Quantum Computing

Subhashis Banerjee
Department of Computer Science and Engineering
IIT Delhi

suban@cse.iitd.ernet.in

April 15, 2006

Computer programming is an art form, like the creation of poetry or music - Donald Knuth

If computers that you build are quantum,
Then spies everywhere will all want 'em.
Our codes will all fail,
And they'll read our email,
Till we get crypto that's quantum, and daunt 'em.

- Jennifer and Peter Shor

To read our E-mail, how mean
of the spies and their quantum machine;
be comforted though,
they do not yet know
how to factorize twelve or fifteen.

- Volker Strassen

Early algorithms

$$n! = \begin{cases} 1 & \text{if } n = 0 \\ n \times \underline{(n-1)!} & \text{otherwise} \end{cases}$$

$O(n)$ multiplications. Euclid's *Elements*. 300 BC.

$$gcd(m,n) = \begin{cases} m & \text{if } n = 0 \\ \underline{gcd(n, m \; mod \; n)} & \text{otherwise} \end{cases}$$

$O(\log n)$ steps. Euclid's *Elements*. 300 BC.

Early algorithms

$$x^n = \begin{cases} 1 & \text{if } n = 0 \\ x \times \underline{x^{n-1}} & \text{otherwise} \end{cases}$$

$O(n)$ multiplications. Dates back to the Egyptians. 2000 BC.

$$x^n = \begin{cases} 1 & \text{if } n = 0 \\ x \times sqr(\underline{x^{n/2}}) & \text{if } odd(x) \\ sqr(\underline{x^{n/2}}) & \text{if } even(x) \end{cases}$$

$O(\log n)$ multiplications. Acharya Pingala in *Chandah Sutra*. 200 BC.

Models of computation

Recursive functions: Inductively defined functions $f : \mathbb{N}^n \rightarrow \mathbb{N}$

RAM model: Any programming language that supports **assignment**, **if-then-else**, **while-do**, an infinite array, 0 and $s \leftarrow s+1$.

Turing machine: A mathematical model due to Alan Turing (1936). Consists of an **infinite tape**, a **finite state control**, a **read-write head** and **a program**.

Circuit model: *Acyclic* logic circuits of n input bits consisting of *NAND*, *FANOUT* and *CROSSOVER*; whose description can be generated by a *Turing machine*.

Church-Turing thesis

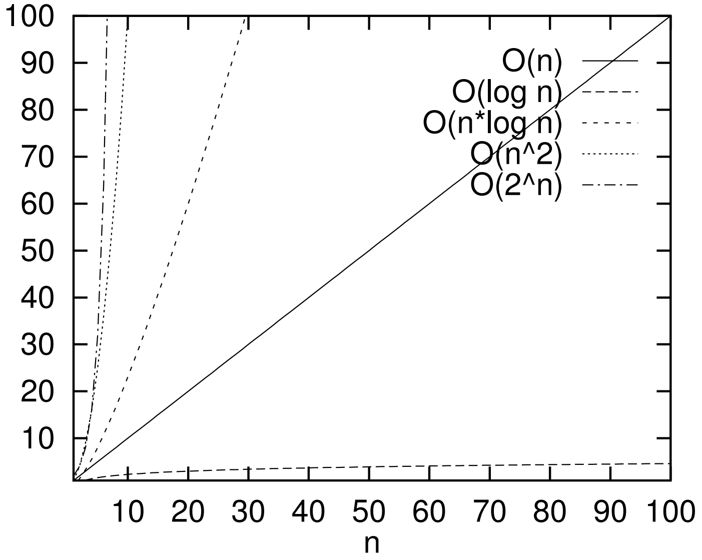
- All reasonable models of computations have turned out to be equivalent in terms of what they can compute.
- There can be a **Universal Turing machine** which can be used to simulate any Turing machine.
- The Universal Turing machine completely captures what it means to perform a computational task by algorithmic means.

