Quantum Computing

Jason Zhang,
Ren Bauer,
Kevin Nadeau
What is a Quantum Computer?

- Moore’s Law: Transistors must be the size of atoms within the next 20 years.
- Qubit: Anything that obeys quantum laws. Ex: photons, ions, electrons
- Superposition: Until measured, a particle is considered to be every possible state.

Figure 5
Limits of Classical Computers

- NP–Complete—common procedures that cannot be solved without exponential time, memory, etc.
- Quantum magic: ex Grover’s Search Algorithm
  - Perform operation $F$ on all values. If a value $x$ is a good candidate, $F(x) = -x$. Else $x$.
  - Skew. Good values grow while bad values shrink.
  - Repeat several times until one value remains.
- Grover’s Algorithm runs in $O(N^{1/2})$ time.
Entanglement

- What is Entanglement?
- How do you entangle?
- Why do you entangle?
Mathematical Entanglement

What is real? If something or its effects can be measured, then it is real.

\[ |\psi\rangle = a|0\rangle + b|1\rangle \quad |a|^2 \text{ and } |b|^2 \text{ are real.} \]

What happens when we entangle a system? Suppose we have an entangled system:

\[ |\psi\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle \]

In measuring the first qubit but not the second, say we measured 0 for qubit 1

\[ P_0 \otimes I |\psi\rangle = \frac{1}{\sqrt{2}}|01\rangle \]
Mathematical Entanglement

We must renormalize after measurement to find the new state:

\[ |\psi'\rangle = \frac{P_0 \otimes I |\psi\rangle}{\sqrt{\langle \psi | P_0 \otimes I |\psi\rangle}} \]

But this is really a special case of Bayes' Theorem, assuming orthonormal basis, a single pure state, and maximal entanglement:

\[ P(A|B) = \frac{P(B|A)P(A)}{P(B)} \]

So entanglement is conservation of probability.
Physical Demonstrations – EPR Paradox

Step 1: Entangle property $p$ of A with $q$ of B

A  B

Step 2: Separate A and B, then measure $p$. Now $q$ has a fixed, definite value.

A  Distance too far for light to travel during observation  B
Fig. 1. The three detectors A, B, and C, viewed from above (down the x axis). Their switch settings are 221. When the button on the source in the middle is pushed, three particles (shown en route) emerge and move in the horizontal plane to the three detectors.
Greenberger-Horne-Zeilinger (GHZ) Observations

Represent states as ABC. So, if all switches are set to 1, we have state 111. If A is set to 1, B to 2, C to 2, we have 122.

What is observed?

If state 111 – An odd number of red lights is never observed

If state 122, 212, or 221 – Odd number of red lights always observed.
GHZ observations

How do they coordinate? They must have coordinated at emission.

Each particle, upon emission, must be encoded with what to do once it reaches a detector and interacts to find the detector's setting. For example,

RGG
GRG

Means that the particle which reaches A is set to make A flash red if A is set to 1, and G if set to 2. B's particle makes B flash green if B is set to 1, and red if 2. C's particle makes C flash green if C is set to 1, and green if 2.
Problem arises

To satisfy 122, we must have one of the following encodings:
R-- R-- G-- G--
-RR -GG -RG -GR

Now in order to satisfy 221 as well:
RRR RGG GRG GGR
RRR RGG GRG GGR
RRR RGG GRG GGR

RGG RRR GGR GRG
GRR GGG RRG RGR

But all these states require 111 to have an odd number of red. Yet it never happens.
Shor’s Factoring Algorithm

- Quantum Fourier Transform
  - Performs FT on state, not large set of inputs.
  - Fast.

- To factor $N$, find the period of $f(x) = y^x \mod N$. $N$’s factors are $\gcd(r+1, N)$, $\gcd(r-1, N)$.

- Implications for Cryptography: Hacking for dummies
  - Modern security involves knowing factors of large numbers. These numbers are easy to build and hard to factor. For now.
Physical Implementation - Theory

- Two routes – Schrodinger equation or unitary gates

Physics approach - Schrodinger equation:

\[ i \hbar \frac{d}{dt} |\psi\rangle = H \frac{d}{dt} |\psi\rangle \]

Computer engineering approach – view computation as applying a series of unitary operators to an initial state

\[ |\psi_i\rangle = U_{i-1} |\psi_{i-1}\rangle \]
Physical Implementation – Practice

- Ion traps
  - Scaling
- Processors
Problems

- Decoherence
  - Threshold Theorem
  - Photosynthesis
Further Reading


Quantum Computing and Quantum Information - Nielsen and Chuang. This particular book is probably the best self-contained one available.

Quantum Computing Explained – McMahon

Branching out from http://en.wikipedia.org/wiki/Quantum_computing is also fun!