} = |G|$. The preceding theorem implies that p is a prime factor of $|G|$ if, and only if, $p \mid \exp(G)$; this is simply an equivalent statement of the classical Cauchy theorem for finite groups.

3.2. **Proof of rank-finiteness.** To prove Theorem 3.1, we first reduce to proving that there are finitely many possible fusion rules using (braided) Ocneanu rigidity, due to Ocneanu, Blanchard and Wassermann (unpublished), a proof of which may be found in [23].

Theorem 3.11. *There are only finitely many (braided, modular) fusion categories which have the same fusion rules up to (braided, modular) monoidal equivalence.*

Remark 3.12. Ocneanu rigidity for fusion categories was first proved by Blanchard and Wasserman, and the extension to the braided case can be found in [23, Remark 2.33]. For the finiteness of spherical structures see Lemma 2.4.

Next we may reduce to bounding the FP-dimension using (see e.g. [23, Proposition 8.38] and [49, Proposition 6.2]).

Corollary 3.13. *There are finitely many (braided, modular) fusion categories $\mathcal{C}$ satisfying $\mathrm{FPdim}(\mathcal{C}) \leq M$ for any fixed number $M > 0$, up to (braided, modular) monoidal equivalence.*

For the reader's convenience, we provide an explicit bound on the N_{ij}^k in terms of $\mathrm{FPdim}(\mathcal{C})$ for fusion categories.

Lemma 3.14. *If $\mathcal{C}$ is a rank n fusion category, then for $a \in \Pi_{\mathcal{C}}$, we have the inequality*

$$\|N_a\|_{\max} \leq \mathrm{FPdim}(V_a) \leq n\|N_a\|_{\max},$$

where $\|A\|_{\max}$ is the max-norm of the complex matrix A given by

$$\|A\|_{max} = \max_{i,j} |A_{ij}| .$$

Proof. Note that

$$R_0 = \sum_{a \in \Pi_{\mathcal{C}}} \mathrm{FPdim}(a) a$$

generates a one-dimensional ideal of $K_{\mathbb{C}}(\mathcal{C}) = K_0(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{C}$, and that $aR_0 = \mathrm{FPdim}(V_a)R_0$ for all $a \in \Pi_{\mathcal{C}}$. In particular, there is unit vector x with positive components such that $N_a x = \mathrm{FPdim}(V_a)x$ for all $a \in \Pi_{\mathcal{C}}$.

Let $\rho(A)$ denote the spectral radius of an $n\times n$ complex matrix A. Recall that the 2-norm of A is given by $\|A\|_2 = \sqrt{\rho(A^*A)}$. Thus, for $a \in \Pi_{\mathcal{C}}$, $\|N_a\|_2 \geq \mathrm{FPdim}(V_a)$. On the other hand,

$$\|N_a\|_2^2 = \rho(N_a^* N_a) = \rho(N_{a^*} N_a) = \rho\left(\sum_{b\in\Pi_{\mathcal{C}}} N_{a^*,a}^b N_b\right)$$
$$\leq \sum_{b\in\Pi_{\mathcal{C}}} N_{a^*,a}^b \,\mathrm{FPdim}(V_b) = \mathrm{FPdim}(V_a^*)\,\mathrm{FPdim}(V_a) = \mathrm{FPdim}(V_a)^2\,.$$

Therefore, $\|N_a\|_2 = \mathrm{FPdim}(V_a)$ for all $a \in \Pi_{\mathcal{C}}$. The result then follows by the inequality

$$\|A\|_{\max} \leq \|A\|_2 \leq n\|A\|_{\max}$$

for any $n \times n$ complex matrix A. □

Next we give an explicit bound on $\mathrm{ord}(T)$ in terms of the rank of $\mathcal{C}$.

Proposition 3.15. *If $\mathcal{C}$ is a modular category of rank r with modular data (S,T), then* $\mathrm{ord}(T) \leq 2^{2r/3+8}3^{2r/3}$.

Proof. By [9], any abelian subgroup G of $\mathfrak{S}_r$ satisfies $|G| \leq 3^{r/3}$. On the other hand, since $\mathrm{Gal}(\mathbb{F}_T/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^*$, by Lemma 2.10, $[\mathbb{F}_T : \mathbb{F}_S] \leq 2^m$ where $m-1$ is the number of prime factors of $\mathrm{ord}(T)$. The fundamental theorem of Galois theory can be utilized to relate m and $[\mathbb{F}_S : \mathbb{Q}]$. To do this, we note that

$$\mathrm{Gal}(\mathbb{F}_S/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{F}_T/\mathbb{Q})\,/\mathrm{Gal}(\mathbb{F}_T/\mathbb{F}_S)\,,$$

where

$$\mathrm{Gal}(\mathbb{F}_T/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^* \cong \prod_i (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$$

