QUANTUM COMPUTING: A QUANTUM GROUP APPROACH

ZHENGHAN WANG

ABSTRACT. There is compelling theoretical evidence that quantum physics will change the face of information science. Exciting progress has been made during the last two decades towards the building of a large scale quantum computer. A quantum group approach stands out as a promising route to this holy grail, and provides hope that we may have quantum computers in our future.

1. QUANTUM GROUP AND QUANTUM COMPUTING

Working at Microsoft Station Q, I am interested in building a quantum computer by braiding non-abelian anyons [22]. The mathematical underpin of anyon theory is unitary modular tensor category theory—an abstraction of the representation theory of quantum groups [14] [22]. A quantum group commonly refers to a certain Hopf algebra such as a quasi-triangular one, though the terminology is used only loosely. I would like to advocate the use of a quantum group to mean a modular category. Modular categories are elaborate algebraic structures that arise in a variety of subjects: Hopf algebras, von Neumann algebras, topological quantum field theories (TQFTs), conformal field theories (CFTs), and topological phases of matter. They are quantum analogues of finite abelian groups in a sense that I will explain below. We could use unitary fusion categories to describe quantum symmetries of quantum phases of matter just as finite groups are used to describe symmetries of crystals.

Qubits are just the modern abstraction of a two-level quantum system and its composites. Theoretically, there is compelling evidence that quantum physics can change the face of information science: the BB84 private key protocol[1], Shor’s factoring algorithm[20], and Hastings’ additivity counterexamples[8]. But for the last two decades, the most interesting challenge has been to realize quantum computation in the real world. A key post-Shor idea is to use topology to protect...
quantum information—a revolutionary idea articulated by A. Kitaev as follows: “if a physical system were to have quantum topological (necessarily nonlocal) degrees of freedom, which were insensitive to local probes, then information contained in them would be automatically protected against errors caused by local interactions with the environment. This would be fault tolerance guaranteed by physics at the hardware level, with no further need for quantum error correction, i.e., topological protection.”[6][13]

Materials with such topological degrees of freedom are called topological phases of matter[17]. The prospect of utilizing topological phases of matter to build a quantum computer has been greatly enhanced by recent experimental progress. This approach to quantum computing at the triple juncture of mathematics, computer science, and physics is referred to as topological quantum computation (TQC). The low energy effective theories of topological phases of matter are TQFTs, and their algebraic data are modular categories. Therefore, unitary modular categories (UMCs) are algebraic models of anyons in topological phases of matter. TQC leads to new perspectives on TQFTs and modular categories.

2. Modular categories as finite abelian groups

A modular category $\mathcal{C}$ is a non-degenerate ribbon fusion category [5][2]. A ribbon fusion category is a fusion category with compatible braiding and pivotal structures. A practical way to describe such a complicated structure $\mathcal{C}$ is to use a representative set $\text{Irr}(\mathcal{C}) = \{X_i\}_{i \in I}$ of the isomorphism classes of simple objects of $\mathcal{C}$, and the various structures on $\text{Irr}(\mathcal{C})$. The finite index set $I$ of $\text{Irr}(\mathcal{C})$ is the isomorphism classes of simple objects of $\mathcal{C}$, and an element of $I$ will be called a label. The cardinality $|I|$ of the label set $I$ is called the rank of the modular category. It is important to keep in mind the difference between labels and the simple object representatives. To make an analogy with a finite group, we will think of each simple object $X_i$ as an analogue of a group element in the modular category $\mathcal{C}$. Then there will be a binary operation on $\text{Irr}(\mathcal{C})$ which satisfies the analogues of associativity, commutativity, and inverse of a group.

