CSCI 2570
Introduction to Nanocomputing

Discrete Quantum Computation

John E Savage

November 27, 2007

What is Quantum Computation

It is very different kind of computation that depends on certain very special transformations of the internal state of a system.

The physical systems that encode quantum information must be isolated from destructive external influences, called “decoherence.”

Computation is done at the atomistic scale where the differences in energy levels is much larger than at the macroscopic level.

Error correction is possible but must be done without knowing the original or corrupted state of the system.

Not at all clear that quantum computation will be practical in our lifetimes. Nonetheless, the unusual nature of such computation makes it very much worth studying.

Classical Versus Quantum Computation

	Classical	**Quantum**
Data	Cbit	Qbit
Computing Elements	Gates	Unitary transformations
Outputs	Gate values	Measurements

Classical State

- State is linear combination of orthogonal functions. We use "ket" notation to represent binary data $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Classically, these are **Cbits**.

- Tensor notation used to represent k-tuple state.

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

Tensor Notation

- $$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \otimes \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \otimes \begin{pmatrix} z_0 \\ z_1 \end{pmatrix} = \begin{pmatrix} x_0y_0z_0 \\ x_0y_0z_1 \\ x_0y_1z_0 \\ x_0y_1z_1 \\ x_1y_0z_0 \\ x_1y_0z_1 \\ x_1y_1z_0 \\ x_1y_1z_1 \end{pmatrix}.$$

  E.g. $|1\rangle\,|0\rangle\,|1\rangle = |101\rangle = |5\rangle_3 = (00000100)^T$, a 1 in 5th position.

- The subscript 3 on $|5\rangle_3$ indicates that 5 is represented by 3 bits.

Classical Computation

- Observation of a classical state component (bit) 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.

Reversible and Irreversible Computation

- Quantum computations, transformations of state, are *reversible*.
- Most classical computations are *irreversible*, e.g. ERASE sets a bit to 0, AND combines two values to one value.
- NOT, denoted by operator $\mathbf{X}$, is reversible.

$$\mathbf{X} : |x\rangle \mapsto |\tilde{x}\rangle\,; \quad \tilde{1} = 0,\ \tilde{0} = 1$$

Let $\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Then $\mathbf{X}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $\mathbf{X}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, and $\mathbf{X}^2 = \mathbf{1}$.

Swap – A Reversible Operation on Multiple Bits

- Swap i and j, S_{ij}, interchanges states of Cbits i and j. $S_{10}\,|xy\rangle = |yx\rangle$ exchanges $|01\rangle = |1\rangle_2$ and $|10\rangle = |2\rangle_2$ but leaves $|00\rangle = |0\rangle_2$ and $|11\rangle = |3\rangle_2$ unchanged. Thus,

$$S_{10} = S_{10} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Control-NOT (c-NOT) – A Reversible Operation

- Control-NOT, C_{ij}, flips the value of the jth *target bit* if the ith *control bit* has value $|1\rangle$ but leaves it unchanged if the control bit is $|0\rangle$.

$$C_{10}\,|x\rangle\,|y\rangle = |x\rangle\,|y \oplus x\rangle\,; \quad C_{01}\,|x\rangle\,|y\rangle = |x \oplus y\rangle\,|y\rangle$$

$\oplus$ is addition modulo-two. C_{10} has no effect on $|00\rangle = |0\rangle_2$ or $|01\rangle = |1\rangle_2$ but changes $|10\rangle = |2\rangle_2$ to $|3\rangle_2$ and $|11\rangle = |3\rangle_2$ to $|2\rangle_2$. Thus,

$$C_{10} = \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right), \quad C_{01} = \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{array}\right)$$

Reversible 2-Cbit Tensor Operators

- It is common to form a 2-Cbit operator through the tensor product of two 1-Cbit operators.

$$(\mathbf{a} \otimes \mathbf{b})\,|xy\rangle = (\mathbf{a} \otimes \mathbf{b})(|x\rangle \otimes |y\rangle) = \mathbf{a}\,|x\rangle \otimes \mathbf{b}\,|y\rangle$$

Let $\mathbf{1}\ \mathbf{a}\ \mathbf{1}\ \mathbf{b}$ denote that $\mathbf{b}$ is applied to the rightmost (zeroth) Cbit and $\mathbf{a}$ to the third Cbit from the right. The shorthand for this is $\mathbf{a}_2\,\mathbf{b}_0$.

Qbits and Their States

- Cbits have two possible states, the two orthonormal vectors $|0\rangle$ and $|1\rangle$.