in terms of distinct prime-power cyclic subgroups. Since $\mathrm{Gal}(\mathbb{F}_T/\mathbb{F}_S)$ is an elementary 2-group by Lemma 2.10, we see that at least $m-3$ (non-trivial) cyclic factors survive in the quotient (the three possible exceptions correspond to primes 2 and 3 in $\mathrm{ord}(T)$). The structure of the maximal abelian subgroup of $\mathfrak{S}_r$ ensures that $m-3 \leq r/3+1$. It follows that

$$[\mathbb{F}_T : \mathbb{Q}] = [\mathbb{F}_T : \mathbb{F}_S]\,[\mathbb{F}_S : \mathbb{Q}] \leq 2^m 3^{r/3} \leq 2^{r/3+4}3^{r/3}\,.$$

On the other hand, $\mathbb{F}_T = \mathbb{Q}_{\mathrm{ord}(T)}$ and so $[\mathbb{F}_T : \mathbb{Q}] = \varphi(\mathrm{ord}(T))$. In particular, if $\mathrm{ord}(T) \neq 2$ or 6, then $[\mathbb{F}_T : \mathbb{Q}] \geq \sqrt{\mathrm{ord}(T)}$. Thus $\mathrm{ord}(T) \leq 2^{2r/3+8}3^{2r/3}$ since $2^{2/3+8}3^{2/3} > 6$. □

The last ingredient of the proof of Theorem 3.1 is a deep result from analytic number theory, which necessitates some further notation and background.

Definition 3.16. Let $\mathbb{K}$ be a number field and $\mathcal{S}$ be a finite set of prime ideals in the ring $\mathcal{O}_{\mathbb{K}}$ of algebraic integers of $\mathbb{K}$. An element $\alpha \in \mathbb{K}^\times$ is a *$\mathcal{S}$-unit* if the prime factors of the principal fractional ideal (α) are all in $\mathcal{S}$.

Remark 3.17. The $\mathcal{S}$-units form a finitely generated multiplicative abelian group which we will denote by $\mathcal{O}_{\mathbb{K},\mathcal{S}}^\times$ [60].

Remark 3.18. It should be noted that $\mathcal{S}$-units are often treated adelically in which case a more delicate treatment involving places is required. While we will not need this level of detail here, it should be mentioned that it is utilized in [25]. A detailed introduction to $\mathcal{S}$-units and their relationship to adeles can be found in most modern texts on advanced number theory, e.g. [60].

The $\mathcal{S}$-units arise in a wide range of subdisciplines in number theory and are typically found to obey an *$\mathcal{S}$-unit equation*,

$$x_0 + \cdots + x_n = 0, \quad \text{such that} \quad x_a \in \mathcal{O}_{\mathbb{K},\mathcal{S}}^{\times}.$$

Such an equation is said to be a *proper $\mathcal{S}$-unit equation* if one requires that

$$x_{i_0} + \cdots + x_{i_r} \neq 0$$

for each proper, non-empty subset $\{i_0, i_1, \ldots, i_r\}$ of $\{0, 1, \ldots, n\}$.

In 1984, Evertse took up a study of $\mathcal{S}$-units and the $\mathcal{S}$-unit equation through analyzing the projective height [25]. By bounding the projective height, he showed that $\mathcal{S}$-units obey a remarkable finiteness condition *loc. cit.*

Theorem 3.19. *If $\mathbb{K}$ is a number field, $\mathcal{S}$ is a finite set of primes of $\mathcal{O}_{\mathbb{K}}$, and n is a fixed positive integer, then there are only finitely many projective points $X = [x_0 : \cdots : x_n] \in \mathbb{P}^n\mathbb{K}$ satisfying the proper $\mathcal{S}$-unit equation,*

$$x_0 + \cdots + x_n = 0.$$

With this last ingredient we can now proceed to the following proof.

Proof of the rank-finiteness theorem. For fixed rank r, [3, Proposition 6] (or Proposition 3.15) ensures that $\operatorname{ord}(T)$ is bounded strictly in terms of r. For such $\operatorname{ord}(T)$, let $\mathcal{S}$ be the (finite) set of primes in $\mathcal{O}_{\operatorname{ord}(T)}$ dividing $\operatorname{ord}(T)$. The Cauchy theorem (Theorem 3.9) coupled with [20, Lemma 1.2] then implies that D^2 and d_a are $\mathcal{S}$-units for all simple objects V_a. Furthermore, the definition of the global dimension of the category, $0 = D^2 - d_0^2 - \cdots - d_{r-1}^2$, and the condition that d_a^2 and D^2 are real positive algebraic integers for all a implies that $\left(D^2, -d_0^2, \ldots, -d_{r-1}^2\right)$ satisfies a proper $\mathcal{S}$-unit equation. In particular, Theorem 3.19 shows that there are finitely many projective solutions to this equation. Recalling that $d_0^2 = 1$ allows us to fix the normalization and conclude that there is an upper bound on D^2 and a lower bound on d_a for all a.