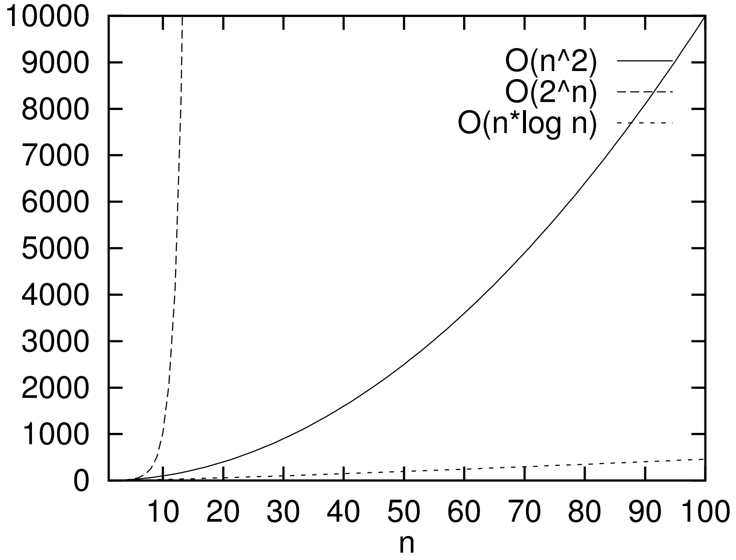
The above has led to the assertion called the **Church-Turing thesis:**

If an algorithm can be performed on any piece of hardware (including a modern computer) then there is an equivalent algorithm for a Universal Turing machine which performs the same task.

What about efficiency?

- Roughly speaking, an efficient algorithm is one which runs in time **polynomial** in the size of the input.
- In contrast, an inefficient algorithm takes super-polynomial (typically exponential) time.



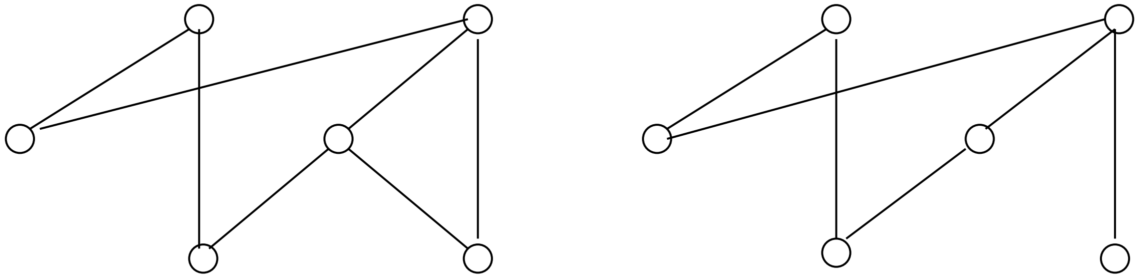


- Strengthened version of **Church-Turing thesis:** Any algorithmic process can be simulated **efficiently** using a Turing machine.

Decision problems and complexity classes

Decision problems:

- Given a composite integer m and $l < m$, does m have a non-trivial factor less than l?
- Does a given graph have a Hamiltonian cycle?



Complexity classes:

- **P** is the class of decision problems that a UTM can solve in polynomial time.
- **NP** is the class of decision problems whose solutions a UTM can verify in polynomial time.

Does “coin toss” help?

- Consider a function $f : \{0, \ldots, 2^{n-1}\} \to \{0, 1\}$.
- Suppose we are given that $f(x)$ is either *constant* (0 or 1 for all values of x) or *balanced* (0 for exactly half for all possible x and 1 for the other half).
- Our problem is to decide what type f is?
- Clearly, any deterministic algorithm will take at least $2^{n-1} + 1$ queries in the worst case.
- Alternatively, we can choose k (fixed) values of x *uniformly at random*. If $f(x)$ is different for any two conclude *balanced*, else conclude *constant*. In the later case there is a non-zero probability of error, equal to 2^{-k}.
- The probability bound is arbitrary. *Chernoff bound* can be used to amplify the probability to near 0 with only a few (logarithmic) repetitions.

Randomized algorithms

- Solovay and Strassen showed, in mid 1970's, that a *randomized algorithm* could determine whether a number n is a prime (with an arbitrarily low probability 2^{-k}) or a composite (with certainty) in $O(k \log^3 n)$ time.
- *No efficient deterministic algorithm was known for the problem till Manindra Agarwal et. al. in 2003.*
- Strengthened version of **Church-Turing thesis:** Any algorithmic process can be simulated **efficiently** using a *probabilistic* Turing machine.
- **BPP** is the class of problems that can solved *efficiently* using a probabilistic TM.

