Quantum Computation

(In Brief)

Investigation by Vince Velocci

November 4, 2016

Exploiting Quantum Weirdness

"I think I can safely say that nobody understands quantum mechanics…

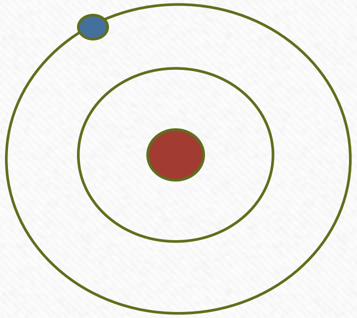
Exploiting Quantum Weirdness

"I think I can safely say that nobody understands quantum mechanics…

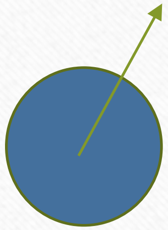
...BUT I know more about quantum mechanics than the generals do, believe me."

Key Ideas About Quantum Physics

- Certain properties can take on discrete values. Examples:



Energy Levels in atom: {ground state, 1st excited state,…}

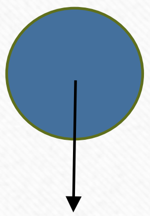
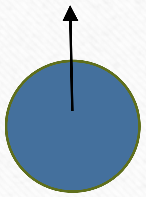


Component of spin about any given axis: {+1, -1} for electrons

- State of a particle described by a vector of length one: $|E_0\rangle$, $|0\rangle$, $|1\rangle$

Important Idea for Quantum Computers

- <u>Superposition</u>: Particle can be in any linear combination of states between measurements.

State = a *  + b * 

$\text{State} = a|0> + b|1>$, where the $|a|^2 + |b|^2 = 1$ (unit vector)

When a spin measurement is performed, State "collapses" to either $|0>$ with probability $|a|^2$ or $|1>$ with probability $|b|^2$.

Classical Computers vs Quantum Computers

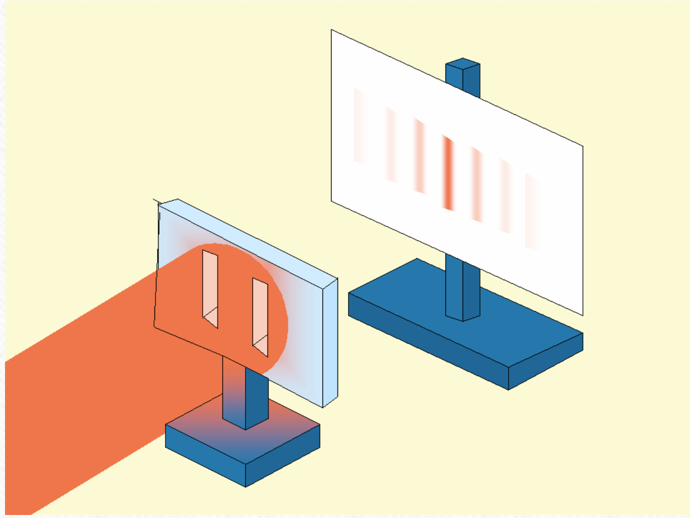
- Unit of information: “bit”…...0 or 1......high voltage or low voltage.....etc.

  Physical implementation: 2-state system in either one state or another.
- Classical computers/Logic gates process bits. Bits in, bits out.
- Quantum computers process bits in SUPERPOSITION. These are “quantum bits”, or qubits. Picture: electron “spin up” + “spin down”:

  Qubit state = a|0> + b|1>
- a and b are complex numbers (eg., 3 -2i, 5i, -145, 11) called “amplitudes”.
- Multiple qubits = multiple two-state quantum systems:
  - |01>, or |10>. In general: |00> + |01> + |10> + |11> (superposition properly normalized)

Interference is a Good Thing!

- In quantum mechanics, states can interfere with each other, cancelling in some places, and reinforcing in others (double-slit experiment with light)



What if we had a device that took every possible answer to a problem, made them interfere so that only the correct answer got reinforced?

That's what Quantum Computers are for!

General Process

Step 1: Input quantum state. Example, |00>. This represents a system of two particles: one spin down, the other also spin down.

Step 2: Apply a "quantum gate" turning the initial state into an equal combination of all the possible states: ½|00> + ½ |01> + ½ |10> + ½ |11>

Step 3: Repeatedly apply another transformation on this new state so that the amplitude for the right answer grows with each application of the transformation.