The binary operation on $\text{Irr}(\mathcal{C})$ is called the tensor product. Just as tensor products of irreps of algebraic structures such as Hopf algebras, the tensor product $X_i \otimes X_j$ is not necessarily an irrep, so it could decompose into a direct sum $\bigoplus_{k=1}^{[I]} N_{i,j,k}^k X_k$, i.e., $X_i \otimes X_j \cong \bigoplus_{k=1}^{[I]} N_{i,j,k}^k X_k$ for some non-negative integers $N_{i,j,k}^k$ (called multiplicities). This is some
kind of quantum multiplication as the outcome is a superposition. Actually the outcomes \{X_k\} are endowed with an intrinsic probability distribution related to the quantum dimensions of the simple objects.

The associativities between \((X_i \otimes X_j) \otimes X_k\) and \(X_i \otimes (X_j \otimes X_k)\) are weakened to be functorial isomorphisms that satisfy the pentagon axioms.

The dual \(X_i^*\) of \(X_i\) is quantum analogue of an inverse. As such we would only require that the tensor unit \(1\) appears in \(X_i \otimes X_i^*\) as a sub-object.

Finally, the commutativity of \(X_i \otimes X_j\) and \(X_j \otimes X_i\) is relaxed to be a functorial isomorphism that satisfies the hexagon axioms.

There is a very convenient picture calculus for a modular category. Basically, the axioms of a ribbon fusion category is to define topological invariants of colored braided trivalent framed graphs in the plane. In particular, we have invariants of colored framed links.

Important numerical data for a modular category \(\mathcal{C}\) are the fusion multiplies \(\{N_{i,j,k}\}_{i,j,k} \in I\), the \(S\)-matrix and \(T\)-matrix. The fusion multiplies are organized into matrices \(N_i, i \in I\) such that \((N_i)_{j,k} = N_{i,j}^k\). The unnormalized \(\tilde{S} = (S_{ij})\)-matrix consists of link invariants of the colored Hopf link: \(S_{ij}\) is the link invariant of the Hopf link with the two components colored by \(X_i\) and \(X_j\). We always identify \(I\) with \(\{0, 1, ..., |I| - 1\}\), and assume \(X_0\) is the tensor unit \(1\). The \(T\)-matrix \(T\) is diagonal with the \(i\)-th diagonal entry equal to the twist \(\theta_i\) of \(X_i\). The first row of the \(\tilde{S}\) matrix consists of the invariants of the unknot colored by \(X_i\), denoted as \(d_i\), called the quantum dimension of the simple object \(X_i\). Let \(D = \sqrt{\sum_{i \in I} d_i^2}, p_{\pm} = \sum_{i \in I} \theta_i^{\pm} d_i^2\). Then an important identity for a modular category is:

\[p_+ p_- = D^2.\]

The \(S\)-matrix \(S\) is \(\frac{1}{p} \tilde{S}\), and \(S, T\) together leads to a projective representation of the modular group \(SL(2, \mathbb{Z})\).

Any finite abelian group \(G\) can be endowed with modular category structures in many different ways so that \(G\) becomes the \(\text{Irr}(\mathcal{C})\)'s. One way to do it is as follows: choose an \(n \times n\) even integral matrix \(B\) so that the cokernel of the map \(B : \mathbb{Z}^n \to \mathbb{Z}^n\) is isomorphic to \(G\), i.e., \(\mathbb{Z}^n/\text{Im}(B) \cong G\). Each element \(g \in G\) can be identified as an equivalence class of vectors \(v_g \in \mathbb{Q}^n\) such that \(Bv_g \in \mathbb{Z}^n\). Two such \(v_g\)'s are equivalent if their difference is in \(\mathbb{Z}^n\). Then there is a modular category \(G_B\) with all \(d_i = 1\), fusion rules as \(G\), and \(\tilde{S}\)-matrix \(S_{ij} = e^{2\pi \sqrt{-1} < v_{g_i}, v_{g_j} >_B}, \theta_i = e^{\pi \sqrt{-1} < v_{g_i}, v_{g_i} >_B}\), where \(< v, w >_B = v^t B w\).
It is obvious that for a fixed order, there exist only finitely many groups. The analogous statement for modular categories would be for a fixed rank, there are only finitely many equivalence classes of modular categories\cite{4}. This rank finiteness property has been proved recently. This fundamental theorem implies that modular categories are amenable to a classification, especially the low rank cases. Modular categories up to rank 5 have been classified\cite{4}\cite{19}.