What is (not) known about complexity?

- Some other complexity classes: **L**, **PSPACE**, **EXP**.
- It is known that $\mathbf{L} \subseteq \mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{PSPACE} \subseteq \mathbf{EXP}$.

  $\boxed{\text{Is } \mathbf{P} = \mathbf{NP}\text{?}}$

- It is also known that $\mathbf{P} \subset \mathbf{EXP}$ and $\mathbf{L} \subset \mathbf{PSPACE}$. Hence at least one of the inclusions above must be strict. Which one?
- Also, clearly, $\mathbf{P} \subseteq \mathbf{BPP}$
- If an **NP**-Complete problem can be solved in time t, then all problems in **NP** can be solved in time $poly(t)$.
- Where does *Quantum* fit in?
- $\mathbf{P} \subseteq \mathbf{BQP} \subseteq \mathbf{PSPACE}$

Quantum bits

- Two possible states $|0\rangle$ and $|1\rangle$.
- A *qubit* can also be in a linear combination (superposition) of states

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \alpha, \beta \in \mathbb{C} \quad \text{and} \quad |\alpha|^2 + |\beta|^2 = 1$$

- Thus, a *qubit* is a vector in a 2D vector space over the complex field.
- $|0\rangle$ and $|1\rangle$ are called *computational basis states*. They form an orthonormal basis.
- We cannot examine a *qubit* to determine its state. That is, we cannot measure α and β. **States are unobservable**.
- When we measure we get $|0\rangle$ with probability $|\alpha|^2$ or $|1\rangle$ with probability $|\beta|^2$. **Measurement collapses the system to one of the basis states**.
- *qubit*'s are decidedly real.

How much information in a qubit*?*

- Infinite number of points on the surface of a sphere. Representation of a state will require infinite number of bits. Can we store the entire *Mahabharat* in a *qubit*?
- *Misleading*, because measurement will collapse the state to either $|0\rangle$ or $|1\rangle$. Only one bit of information from a measurement.
- But how much information if we do not measure?
- Trick question. But it appears that when nature evolves *closed quantum systems* it maintains all continuous variable. *Key to quantum computation*.
- *qubit* states can be manipulated and transformed in interesting ways that can lead to meaningful measurement outcomes.

Multiple qubits

- For two classical bits we can have four states 00, 01, 10 and 11.
- Correspondingly, for a 2 *qubit* system we have four computational basis states: $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$.
- The 2 *qubit* state is
  $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \sum_{x\in\{0,1\}^2} \alpha_x|x\rangle$
- We could measure only the first *qubit*. If we get $|0\rangle$ *wp* $|\alpha_{00}|^2 + |\alpha_{01}|^2$, the post measurement state is $|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2+|\alpha_{01}|^2}}$
- Tensor product of two vector spaces V (dimension k) and W (dimension l) is $V\otimes W$ (dimension kl). If $|v_1\rangle|v_2\rangle\ldots|v_k\rangle$ and $|w_1\rangle|w_2\rangle\ldots|w_l\rangle$ are the bases for V and W, then a basis for $V\otimes W$ is
  $\{|v_i\rangle\otimes|w_j\rangle : 1\le i\le k, 1\le j\le l\}$.
- *Hilbert space is a very large space*. Nature somehow finds extra storage when we combine two subsystems.

Entangled states

- A fantastic 2 *qubit* state is the *Bell state* or *EPR pair*

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

- There are no single *qubit* states $|a\rangle$ and $|b\rangle$ such that $|\psi\rangle = |ab\rangle$.
- On measuring the first *qubit* we get $|0\rangle$ or $|1\rangle$ with equal probability.
- Post measurement state is $|\psi'\rangle = |00\rangle$ or $|\psi'\rangle = |11\rangle$. Measurement of the second *qubit* gives *exactly* the same result as the first.
- The two *qubits* are *correlated* or *entangled*.
- The measurement correlations in the *Bell state* is stronger than could exist in two components of any classical system.
- Another key component of quantum computing.

