# CS257
# Discrete Quantum Computation

John E Savage

April 30, 2007

# Classical Computation

- State is a vector of reals; e.g. Booleans, positions, velocities, or momenta.
- Observation of a state component does not change its value.
  - Classical states are robust.
- Computations can be analog or discrete but are assumed deterministic, i.e. they are predictable from inputs.

# Quantum Mechanics

- State is vector of complex numbers.
- Observation of state components changes (collapses) the state.
  - Quantum states are fragile.
- An observation probabilistically samples the quantum state.
  - Observations may yield different results.
  - Frequency of outcomes determined by state.

# Quantum Computation

- Quantum computation specified in terms of basis states, such as $|0\rangle$ and $|1\rangle$ denoting two physical states, such as "spin up" and "spin down."
- Represent basis vectors as column vectors, e.g. $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- The state is a linear combination of basis vectors using complex coefficients (**superposition**), such as, $|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle$.
- The state of quantum system that is the superposition of two basis states is called a **quantum bit** or **qubit**.

# Discrete Quantum States

- A quantum state is a mixture of orthogonal basis states (vectors) $\{p_j\}$.
  - Denote 3D basis states as $|000\rangle, |001\rangle, |010\rangle, \ldots |111\rangle$ where $|a_2a_1a_0\rangle$ denotes the 8-vector with a single 1 in position $a_2 2^2 + a_1 2^1 + a_0$.
- Each quantum state $|\phi\rangle = \sum_{1 \le j \le n} c_j p_j$ is a ray in a multidimensional space where $c_j$ are complex. ($c_j^*$ is the complex conjugate of $c_j$.)
- Each **observation** of a quantum state $|\phi\rangle = \sum_{1 \le j \le n} c_j p_j$ produces a single basis state. State $p_j$ occurs with probability $|c_j|^2 = c_j^* c_j$.
- Because the probability that some outcome occurs must be 1, the **normalization condition** $\sum_j |c_j|^2 = 1$ holds.

# Correlation Between Quantum States

- Consider the Bell or EPR state $|\phi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. (It is involved in quantum teleportation.)

- Measurement of the first qubit reveals either the basis state $|00\rangle$ or $|11\rangle$. Whatever the outcome, the measurement of the second qubit will give the same result as the first measurement.

- This exercise demonstrates that quantum states exhibit correlation. Bell has shown that this measurement correlation is stronger than can be found in classical systems.

# The Quantum NOT Gate

- NOT should map the qubit $|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ to $|\phi'\rangle = \beta\,|0\rangle + \alpha\,|1\rangle$.
- Since $|\phi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$, the NOT of $|\phi\rangle$ should be $|\phi'\rangle = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$.
- This can be done by forming the product $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |\phi\rangle$
- Such a mapping is called a **quantum computation**.

# Quantum Circuits

- **All quantum computations are represented by linear transformations of quantum states** $|\psi\rangle = U\,|\phi\rangle$.
  - If non-linear operations were possible, time travel would be possible and the second law of thermodynamics would not hold.

- $\langle\phi|$ denotes a row $n$-vector.

- Because the normalization condition $\langle\psi^\dagger|\,|\psi\rangle = \langle\phi^\dagger|\,U^\dagger U\,|\phi\rangle = 1$ must hold, $U$ must be **unitary**, that is, it must satisfy the property $U^\dagger U = I$ where $U^\dagger$ is the complex transpose of $U$ and $I$ is the identity matrix.

# Evolution of Quantum State

- A quantum state **evolves without change** under an **evolutionary operator** and **with change** under an **observable operator**.

- An **evolutionary operator** transforms a state $|\phi\rangle$ through multiplication by a unitary linear operator $U$, i.e. $U|\phi\rangle$.

- Because each unitary operator satisfies $U^\dagger U = I$, $U^{-1} = U^\dagger$ is the inverse of $U$. Thus, **evolutionary computations are reversible**.
  - Input can be determined from output.
  - To classically compute a function $f(\boldsymbol{x})$ reversibly, compute $(\boldsymbol{x}, f(\boldsymbol{x}))$.

# Quantum Observations

- A **quantum observation** projects the current state to a orthogonal basis state. It is non-reversible and fundamentally alters the quantum state.

- Given a qubit $|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, an observation projects quantum state to basis states $|0\rangle$ or $|1\rangle$ with probability $\alpha^2$ or $\beta^2$, respectively.

- The vectors $|+\rangle = \frac{1}{2}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{2}(|0\rangle - |1\rangle)$ also form an orthonormal basis. It follows that

$$|\phi\rangle = \alpha\frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta\frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{\alpha+\beta}{\sqrt{2}}\,|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}\,|-\rangle$$

  In this basis $|+\rangle$ ($|-\rangle$) is observed with probability $|\alpha+\beta|^2/2$ ($|\alpha-\beta|^2/2$).