- Qbits have have an uncountable number of states. The state $|\psi\rangle$ of a Qbit is a **unit vector** that is the complex combination (**superposition**) of $|0\rangle$ and $|1\rangle$, two orthonormal vectors, via complex numbers α_0 and α_1 (**amplitudes**) satisfying $|\alpha_0|^2 + |\alpha_1|^2 = 1$. ($|\psi\rangle$ lies on **Bloch sphere**.)

$$|\psi\rangle = \alpha_0 \,|0\rangle + \alpha_1 \,|1\rangle$$

Note: $\alpha = u + iv$ is a complex number where u and v are reals and $i = \sqrt{-1}$. The complex conjugate of α is $\alpha^\dagger = u - iv$. Its magnitude square is $\alpha\alpha^\dagger = |\alpha|^2 = u^2 + v^2$.

Comments on Quantum States

- Qbits don't have values but they are associated with states. A Qbit can have state $|0\rangle$ or $|1\rangle$ but which is not known until a measurement is made. (More on this later.)

- The state of two Qbits is the superposition of four orthogonal states

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle$$

  where $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$.

- n Qbits have state $|\psi\rangle = \sum_{0 \le x < 2^n} \alpha_x\,|x\rangle_n$ where $\sum_{0 \le x < 2^n} |\alpha_x|^2 = 1$.

Entanglement of Qbits

- Let $|\psi\rangle = \mu_0 |0\rangle + \mu_1 |1\rangle$ and $|\phi\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$ be two Qbits. Their tensor product $|\Psi\rangle = |\psi\rangle \otimes |\phi\rangle$ is given below. This state is **separable**.

$$\begin{aligned} |\Psi\rangle &= (\mu_0 |0\rangle + \mu_1 |1\rangle) \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle) \\ &= \mu_0\beta_0 |00\rangle + \mu_0\beta_1 |01\rangle + \mu_1\beta_0 |10\rangle + \mu_1\beta_1 |11\rangle \end{aligned}$$

  Comparing this expansion with one in previous slide, we have that $\alpha_{00} = \mu_0\beta_0$, $\alpha_{01} = \mu_0\beta_1$, $\alpha_{10} = \mu_1\beta_0$, and $\alpha_{11} = \mu_1\beta_1$. Clearly, $\alpha_{00}\alpha_{11} = \alpha_{10}\alpha_{01}$. Because this constraint is not generally satisfied by a 2-Qbit system, it follows that such a system is different from the composition of two 1-Qbit systems.

  The states of the Qbits in the 2-Qbit system are **entangled**.

Quantum Observation

- Observation of a quantum state components collapses the state to a classical state, that is, to one of the orthonormal vectors.

- An observation probabilistically samples the quantum state.
  - Observations at different times are likely to yield different results.
  - Frequency of outcomes is determined by state amplitudes.

- An **observation** of a quantum state $|\psi\rangle = \sum_{0 \le x < 2^n} \alpha_x \, |x\rangle$ produces a single classical state $|y\rangle$. State $|y\rangle$ occurs with probability $|\alpha_y|^2$.
  - Quantum states are **fragile**; contact with the outside world represents an observation. Unwanted measurements are called **decoherence**.

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 Qbit reveals that the basis state is $|00\rangle$ or $|11\rangle$. Whatever the outcome, the measurement of the second Qbit will give the same result as the measurement of the first Qbit.

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

- This does not imply communication faster than light because it does not imply that one observer knows when the other makes a measurement.

Quantum Computations

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

- The operation $\mathbf{U}\,|\phi\rangle$ maps the underlying orthonormal basis used in $|\phi\rangle$ to a new basis.

Dirac Notation

- $|x\rangle$ is called "ket" and denotes a column vector.

- $\langle x|$ is called "bra" and denotes a row vector.

- The normalization condition $\sum_{0 \leq x < 2^n} |\alpha_x|^2 = 1$ can be restated as $\langle \psi^\dagger| \, |\psi\rangle = \langle \psi^\dagger|\psi\rangle$.

- Because the normalization condition $\langle \psi^\dagger| \, |\psi\rangle\rangle = \langle \phi^\dagger| \, U^\dagger U \, |\phi\rangle = 1$ 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 (unitary) 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 $(\boldsymbol{x}, f(\boldsymbol{x}))$.

Qbit Analogs of NOT

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

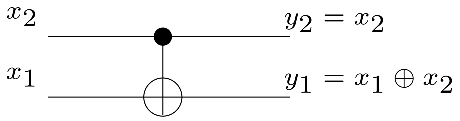
Quantum Observations

- A measurement produces a basis vector in an orthonormal system. Since $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ are orthonormal, a measurement in this basis will produce a different value than one in the basis $(|0\rangle, |1\rangle)$. Let $|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. Since

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

A measurement in the new basis produces $|+\rangle$ or $|-\rangle$ with probability $|\alpha+\beta|^2/2$ and $|\alpha-\beta|^2/2$, respectively.

