Communications in
**Mathematical
Physics**

On Classification of Modular Tensor Categories

Eric Rowell[1,*], **Richard Stong**[2,**], **Zhenghan Wang**[3,**]

[1] Department of Mathematics, Texas A&M University, College Station,
TX 77843, U.S.A.
E-mail: rowell@math.tamu.edu

[2] Center for Communications Research, 4320 Westerra Court, San Diego,
CA 92121-1969, U.S.A.
E-mail: stong@ccrwest.org

[3] Microsoft Station Q, University of California, CNSI Bldg, Rm 2237, Santa Barbara,
CA 93106-6105, U.S.A.
E-mail: zhewang@indiana.edu; zhenghwa@microsoft.com

Abstract: We classify all unitary modular tensor categories (UMTCs) of rank ≤ 4.
There are a total of 35 UMTCs of rank ≤ 4 up to ribbon tensor equivalence. Since the
distinction between the modular S-matrix S and $-S$ has both topological and physical
significance, so in our convention there are a total of 70 UMTCs of rank ≤ 4. In particu-
lar, there are two trivial UMTCs with $S = (\pm 1)$. Each such UMTC can be obtained from
10 non-trivial prime UMTCs by direct product, and some symmetry operations. Explicit
data of the 10 non-trivial prime UMTCs are given in Sect. 5. Relevance of UMTCs to
topological quantum computation and various conjectures are given in Sect. 6.

1. Introduction

A modular tensor category (MTC) in the sense of V. Turaev determines uniquely a
(2+1)-topological quantum field theory (TQFT) [Tu] (a seemingly different definition
appeared in [MS1].) The classification of MTCs is motivated by the application of
MTCs to topological quantum computing [F,Ki1,FKW,FLW1,FKLW,P], and by the
use of MTCs in developing a physical theory of topological phases of matter [Wil,MR,
FNTW,Ki2,Wa,LWe,DFNSS]. G. Moore and N. Seiberg articulated the viewpoint that
rational conformal field theory (RCFT) should be treated as a generalization of group
theory [MS2]. The algebraic content of both RCFTs and TQFTs is encoded by MTCs.
Although two seemingly different definitions of MTCs were used in the two contexts
[MS1,Tu], the two notions are essentially equivalent: an MTC in [MS1] consists of
essentially the basic data of a TQFT in [Wal]. The theory of MTCs encompasses the
most salient feature of quantum mechanics in the tensor product: superposition. There-
fore, even without any applications in mind, the classification of MTCs could be pursued
as a quantum generalization of the classification of finite groups.

There are two natural ways to organize MTCs: one by fixing a pair (G, λ), where G is a compact Lie group, and λ a cohomology class $\in H^4(BG; \mathbb{Z})$; and the other by fixing the rank of an MTC, i.e. the number of isomorphism classes of simple objects. If a conjecture of E. Witten were true, then every MTC would come from a Chern-Simons-Witten (CSW) TQFT labelled by a pair (G, λ) [Witt,MS1,HRW]. Classification by fixing a compact Lie group G has been carried out successfully for G=finite groups [DW,FQ], $G = T^n$ torus [Ma,BM], and $G = A$, B, C, D simple Lie groups [FK,KW,TW]. In this paper, we will pursue the classification by fixing the rank. This approach is inspired by the study of topological phases of matter and topological quantum computing. Another reason is that we have evidence that there might be exotic (2+1)-TQFTs other than CSW theories [HRW].

Topological phases of matter are like artificial elements. The only known topological phases of matter are fractional quantum Hall liquids: electron systems confined on a disk immersed in a strong perpendicular magnetic field at extremely low temperatures [Wil,DFNSS]. Electrons in the disk, pictured classically as orbiting inside concentric annuli around the origin, organize themselves into some topological order [Wen,WW1,WW2]. Therefore, the classification of topological phases of matter resembles the periodic table of elements. The periodic table does not go on forever, and simpler elements are easier to find. The topological quantum computing project is to find MTCs in Nature, in particular those with non-abelian anyons. Therefore, it is important that we know the simplest MTCs in a certain sense because the chance for their existence is better.

There is a hierarchy of structures on a tensor category: rigidity, pivotality, sphericity. We will always assume that our category is a fusion category: a rigid, semi-simple, $\mathbb{C}$-linear monoidal category with finitely many isomorphism classes of simple objects, and the trivial object is simple. It has been conjectured that every fusion category has a pivotal structure [ENO]. Actually, it might be true that every fusion category is spherical. Another important structure on a tensor category is braiding. A tensor category with compatible pivotal and braiding structures is called ribbon. In our case a ribbon category is always pre-modular since we assume it is a fusion category. For each structure, we may study the classification problem. The classification of fusion categories by fixing the rank has been pursued in [O1,O2]. Since an MTC has considerably more structures than a fusion category, the classification is potentially easier, and we will see that this is indeed the case in Sects. 3 and 4. The advantage in the MTC classification is that we can work with the modular S matrix and T matrix to determine the possible fusion rules without first solving the pentagon and hexagon equations. For the classification of MTCs of a given rank, we could start with the infinitely many possible fusion rules, and then try to rule out most of the fusion rules by showing the pentagon equations have no solutions. However, pentagon equations are notoriously hard to solve, and we have no theories to practically determine when a solution exists for a particular set of fusion rules (Tarski's theorem on the decidability of the first-order theory of real numbers provides a logical solution). So being able to determine all possible fusion rules without solving the pentagon equations greatly simplifies the classification for MTCs. As shown in [HH], all structures on an MTC can be formulated as polynomial equations over $\mathbb{Z}$. Hence the classification of MTC is the same as counting points on certain algebraic varieties up to equivalence. But all the data of an MTC can be presented over a certain finite degree Galois extension of $\mathbb{Q}$, probably over an abelian Galois extension of $\mathbb{Q}$ if normalized appropriately. Therefore, the classification problem is closer to number theory than to algebraic geometry. The argument in Sects. 3 and 4 is basically Galois theory

plus elementary yet complicated number theory. To complete the classification, we need to solve the pentagons and hexagons given the fusion rules. A significant complication comes from the choices of bases of the Hom spaces when solving the pentagon equations. The choices of basis make the normalization of $6j$ symbols into an art: so far no computer programs are available to solve pentagons with a fusion coefficient > 1, but one set of such fusion rules is solved completely [HH]. Currently, there are no theories to count the number of solutions of pentagon equations for a given set of fusion rules without solving the pentagons. For unitary MTCs, there is tension between two desirable normalizations for $6j$ symbols: to make the F matrix unitary, or to present all data of the theory in an abelian Galois extension of $\mathbb{Q}$. For the Fibonacci theory, unitarity of the F matrix and abelianess of the Galois extension of $\mathbb{Q}$ cannot be achieved simultaneously, but with different F matrices, each can be obtained separately [FW]. This is the reason that we will only define the Galois group of a modular fusion rule and a modular data, but not the Galois group of an MTC.

The main result of this paper is the classification of MTCs with rank=2, 3 and unitary MTCs of rank=4. The authors had obtained the classification of all unitary MTCs of rank ≤ 4 in 2004 [Wa]. The delay is related to the open finiteness conjecture: *There are only finitely many equivalence classes of MTCs for any given rank.* By Ocneanu rigidity the conjecture is equivalent to: *There are only finitely many sets of fusion rules for MTCs of a given rank.* Our classification of MTCs of rank ≤ 4 supports the conjecture. We also listed all quantum group MTCs up to rank ≤ 12 in Sect. 5. Two well-known constructs of MTCs are the quantum group method, and the quantum double of spherical tensor categories or the Drinfeld center. The quantum double is natural for MTCs from subfactor theory using Ocneanu's asymptotic inclusions [EK]. It seems that this method might produce exotic MTCs in the sense of [HRW].

Our main technique is Galois theory. Galois theory was introduced into the study of RCFT by J. de Boer and J. Goeree [dBG], who considered the Galois extension K of $\mathbb{Q}$ by adjoining all the eigenvalues of the fusion matrices. They made the deep observation that the Galois group of the extension K over $\mathbb{Q}$ is always abelian. This result was extended by A. Coste and T. Gannon who used their extension to study the classification of RCFTs [CG]. Fusion rules of an MTC are determined by the modular S-matrix through Verlinde formulas. It follows that the Galois extension K is the same as adjoining to $\mathbb{Q}$ all entries of the modular $\tilde{S}$ matrix. When a Galois group element applies to the $\tilde{S}$ matrix entry-wise, this action is a multiplication of $\tilde{S}$ by a signed permutation matrix, which first appeared in [CG]. It follows that the entries of the $\tilde{S}$ matrix are the same up to signs if they are in the same orbit of a Galois group element. For a given rank ≤ 4, this allows us to determine all possible $\tilde{S}$-matrices, therefore, all possible fusion rules.

Note that the Galois group of a modular data does not change the fusion matrices, but it can change a unitary theory into a non-unitary theory. For example, the Galois conjugate of the Fibonacci theory is the Yang-Lee theory, which is non-unitary. We might expect that for each modular data, one of its Galois conjugates would be realized by a unitary MTC. This is actually false. For example, take a rank=2 modular data with $\tilde{S} = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$, and $T = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$. No Galois actions can change the $\tilde{S}$ matrix, hence the quantum dimension of the non-trivial simple object from -1 to 1, though the same fusion rules can be realized by a unitary theory: the semion theory. Reference [Ro1] contains a set of fusion rules which has non-unitary MTC realizations, but has no unitary realizations at all.

Table 1. Unitary MTCs of rank≤ 4

	A　　2 $\mathbf{1}$			
	A　　4 $\mathbb{Z}_2$		N　　4 $(A_1, 3)_{\frac{1}{2}}$ U	
	A　　4 $\mathbb{Z}_3$	N　　16 $(A_1, 2)$	N　　4 $(A_1, 5)_{\frac{1}{2}}$ U	
A　　10 $\mathbb{Z}_2 \times \mathbb{Z}_2$	A　　8 $\mathbb{Z}_4$	N　　8 $(A_1, 3)$ U	N　　4 $(A_1, 7)_{\frac{1}{2}}$ U	N　　6 $Fib \times Fib$ U

The paper is organized as follows. In Sect. 2, we study the implications of the Verlinde formulas using Galois theory. In Sects. 3 and 4, we determine all self-dual modular $\tilde{S}$ matrices of modular symbols of rank=2, 3, and unitary ones for rank=4. Rank=2 is known to experts, and rank=3 fusion rules have been previously classified [CP]. For modular data, Theorems 3.1 and 3.2 can also be deduced from [O1,O2]. In Sect. 5, we determine all UMTCs of rank ≤ 4. In Sect. 6, we discuss some open questions about the structure and application of MTCs. In the Appendix, together with S. Belinschi, we determine all non-self dual unitary modular data of rank ≤ 4.

We summarize the classification of all rank ≤ 4 unitary MTCs into Table 1. There are a total of 70 unitary MTCs of rank ≤ 4 (a total of 35 up to ribbon tensor equivalence). The count is done in Sect. 5.4. Each such UMTC can be obtained from 10 non-trivial prime UMTCs by direct product, and some symmetry operations. The 10 non-trivial prime UMTCs are the semion MTC, the Fibonacci MTC or $(A_1, 3)_{\frac{1}{2}}$, the $\mathbb{Z}_3$ MTC, the Ising MTC, the $(A_1, 2)$ MTC, the even half of an $SU(2)$ MTC at level 5 or $(A_1, 5)_{\frac{1}{2}}$, the $\mathbb{Z}_4$ MTC, the toric code MTC, the $(D_4, 1)$ MTC, and the even half of an $SU(2)$ MTC at level 7 or $(A_1, 7)_{\frac{1}{2}}$. Their explicit data are listed in Sect. 5.3. Out of the 10 non-trivial prime UMTCs, 9 are quantum group categories for a simple Lie group: the semion=$SU(2)_1$, the Fibonacci=$(G_2)_1$, the $\mathbb{Z}_3$=$SU(3)_1$, the Ising=complex conjugate of $(E_8)_2$, the $(A_1, 2)$=$SU(2)_2$, the $\mathbb{Z}_4 = SU(4)_1$, the toric code= $Spin(16)_1$, the $(D_4, 1) = Spin(8)_1$, and the $(A_1, 7)_{\frac{1}{2}}$=complex conjugate of $(G_2)_2$. The Ising MTC and the $SU(2)_2$ MTC have the same fusion rules, but the Frobenius-Schur indicators of the non-abelian anyon σ are $+1, -1$, respectively. The toric code MTC and the $Spin(8)_1$ MTC have the same fusion rules, but the twists are $\{1, 1, 1, -1\}$, and $\{1, -1, -1, -1\}$, respectively. We choose $q = e^{\frac{\pi i}{\ell}}$ in the quantum group construction. In the Ising case, it is the $q = e^{-\frac{\pi i}{\ell}}$ theory for E_8 at level=2. For notation and more details, see Sect. 5.3. We do not know how to construct $(A_1, 5)_{\frac{1}{2}}$ by cosets of quantum group categories.

The information for each rank is contained in one row of Table 1. Each box contains information of the MTCs with the same fusion rules. The center entry in a box denotes the realization of the fusion by a quantum group category or their products. We also use Fib to denote the Fibonacci category $(A_1, 3)_{\frac{1}{2}}$. The upper left corner has either A or N, where A means that all anyons are abelian, and N that at least one type of anyons is

non-abelian. The right upper corner has a number which is the number of different unitary theories with that fusion rule. If the lower right corner has a U, it means that at least one type of anyons has universal braiding statistics for topological quantum computation. The detailed information about which anyon is abelian or non-abelian, universal or non-universal is given in Sect. 6.3. It is worth noticing that the list of all fusion rules up to rank=4 agrees with the computer search for RCFTs in [GK]. We believe this continues to be true for rank=5. The rank= 6 list in [GK] is not complete.

Finally, we comment on the physical realization of UMTCs. The existence of abelian anyons in $\nu = \frac{1}{3}$ FQH liquids is established theoretically with experimental support, while non-abelian anyons are believed to exist at the $\nu = \frac{5}{2}$ and $\nu = \frac{12}{5}$ plateaus (see [DFNSS] and the references therein). Current experimental effort is focused on FQH liquids at $\nu = \frac{5}{2}$. But the fermionic nature of electrons complicates direct application of MTCs to FQH liquids because only anyonic properties of bosonic systems can be described fully by MTCs. In other words, we need a refined theory, e.g. a spin MTC, to describe a fermionic system [DW, BM].

2. Galois Theory of Fusion Rules

In this section, we study the implication of Verlinde formulas for fusion rules of MTCs. For more related discussion, see the beautiful survey [G].

Definition 2.1. (1) *A rank=n label set is a finite set $\mathcal{L}$ of n elements with a distinguished element, denoted by 0, and an involution $\hat{\ }: \mathcal{L} \to \mathcal{L}$ such that $\hat{0} = 0$. A label $i \in \mathcal{L}$ is self dual if $\hat{i} = i$.*
   The charge conjugation matrix is the $n \times n$ matrix $C = (\delta_{i, \hat{j}})$. Note that C is symmetric and $C^2 = I_n$, the $n \times n$ identity matrix.

(2) *A rank=n modular fusion rule is a pair $(\mathcal{N}; \tilde{S})$, where $\mathcal{N}$ is a set of n $n \times n$ matrices $N_i = (n_{i,j}^k)_{0 \leq j,k \leq n-1}$, indexed by a rank=n label set $\mathcal{L}$, with $n_{i,j}^k \in \mathbb{Q}$, and $\tilde{S} = (\tilde{s}_{ij})_{0 \leq i,j \leq n-1}$ is an $n \times n$ matrix satisfying the following:*

   (a) *$\tilde{s}_{00} = 1, \tilde{s}_{i,\hat{j}} = \overline{\tilde{s}_{i,j}}$, and all $\tilde{s}_{i,0}$'s are non-zero;*

   (b) *If we let $D = \sqrt{\sum_{i=0}^{n-1} \tilde{s}_{i,0}^2}$, then $S = \frac{\tilde{S}}{D}$ is a symmetric, unitary matrix.*

   Furthermore, the matrices N_i in $\mathcal{N}$ and $\tilde{S}$ are related by the following:

$$N_i \tilde{S} = \tilde{S} \Lambda_i \tag{2.1}$$

   for all $i \in \mathcal{L}$, where $\Lambda_i = (\delta_{ab}\lambda_{ia})_{n \times n}$ is diagonal, and $\lambda_{ia} = \frac{\tilde{s}_{ia}}{\tilde{s}_{0a}}$.
   The identities (2.1) or equivalently the Verlinde formulas (2.3) below imply many symmetries among $n_{i,j}^k$: $n_{0,j}^k = \delta_{jk}, n_{i,j}^k = n_{j,i}^k = n_{\hat{i},\hat{j}}^{\hat{k}} = n_{i,\hat{k}}^{\hat{j}}$.
   The matrix N_i will be called the ith fusion matrix. From identities (2.1), the diagonal entries in Λ_i are the eigenvalues of N_i, and the columns of $\tilde{S}$ are the corresponding eigenvectors. The non-zero number D will be called the total quantum order, $d_i = \tilde{s}_{i0}$ the quantum dimension of the ith label, and $D^2 = \sum_{i=0}^{n-1} d_i^2$ the global quantum dimension.

(3) *A rank=n modular symbol consists of a triple $(\mathcal{N}; S, T)$. The pair $(\mathcal{N}; \frac{S}{s_{00}})$ is a rank=n modular fusion rule with all $n_{i,j}^k \in \mathbb{N} = \{0, 1, 2, \cdots\}$ (here s_{00} is the (0,0)-entry of the unitary matrix $S = (s_{ij})_{0 \leq i,j \leq n-1}$), and the $n \times n$ matrix $T = (\delta_{ab}\theta_a)_{n \times n}$ is diagonal, and $\theta_0 = 1$. Furthermore, S and T satisfy*

(i) $(ST)^3 = (D_+s_{00})S^2$;

(ii) $S^2 = C$;

(iii) $\theta_i \in U(1)$ and $\theta_{\hat{i}} = \theta_i$ for each i,

   where $D_\pm = \sum_{i=0}^{n-1} \theta_i^{\pm 1} d_i^2$. The following identity can be deduced:

$$D_+ D_- = D^2. \tag{2.2}$$

The complex number θ_i will be called the twist of the ith label. Note that s_{00} might be $-\frac{1}{D}$. A modular symbol is called unitary if each quantum dimension d_i is the Frobenius-Perron eigenvalue of the corresponding fusion matrix N_i. In particular, the quantum dimensions d_i's are positive real numbers ≥ 1.

(4)   A modular symbol $(\mathcal{N}; S, T)$ is called a modular data if there is an MTC whose fusion rules, modular $\tilde{S}$-matrix, and T-matrix are given by $\mathcal{N}$, $\frac{S}{s_{00}}$, T of the modular symbol.

(5)   Let $\Lambda = \{\lambda_{ij}\}_{i,j \in \mathcal{L}}$ for a rank=n modular fusion rule, and let $K = \mathbb{Q}(\lambda_{ij})$, $i, j \in \mathcal{L}$ be the Galois extension of $\mathbb{Q}$. Then the Galois group G of the Galois field K over $\mathbb{Q}$ is called the Galois group of the modular fusion rule.

   We are interested in searching for $n + 2$ tuples $(N_0, \ldots, N_{n-1}; \tilde{S}, T)$ related in the correct fashion. We will index the rows and columns of matrices by $0, 1, \ldots, n - 1$. Since $N_i \tilde{S} = \tilde{S} \Lambda_i$, the columns of $\tilde{S}$ must be eigenvectors of N_i with eigenvalues $\lambda_{i,0}$, $\lambda_{i,1}$, ..., and $\lambda_{i,n-1}$, respectively. Looking at the first entries of these columns and of $N_i \tilde{S}$, and using the only non-zero 1 of the first row of N_i, we see that $\lambda_{i,0} = d_i$, and $d_j \lambda_{i,j} = \tilde{s}_{i,j}$. It follows that K is the same as $\mathbb{Q}(\tilde{s}_{ij})$, $i, j \in \mathcal{L}$. Since $\tilde{S}$ is symmetric, we see that for $i \neq j$ we have $d_j \lambda_{i,j} = d_i \lambda_{j,i}$, and $\tilde{s}_{i,j} = d_i \lambda_{j,i} = d_j \lambda_{i,j}$ for all i and j. Let $n_{i,j}^k$ denote the (j, k) entry of N_i. Since

$$N_i = \frac{1}{D^2} \tilde{S} \begin{pmatrix} \lambda_{i,0} & 0 & \cdots & 0 \\ 0 & \lambda_{i,1} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \lambda_{i,n-1} \end{pmatrix} \tilde{S}^\dagger,$$

we compute for $0 \leq j, k \leq n - 1$,

$$n_{i,j}^k = \sum_{m=0}^{n-1} \frac{\tilde{s}_{i,m} \tilde{s}_{j,m} \overline{\tilde{s}_{k,m}}}{d_m} D^{-2} = \sum_{m=0}^{n-1} \lambda_{i,m} \lambda_{j,m} \overline{\lambda_{k,m}} \frac{d_m^2}{D^2}. \tag{2.3}$$

The fusion matrices can also be described equivalently by fusion algebras. For a rank=n fusion rule, each label i is associated with a variable X_i. Then the fusion ring R is the free abelian ring $\mathbb{Z}[X_0, \ldots, X_{n-1}]$ generated by X_i's modulo relations (called fusion rules) $X_i X_j = \sum_{i=0}^{n-1} n_{i,j}^k X_k$. The fusion algebra will be $F = R \otimes_{\mathbb{Z}} K$, where K is the Galois field of the fusion rules above. We may replace K by $\mathbb{C}$. If the modular fusion rule is realized by an MTC, then X_i is an equivalence class of simple objects, and the multiplication $X_i X_j$ is just the tensor product.

   There are modular symbols that are not modular data.

Example 2.2. Take the following:

$$S = \frac{1}{2} \begin{pmatrix} 1 & \sqrt{2} & 1 \\ \sqrt{2} & 0 & -\sqrt{2} \\ 1 & -\sqrt{2} & 1 \end{pmatrix},$$

and $T = \mathrm{Diag}(1, \theta, -1)$. The fusion matrices N_i are determined by the formulas (2.3), hence are independent of θ. They are the same as those of the Ising MTC in Sect. 5.3. Therefore, for any $\theta \in U(1)$, we get a modular symbol. But only when θ is a 16th root of unity, do we have modular data.

Very likely the modular symbol of an MTC determines the MTC , and we do not know when a modular symbol becomes a modular data.