# Quantum Superposition

- A set of $n$-dimensional basis states is the direct product of $n$ qubits, as indicated below.

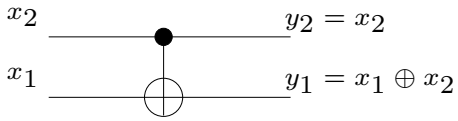
$$\boldsymbol{q}^T = (|0\rangle, |1\rangle, |2\rangle, \ldots, |2^n - 1\rangle)$$

- Superposition is denoted $|\phi\rangle = \boldsymbol{c}^T\boldsymbol{q}$. That is, superposition is the complex combination of basis states.

# Qubit Analogs of NOT

- NOT gate $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.
  - Input: $\alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha & \beta \end{bmatrix}^T$ ; Output $\beta|0\rangle + \alpha|1\rangle$
- Z gate $Z = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.
  - Input: $\alpha|0\rangle + \beta|1\rangle$; Output $\alpha|0\rangle - \beta|1\rangle$
- Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.
  - Input: $\alpha|0\rangle + \beta|1\rangle$; Output $\alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$

# Qubit Analogs of EXOR Gate




$$H = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

The control-NOT gate

- The controlled-NOT is the quantum equivalent of the EXOR. EXOR does a reversible computation, unlike NAND. Wires model passage of time or physical movement of a particle. Operations model interactions.

- The controlled-NOT maps inputs as follows:

$$|00\rangle \mapsto |00\rangle\,; \quad |01\rangle \mapsto |01\rangle\,; \quad |10\rangle \mapsto |11\rangle\,; \quad |11\rangle \mapsto |10\rangle\,;$$

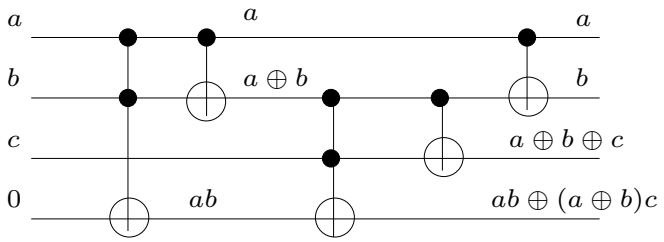
- Unitary matrix $H$ provides another way to see the effect of this gate.

# Reversible Boolean Circuits


The control-NOT and control-control-NOT gates

- The control-NOT (c-NOT) and control-control-NOT (c-c-NOT) gates are reversible. (Why?)
- c-c-NOT and constants 0, 1 form a **universal basis for classical Boolean reversible computation**. (Why?)
- Reversibility increases circuit size for $f : \{0,1\}^n \mapsto \{0,1\}$ by $O(n^{\log_2 3})$.
- c-NOT and qubits are a **universal basis for quantum computation**.

# Example of a Reversible Circuit




Feynam's Full Adder

- The Full Adder output is a two-digit representation for the number of 1s among three inputs, in this case $a$, $b$, and $c$.

- The least significant digit is $a \oplus b \oplus c$. The most significant is $ab \vee ac \vee bc$ which is equivalent to $ab \oplus (a \oplus b)c$.

# Example of a Quantum Computation I

- Quantum parallelism allows for evaluation of a function at many different points simultaneously. We illustrate for function $f(x)$, $x \in \{0, 1\}$.

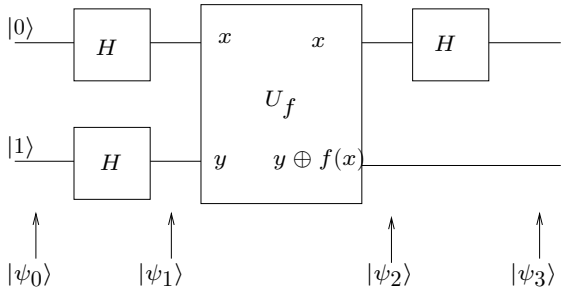
- Consider a two-qubit quantum computer with state $|x, y\rangle$.
  - Form the state $|0, 0\rangle = |0\rangle \times |0\rangle$ by creating $|0\rangle$ and $|0\rangle$ in parallel.
  - Use the Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ on the first $|0\rangle$ to produce the state $(|0\rangle + |1\rangle)/\sqrt{2}$.
  - The result is the state $(|0\rangle + |1\rangle)/\sqrt{2} \times |0\rangle$.

- A quantum state is **entangled** if it cannot be written as the direct product of multiple basis states. $(|0\rangle + |1\rangle)/\sqrt{2} \times |0\rangle$ is **not entangled**.

