

Preface

These days it is impossible to turn on the news, open a book, or browse the internet without seeing some mention of quantum mechanics and quantum computation (see Figure 1). Even when delving into the dusty recesses of math and physics academic journals, quantum computing is lurking. Aside from our cultural fascination with the strangeness of quantum mechanics, quantum computing seems to be so pervasive because of its futuristic claims and its near-term realization. Indeed, not only have researchers constructed small devices, but these devices will eventually enable breaking conventional encryption techniques through the rapid factorization of large integers and provide a means to combat global warming through the development of novel catalysts for fertilizer and carbon fixation [1]. Even in the academic realm it is no longer a niche subject, and in many ways quantum computing has become a crosscutting discipline. We would venture to guess that there is no other subject studied by physicists, mathematicians, computer scientists, chemists, and engineers.

Quantum computing comes in a variety of flavors, from the qubit model to adiabatic constructions to the topological paradigm. The qubit model is arguably the most well known and operates through a seemingly simple extension of our classical binary computer systems. This model was arguably the first model for quantum computing and has been widely studied. A host of algorithms exist for qubit based devices and small scale qubit systems have been constructed in the laboratory. However, for all of their promise, they have yet to live up to expectations. This is due to a phenomenon known as *decoherence* wherein a quantum system couples with its environment and information “leaks out.”

In the qubit realm decoherence has been combated in two ways; the first is through engineering. By operating these devices in highly isolated cryogenic environments, researchers are able to stave off the effects of decoherence for a short time. This volume will have little to say about these engineering solutions. However, articles in this text will touch on a software based solution, *error correcting codes*. In an error correcting code, one uses a collection of physical qubits to simulate a logical qubit. By incorporating redundancy into the physical qubits, one can correct errors in the logical qubits. Intuitively, the simplest mechanism for accomplishing this would simply be to repeat each qubit several times, operate on each qubit in the collection in an identical manner, periodically vote on the correct value, and alter the values in the minority. Such a system can be easily implemented in a classical computer, but there are several obstructions in the quantum realm. For instance, the no-cloning theory forbids the cloning of a qubit while the measurement problem essentially prevents voting in the obvious way. Nonetheless, these

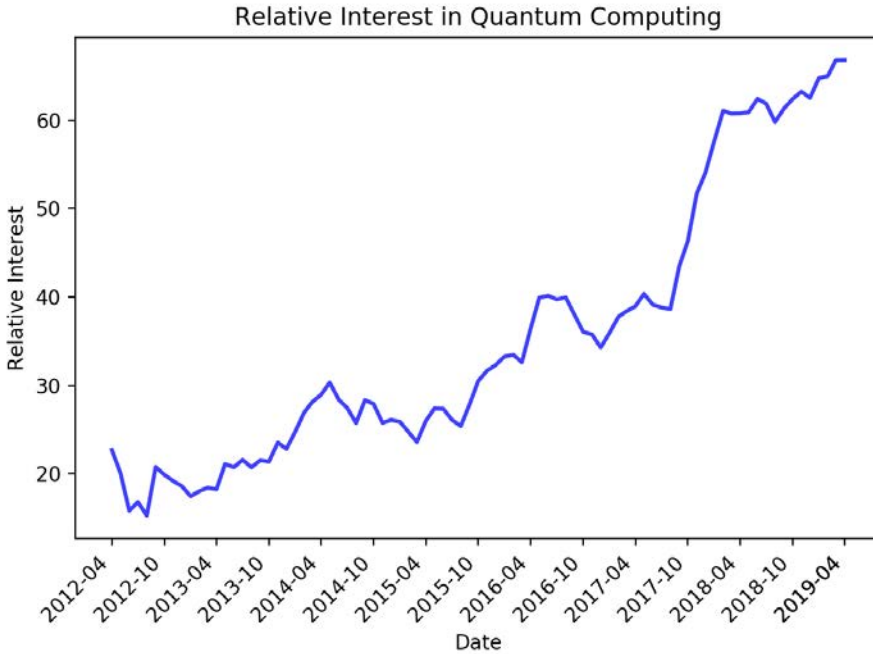


FIGURE 1. Interest in quantum computing as gauged by Google Trends for “What is quantum computing” [7]. A value of 100 indicates peak popularity while lower values indicate the popularity as a fraction of the peak popularity. For instance, a value of 50 indicates that the term is half as popular as it was at its peak. The data in this plot has been exponentially windowed ($\beta = 0.9$) to illustrate the trend.

ideas can be modified and refined to produce exotic new coding schemes unique to quantum computers [2].