On the other hand, $\operatorname{FPdim}(\mathcal{C}) = D^2/d_a^2$ for some simple dimension d_a. Consequently, the lower bound on d_a and an upper bound on D^2 imply an upper bound on $\operatorname{FPdim}(\mathcal{C})$. The result then follows from Corollary 3.13 and the observation that these bounds depend only on the rank. □

3.3. **Extensions of rank-finiteness.** A premodular category $\mathcal{C}$ is called *modularizable* [6] if there exists a modular category $\mathcal{D}$ and a dominant ribbon functor $F : \mathcal{C} \to \mathcal{D}$. For a premodular category $\mathcal{C}$ the failure of modularity is encoded in the *Müger centralizer* $\mathcal{C}'$—the symmetric fusion subcategory of $\mathcal{C}$ generated by all X such that $c_{X,Y}c_{Y,X} = \mathrm{id}_{X\otimes Y}$ for all objects Y [40]. It is known ([6, Cor. 3.5], [13]) $\mathcal{C}$ is modularizable if and only if $\mathcal{C}' \cong \operatorname{Rep}(G)$ as a symmetric fusion category, for some finite group G (i.e. $\mathcal{C}'$ is Tannakian). Modularization is a special case of a general construction called *de-equivariantization* [15] in which one quotients out an action of a finite group G on a category $\mathcal{C}$ obtaining a new category $\mathcal{C}_G$.

The inverse operation *equivariantization* gives a way to recover $\mathcal{C}$ from $\mathcal{C}_G$. We can easily extend rank-finiteness to modularizable premodular categories.

Corollary 3.20. *There are finitely many modularizable, premodular categories of rank r.*

Proof. We follow the notation in [15]. Let $\mathcal{C}$ be a premodular category such that $\mathcal{C}' \cong \mathrm{Rep}(G)$ is Tannakian and $\mathcal{C}_G = \mathcal{D}$ its modularization. Note that the equivariantization $\mathcal{D}^G \cong \mathcal{C}$ by [15]. First observe that under the (faithful) forgetful functor $\mathcal{C} \to \mathcal{D}$ the image of each simple object $X \in \mathcal{C}$ is a sum of at most $|G|$ distinct simple objects in $\mathcal{D}$ (see [7, Prop. 2.1]). Since the rank of $\mathrm{Rep}(G)$ is at most r, $|G|$ is bounded as a function of r [33]. Therefore, the rank of $\mathcal{C}_G$ is bounded in terms of r. By Theorem 3.1 there are only finitely many modularizations of rank r premodular categories. On the other hand, each modular category $\mathcal{D}$ has only finitely many equivariantizations of bounded rank for groups of bounded order [22]. □

We remark that to extend rank-finiteness to all premodular categories, it is enough to consider only premodular categories with $\mathcal{C}' \cong sVec$. Indeed, if $\mathrm{Rep}(G) \subset \mathcal{C}'$ is a maximal central Tannakian subcategory, then the de-equivariantization $\mathcal{C}_G$ is premodular with no Tannakian subcategories. Hence, the resulting category is either modular or has $\mathcal{C}' \cong sVec$ (cf. [15]).

We have assumed throughout that $\mathcal{C}$ has base field $\mathbb{C}$. A referee pointed out that rank-finiteness for modular categories holds in more general settings.

First, it is clear that these results are equally valid over an algebraically closed field of characteristic 0. Second, [19, Proposition 3.8] implies that there are only finitely many rational forms for modular categories, so rank-finiteness holds over any field of characteristic 0.

Over fields of characteristic p, rank-finiteness can be extended for modular categories $\mathcal{C}$ with $D^2 \neq 0$. By applying the methods of [23, Section 9], we see that such a category has finitely many lifts to a field of characteristic 0, and equivalence of the lifts implies equivalence of the original categories.

4. Asymptotics and future directions

4.1. **Asymptotics.** The proof of Theorem 3.1 can be naively algorithmized to determine possible sets of fusion rules for modular categories of a given rank r.

Recall that $\mathcal{O}^{\times}_{\mathbb{K},\mathcal{S}}$ is a finitely generated abelian group [60]. A set of generators for the free part of $\mathcal{O}^{\times}_{\mathbb{K},\mathcal{S}}$ is known as a *system of fundamental $\mathcal{S}$-units* and there are known algorithms for computing such a system, e.g. [10]. We have the following algorithm.

Algorithm 4.1.

(0) Specify the rank, r.

(1) For each integer N with $1 \leq N \leq 2^{2r/3+8}3^{2r/3}$ perform steps 2–6.

(2) Form the set of primes $\mathcal{S}$, consisting of the prime factors of N over $\mathbb{Q}(\zeta_N)$.

(3) Determine a fundamental system of $\mathcal{S}$-units, $\epsilon_1, \ldots, \epsilon_{s-1}$.