Proposition 2.3. *If $(\mathcal{N}; S, T)$ is a modular data, then we have:*

(1) $\theta_i \theta_j s_{ij} = \sum_k n_{ij}^k s_{k0} \theta_k.$

(2) $\prod_j \theta_j^{A_{ij}} = \theta_i^{\frac{4}{3} \sum_j A_{ij}},$
     where $A_{ij} = 2n_{i\hat{i}}^j n_{ij}^i + n_{ii}^j n_{ji}^i.$

(3) *Let $\nu_k = \frac{1}{D^2} \sum_{i,j \in \mathcal{L}} n_{k,j}^i d_i d_j \frac{\theta_i^2}{\theta_j^2}$, then ν_k is 0 if $k \neq \hat{k}$, and is ± 1 if $k = \hat{k}$. ν_k is called the Frobenius-Schur indicator of k.*

(4) $D_+ s_{00} = e^{\frac{\pi i c}{4}}$ *for some $c \in \mathbb{Q}$. The rational number $c \bmod 8$ is called the topological central charge of the modular data.*

Proof. For (1), see [BK, Eq. (3.1.2)] on p. 47. For (2), it is [BK, Theorem 3.1.19] found on p. 57. Formula (3) from [Ba] for RCFTs can be generalized to MTCs. (4) follows from Theorem 2.5. □

Proposition 2.3 (2) implies that the θ_i are actually roots of unity of finite order, which is often referred to as *Vafa's Theorem*. But from Example 2.2, we know that this is not true for general modular symbols, in particular $\mathbb{Q}(\theta_i)$ might not be algebraic for modular symbols. This leads to:

Definition 2.4. *Given a modular data $(\mathcal{N}; S, T)$, let $\mathcal{K}_N$ be the Galois field $\mathbb{Q}(\tilde{s}_{ij}, D, \theta_i)$, $i, j \in \mathcal{L}$. Then the Galois group of $\mathcal{K}_N$ over $\mathbb{Q}$ will be called the Galois group of the modular data.*

Theorem 2.5. (1) *(de Boer-Goeree theorem): The Galois group of a modular fusion rule is abelian.*
(2) *The Galois group of a modular data is abelian.*

By the Kronecker-Weber theorem, there is an integer m such that $\mathcal{K}_N \subset \mathbb{Q}(\zeta_m)$, where $\zeta_m = e^{\frac{2\pi i}{m}}$. The smallest such m for $\mathcal{K}_N$ is called the conductor of $\mathcal{K}_N$, and the order of T always divides N (we intentionally build N into the notation $\mathcal{K}_N$). The Galois group of $\mathbb{Q}(\zeta_N)$ is the cyclic group of units l such that $\gcd(l, N) = 1$. Each l acts on $\mathcal{K}_N$ as the Frobenius map $\sigma_l : \zeta_N \to \zeta_N^l$. Consequently, $\sigma_l(T) = T^l$ and $\sigma_l(S) = S\tilde{P}_\sigma$, where the signed permutation matrix $\tilde{P}_\sigma$ corresponds to the Galois element σ in the Galois group of the modular fusion rule.

It is known that the fusion algebra of a rank=n MTC is isomorphic to the function algebra of n points. A Galois group element σ of the associated modular fusion rule induces an isomorphism of the fusion algebra. It follows that σ determines a permutation of the label set. When we have only a modular fusion rule, the two algebra structures on the fusion algebra a priori might not be isomorphic to each other. But still a Galois group element of the modular fusion determines a permutation of the label set and the

de Boer-Goeree theorem holds. Actually what we are using in this paper are identities among modular $\tilde{S}$ entries up to some parity signs $\epsilon_{i,\sigma} = \pm 1$ associated to each Galois element σ. Such parity signs first appeared in [CG] for Galois automorphisms of $\mathbb{Q}(\lambda_{i,j}, D)$.

First we note the following easy, but very useful fact that the ordered set of eigenvalues of N_i determines the label i uniquely.

Proposition 2.6. *There do not exist indices $j \neq k$ such that $\lambda_{i,j} = \lambda_{i,k}$ for all i for any modular fusion rule $(\mathcal{N}; \tilde{S})$.*

Proof. If there were such indices, then the dot product of rows j and k of $\tilde{S}$ would be $D^2 = \sum_{i=0}^{n-1} |\tilde{s}_{i,j}|^2 > 0$, a contradiction.   □

Except (5), the following theorem is contained in [CG].

Theorem 2.7. *Let G be the Galois group of a rank=n modular fusion rule $(\mathcal{N}; \tilde{S})$. Then*

(1) *the simultaneous action of the Galois group G on the set $\Lambda = \{\lambda_{ij}\}$ gives an injective group homomorphism $\iota : G \rightarrow S_n$, where S_n is the permutation group of n letters; for $\sigma \in G$, $\iota(\sigma)(i)$ is the associated element in S_n.*
(2) *For any $\sigma \in G$, the matrix $\tilde{P}_\sigma = d_{\sigma(0)} \tilde{S}^{-1} \sigma(\tilde{S})$ is a signed permutation matrix; furthermore, the map $\sigma \rightarrow \tilde{P}_\sigma$ gives a group homomorphism from G to the signed permutation matrices modulo ± 1 which lifts ι.*
(3) *For each $\sigma \in G$, there are $\epsilon_{i,\sigma} = \pm 1$ such that*

$$\sigma(\tilde{s}_{j,k}) = \frac{1}{d_{\sigma(0)}} \epsilon_{\sigma(k),\sigma} \tilde{s}_{j,\sigma(k)}. \tag{2.4}$$

Moreover,

$$\tilde{s}_{j,k} = \epsilon_{\sigma(j),\sigma} \epsilon_{k,\sigma} \tilde{s}_{\sigma(j),\sigma^{-1}(k)}, \tag{2.5}$$

and

$$\epsilon_{\sigma^{-1}(k),\sigma^{-1}} = \epsilon_{\sigma(0),\sigma} \epsilon_{0,\sigma} \epsilon_{k,\sigma}. \tag{2.6}$$

(4) *The Galois group G is abelian.*
(5) *If n is even, then $\prod_{i=0}^{n-1} \epsilon_{i,\sigma} = (-1)^\sigma$. If n is odd, then $D \in K$, and $\sigma(D) = \epsilon_\sigma \cdot \frac{D}{d_{\sigma(0)}}$, where $\epsilon_\sigma = \pm 1$. We have $\prod_{i=0}^{n-1} \epsilon_{i,\sigma} = \epsilon_\sigma \cdot (-1)^\sigma$.*

We are going to use σ for both the element of the Galois group G and its associated element of S_n. When $\sigma \in G$ applies to a matrix, σ applies entry-wise.

Proof. Let $K = \mathbb{Q}[\{\lambda_{i,j}\}_{0 \leq i,j \leq n-1}]$ be the Galois extension of $\mathbb{Q}$ generated by the eigenvalues of all the N_i and let G be the associated Galois group as above. The action of G on the eigenvalues gives an injection $G \rightarrow S_n \times S_n \times \cdots \times S_n$, where there are $n - 1$ factors. Note that we have not assumed the N_i have distinct eigenvalues, therefore this map is not necessarily unique and is not necessarily a group homomorphism. This is not a problem as we will resolve the ambiguity shortly. Just fix one such map for now. Let $(\sigma_1, \sigma_2, \ldots, \sigma_{n-1})$ denote the image of $\sigma \in G$ under this injection. Note that a priori,

there is no relationship between the σ_i. Let Λ_i be the diagonal matrix with diagonal entries $\lambda_{i,j}$, so

$$N_i = \tilde{S}\Lambda_i \tilde{S}^{-1}.$$

Let $P_{\sigma_i} = (\delta_{i=\sigma_i(j)})_{0 \leq i,j \leq n-1}$ be the permutation matrix corresponding to to σ_i. Since $\sigma(\lambda_{i,j}) = \lambda_{i,\sigma_i(j)}$, we have $\sigma(\Lambda_i) = P_{\sigma_i}^{-1}\Lambda_i P_{\sigma_i}$. Since N_i is rational we have

$$\tilde{S}\Lambda_i \tilde{S}^{-1} = N_i = \sigma(N_i) = \sigma(\tilde{S})P_{\sigma_i}^{-1}\Lambda_i P_{\sigma_i}\sigma(\tilde{S})^{-1}.$$

Rewriting this gives

$$\Lambda_i[\tilde{S}^{-1}\sigma(\tilde{S})P_{\sigma_i}^{-1}] = [\tilde{S}^{-1}\sigma(\tilde{S})P_{\sigma_i}^{-1}]\Lambda_i.$$

Hence $B_{i,\sigma} = \tilde{S}^{-1}\sigma(\tilde{S})P_{\sigma_i}^{-1}$ commutes with Λ_i. It follows that $B_{i,\sigma}$ is block diagonal, with blocks corresponding to the equal eigenvalues of N_i. In formulas, if the (j,k) entry of $B_{i,\sigma}$ is nonzero, then $\lambda_{i,j} = \lambda_{i,k}$. Let $\tilde{S}^{-1}\sigma(\tilde{S}) = B_{i,\sigma}P_{\sigma_i} = C_\sigma$. Note two facts, if the (j,k) entry of C_σ is nonzero, then the $(j,\sigma_i(k))$ entry of $B_{i,\sigma}$ is nonzero and hence $\lambda_{i,j} = \lambda_{i,\sigma_i(k)}$. The second fact is that C_σ (as the notation suggests) does not depend on i, only on σ. Suppose C_σ has 2 nonzero entries in column k, say the (j,k) and (ℓ,k) entries. Then $\lambda_{i,j} = \lambda_{i,\sigma_i(k)} = \lambda_{i,\ell}$ for all i, contradicting Proposition 2.6 above. If a row or column of C_σ is all zeroes, then $\det(C_\sigma) = 0$, a contradiction. Hence C_σ has exactly one nonzero entry in every row and in every column. Thus there is a unique permutation $\sigma \in S_n$ and a diagonal matrix B_σ such that $C_\sigma = B_\sigma P_\sigma$. Note that we are now using σ for both the element of the Galois group and its associated element of S_n. Note that

$$C_{\sigma\sigma'} = \tilde{S}^{-1}\sigma\sigma'(\tilde{S}) = \tilde{S}^{-1}\sigma(\tilde{S})\sigma(\tilde{S}^{-1}\sigma'(\tilde{S})) = C_\sigma\sigma(C_{\sigma'}),$$

from which it follows that the map $G \to S_n$ is a group homomorphism. Thus we have proved that the simultaneous action of the Galois group G on the eigenvalues $\lambda_{i,j}$ of N_i for all i gives an injective group homomorphism $G \to S_n$.

Note that the squared length of column zero of $\tilde{S}$ is $D^2 = \sum_{i=0}^{n-1} d_i^2$, which must be equal to the squared length of column $\sigma(0)$. Hence

$$D^2 = \sum_{i=0}^{n-1} d_{\sigma(0)}^2 \lambda_{i,\sigma(0)}^2 = d_{\sigma(0)}^2 \sigma\left(\sum_{i=0}^{n-1} \lambda_{i,0}^2\right) = d_{\sigma(0)}^2 \sigma(D^2).$$

Rewriting gives

$$\sigma\left(\frac{1}{D^2}\right) = \frac{d_{\sigma(0)}^2}{D^2}.$$

It follows that G acts in the same way on the quantities $\{d_j/D^2\}$. The Verlinde formulas (2.3) encode the symmetry of the N_i matrices, and give us the complete symmetry under interchanging the last $n-1$ N_i and simultaneously reordering the last $n-1$ rows and columns of all matrices. Thus $n_{i,j}^k$ is invariant under G and hence is necessarily rational if we define it first to be only in $\mathbb{R}$.

Transposing the identity $\tilde{S}^{-1}\sigma(\tilde{S}) = C_\sigma$ and inverting this identity gives the two equations $\sigma(\tilde{S})\tilde{S}^{-1} = C_\sigma^T$ and

$$C_\sigma^{-1} = \sigma(\tilde{S})^{-1}\tilde{S} = \frac{D^2}{\sigma(D^2)}\sigma(\tilde{S})\tilde{S}^{-1} = d_{\sigma(0)}^2 C_\sigma^T.$$

Hence the matrices $d_{\sigma(0)}C_\sigma$ and $d_{\sigma(0)}B_\sigma$ are orthogonal. Since B_σ is diagonal it follows that

$$B_\sigma = \frac{1}{d_{\sigma(0)}}\begin{pmatrix} \epsilon_{0,\sigma} & 0 & \cdots & 0 \\ 0 & \epsilon_{1,\sigma} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & \epsilon_{n-1,\sigma} \end{pmatrix}$$

for some choices of $\epsilon_{i,\sigma} = \pm 1$. The map $\sigma \mapsto d_{\sigma(0)}C_\sigma$ gives a group homomorphism from G to the signed permutation matrices modulo ± 1 which lifts the homomorphism ι of (1).

Rewrite the definition of C_σ as $\sigma(\tilde{S}) = \tilde{S}B_\sigma P_\sigma$. Picking out the (j,k) entry, we have $\sigma(\tilde{s}_{j,k}) = \frac{1}{d_{\sigma(0)}}\epsilon_{\sigma(k),\sigma}\tilde{s}_{j,\sigma(k)}$. Moreover, since the left-hand side is symmetric we get $\tilde{S}B_\sigma P_\sigma = P_\sigma^{-1}B_\sigma \tilde{S}$. In coordinates this condition becomes $\tilde{s}_{j,k} = \epsilon_k\epsilon_{\sigma(j)}\tilde{s}_{\sigma(j),\sigma^{-1}(k)}$. Consider the action of G on pairs (j,k) defined by $\sigma \times (j,k) \mapsto (\sigma(j),\sigma^{-1}(k))$. Then we see that $|\tilde{s}_{j,k}|$ is constant on orbits of this action.

To see identity (2.6), we apply σ^{-1} to identity (2.4) and compare with identity (2.5). Note that $\tilde{s}_{\sigma^{-1}(0),\sigma(0)} = \epsilon_{\sigma(0),\sigma}\epsilon_{0,\sigma}$ by identity (2.5).

Given $\sigma_1, \sigma_2 \in G$, consider first $\sigma_2\sigma_1(\tilde{s}_{j,k}) = \sigma_2(\frac{1}{d_{\sigma_1(0)}}\epsilon_{\sigma_1(k),\sigma_1}\tilde{s}_{j,\sigma_1(k)})$
$= \sigma_2(\frac{1}{d_{\sigma_1(0)}}\epsilon_{\sigma_1(k),\sigma_1}\tilde{s}_{\sigma_1(k),j}) = \frac{1}{d_{\sigma_2(0)}\lambda_{\sigma_1(0),\sigma_2(0)}}\epsilon_{\sigma_1(k),\sigma_1}\epsilon_{\sigma_2(j),\sigma_2}\tilde{s}_{\sigma_1(k),\sigma_2(j)}$.
Then consider

$$\sigma_1\sigma_2(\tilde{s}_{j,k}) = \sigma_1\sigma_2(\tilde{s}_{k,j}) = \sigma_1\left(\frac{1}{d_{\sigma_2(0)}}\epsilon_{\sigma_2(j),\sigma_2}\tilde{s}_{k,\sigma_2(j)}\right)$$

$$= \sigma_1\left(\frac{1}{d_{\sigma_2(0)}}\epsilon_{\sigma_2(j),\sigma_2}\tilde{s}_{\sigma_2(j),k}\right) = \frac{1}{d_{\sigma_1(0)}\lambda_{\sigma_2(0),\sigma_1(0)}}\epsilon_{\sigma_2(j),\sigma_2}\epsilon_{\sigma_1(k),\sigma_1}\tilde{s}_{\sigma_2(j),\sigma_1(k)}.$$

Hence $\sigma_1\sigma_2 = \sigma_2\sigma_1$ using $d_i\lambda_{j,i} = d_j\lambda_{i,j}$, i.e. G is abelian.

Suppose now that the rank $n = 2r$ is even. Then $\det(\tilde{S})^2 = D^{2n}$, hence $\det(\tilde{S}) = \pm D^{2r}$. Since the determinant is a polynomial in the entries of the matrix $\det(\sigma(\tilde{S})) = \pm\sigma(D^2)^r$, with the same sign as $\det(\tilde{S})$. Hence $\det(\tilde{S}^{-1}\sigma(\tilde{S})) = d_{\sigma(0)}^{-n}$. Since $\det(C_\sigma) = d_{\sigma(0)}^{-n}(-1)^\sigma\prod_{j=0}^{n-1}\epsilon_{j,\sigma}$, we conclude $\prod_{j=0}^{n-1}\epsilon_{j,\sigma} = (-1)^\sigma$. For odd rank $n = 2r+1$, $\det(\tilde{S}) = \pm D^{2r+1}$, hence $D \in K$. Hence $\sigma(D) = \epsilon_\sigma D/d_{\sigma(0)}, \epsilon_\sigma = \pm 1$ and one gets the formula $\prod_{j=0}^{n-1}\epsilon_{j,\sigma} = \epsilon_\sigma(-1)^\sigma$. $\quad\square$

Note that the resulting Eqs. (2.5) for the entries $\tilde{s}_{j,k}$ are unchanged if we replace B_σ with $-B_\sigma$. We will use this to assume $\epsilon_0 = 1$ below.

Next we will use the fact that the $\theta_i \in U(1)$ to produce a series of twist inequalities on the entries of $\tilde{S}$.

Theorem 2.8. *Given a modular symbol $(\mathcal{N}; S, T)$ and S is a real matrix, then*

(1) $2\max_i \tilde{s}_{i,j}^2 \le D|\tilde{s}_{jj}| + D^2$ *for any j.*

(2) *If $j \neq k$, then $D \le \frac{1}{|\tilde{s}_{j,k}|}\sum_{i=0}^{n-1}|\tilde{s}_{i,j}\tilde{s}_{i,k}|$.*

(3) $\sum_{j=0}^{n-1}\frac{\epsilon_{\sigma(j)}\tilde{s}_{j,\sigma(j)}}{\theta_j\theta_{\sigma(j)}} = D - \sum_{i:\,\sigma(i)=i}\theta_i\epsilon_{\sigma(i)}$.

Proof. Rewrite the twist equation as $T\tilde{S}T\tilde{S}T = D_+\tilde{S}$. Then taking the (j,k) entry of this formula gives

$$\theta_j\theta_k \sum_{i=0}^{n-1} \theta_i\tilde{s}_{i,j}\tilde{s}_{i,k} = D_+\tilde{s}_{j,k}.$$

Since $|D_+| = D$ and $|\theta_i| = 1$, the largest of the $n+1$ numbers $|\tilde{s}_{i,j}\tilde{s}_{i,k}|, 0 \le i \le n-1$, and $D|\tilde{s}_{j,k}|$ must be at most the sum of the other n. If $j = k$, then $\sum_i \tilde{s}_{i,j}^2 = D^2 > D|\tilde{s}_{jj}|$. Hence this inequality is trivial unless the largest is one of the first n and we get

$$2\max_i \tilde{s}_{i,j}^2 \le D|\tilde{s}_{jj}| + \sum_{i=0}^{n-1} \tilde{s}_{i,j}^2.$$

If $j \ne k$ then $\sum_i \tilde{s}_{i,j}\tilde{s}_{i,k} = 0$ and the nontrivial case is

$$D \le \frac{1}{|\tilde{s}_{j,k}|} \sum_{i=0}^{n-1} |\tilde{s}_{i,j}\tilde{s}_{i,k}|.$$

We will refer to these as the twist inequalities.

Suppose $\sigma \in G$ corresponds to signs ϵ_i as above. We drop σ for notational easiness. Multiply the identity above by $\epsilon_{\sigma(j)}/(\theta_j\theta_{\sigma(j)})$, set $k = \sigma(j)$, and sum over j. The result is

$$\sum_{j=0}^{n-1} \epsilon_{\sigma(j)} \sum_{i=0}^{n-1} \theta_i\tilde{s}_{i,j}\tilde{s}_{i,\sigma(j)} = D_+ \sum_{j=0}^{n-1} \frac{\epsilon_{\sigma(j)}\tilde{s}_{j,\sigma(j)}}{\theta_j\theta_{\sigma(j)}}.$$

Interchanging the sums and using the fact that $\tilde{s}_{i,\sigma(j)} = \epsilon_{\sigma(j)}\epsilon_{\sigma(i)}\tilde{s}_{\sigma(i),j}$ gives

$$\sum_{i=0}^{n-1} \theta_i\epsilon_{\sigma(i)} \sum_{j=0}^{n-1} \tilde{s}_{i,j}\tilde{s}_{\sigma(i),j} = D_+ \sum_{j=0}^{n-1} \frac{\epsilon_{\sigma(j)}\tilde{s}_{j,\sigma(j)}}{\theta_j\theta_{\sigma(j)}}.$$

By orthogonality of the rows of $\tilde{S}$, the innermost sum on the left is zero if $i \ne \sigma(i)$ and $D^2 = D_+D_-$ if $i = \sigma(i)$. Hence

$$\sum_{j=0}^{n-1} \frac{\epsilon_{\sigma(j)}\tilde{s}_{j,\sigma(j)}}{\theta_j\theta_{\sigma(j)}} = D_- \sum_{i: \sigma(i)=i} \theta_i\epsilon_{\sigma(i)}.$$

If σ is fixed point free, then $\sum_{j=0}^{n-1} \frac{\epsilon_{\sigma(j)}\tilde{s}_{j,\sigma(j)}}{\theta_j\theta_{\sigma(j)}} = 0$. $\qquad\square$

3. Rank=2 and 3 Modular *S* Matrices

In this section, we determine all possible modular S matrices for rank=2 and 3 modular symbols. The rank=3 case first appeared in [CP], but our proof is new.

Theorem 3.1. *The only possible rank=2 modular $\tilde{S}$ matrices of some modular symbols are*

(1)

$$\begin{pmatrix} 1 & \epsilon \\ \epsilon & -1 \end{pmatrix},$$

where $\epsilon^2 = 1$;

(2)

$$\begin{pmatrix} 1 & \varphi \\ \varphi & -1 \end{pmatrix},$$

where $\varphi^2 = 1 + \varphi$.