An alternative to solving the decoherence problem in the qubit system is to reimagine quantum computing altogether. This was done in the early 2000s by Alexei Kitaev [3]. Rather than trying to devise a clever new coding scheme, Kitaev asked for a physical system that would resist environmental disruption at the hardware level and enable the simulation of a qubit system. This led to the birth of *topological quantum computing*. Under this paradigm one produces quasiparticles known as anyons in $(2+1)$ -dimensions. As these anyons are moved around one another, their worldlines trace out a braid (see Figure 2). For simple topological reasons, it is possible to produce nontrivial braids and thus particle exchange in these systems is governed by the braid group rather than the symmetric group. The amazing fact is that if the anyons have the correct particle statistics, then a quantum computation can be encoded in such a braid and evaluated by fusing the particles [4]. The major advantage of producing a calculation in this manner is that it depends only on the topology of the braid and thus is resistant to thermal effects. Indeed, thermal fluctuations will tend to have one of two effects, the first

being that the anyons will jitter, but this will not affect the topology of the braid if the jitter is small enough. Second, thermal effects may cause the pair production of anyons which will wander through the system. This is problematic only if the errant particles braid nontrivially with the computational anyons and then recombine; the likelihood of this happening can be made quite small with careful engineering. While the major hurdle to overcome in the qubit model is one of engineering, the obstruction to a topological quantum computer appears to be one of existence. It has long been known that anyons of the correct statistics exist in theory, but we have yet to find them in nature.

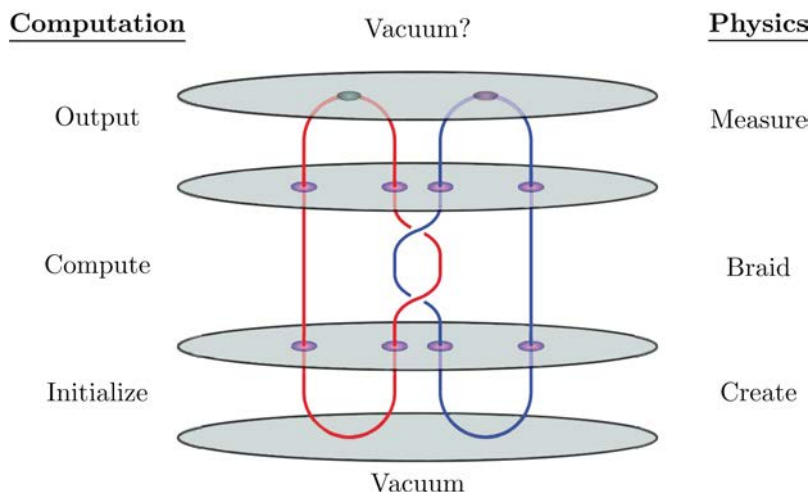


FIGURE 2. In topological quantum computing, particles are created in a (2+1)-dimensional space, exchanged so that their world lines form a braid, and then pairwise fused. Given the correct particle statistics, a computation can be embedded in the topology of these braids. In fact, not only can the qubit model be simulated, but such a process is inherently resistant to decoherence.

The study of topological quantum computation is related to two new branches of mathematics, *modular categories* and *subfactors*. These theories are really two sides of the same coin, and in fact one can often translate between them [5]. Their major distinction is that the study of modular categories has its roots in representation theory, algebra, and topology, while subfactors owe their lineage to analysis. A large portion of the articles in this text are devoted to these two subjects. While these mathematical theories are interesting in their own right, the main focus here will be on their use as mathematical models for topological quantum computing. These models allow researchers to understand properties of topological quantum computers, such as universality, as well as provide a taxonomy of possible systems [6]. Furthermore, these theories can lead to insights in modern mathematics and computer science, such as the computational complexity of computing link invariants and new representations of the braid group.

Quantum computing occupies the triple point of mathematics, physics, and computer science. We have made an effort to include articles coming from each of these disciplines. Furthermore, in the mathematics realm we have included articles

on both modular categories and subfactors. As such we believe there is something that almost everyone will find familiar, in addition to new topics closely related to their discipline from which researchers can draw inspiration. We sincerely hope that you enjoy.

Bibliography

- [1] Troyer, Matthias, “What Can We Do with a Quantum Computer?” Presentation available at https://www.microsoft.com/en-us/research/wp-content/uploads/2015/03/Matthias-Troyer_Quantum-applications.pdf (2017).
- [2] Michael A. Nielsen and Isaac L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000. MR1796805
- [3] A. Yu. Kitaev, *Fault-tolerant quantum computation by anyons*, Ann. Physics **303** (2003), no. 1, 2–30, DOI 10.1016/S0003-4916(02)00018-0. MR1951039
- [4] Zhenghan Wang, *Topological quantum computation*, CBMS Regional Conference Series in Mathematics, vol. 112, Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2010. MR2640343
- [5] S. Popa, *Classification of subfactors: the reduction to commuting squares*, Invent. Math. **101** (1990), no. 1, 19–43, DOI 10.1007/BF01231494. MR1055708
- [6] Paul Bruillard, Siu-Hung Ng, Eric C. Rowell, and Zhenghan Wang, *Rank-finiteness for modular categories*, J. Amer. Math. Soc. **29** (2016), no. 3, 857–881, DOI 10.1090/jams/842. MR3486174
- [7] Google Trends, “What is quantum computing” Available at <https://trends.google.com/trends/explore?date=2012-01-01%202019-04-14&geo=US&q=what%20is%20quantum%20computing> (2012).