(4) Solve the exponential Diophantine system,

$$1 = \epsilon_1^{a_{r,1}} \cdots \epsilon_{s-1}^{a_{r,s-1}} - \sum_{j=1}^{r-1} \epsilon_1^{a_{j,1}} \cdots \epsilon_{s-1}^{a_{j,s-1}}, \qquad a_{j,k} \in \mathbb{Z}\,. \tag{4.1}$$

(5) Set $D^2 = \epsilon_1^{a_{s,1}} \cdots \epsilon_{s-1}^{a_{s,s-1}}$ and $d_j^2 = \epsilon_1^{a_{j,1}} \cdots \epsilon_{s-1}^{a_{j,s-1}}$.

(6) Determine the possible sets of fusion rules $N_{a,b}^c$ using Lemma 3.14 and the fact that $\mathrm{FPdim}(V_a) \leq \mathrm{FPdim}(\mathcal{C}) \leq \max\{D^2/d_j^2 : 0 \leq j \leq r-1\}$.

Remark 4.2. Given all possible sets of fusion rules in a given rank we can solve for all admissible modular data. The balancing equation (2.3) determines the S-matrix given all d_i, θ_i, and N_{ij}^k, which Algorithm 4.1 provides.

We can also effectively decide whether a particular set of fusion rules corresponds to a modular category, using Tarski's theorem (see [12]). We cannot, however, effectively determine all modular categories in a given rank, or even count them up to equivalence.

In any case, Algorithm 4.1 is very inefficient, and does not admit any obvious improvements for several reasons.

First, we cannot expect a bound on $\mathrm{ord}\,(T)$ that is polynomial in the rank. For example, $\mathrm{ord}\,(T)$ for $\mathcal{C} = \mathrm{Rep}\,(D\mathfrak{S}_n)$ grows faster than any polynomial in the rank of $\mathcal{C}$. Indeed, $\mathrm{ord}(T) = \exp(\mathfrak{S}_n) = \mathrm{lcm}(1, \ldots, n) \approx e^n$, while the rank of $\mathrm{Rep}(D\mathfrak{S}_n)$ is superpolynomial but subexponential, with generating function: $\Pi_{k=1}^{\infty}(1-x^k)^{-\sigma(k)}$ where $\sigma(k) = \sum_{d|k} d$ [5]. However, for modular categories coming from quantum groups, $\mathrm{ord}(T)$ is linearly bounded in r. Second, the known algorithms for computing fundamental systems of $\mathcal{S}$-units rely on computing a shortest vector in a lattice, a problem which is known to be NP-hard. Third, solving Equation (4.1) is very difficult—our best bound on the number of solutions is quadruplely exponential.

Proposition 4.3. *For fixed rank r there are at most*

$$\sum_{m=1}^{2^{2r/3+8}3^{2r/3}} \left(2^{35}r^2\right)^{r^3\left(\varphi(m)^{\log_2(m)}+\varphi(m)/2+1\right)-r/2}$$

possible solutions to the dimension equation,

$$D^2 = 1 + d_1^2 + \cdots + d_{r-1}^2\,.$$

Proof. First note that by [26, Theorem 3], there are at most $\left(2^{35}r^2\right)^{r^3(s+r_1+r_2)-r/2}$ solutions to the proper $\mathcal{S}$-unit equation,

$$x_1 + x_2 + \cdots + x_r = 1,$$

subject to $x_j \leq x_{j+1}$ over a field $\mathbb{K}$, where s is the cardinality of $\mathcal{S}$, r_1 is the number of real embeddings of $\mathbb{K}$, and r_2 is the number of conjugate pair complex embeddings.

However, s depends on the prime factorization of $\mathrm{ord}\,(T)$. In particular, if p is a rational prime of $\mathrm{ord}\,(T)$, and there are at worst $\varphi\,(\mathrm{ord}\,(T))$ primes lying over p in $\mathbb{Q}\left(\zeta_{\mathrm{ord}(T)}\right)$. Thus there are at most $\mathrm{ord}\,(T)^{\omega(\mathrm{ord}(T))}$ primes in $\mathcal{S}$, where $\omega\,(m)$ is defined to be the number of rational prime divisors of m. Elementary analysis reveals that $\omega\,(m) \leq \log_2\,(m)$, and so $s \leq \varphi\,(\mathrm{ord}\,(T))^{\log_2(\mathrm{ord}(T))} + r_1 + r_2$ where r_1 is the number of distinct real field embeddings of $\mathbb{K}$ into $\mathbb{C}$, and r_2 is the number

of conjugate pair complex field embeddings. However, it is well-known that a non-trivial cyclotomic field has no real embeddings, in particular $r_2 = \varphi(\operatorname{ord}(T))/2$ and $s + r_1 + r_2 \leq \varphi(\operatorname{ord}(T))^{\log_2 \operatorname{ord}(T)} + \varphi(\operatorname{ord}(T))/2 + 1$. Combining these two results reveals that an upper bound on the number of possible dimension tuples $\left(D^2, 1, d_1^2, \ldots, d_{r-1}^2\right)$ for a rank r modular category with T-matrix of order $\operatorname{ord}(T)$ is $\left(2^{35} r^2\right)^{r^3 \left(\varphi(\operatorname{ord}(T))^{\log_2(\operatorname{ord}(T))} + \varphi(\operatorname{ord}(T))/2 + 1\right) - r/2}$. The result then follows by summing over all possible values of $\operatorname{ord}(T)$ as determined by Proposition 3.15. □

