EE641000
Quantum Information and Computation

Chung-Chin Lu （呂忠津）
Department of Electrical Engineering
National Tsing Hua University

February 19, 2003

Textbook

- M.A. Nielsen and I.L. Chuang

  Quantum Computation and Quantum Information

  Cambridge University Press, 2000

Unit One

Overview of Quantum Information and Computation

Quantum Bits

Quantum Bits (Qubits)

- A classical bit : A physical system with two definite states 0 (off) and 1 (on)
- A Qubit : A quantum system with two states $|0>$ and $|1>$ and their superpositions

$$a\,|0> + b\,|1>$$

with $|a|^2+|b|^2 = 1$

  - A unit vector in a two-dimensional complex inner product space (i.e., a two-dimensional Hilbert space)
  - $|0>$ and $|1>$ form an orthonormal basis

Measurement of a Qubit

- Measure a qubit |s> = a |0> + b |1>
  - Get state |0> with probability |a|^2
  - Get state |1> with probability |b|^2
  - |a|^2 + |b|^2=1
- An example

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

Measurement in Other Orthonormal Basis

$$|+>=(|0>+|1>)/\sqrt{2}$$

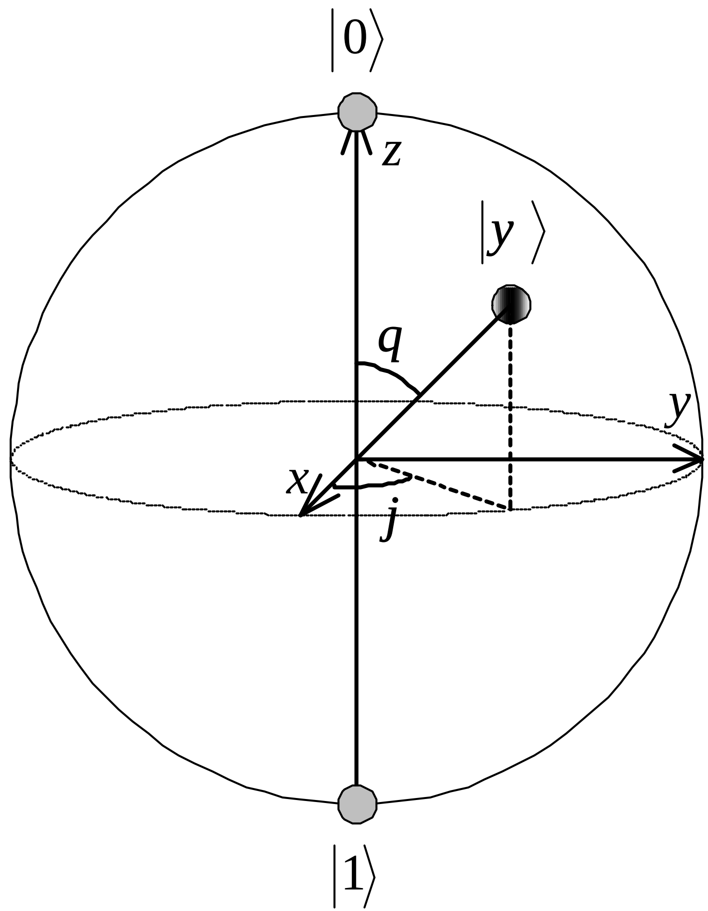
$$|->=(|0>-|1>)/\sqrt{2}$$

$$|y\ >=a\,|0>+b\,|1>$$

$$=a\,\frac{|+>+|->}{\sqrt{2}}+b\,\frac{|+>-|->}{\sqrt{2}}$$

$$=\frac{a+b}{\sqrt{2}}|+>+\frac{a-b}{\sqrt{2}}|->$$

