What is a Quantum Computer?

A quantum computer is a physical system designed to take advantage of quantum phenomena in carrying out a computational task.

The distinguishing features of a quantum computer are

- At any time the computer can be in a superposition of all possible machine states. This gives quantum computing the potential power of proceeding through all computational paths simultaneously.

- Between measurements, the machine state evolves unitarily. This restricts the power of quantum computing. Only reversible computations are possible.

- At the time of measurement, the probability of a certain outcome is determined by adding the amplitudes of all paths that lead to that outcome and then squaring the absolute value of the sum.

Computational power

- Quantum computers cannot compute anything non-computable by classical computers.

- Quantum computation may have enormous speed advantages over classical computers in solving certain problems.

  Example: Classical complexity of factoring an n digit number is

  $$\exp[1.9(\ln n)^{1/3}(\ln\ln n)^{2/3}]$$

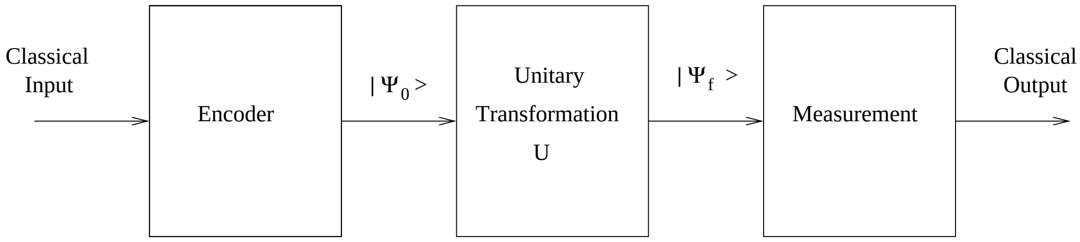
  Complexity of Shor's 1994 quantum algorithm

  $$(\ln n)^3$$

  An exponential improvement in the running time.

- QC's first proposed by Feynman in 1982 for simulation of quantum systems. 100 photons require processing $2^{100} \sim 10^{30}$ complex numbers, impossible task for a classical machine.

Elements of Quantum Computation



- Begin in some initial state $|\Psi_0\rangle$ of the machine that encodes the program input in some form.

- Apply a unitary transformation U to the machine state as directed by the program to reach a final state $|\Psi_f\rangle$.

- Perform a measurement on $|\Psi_f\rangle$ and print the result.

Quantum computation inherently probabilistic due to the randomness of the measurement outcome.

Qubit

A qubit is a two-dimensional quantum system

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

where

$$|\alpha|^2 + |\beta|^2 = 1.$$

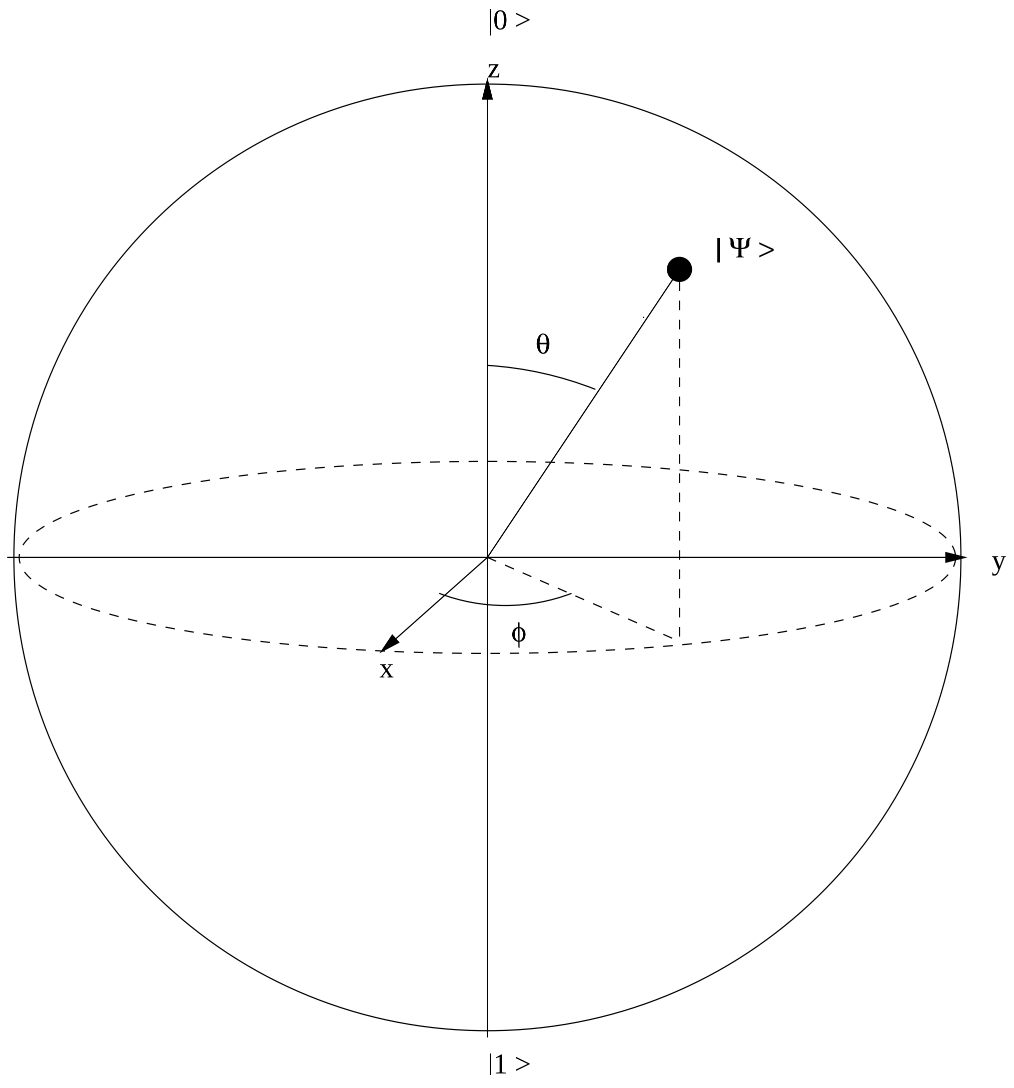
If we 'measure' the qubit in the measurement basis, the result equals $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$.