3. MODULAR CATEGORIES AS TOPOLOGICAL PHASES OF MATTER

Solid, liquid, and gas are all familiar states of matter. But by a more refined classification, each state consists of many different phases of matter. For example, within the crystalline solid state, there are many different crystals distinguished by their different lattice structures. All those phases are classical in the sense they depend crucially on the temperature. More mysterious and challenging to understand are quantum phases of matter: phases of matter at zero temperature (in reality very close to zero). Quantum phases of matter whose low energy physics can be modeled well by TQFTs are called topological phases of matter. There are two classes of topological phases of matter in real materials: two dimensional electron systems that exhibit the fractional quantum Hall effect (FQHE), and topological insulators and superconductors. The universal properties of those materials can be modeled well by TQFTs, and their variations—symmetry enriched TQFTs.

Traditionally, phases of matter are classified by classical symmetries modeled by groups. Quantum phases of matter cannot be fit into this Landau paradigm. Intensive effort in physics right now is to develop a post-Landau paradigm to classify quantum phases of matter. The well-studied classes of quantum phases of matter are topological phases of matter. To characterize topological phases of matter, we focus on both the ground states and first excited states. The algebraic models of elementary excitations of the topological phases are unitary modular categories (UMCs). If a classical symmetry modeled by a group $G$ is also present, then the UMC is $G$-graded. An interesting example is the trivial case with symmetry including the topological insulators discovered in the last few years—symmetry protect topological phases of matter.

Anyons are localized quantum fields. The mathematical model of an anyon under UMCs is a simple object $X$ in a UMC, and in picture calculus, described as a small arrow. Therefore its world line in $\mathbb{R}^3$ is
a ribbon. The isomorphism class $x$ of an anyon $X$ is called the anyon type of $X$, or the anyonic charge.

A dictionary of terminologies between anyon theory and UMC theory is given in the following table.

| $\text{UMC}$                  | $\text{Anyonic system}$                  |
|-------------------------------|-----------------------------------------|
| simple object                 | anyon                                   |
| label                         | anyon type or anyonic charge            |
| tensor product                | fusion rules                            |
| fusion rules                  | fusion rules                            |
| triangular space $V_{ab}^c$ or $V_{ac}^b$ | fusion/splitting space                 |
| dual                          | antiparticle                            |
| birth/death                   | creation/annihilation                    |
| mapping class group representations | generalized anyon statistics           |
| nonzero vector in $V(Y)$      | ground state vector                     |
| unitary $F$-matrices           | recoupling rules                        |
| twist $\theta_x = e^{2\pi i x}$ | topological spin                       |
| morphism                      | physical process or operator            |
| colored braided framed trivalent graphs | anyon trajectories                 |
| quantum invariants            | topological amplitudes                  |

**Table 1**

A UMC leads to an Atiyah-Segal type unitary TQFT[21]. An $(n+1)$-Atiyah-Segal-type TQFT is a symmetric monoidal functor from the $(n+1)$-bordism category $\text{Bord}(n+1)$ of $n$ and $n+1$-manifolds to the category of finitely dimensional vector spaces. An important question is when such a TQFT has a Hamiltonian realization on triangulations such as the quantum double of finite groups and Turaev-Viro type $(2+1)$-TQFTs[13][15].

4. **Modular categories as anyonic quantum computers**

Given $n$ anyons of type $x$ in a disk $D^2$, their ground state degeneracy $\dim(V(D,x,\cdots,x))$ has the asymptotic growth rate $d_x$—the quantum dimension of $x$. An anyon $X$ with $d_X = 1$ is called an abelian anyon, and an anyon with $d_X > 1$ an non-abelian anyon.