Quantum computation

- In the *classical circuit model* computational algorithms are described by wires and logic gates (*NAND*).
- Only one non-trivial 1 bit gate - *NOT*.
- Quantum analogue: $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|1\rangle + \beta|0\rangle$ (the quantum *NOT* acts linearly).
- Can be represented by a matrix

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

- All quantum gates U must be *unitary operators*: $U^{\dagger}U = I$.
- Quantum operations are reversible.

Important single qubit gates

- Pauli matrices:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}; \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix};$$

- Hadamard:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

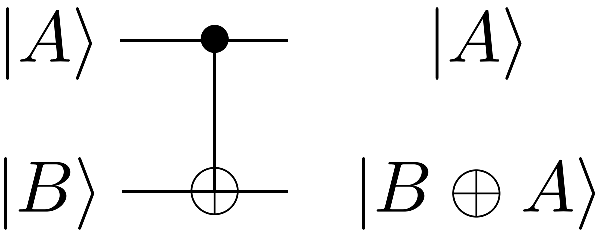
$$\alpha|0\rangle + \beta|1\rangle \;-\!\!-\!\!\boxed{H}\!\!-\!\!-\; \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

$$|0\rangle \;-\!\!-\!\!\boxed{H}\!\!-\!\!-\; \frac{|0\rangle+|1\rangle}{\sqrt{2}}$$

$$|1\rangle \;-\!\!-\!\!\boxed{H}\!\!-\!\!-\; \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

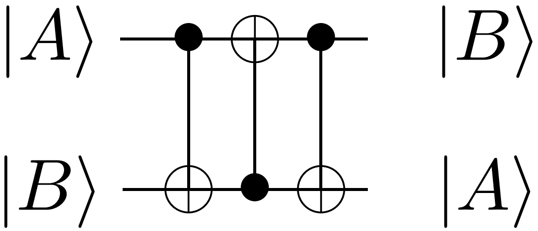
Multiple qubit *gates*

Controlled NOT (*CNOT*)



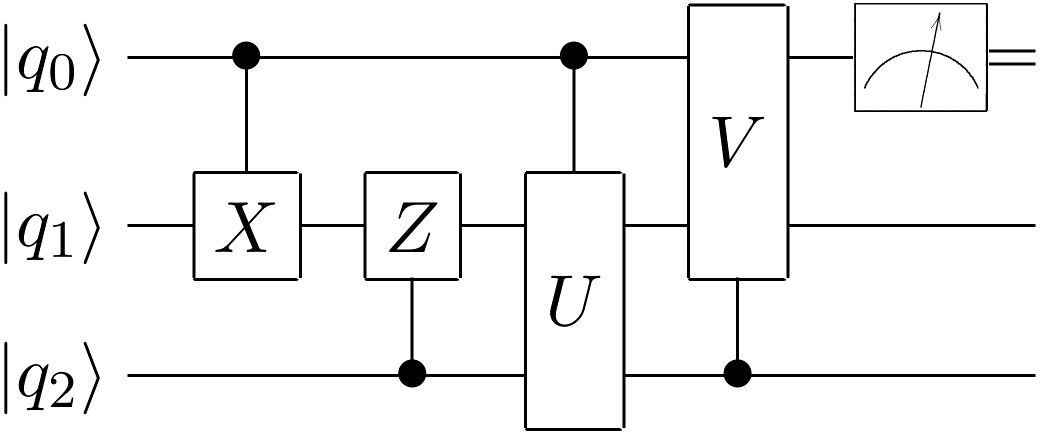
$$|00\rangle \rightarrow |00\rangle; \;\; |01\rangle \rightarrow |01\rangle;$$
$$|10\rangle \rightarrow |11\rangle; \;\; |11\rangle \rightarrow |10\rangle$$