Bloch Sphere

A qubit can be written in the form

$$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

and visualized as a point on the 'Bloch' sphere.



Multiple Qubits

For two qubits, the state space is 4 dimensional

$$
\begin{aligned}
|0\rangle &= |00\rangle = |0\rangle \otimes |0\rangle \\
|1\rangle &= |01\rangle = |0\rangle \otimes |1\rangle \\
|2\rangle &= |10\rangle = |1\rangle \otimes |0\rangle \\
|3\rangle &= |11\rangle = |1\rangle \otimes |1\rangle
\end{aligned}
$$

For n qubits, state-space is 2^n dimensional with basis vectors

$$|i\rangle = |i_1 i_2 \cdots i_n\rangle = |i_1\rangle \otimes \cdots \otimes |i_n\rangle$$

where $0 \leq i \leq 2^n - 1$ is an integer and

$$i = 2^{n-1} i_1 + 2^{n-2} i_2 + \cdots + i_n$$

General state expansion in measurement basis:

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

where $\sum_i |a_i|^2 = 1$.

Measurements

Possible measurement outcomes for

$$\frac{1}{\sqrt{3}}(|00\rangle + |01\rangle - |11\rangle)$$

are 00, 01, or 11 with probability 1/3 each.

On outcome 00, state after the measurement collapses to

$$|00\rangle.$$

If we measure only the 1st qubit, possible outcomes are 0 with probability 2/3, and 1 with probability 1/3.

On measuring 0, the joint state collapses to

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle);$$

on outcome 1, state collapses to

$$|11\rangle.$$

Measurements (cont'd)

Another possible measurement on the state

$$\frac{1}{\sqrt{3}}(|00\rangle + |01\rangle - |11\rangle)$$

is

$$x_1 \oplus x_2$$

mod(2) sum of the values of the two qubits.

Possible outcomes: 0 and 1, with probabilities 2/3 and 1/3.

State after measuring 0 is

$$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

State after measuring 1 is

$$|01\rangle.$$

Single Qubit Gates

NOT gate X: Inverts $|0\rangle$ and $|1\rangle$.

$$X|0\rangle = |1\rangle$$
$$X|1\rangle = |0\rangle$$

Matrix representation of in the measurement basis

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

Linearity:

$$X(\alpha|0\rangle + \beta|1\rangle) = \alpha X|0\rangle + \beta X|1\rangle = \alpha|1\rangle + \beta|0\rangle$$

In matrix notation,

$$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}.$$

Hadamard Gate

$$H = \frac{1}{\sqrt{2}} \left[\begin{array}{rr} 1 & 1 \\ 1 & -1 \end{array} \right]$$

Transforms the measurement basis into the "cross-polarization" basis:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

and

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Bloch's Theorem

All single qubit operations can be synthesized in terms of the following elementary operations (Pauli spin matrices):

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

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Controlled–NOT

CNOT is a two-qubit gate:

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

$$|A, B\rangle \rightarrow |A, A \oplus B\rangle$$

Qubit A is called the control qubit.

CNOT in matrix form:

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Universality Theorem

The CNOT gate and single qubit gates are *universal*: Any multiple qubit gate can be synthesized to any desired degree of accuracy in terms of them.

The Hadamard Transform

Let $|x\rangle = |x_1, x_2, \ldots, x_n\rangle$ be a basis vector for an n-qubit system, such as $|00110\cdots010\rangle$.