Given a non-abelian anyon of type $x$, we can construct an anyonic quantum computation model as follows: choose $V_{n,x}^a$ as the computational subspace—the Hilbert space of $n$ anyons of type $x$ and boundary label $a$—the total anyonic charge.
To simulate a traditional quantum circuit $U_L : (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes n}$ we need to find a braid $b$ making the square commute, where $\rho(b)$ is the braid matrix and $\iota$ is an efficient embedding of the $n$-qubit space $(\mathbb{C}^2)^{\otimes n}$ into the ground states $V_{n,x}^a$. This is rarely achievable. Therefore we seek $b$ making the square commute up to arbitrary precision. To achieve universality for quantum computation, we need to implement a universal gate set of unitary matrices. Then universality for anyonic quantum computing becomes the question: can we find braids $b$ whose $\rho(b)$’s approximate a universal gate set efficiently to arbitrary precision? For non-abelian anyons, since the Hilbert spaces always grow exponentially, universality is usually guaranteed if the braid group representations afforded by the UMC have a dense image in the special unitary groups $\text{SU}(V_{n,x}^a)$.

4.0.1. Braiding universal anyons. To simulate the standard quantum circuit model with braiding alone, we choose a non-abelian anyon type $x$ and use $m$ and $n$ anyons respectively to encode one and two qubits. If the braid group representations $B_m \rightarrow \text{SU}(V_{m,x}^a)$ and $B_n \rightarrow \text{SU}(V_{n,x}^b)$ are independently dense for all anyon types $a, b$, then the anyonic quantum computing model is universal. Anyon with such properties will be called braiding universal. An example of a braiding universal anyon is the Fibonacci anyon $\tau$.

4.0.2. Resource assisted universal anyons. It is conjectured that anyons with quantum dimensions $d_x^2 \notin \mathbb{Z}$ are essentially braiding universal. But current experimentally accessible anyons are those $d_x^2 \in \mathbb{Z}$. An example of such anyons is the Ising anyon $\sigma$ with $d_\sigma = \sqrt{2}$. More examples are the metaplectic anyons[9]. It is conjectured that such anyons always lead to representations of the braid groups with finite images, hence not braiding universal[18]. Therefore, to obtain a universal braiding gate set, we need to supplement the braiding with other gates such as measurement, magic state distillation, ... We will call an anyon $R$-assisted universal if the braidings supplemented with the resource $R$ give rise to a universal gate set. For example, the Ising anyon is (magic-state-distillation)-assisted universal[3].
5. Majorana physics and its realization

At the writing, we are the closest to detecting and harnessing Majoranas. Majoranas mean various things in the literature, and sometimes are very misleading. We will distinguish between Majorana fermions from Majorana zero modes. By Majorana fermions, we will mean abelian anyons with twist \( \theta = -1 \). Therefore, Majorana fermions are never non-abelian. An example of a Majorana fermion is the \( \psi \) particle in the Ising theory. By Majorana zero modes, we will mean the zero modes \( \{ \sum_\alpha c_\alpha | \psi_\alpha > \} \) obtained from the Majorana algebras \( M_n \) through the state-operator correspondence \( \gamma = \sum_\alpha | \psi_\alpha > < \psi_\alpha | \). In the Ising theory, the ground state manifolds of many Ising anyons \( \sigma \)’s consist of Majorana zero modes. However, Majorana zero modes can arise without the presence of Ising anyons.

The Majorana algebra \( M_n \) is generated by the operators \( \{ \gamma_i \} \), \( i = 1, \cdots, n-1 \) such that \( \gamma_i^\dagger = \gamma_i \), \( \{ \gamma_i, \gamma_j \} = 2\delta_{ij} \). \( M_n \) supports a representation \( \rho_{M_n} \) of the braid group \( B_n \) by sending the braid generator \( \sigma_i \) to an automorphism \( \rho_{M_n}(\sigma_i) = \frac{1}{\sqrt{2}}(1 - \gamma_i \gamma_{i+1}) \) of the Majorana zero modes:

\[
\rho_{M_n}(\sigma_i)\gamma = \frac{1}{\sqrt{2}}(1 - \gamma_i \gamma_{i+1}) \cdot \gamma \cdot \frac{1}{\sqrt{2}}(1 - \gamma_i \gamma_{i+1})^\dagger,
\]

for any \( \gamma \in M_n \).

