Quantum Computing: How to do 2^n things all at once

Chuck Cusack

The Focus of This Talk

- Quantum Bits (Qubits)
- Quantum Transformations
- Entanglement of Qubits
- Grover's Algorithm

Other Quantum Computing Topics

- The history of Quantum Computing
- Shor's Algorithms
- Teleportation
- Dense Coding
- Quantum Cryptography
- Quantum Complexity Theory
- Quantum Error-Correction Codes

Bits and Qubits

- Modern-day computers store information in *bits*.
- A bit can be either '0' or '1'.
- Quantum computers store information in *quantum bits*, or *qubits*
- A qubit is a quantum two-level system which can be in state '0' or '1', or a *superposition* of both.
- That is, a qubit can be in state $a \cdot 0 + b \cdot 1$, where a and b are complex numbers satisfying $|a|^2 + |b|^2 = 1$.
- A set of n qubits is called an n-qubit *quantum register*.
- This is *not* the same as probabilistic computing.

Mathematical Representation of a Qubit

- The state of a qubit can be thought of as a unit vector in a complex Hilbert space of dimension 2.
- Let $\mathcal{H}_1$ be a 2-dimensional complex Hilbert space.
- A basis for $\mathcal{H}_1$ is $\left\{\binom{1}{0}, \binom{0}{1}\right\}$.
- A generic vector in $\mathcal{H}_1$ is of the form

$$a\binom{1}{0} + b\binom{0}{1},$$

where a and b are complex numbers with $|a|^2 + |b|^2 = 1$.

Mathematical Representation of a Quantum Register

- The state of an n-qubit register can be thought of as a unit vector in a Hilbert space of dimension 2^n.
- Let $\mathcal{H}_n$ be a complex Hilbert space of dimension 2^n.
- We can define $\mathcal{H}_n$ recursively by

$$\mathcal{H}_n = \mathcal{H}_{n-1} \otimes \mathcal{H}_1,$$

where $\otimes$ is the *tensor product*.

$\mathcal{H}_2$

- A basis for $\mathcal{H}_2$ is

$$\left\{ \binom{1}{0} \otimes \binom{1}{0}, \binom{1}{0} \otimes \binom{0}{1}, \binom{0}{1} \otimes \binom{1}{0}, \binom{0}{1} \otimes \binom{0}{1} \right\}$$

$$= \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\},$$

- A generic vector in $\mathcal{H}_2$ is written as

$$a_0 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + a_1 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + a_2 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + a_3 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix},$$

  where $|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 = 1$.

- Before we talk about larger dimensions, we need to define a compact notation for vectors, called *ket notation*.

Ket Notation

- We label $|0\rangle = \binom{1}{0}$ and $|1\rangle = \binom{0}{1}$.
- Then the basis vectors in $\mathcal{H}_2$ are written as

$$|0\rangle = |00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \; |1\rangle = |01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|2\rangle = |10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad \text{and } |3\rangle = |11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

More Ket Notation

- In general, a basis for $\mathcal{H}_n$ is given by

$$\{|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle\},$$

  where the numbers in the kets are thought of in terms of their binary expansions.

- Finally, we can write a vector in $\mathcal{H}_n$ as

$$\sum_{i=0}^{2^n-1} a_i |i\rangle,$$

  where the a_i are complex numbers such that $\displaystyle\sum_{i=0}^{2^n-1} |a_i|^2 = 1$.

Quantum States and Measurement

- A classical register can store *just one* of the possible 2^n states.
- An n-qubit register can be in a superposition of *all* 2^n states.
- It is evident that a quantum register can store exponentially more information than a classical one.
- However, the state of a quantum register is not known unless we make a *measurement* of the register.
- When we measure a quantum register, the state is *collapsed* into a basis state.
- The probability that the state collapses to $|k\rangle$ is $|a_k|^2$.
- In the measurement process, the original state of the register is destroyed, and cannot be reconstructed.

Examples

Example 1 *Let* $q = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

- If we measure the qubit, it will collapse to state $|0\rangle$ with probability 1/2, and to state $|1\rangle$ with probability 1/2.
- If we measure the state again, we will get the same result, because the state has collapsed to the state which we measured it to be in.

Example 2 *Consider a 2-qubit register in state* $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

- Two qubits in this state are called an *EPR pair*
- If we measure either qubit of the register, the whole register will collapse to state $|00\rangle$ with probability 1/2, and to state $|11\rangle$ with probability 1/2.
- The two qubits in this register are said to be *entangled* because the value of one is not independent of the other.

Entanglement

- A collection of qubits is entangled if it can't be expressed as a tensor products of single qubits.
- **Examples:**
  - It is not too difficult to see that the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ cannot be written as a tensor product of single qubits.
  - A register in the state $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ is not entangled, since it can be written as $|0\rangle \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)$.
- Entanglement does not exist with classical information.
- It is entanglement that gives quantum computing an *edge* over classical computing.

Quantum Transformations

- Quantum registers are transformed by *unitary transformations.*
- A matrix U is unitary if $UU^\dagger = U^\dagger U = 1$, where $U^\dagger$ is the conjugate transpose of U.
- It is an important fact that unitary transformations are linear.
- We can think of the unitary transformations as gates, much like classical boolean logic gates. They have inputs and outputs, the outputs depending on the inputs and the type of gate.
- There are several very important differences, however.