Low-rank classification suggests that these bounds are far from sharp. We ask the following question.

Question 4.4. *Is there an asymptotic bound on the number of modular categories (up to equivalence) in terms of the rank which is better than those implied by Proposition 4.3?*

Remark 4.5. Etingof [18] has pointed out that the number of modular categories of rank r is not polynomially bounded. His example is as follows: Consider $V = (\mathbb{Z}/p)^m$, a vector space over F_p of dimension m, where $p > 3$ is a prime and m is large. It is well-known that $H^3(V, \mathbb{C}^*) = S^2V^* \oplus \wedge^3 V^*$ (see e.g. [21, Lemma 7.6(iii)]). Because of the summand $\wedge^3 V^*$, the number of such cohomology classes for large m is at least p^{Cm^3}, for some $C > 0$, even if we mod out by automorphisms (which form a group of order at most p^{m^2}). Now take the category $\operatorname{Vec}(V, \omega)$ of V-graded vector spaces with associativity defined by the cohomology class ω, and let $Z(V, \omega)$ be the Drinfeld center of such a category. It is known [22] that such categories $Z(V, \omega)$ and $Z(V, \omega')$ are braided equivalent if and only if $\operatorname{Vec}(V, \omega)$ is Morita equivalent to $\operatorname{Vec}(V, \omega')$ via an indecomposable module category. But the indecomposable module categories over $\operatorname{Vec}(V, \omega)$ are known to be parameterized [47] by subspaces $W \subset V$ and 2-cochain ψ on W such that $d\psi = \omega|_W$, up to gauge transformation. There are at most p^{m^2} subspaces, and freedom in choosing ψ is in $\wedge^2 W^*$, so again there are at most p^{m^2}. As m^3 dominates m^2, we still have at least p^{Cm^3} such categories, even up to Morita equivalence, and hence modular categories up to equivalence. On the other hand, $\operatorname{FPdim}(Z(V, \omega)) = p^{2m}$, so the rank is at most p^{2m}. Thus we get that the number of modular categories of rank$\leq r$ is at least $e^{(c \log(r)^3)} = r^{c \log(r)^2}$, for some $c > 0$, which is faster than any polynomial in r.

Along similar lines, one might ask the following question.

Question 4.6. *Is there an explicit upper bound on* $\operatorname{FPdim}(\mathcal{C})$ *solely in terms of the rank?*

Remark 4.7. This question seems tractable as the analysis of Evertse shows that the projective height of $\left[-D^2 : 1 : d_1^2 : \cdots : d_{r-1}^2\right]$ can be bounded in terms of field data and hence in terms of $\operatorname{ord}(T)$. This suggests that the relationship between the FP-dimension and the categorical dimension can be combined, as in the proof of Theorem 3.1, to study this question.

On the other hand, Etingof asked [18] the following question.

Question 4.8. *Can* $\left|D^2 - 1\right|$ *be explicitly bounded away from* 0 *in terms of the rank?*

Remark 4.9. This question can be reduced to the problem of finding a shortest vector by exploiting the lattice structure of $\mathcal{O}_{\mathbb{K},S}^{\times}$ under an appropriate embedding into Euclidean space.

4.2. **Future directions.** Besides obtaining better asymptotics and classification of low rank modular categories, there are several other open problems.

Physicists propose to use the modular S, T matrices as order parameters for the classification of topological phases of matter [35]. Therefore, a natural question is if a modular category is uniquely determined by its modular S, T matrices. We believe that unitary modular categories are determined by their modular S, T matrices.

The S, T matrices satisfy many constraints as given in Section 2.2.6. It is interesting to characterize realizable modular data in terms of such constraints, in particular, whether or not admissible modular data are always realizable.

For the application to topological quantum computation, it is important to understand the images of the representations of the mapping class groups from a modular category. In particular, when do all representations have finite images? If so, which finite groups arise as such images? The property F conjecture says that the representations of all mapping class groups from a modular category have finite images if and only if $D^2 \in \mathbb{Z}$ [41,49].