It is easy to check:

\[
\begin{cases}
\rho_{M_n}(\sigma_i)\rho_{M_n}(\sigma_i)^\dagger = \text{Id}, \\
\rho_{M_n}(\sigma_i)\gamma_i = \gamma_{i+1}, \\
\rho_{M_n}(\sigma_i)\gamma_{i+1} = -\gamma_i, \\
\rho_{M_n}(\sigma_i)\gamma_j = \gamma_j, \quad \text{if } j \neq i, i+1.
\end{cases}
\]

This projective braid group representation \( \rho_{M_n}(\sigma_i) = -\frac{1}{\sqrt{2}}(1 - \gamma_i \gamma_{i+1}) \) is essentially the Jones representation of the braid groups at the 4-th root of unity \( q = e^{\frac{2\pi i}{4}} \) because the Temperley-Lieb Jones algebra at \( q = e^{\frac{2\pi i}{4}} \) is the Majorana algebra \( M_n[11][22] \).

There are important experimental progress towards the confirmation of Majorana physics in real materials. Interferometry experiments for the FQH liquids at filling fraction \( \mu = \frac{5}{2} \) agree with the Ising physics[23], and nanowires experiments are consistent with Majorana zero modes[16].

Recently, a generalization of Majorana physics to metaplectic physics is proposed[9]. Potentially, metaplectic anyons can be used to perform universal quantum computation more easily than Majorana anyons.
6. Open problems and future directions

There are new problems in mathematics, physics, and computer science inspired by the quantum group approach to quantum computing. The classification of modular categories is both an interesting question in mathematics and physics. As beautiful mathematical structures, modular category theory could be regarded as quantum version of group theory. In physics, a classification is very beneficial to the identification of topological phases of matter\cite{10}.

As the theory of modular category reaches certain maturity, many new directions emerge. UMCs capture topological properties of bosonic physical systems in 2-spatial dimension. Three directions that we would like to explore are for fermion systems, for boson systems with group symmetries, and for 3-spatial dimension.

6.0.3. SPT and SET. Topological phases of matter can have conventional group symmetries $G$. Such topological phases of matter are called symmetry enriched topological (SET) phases. When the intrinsic topological order is trivial, SET is called symmetry protect topological (SPT) phase. Important examples of SPTs are topological insulators and topological superconductors. In 2-spatial dimension, SETs are described by $G$-equivariant TQFTs/modular categories. Classification of SETs then involves the interplay between group theory and modular category theory.

6.0.4. Fermion systems. Fermion systems share similar Hilbert space as bosonic spin systems, but the meaning of locality is different\cite{7}. A local Hamiltonian for a fermion system is actually non-local. Therefore, fermionic topological phases of matter are strictly richer than their bosonic counterparts.

6.0.5. (3+1)-TQFTs. Topological phases of matter behave differently in different spatial dimensions. In 1D, there are no intrinsic non-trivial topological order. In 2D, there is a richness of topological orders. In 3D, the situation is more intrigue. $(3+1)$-TQFTs whose partitions that can detect smooth structures are very rare\cite{12}. I would conjecture that all unitary Atiyah-Segal-type $(3+1)$-TQFTs give rise to partition functions that are simple homotopy invariants. For 3D, an algebraic framework analogous to modular category is lacking, at least we do not understand higher category for 3D to have a good understanding.

Quantum computers are still hypothetical models that promise revolutionary advance in information science. The quantum algebra/topology approach provides substantial evidence that we may see quantum computers in our future, so the time of machines is coming.
Acknowledgments

The author is partially supported by NSF DMS 1108736.

References

[1] Bennett, C.H. and Brassard, G. (1984) Quantum Cryptography: Public key distribution and coin tossing, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175 (1984).

[2] Bakalov, B. and Kirillov, Jr., Lectures on Tensor Categories and Modular Functors, University Lecture Series 21, Amer. Math. Soc., 2001.