Proof. Since all labels are self-dual, $\tilde{S}$ is a symmetric real unitary matrix of the form $\begin{pmatrix} 1 & d \\ d & -1 \end{pmatrix}$. The fusion matrix N_1 is of the form $\begin{pmatrix} 0 & 1 \\ 1 & m \end{pmatrix}$, so we have $d^2 = 1 + md$. Simplifying $D_+ D_- = D^2$ leads to $\theta + \theta^{-1} = 1 - d^2 = -m \cdot d$. Since $\theta \in U(1)$, so $|md| \le 2$. If $d > 0$, then $d = \frac{m + \sqrt{m^2 + 4}}{2}$, hence $m = 0, 1$. If $d < 0$, then $d = \frac{m - \sqrt{m^2 + 4}}{2}$, hence $[\mathbb{Q}(\theta + \theta^{-1}) : \mathbb{Q}] \le 2$. It follows that $\theta = e^{\frac{p\pi i}{q}}$ for some $(p, q) = 1$, and q is one of $\{1, 2, 3, 4, 5, 6\}$. Direct computation shows there are no integral solutions p, q for $2\cos(\frac{p\pi}{q}) = -m \cdot \frac{m - \sqrt{m^2 + 4}}{2}$ except for $q = 2, 5$ and $m = 0, 1$. $\square$

Theorem 3.2. *Then the only possible rank=3 modular $\tilde{S}$ matrices of some modular symbols up to permutations are*

(1)

$$\begin{pmatrix} 1 & \epsilon & \epsilon \\ \epsilon & \omega & \omega^2 \\ \epsilon & \omega^2 & \omega \end{pmatrix},$$

where $\epsilon^2 = 1$, and $\omega^3 = 1, \omega \ne 1$.

(2)

$$\begin{pmatrix} 1 & d & 1 \\ d & 0 & -d \\ 1 & -d & 1 \end{pmatrix},$$

where $d^2 = 2$.

(3)

$$\begin{pmatrix} 1 & d_1 & d_2 \\ d_1 & -d_2 & 1 \\ d_2 & 1 & -d_1 \end{pmatrix},$$

where d_1 is a real root of $x^3 - 2x^2 - x + 1$ and $d_2 = d_1/(d_1 - 1)$ which is a root of $x^3 - x^2 - 2x + 1$. The largest $d_1 = \frac{2\cos(\pi/7)}{2\cos(\pi/7) - 1} = 2.246979604\ldots$, and $d_2 = 2\cos(\pi/7) = 1.801937736\ldots$.

Proof. The non-self dual case is given in the Appendix. Hence we assume all fusion rules are self-dual, so $\tilde{S}$ is a real, symmetric, unitary matrix up to the scalar D. It follows that the fusion matrices N_i's are commutative, symmetric, integral matrices. One approach to proving the theorem is to analyze case by case for the Galois groups of fusion rules $G \cong 1, \mathbb{Z}_2, \mathbb{Z}_3$. This strategy will be fully exploited in the rank=4 case in the next section. Instead we will argue directly from the $\tilde{S}$-matrix in this section.

The fusion matrices N_1, N_2 are symmetric, and $N_1 N_2 = N_2 N_1$. Therefore, they can be written as

$$N_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & m & k \\ 0 & k & l \end{pmatrix}$$

and

$$N_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & k & l \\ 1 & l & n \end{pmatrix}$$

such that

$$1 + ml + kn = k^2 + l^2.$$

There characteristic polynomials are

$$p_1(x) = x^3 - (\ell + m)x^2 + (m\ell - k^2 - 1)x + \ell = 0$$

and

$$p_2(x) = x^3 - (k + n)x^2 + (nk - \ell^2 - 1)x + k = 0,$$

respectively.

Next we turn to the $\tilde{S}$ matrix, which is of the following form:

$$\tilde{S} = \begin{pmatrix} 1 & d_1 & d_2 \\ d_1 & \tilde{s}_{11} & \tilde{s}_{12} \\ d_2 & \tilde{s}_{12} & \tilde{s}_{22} \end{pmatrix}.$$

Orthogonality of the columns of the $\tilde{S}$ matrix translates into the equations

$$d_1 + d_1 \tilde{s}_{11} + d_2 \tilde{s}_{12} = 0,$$
$$d_2 + d_1 \tilde{s}_{12} + d_2 \tilde{s}_{22} = 0,$$
$$d_1 d_2 + \tilde{s}_{12}(\tilde{s}_{11} + \tilde{s}_{22}) = 0.$$

The first two equations give $\tilde{s}_{11} = -1 - d_2 \tilde{s}_{12}/d_1$ and $\tilde{s}_{22} = -1 - d_1 \tilde{s}_{12}/d_2$. Plugging these into the third equation gives

$$(d_1^2 + d_2^2)\tilde{s}_{12}^2 + 2d_1 d_2 \tilde{s}_{12} - d_1^2 d_2^2 = 0,$$

hence

$$\tilde{s}_{12} = \frac{d_1 d_2}{1 \pm D}.$$

Thus

$$\tilde{s}_{11} = -1 - \frac{d_2^2}{1 \pm D},$$

and

$$\tilde{s}_{22} = -1 - \frac{d_1^2}{1 \pm D}.$$

Thus the eigenvalues of N_1 are

$$d_1, b = \frac{\tilde{s}_{12}}{d_2} = \frac{d_1}{1 \pm D}, \text{ and } c = \frac{\tilde{s}_{11}}{d_1} = -\frac{1}{d_1} - \frac{d_2^2}{d_1(1 \pm D)}$$

and the eigenvalues of N_2 are

$$d_2, e = \frac{\tilde{s}_{12}}{d_1} = \frac{d_2}{1 \pm D}, \text{ and } f = -\frac{1}{d_2} - \frac{d_1^2}{d_2(1 \pm D)}.$$

We compute

$$d_1 b + d_2 f = d_1 c + d_2 e = bc + ef = -1.$$

Since $d_1 bc = -\ell$ and $d_2 ef = -k$, these are equivalent to

$$\frac{\ell}{c} + \frac{k}{e} = \frac{\ell}{b} + \frac{k}{f} = \frac{\ell}{d_1} + \frac{k}{d_2} = 1.$$

Also note that

$$d_1 e = d_2 b.$$

Let's deal with the case where $\ell = 0$ first. Then we have $k^2 = kn + 1$. Hence $k = 1$ and $n = 0$. Thus the eigenvalues of N_2 are 1, 1, and -1 and the eigenvalues of N_1 are $(m + \sqrt{m^2 + 8})/2$, 0, and $(m - \sqrt{m^2 + 8})/2$. Since N_1 has eigenvalues $d_1, b, c,$ and $d_1 \neq 0$, hence $c = 0$ which implies $m = 0$. This gives $(k, \ell, m, n) = (1, 0, 0, 0)$ and

$$\tilde{S} = \begin{pmatrix} 1 & d & 1 \\ d & 0 & -d \\ 1 & -d & 1 \end{pmatrix},$$

where $d^2 = 2$. The case $k = 0$ gives essentially the same solution, so we will henceforth assume ℓ and k are positive. Since $p_1(\ell) = -k^2\ell \leq 0$ and $p_1(0) = \ell \geq 0$, we see that the largest root of p_1 is $> \ell$, one of the remaining roots is in $(0, \ell)$ and the other root is negative. Similarly the largest root of p_2 is $> k$ and the other roots are in $(0, k)$ and $(-\infty, 0)$.

Case 1. The polynomial $p_1(x)$ is reducible. Since $d_1 > \ell$, d_1 cannot be an integer. Thus p_1 must split into a linear and an irreducible quadratic. Thus $\mathbb{Q}[d_1, D]$ is a quadratic extension of $\mathbb{Q}$. Hence $\mathbb{Q}[d_1, d_2, D]$ has degree 2 or 4 over $\mathbb{Q}$. Thus p_2 is also reducible and also splits into a linear and an irreducible quadratic. Since the $\ell/b + k/f = \ell/c + k/e = 1$, the integral roots must be either b and f or c and e. Without loss, we may assume the integer roots are b and f. Let

$$d_2 = \alpha + \beta\sqrt{s} \quad \text{and} \quad e = \alpha - \beta\sqrt{s}$$

for rational (in fact integer or half-integer) α and β and integer s. Then since $d_1 e = d_2 b$ and c is the conjugate of d_1 we have

$$d_1 = b\frac{\alpha + \beta\sqrt{s}}{\alpha - \beta\sqrt{s}} \quad \text{and} \quad c = b\frac{\alpha - \beta\sqrt{s}}{\alpha + \beta\sqrt{s}}.$$

Hence $\ell = -d_1 bc = -b^3$. Since $f = -k/(d_2 e) = -k/(\alpha^2 - \beta^2 s)$ and $-b^2 = \ell/b = 1 - k/f = \alpha^2 + 1 - \beta^2 s$. Therefore solving $1 = k/d_2 + \ell/d_1$ for k gives

$$k = d_2 - \ell\frac{d_2}{d_1} = \alpha + \beta\sqrt{s} + b^3\frac{e}{b} = \alpha + \beta\sqrt{s} - (\alpha^2 + 1 - \beta^2 s)(\alpha - \beta\sqrt{s})$$
$$= -\alpha(\alpha^2 - \beta^2 s) + \beta[\alpha^2 + 2 - \beta^2 s]\sqrt{s}.$$

Since k is an integer, this forces $\alpha^2 - \beta^2 s = -2$, hence $b^2 = 1$. Since $\ell > 0$, this means $\ell = 1$ and $b = -1$. Also from the equations above we get $k = 2\alpha$, $d_2 = \alpha + \sqrt{\alpha^2 + 2}$, $e = \alpha - \sqrt{\alpha^2 + 2}$, $f = \alpha$, $d_1 = \alpha^2 + 1 + \alpha\sqrt{\alpha^2 + 2} = d_2^2/2$, $c = \alpha^2 + 1 - \alpha\sqrt{\alpha^2 + 2}$, and $D = \alpha^2 + 2 + \alpha\sqrt{\alpha^2 + 2}$. Thus

$$p_1(x) = x^3 - (2\alpha^2 + 1)x^2 - (2\alpha^2 + 1)x + 1$$

and

$$p_2(x) = x^3 - 3\alpha x^2 + (2\alpha^2 - 2)x + 2\alpha.$$

Thus $(k, \ell, m, n) = (2\alpha, 1, 2\alpha^2, \alpha)$ and

$$\tilde{S} = \begin{pmatrix} 1 & \alpha^2 + 1 + \alpha\sqrt{\alpha^2 + 2} & \alpha + \sqrt{\alpha^2 + 2} \\ \alpha^2 + 1 + \alpha\sqrt{\alpha^2 + 2} & 1 & -\alpha - \sqrt{\alpha^2 + 2} \\ \alpha + \sqrt{\alpha^2 + 2} & -\alpha - \sqrt{\alpha^2 + 2} & \alpha^2 + \alpha\sqrt{\alpha^2 + 2} \end{pmatrix}.$$

Note that $n = \alpha$ must be a non-negative integer. Setting $\alpha = 0$ gives the example found above again. Thus we may assume $\alpha \geq 1$. Since $d_1 = d_2^2/2$, the equation for the θ's is

$$|1 + \theta_2 d_2^2 + (1/4)\theta_1 d_2^4| = D = 1 + (1/2)d_2^2.$$

If a solution did exist, then we would have $1 + (1/2)d_2^2 \geq (1/4)d_2^4 - d_2^2 - 1$, hence $17 \geq (d_2^2 - 3)^2$ or $d_2 \leq \sqrt{3 + \sqrt{17}} = 2.66891\ldots$. Since $d_2 \geq 1 + \sqrt{3} = 2.73205\ldots$, this cannot occur. Thus these $\tilde{S}$ matrices, for positive α, do not give a modular symbol.

Case 2. The polynomial $p_1(x)$ is an irreducible cubic. By Case 1, we see that $p_2(x)$ is also an irreducible cubic. Then there must be a Galois symmetry σ with $\sigma(d_1) = b$, $\sigma(b) = c$ and $\sigma(c) = d_1$. Hence $\sigma(d_2) = f, \sigma(f) = e$, and $\sigma(e) = d_2$ since these roots of p_2 pair with the corresponding roots of p_1. Applying σ to the identity $d_1 e = d_2 b$, gives $d_2 b = f c$. Thus we must have $f c = d_1 d_2/(1 \pm D)$. Since

$$f c = \frac{d_1 d_2}{(1 \pm D)^2} + \frac{d_1^2 + d_2^2}{d_1 d_2 (1 \pm D)} + \frac{1}{d_1 d_2} = \frac{d_1 d_2}{(1 \pm D)^2} + \frac{D^2 \pm D}{d_1 d_2 (1 \pm D)},$$

we compute

$$1 \pm D = \frac{(1 \pm D)^2}{d_1 d_2} f c = 1 \pm \frac{D(1 \pm D)^2}{d_1^2 d_2^2},$$

and hence

$$\left(\frac{1 \pm D}{d_1 d_2} \right)^2 = 1.$$

Since $D > 1$, we get that

$$\tilde{s}_{12} = \frac{d_1 d_2}{1 \pm D} = \pm 1,$$

and hence $b = \pm 1/d_2$ and $e = \pm 1/d_1$. Thus d_1 and d_2 are units in the ring of algebraic integers. Hence $k = \ell = 1$ and hence $m + n = 1$. Without loss we may assume $m = 1$ and $n = 0$. Then $p_1(x) = x^3 - 2x^2 - x + 1$ and $p_2(x) = x^3 p_1(1/x) = x^3 - x^2 - 2x + 1$. Then one computes

$$d_1 = \frac{2\cos(\pi/7)}{2\cos(\pi/7) - 1} = 2.246979604\ldots,$$

$b = 1 - 1/d_1$, $c = -1/(d_1 - 1)$, $d_2 = d_1/(d_1 - 1) = 1.801937736\ldots$, $e = 1/d_1$, and $f = 1 - d_1$ and

$$\tilde{S} = \begin{pmatrix} 1 & d_1 & d_2 \\ d_1 & -d_2 & 1 \\ d_2 & 1 & -d_1 \end{pmatrix}.$$

□

4. Rank = 4 Modular S Matrices

First we introduce the following notation. For an integer m, define

$$\phi_m = \frac{m + \sqrt{m^2 + 4}}{2},$$

that is, ϕ_m is the unique positive root of $x^2 - mx - 1 = 0$. Note that any algebraic number ϕ whose only conjugate is $-1/\phi$ must be ϕ_m for some integer m. Also note the only rational ϕ_m is $\phi_0 = 1$.

Theorem 4.1. *The only possible rank=4 modular* $\tilde{S}$ *matrices of* unitary *modular symbols up to permutations are*

(1)

$$
\begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 \\
1 & -1 & \omega & \bar{\omega} \\
1 & -1 & \bar{\omega} & \omega
\end{pmatrix},
$$

where $\omega = \pm i$;

(2)

$$
\begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 \\
1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1
\end{pmatrix};
$$

(3)

$$
\begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1
\end{pmatrix};
$$

(4)

$$
\begin{pmatrix}
1 & \varphi & 1 & \varphi \\
\varphi & -1 & \varphi & -1 \\
1 & \varphi & -1 & -\varphi \\
\varphi & -1 & -\varphi & 1
\end{pmatrix},
$$

where $\varphi = \frac{1+\sqrt{5}}{2}$ is the golden ratio;

(5)

$$
\begin{pmatrix}
1 & \varphi & \varphi & \varphi^2 \\
\varphi & -1 & \varphi^2 & -\varphi \\
\varphi & \varphi^2 & -1 & -\varphi \\
\varphi^2 & -\varphi & -\varphi & 1
\end{pmatrix};
$$

(6)

$$
\begin{pmatrix}
1 & d^2-1 & d+1 & d \\
d^2-1 & 0 & -d^2+1 & d^2-1 \\
d+1 & -d^2+1 & d & -1 \\
d & d^2-1 & -1 & -d-1
\end{pmatrix},
$$

where d is the largest real root of $x^3 - 3x - 1$.

Proof. The non-self dual case is treated in the Appendix, so we will assume that $\tilde{S}$ is real in the following. Since the fusion coefficients $n_{i,j}^k$ are totally symmetric in i, j and k for self-dual categories, we will instead write $n_{i,j,k}$ in what follows. For notational easiness, when the Galois group element σ is clear from the context, we simply write $\epsilon_{i,\sigma}$ as ϵ_i. Identities for ϵ_i and $\tilde{s}_{jk}$ that are not referenced are all from Theorem 2.7. All the twist inequalities are from Theorem 2.8.

Case 1. G contains a 4-cycle. By symmetry we may assume $\sigma = (0\ 1\ 2\ 3) \in G$. The conditions $\tilde{s}_{j,k} = \epsilon_k \epsilon_{\sigma(j)} \tilde{s}_{\sigma(j),\sigma^{-1}(k)}$ and $\epsilon_1 \epsilon_2 \epsilon_3 = -1$ give

$$
\tilde{S} = \begin{pmatrix}
1 & d_1 & d_2 & d_3 \\
d_1 & \epsilon_1 \epsilon_2 d_2 & -\epsilon_2 d_3 & \epsilon_1 \\
d_2 & -\epsilon_2 d_3 & -1 & \epsilon_2 d_1 \\
d_3 & \epsilon_1 & \epsilon_2 d_1 & -\epsilon_1 \epsilon_2 d_2
\end{pmatrix}.
$$

By symmetry under interchanging N_1 and N_3, we may assume $\epsilon_2 = +1$. Note that $\sigma^2(d_2) = \lambda_{2,2} = -1/d_2 \neq d_2$. Hence the characteristic polynomial p_2 of N_2 is irreducible. Since $\sigma^2(d_1) = -d_3/d_2 < 0$. Hence $\sigma^2(d_1) \neq d_1$. Thus p_1 is irreducible. Since ϵ_1/d_3 is a root of p_1, it follows that p_3 is also irreducible.

We see that $\lambda_{1,1} = \epsilon_1 d_2/d_1$, $\lambda_{1,2} = -d_3/d_2$, and $\lambda_{1,3} = \epsilon_1/d_3$. In particular $d_1 \lambda_{1,1} \lambda_{1,2} \lambda_{1,3} = -1$. Orthogonality of the rows of $\tilde{S}$ is equivalent to

$$
d_1 + \epsilon_1 d_1 d_2 - d_2 d_3 + \epsilon_1 d_3 = 0, \quad \text{or}
$$
$$
\frac{1}{d_1} + \lambda_{1,3} = \lambda_{1,1} + \frac{1}{\lambda_{1,2}}.
$$

Write $p_1(x) = x^4 - c_1 x^3 + c_2 x^2 + c_3 x - 1$. Then $p_4(x) = x^4 - \epsilon_1 c_3 x^3 - c_2 x^2 + \epsilon_1 c_1 x - 1$. Note that $c_1 = \text{Trace}(N_1) \geq 0$ and $\epsilon_1 c_3 = \text{Trace}(N_3) \geq 0$. Multiplying together the orthogonality condition above and five of its formal conjugates gives

$$
128 + (c_3^2 - c_1^2)^2 - 16 c_1 c_3 + 12(c_3^2 - c_1^2) c_2 + 32 c_2^2 = 0.
$$

This equation forces c_1 and c_3 to be even. Let $\Delta = c_1 - c_3$ and $\Sigma = c_1 + c_3$ (hence Σ and Δ are even and congruent mod 4). Then solving the quadratic equation above for c_2 we see that we must have $(\Sigma^2 - 32)(\Delta^2 + 32)$ to be a square and $c_2 = \frac{3\Delta\Sigma \pm \sqrt{(\Sigma^2 - 32)(\Delta^2 + 32)}}{16}$. It follows that $|\Sigma| \geq 6$. If Σ and Δ are multiples of 4, then we see they are multiples of 8 and either sign gives an integral c_2. If Σ and Δ are both 2 mod 4, then there is a unique choice of the sign for which c_2 is integral.

The Galois group of p_1 must be $\mathbb{Z}/4\mathbb{Z}$, otherwise it would contain the $(0\ 1)(2\ 3)$. Applying this to the orthogonality identity above gives $1/\lambda_{1,3} + d_1 = \lambda_{1,2} + 1/\lambda_{1,1}$. Multiplying this by the original identity gives $\frac{1}{d_1 \lambda_{1,3}} + d_1 \lambda_{1,3} = \frac{1}{\lambda_{1,1} \lambda_{1,2}} + \lambda_{1,1} \lambda_{1,2}$. Hence $d_1 \lambda_{1,3} = (\lambda_{1,1} \lambda_{1,2})^{\pm 1}$, either of which contradicts the product of all four roots being -1. In particular, p_1 cannot have complex roots, since complex conjugation would give a transposition in the Galois group. Applying σ to the orthogonality identity gives $d_1 + 1/\lambda_{1,1} = \lambda_{1,2} + 1/\lambda_{1,3}$.

We know from the preliminary discussion that all three of the resulting N_i matrices will be rational. Define $P = \frac{16c_2 - 3\Delta\Sigma}{\Delta^2 + 32} = \pm\sqrt{\frac{\Sigma^2 - 32}{\Delta^2 + 32}}$, then we compute

$$n_{1,1,1} = \frac{5c_1 - 3c_3}{8} - \frac{c_1 - c_3}{8}P,$$

$$n_{1,1,2} = \epsilon_1(P - 1),$$

$$n_{1,1,3} = \epsilon_1\left(\frac{c_1 + c_3}{8} - \frac{c_1 - c_3}{8}P\right),$$

$$n_{1,2,2} = \frac{c_1 + c_3}{4} + \frac{c_1 - c_3}{4}P,$$

$$n_{1,2,3} = P,$$

$$n_{1,3,3} = \frac{c_1 + c_3}{8} - \frac{c_1 - c_3}{8}P,$$

$$n_{2,2,2} = \epsilon_1\left(2c_2 - \frac{c_3^2 + c_1^2}{4} - 2P\right),$$

$$n_{2,2,3} = \epsilon_1\left(\frac{c_1 + c_3}{4} + \frac{c_1 - c_3}{4}P\right),$$

$$n_{2,3,3} = \epsilon_1(P + 1), \quad \text{and}$$

$$n_{3,3,3} = \epsilon_1\left(\frac{5c_3 - 3c_1}{8} - \frac{c_1 - c_3}{8}P\right).$$

Recall that the $n_{i,j,k}$ must be nonnegative integers. This restricts the c_i. First looking at $n_{1,2,3}$, we see that P must be a positive integer. Hence c_2 must be given by the upper sign. This condition in fact guarantees integrality of all the $n_{i,j,k}$. (The additional factors of 2 in the denominator cancel out if c_2 is integral and can be ignored.) Integrality of P severely restricts Δ, since it requires all odd prime factors of $\Delta^2 + 32$ to be congruent to 1 mod 8 (since 2 and -2 are both squares mod any such prime). In particular either $\Delta = 0$ or $|\Delta| \geq 6$. Since $P \neq 0$, we see that $\Sigma^2 \geq \Delta^2 + 64$, hence $|\Sigma| > |\Delta|$. Thus c_3 must be positive and $\Sigma > 0$. Since we saw above $\epsilon_1 c_3 \geq 0$, we see that $\epsilon_1 = +1$. Thus rewriting the orthogonality relation gives $d_1/d_3 = (d_2 - 1)/(d_2 + 1)$.