Acknowledgments

This project began at a workshop at the American Institute of Mathematics and was completed while the third author was visiting the Beijing International Center for Mathematical Research, Peking University—the support and hospitality of both institutions are gratefully acknowledged. The authors thank Vladimir Turaev and Pavel Etingof for valuable comments.

References

[1] B. Bakalov and A. Kirillov Jr., *Lectures on tensor categories and modular functors*, University Lecture Series, vol. 21, American Mathematical Society, Providence, RI, 2001. MR1797619 (2002d:18003)

[2] P. Bantay, *The Frobenius-Schur indicator in conformal field theory*, Phys. Lett. B **394** (1997), no. 1-2, 87–88, DOI 10.1016/S0370-2693(96)01662-0. MR1436801 (98c:81195)

[3] P. Bantay, *The kernel of the modular representation and the Galois action in RCFT*, Comm. Math. Phys. **233** (2003), no. 3, 423–438, DOI 10.1007/s00220-002-0760-x. MR1962117 (2004g:81240)

[4] J. de Boer and J. Goeree, *Markov traces and* II_1 *factors in conformal field theory*, Comm. Math. Phys. **139** (1991), no. 2, 267–304. MR1120140 (93i:81211)

[5] J. R. Britnell, *A formal identity involving commuting triples of permutations*, J. Combin. Theory Ser. A **120** (2013), no. 4, 941–943, DOI 10.1016/j.jcta.2013.01.009. MR3022621

[6] A. Bruguières, *Catégories Prémodulaires, Modularisations et Invariants des Variétés de Dimension 3*, Math. Ann. **316** (2000), 215–236.

[7] S. Burciu and S. Natale, *Fusion rules of equivariantizations of fusion categories*, J. Math. Phys. **54** (2013), no. 1, 013511, 21, DOI 10.1063/1.4774293. MR3059899

[8] F. J. Burnell, X. Chen, L. Fidowski, and A. Vishwanath, *Exactly Soluble Models of a 3D Symmetry Protected Topological Phase of Bosons with Surface Topological Order*, available at `arXiv:1302.7072v1`.

[9] J. M. Burns and B. Goldsmith, *Maximal order abelian subgroups of symmetric groups*, Bull. London Math. Soc. **21** (1989), no. 1, 70–72, DOI 10.1112/blms/21.1.70. MR967793 (89i:20013)

[10] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000. MR1728313 (2000k:11144)

[11] A. Coste and T. Gannon, *Remarks on Galois symmetry in rational conformal field theories*, Phys. Lett. B **323** (1994), no. 3-4, 316–321, DOI 10.1016/0370-2693(94)91226-2. MR1266785 (95h:81031)

[12] C. Davidovich, T. Hagge, and Z. Wang, *On Arithmetic Modular Categories*, available at `arXiv:1305.2229`.

[13] P. Deligne, *Catégories tensorielles* (French, with English summary), Mosc. Math. J. **2** (2002), no. 2, 227–248. Dedicated to Yuri I. Manin on the occasion of his 65th birthday. MR1944506 (2003k:18010)

[14] C. Dong, X. Lin, and S.-H. Ng, *Congruence Property in Conformal Field Theory*, available at `arXiv:1201.6644v5`.

[15] V. Drinfeld, S. Gelaki, D. Nikshych, and V. Ostrik, *On braided fusion categories. I*, Selecta Math. (N.S.) **16** (2010), no. 1, 1–119, DOI 10.1007/s00029-010-0017-z. MR2609644 (2011e:18015)

[16] P. Etingof, *On some properties of quantum doubles of finite groups*, J. Algebra **394** (2013), 1–6, DOI 10.1016/j.jalgebra.2013.07.004. MR3092709

[17] P. Etingof, *On Vafa's theorem for tensor categories*, Math. Res. Lett. **9** (2002), no. 5-6, 651–657, DOI 10.4310/MRL.2002.v9.n5.a8. MR1906068 (2003i:18009)

[18] P. Etingof. Private communication, Feb. 2013.

[19] P. Etingof and S. Gelaki, *Descent and forms of tensor categories*, Int. Math. Res. Not. IMRN **13** (2012), 3040–3063, DOI 10.1093/imrn/rnr119. MR2946231

[20] P. Etingof and S. Gelaki, *Some properties of finite-dimensional semisimple Hopf algebras*, Math. Res. Lett. **5** (1998), no. 1-2, 191–197, DOI 10.4310/MRL.1998.v5.n2.a5. MR1617921 (99e:16050)

[21] P. Etingof, S. Gelaki, and V. Ostrik, *Classification of fusion categories of dimension pq*, Int. Math. Res. Not. **57** (2004), 3041–3056, DOI 10.1155/S1073792804131206. MR2098028 (2005m:18008)

[22] P. Etingof, D. Nikshych, and V. Ostrik, *Fusion categories and homotopy theory*, Quantum Topol. **1** (2010), no. 3, 209–273, DOI 10.4171/QT/6. With an appendix by Ehud Meir. MR2677836 (2011h:18007)

