Quantum Computing

Nathan Chapman

Central Washington University

CS 530: High Performance Computing, Spring 2024

Why do we care?

- Because it's cool
- It turns out quantum computers can easily break classical cryptography

Qubits - Heads or Tails?

Does a coin show heads or tails?

Qubits - Single

- Classical - "Bit"
  - State is true or false
  - Always
- Quantum - "Qubit"
  - State is true or false or tralse or frue
  - State is a little bit of both
  - Until measured
  - At measurement, the state is true or false
- Example - A simple coin
  - Classical - Deterministic via applied force, torque, height, etc.
  - Quantum - Probabilistic until measured

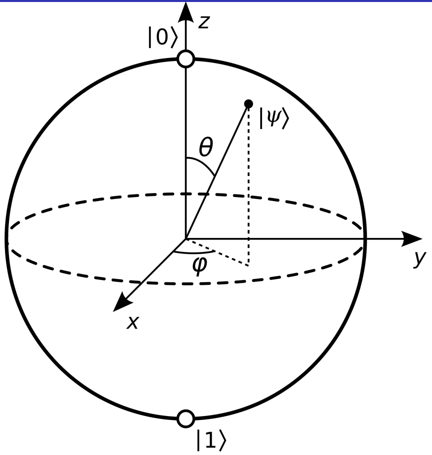

Figure: The Bloch sphere reprensetation of a qubit $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$

Qubits - Multiple

- 2 qubits $\implies$ state is a mix between the 4 permutations $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$
- Each permutation has its own probability such that the total is 1
- Measure only qubit $\implies$ state renormalizes to only include remaining possible states
- Bell State: 50% $|00\rangle$ and 50% $|11\rangle$

Demo: 2 quantum coins with a volunteer

Qubits - Quantum Registers

Classical

- Register of size $N \equiv N$ flip-flops
- Stores 1 permutation of states

Quantum

- Register of size $N \equiv N$ qubits
- Stores ALL 2^N permutations of states

The information density of a quantum computer can be massive

Quantum Computation - Single Qubit Gates

Classical

- Only one non-trivial gate
- NOT - $0 \rightarrow 1$

Quantum

- Several non-trivial gates
- NOT (X) - swaps the probabilities
- Z - flips the sign of the probability on the $|1\rangle$ state
- Hadamard - "mixes" the pure states toward the other
  - $|0\rangle \rightarrow 50\% \, |0\rangle$ and $50\% \, |1\rangle$
  - $|1\rangle \rightarrow 50\% \, |0\rangle$ and $-50\% \, |1\rangle$

Quantum Computation - Single Bit Gates

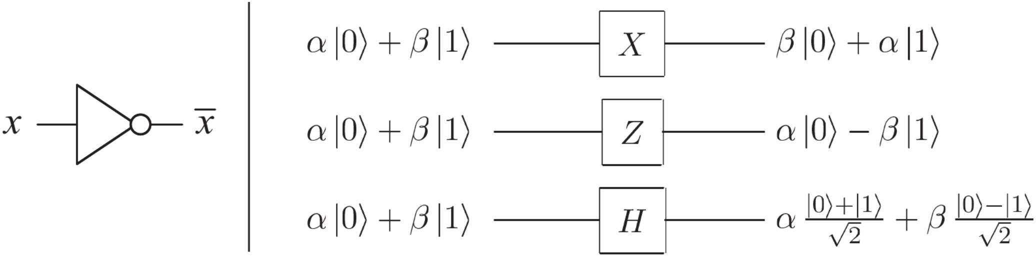

Figure: A comparison between logic gates that can act on a single classical or quantum bit.

Quantum Computation - Multi-Qubit Gates

Classical

- AND, OR, XOR, NAND, NOR
- XOR isn't invertible
- NAND makes up all gates

Quantum

- Controlled not - CNOT
- Uses a *control* bit and a *target*
- If control is 1, NOT target, otherwise do nothing
- CNOT is invertible
- CNOT and single-gates make up all multi-gates

Quantum gates need to conserve information

Quantum Computation - Circuits

- Sequence of gates
- Read left to right
- Lines are “wires”
- No loops
- Wires can’t connect to conserve information
- Can connect from one bit (black dot) to a target bit ($\oplus$)
- $\oplus$ represents addition mod 2

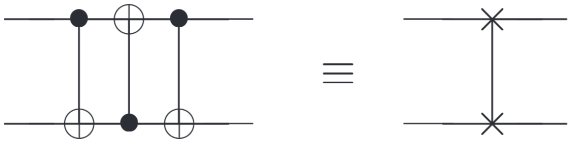

Figure: A quantum circuit to swap the states of two given qubits (left) and its compact notation (right).

- Classical DFT $y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} x_j$
- FFT uses $\Theta(N2^N)$ gates
- Quantum FT $|j\rangle \rightarrow \frac{1}{\sqrt{2^N}} \sum_{k=0}^{2^N-1} e^{2\pi ijk/2^N} |k\rangle$
- QFT uses $\Theta(N^2)$ gates

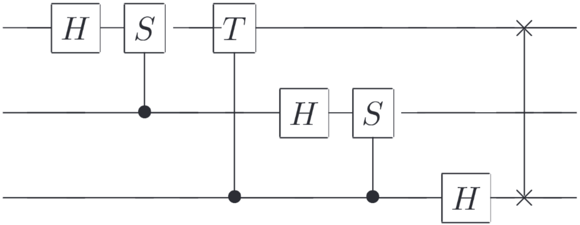

Figure: A 3-qubit quantum Fourier transform circuit. S, T are the phase and $\pi/8$ gates, respectively.

Quantum computers calculate the Fourier Transform with *exponentially* fewer operations

Demo - Qiskit

- Many quantum cloud computing platforms
- Most popular is Qiskit by IBM
- Allows jobs to be submitted to IBM's quantum computer with 127 qubits
- Demo

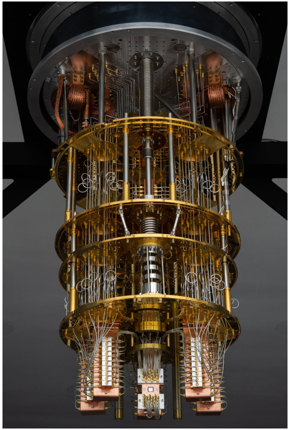

Figure: A real quantum computer

Conclusion

- Quantum computation is different at the most fundamental levels
- A collection of N qubits stores 2^N values
- Every quantum gate can be made of CNOT and single-qubit gates
- Quantum gates conserve information
- A quantum circuit is a sequence of applied quantum gates
- The quantum Fourier Transform requires exponentially fewer operations
- There are real quantum computers in the world and we can use them with Qiskit!