[3] Bravyi, S. and Kitaev, Universal Quantum Computation with ideal Clifford gates and noisy ancillas, Phys. Rev. A 71, 022316 (2005), arXiv:quant-ph/0403025.

[4] Bruillard, P., Ng, E., Rowell, Z., and Wang, On modular categories, in preparation.

[5] Etingof, P., Nikshych, D., and Ostrik, On fusion categories, Ann. of Math. (2) 162, 2 (2005), 581–642, arXiv:math/0203060.

[6] Freedman, P/NP, and the quantum field computer, Proc. Natl. Acad. Sci. USA 95, 1 (1998), 98–101.

[7] Gu, Z.-G., Wang, Z., Wen, X.-G., A classification of 2D fermionic and bosonic topological orders, arXiv:1010.1517.

[8] Hastings, M.B. (2009), Superadditivity of communication capacity using entangled inputs, Nature Physics 5, 255 - 257 (2009).

[9] Hastings, M.B., Nayak, C., and Wang, Metaplectic Anyons, Majorana Zero Modes, and their Computational Power, arXiv:1210.5477.

[10] Jiang, H.C., Balents, L., and Wang, Identifying topological order by entanglement entropy, Nature Physics 8, 902–905 (2012), doi:10.1038/nphys2465, arXiv:1205.4289.

[11] Jones, V. Braid groups, Hecke algebras and type II1 factors, in Geometric Methods in Operator Algebras (Kyoto, 1983), Pitman Res. Notes Math. Ser. 123, Longman Sci. Tech., Harlow, 1986, 242–273. Harlow, 1986.

[12] Walker, K. and Wang, (3+1)-TQFTs and Topological Insulators, Front. Phys., 2012, 7(2): 150-159, arXiv:1104.2632.

[13] Kitaev, A. Fault-tolerant quantum computation by anyons, Ann. Physics 303, 1 (2003), 2–30, arXiv:quant-ph/9707021.

[14] Kitaev, A. Anyons in an exactly solved model and beyond, Ann. Physics 321, 1 (2006), 2–111, arXiv:cond-mat/0506438.

[15] Levin, M. and Wen, X.-G., String-net condensation: A physical mechanism for topological phases, Phys. Rev. B 71, 4 (2005), 045110, arXiv:cond-mat/0404617.

[16] Mourik, V., Zuo, K., Frolov, S., Plissard, S., Bakkers, E., and Kouwenhoven, Signatures of Majorana Fermions in Hybrid Superconductor-Semiconductor Nanowire Devices, Science 122360 DOI:10.1126/science.122360.

[17] Nayak, C., Simon, S., Stern, M., Freedman, and S. Das Sarma, Non-abelian anyons and topological quantum computation, Rev. Mod. Phys. 80, 3 (2008), 1083–1159, arXiv:0707.1889.

[18] Naidu, D. and Rowell, E. C. A finiteness property for braided fusion categories, Algebr. Representation Theory. 15 (2011) no. 5, 837–855.
[19] E. Rowell, R. Stong, and Z. Wang, *On classification of modular tensor categories*, Communications in Mathematical Physics **292**, 2 (2009), 343–389, arXiv:0712.1377.

[20] Shor, P. W. (1994), Algorithms for quantum computation: discrete logarithms and factoring, 35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994), 124–134, IEEE Comput. Soc. Press, Los Alamitos, CA, 1994.

[21] V. Turaev, *Quantum Invariants of Knots and 3-Manifolds*, De Gruyter Studies in Mathematics **18**, Walter de Gruyter & Co., Berlin, 1994.

[22] Z. Wang, *Topological quantum computation*, CBMS monograph vol. 112, American Mathematical Society, 2010.

[23] R. L. Willett, L. N. Pfeiffer, and K. W. West, *Measurement of filling factor 5/2 quasiparticle interference with observation of charge e/4 and e/2 period oscillations*, PNAS (2009), vol. 106, no. 22, 8853—8858.