The twist inequality coming from the $(0, 3)$ entry reads

$$D \leq \left(1 + \frac{d_1}{d_3}\right)(1 + d_2).$$

Plugging in the preceding identity simplifies this to $D \leq 2d_2$. Rearranging gives $3d_2^2 \geq d_1^2 + d_3^2 + 1 > d_1^2 + d_3^2$ and plugging in the identity $d_1 = d_3(d_2 - 1)/(d_2 + 1)$ yields

$$\left(\frac{d_3}{d_2 + 1}\right)^2 < \frac{3d_2^2}{2(d_2^2 + 1)} < \frac{3}{2}.$$

To see why this is helpful, expand the equations $\text{Trace}(N_i) = c_i$ for $i = 1, 3$ and use the identity above to eliminate d_1. The result is

$$c_1 = \frac{d_2^2 - 2d_2 - 1}{d_2(d_2 + 1)}d_3 + \frac{d_2^2 + 2d_2 - 1}{d_2 - 1} \cdot \frac{1}{d_3}, \quad \text{and}$$

$$c_3 = \frac{d_2^2 + 2d_2 - 1}{d_2(d_2 + 1)}d_3 - \frac{d_2^2 - 2d_2 - 1}{d_2 - 1} \cdot \frac{1}{d_3}.$$

Subtracting these gives

$$\Delta = c_1 - c_3 = -4\frac{d_3}{d_2 + 1} + 2\frac{d_2 + 1}{d_2 d_3}.$$

Hence $\Delta > -4\frac{d_3}{d_2+1} > -4\sqrt{3/2} > -4.9$. However, we saw above that either $\Delta = 0$ or $|\Delta| \geq 6$. It follows that $\Delta \geq 0$. Since $\Sigma \geq 6$ and $c_2 \geq 3\Delta\Sigma/16$, it follows that $c_2 > \Delta = c_1 - c_3$. Thus $p_3(1) = c_1 - c_2 - c_3 < 0$. Thus $d_3 > 1$. Hence we see $\Delta < 2(d_2 + 1)/(d_2 d_3) < 4$. It follows that $\Delta = 0$, i.e., $c_1 = c_3$.

Since $\Delta = 0$, $\Sigma = 2c_1$ is a multiple of 8 and

$$\left(\frac{P}{32}\right)^2 - 2\left(\frac{c_1}{4}\right)^2 = -1.$$

In this case the characteristic polynomials become

$$p_1(x) = x^4 - c_1 x^3 + 2\sqrt{2(c_1/4)^2 - 1}x^2 + c_1 x - 1,$$

$$p_2(x) = x^4 - 4\sqrt{2(c_1/4)^2 - 1}x^3 - 6x^2 + 4\sqrt{2(c_1/4)^2 - 1}x + 1, \quad \text{and}$$

$$p_3(x) = x^4 - c_1 x^3 - 2\sqrt{2(c_1/4)^2 - 1}x^2 + c_1 x - 1.$$

In particular $p_1(x) > 0$ for $x \geq c_1$. Hence $d_1 < c_1$. We have

$$p_2(x) = (x^2 - t_1 x - 1)(x_2 - t_2 x - 1),$$

where $t_1 > 0 > t_2$ are the two roots of $t^2 - 4\sqrt{2(c_1/4)^2 - 1}t - 4 = 0$. Since the larger root of $x^2 - tx - 1$ is an increasing function of t, d_2 must correspond to t_1. Hence

$$d_2 = t_1 + \frac{1}{d_2} > t_1 = 4\sqrt{2(c_1/4)^2 - 1} + \frac{4}{t_1} > 4\sqrt{2(c_1/4)^2 - 1}.$$

In particular, $d_2 > 4$ since the square root above is integral. Finally the twist inequality coming from the $(0, 2)$ entry reads

$$D \leq 2\left(1 + \frac{d_1 d_3}{d_2}\right).$$

Squaring and using the identity $d_3 = d_1(d_2 + 1)/(d_2 - 1)$ to eliminate d_3 gives the inequality

$$4(d_2 + 1)^2 d_1^4 - 2d_2(d_2^3 - 4d_2^2 + d_2 + 4)d_1^2 - d_2^2(d_2 - 1)^2(d_2^2 - 3) \geq 0.$$

Dividing through by $4(d_2 + 1)^2 d_1^2$ and rearranging gives

$$d_1^2 \geq \frac{d_2}{2(d_2 + 1)^2}(d_2^3 - 4d_2^2 + d_2 + 4) + \frac{d_2^2(d_2 - 1)^2(d_2^2 - 3)}{4(d_2 + 1)^2 d_1^2}.$$

The right-hand side of this inequality is an increasing function of d_2 for $d_2 > 4$ and a decreasing function of d_1, hence we may replace d_1 by its upper bound c_1 and d_2 by the lower bound above. The result is

$$4560 - 2138c_1^2 + 264c_1^4 - 8c_1^6 + (608 - 276c_1^2 + 32c_1^4)\sqrt{2c_1^2 - 16} \geq 0.$$

Since the coefficient of the square root is nonnegative it follows that

$$4560 - 2138c_1^2 + 264c_1^4 - 8c_1^6 + (608 - 276c_1^2 + 32c_1^4)c_1\sqrt{2} \geq 0.$$

This polynomial in c_1 is negative for $c_1 > 6\sqrt{2}$, hence $c_1 \leq 8$. The only multiple of 4 in the range $3 \leq c_1 \leq 8$ for which the Pell equation above is satisfiable is $c_1 = 4$. This gives $c_1 = c_3 = 4$, $c_2 = 2$, $P = 32$. However plugging in shows that the twist inequality $D \leq 2(1 + d_1d_3/d_2)$ does not actually hold in this case. Thus there are no solutions in this case.

Case 2. G is the Klein 4-group. Let σ_1, σ_2, and σ_3 be the elements of G which correspond to $(0\ 1)(2\ 3)$, $(0\ 2)(1\ 3)$, and $(0\ 3)(1\ 2)$, respectively. Let B_{σ_1} correspond to signs ϵ_i with $\epsilon_1\epsilon_2\epsilon_3 = 1$ and B_{σ_2} correspond to signs δ_i with $\delta_1\delta_2\delta_3 = 1$. Then using the usual identities gives

$$\tilde{S} = \begin{pmatrix} 1 & d_1 & d_2 & d_3 \\ d_1 & \epsilon_1 & \epsilon_2 d_3 & \epsilon_1\epsilon_2 d_2 \\ d_2 & \epsilon_2 d_3 & \tilde{s}_{2,2} & \tilde{s}_{2,3} \\ d_3 & \epsilon_1\epsilon_2 d_2 & \tilde{s}_{2,3} & \epsilon_1\tilde{s}_{2,2} \end{pmatrix} = \begin{pmatrix} 1 & d_1 & d_2 & d_3 \\ d_1 & \tilde{s}_{1,1} & \delta_1 d_3 & \tilde{s}_{1,3} \\ d_2 & \delta_1 d_3 & \delta_2 & \delta_1\delta_2 d_1 \\ d_3 & \tilde{s}_{1,3} & \delta_1\delta_2 d_1 & \delta_2\tilde{s}_{1,1} \end{pmatrix}.$$

Comparing these we see $\epsilon_2 = \delta_1$, $\tilde{s}_{1,1} = \epsilon_1$, and $\tilde{s}_{2,2} = \delta_2$, hence

$$\tilde{S} = \begin{pmatrix} 1 & d_1 & d_2 & d_3 \\ d_1 & \epsilon_1 & \epsilon_2 d_3 & \epsilon_1\epsilon_2 d_2 \\ d_2 & \epsilon_2 d_3 & \delta_2 & \epsilon_2\delta_2 d_1 \\ d_3 & \epsilon_1\epsilon_2 d_2 & \epsilon_2\delta_2 d_1 & \epsilon_1\delta_2 \end{pmatrix}.$$

Orthogonality of the rows of $\tilde{S}$ gives the three conditions

$$(1 + \epsilon_1)(d_1 + \epsilon_2 d_2 d_3) = (1 + \delta_2)(d_2 + \epsilon_2 d_1 d_3) = (1 + \epsilon_1\delta_2)(d_3 + \epsilon_1\epsilon_2 d_1 d_2) = 0.$$

Suppose $\epsilon_1 = +1$, then we see $d_1 = -\epsilon_2 d_2 d_3$, hence $\epsilon_2 = -1$ and the remaining orthogonality relations become $d_2(1+\delta_2)(1-d_3) = d_3(1+\delta_2)(1-d_2)$. We cannot have $d_2 = d_3 = 1$, since this would make $d_1 = 1$, hence $\delta_2 = -1$. This gives

$$\tilde{S} = \begin{pmatrix} 1 & d_2 d_3 & d_2 & d_3 \\ d_2 d_3 & 1 & -d_3 & -d_2 \\ d_2 & -d_3 & -1 & d_2 d_3 \\ d_3 & -d_2 & d_2 d_3 & -1 \end{pmatrix}.$$

The eigenvalues of N_2 are d_2 and $-1/d_2$ each with multiplicity 2. Hence $d_2 = \phi_m$ for some integer m. The eigenvalues of N_3 are d_3 and $-1/d_3$ each with multiplicity 2, hence $d_3 = \phi_n$ for some integer n. So

$$\tilde{S} = \begin{pmatrix} 1 & \phi_m\phi_n & \phi_m & \phi_n \\ \phi_m\phi_n & 1 & -\phi_n & -\phi_m \\ \phi_m & -\phi_n & -1 & \phi_m\phi_n \\ \phi_n & -\phi_m & \phi_m\phi_n & -1 \end{pmatrix}.$$

The resulting N_i matrices are necessarily rational, but in this case they are all integral, namely,

$$N_1 = N_2 N_3 = N_3 N_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & mn & m & n \\ 0 & m & 0 & 1 \\ 0 & n & 1 & 0 \end{pmatrix},$$

$$N_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & m & 0 & 1 \\ 1 & 0 & m & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \text{and} \quad N_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & n & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & n \end{pmatrix}.$$

Note that nonnegativity of the entries forces $m, n \geq 0$ and hence $\phi_m, \phi_n \geq 1$. The strongest twist inequalities are the $(0, 1)$ and $(2, 3)$ cases which give $D \leq 4$ or $(\phi_m^2 + 1)(\phi_n^2 + 1) \leq 16$. This gives, up to symmetry, the solutions $(m, n) = (0, 0), (0, 1), (0, 2),$ or $(1, 1)$. These are all excluded since the resulting Galois group G is at most $\mathbb{Z}/2\mathbb{Z}$. (These examples will return when we look at smaller Galois groups.)

Case 3. G contains a 3-cycle. Since we can exclude Cases 1 and 2 above, the image of G in S_4 cannot be transitive. It follows that G must fix the point j not on the 3-cycle. Thus $\lambda_{i,j}$ is rational (hence integral) for every i. Up to symmetry there are two cases for the 3-cycle. We could have $\sigma = (1\ 2\ 3)$ or $\sigma = (0\ 1\ 2)$. If $\sigma = (1\ 2\ 3)$, then the d_i are integral. The identities $\tilde{s}_{j,k} = \epsilon_{\sigma(j)} \epsilon_k \tilde{s}_{\sigma(j),\sigma^{-1}(k)}$ and $\epsilon_1 \epsilon_2 \epsilon_3 = 1$ give $\epsilon_i = 1$ for all i (since $d_i = \tilde{s}_{0,i} = \epsilon_i \tilde{s}_{0,i+1} = \epsilon_i d_{i+1}$ for $1 \leq i \leq 2$) and

$$\tilde{S} = \begin{pmatrix} 1 & d_1 & d_1 & d_1 \\ d_1 & \tilde{s}_{1,1} & \tilde{s}_{3,3} & \tilde{s}_{2,2} \\ d_1 & \tilde{s}_{3,3} & \tilde{s}_{2,2} & \tilde{s}_{1,1} \\ d_1 & \tilde{s}_{2,2} & \tilde{s}_{1,1} & \tilde{s}_{3,3} \end{pmatrix}.$$

Orthogonality of the columns of $\tilde{S}$ gives $\tilde{s}_{1,1} + \tilde{s}_{2,2} + \tilde{s}_{3,3} = -1$ and $\tilde{s}_{1,1}\tilde{s}_{2,2} + \tilde{s}_{2,2}\tilde{s}_{3,3} + \tilde{s}_{3,3}\tilde{s}_{1,1} = -d_1^2$. The first of these gives $-1/d_1 = \lambda_{1,1} + \lambda_{1,2} + \lambda_{1,3}$ from which we see $-1/d_1$ is an algebraic integer. Hence $d_1 = 1$ and $\lambda_{1,i} < 1$. The second equation gives $\lambda_{1,1}\lambda_{1,2} + \lambda_{1,2}\lambda_{1,3} + \lambda_{1,3}\lambda_{1,1} = -1$. Hence $\lambda_{1,1}, \lambda_{1,2},$ and $\lambda_{1,3}$ are the three roots of $g(x) = x^3 + x^2 - x + n$ for some integer n. This cubic must be irreducible and have three real roots all less than 1. Irreducibility excludes $n = 0$ and $n = -1$. For the roots of g to be less than 1, we must have $g(1) > 0$ or $n + 1 > 0$. Hence $n \geq 1$. However, this results in complex roots. Thus this case gives no solutions.

Thus we must have $\sigma = (0\ 1\ 2)$ and $\lambda_{i,3}$ is integral for all i. The identities for $\tilde{s}_{j,k}$ give

$$\tilde{S} = \begin{pmatrix} 1 & d_1 & d_2 & d_3 \\ d_1 & \epsilon_1 \epsilon_2 d_2 & \epsilon_1 & \epsilon_2 d_3 \\ d_2 & \epsilon_1 & \epsilon_2 d_1 & \epsilon_1 \epsilon_2 d_3 \\ d_3 & \epsilon_2 d_3 & \epsilon_1 \epsilon_2 d_3 & \tilde{s}_{3,3} \end{pmatrix}.$$

Since $\sigma(d_3) = \lambda_{3,1} = \epsilon_2 d_3/d_1$ and $\sigma^2(d_3) = \epsilon_1 \epsilon_2 d_3/d_2$, we must have $\sigma(d_3) \neq d_3$. (Otherwise $\epsilon_1 = \epsilon_2 = d_1 = d_2 = 1$ which fails.) Thus d_3 is a root of an irreducible cubic $g(x) = x^3 - c_1 x^2 + c_2 x - c_3$ and $\epsilon_2 d_1$ and $\epsilon_1 \epsilon_2 d_2$ are ratios of roots of g. If g had

Galois group S_3, then the ratios of the roots of g would be roots of an irreducible sextic. Thus g has Galois group $\mathbb{Z}/3\mathbb{Z}$ and $G = \{1, \sigma, \sigma^2\}$. Note that

$$c_1 = d_3 + \lambda_{3,1} + \lambda_{3,2} = \frac{d_3}{d_1 d_2}(d_1 d_2 + \epsilon_2 d_2 + \epsilon_1 \epsilon_2 d_1),$$

$$c_2 = d_3 \lambda_{3,1} + \lambda_{3,1}\lambda_{3,2} + \lambda_{3,2}d_3 = \frac{d_3^2}{d_1 d_2}(\epsilon_2 d_2 + \epsilon_1 + \epsilon_1\epsilon_2 d_1), \quad \text{and}$$

$$c_3 = d_3 \lambda_{3,1}\lambda_{3,2} = \epsilon_1 \frac{d_3^3}{d_1 d_2}.$$

Orthogonality of the columns of $\tilde{S}$ gives

$$\frac{c_1}{c_3} = \frac{\epsilon_2 d_1 + \epsilon_1 \epsilon_2 d_2 + \epsilon_1 d_1 d_2}{d_3^2} = -1, \quad \text{and}$$

$$\frac{c_2}{c_3} = \frac{1 + \epsilon_2 d_1 + \epsilon_1 \epsilon_2 d_2}{d_3} = -\frac{\tilde{s}_{3,3}}{d_3} = -\lambda_{3,3} \in \mathbb{Z}.$$

Thus $g(x) = x^3 - cx^2 + ncx + c$ for integer n, c. Since g has Galois group $\mathbb{Z}/3\mathbb{Z}$,

$$\delta^2 = \frac{1}{c^2}\mathrm{discr}(g) = (n^2 + 4)c^2 - 2n(2n^2 + 9)c - 27$$

must be a square. The resulting $n_{i,j,k}$ are

$$n_{1,1,1} = \frac{\epsilon_2}{2}(\delta - nc - 1) - \frac{\epsilon_2 \delta}{n^2 + 3},$$

$$n_{1,1,2} = \frac{\epsilon_1 \epsilon_2}{2(n^2 + 3)}(-\delta + nc - 2n^2 + 3),$$

$$n_{1,1,3} = \frac{1}{2(n^2 + 3)}(-n\delta + (n^2 + 2)c + 3n),$$

$$n_{1,2,2} = \frac{\epsilon_2}{2(n^2 + 3)}(\delta + nc - 2n^2 + 3),$$

$$n_{1,2,3} = \frac{\epsilon_1}{n^2 + 3}(3n - c),$$

$$n_{1,3,3} = \frac{\epsilon_2}{2(n^2 + 3)}(\delta - nc + 2n^2 - 3),$$

$$n_{2,2,2} = -\frac{\epsilon_1 \epsilon_2}{2}(\delta + nc + 1) + \frac{\epsilon_1 \epsilon_2 \delta}{n^2 + 3},$$

$$n_{2,2,3} = \frac{1}{2(n^2 + 3)}(n\delta + (n^2 + 2)c + 3n),$$

$$n_{2,3,3} = \frac{\epsilon_1 \epsilon_2}{2(n^2 + 3)}(-\delta - nc + 2n^2 - 3),$$

$$n_{3,3,3} = \frac{c + n^3}{n^2 + 3}.$$

Integrality of $n_{1,2,3}$ requires $c \equiv 3n \pmod{n^2 + 3}$. If we write $c = 3n + a(n^2 + 3)$ for integer a, then we compute $\delta^2 = (n^2 + 3)^2(a^2(n^2 + 4) + 2an - 3)$. Hence $\delta = (n^2 + 3)\beta$, where β is integral and $\beta^2 = a^2(n^2 + 4) + 2an - 3$. Note that in particular this forces

$a \neq 0$. Rewriting it as $\beta^2 = (an+1)^2 + 4a^2 - 4$, we see that $\beta \equiv an+1 \pmod 2$. Thus we compute

$$n_{1,1,1} = \frac{\epsilon_2}{2}((n^2+1)\beta - 3n^2 - an(n^2+3) - 1),$$

$$n_{1,1,2} = \frac{\epsilon_1 \epsilon_2}{2}(-\beta + an + 1),$$

$$n_{1,1,3} = \frac{1}{2}(-n\beta + 3n + a(n^2+2)),$$

$$n_{1,2,2} = \frac{\epsilon_2}{2}(\beta + an + 1),$$

$$n_{1,2,3} = -\epsilon_1 a,$$

$$n_{1,3,3} = \frac{\epsilon_2}{2}(\beta - an - 1),$$

$$n_{2,2,2} = -\frac{\epsilon_1 \epsilon_2}{2}((n^2+1)\beta + 3n^2 + an(n^2+3) + 1),$$

$$n_{2,2,3} = \frac{1}{2}(n\beta + 3n + a(n^2+2)),$$

$$n_{2,3,3} = \frac{\epsilon_1 \epsilon_2}{2}(-\beta - an - 1),$$

$$n_{3,3,3} = a + n,$$

and these are all integral. Nonnegativity of these entries gives further restrictions on the parameters. Looking at $n_{1,2,2} + n_{1,3,3} = \epsilon_2 \beta$, we see that ϵ_2 is the sign of β (or $\beta = 0$, but this gives $a = \pm 1$, $n = -a$, $c = a$ and $g(x) = (x-a)(x^2-1)$ which is reducible). Looking at $n_{1,1,2} + n_{2,3,3} = -\epsilon_1 \epsilon_2 \beta$, we see that $\epsilon_1 = -1$. Looking at $n_{1,2,3}$ we see that $a > 0$. Nonnegativity provides additional constraints on the parameters, but instead we look at the twist inequalities.

We saw above that $a > 0$, hence $c = 3n + a(n^2+3) \geq n^2 + 3n + 3 > 0$. Thus two of the roots d_3, $\lambda_{3,1}$ and $\lambda_{3,2}$ of g must be positive. By symmetry, we may assume $d_3 > \lambda_{3,1} > 0 > \lambda_{3,2}$. Then $\epsilon_2 = 1$ and we have

$$\tilde{S} = \begin{pmatrix} 1 & d_3/\lambda_{3,1} & -d_3/\lambda_{3,2} & d_3 \\ d_3/\lambda_{3,1} & d_3/\lambda_{3,2} & -1 & d_3 \\ -d_3/\lambda_{3,2} & -1 & d_3/\lambda_{3,1} & -d_3 \\ d_3 & d_3 & -d_3 & nd_3 \end{pmatrix}.$$

Let $M = \max(1/\lambda_{3,1}, 1/|\lambda_{3,2}|)$ so that $Md_3 = \max(d_1, d_2)$. Since $D^2 = (n^2+3)d_3^2$ and

$$\frac{1}{d_3^2} + \frac{1}{\lambda_{3,1}^2} + \frac{1}{\lambda_{3,2}^2} = n^2 + 2,$$

the diagonal twist inequality coming from the $(0,0)$ entry gives

$$2M^2 \leq n^2 + 3 + \frac{\sqrt{n^2+3}}{d_3}.$$

This inequality allows only finitely many choices of the parameters.

If $n > 0$, then $g(-1/\phi_n) = -\phi_n^{-3} < 0$ and therefore $\lambda_{3,2} > -1/\phi_n$. Thus $M > \phi_n$ and we get

$$2\phi_n^2 < n^2 + 3 + \frac{\sqrt{n^2+3}}{d_3}.$$

Further since $d_3\lambda_{3,1} = Mc$ and $d_3 > \lambda_{3,1}$, we have

$$d_3 > \sqrt{\phi_n c} \geq \sqrt{\phi_n(n^2 + 3n + 3)}.$$

For $n \geq 2$, we get a contradiction by noting that $\phi_n > n$, hence these equations force

$$2n^2 < n^2 + 3 + \frac{1}{\sqrt{n}},$$

a contradiction. For $n = 1$, plugging in gives a contradiction.