[23] P. Etingof, D. Nikshych, and V. Ostrik, *On fusion categories*, Ann. of Math. (2) **162** (2005), no. 2, 581–642, DOI 10.4007/annals.2005.162.581. MR2183279 (2006m:16051)

[24] D. E. Evans and Y. Kawahigashi, *Quantum symmetries on operator algebras*, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1998. Oxford Science Publications. MR1642584 (99m:46148)

[25] J.-H. Evertse, *On sums of S-units and linear recurrences*, Compos. Math. **53** (1984), no. 2, 225–244. MR766298 (86c:11045)

[26] J.-H. Evertse, *The number of solutions of decomposable form equations*, Invent. Math. **122** (1995), no. 3, 559–601, DOI 10.1007/BF01231456. MR1359604 (96i:11034)

[27] J. Fuchs, A. Ch. Ganchev, K. Szlachányi, and P. Vecsernyés, *S_4 symmetry of 6j symbols and Frobenius-Schur indicators in rigid monoidal C^* categories*, J. Math. Phys. **40** (1999), no. 1, 408–426, DOI 10.1063/1.532778. MR1657800 (99k:81111)

[28] S. Gelaki and D. Nikshych, *Nilpotent fusion categories*, Adv. Math. **217** (2008), no. 3, 1053–1071, DOI 10.1016/j.aim.2007.08.001. MR2383894 (2009b:18015)

[29] Y.-Z. Huang, *Vertex operator algebras, the Verlinde conjecture, and modular tensor categories*, Proc. Natl. Acad. Sci. USA **102** (2005), no. 15, 5352–5356 (electronic), DOI 10.1073/pnas.0409901102. MR2140309 (2006a:17026)

[30] A. Joyal and R. Street, *Braided tensor categories*, Adv. Math. **102** (1993), no. 1, 20–78, DOI 10.1006/aima.1993.1055. MR1250465 (94m:18008)

[31] Y. Kashina, Y. Sommerhäuser, and Y. Zhu, *On higher Frobenius-Schur indicators*, Mem. Amer. Math. Soc. **181** (2006), no. 855, viii+65, DOI 10.1090/memo/0855. MR2213320 (2007k:16071)

[32] C. Kassel, *Quantum groups*, Graduate Texts in Mathematics, vol. 155, Springer-Verlag, New York, 1995. MR1321145 (96e:17041)

[33] E. Landau, *Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante* (German), Math. Ann. **56** (1903), no. 4, 671–676, DOI 10.1007/BF01444311. MR1511192

[34] V. Linchenko and S. Montgomery, *A Frobenius-Schur theorem for Hopf algebras*, Algebr. Represent. Theory **3** (2000), no. 4, 347–355, DOI 10.1023/A:1009949909889. Special issue dedicated to Klaus Roggenkamp on the occasion of his 60th birthday. MR1808131 (2001k:16073)

[35] F. Liu, Z. Wang, Y.-Z. You, and X.-G. Wen, *Quantum fidelity, modular transformations, and topological orders in two dimensions*, available at `arXiv:1303.0829`.

[36] S. MacLane, *Categories for the working mathematician*, Springer-Verlag, New York-Berlin, 1971. Graduate Texts in Mathematics, Vol. 5. MR0354798 (50 #7275)

[37] G. Mason and S.-H. Ng, *Central invariants and Frobenius-Schur indicators for semisimple quasi-Hopf algebras*, Adv. Math. **190** (2005), no. 1, 161–195, DOI 10.1016/j.aim.2003.12.004. MR2104908 (2005h:16066)

[38] G. Moore and N. Seiberg, *Classical and quantum conformal field theory*, Comm. Math. Phys. **123** (1989), no. 2, 177–254. MR1002038 (90e:81216)

[39] M. Müger, *From subfactors to categories and topology. II. The quantum double of tensor categories and subfactors*, J. Pure Appl. Algebra **180** (2003), no. 1-2, 159–219, DOI 10.1016/S0022-4049(02)00248-7. MR1966525 (2004f:18014)

[40] M. Müger, *On the structure of modular categories*, Proc. Lond. Math. Soc. (3) **87** (2003), no. 2, 291–308, DOI 10.1112/S0024611503014187. MR1990929 (2004g:18009)

[41] D. Naidu and E. C. Rowell, *A finiteness property for braided fusion categories*, Algebr. Represent. Theory **14** (2011), no. 5, 837–855, DOI 10.1007/s10468-010-9219-5. MR2832261

[42] S.-H. Ng and P. Schauenburg, *Central invariants and higher indicators for semisimple quasi-Hopf algebras*, Trans. Amer. Math. Soc. **360** (2008), no. 4, 1839–1860, DOI 10.1090/S0002-9947-07-04276-6. MR2366965 (2009d:16065)