Swap



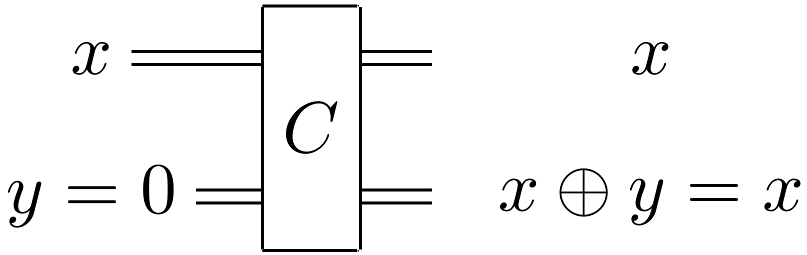
$$\begin{aligned} |A,B\rangle &\rightarrow |A, A \oplus B\rangle \\ &\rightarrow |A \oplus (A \oplus B), A \oplus B\rangle = |B, A \oplus B\rangle \\ &\rightarrow |B, ((A \oplus B) \oplus B\rangle = |B, A\rangle \end{aligned}$$

A typical quantum circuit

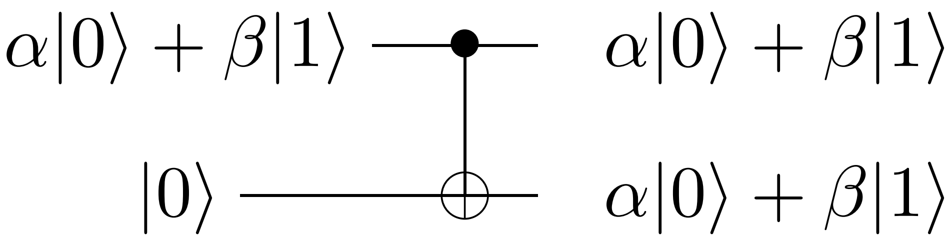


Quantum copying?

Classical cloning



Quantum cloning?


$\alpha|0\rangle + \beta|1\rangle$
$|0\rangle$
$\alpha|0\rangle + \beta|1\rangle$
$\alpha|0\rangle + \beta|1\rangle$

$$[\alpha|0\rangle + \beta|1\rangle]\,|0\rangle = \alpha|00\rangle + \beta|10\rangle \rightarrow \alpha|00\rangle + \beta|11\rangle$$

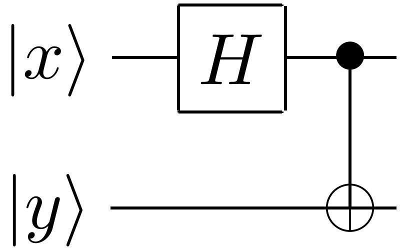
Have we cloned? For a general state $\psi = \alpha|0\rangle + \beta|1\rangle$,

$$|\psi\rangle\,|\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$$

Actually quantum cloning is not possible

Bell states

- Use *Hadamard* and *CNOT*

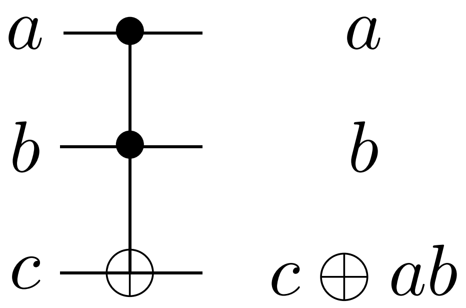


-

$$\begin{aligned}
|00\rangle &\rightarrow (|00\rangle + |11\rangle)/\sqrt{2} = \beta_{00} \\
|01\rangle &\rightarrow (|01\rangle + |10\rangle)/\sqrt{2} = \beta_{01} \\
|10\rangle &\rightarrow (|00\rangle - |11\rangle)/\sqrt{2} = \beta_{10} \\
|11\rangle &\rightarrow (|01\rangle - |10\rangle)/\sqrt{2} = \beta_{11}
\end{aligned}$$

Classical computation on quantum machines: Toffoli gates

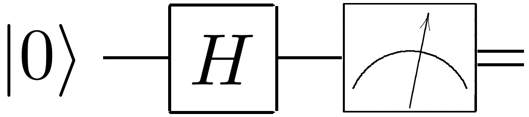
- Any classical computation can be realized by logic circuits consisting *NAND* gates, *FANOUT* and *CROSSOVER*.
- Reversible quantum gates can realize the above:



-

$$\begin{aligned} (a,b,1) &\rightarrow (a,b,1\oplus\neg(ab)) = \neg(ab) \\ (1,b,0) &\rightarrow (1,b,b) \end{aligned}$$

- What about coin toss?