If $n = 0$, then $\beta^2 = 4a^2 - 3$, hence $a = 1$ and $g(x) = x^3 - 3x^2 + 3$. Since $\tilde{s}_{3,3} = 0$, the $(3, 3)$ entry of the twist equation gives $\theta_3^2 d_3^2(1 + \theta_1 + \theta_2) = 0$, hence $\theta_1 = \bar{\theta}_2 = e^{\pm 2\pi i/3}$. The $(0, 3)$ and $(1, 3)$ entries give

$$\theta_3(1 + d_1\theta_1 - d_2\theta_2) = D_+ = \theta_1\theta_3(d_1 - d_2\theta_1 + \theta_2).$$

This case is realized by $(A_1, 7)_{\frac{1}{2}}$.

If $n < 0$, then $1/M = \lambda_{3,1}$. One easily checks that M and d_3 are increasing functions of c, therefore it suffices to check that the inequality $2M^2 \leq n^2 + 3 + (n^2 + 3)^{1/2}d_3^{-1}$ fails for $a = 1$ and hence $c = n^2 + 3n + 3$. The inequality fails for $n \leq -2$. (To see this simply compute both sides for $n = -2$. For $n \leq -3$, note that $g(-1/n) = -((n+1)/n)^3 < 0$ and $g((n+1)^2) = -(n+1)^4 + n + 2 < 0$. Therefore $M < -n$ and $d_3 > (n+1)^2$. Hence we have $2M^2 > 2n^2 > n^2 + 4$ and $(n^2+3)^{1/2}/d_3 < 1$, but these combine to contradict the inequality.) For $n = -1$, $a = 1$, the inequality holds, but the resulting polynomial $g(x) = x^3 - x^2 - x + 1$ is reducible. Moving up to the next case $n = -1$, $a = 3$, the inequality fails. Thus there are no solutions in this case.

With the cases above completed, we consider G which is not transitive and contains no 3-cycle. Up to symmetry, it follows that G must be a subgroup of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \langle (0\ 1), (2\ 3) \rangle$.

Case 4. G contains the transposition $\sigma = (2\ 3)$. In this case the parity condition gives $\epsilon_1\epsilon_2\epsilon_3 = -1$. Three instances of the usual identity give $d_2 = \tilde{s}_{0,2} = \epsilon_2\tilde{s}_{0,3} = \epsilon_2 d_3$, $d_3 = \tilde{s}_{0,3} = \epsilon_3\tilde{s}_{0,2} = \epsilon_3 d_2$, and $d_1 = \tilde{s}_{0,1} = \epsilon_1\tilde{s}_{0,1} = \epsilon_1 d_1$. Since the d_i are positive we conclude $\epsilon_1 = \epsilon_2 = \epsilon_3 = 1$, a contradiction. Thus we are left with only three possibilities. Either $G = \mathbb{Z}/2\mathbb{Z} = \langle (0\ 1)(2\ 3) \rangle$, $G = \mathbb{Z}/2\mathbb{Z} = \langle (0\ 1) \rangle$, or G is trivial.

Case 5. G contains $\sigma = (0\ 1)(2\ 3)$. Using the identities $\tilde{s}_{j,k} = \epsilon_{\sigma(j)}\epsilon_k\tilde{s}_{\sigma(j),\sigma^{-1}(k)}$ and $\epsilon_1\epsilon_2\epsilon_3 = 1$ gives

$$\tilde{S} = \begin{pmatrix} 1 & d_1 & d_2 & d_3 \\ d_1 & \epsilon_1 & \epsilon_2 d_3 & \epsilon_1\epsilon_2 d_2 \\ d_2 & \epsilon_2 d_3 & \tilde{s}_{2,2} & \tilde{s}_{2,3} \\ d_3 & \epsilon_1\epsilon_2 d_2 & \tilde{s}_{2,3} & \epsilon_1\tilde{s}_{2,2} \end{pmatrix}.$$

Suppose first that $\epsilon_1 = 1$. Then, orthogonality of the first two columns of $\tilde{S}$ forces $\epsilon_2 = -1$ and $d_1 = d_2 d_3$. Orthogonality of the last column with the first three gives the equations

$$\tilde{s}_{2,2} d_2 + \tilde{s}_{2,3} d_3 = d_2(d_3^2 - 1), \quad \tilde{s}_{2,2} d_3 + \tilde{s}_{2,3} d_2 = d_3(d_2^2 - 1), \quad \text{and } \tilde{s}_{2,2} \tilde{s}_{2,3} = -d_2 d_3.$$

Looking at the cases $d_2 = d_3$ and $d_2 \neq d_3$ separately, these solve to give

$$\tilde{s}_{2,2} = -1 \quad \text{and} \quad \tilde{s}_{2,3} = d_1 = d_2 d_3.$$

Hence

$$\tilde{S} = \begin{pmatrix} 1 & d_2 d_3 & d_2 & d_3 \\ d_2 d_3 & 1 & -d_3 & -d_2 \\ d_2 & -d_3 & -1 & d_2 d_3 \\ d_3 & -d_2 & d_2 d_3 & -1 \end{pmatrix}.$$

This is exactly the $\tilde{S}$ matrix of Case 2 above. Exactly as in that case, we get $d_2 = \phi_m$, $d_3 = \phi_n$, and $d_1 = d_2 d_3$. The N_i matrices and the twist inequalities are the same, hence we conclude $(m, n) = (0, 1)$, $(0, 2)$, or $(1, 1)$. (Here we exclude $m = n = 0$ since it gives G trivial.) In the first case, $(m, n) = (0, 1)$, the possible twist matrices are given by $\theta_3 = e^{\pm 4\pi i/5}$, $\theta_2 = \pm i$, and $\theta_1 = \theta_2 \theta_3$. In the second case, $(m, n) = (0, 2)$, no twist matrix exists. (To see this, note that the $(1, 1)$ and $(3, 3)$ entries in the twist equation give

$$\theta_1^2 (\phi_2^2 + \theta_1 + \theta_2 \phi_2^2 + \theta_3) = D_+,$$
$$-\theta_3^2 (\phi_2^2 + \theta_1 + \theta_2 \phi_2^2 + \theta_3) = D_+.$$

Thus $\theta_1 = \pm i \theta_3$. The $(0, 1)$ and $(0, 3)$ entries give

$$\theta_1(1 + \theta_1 - \theta_2 - \theta_3) = D_+,$$
$$\theta_3(1 - \theta_1 + \theta_2 - \theta_3) = D_+.$$

Subtracting these and using the result above gives $\theta_2 = \pm i$. Plugging these equations into $1 + \theta_1 \phi_2^2 + \theta_2 + \theta_3 \phi_2^2 = D_+$, gives $D_+ = (1 \pm i)(1 + \theta_3 \phi_2^2)$. Equating squared norms gives $\theta_3 + \bar{\theta}_3 = 1 - \phi_2^2$. However $1 - \phi_2^2 = -2 - 2\sqrt{2} < -2$, so this is impossible.) In the third case, $(m, n) = (1, 1)$, the possible twist matrices are given by $\theta_2 = e^{\pm 4\pi i/5}$, $\theta_3 = e^{\pm 4\pi i/5}$, and $\theta_1 = \theta_2 \theta_3$.

Next consider the case $\epsilon_1 = -1$ so

$$\tilde{S} = \begin{pmatrix} 1 & d_1 & d_2 & d_3 \\ d_1 & -1 & \epsilon_2 d_3 & -\epsilon_2 d_2 \\ d_2 & \epsilon_2 d_3 & \tilde{s}_{2,2} & \tilde{s}_{2,3} \\ d_3 & -\epsilon_2 d_2 & \tilde{s}_{2,3} & -\tilde{s}_{2,2} \end{pmatrix}.$$

By symmetry under interchanging N_2 and N_3, we may assume $\epsilon_2 = +1$. Since σ is the only nontrivial element of the Galois group, we conclude that

$$d_1 - \frac{1}{d_1} = n, \quad d_2 + \frac{d_3}{d_1} = r, \quad \text{and } d_3 - \frac{d_2}{d_1} = s.$$

are integers. Hence $d_1 = \phi_n$. If $n < 0$, then $d_1 < 1$ and since it is the largest root $d_3 < d_2$. But then it follows that trace$(N_1) = d_1 - 1/d_1 + d_3/d_2 - d_2/d_3 < 0$, an impossibility. Further if $n = 0$, then the same argument shows $d_1 = 1$ and $d_3 = d_2$. However, looking at the eigenvalues of N_2 shows $\sigma(d_2) = d_3/d_1 > 0$ and looking at N_3 shows $\sigma(d_3) = -d_2/d_1 < 0$. Thus $n \geq 1$ and d_1 is irrational. Since $G = \mathbb{Z}/2\mathbb{Z}$, it follows that $K = \mathbb{Q}[d_1]$. Hence we can write $d_2 = ad_1 + b$ and $d_3 = \tilde{a}d_1 + \tilde{b}$ for rational $a, \tilde{a}, b, \tilde{b}$. Hence

$$r = d_2 + \frac{d_3}{d_1} = (a + \tilde{b})d_1 + b + \tilde{a} - n\tilde{b}, \quad \text{and} \quad s = d_3 - \frac{d_2}{d_1} = (\tilde{a} - b)d_1 + \tilde{b} - a + nb.$$

Hence $\tilde{b} = -a$, $\tilde{a} = b$, $r = na + 2b$ and $s = nb - 2a$. Note that in complex terms this gives $d_2 + id_3 = (a + ib)(d_1 - i)$ and $r + is = (a + ib)(n - 2i)$. In particular $D^2 = 1 + d_1^2 + d_2^2 + d_3^2 = (1 + d_1^2)(n^2 + r^2 + s^2 + 4)/(n^2 + 4)$.

Since the columns of $\tilde{S}$ are of equal length $\tilde{s}_{2,2}^2 + \tilde{s}_{2,3}^2 = 1 + d_1^2$. Since $\tilde{s}_{2,2}/d_2$ is an eigenvalue of N_2, $(\tilde{s}_{2,2}/d_2)\sigma(\tilde{s}_{2,2}/d_2) = \tilde{s}_{2,2}\tilde{s}_{2,3}/(d_2 d_3)$ is an integer. Further $\tilde{s}_{2,2} \neq 0$, since $\tilde{s}_{2,2} = 0$ would force $\sigma(\tilde{s}_{2,2}) = 0$ and hence $\tilde{s}_{2,3} = 0$. Thus

$$\frac{1 + d_1^2}{2d_2 d_3} \geq \frac{|\tilde{s}_{2,2}\tilde{s}_{2,3}|}{d_2 d_3} \geq 1.$$

The twist inequality coming from the $(0, 1)$ entry of $\tilde{S}$ gives

$$(1 + d_1^2)^{1/2}(1 + a^2 + b^2)^{1/2} = D \leq 2 + 2\frac{d_2 d_3}{d_1}$$

$$\leq 2 + \frac{2d_2 d_3}{1 + d_1^2} \cdot \frac{1 + d_1^2}{d_1}$$

$$\leq 2 + \frac{1 + d_1^2}{d_1} = \frac{(1 + d_1)^2}{d_1}.$$

Rewriting this gives using

$$r^2 + s^2 \leq (n^2 + 4)\frac{4d_1^3 + 5d_1^2 + 4d_1 + 1}{d_1^2(1 + d_1^2)}.$$

The twist inequality coming from the $(0, 0)$ entry of $\tilde{S}$ is $2d_1^2 \leq D^2 + D$, hence

$$2d_1^2 \leq \frac{(1 + d_1)^4}{d_1^2} + \frac{(1 + d_1)^2}{d_1}, \quad \text{or}$$

$$d_1^4 \leq 5d_1^3 + 8d_1^2 + 5d_1 + 1.$$

It follows that $d_1 < 7$, hence $1 \leq n \leq 6$. Together with the bound on $r^2 + s^2$ above, this leaves only finitely many possibilities (110 of them, insisting that d_2 and d_3 be positive, but finite).

Since $G = \mathbb{Z}/2\mathbb{Z}$, the quantities

$$\frac{d_2 d_3}{d_1} = \frac{r^2 + nrs - s^2}{n^2 + 4},$$

$$\frac{d_3}{d_2} - \frac{d_2}{d_3} = n + \frac{(n^2 + 4)rs}{r^2 + nrs - s^2},$$

$$\frac{\tilde{s}_{2,2}}{d_2} + \frac{\tilde{s}_{2,3}}{d_3} = \frac{(n^2 - 4)r^3 - 12nr^2s - 3(n^2 - 4)rs^2 + 4ns^3}{(r^2 + s^2)(r^2 + nrs - s^2)},$$

$$\frac{\tilde{s}_{2,3}}{d_2} - \frac{\tilde{s}_{2,2}}{d_3} = \frac{4nr^3 + 3(n^2 - 4)r^2s - 12nrs^2 - (n^2 - 4)s^3}{(r^2 + s^2)(r^2 + nrs - s^2)},$$

$$\frac{\tilde{s}_{2,2}\tilde{s}_{2,3}}{d_2 d_3} = \frac{(4 - 3n^2)(r^4 - 6r^2s^2 + s^4) - 2n(n^2 - 12)rs(r^2 - s^2)}{(r^2 + s^2)^2(r^2 + nrs - s^2)}$$

are all integers. Only 6 of the 110 examples pass these integrality conditions. These are $(n, r, s) = (1, 2, 1)$, $(1, 3, -1)$, $(2, 2, 2)$, $(3, 2, 3)$, $(4, 2, 4)$, and $(4, 3, 1)$. The cases with $n = s$ and $r = 2$ can be ignored since they give $a = 0$ and $b = 1$, hence $d_2 = 1$, $d_3 = d_1$, and $\tilde{s}_{2,2} = -1$. Thus $\tilde{s}_{3,3} = 1$. Invoking the symmetry under interchanging N_1 and N_3 puts us back in the case $\epsilon_1 = 1$. These are just the $(0, n)$ examples discussed above. The remaining two examples fail to give integral N_i matrices and also fail the twist inequalities. Thus there are no new examples in this case.

Case 6. G contains the transposition $\sigma = (0\ 1)$. Since we can exclude the cases above, σ must be the only non-trivial element of G. Up to symmetry there are two cases. The parity condition gives $\epsilon_1\epsilon_2\epsilon_3 = -1$. Since $d_2 = \tilde{s}_{0,2} = \epsilon_1\epsilon_2\tilde{s}_{1,2}$ and $\tilde{s}_{1,2} = \epsilon_2\tilde{s}_{0,2} = \epsilon_2 d_2$, we conclude $\epsilon_1 = 1$ and $\epsilon_3 = -\epsilon_2$. Then $\tilde{s}_{2,3} = \epsilon_2\epsilon_3\tilde{s}_{3,2}$ and the fact that $\tilde{S}$ is symmetric forces $\tilde{s}_{2,3} = \tilde{s}_{3,2} = 0$. By symmetry we may assume $\epsilon_2 = 1$ and $\epsilon_3 = -1$. Thus we get

$$\tilde{S} = \begin{pmatrix} 1 & d_1 & d_2 & d_3 \\ d_1 & 1 & d_2 & -d_3 \\ d_2 & d_2 & \tilde{s}_{2,2} & 0 \\ d_3 & -d_3 & 0 & \tilde{s}_{3,3} \end{pmatrix}.$$

Note that $\lambda_{2,2} = \tilde{s}_{2,2}/d_2$ and $\lambda_{3,3} = \tilde{s}_{3,3}/d_3$ are integers. Note that orthogonality of the third column of $\tilde{S}$ with the first forces $\lambda_{2,2} < 0$. Since $d_1 \geq \sigma(d_1) = 1/d_1$, we conclude $d_1 \geq 1$. Thus orthogonality of the first and fourth columns of $\tilde{S}$ gives $\lambda_{3,3} \geq 0$. It is straightforward, though somewhat tedious, to build the N_i matrices in this case and worry about their integrality and nonnegativity; however, there is an easier approach. Since $\tilde{s}_{2,3} = \tilde{s}_{3,2} = 0$, the twist equation for the $(2, 3)$ entry becomes

$$\theta_2\theta_3(d_2 d_3 - \theta_1 d_2 d_3) = 0.$$

Thus we conclude $\theta_1 = 1$. Using this fact the $(2, 2)$ entry becomes

$$\theta_2^2(2d_2^2 + \theta_2\tilde{s}_{2,2}^2) = D_+\tilde{s}_{2,2}.$$

Since $\tilde{s}_{2,2}/d_2 = \lambda_{2,2} < 0$ is integral and $|D_+|^2 = D^2 = (\lambda_{2,2}^2 + 2)d_2^2$, equating the squared norms of the sides of this equation gives

$$\theta_2 + \bar{\theta}_2 = 1 - \frac{2}{\lambda_{2,2}^2}.$$

The left-hand side is an algebraic integer, hence we conclude $\lambda_{2,2} = -1$ and $\theta_2 = \exp(\pm 2\pi i/3)$. Similarly, the $(3, 3)$ entry gives $\lambda_{3,3} = 1$ and $\theta_3 = \exp(\pm 2\pi i/3)$. Equating the squared lengths of the last two columns of $\tilde{S}$ now gives $d_2^2 = d_3^2$, hence $d_2 = d_3$. This is a contradiction, since $\sigma(d_2) = \lambda_{2,1} = d_2/d_1$ but $\sigma(d_3) = \lambda_{3,1} = -d_3/d_1$.

Case 7. G is trivial. This case is also contained in [CZ].

In this case all the d_i and $\lambda_{i,j}$ are integral. By symmetry, we may assume $1 \leq d_1 \leq d_2 \leq d_3$. Since every column of $\tilde{S}$ must have squared length D^2, we see that D^2 must be a multiple of d_i^2 for all i. If $d_1 = d_2 = d_3$, then d_1^2 must divide $D^2 = 3d_1^2 + 1$. Hence $d_1 = d_2 = d_3 = 1$. Up to symmetry orthogonality of the columns of $\tilde{S}$ forces

$$\tilde{S} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix},$$

or

$$\tilde{S} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

For the first $\tilde{S}$ matrix, this gives integral N_i matrices

$$N_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad N_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \text{and } N_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

The possibilities for the corresponding twist matrix are

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -i \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix},$$

or their complex conjugates. (Note that this is the case $m = n = 0$ of the form found in Cases 2 and 5.) For the second $\tilde{S}$ matrix, the compatible T matrices are listed in Table 2.

If the d_i are not all equal, then $d_1 < d_3$, hence $1 + d_1^2 < d_3^2$ and $d_3^2 < D^2 < 3d_3^2$. Thus we must have $D^2 = 2d_3^2$, i.e., two of the $\tilde{s}_{i,3}$ are zero and the other two are $\pm d_3$. Of course $\tilde{s}_{0,3} = d_3$. Suppose $\tilde{s}_{j,3} = \pm d_3$ is the other nonzero entry in the last column. Orthogonality of the first and last columns gives $d_3(1 \pm d_j) = 0$, hence the lower sign is correct and $d_j = 1$. Thus using symmetry we may assume $j = 1$. Orthogonality of the remaining columns with the last column gives $\tilde{s}_{1,1} = d_1 = 1$ and $\tilde{s}_{2,1} = d_2$. Orthogonality of the third column and the first two gives $\tilde{s}_{2,2} = -2$ and

$$\tilde{S} = \begin{pmatrix} 1 & 1 & d_2 & d_3 \\ 1 & 1 & d_2 & -d_3 \\ d_2 & d_2 & -2 & 0 \\ d_3 & -d_3 & 0 & 0 \end{pmatrix}.$$

However equality of the squared lengths of the last two columns now gives $D^2 = 2d_3^2 = 2d_2^2 + 4$ or $d_3^2 = d_2^2 + 2$, an impossibility. $\quad\square$

5. Realization of Fusion Rules and Classification of MTCs

In this section, for each modular fusion rule $(\mathcal{N}; \tilde{S})$ in Theorems 3.1, 3.2, 4.1, we will first determine all modular symbols with this fusion rule which also satisfy (1), (2) of Proposition 2.3, then classify all MTCs realizing each such modular symbol.

For each modular fusion rule $(\mathcal{N}; \tilde{S})$, there are two choices of compatible S matrices: $S = \frac{1}{D}\tilde{S}$ or $-\frac{1}{D}\tilde{S}$. When the two modular symbols are realized by (2+1)-TQFTs, respectively, one TQFT is obtained from the other by tensoring the trivial theory with $S = (-1)$. The quantum invariant of the 3-sphere will be $\frac{1}{D}$ or $-\frac{1}{D}$, respectively. Also the topological central charge c of the two theories will differ by 4. Another symmetry for modular symbols is complex conjugation: to change $(\mathcal{N}; S, T)$ to $(\mathcal{N}; S^\dagger, T^\dagger)$. Complex conjugation of a modular symbol gives rise to a different modular symbol if one of the S, T is not a real matrix.

Given an $\tilde{S}$ matrix, we can obtain all fusion matrices by using the Verlinde formulas. Instead of listing fusion matrices, we will present them as fusion rules. In the following, we will not list trivial fusion rules such as $1 \otimes x = x$ and those that can be obtained from obvious identities such as $x \otimes y = y \otimes x$. We will also write $x \otimes y$ as xy sometimes. Then we use relations (3)(i)-(iv) of Definition 2.1 together with (1) (2) of Proposition 2.3 to determine the possible T-matrices. As Example 2.2 illustrates, Proposition 2.3 is necessary to get finitely many solutions in some cases. We find that there are finitely many modular symbols $(\mathcal{N}; S, T)$ of rank≤ 4 satisfying Proposition 2.3. Modulo the symmetry $S \to -S$, these modular symbols are classified in Table 2. In the table, $\zeta_m = e^{\frac{2\pi i}{m}}$. The labels will be $\{1, X\}$ for rank=2, $\{1, X, Y\}$ for rank=3, and $\{1, X, Y, Z\}$ for rank=4. They will correspond to rows 1, 2, 3, 4 of the $\tilde{S}$ matrices. The # is the number of modular symbols satisfying Proposition 2.3 modulo the symmetry $S \to -S$. The column P stands for primality, and the column G is the Galois group of the modular fusion rule.

With modular symbols determined, we turn to realizing each of them with MTCs. First let us consider the $\tilde{S}$-matrices corresponding to Theorem 4.1(3)-(5). In each of these cases there is a rank=2 tensor subcategory corresponding to the objects labelling columns 1 and 3 of the $\tilde{S}$ matrix. Further inspection shows that the submatrix of $\tilde{S}$ corresponding to rows and columns 1 and 3 is invertible. It is obvious that the tensor subcategory generated by the trivial object and the object labelling column 3 is a modular subcategory. For the $\tilde{S}$-matrices of Theorem 4.1(3),(4) these rank=2 modular subcategories are equivalent to the UMTCs corresponding to Theorem 3.1(1), while the modular subcategory corresponding to the $\tilde{S}$-matrix of Theorem 4.1(5) is equivalent to (one of) the UMTCs coming from Theorem 3.1(2). By [M2, Theorem 4.2] this implies that the MTCs corresponding to these $\tilde{S}$ matrices are direct products of rank=2 MTCs. For this reason we will not write down realizations or complete data for these MTCs as they can be deduced from their product structure.