Step 4: Perform a measurement on the system. You will observe the correct answer with high probability.

Grover's Search Algorithm

- Unordered list of N items. Want to match a search query.
- Classical computers can match with O(N) at best.
- Quantum computers can do this with O($\sqrt{N}$)

- Suppose N = 2^n. We can write the i^{th} index of the list in binary. We can represent each index as a physical n qubit system.

Example: 8 entries in the list → The list indices are can be written as:
|000>, |001>, |010>, |011>, |100>, |101>, |110>, |111>. Think of each as 3 electrons, each of which can be spin down (0) or spin up (1).
By putting these in a uniform superposition, applying certain transformations, then measuring the system, we can arrive at the desired index with high enough probability. I.E. Suppose the desired index was 6. 6 = 110. So result of measurement will be the 3-qubit state |110>

Limitations

- System must be kept in a superposition for as long as the transformations need to work their interference MAGIC.
- Interactions between the qubits and the outside world will destroy the superposition!
- Quantum computers beat classical computers hands down only for certain tasks (eg., searching – Grover's algorithm; factoring – Shor's algorithm)
- Other tasks don't run any faster on a QC than on a CC (eg, our routine use)
- Just protecting the quantum nature of the systems you use as qubits will likely make the QC's slower than CC's for a long, long time.
- NSA likely has nothing to worry about.

National Security

NSA seeks to build quantum computer that could crack most types of encryption

By Steven Rich and Barton Gellman January 2, 2014

Most Read

“ OUR
QUANTUM COMPUTER
IS
100 MILLION TIMES FASTER
THAN PC.
- GOOGLE

physicsworld.com

Home | News | Blog | Multimedia | In depth | Events

News archive

- 2016
- 2015

Is D-Wave's quantum computer actually a quantum computer?

Jun 20, 2014 14 comments

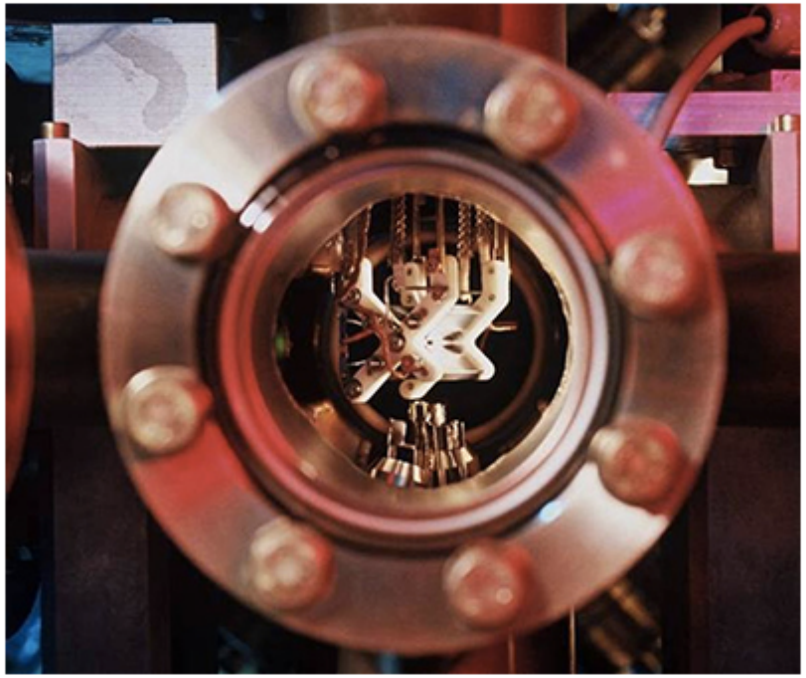
Programming Your Quantum Computer

The hardware doesn't yet exist, but languages for quantum coding are ready to go.

Brian Hayes

Shor's algorithm is implemented using five trapped ions

Mar 4, 2016 2 comments



Quantum factor: the Paul trap used by Monz and colleagues

Nice blog post about Shor's algorithm for factoring large numbers and quantum computing:
http://www.scottaaronson.com/blog/?p=208

Scott Aaronson: Quantum Computing researcher at UT Austin – very cool blog if you're interested

A new quantum approach to big data

System for handling massive digital datasets could make impossibly complex problems solvable.

David L. Chandler | MIT News Office
January 25, 2016

Press Inquiries

RELATED