Quantum Fault Tolerance

Peter Shor
M.I.T.
Cambridge, MA

When the quantum prime factorization algorithm was announced in 1994, one reaction was that this would never work because errors would inevitably disrupt the computation.

How bad is the situation?

To do 10^9 steps on a quantum computer, you need to do each step with inaccuracy less than 10^{-9}. This seems virtually impossible to experimental physicists.

The same objection was raised to scaling up classical computers in the 1950's.

Von Neumann showed that you could build reliable classical computers out of unreliable classical components.

Currently, we don't use many of these techniques because we have *extremely* reliable chips, so we don't need them.

Can you use the classical fault tolerance techniques on quantum computers? For a while it was thought you couldn't, as it appeared there were some fundamental obstacles to doing this.

- No-cloning theorem:

  You cannot duplicate an unknown quantum state.

- Heisenberg uncertainty principle:

  You cannot completely measure a quantum state.

Quantum Error Correcting Codes Exist

How do they get around the no-go theorems?

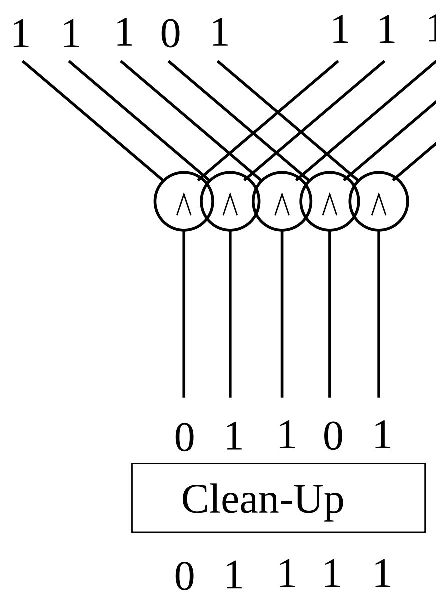
- Measuring the state of one (or a few) qubits doesn't reveal any information about the encoded state, so the quantum state doesn't leak into the environment.
- The error can be measured (and then subsequently corrected) without measuring (and disturbing) the encoded state.

Best current results: Using quantum error-correcting codes, we can show that if the quantum gates are accurate to around 1 part in 10^4, you can make fault-tolerant quantum circuits.

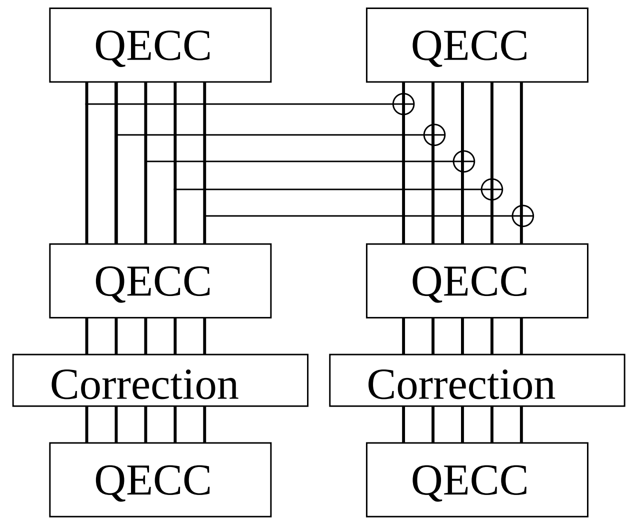
The best upper bound is around 1 part in 5.

Fault Tolerant Computing with Active Error Correction

Classically



Quantum Mechanically



Intrinsic Fault-Tolerance

Topological fault-tolerance. You can use topological properties of quantum states on two-dimensional sufaces to ensure low error rates.

Simplest model (Kitaev). Compute on a torus. Errors on edges can get corrected unless there is a non-trivial closed loop of errors wrapping around the torus.

Non-abelian anyons surfaces (Kitaev). Compute with anyon quasi-particles. The states are fault-tolerant unless the anyons get too close to each other. Computation can be done by braiding the anyons around each other.