MTCs realizing the remaining 8 nontrivial modular symbols are *prime*, i.e. they do not have non-trivial modular subcategories. To complete the classification, we need to solve the pentagon and hexagon equations for all 8 modular symbols. The solutions of the pentagon equations are organized into the F-matrices whose entries are called $6j$ symbols. The solutions of hexagons are given by the braiding eigenvalues.

5.1. F-matrices. Given an MTC $\mathcal{C}$, a 4-punctured sphere $S^2_{a,b,c,d}$, where the 4 punctures are labelled by a, b, c, d, can be divided into two pairs of pants (=3-punctured spheres) in two different ways. In the following figure, the 4-punctured sphere is the boundary of a thickened neighborhood of the graph in either side, and the two graphs encode the

Table 2. Rank≤ 4 unitary modular symbols

$\tilde{S}$ matrix	Fusion rules	T matrix	#s	P	G
$\tilde{S} = (1)$		(1)	1	Yes	1
Thm 3.1(1)	$X^2 = 1$	$\mathrm{Diag}(1, \pm i)$	2	Yes	1
Thm 3.1(2)	$X^2 = 1 + X$	$\mathrm{Diag}(1, (\zeta_5)^{\pm 2})$	2	Yes	$\mathbb{Z}_2$
Thm 3.2(1)	$X^2 = X^*, XX^* = 1,$ $(X^*)^2 = X$	$\mathrm{Diag}(1, \zeta_3^{\pm 1}, \zeta_3^{\pm 1})$	2	Yes	$\mathbb{Z}_2$
Thm 3.2(2)	$X^2 = 1 + Y,$ $XY = X, Y^2 = 1$	$\mathrm{Diag}(1, (\zeta_{16})^{2k+1}, -1)$	8	Yes	$\mathbb{Z}_2$
Thm 3.2(3)	$X^2 = 1 + X + Y,$ $XY = X + Y,$ $Y^2 = 1 + X$	$\mathrm{Diag}(1, (\zeta_7)^{\pm 5}, (\zeta_7)^{\pm 1})$	2	Yes	$\mathbb{Z}_3$
Thm 4.1(1)	$X^2 = Y = (X^*)^2,$ $XX^* = 1 = Y^2,$ $XY = X^*, X^*Y = X$	$\mathrm{Diag}(1, -1, (\zeta_8)^{\pm m}, (\zeta_8)^{\pm m}), m{=}1,3$	4	Yes	$\mathbb{Z}_2$
Thm 4.1(2)	$X^2 = 1, XY = Z,$ $XZ = Y, Y^2 = 1,$ $YZ = X, Z^2 = 1$	$\mathrm{Diag}(1, -1, \epsilon_1, \epsilon_1), \epsilon_1^2 = 1$	2	Yes	1
Thm 4.1(3)	$X^2 = 1, XY = Z,$ $XZ = Y, Y^2 = 1,$ $YZ = X, Z^2 = 1$	$\mathrm{Diag}(1, \theta_1, \theta_2, \theta_1\theta_2), \theta_i^2 = -1$	3	No	1
Thm 4.1(4)	$X^2 = 1 + X,$ $XY = Z,$ $XZ = Y + Z, Y^2 = 1,$ $YZ = X, Z^2 = 1 + X$	$\mathrm{Diag}(1, \theta_1, \theta_2, \theta_1\theta_2), \theta_1 = (\zeta_5)^{\pm 2}, \theta_2 = \pm i$	4	No	$\mathbb{Z}_2$
Thm 4.1(5)	$X^2 = 1 + X,$ $XY = Z,$ $XZ = Y + Z,$ $Y^2 = 1 + Y,$ $YZ = X + Z,$ $Z^2 = 1 + X + Y + Z$	$\mathrm{Diag}(1, \theta_1, \theta_2, \theta_1\theta_2), \theta_1 = (\zeta_5)^{\pm 2}, \theta_2 = (\zeta_5)^{\pm 2}$	3	No	$\mathbb{Z}_2$
Thm 4.1(6)	$X^2 = 1 + X + Y,$ $XY = X + Y + Z,$ $XZ = Y + Z,$ $Y^2 = 1 + X + Y + Z,$ $YZ = X + Y,$ $Z^2 = 1 + X$	$\mathrm{Diag}(1, \zeta_9^{\pm 2}, (\zeta_9)^{\pm 6}, (\zeta_9)^{\mp 6})$	2	Yes	$\mathbb{Z}_3$

two different pants-decompositions of the 4-punctured sphere. The F-move is just the change of the two pants-decompositions.

When bases of all pair of pants spaces $\mathrm{Hom}(a \otimes b, c)$ are chosen, then the two pants decompositions of $S^2_{a,b,c,d}$ determine bases of the vector spaces $\mathrm{Hom}((a \otimes b) \otimes c, d)$, and $\mathrm{Hom}(a \otimes (b \otimes c), d)$, respectively. Therefore the F-move induces a matrix $F_d^{a,b,c}$: $\mathrm{Hom}((a \otimes b) \otimes c, d) \rightarrow \mathrm{Hom}(a \otimes (b \otimes c), d)$, which are called the F-matrices. Consistency of the F matrices are given by the pentagon equations.

For each quadruple (a, b, c, d), we have an F-matrix whose entries are indexed by a pair of triples $((m, s, t), (n, u, v))$, where m, n are the labels for the internal edges, and s, t, u, v are indices for a basis of the $\mathrm{Hom}(x \otimes y, z)$ spaces with dim > 1. For the MTCs in our paper, none of the $\mathrm{Hom}(a \otimes b, c)$ has dim > 1, so we will drop the s, t, u, v from our notation. If one of the a, b, c in $F_d^{a,b,c}$ is the trivial label, then we may assume $F_d^{a,b,c}$ is the identity matrix. But we cannot always do so if d is the trivial label.

In the following, any unlisted F matrix is the identity.

$$a\ b\ c \qquad\qquad a\ b\ c$$
$$F_d^{abc}$$
$$m \qquad\qquad n$$
$$d \qquad\quad d$$

5.2. Braidings and twists.
The twist of the simple type X_i will be denoted by θ_i, and it is defined by the following positive twist:

$$= \theta_i$$

The braiding eigenvalues are defined by the following diagram:

$$a\quad b \qquad\qquad a\quad b$$
$$= R_c^{ab}$$
$$c \qquad\qquad c$$

The consistency equations of the braidings are given by two independent families of hexagon equations. If c is the trivial label, and label a is self-dual, then $R_1^{aa} = \nu_a \theta_a^{-1}$, where ν_a is the Frobenius-Schur indicator of a.

5.3. Explicit data.
In this section, we give the explicit data for at least one realization of each prime modular fusion rule. Since each modular symbol can have up to 4 MTC realizations, we will present the complete data for only one of them. We choose one with the following properties:

(1) The $(0, 0)$ entry of the S matrix is $\frac{1}{D}$, where D is the total quantum order.
(2) In a category with a generating non-abelian simple object X, we choose a theory with the positive exponent of the twist θ_X being the smallest. This is inspired by anyon theory that the simple object with the smallest exponent is the most relevant in physical experiments.

If a modular symbol $(\mathcal{N}; S, T)$ is realized by an MTC, then the modular symbol $(\mathcal{N}; -S, T)$ is also realized by an MTC. The modular symbol $(\mathcal{N}; \tilde{S}^\dagger, T^\dagger)$ is realized by complex conjugating all F matrices and braidings of $(\mathcal{N}; S, T)$. So in the following each group of data will be for 4 MTCs if any of S, T, F and braidings are not real; otherwise there will be two. We choose the F matrices to be unitary, and real if possible.

In anyon theory, labels will be called anyon types. The smallest positive exponent of a twist θ_i will be called the topological spin of the anyon type i. Topological spins are the

conformal dimensions modulo integers of the corresponding primary field if the MTC has a corresponding RCFT. The last line of the data lists all quantum group realizations of the same theory. We did not list the Frobenius-Schur indicators of anyons because they can be calculated by the formula in Proposition 2.3. In the following data, only the semion s and the $(A_1, 2)$ non-abelian anyon σ have Frobenius-Schur indicator$=-1$.

5.3.1. Semion MTC We will use s to denote the non-trivial label.

Anyon types: $\{1, s\}$
Fusion rules: $s^2 = 1$
Quantum dimensions: $\{1, 1\}$
Twists: $\theta_1 = 1, \theta_s = i$
Total quantum order: $D = \sqrt{2}$
Topological central charge: $c = 1$
Braidings: $R_1^{ss} = i$
S-matrix: $S = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
F-matrices: $F_s^{s,s,s} = (-1)$
Realizations: $(A_1, 1), (E_7, 1)$

5.3.2. Fibonacci MTC We will use φ to denote the golden ratio $\varphi = \frac{1+\sqrt{5}}{2}$ and τ the non-trivial label.

Anyon types: $\{1, \tau\}$
Fusion rules: $\tau^2 = 1 + \tau$
Quantum dimensions: $\{1, \varphi\}$
Twists: $\theta_1 = 1, \theta_\tau = e^{\frac{4\pi i}{5}}$
Total quantum order: $D = 2\cos(\frac{\pi}{10}) = \frac{\sqrt{5}}{2\sin(\frac{\pi}{5})}$
Topological central charge: $c = \frac{14}{5}$
Braidings: $R_1^{\tau\tau} = e^{-\frac{4\pi i}{5}}, R_\tau^{\tau\tau} = e^{\frac{3\pi i}{5}}$
S-matrix: $S = \frac{1}{\sqrt{2+\varphi}} \begin{pmatrix} 1 & \varphi \\ \varphi & -1 \end{pmatrix}$
F-matrices: $F_\tau^{\tau,\tau,\tau} = \begin{pmatrix} \varphi^{-1} & \varphi^{-1/2} \\ \varphi^{-1/2} & -\varphi^{-1} \end{pmatrix}$
Realizations: $(A_1, 3)_{\frac{1}{2}}, (G_2, 1)$, complex conjugate of $(F_4, 1)$

5.3.3. $\mathbb{Z}_3$ MTC We will use ω for both a non-trivial label and the root of unity $\omega = e^{2\pi i/3}$. No confusions should arise.

Anyon types: $\{1, \omega, \omega^*\}$
Fusion rules: $\omega^2 = \omega^*, \omega\omega^* = 1, (\omega^*)^2 = \omega$
Quantum dimensions: $\{1, 1, 1\}$
Twists: $\theta_1 = 1, \theta_\omega = \theta_{\omega^*} = e^{\frac{2\pi i}{3}}$
Total quantum order: $D = \sqrt{3}$
Topological central charge: $c = 2$
Braidings: $R_1^{\omega,\omega^*} = R_1^{\omega^*,\omega} = e^{-\frac{2\pi i}{3}}, R_{\omega^*}^{\omega,\omega} = R_\omega^{\omega^*,\omega^*} = e^{-\frac{4\pi i}{3}}$
S-matrix: $S = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$

F-matrices: $F_d^{a,b,c} = (1)$ for any a, b, c, d
Realizations: $(A_2, 1), (E_6, 1)$

5.3.4. *Ising MTC* We will use $1, \sigma, \psi$ to denote the non-trivial labels.

Anyon types: $\{1, \sigma, \psi\}$
Fusion rules: $\sigma^2 = 1 + \psi, \sigma\psi = \psi\sigma = \sigma, \psi^2 = 1$
Quantum dimensions: $\{1, \sqrt{2}, 1\}$
Twists: $\theta_1 = 1, \theta_\sigma = e^{\frac{\pi i}{8}}, \theta_\psi = -1$
Total quantum order: $D = 2$
Topological central charge: $c = \frac{1}{2}$
Braidings: $R_1^{\sigma\sigma} = e^{-\frac{\pi i}{8}}, R_1^{\psi\psi} = -1, R_\sigma^{\psi\sigma} = R_\sigma^{\sigma\psi} = -i, R_\psi^{\sigma\sigma} = e^{\frac{3\pi i}{8}}$
S-matrix: $S = \frac{1}{2} \begin{pmatrix} 1 & \sqrt{2} & 1 \\ \sqrt{2} & 0 & -\sqrt{2} \\ 1 & -\sqrt{2} & 1 \end{pmatrix}$
F-matrices: $F_\sigma^{\sigma,\sigma,\sigma} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, F_\sigma^{\psi,\sigma,\psi} = (-1), F_\psi^{\sigma,\psi,\sigma} = (-1)$
Realizations: complex conjugate of $(E_8, 2)$

5.3.5. $(A_1, 2)$ *MTC* We will use $1, \sigma, \psi$ to denote the non-trivial labels again.

Anyon types: $\{1, \sigma, \psi\}$
Fusion rules: $\sigma^2 = 1 + \psi, \sigma\psi = \psi\sigma = \sigma, \psi^2 = 1$
Quantum dimensions: $\{1, \sqrt{2}, 1\}$
Twists: $\theta_1 = 1, \theta_\sigma = e^{\frac{3\pi i}{8}}, \theta_\psi = -1$
Total quantum order: $D = 2$
Topological central charge: $c = \frac{3}{2}$
Braidings: $R_1^{\sigma\sigma} = -e^{-\frac{\pi i}{8}}, R_1^{\psi\psi} = -1, R_\sigma^{\psi\sigma} = R_\sigma^{\sigma\psi} = i, R_\psi^{\sigma\sigma} = e^{\frac{\pi i}{8}}$
S-matrix: $S = \frac{1}{2} \begin{pmatrix} 1 & \sqrt{2} & 1 \\ \sqrt{2} & 0 & -\sqrt{2} \\ 1 & -\sqrt{2} & 1 \end{pmatrix}$
F-matrices: $F_\sigma^{\sigma,\sigma,\sigma} = -\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, F_\sigma^{\psi,\sigma,\psi} = (-1), F_\psi^{\sigma,\psi,\sigma} = (-1)$
Realizations: $(A_1, 2)$

5.3.6. $(A_1, 5)_{\frac{1}{2}}$ *MTC* We will use $1, \alpha, \beta$ to denote the non-trivial labels. Note that $1, \alpha, \beta$ are special labels for $1, Y, X$ in Theorem 3.2(3) of Table 2.

Anyon types: $\{1, \alpha, \beta\}$
Fusion rules: $\alpha^2 = 1 + \beta, \alpha\beta = \alpha + \beta, \beta^2 = 1 + \alpha + \beta$
Quantum dimensions: $\{1, d, d^2 - 1\}$, where $d = 2\cos(\frac{\pi}{7})$
Twists: $\theta_1 = 1, \theta_\alpha = e^{\frac{2\pi i}{7}}, \theta_\beta = e^{\frac{10\pi i}{7}}$
Total quantum order: $D = \frac{\sqrt{7}}{2\sin(\frac{\pi}{7})}$
Topological central charge: $c = \frac{48}{7}$
Braidings: $R_1^{\alpha\alpha} = e^{-\frac{2\pi i}{7}}, R_1^{\beta\beta} = e^{-\frac{10\pi i}{7}}$
$R_\alpha^{\beta\beta} = e^{-\frac{2\pi i}{7}}, R_\alpha^{\alpha\beta} = R_\alpha^{\beta\alpha} = e^{\frac{9\pi i}{7}}$
$R_\beta^{\beta\beta} = e^{-\frac{5\pi i}{7}}, R_\beta^{\alpha\beta} = R_\beta^{\beta\alpha} = e^{\frac{6\pi i}{7}}, R_\beta^{\alpha\alpha} = e^{-\frac{4\pi i}{7}}$

S-matrix: $S = \frac{1}{D} \begin{pmatrix} 1 & d & d^2 - 1 \\ d & -d^2 + 1 & 1 \\ d^2 - 1 & 1 & -d \end{pmatrix}$

F-matrices: see the end of this subsection

Realizations: $(A_1, 5)_{\frac{1}{2}}$

5.3.7. $\mathbb{Z}_4$ MTC
We will use $1, \epsilon, \sigma, \sigma^*$ to denote the non-trivial labels.

Anyon types: $\{1, \epsilon, \sigma, \sigma^*\}$

Fusion rule: $\epsilon^2 = \sigma\sigma^* = 1, \sigma^2 = (\sigma^*)^2 = \epsilon, \sigma\epsilon = \sigma^*, \sigma^*\epsilon = \sigma$

Quantum dimensions: $\{1, 1, 1, 1\}$

Twists: $\theta_1 = 1, \theta_\epsilon = -1, \theta_\sigma = \theta_{\sigma^*} = e^{\frac{\pi i}{4}}$

Total quantum order: $D = 2$

Topological central charge: $c = 1$

Braidings: $R_1^{\epsilon,\epsilon} = -1, R_\epsilon^{\sigma,\sigma} = R_\epsilon^{\sigma^*,\sigma^*} = e^{\frac{\pi i}{4}}, R_1^{\sigma,\sigma^*} = R_1^{\sigma^*,\sigma} = e^{-\frac{\pi i}{4}},$
$R_{\sigma^*}^{\sigma,\epsilon} = R_{\sigma^*}^{\epsilon,\sigma} = R_\sigma^{\sigma^*,\epsilon} = R_\sigma^{\epsilon,\sigma^*} = -i$

S-matrix: $S = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -i & i \\ 1 & -1 & i & -i \end{pmatrix}$

F-matrices: $F_{\sigma^*}^{\sigma,\sigma,\sigma} = F_\sigma^{\sigma^*,\sigma^*,\sigma^*} = F_\sigma^{\epsilon,\sigma,\epsilon} = F_{\sigma^*}^{\epsilon,\sigma^*,\epsilon} = F_\epsilon^{\sigma,\epsilon,\sigma} = F_\epsilon^{\sigma^*,\epsilon,\sigma} = (-1)$

Realizations: $(A_3, 1), (D_9, 1)$

5.3.8. Toric code MTC
The fusion rules are the same as $\mathbb{Z}_2 \times \mathbb{Z}_2$, but the theory is not a direct product. We will use $1, e, m, \epsilon$ to denote the non-trivial labels.

Anyon types: $\{1, e, m, \epsilon\}$

Fusion rules: $e^2 = m^2 = \epsilon^2 = 1, em = \epsilon, e\epsilon = m, m\epsilon = e$

Quantum dimensions: $\{1, 1, 1, 1\}$

Twists: $\theta_1 = \theta_e = \theta_m = 1, \theta_\epsilon = -1$

Total quantum order: $D = 2$

Topological central charge: $c = 0$

Braidings: $R_1^{\epsilon,\epsilon} = -1, R_\epsilon^{e,m} = 1, R_\epsilon^{m,e} = -1, R_1^{e,e} = R_1^{m,m} = 1,$
$R_e^{\epsilon,m} = 1, R_e^{m,\epsilon} = -1, R_m^{e,\epsilon} = 1, R_m^{\epsilon,e} = -1$

S-matrix: $S = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$

F-matrices: $F_d^{a,b,c} = (1)$ for all a, b, c, d

Realizations: $(D_8, 1), D(\mathbb{Z}_2)$—quantum double of $\mathbb{Z}_2$

5.3.9. $(D_4, 1)$ MTC
The fusion rules are the same as $\mathbb{Z}_2 \times \mathbb{Z}_2$, but the theory is not a direct product. We will use $1, e, m, \epsilon$ to denote the non-trivial labels again.

Anyon types: $\{1, e, m, \epsilon\}$

Fusion rules: $e^2 = m^2 = \epsilon^2 = 1, em = \epsilon, e\epsilon = m, m\epsilon = e$

Quantum dimensions: $\{1, 1, 1, 1\}$

Twists: $\theta_1 = 1, \theta_e = \theta_m = \theta_\epsilon = -1$

Total quantum order: $D = 2$

Topological central charge: $c = 4$

Braidings: $R_1^{\epsilon,\epsilon} = -1$, $R_\epsilon^{e,m} = -1$, $R^{m,e} = 1$, $R_1^{e,e} = R_1^{m,m} = -1$, $R_e^{\epsilon,m} = 1$, $R_e^{m,\epsilon} = -1$, $R_m^{\epsilon,\epsilon} = 1$, $R_m^{\epsilon,e} = -1$

S-matrix: $S = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$

F-matrices: $F_d^{a,b,c} = (1)$ for all a, b, c, d

Realizations: $(D_4, 1)$

5.3.10. $(A_1, 7)_{\frac{1}{2}}$ *MTC* We will use $1, \alpha, \omega, \rho$ to denote the non-trivial labels. Note that $1, \alpha, \omega, \rho$ are special labels for $1, Z, Y, X$ in Theorem 4.1(6) of Table 2.

