Quantum Computing

4/29/2009

Opening Discussion

- Do you have any questions about the project?

Quantum Basics

- In order to discuss quantum computing, you need to have at least a bit of knowledge of quantum mechanics.
- In QM systems are described by complex valued waveform functions. The probability of finding a particular state is given by the square of the magnitude at that function.
- In some systems only certain states are allowed. These systems are quantized.

Superposition

- For quantized systems we often describe the system as a linear sum of the allowed states.
- Again, the weights are complex values and the probabilities are their magnitudes squared.
- So a system can in some sense be partially in one state and partially in another state.

Entanglement

- This is where things get weird.
- Multiple elements in a quantum system can be entangled. So the state of the system as a whole isn't just the sum of the two parts. Instead, there is a probability associated with every possible combination of one value and the other.
- This means measuring one part of the system implicitly gives you information about the other. (It's a bit deeper than that.)

Waveform Collapse

- When a measurement is made of a system, the waveform collapses to a single state. The probabilities are the odds that it will collapse to a given state.
- So while a system can be in a superposition of states, it will never be measured as a superposition. The measurement forces it into a single state.
- This is significant for the information on the previous two slides.

Qubits

- Quantum computers are based on these ideas of superposition and entanglement.
- Values are stored in qubits instead of standard bits.
- A qubit has allowed states of |0> and |1>. During a computation a single qubit is a superposition of those states. a|0>+b|1>.
- When you read the qubit you will see either |0> or |1> with probabilities of a^2 and b^2 respectively.

Entangled Qubits

- The power of a quantum computer comes from the fact that qubits are entangled.
- So in a three qubit system there are 8 states the system can be in and at any instant it is a superposition of all three.
- Without entanglement, each qubit would be in a superposition of its two states, but the states wouldn't be linked. With entangled qubits, the values are linked because the probabilities are for entangled states.

Many Qubits

- So a system of n qubits is described by 2^n different coefficients on the 2^n different entangled states.
- For a machine with 300 qubits, a classical computer would need to store 2^{300} values for those probabilities and do operations on those.

Quantum Operations

- Quantum operations can be expressed as matrices, U. The condition is that they be unitary, $U^tU=I$.
- All operations are reversible.
- Single qubit
  - For classical bits there is only one single bit operation, not.
  - For qubits there are an infinite number. Several of those happen to be useful.
- Multiple qubits

Quantum Algorithms

- Shor's algorithm (1994)
  - This was what really brought quantum computing into the limelight. It is an algorithm that can find factors of numbers in polynomial time assuming some operations can be done on a quantum computer. $O((\log N)^3)$
- Grover's algorithm (1996)
  - Allows searching an unsorted set in $O(N^{1/2})$ time and O(log N) spaces. While not an exponential speed up, this is big.

Quantum Simulation

- The real reason we are discussing this in this class is that it was mentioned that quantum computers could do quantum simulations more quickly. The reason for this is the entanglement factor. The number of entangled states grows exponentially, limiting the size of systems we can do with classical computers.
- Quantum computers implicitly get to represent the exponential states in linear space and with linear operations.

Minute Essay

- Should I consider teaching a whole class on quantum computing?
- Work on your projects.