Qbit 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

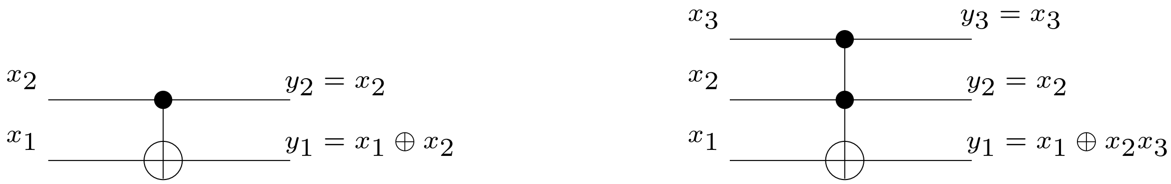
- The control-NOT is the quantum equivalent of the EXOR. EXOR does a reversible computation, unlike NAND. Wires model passage of time or physical movement of a particle. Operations model interactions.

- The control-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

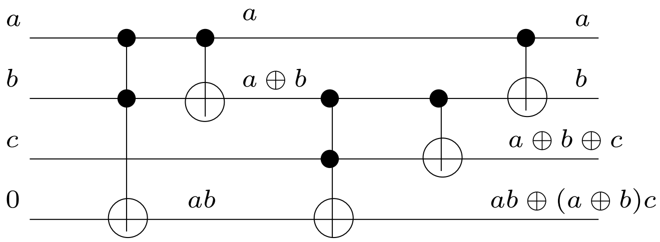


The control-NOT and control-control-NOT gates

- 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?)
  - c-NOT and single Qbit gates form a **universal basis for quantum computation**.

- Reversibility increases circuit size for $f : \{0,1\}^n \mapsto \{0,1\}$ by $O(n^{\log_2 3})$.

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

- 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-Qbit 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 $(|0\rangle + |1\rangle)/\sqrt{2} \times |0\rangle$.

- $(|0\rangle + |1\rangle)/\sqrt{2} \times |0\rangle$ is separable.

Quantum Computation of a Binary Function

- A reversible quantum computation of $f : \{0,1\}^n \mapsto \{0,1\}^m$ can be done with an n-Qbit input state $|x\rangle$ and an m-Qbit output state $|f(x)\rangle$ via the unitary operator $\mathbf{U}_f$ shown below.

$$\mathbf{U}_f(|x\rangle_n |y\rangle_m) = |x\rangle_n |y \oplus f(x)\rangle_m$$

Note that $\mathbf{U}_f$ is its own inverse, i.e. $\mathbf{U}_f \mathbf{U}_f = \mathbf{1}$.

Superposition of all Basis States

- Given the tensor product of two Qbits, the following trick generates the superposition of all 2-Qbit basis states.

$$
\begin{aligned}
(\mathbf{H} \otimes \mathbf{H})(|0\rangle \otimes |0\rangle) &= \mathbf{H}_1\mathbf{H}_0\,|0\rangle\,|0\rangle = (\mathbf{H}\,|0\rangle)(\mathbf{H}\,|0\rangle) \\
&= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
&= \frac{1}{2}(|0\rangle\,|0\rangle + |0\rangle\,|1\rangle + |1\rangle\,|0\rangle + |1\rangle\,|1\rangle) \\
&= \frac{1}{2}(|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2)
\end{aligned}
$$

Superposition of all Basis States

- Let $\mathbf{H}^{\otimes n}$ denote $\mathbf{H} \otimes \mathbf{H} \otimes \cdots \otimes \mathbf{H}$, n times.

$$\begin{aligned}
\mathbf{U}_f(\mathbf{H}^{\otimes n}) \left|0\right\rangle_n \left|0\right\rangle_m &= \frac{1}{2^{n/2}} \sum_{0 \le x < 2^n} \mathbf{U}_f(\left|x\right\rangle_n \left|0\right\rangle_m) \\
&= \frac{1}{2^{n/2}} \sum_{0 \le x < 2^n} \left|x\right\rangle_n \left|f(x)\right\rangle_m
\end{aligned}$$

This calculation exhibits **quantum parallelism**.

Example of a Quantum Computation

- Build a circuit $\mathbf{U}_f$ 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 tells if f is a constant function or not. Classically this requires two tests. Deutch's algorithm does it with one query.

Deutch's Problem

- Given $f : \{0,1\} \mapsto \{0,1\}$, is $f(0) = f(1)$ or not? This takes two classical measurements. It can be done with one quantum measurement.

- The four functions of this type are shown below where $\mathbf{X}$ is NOT, $\mathbf{C}_{io}$ is c-NOT, and $\mathbf{C}_{io}\mathbf{X}_0$ denotes the application of $\mathbf{X}_0$ followed by $\mathbf{C}_{io}$.