Anyon types: $\{1, \alpha, \omega, \rho\}$

Fusion rules: $\alpha^2 = 1 + \omega$, $\alpha\omega = \alpha + \rho$, $\alpha\rho = \omega + \rho$, $\omega^2 = 1 + \omega + \rho$
$\omega\rho = \alpha + \omega + \rho$, $\rho^2 = 1 + \alpha + \omega + \rho$

Quantum dimensions: $\{1, d, d^2 - 1, d + 1\}$, where $d = 2\cos(\frac{\pi}{9})$ and $d^3 = 3d + 1$

Twists: $\theta_1 = 1$, $\theta_\alpha = e^{\frac{2\pi i}{3}}$, $\theta_\omega = e^{\frac{4\pi i}{9}}$, $\theta_\rho = e^{\frac{4\pi i}{3}}$

Total quantum order: $D = \frac{3}{2\sin(\frac{\pi}{9})}$

Topological central charge: $c = \frac{10}{3}$

Braidings: $R_1^{\alpha\alpha} = e^{-\frac{2\pi i}{3}}$, $R_1^{\omega\omega} = e^{-\frac{4\pi i}{9}}$, $R_1^{\rho\rho} = e^{-\frac{4\pi i}{3}}$
$R_\alpha^{\alpha\omega} = R_\alpha^{\omega\alpha} = e^{\frac{7\pi i}{9}}$, $R_\alpha^{\omega\rho} = R_\alpha^{\rho\omega} = e^{\frac{4\pi i}{9}}$, $R_\alpha^{\rho\rho} = -1$
$R_\omega^{\alpha\rho} = R_\omega^{\rho\alpha} = e^{\frac{2\pi i}{9}}$, $R_\omega^{\omega\rho} = R_\omega^{\rho\omega} = e^{-\frac{2\pi i}{3}}$, $R_\omega^{\alpha\alpha} = e^{\frac{5\pi i}{9}}$, $R_\omega^{\rho\rho} = e^{-\frac{\pi i}{9}}$, $R_\omega^{\omega\omega} = e^{\frac{7\pi i}{9}}$
$R_\rho^{\alpha\omega} = R_\rho^{\omega\alpha} = e^{-\frac{8\pi i}{9}}$, $R_\rho^{\alpha\rho} = R_\rho^{\rho\alpha} = e^{-\frac{\pi i}{3}}$, $R_\rho^{\rho\omega} = R_\rho^{\omega\rho} = e^{\frac{7\pi i}{9}}$, $R_\rho^{\omega\omega} = e^{\frac{2\pi i}{9}}$,
$R_\rho^{\rho\rho} = e^{-\frac{2\pi i}{3}}$

S-matrix: $S = \frac{1}{D} \begin{pmatrix} 1 & d & d^2 - 1 & d + 1 \\ d & -d - 1 & d^2 - 1 & -1 \\ d^2 - 1 & d^2 - 1 & 0 & -d^2 + 1 \\ d + 1 & -1 & -d^2 + 1 & d \end{pmatrix}$

F-matrices: see below

Realizations: $(A_1, 7)_{\frac{1}{2}}$, complex conjugate of $(G_2, 2)$

The list of all F matrices for an MTC can occupy many pages. But they are needed for the computation of quantum invariants using graph recouplings, the Hamiltonian formulation of MTCs as in [LWe] or the study of anyon chains [FTL]. For the MTCs $(A_1, k)_{\frac{1}{2}}$ with odd k, all the data of the theory can be obtained from [KL]. For $k = 5$, choose $A = ie^{-\frac{2\pi i}{28}}$, the label set is $\mathcal{L} = \{0, 2, 4\}$ in [KL] and $0 = 1, 4 = \alpha, 2 = \beta$. For $k = 7$, set $A = ie^{\frac{2\pi i}{36}}$, the label set is $\mathcal{L} = \{0, 2, 4, 6\}$ in [KL] and $0 = 1, 6 = \alpha, 2 = \omega, 4 = \rho$. The twist is given by $\theta_a = (-1)^a A^{a(a+2)}$, and the braiding $R^{ab}_c = (-1)^{\frac{a+b-c}{2}} A^{-\frac{a(a+2)+b(b+2)-c(c+2)}{2}}$. The formulas for $6j$ symbols can be found in Chap. 10 of [KL]. The F matrices from [KL] are not unitary, but the complete data can be presented over an abelian Galois extension of $\mathbb{Q}$. To have unitary F matrices, we need to normalize the θ symbols as $\theta(i, j, k) = \sqrt{d_i d_j d_k}$.

The $(A_1, k)_{\frac{1}{2}}$, k odd, MTCs have peculiar properties regarding the relation between the bulk $(2 + 1)$-TQFTs and the boundary RCFTs. To realize $(A_1, k)_{\frac{1}{2}}$, k odd, using the Kauffman bracket formalism, we set $A = ie^{\pm\frac{2\pi i}{4(k+2)}}$. In order to follow the convention above, we choose $A = ie^{-\frac{2\pi i}{4(k+2)}}$ if $k = 1 \mod 4$, and $A = ie^{\frac{2\pi i}{4(k+2)}}$ if $k = -1 \mod 4$.

Note that in both cases A is a $2(k+2)^{\text{th}}$ root of unity. We have

$$(A_1, k) = \overline{(A_1, k)_{\frac{1}{2}}} \times \text{ the semion}, \qquad (5.1)$$

if $k = 1 \bmod 4$, and

$$(A_1, k) = (A_1, k)_{\frac{1}{2}} \times \overline{\text{ the semion}}, \qquad (5.2)$$

if $k = -1 \bmod 4$. The central charge of (A_1, k) is $\frac{3k}{k+2}$, which implies that the central charge of $(A_1, k)_{\frac{1}{2}}$ is $c_k = 1 - \frac{3k}{k+2}$ if $k = 1 \bmod 4$, and $c_k = 1 + \frac{3k}{k+2}$ if $k = -1 \bmod 4$.

In Table 3, we list all unitary quantum groups categories of rank≤ 12 from the standard construction. For notation, see [HRW].

Remark 5.1. The following serves as a guide to Table 3.

(1) In general we will list these categories as (X_r, k) for the category obtained from a quantum group of type X_r at level k. Observe that the corresponding root of unity is of order $\ell = mk + h$, where $m = 1$ for $X = A, D$, or E; $m = 2$ for $X = B, C$ or F and $m = 3$ for $X = G$, and h is the dual Coxeter number.

(2) The category (A_r, k) has a modular subcategory $(A_r, k)_{\frac{1}{r+1}}$ generated by the objects with integer weights provided $\gcd(r+1, k) = 1$. These are found on line 5 of Table 3 where

$$L = \{(1, 2s + 1), (2s, 2), (2, 4), (2, 5), (2, 7), (3, 3), (4, 3), (6, 3) : 1 \leq s \leq 11\}.$$

(3) We include the examples of pseudo-unitary categories coming from low-rank coincidences for quantum groups of types F_4 and G_2 at roots of unity of order coprime to 2 and 3 respectively.

(4) This list includes different realizations of equivalent categories. We eliminate those coincidences that occur because of Lie algebra isomorphisms such as $\mathfrak{sp}_4 \cong \mathfrak{so}_5$ etc., and do not include the trivial rank$= 1$ category.

(5) NSD means the category contains non-self-dual objects.

(6) "c.f. (X_r, k)" means the categories in question have the same fusion rules as those of (X_r, k).

(7) We include the three categories coming from doubles of finite groups with rank≤ 12, although they are not strictly speaking of quantum group type.

5.4. Classification. In this section, we explain Table 1. We identify MTCs whose label sets differ by permutations. For the trivial MTCs, the two MTCs are distinguished by the S matrices: $S = (\pm 1)$.

For the $\mathbb{Z}_2$ fusion rule, unitary MTCs are the semion MTC and those from the two symmetries $S \to -S$ and complex conjugate.

For the Fibonacci fusion rule, unitary MTCs are the Fibonacci MTC and those from the two symmetries $S \to -S$ and complex conjugate.

For the $\mathbb{Z}_3$ fusion rule, all unitary MTCs are the one listed in the last subsection and those from the two symmetries $S \to -S$ and complex conjugate.

For the Ising fusion rule, there are a total of 16 theories divided into two groups according to the Frobenius-Schur indicator of the non-abelian anyon X, $X^2 = 1 + Y$. There are 8 unitary MTCs with Frobenius-Schur indicator=1. Their twists are given

Table 3. Unitary Quantum Group Categories of rank ≤ 12

(X_r, k)	Rank	Notes	ℓ
$(A_r, 1), r \leq 11$	$r + 1$	$r \geq 2$ NSD, abelian	$r + 2$
$(A_1, k), k \leq 11$	$k + 1$		$k + 2$
$(A_2, 2)$	6	NSD	5
$(A_2, 3), (A_3, 2)$	10	NSD	6
$(A_r, k)_{\frac{1}{r+1}}, (r, k) \in L$	$\frac{1}{r+1}\binom{k+r}{k}$	$r \geq 2$ NSD	$k + r + 1$
$(B_r, 1)$	3	c.f. $(A_1, 2)$	$4r$
$(B_r, 2), r \leq 8$	$r + 4$	finite braid image?	$4r + 2$
$(B_2, 3)$	10		12
$(C_r, 1) \, r \leq 11$	$r + 1$	c.f. (A_1, r)	$2(r + 2)$
$(C_3, 2)$	10		12
$(D_{2r}, 1)$	4	r even c.f. $D^\omega(\mathbb{Z}_2)$	$4r - 1$
$(D_{2r+1}, 1)$	4	c.f. $(A_3, 1)$	$4r + 1$
$(D_r, 2), r = 4, 5$	11, 12	$r = 5$ NSD	8, 10
$(E_6, k), k = 1, 2$	3, 9	NSD	13, 14
$(E_7, k), 1 \leq k \leq 3$	2, 6, 11		19, 20, 21
$(E_8, k), 2 \leq k \leq 4$	3, 5, 10		32, 33, 34
$(F_4, k), 1 \leq k \leq 3$	2, 5, 9		20, 22, 24
$(G_2, k), 1 \leq k \leq 5$	2, 4, 6, 9, 12		15, 18, 21, 24, 27
F_4	10	c.f. $(E_8, 4)$	17
G_2	5, 8, 10		11, 13, 14
$D^\omega(\mathbb{Z}_2)$	4	prime	
$D^\omega(\mathbb{Z}_3)$	9	prime	
$D^\omega(S_3)$	8	c.f. $(B_4, 2)$	

by $\theta_X = e^{\frac{m\pi i}{8}}$ for $m = 1, 7, 9, 15$. The Ising MTC is the simplest one with $m = 1$ and central charge $c = \frac{1}{2}$. The theory $m = 1, m = 15$ are complex conjugate of each other, so are the $m = 7, 9$. The other 4 MTCs are obtained by choosing $-S$. There are 8 unitary MTCs with Frobenius-Schur indicator$=-1$. Their twists are $\theta_X = e^{\frac{m\pi i}{8}}$ for $m = 3, 5, 11, 13$. The $SU(2)$ at level $k = 2$ is the simplest one with $m = 3$ and central charge $c = \frac{3}{2}$. The MTCs $m = 3$ and $m = 13$ are complex conjugate, so are $m = 5, 11$. The other 4 are those with $-S$. The Ising MTC is not an $SU(2)$ theory. It can, however, be obtained as a quantum group category as the complex conjugate of E_8 at level$=2$. Note that the F matrices in each group of 8 are the same, but their braidings are different. The $SU(2)$ level$=2$ theory has $F_X^{XXX} = -F_\sigma^{\sigma\sigma\sigma}$ with the other F matrices the same as the Ising theory.

For the $(A_1, 5)_{\frac{1}{2}}$ fusion rule, all unitary MTCs are the one listed in the last subsection and those from the two symmetries $S \to -S$ and complex conjugate.

For the $\mathbb{Z}_2 \times \mathbb{Z}_2$ fusion rules, there are two groups of theories depending on whether or not the theory is a product. There are 4 theories which are not direct products, and 6 product theories. The toric code MTC has another version, which could also be called the toric code: it has $\theta_e = \theta_m = -1$. All F matrices are 1. The braidings $R_1^{ee} = R_1^{mm} = R_\epsilon^{em} = -1$, $R_\epsilon^{me} = 1$, and others are the same as the toric code. Another two are the $-S$ versions. The product theories are the products of the semion MTC and its complex

conjugate. There are 4 possible theories, but two of them are the same: semion × complex conjugate is the same as complex conjugate × semion. Hence there are 3 theories here. With the $-S$ versions, we have 6 product theories.

For the $\mathbb{Z}_4$ fusion rule, the Galois group action of the MTC listed above is $\mathbb{Z}_4$. Its actions give rise to 4 theories with $\theta_X = \theta_{X^*} = e^{\frac{m\pi i}{4}}$ for $m = 1, 3, 5, 7$. They all have the same F matrices. The $-S$ versions give a total of 8.

For the $(A_1, 3)$ fusion rule, this is the product of the semion fusion rule with the Fibonacci fusion rule. There are 4 product theories from semion, Fibonacci and their complex conjugates. These 4 theories are different, and the other 4 come from their $-S$ versions. Let us choose the product of the semion with the Fibonacci as a representative theory, then we have 4 anyons, $1, \varphi, \tau, s$, where τ is the Fibonacci anyon, and φ is the same as τ tensoring the semion s.

For the $(A_1, 7)_{\frac{1}{2}}$ fusion rule, all unitary MTCs are the ones listed in last subsection and those from the two symmetries $S \rightarrow -S$ and complex conjugate.

The analysis of the Fibonacci × Fibonacci fusion rule is the same as that of the semion × semion fusion rule.

6. Conjectures and Further Results

In this section we briefly discuss several conjectures concerning the structure and application of MTCs.

6.1. Fusion rules and the finiteness conjecture. Since topological phases of matter are discrete in the space of theories, therefore, MTCs, encoding the universal properties of topological phases of matter, should also be discrete.

It is conjectured [Wa]:

Conjecture 6.1. *If the rank of MTCs is fixed, then there are only finitely many equivalence classes of MTCs.*

By Ocneanu rigidity, this is equivalent to there are only finitely many modular fusion rules realizing by MTCs of a fixed rank.

Proposition 6.2. *There are only finitely many equivalence classes of unitary MTCs with total quantum order $D \leq c$, where c is any given universal constant.*

Proof. For a unitary rank=n MTC, all quantum dimensions $d_r \geq 1, r \in \mathcal{L}$. So $D \geq \sqrt{n}$. If $D \leq c$, then $n \leq c^2$. By Verlinde formula 2.3, we have $n_{i,j}^k = |\sum_{r=0}^{n-1} \frac{s_{ir} s_{jr} s_{kr}^*}{s_{0r}}| \leq D \sum_{r=0}^{n-1} \frac{1}{d_r} \leq nD \leq c^3$ for any i, j, k. Therefore, there are only finitely many possible fusion rules. By Ocneanu rigidity, there are only finitely many possible MTCs. $\square$

6.2. Topological qubit liquids and the fault-tolerance conjecture. Topological phases of matter are quantum liquids such as the electron liquids exhibiting the FQHE, whose topological properties emerged from microscopic degrees of freedom. This inspires the following discussion.

Let Δ be a triangulation of a closed surface Σ, Γ_Δ be its dual triangulation: vertices are centers of the triangles in Δ, and two vertices are connected by an edge if and only

if the corresponding triangles of Δ share an edge. The dual triangulation Γ_Δ of Δ is a celluation of Σ whose 1-skeleton is a tri-valent graph. It is well-known that any two triangulations of the same surface Σ can be transformed from one to the other by a finite sequence of two moves and their inverses: the subdivision of a triangle into 3 new triangles; and the diagonal flip of two adjacent triangles that share an edge (=the diagonal). Dualizing the triangulations into celluations, the two moves become the inflation of a vertex to a triangle and the F move.

Definition 6.3. (1) *Given an integer $k > 0$, a k-local, or just local, qubit model on (Σ, Γ_Δ) is a pair $(\mathcal{H}_\Delta, H_\Delta)$, where $\mathcal{H}_\Delta$ is the Hilbert space $\otimes_{e \in \Gamma_\Delta} \mathbb{C}^2$, and H_Δ is a k local Hamiltonian in the following sense: H_Δ is a sum of Hermitian operators of the form $id \otimes \cdots \otimes id \otimes O_k \otimes id \otimes \cdots \otimes id$, where O_k acts on $\leq k$ qubits.*
(2) *A modular functor V is realized by a topological qubit liquid if there is a sequence of triangulations $\{\Delta_i\}_{i=1}^\infty$ of Σ whose meshes $\to 0$ as $i \to \infty$, an integer k, and uniform local qubit models on $(\Sigma, \Gamma_{\Delta_i})$ such that*
   (i) *the groundstates manifold of each H_{Δ_i} is canonically isomorphic to the modular functor $V(\Sigma)$ as Hilbert spaces;*
   (ii) *the mapping class group acts as unitary transformations compatibly;*
   (iii) *there is a spectral gap in the following sense: if the eigenvalues of the Hamiltonians H_{Δ_i} are normalized such that $0 = \lambda_0^i < \lambda_1^i < \cdots$, then $\lambda_1^i \geq c$ for all i, where $c > 0$ is some universal constant.*

The scheme for the local qubit models should be independent of the geometry of the surface Σ, and have a uniform local description. The modular functor determines a unique topological inner product on $V(\Sigma)$. We require that the restricted inner products from $\mathcal{H}_{\Delta_i}$ to the groundstates of H_{Δ_i} agree with the topological inner product on $V(\Sigma)$. To identify the Hilbert space $\mathcal{H}_{\Delta_i}$ of one triangulation with another, we consider the two basic moves: F move and inflation of a vertex. The F move does not change the number of qubits, so the two Hilbert spaces $\mathcal{H}_{\Delta_i}$ have the same number of qubits. We require that the identification be an isometric. For the inflation of a vertex, the inflated celluation has 3 new qubits, so we need to choose a homothetic embedding with a universal homothecy constant.

The action of the mapping class group is defined as follows: consider the moduli space of all triangulations of Σ that two triangulations are equivalent if there dual graphs Γ_Δ are isomorphic as abstract graphs. By a sequence of diagonal flips, we can realize a Dehn twist. Each diagonal flip is an F move, and their composition is the unitary transformation associated to the Dehn twist.

Conjecture 6.4. (1) *Every doubled MTC $\mathcal{C}$ can be realized as a topological qubit liquid.*
(2) *The groundstates $V(\Sigma) \cong H_{\Delta_i} \subset \mathcal{H}_{\Delta_i}$ form an error-correction code for each triangulation Δ_i.*

6.3. Topological quantum compiling and the universality conjecture. Every unitary MTC gives rise to anyonic models of quantum computers as in [FKLW]. Quantum gates are realized by the braiding matrices of anyons, i.e. the afforded representations of the braid groups. Topological quantum compiling is the question of realizing desired unitary transformations by braiding matrices in quantum algorithms, in particular for those algorithms which are first described in the quantum circuit model such as Shor's famous factoring algorithm.

To choose a computational subspace, we will use the so-called conformal block basis for the Hilbert space $V(D^2, a_i; a_\infty)$ of a punctured disk, where a_∞ labels the boundary. Conformal block basis is in one-one correspondence to admissible labelings $m, n, \ldots, p$ of the internal edges of the following graph subject to the fusion rules at each trivalent vertex. As explained in Sect. 5.1, the tri-valent vertices also need to be indexed if multiplicities $n_{i,j}^k > 1$.
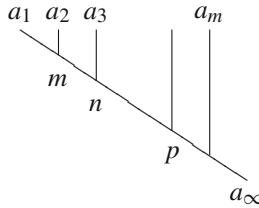
The braiding of two anyons a_i, a_{i+1} in a conformal block basis state is represented by stacking the braid on top of the above graph at $i, i+1$ positions.

Definition 6.5. *An MTC $\mathcal{C}$ has* **property F** *if for every object X in $\mathcal{C}$ and every m the representation ρ_X^m of $\mathcal{B}_m$ on $V(D^2, X, \cdots, X; a_\infty)$ factors over a finite group for any $a_\infty \in \mathcal{L}$.*

The following is conjectured by the first author (see [NR]):

Conjecture 6.6. *Let $\mathcal{C}$ be an MTC.*

(a) *If $\mathcal{C}$ is unitary, then it has property F if and only if $(d_i)^2 \in \mathbb{N}$ for each simple object X_i or, equivalently, if and only if the global quantum dimension $D^2 \in \mathbb{N}$.*
(b) *In general, $\mathcal{C}$ has property F if and only if $(\mathrm{FPdim}(X_i))^2 \in \mathbb{N}$ for each simple object X_i, where FPdim is the Frobenius-Perron dimension, i.e. the Frobenius-Perron eigenvalue of the fusion matrix N_i.*

The verification of this conjecture for UMTCs of rank≤ 4 is summarized in Table 4.

Theorem 6.7. *The following anyons are universal in the sense of [FKLW]:*
the Fibonacci anyon τ, the $(A_1, 5)_{\frac{1}{2}}$ anyons α, β, the $(A_1, 7)_{\frac{1}{2}}$ anyons α, ω, ρ, the two anyons φ, τ in $(A_1, 3)$ (see 5.4 for notation), and the two τ's in $Fib \times Fib$.

Table 4. Unitary prime MTCs rank≤ 4

Realization	PSL$(2, \mathbb{Z})$, Relations	Property F?	Universal Anyons
Vect$_\mathbb{C}$	1, $S = T = 1$	Yes	
$(A_1, 1)$	PSL$(2, 3)$, $T^4 = I$	Yes	
$(A_1, 3)_{\frac{1}{2}}$	PSL$(2, 5)$, $T^5 = I$	No	τ
$(A_2, 1)$	PSL$(2, 3)$, $T^3 = I$	Yes	
$(A_1, 2)$	PSL$(2, 8)$, $T^{16} = (T^2ST)^3 = I$	Yes	
$(A_1, 5)_{\frac{1}{2}}$	PSL$(2, 7)$, $T^7 = (T^4ST^4S)^2 = I$	No	α, β
$(A_3, 1)$	PSL$(2, 8)$, $T^8 = (T^2ST)^3 = I$	Yes	
$D(\mathbb{Z}_2)$	PSL$(2, 2)$, $T^2 = I$	Yes	
$(A_1, 7)_{\frac{1}{2}}$	PSL$(2, 9)$, $T^9 = (T^4ST^5S)^2 = I$	No	α, ω, ρ

Universal anyonic quantum computation can also be achieved with the anyon $\tau \times \tau$ in $Fib \times Fib$, but images of the representations of the braid groups from this anyon are not as large as possible.

Anyons that correspond to $\varphi, \tau, \alpha, \beta, \omega, \rho$ in other versions are also universal.

Proof. We deduce the proof from [FLW2,LRW,LWa].

Universality of φ and τ is given in [FLW2]. The anyons α are both the fundamental representations of (A_1, k) up to abelian anyons. The universality of fundamental representation anyons are established in [FLW2]. Therefore, both α's are universal.

To prove that β, ω, ρ are universal, we first show that their braid representations are irreducible. By inspecting the braiding eigenvalues in Section 5.3, we see that they satisfy the conditions of [TW][Lemma 5.5] [HRW][Proposition 6.1]. It follows that the braid representations are irreducible. Universality now can be proved following [FLW2 or LRW]. □

Appendix. Non-Self Dual Rank $\leq$ 4 MTCs with S. Belinschi

Every rank=1, 2 MTC is self-dual, so we will start with rank=3.

A.1. Nonselfdual rank=3. The three labels will be 0, 1, 2 such that $\hat{0} = 0$, $\hat{1} = 2$, $\hat{2} = 1$. The modular $\tilde{S}$ matrix is of the form:

$$\begin{pmatrix} 1 & d & d \\ d & x & \bar{x} \\ d & \bar{x} & x \end{pmatrix}.$$

$\tilde{s}_{22} = \tilde{s}_{11}, \tilde{s}_{12} = \overline{\tilde{s}_{11}}$ follows from $\tilde{s}_{\hat{i}, j} = \overline{\tilde{s}_{i, j}}$. Unitarity of S implies

$$1 + d^2 = 2|x|^2, \tag{A.1}$$
$$d^2 + x^2 + \bar{x}^2 = 0, \tag{A.2}$$
$$1 + x + \bar{x} = 0. \tag{A.3}$$

The fusion matrix N_1 has eigenvalues $d, \frac{x}{d}, \frac{\bar{x}}{d}$. Their sum $d + \frac{x+\bar{x}}{d} = d - \frac{1}{d}$ is an integer. Their product $\frac{|x|^2}{d} = \frac{1+d^2}{2d} = \frac{1}{2}(\frac{1}{d} + d)$ is also an integer. Therefore, d is an integral multiple of $\frac{1}{2}$, so d is an integer.