Hadamard transform of $|x\rangle$ is defined as

$$H^{\otimes n}|x\rangle = H|x_1\rangle \otimes \cdots \otimes H|x_n\rangle$$

where

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

E.g., if we label the basis elements of a 2-qubit system as

$$\begin{aligned} |0\rangle &= |00\rangle = |0\rangle \otimes |0\rangle \\ |1\rangle &= |01\rangle = |0\rangle \otimes |1\rangle \\ |2\rangle &= |10\rangle = |1\rangle \otimes |0\rangle \\ |3\rangle &= |11\rangle = |1\rangle \otimes |1\rangle \end{aligned}$$

the Hadamard transform matrix in this basis is

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

The Hadamard Transform (cont'd)

Let $H_n = H^{\otimes n}$ denote the Hadamard transform for an n-qubit system. Then, if we label the basis states in lexicographic order,

$$H_{n+1} = \frac{1}{\sqrt{2^n}} \left[\begin{array}{cc} H_n & H_n \\ H_n & -H_n \end{array} \right]$$

It is easy to verify that

1. $H_n^2 = I_n$, i.e., H is unitary.

2. The Hadamard transform of $|0^n\rangle$ is the uniform superposition of all basis states

$$H_n|0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

3. The Hadamard transform of a general basis state $|x\rangle = |x_1, \ldots, x_n\rangle$ is given by

$$H_n|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} (-1)^{x \cdot z}|z\rangle$$

where the sum is over all states $|z\rangle = |z_1, \ldots, z_n\rangle$ and $x \cdot z = \sum_{i=1}^{n} x_i z_i$.

Deutsch's Problem

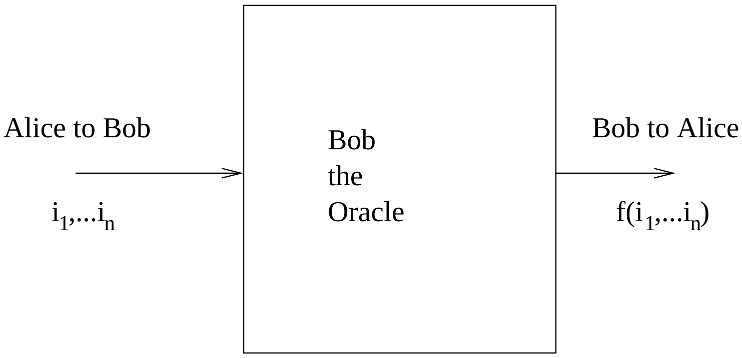
Bob has a function f about which Alice knows nothing except that

- f is a function from n bits to one bit.
- f is either constant or even.

Example: Parity function

$$f(i_1, \ldots, i_n) = i_1 \oplus \cdots \oplus i_n.$$

Bob tells Alice the value $f(i_1, \ldots, i_n)$ for any $i_1, \ldots, i_n$ that Alice may choose.



Alice is to determine whether f is constant or even with as few calls to Bob as possible.

Deutsch's Problem (cont'd)

Classical solution of Deutsch's problem requires $2^{n-1}+1$ calls to Bob in the worst case.

Can quantum computation speed things up?

Quantum Oracle: Bob implements the unitary transformation

$$U_f|i_1,\ldots,i_n\rangle|d\rangle = |i_1,\ldots,i_n\rangle|d \oplus f(i_1,\ldots,i_n)\rangle$$

for all $i_1,\ldots,i_n,d \in \{0,1\}$.

Alice can now determine if f is even or constant with just one call to Bob.

The Deutsch–Josza Algorithm

1. Initialize the registers

$$|0\rangle^{\otimes n}|1\rangle$$

2. Apply Hadamard transform to each qubit

$$\to \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

3. Call the oracle U_f

$$\to \frac{1}{\sqrt{2^n}} \sum_{x} (-1)^{f(x)} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

4. Apply (inverse) Hadamard transform to the first register

$$\to \frac{1}{\sqrt{2^n}} \sum_{z} \sum_{x} \frac{(-1)^{x \cdot z + f(x)}}{\sqrt{2^n}} |z\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

5. Measure the first register to determine the final outcome

$$\to z$$

   Decide that f is constant if $z = 0^n$; otherwise, decide that f is even.

The Deutsch–Josza Algorithm (cont'd)

The oracle action at step 3 produces

$$\begin{aligned} U_f|x\rangle(|0\rangle - |1\rangle) &= |x\rangle(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle) \\ &= \begin{cases} |x\rangle(|0\rangle - |1\rangle) & \text{if } f(x) = 0 \\ |x\rangle(|1\rangle - |0\rangle) & \text{if } f(x) = 1 \end{cases} \\ &= (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle) \end{aligned}$$

The probability of observing state $|z\rangle$ in the final step is

$$|\frac{1}{2^n}\sum_x (-1)^{(x\cdot z + f(x))}|^2$$

For $z = 0^n$, this probability is

$$|\frac{1}{2^n}\sum_x (-1)^{f(x)}|^2 = \begin{cases} 1 & \text{if } f \text{ is constant} \\ 0 & \text{if } f \text{ is even.} \end{cases}$$

Thus, the algorithm determines whether f is constant or even with probability 1.