# Example of a Quantum Computation II

- Build the circuit $U_f$ that computes $|x, y\rangle \mapsto |x, y \oplus f(x)\rangle$
- Let its inputs be $x = (|0\rangle + |1\rangle)/\sqrt{2}$ and $y = |0\rangle$.
- Its output is $\frac{|0,f(0)\rangle+|1,f(1)\rangle}{\sqrt{2}}$, which involves computing both $f(0)$ and $f(1)$ simultaneously.
- When an observation is made, either $|0, f(0)\rangle$ or $|1, f(1)\rangle$ is produced with probability $1/2$. Thus, although both values of $f(x)$ are computed simultaneously, an observation doesn't combine them.
- Deutch's algorithm produces a combination of $f(0)$ and $f(1)$.

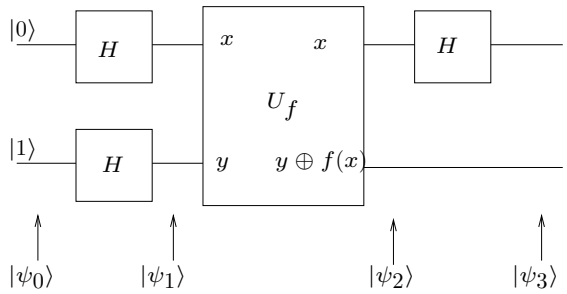
# Deutch's Algorithm




- Input state is $|\psi_0\rangle = |01\rangle$. State after Hadamard transforms is

$$|\psi_1\rangle = |x, y\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \times \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

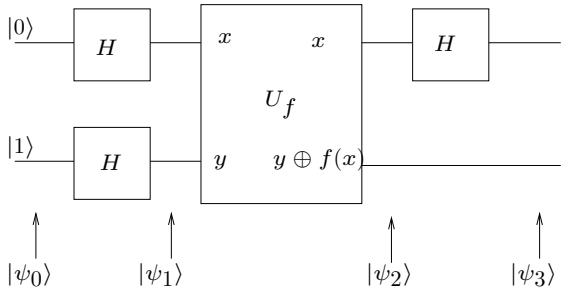
# Deutch's Algorithm




- State after $U_f$ is

$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right] \times \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \times \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1) \end{cases}$$

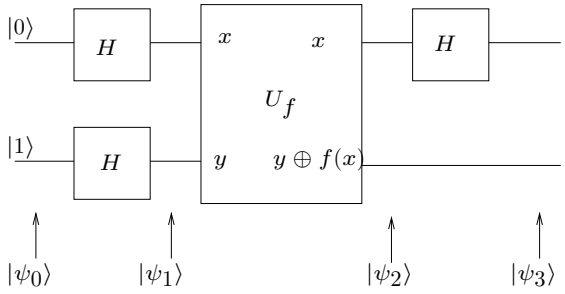
# Deutch's Algorithm




- State after last Hadamard transform is

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0)=f(1) \\ \pm|1\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0)\neq f(1) \end{cases}$$

# Deutch's Algorithm




- Simplifying state after last Hadamard transform, we have
- $|\psi_3\rangle = \pm\,|f(0) \oplus f(1)\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$ since $f(0) \oplus f(1) = 0$ if $f(0) = f(1)$ and $f(0) \oplus f(1) = 1$ if $f(0) \neq f(1)$.
- Quantum computation has provided global information about $f(x)$, namely, $f(0) \oplus f(1)$, in one step, namely, the computation by $U_f$. Two steps would be required by a classical computation.

# Solving Satisfiability or Unordered Search

- Problem: Given instance of SATISFIABILITY, find satisfying assignment to the input variables. Classically it appears to take $O(2^n)$ time.
  - Example $(\bar{x}_1 + x_3 + \bar{x}_4)(x_2 + \bar{x}_3 + x_4)(x_1 + \bar{x}_2 + \bar{x}_4)$
- The approach:
  - Each assignment is given equal probability initially.
  - An iterative algorithm due to Grover increases the probability of the satisfying assignments while decreasing the probabibility of non-satisfying assignments.
  - When the probability of satisfying assignments is high, sample the assignments. With high probability a satisfying assignment is discovered.

# Factoring Integers

- Problem: Given an integer which is the product of two primes, find one of the primes.

  – 750,089 = 827*907

- Factoring is considered a difficult classical computation. If an effective quantum factorization computer could be built, the RSA public key encryption system would be undermined.

- The approach: Probabilistic quantum computation based on number theory.

# Prospects for Quantum Computing

- Quantum computing requires that the state of qubits be maintained a long enough for a computation to complete. If a quantum state comes in connect with the external environment, an observation occurs and the quantum state is changed. Unfortunately, it is extremely difficult to maintain quantum state coherence for more than very short periods of time. Given that a substantial amount of time is needed to set up the superposition of qubits, quantum computing may be infeasible in practice.

- Only a few problems have been exhibited for which quantum computation offers an advantage, although an effective quantum factorization algorithm could invalidate the RSA algorithm.