Let θ be the twist of label 1, hence of label 2. Using identity (2.2), we get

$$1 - 2d^2 + \theta + \theta^{-1} = 0. \tag{A.4}$$

Therefore, $2d^2 \leq 3$. Since $d \neq 0$, the only possible integers are $d^2 = 1$, hence $|x| = 1$. Then $1 + x + \bar{x} = 0$ leads to $x = e^{\pm \frac{2\pi i}{3}}$.

A.2. Nonselfdual rank=4. Now we turn to the non-self dual rank=4 case. The 4 labels will be denoted as 1, Y, X, X^*, where Y is self dual and X, X^* dual to each other. Taking into account all symmetries among $n_{i,j}^k$, we can write the non-trivial fusion matrices as:

$$N_Y = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & n_1 & n_2 & n_2 \\ 0 & n_2 & n_3 & n_4 \\ 0 & n_2 & n_4 & n_3 \end{pmatrix};$$

$$N_X = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & n_2 & n_3 & n_4 \\ 0 & n_4 & n_5 & n_6 \\ 1 & n_3 & n_7 & n_7 \end{pmatrix};$$

$$N_{X^*} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & n_2 & n_4 & n_3 \\ 1 & n_3 & n_7 & n_7 \\ 0 & n_4 & n_6 & n_5 \end{pmatrix}.$$

The modular $\tilde{S}$ matrix is of the form:

$$\tilde{S} = \begin{pmatrix} 1 & d_1 & d_2 & d_2 \\ d_1 & x & y & y \\ d_2 & y & z & \bar{z} \\ d_2 & y & \bar{z} & z \end{pmatrix}, \text{ where } x, y \text{ are real, and } z \text{ is not real.}$$

We will work on unitary modular symbols, so $d_1 \geq 1$, $d_2 \geq 1$. The argument for the general case should have only minor changes.

The identity $N_X N_Y = N_Y N_X$ leads to the identities:

$$1 + n_1 n_3 + n_2(n_5 + n_7) = n_2^2 + n_3^2 + n_4^2, \tag{A.5}$$

$$n_1 n_4 + n_2(n_6 + n_7) = n_2^2 + 2n_3 n_4, \tag{A.6}$$

$$n_1 n_4 + n_2(n_5 + n_6) = n_2^2 + 2n_3 n_4. \tag{A.7}$$

$N_Y N_{X^*} = N_{X^*} N_Y$ gives no new identities. But $N_X N_{X^*} = N_{X^*} N_X$ gives us:

$$n_2 n_4 + n_4 n_6 = n_2 n_3 + n_4 n_5, \tag{A.8}$$

$$n_5 = n_7, \tag{A.9}$$

$$n_4^2 + n_6^2 = 1 + n_3^2 + n_7^2. \tag{A.10}$$

Case 1. $n_4 = 0$. If $n_4 = 0$, then $n_2 n_3 = 0$. First if $n_2 = 0$, then $1 + n_1 n_3 = n_3^2$ which implies $n_3 = 1$, $n_1 = 0$. It follows that $n_1 = n_2 = n_4 = 0$, $n_3 = 1$. This leads to $n_6^2 = 2 + n_7^2$ which has no solutions. Secondly if $n_3 = 0$, then $n_6^2 = 1 + n_7^2$ which implies $n_6 = 1$, $n_7 = 0$. Hence $n_3 = n_4 = n_5 = n_7 = 0$, $n_6 = 1$. This leads to $n_2 = 1$, and n_1 is arbitrary. To rule out this case, notice that the labels 1, X, X^* have exactly the same fusion rules as the rank=3 non-self dual theory. Therefore, it is a pre-modular category with the same fusion rules, which is necessarily modular by [Br]: Suppose otherwise, then $(d_2, z, \bar{z})$ would be a d_2 times $(1, d_2, d_2)$ as vectors, contradicting z is not real. It follows $d_2 = 1$, $z = \omega$ for some $\omega^3 = 1$. Comparing the squared lengths of row 1 and row 3 of the $\tilde{S}$ matrix, we see that $y^2 = d_1^2$. Also note that $d_1^2 = 3 + n_1 d_1$. Equality of the squared lengths of row 1 and row 2 implies $x^2 + 2d_1^2 = 3$. Since x is real, this does not hold if $d_1 > 0$.

Case 2. $n_4 \neq 0$. If $n_2 = 0$, then $n_1 = 2n_3$, $1 + n_1 n_3 = n_3^2 + n_4^2$. Hence $1 + n_3^2 = n_4^2$ which implies $n_4 = 1$, $n_3 = 0$. So we have $n_1 = n_2 = n_3 = 0$, $n_4 = 1$, $n_5 = n_6 = n_7$. The labels 1, Y form a subcategory the same as the $\mathbb{Z}_2$ theory, hence $d_1^2 = 1$, $x^2 = 1$. If $x = -1$, then $y = 0$, and $d_1 d_2 = 0$ which is a contradiction. If $x = 1$, then $y^2 = d_2^2$.

So $d_2^2 = d_1^2 = 1$. Using $d_2^2 = 1 + n_3 d_1 + 2n_5 d_2$ below, we see that n_3, n_5, hence $n_6 = n_7 = 0$. So we have $n_1 = n_2 = n_3 = n_5 = n_6 = n_7 = 0, n_4 = 1$, which is the $\mathbb{Z}_4$ fusion rule.

Suppose $n_4 \neq 0, n_2 \neq 0$.
The fusion rules in Table 4 gives us the following identities:

$$d_1^2 = 1 + n_1 d_1 + 2n_2 d_2, \tag{A.11}$$
$$d_1 d_2 = n_2 d_1 + (n_3 + n_4)d_2, \tag{A.12}$$
$$d_2^2 = n_4 d_1 + (n_5 + n_6)d_2, \tag{A.13}$$
$$d_2^2 = 1 + n_3 d_1 + 2n_5 d_2. \tag{A.14}$$

Combining equations, we have

$$(n_4 - n_3)d_1 + (n_6 - n_5)d_2 = 1. \tag{A.15}$$

If $n_4 = n_3$, then $n_6 = 1 + n_7^2$ which implies $n_6 = 1, n_7 = 0$. Hence $n_5 = 0$. By Eq. (A.15), $n_5 = n_6$ which is a contradiction.
If $n_5 = n_6$, then $n_4^2 = 1 + n_3^2$ which implies $n_3 = 0, n_4 = 1$. Solving all equations, we get $n_1 = n_2 = n_3 = 0, n_4 = 1, n_5 = n_6 = n_7$, which is the $\mathbb{Z}_4$ fusion rule.
So we may assume from now on $n_2 \neq 0, n_4 \neq 0, n_4 \neq n_3, n_5 \neq n_6$. By Eq. (A.8), we have

$$n_4(n_5 - n_6) = n_2(n_4 - n_3). \tag{A.16}$$

Hence we have

$$d_2 = \frac{n_4}{n_2}d_1 - \frac{n_4}{n_2(n_4 - n_3)}. \tag{A.17}$$

Plugging into (A.15) and simplifying, we have

$$d_1^2 = (n_1 + 2n_4)d_1 - \frac{n_3}{n_4 - n_3}. \tag{A.18}$$

The orthogonality of $\tilde{S}$ gives us:

$$x^2 + 2y^2 = 1 + 2d_2^2, \tag{A.19}$$
$$y^2 + 2|z|^2 = 1 + d_1^2 + d_2^2, \tag{A.20}$$
$$(1 + x)d_1 + 2yd_2 = 0, \tag{A.21}$$
$$yd_1 + (1 + z + \bar{z})d_2 = 0, \tag{A.22}$$
$$d_1 d_2 + (x + z + \bar{z})y = 0, \tag{A.23}$$
$$d_2^2 + y^2 + z^2 + \bar{z}^2 = 0. \tag{A.24}$$

Note that y cannot be 0. Suppose otherwise, then $x = -1$, so $d_2 = 0$, a contradiction. The eigenvalues of N_Y are $d_1, \frac{x}{d_1}, \frac{y}{d_2}, \frac{y}{d_2}$. Their sum $d_1 + \frac{x}{d_1} - \frac{(1+x)d_1}{d_2^2} = d_1 - \frac{d_1}{d_2^2} + (\frac{1}{d_1} - \frac{d_1}{d_2^2})x$ is an integer. The eigenvalues of N_X are $d_2, \frac{y}{d_1}, \frac{z}{d_2}, \frac{\bar{z}}{d_2}$. Their sum $d_2 + \frac{y}{d_1} + \frac{z+\bar{z}}{d_2}$ is an integer.

If $\frac{1}{d_1} - \frac{d_1}{d_2^2} = 0$, then $d_1^2 = d_2^2$. By Eq. (A.12), $\pm d_1 = n_2 + n_3 + n_4$, then d_1, d_2 are integers. But the sum of the eigenvalues of N_Y $d_1 - \frac{1}{d_1}$ is also an integer, so $d_1 = \pm 1$. It follows that $\pm 1 = n_2 + n_3 + n_4$, but n_2, n_4 are both $\neq 0$, a contradiction.

If $\frac{1}{d_1} - \frac{d_1}{d_2^2} \neq 0$, then x and subsequently all $y, z + \bar{z}, |z|^2$ are in $\mathbb{Q}(d_1, d_2)$. So all $x, y, z + \bar{z}, |z|^2, z^2 + \bar{z}^2$ are in $\mathbb{Q}(d_1, d_2)$. By Eq. A.15, $\mathbb{Q}(d_1, d_2)$ is a degree≤ 2 Galois extension of $\mathbb{Q}$. Therefore, the Galois group of the characteristic polynomial $p_1(t)$ of N_Y is either trivial or $\mathbb{Z}_2$. If it is trivial, then all eigenvalues $d_1, \frac{x}{d_1}, \frac{y}{d_2}, \frac{y}{d_2}$ and d_2 are integers. So d_1, d_2, x, y are all integers.

From the unitary assumption, $d_1, d_2 \geq 1$. Since $\frac{x}{d_1}, \frac{y}{d_2}$ are integers, $|x| \geq d_1, |y| \geq d_2$. Equation (A.19) implies $x = \pm 1, y = \pm d_2$. Since $\frac{x}{d_1}$ is an integer, $|x| = d_1 = 1$. Then $2yd_2 = -2$ implies $d_2 = 1$, contradicting $\frac{1}{d_1} - \frac{d_1}{d_2^2} \neq 0$.

Therefore the Galois group of $p_1(t)$ is $\mathbb{Z}_2$. Since $p_1(t)$ has a pair of repeated roots, then $p_1(t)$ is $(t - m)^2 q_1(t)$ for some irreducible quadratics $q_1(t)$ and integer m or $(q_1(t))^2$. Assume $q_1(t) = t^2 + bt + c$, where b, c are integers. Note that d_1 has to be an irrational root of $p_1(t)$. If $p_1(t)$ has integral roots m, then $\frac{y}{d_2} = m$, so $y^2 \geq d_2^2$. $x = d_1 \frac{x}{d_1} = c$ implies $|x| \geq 1$. By Eq. (A.19), $y^2 \geq d_2^2$ implies $x^2 \leq 1$, hence $|x| = 1, y^2 = d_2^2$. It follows from Eq. (A.21) that $d_1 = d_2^2$. By Eq. (A.13), $(n_4 - 1)d_1 + (n_5 + n_6)d_2 = 0$. Since $n_4 \geq 1$, it follows that $n_4 = 1, n_5 = n_6 = 0$, contradicting $n_5 \neq n_6$.

Hence $p_1(t) = q_1(t)^2$, and $d_1 = \frac{x}{d_1}$, i.e. $x = d_1^2 \geq 1$, and $y^2 \leq d_2^2$. So the roots of $p_1(t)$ are $d_1, d_1, \frac{y}{d_2}, \frac{y}{d_2}$. Then $d_1 + \frac{y}{d_2}$ and $\frac{d_1 y}{d_2}$ are both integers. By Eqs. A.22, A.23, $\frac{d_1 d_2}{y} + x = -(z + \bar{z}) = \frac{y d_1}{d_2} + 1$ is an integer. On the other hand, $\frac{d_1 d_2}{y} + x = x(\frac{d_2}{d_1 y} + 1)$, so $x = d_1^2$ would be a rational number s if $\frac{d_2}{d_1 y} + 1 \neq 0$. Then $d_1 = \sqrt{s}$, which is also $\frac{-b \pm \sqrt{b^2 - 4c}}{2}$, but not a rational number, hence $b = 0$, a contradiction. If $\frac{d_2}{d_1 y} + 1 = 0$, then $y = -\frac{d_2}{d_1}$. Substituting this and $x = d_1^2$ into Eq. (A.21), we get $d_1^2 = 2\frac{d_2^2}{d_1^2} - 1$. By Eq. (A.15), $\frac{d_2}{d_1} \in \mathbb{Q}$, hence d_1^2 would be a rational number s again, a contradiction.

Putting everything together, we have the only desired modular $\tilde{S}$ matrix.

References

[Ba] Bantay, P.: The Frobenius-Schur indicator in conformal field theory. Phys. Lett. B **394**(1–2), 87–88 (1997)

[BM] Belov, D., Moore, G.: *Classification of spin abelian Chern-Simons theories.* http://arxiv.org/abs/hep-th/0505235v1, 2005

[BK] Bakalov, B., Kirillov, A. Jr.: *Lectures on Tensor Categories and Modular Functors.* University Lecture Series, Vol. **21**, Providence, RI: Amer. Math. Soc., 2001

[Br] Bruguières, A.: Catégories prémodulaires, modularisations et invariants des variétés de dimension 3. (French) Math. Ann. **316**(2), 215–236 (2000)

[CG] Coste, A., Gannon, T.: Remarks on Galois symmetry in rational conformal field theories. Phys. Lett. B **323**(3–4), 316–321 (1994)

[CP] Caselle, M., Ponzano, G.: Analyticity, modular invariance and the classification of three operator fusion algebras. Phys. Lett. B **242**(1), 52–58 (1990)

[CZ]   Cuntz, M.: Integral modular data and congruences. J. Alg. Comb. **29**(3), 357–387 (2009)
[dBG]   de Boer, J., Goeree, J.: Markov traces and II_1 factors in conformal field theory. Commun. Math. Phys. **139**(2), 267–304 (1991)
[DFNSS]   Das Sarma, S., Freedman, M., Nayak, C., Simon, S.H., Stern, A.: Non-Abelian Anyons and Topological Quantum Computation. Rev. Mod. Phys. **80**, 1083 (2008)
[DW]   Dijkgraaf, R., Witten, E.: Topological gauge theories and group cohomology. Commun. Math. Phys. **129**(2), 393–429 (1990)
[ENO]   Etingof, P., Nikshych, D., Ostrik, V.: On fusion categories. Ann. of Math. (2) **162**(2), 581–642 (2005)
[EK]   Evans, D., Kawahigashi, Y.: *Quantum Symmetries on Operator Algebras*. Oxford Mathematical Monographs. New York: Oxford Science Publications. The Clarendon Press/Oxford University Press, 1998
[F]   Freedman, M.H.: P/NP, and the quantum field computer. Proc. Natl. Acad. Sci. USA **95**(1), 98–101 (1998)
[FKLW]   Freedman, M., Kitaev, A., Larsen, M., Wang, Z.: Topological quantum computation. Bull. Amer. Math. Soc. (N.S.) **40**(1), 31–38 (2003)
[FKW]   Freedman, M.H., Kitaev, A., Wang, Z.: Simulation of topological field theories by quantum computers. Commun. Math. Phys. **227**(3), 587–603 (2002)
[FLW1]   Freedman, M.H., Larsen, M.J., Wang, Z.: A modular functor which is universal for quantum computation. Commun. Math. Phys. **227**(3), 605–622 (2002)
[FLW2]   Freedman, M.H., Larsen, M.J., Wang, Z.: The two-eigenvalue problem and density of Jones representation of braid groups. Commun. Math. Phys. **228**, 177–199 (2002)
[FW]   Freedman, M.H., Wang, Z.: Large quantum Fourier transforms are never exactly realized by braiding conformal blocks. Phys. Rev. A (3) **75**(3), 032322 (2007)
[FQ]   Freed, D., Quinn, F.: Chern-Simons theory with finite gauge group. Commun. Math. Phys. **156**(3), 435–472 (1993)
[FK]   Frohlich, J., Kerler, T.: *Quantum Groups, Quantum Categories and Quantum Field Theory*. Lecture Notes in Mathematics, **1542**. Berlin: Springer-Verlag, 1993
[FNTW]   Fradkin, E., Nayak, C., Tsvelik, A., Wilczek, F.: A Chern-Simons effective field theory for the Pfaffian quantum Hall state. Nucl. Phys. **B516**, 704–718 (1998)
[FTL]   Feiguin, A., Trebst, S., Ludwig, A.W.W., Troyer, M., Kitaev, A., Wang, Z., Freedman, M.: Interacting anyons in topological quantum liquids: The golden chain. Phys. Rev. Lett. **98**, 160409 (2007)
[G]   Gannon, T.: Modular data: the algebraic combinatorics of conformal field theory. J. Alg. Comb. **22**(2), 211–250 (2005)
[GK]   Gepner, D., Kapustin, A.: On the classification of fusion rings. Phys. Lett. B **349**(1–2), 71–75 (1995)
[HH]   Hagge, T., Hong, S.: *Some non-braided fusion categories of rank 3*. http://arxiv.org/abs/0704. 0208v2[math.GT], 2007
[HRW]   Hong, S.-M., Rowell, E.C., Wang, Z.: On exotic modular tensor categories. Commun. Contemp. Math. **10**(Suppl. 1), 1049–1074 (2008)
[Ki1]   Kitaev, A.: Fault-tolerant quantum computation by anyons. Ann. Physics **303**(1), 2–30 (2003)
[Ki2]   Kitaev, A.: Anyons in an exactly solved model and beyond. Ann. Physics **321**(1), 2–111 (2006)
[KL]   Kauffman, L., Lins, S.: *Temperley-Lieb Recoupling Theory and Invariants of 3-Manifolds*. Ann. Math. Studies, **134**. Princeton, NJ: Princeton University Press, 1994
[KW]   Kazhdan, D., Wenzl, H.: Reconstructing monoidal categories. In: I. M. Gelfand Seminar, Adv. Soviet Math. **16**, Part 2, Providence, RI: Amer. Math. Soc., 1993, pp. 111–136
[LRW]   Larsen, M.J., Rowell, E.C., Wang, Z.: The N-eigenvalue problem and two applications. Int. Math. Res. Not. **2005**(64), 3987–4018 (2005)
[LWa]   Larsen, M., Wang, Z.: Density of the SO(3) TQFT representation of mapping class groups. Commun. Math. Phys. **260**(3), 641–658 (2005)
[LWe]   Levin, M., Wen, X.-G.: String-net condensation: A physical mechanism for topological phases. Phys. Rev. **B71**, 045110 (2005)
[Ma]   Manoliu, M.: Abelian Chern-Simons theory. I. a topological quantum field theory. J. Math. Phys. **39**(1), 170–206 (1998)
[M1]   Müger, M.: From subfactor to categories and topology, II. J. Pure Appl. Alg. **180**(1–2), 159–219 (2003)
[M2]   Müger, M.: On the structure of modular categories. Proc. London Math. Soc. (3) **87**(2), 291–308 (2003)
[MR]   Moore, G., Read, N.: Nonabelions in the fractional quantum Hall effect. Nucl. Phys. B **360**(2–3), 362–396 (1991)

[MS1]   Moore, G., Seiberg, N.: *Lectures on RCFT*. Superstrings '89 (Trieste, 1989), River Edge, NJ:
          World Sci. Publ., 1990 pp. 1–129
[MS2]   Moore, G., Seiberg, N.: Classical and quantum conformal field theory. Commun. Math.
          Phys. **123**(2), 177–254 (1989)
[NR]   Naidu, D., Rowell, E.C.: *A finiteness property for braided fusion categories*. http://arxiv.org/abs/
          0903.4157v1[math.QA], 2009
[O1]   Ostrik, V.: Fusion categories of rank 2. Math. Res. Lett. **10**(2–3), 177–183 (2003)
[O2]   Ostrik, V.: Pre-modular categories of rank 3. Mosc. Math. J. **8**(1), 111–118 (2008)
[P]   Preskill, J.: Chapter 9 at http://www.theory.caltech.edu/~preskill/ph229/
[Ro1]   Rowell, E.C.: From quantum groups to unitary modular tensor categories. In: Contemp.
          Math. **413**, 215–230 (2006)
[Tu]   Turaev, V.: *Quantum Invariants of Knots and 3-Manifolds*. De Gruyter Studies in Mathematics,
          Berlin: Walter de Gruyter, 1994
[TV]   Turaev, V., Viro, O.: State sum invariants of 3-manifolds and quantum $6j$-symbols. Topology
          31(4), 865–902 (1992)
[TW]   Tuba, I., Wenzl, H.: On braided tensor categories of type BCD. J. Reine Angew. Math. **581**, 31–69
          (2005)
[Wa]   Wang, Z.: Topologization of electron liquids with Chern-Simons theory and quantum computa-
          tion. In: *Differential Geometry and Physics*, Nankai Tracts Math., **10**, Hackensack, NJ: World
          Sci. Publ., 2006 pp. 106–120
[Wal]   Walker, K.: *On Witten's 3-manifold Invariants*. 1991 notes at http://canyon23.net/math/
[Wen]   Wen, X.-G.: Topological orders and edge excitations in fractional quantum Hall states. Adv. in
          Phys. **44**, 405 (1995)
[WW1]   Wen, X.-G., Wang, Z.: A classification of symmetric polynomials of infinite variables- a con-
          struction of Abelian and non-Abelian quantum Hall states. Phys. Rev. B **77**, 235108 (2008)
[WW2]   Wen, X.-G., Wang, Z.: Topological properties of Abelian and non-Abelian quantum Hall states
          from the pattern of zeros. Phys. Rev. B **78**, 155109 (2008)
[Wenz]   Wenzl, H.: C^* tensor categories from quantum groups. J. Amer. Math. Soc. **11**(2), 261–282 (1998)
[Wil]   Wilczek, F.: *Fractional Statistics and Anyon Superconductivity*, Singapore: World Scientific Pub.
          Co. Inc., 1990
[Witt]   Witten, E. (1989) The search for higher symmetry in string theory. In: *Physics and Mathematics
          of Strings*. Philos. Trans. Roy. Soc. London Ser. A **329**(1605), 349–357 (1989)