	$x = 0$	$x = 1$	
f_0	0	0	$\mathbf{U}_{f_0} = \mathbf{1}$
f_1	0	1	$\mathbf{U}_{f_1} = \mathbf{C}_{io}$
f_2	1	0	$\mathbf{U}_{f_0} = \mathbf{C}_{io}\mathbf{X}_0$
f_3	1	1	$\mathbf{U}_{f_0} = \mathbf{X}_0$

Deutch's Algorithm

$$
\begin{aligned}
(\mathbf{H} \otimes \mathbf{H})(\mathbf{X} \otimes \mathbf{X})(|0\rangle\,|0\rangle) &= (\mathbf{H} \otimes \mathbf{H})(|1\rangle\,|1\rangle) \\
&= (\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)) \\
&= \frac{1}{2}(|0\rangle\,|0\rangle - |1\rangle\,|0\rangle - |0\rangle\,|1\rangle + |1\rangle\,|1\rangle)
\end{aligned}
$$

Applying $\mathbf{U}_f$ to this gives the following.

$$
\frac{1}{2}(\mathbf{U}_f(|0\rangle\,|0\rangle) - \mathbf{U}_f(|1\rangle\,|0\rangle) - \mathbf{U}_f(|0\rangle\,|1\rangle) + \mathbf{U}_f(|1\rangle\,|1\rangle))
$$

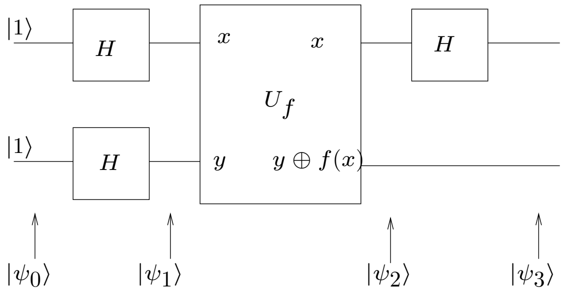
Deutch's Algorithm

$$\frac{1}{2}(\mathbf{U}_f(|0\rangle\,|0\rangle) - \mathbf{U}_f(|1\rangle\,|0\rangle) - \mathbf{U}_f(|0\rangle\,|1\rangle) + \mathbf{U}_f(|1\rangle\,|1\rangle))$$
$$= \frac{1}{2}(|0\rangle\,|f(0)\rangle - |1\rangle\,|f(1)\rangle - |0\rangle\,|\tilde{f}(0)\rangle + |1\rangle\,|\tilde{f}(1)\rangle)$$

When $f(0) = f(1)$ and $f(0) \neq f(1)$ (which implies $f(1) = \tilde{f}(0)$ and $\tilde{f}(1) = f(0)$), we have the following where

$f(0) = f(1)$	$f(0) \neq f(1)$
$\frac{1}{2}(\|0\rangle - \|1\rangle)(\|f(0)\rangle - \|\tilde{f}(0)\rangle)$	$\frac{1}{2}(\|0\rangle + \|1\rangle)(\|f(0)\rangle - \|\tilde{f}(0)\rangle)$

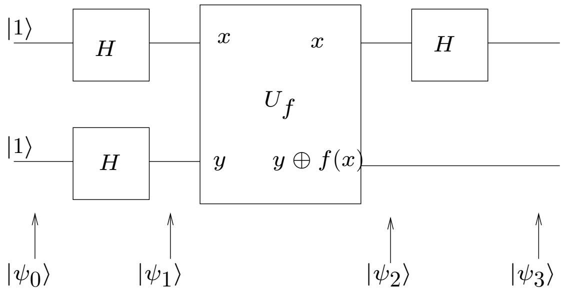
Deutch's Algorithm



If we apply the Hadamard transform to the leftmost Qbit, we have $\mathbf{H}(|0\rangle - |1\rangle) = |0\rangle$ and $\mathbf{H}(|0\rangle + |1\rangle) = |1\rangle$. The result is shown below.

$$
\begin{aligned}
&(\mathbf{H} \otimes \mathbf{1})\mathbf{U}_f(\mathbf{H} \otimes \mathbf{H})(\mathbf{X} \otimes \mathbf{X})(|0\rangle\,|0\rangle) \\
&\quad = \begin{cases} |1\rangle\,\frac{1}{2}(|f(0)\rangle - |\tilde{f}(0)\rangle), & f(0) = f(1) \\ |0\rangle\,\frac{1}{2}(|f(0)\rangle - |\tilde{f}(0)\rangle), & f(0) \neq f(1) \end{cases}
\end{aligned}
$$

Deutch's Algorithm



- Quantum computation has provided global information about $f(x)$, namely, $f(0) \oplus f(1)$, in one step, namely, the computation by $\mathbf{U}_f$. 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 intially.
  - 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
- Factorization 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 Qbits be maintained for a long enough for a computation to complete. If a quantum states 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 Qbits, 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.