Properties of Quantum Transformations

- Can place qubits in superpositions, not just '0' or '1'.
- Can introduce entanglement between two or more qubits.
- Can be described fully by their effect on the basis states.
- Operate on each basis state of a qubit independently.
- Are reversible.

Single-Qubit Transformations

Example 3 *The Pauli matrices.*

Identity	I :	$\|0\rangle$	$\mapsto$	$\|0\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
		$\|1\rangle$	$\mapsto$	$\|1\rangle$	
NOT	X :	$\|0\rangle$	$\mapsto$	$\|1\rangle$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
		$\|1\rangle$	$\mapsto$	$\|0\rangle$	
phase shift	Z :	$\|0\rangle$	$\mapsto$	$\|0\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
		$\|1\rangle$	$\mapsto$	$-\|1\rangle$	
(ZX)	Y :	$\|0\rangle$	$\mapsto$	$\|1\rangle$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
		$\|1\rangle$	$\mapsto$	$-\|0\rangle$	

Example 4 *The Hadamard transformation.*

H :	$\|0\rangle$	$\mapsto$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
	$\|1\rangle$	$\mapsto$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	

Multiple-Qubit Transformations

Example 5 *The* controlled-NOT *gate.*

$$C_{not}: \quad \begin{array}{lcl} |00\rangle & \mapsto & |00\rangle \\ |01\rangle & \mapsto & |01\rangle \\ |10\rangle & \mapsto & |11\rangle \\ |11\rangle & \mapsto & |10\rangle \end{array} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Example 6 *The Walsh-Hadamard transformation,*

$$W_1 = H, \quad W_n = H \otimes W_{n-1}.$$

W_n transforms the state $|0\rangle$ to an equal superposition of all basis states:

$$W_n|0\rangle \quad = \quad \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle.$$

Example 7 *The quantum Fourier transform.*

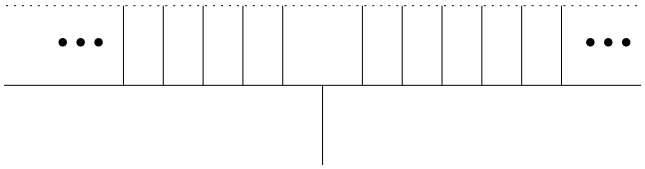
$$U_{QFT} : |a\rangle \mapsto \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{\frac{2\pi i c a}{q}} |c\rangle.$$

Grover's Search Algorithm

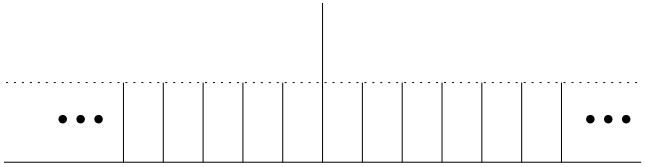
- **The Problem:** Given an unstructured list, and a property P, find the unique item x with $P(x) = 1$
- **Classical Algorithm:** Linear or random searching is the best one can do. Complexity is $O(n)$.
- **Grover's Algorithm:** Takes advantage of quantum parallel. Complexity is $O(\sqrt{n})$.
- The existence of Grover's algorithm is a "proof" that quantum computers are more powerful than classical computers.

Grover's Algorithm

1. Start with an m-qubit register a in state $|0\rangle$, $2^m \geq n$.
2. Apply W_m to a to put it in an equal superposition of the integers from 0 to $2^m - 1$.
3. Change the sign of the state $|x\rangle$ for which $P(x) = 1$.



4. Invert about the average.



5. Repeat steps 3 through 5 $\left(\frac{\pi}{4}\sqrt{2^m}\right)$ times.
6. The amplitude of x will now be large (close to 1), and the amplitude of the other states will be very small (close to 0).
7. Measuring a will yield x with high probability.

Quantum Computer Implementation

- There are four requirements to implement a quantum computer
  - Store quantum information robustly
  - Perform various unitary operations accurately
  - Prepare the input states
  - Measure the output
- There are several good choices for implementing a quantum computer: harmonic oscillator, optical photon, optical cavity electrodynamics, ion trap, nuclear magnetic resonance.
- So, what is the problem?

Quantum Computer Implementation Problems

- The problem with implementing a quantum computer is that we must be able to meet all four of the requirements.
- Each of the possible implementations does some things well, and other things not so well.
- Another major problem is **Decoherence**. That is, when qubits interact with the environment around them in undesirable ways.
- In addition, noise makes it impossible to implement a quantum algorithm without including error correction at every step of the computation.

Quantum Computers: A Reality?

- So, when should we expect to see quantum computers on our desks?
- The answer depends on who you ask, but most people believe it will not occur for at least another 20 years.

Conclusions

- Quantum computing is a very intriguing and difficult field which lies somewhere between physics, mathematics, and computer science.
- Quantum computing is based on some pretty neat principles.
- Quantum algorithms are very different than classical algorithms.
- There are major hurdles to be jumped in order to implement a useful quantum computer.
- Quantum computers, are *theoretically* capable of performing some tasks faster than any classical computer.
- If quantum computing becomes a reality, most (if not all) public-key cryptosystems in use today will be totally insecure.