The Topological Quantum Menace

Andrea Shepard <andrea@persephoneslair.org>

2015-05-30

Noise sensitivity in quantum algorithms

Shor's algorithm uses the quantum Fourier transform:

$$U_{QFT} \left|x\right\rangle = 2^{-N/2} \sum_{y=0}^{2^N-1} e^{\frac{2\pi i x y}{2^N}} \left|y\right\rangle$$

Notice the phases spaced out by $2\pi i/2^N$ here become exponentially precise as N becomes large; the N in the application to factoring is on the order of the square of the number to be factored.

Factoring a 1024-bit semiprime means approximately 616 decimal places of phase precision!

Error correction

Error-correcting codes can map one error-corrected qubit to several physical ones, and then you can build error-corrected quantum logic gates (e.g. CNOT) out of physical ones that also repair errors, and do extended computations if the error amplitudes are below a critical threshold.

- Shor's 9-qubit code
- Laflamme's 5-qubit code

For one qubit there are two possible error modes (bit-flip and phase-flip), but for multiple qubits things get worse.

Scaling to multiple qubits

One qubit has a two-dimensional state space - the Bloch sphere. The number of distinct error syndromes corresponds to the dimension of the space of error vectors. N qubits have a 2^{2N-1} dimensional state space, and the number of possible error syndromes grows exponentially.

Simple one-qubit error correction, the Shor code, handles two error syndromes (bit flip, phase flip) as a sort of 'tensor product' of a quantum analog of triple redundant encoding for each. The obvious generalization leads to exponentially growing complexity: 9^N physical qubits to encode an error-corrected N-qubit register.

Exponential complexity of error handling

There are more efficient schemes even for one error-corrected qubit (e.g. 5-qubit stabilizer code), but it is not clear where the lower bound for scaling to N qubits lies. It may well be the case that correcting all error syndromes on N qubits requires $O(B^N)$ hardware complexity for some $B > 1$.

Thus, it becomes relevant how much we need. We can expect k-qubit entangled errors to be exponentially rare in k, so different behavior emerges for Shor's algorithm with its exponentially precise phases vs. less precise cases like Grover's algorithm.

Is another approach to building the underlying hardware, though, which makes that error rate sufficiently small even for a single physical qubit?

The Topological Approach

Idea: map quantum computation onto operators and observables of some underlying physical system which are topological invariants, so that they inherently resist small perturbations.

Topological quantum field theories in 2+1 dimensions are of interest here; there's much evidence that they are approximated by particular states of the fractional quantum hall effect.

What's Special About Two Dimensions?

Particle statistics: if we continuously deform a state such that two particles exchange position, the resulting endpoint state is physically identical to the initial one, so the quantum state vector should be equal up to a phase.

Paths like this are homotopies on the configuration space, so particle statistics are projective representations of the homotopy group of the configuration space.

In 3 or more space dimensions, we have enough room (4 or more dimensions in total counting the parameter along the homotopy) to slide paths of each particle in such a path around the others - same reason knots stay tied in 3 dimensions but not more.

Braids versus permutations; particle statistics

So, in three or more space dimensions, for n identical particles the homotopy group of the configuration space is just the permutation group S_n, but in two space dimensions it is the braid group B_n.

In a projective representation of S_n, exchanging any two particles yields a phase $e^{i\theta}$, but exchanging them twice then must yield $e^{2i\theta}$ as the representation of the group identity of S_n, which must be 1, so we have either $e^{i\theta} = 1$ (bosonic statistics) or $e^{i\theta} = -1$ (fermionic statistics).

In B_n, though, it is not true that exchanging the same pair of particles twice yields the group identity, so the possible representations are far more complex, and also admit so-called anyonic statistics.

/* You are not expected to understand this */

To do interesting computations, we need something stronger: anyons which form a non-Abelian representation of B_n, and we need a way to describe changes to the state involving creation/annihilation of anyons.

The mathematical framework to describe this is a unitary modular tensor category. The objects of the category are tensor products of different anyon types, labeling the topologically invariant states of the theory by their content, and the morphisms are diagrams encoding different ways of braiding and splitting/fusing the anyons, enriched with vector space structure.

Is this mathematical model realized physically?

tl;dr: nobody knows yet

Long version: in a thin conductive sheet at sufficiently low temperatures and high magnetic fields, the fractional quantum Hall effect occurs, involving collective states of conduction-band electrons together with magnetic flux. These states are parametrized by the filling fraction ν, depending on the ratio of electrons to magnetic flux. Many have anyons, but most are Abelian anyons we can't compute with. The $\nu = 5/2$ state may correspond to the Ising TQFT.

Can we emulate the quantum circuit model?

Exact mappings between multi-qubit states and TQFTs seem rare; most TQFTs don't come with power-of-2 dimensions that correspond cleanly to an n-qubit QCM machine - the Ising TQFT does, though.

We'd like to be able to do computation solely by braiding in the TQFT, since this corresponds to just moving anyons localized away from each other around. This appears to be possible in the Fibonacci TQFT, but not the Ising one.

In general, we want a way to map qubit states to the TQFT state space such that we can approximate a given quantum gate arbitrarily well with with a braiding on the anyons. How does the complexity of the braiding scale with the required precision?

TQC and complexity theory

In the quantum circuit model, the usual complexity class of interest is BQP, the quantum analogue of BPP. As we saw earlier, some quantum algorithms are much more noise-sensitive than others. Shor's algorithm and Grover's algorithm are both in BQP, but the former has exponential noise sensitivity and the latter only has polynomial.

These topological approaches to quantum computation potentially present new complexity classes - what is the analogue of BQP for things that can be accomplished in polynomially many operations on a particular TQFT? Then the existence of sufficienctly efficient ways of embedding the QCM would imply that class contains BQP.

References / Further Reading

Zhenghan Wang, Topological Quantum Computation

http://www.math.ucsb.edu/ zhenghwa/data/course/cbms.pdf

D. Gottesman, Stabilizer Codes and Quantum Error Correction

http://arxiv.org/abs/quant-ph/9705052