[43] S.-H. Ng and P. Schauenburg, *Congruence subgroups and generalized Frobenius-Schur indicators*, Comm. Math. Phys. **300** (2010), no. 1, 1–46, DOI 10.1007/s00220-010-1096-6. MR2725181 (2012g:81193)

[44] S.-H. Ng and P. Schauenburg, *Frobenius-Schur indicators and exponents of spherical categories*, Adv. Math. **211** (2007), no. 1, 34–71, DOI 10.1016/j.aim.2006.07.017. MR2313527 (2008b:16067)

[45] S.-H. Ng and P. Schauenburg, *Higher Frobenius-Schur indicators for pivotal categories*, Hopf algebras and generalizations, Contemp. Math., vol. 441, Amer. Math. Soc., Providence, RI, 2007, pp. 63–90, DOI 10.1090/conm/441/08500. MR2381536 (2008m:18015)

[46] V. Ostrik, *On formal codegrees of fusion categories*, Math. Res. Lett. **16** (2009), no. 5, 895–901, DOI 10.4310/MRL.2009.v16.n5.a11. MR2576705 (2011a:18005)

[47] V. Ostrik, *Module categories over the Drinfeld double of a finite group*, Int. Math. Res. Not. **27** (2003), 1507–1520, DOI 10.1155/S1073792803205079. MR1976233 (2004h:18005)

[48] N. Reshetikhin and V. G. Turaev, *Invariants of* 3*-manifolds via link polynomials and quantum groups*, Invent. Math. **103** (1991), no. 3, 547–597, DOI 10.1007/BF01239527. MR1091619 (92b:57024)

[49] E. Rowell, R. Stong, and Z. Wang, *On classification of modular tensor categories*, Comm. Math. Phys. **292** (2009), no. 2, 343–389, DOI 10.1007/s00220-009-0908-z. MR2544735 (2011b:18013)

[50] P. Schauenburg, *On the Frobenius-Schur indicators for quasi-Hopf algebras*, J. Algebra **282** (2004), no. 1, 129–139, DOI 10.1016/j.jalgebra.2004.08.015. MR2095575 (2005h:16068)

[51] Y. Sommerhäuser and Y. Zhu, *Hopf algebras and congruence subgroups*, Mem. Amer. Math. Soc. **219** (2012), no. 1028, vi+134, DOI 10.1090/S0065-9266-2012-00649-6. MR2985696

[52] V. G. Turaev, *Quantum invariants of knots and 3-manifolds*, de Gruyter Studies in Mathematics, vol. 18, Walter de Gruyter & Co., Berlin, 1994. MR1292673 (95k:57014)

[53] V. G. Turaev, *Modular categories and* 3*-manifold invariants*, Internat. J. Modern Phys. B **6** (1992), no. 11-12, 1807–1824, DOI 10.1142/S0217979292000876. Topological and quantum group methods in field theory and condensed matter physics. MR1186845 (93k:57040)

[54] C. Vafa, *Toward classification of conformal theories*, Phys. Lett. B **206** (1988), no. 3, 421–426, DOI 10.1016/0370-2693(88)91603-6. MR944264 (89k:81178)

[55] K Walker and Z. Wang, $(3+1)$*-TQFTS and Topological Insulators*, Front. Phys. **7** (2012), no. 2, 150–159.

[56] Z. Wang, *Quantum computing: a quantum group approach*, Symmetries and groups in contemporary physics, Nankai Ser. Pure Appl. Math. Theoret. Phys., vol. 11, World Sci. Publ., Hackensack, NJ, 2013, pp. 41–50, DOI 10.1142/9789814518550_0009. MR3221449

[57] Z. Wang, *Topological quantum computation*, CBMS Regional Conference Series in Mathematics, vol. 112, Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2010. MR2640343 (2011f:81054)
[58] Z. Wang, *Topologization of electron liquids with Chern-Simons theory and quantum computation*, Differential geometry and physics, Nankai Tracts Math., vol. 10, World Sci. Publ., Hackensack, NJ, 2006, pp. 106–120. MR2322390 (2008g:81301)
[59] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR1421575 (97h:11130)
[60] E. Weiss, *Algebraic number theory*, Chelsea Publishing Co., New York, 1976. Reprinting of the 1963 original. MR0417112 (54 #5172)

Department of Mathematics, Texas A&M University, College Station, Texas 77843
E-mail address: pjb2357@gmail.com
Current address: Pacific Northwest National Laboratory, 902 Battelle Boulevard, Richland, Washington 99354

Department of Mathematics, Louisiana State University, Baton Rouge, Louisiana 70803
E-mail address: rng@math.lsu.edu

Department of Mathematics, Texas A&M University, College Station, Texas 77843
E-mail address: rowell@math.tamu.edu

Microsoft Research Station Q and Department of Mathematics, University of California, Santa Barbara, California 93106
E-mail address: zhenghwa@microsoft.com