Classical computation on quantum machines: clean-up

- We have that $(x,a) \longrightarrow (f(x), g(x))$
- We have *CNOT*, so we can create a as needed $(x,0) \longrightarrow (f(x), g(x))$
- We can also use *CNOT* to create a copy of x, not to be changed later

$$(x,0,0) \longrightarrow (x, f(x), g(x))$$

- Suppose we start with a fourth register also

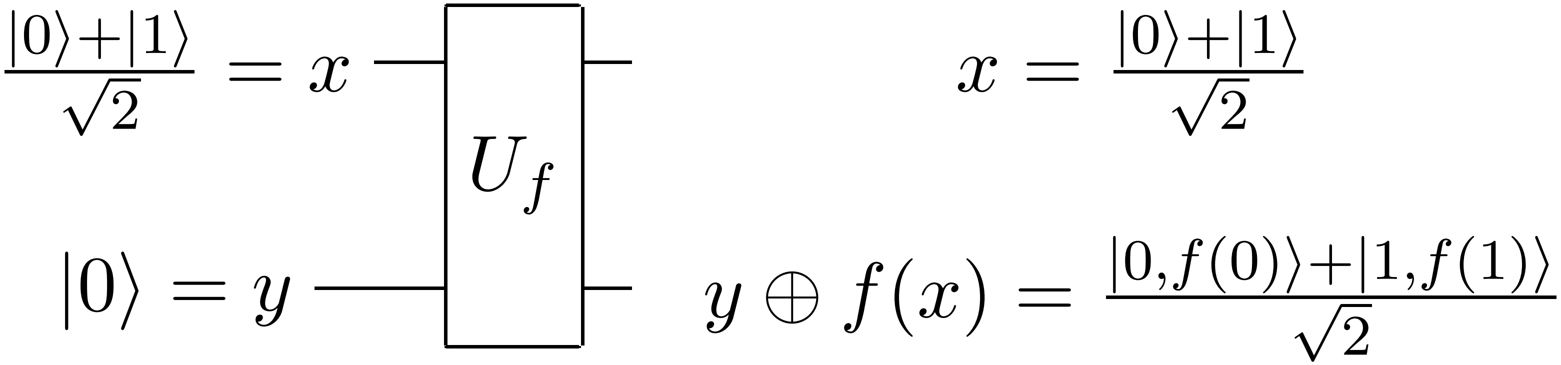
$$(x,0,0,y) \longrightarrow (x, f(x), g(x), y)$$

- Use *CNOT* to add $f(x)$ to the fourth register leaving the machine in state

$$(x, f(x), g(x), y \oplus f(x))$$

- Using the circuit to reverse $f(x)$, we obtain $(x,0,0,y \oplus f(x))$
- Write the action of the circuit as $(x,y) \longrightarrow (x, y \oplus f(x))$
- Only polynomial overheads. $\mathbf{P} \subseteq \mathbf{BQP}$.

Quantum parallelism

- 

$$\frac{|0\rangle+|1\rangle}{\sqrt{2}} = x$$

$$|0\rangle = y$$

$$U_f$$

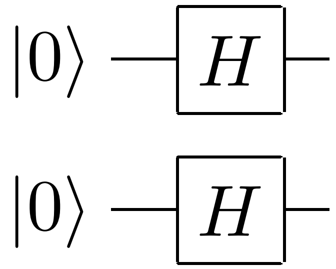
$$x = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$$

$$y \oplus f(x) = \frac{|0,f(0)\rangle+|1,f(1)\rangle}{\sqrt{2}}$$

- A single $f(x)$ circuit can evaluate the function at multiple values of x.
- Input and output *entangled*.
- What can we do with this?

Extension to multiple qubits

- Parallel action of two *Hadamard* gates: $H^{\otimes 2}$



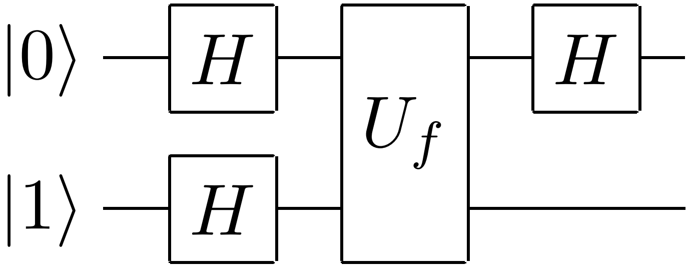
$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

- More generally, the result of performing *Hadamard* on *n qubits* initially all in $|0\rangle$ state is $(H^{\otimes n})$

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

- *Extremely efficient*: n gates produce equal superposition of 2^n states.

Deutsch's algorithm



- $\left|\psi_0\right\rangle = \left|01\right\rangle$; $\left|\psi_1\right\rangle = \left[\frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle)\right]\left[\frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle)\right]$
- Applying U_f to the state $\left|x\right\rangle(\left|0\right\rangle - \left|1\right\rangle)/\sqrt{2}$ we obtain

$$\begin{aligned} & \left|x\right\rangle(\left|0 \oplus f(x)\right\rangle - \left|1 \oplus f(x)\right\rangle)/\sqrt{2} \\ = \;& \left|x\right\rangle(\left|f(x)\right\rangle - \left|1 \oplus f(x)\right\rangle)/\sqrt{2} \\ = \;& (-1)^{f(x)}\left|x\right\rangle(\left|0\right\rangle - \left|1\right\rangle)/\sqrt{2} \end{aligned}$$

-

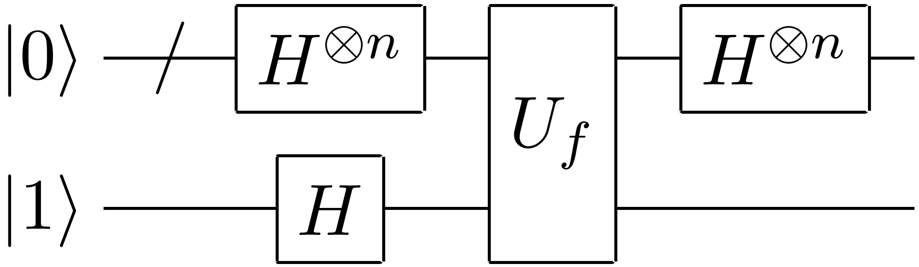
$$\left|\psi_2\right\rangle = \begin{cases} \pm\left[\frac{\left|0\right\rangle + \left|1\right\rangle}{\sqrt{2}}\right]\left[\frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm\left[\frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}\right]\left[\frac{\left|0\right\rangle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

Deutsch's algorithm

- After the final *Hadamard*

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

- $|\psi_3\rangle = \pm|f(0)\oplus f(1)\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$
- Measuring first *qubit* gives $f(0)\oplus f(1)$. Only one evaluation of $f(x)$.
- Faster than is possible with any classical apparatus.
- Can easily be extended to n bits



Other results

- Peter Shor (1994) gave an $O(n^3)$ quantum algorithm for *factoring* an n bit number. The best known classical algorithm for the problem is *number field sieve* which works in $exp(O(n^{1/3}\log^{2/3} n))$.
- Lov Grover (1995) gave an $O(\sqrt{n})$ quantum algorithm for *search* in an *unstructured search space* of size n.
- If an $O(\log n)$ algorithm could be found for search it would have established that **NPC** problems can be solved efficiently on quantum computers.

  Not to be - Grover's algorithm has been proved to be optimal.
- $\boxed{\text{Is } \mathbf{P} \subset \mathbf{BQP}?}$.

Some wisdom

“All of this will lead to theories [of computation] which are much less rigidly of an all-or-none nature than past and present formal logic. They will be of a much less combinatorial, and much more analytical, character. In fact, there are numerous indications to make us believe that this new system of formal logic will move closer to another discipline that has been little linked in the past with logic. This is thermodynamics, primarily in the form it was received from Boltzmann, and is that part of theoretical physics which comes nearest in some of its aspects to manipulating and measuring information”

- John Von Neumann, Collected Works, *Vol. 5, pg. 304.*