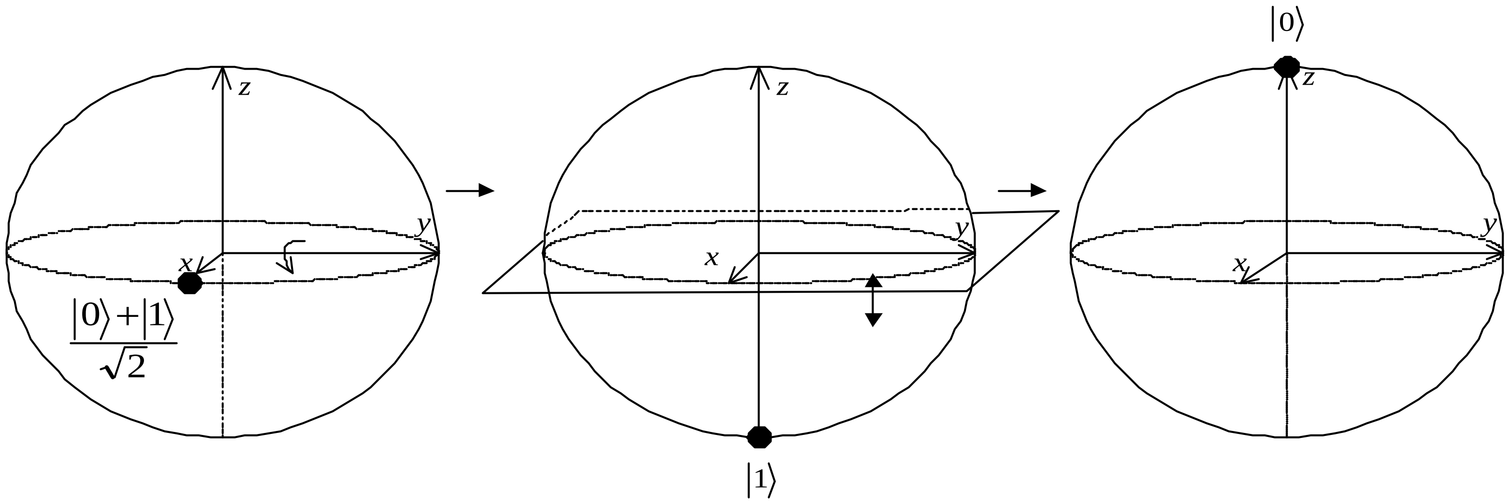
Representation of a State in a Qubit



$$|y>=\cos\frac{q}{2}|0>+e^{ij}\sin\frac{q}{2}|1>$$

$$\left(\sin q\cos j,\ \sin q\sin j,\ \cos q\right)$$

Other States



Physical Realization of a Qubit

- Nuclear spin
- Electron spin
- Polarization of photon
- Optical cavity
- Quantum dot
- Ion trap
- Microwave cavity

Two Qubits

- Two classical bits : A physical system with four possible definite states

  00 01 10 11

- Two qubits : A quantum system with an orthonormal basis

  { |0>|0>, |0>|1>, |1>|0>, |1>|1>}

  and their superpositions

$$a_{00}\,|00> + a_{01}\,|01> + a_{10}\,|10> + a_{11}\,|11>$$

$$\sum |a_{ij}|^2 = 1$$

Bell States or EPR Pairs

- Einstein, Podolsky and Rosen

$$\frac{|00>+|11>}{\sqrt{2}}$$

- Correlated measurement
  - |00> with probability 1/2
  - |11> with probability 1/2

Quantum Circuits

Single Qubit Gates

- Classical NOT gate
  - The only non-trivial single classical
  - 0 → 1 and 1 → 0
- Analogous quantum NOT gate
  - $|0\rangle \rightarrow |1\rangle$ and $|1\rangle \rightarrow |0\rangle$
  - A ***linear operator*** on the qubit (a two-dimensional Hilbert space)

Quantum NOT Gate

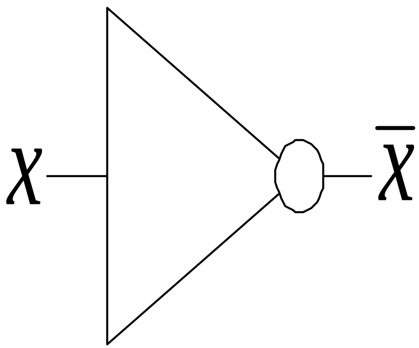
- A linear operator

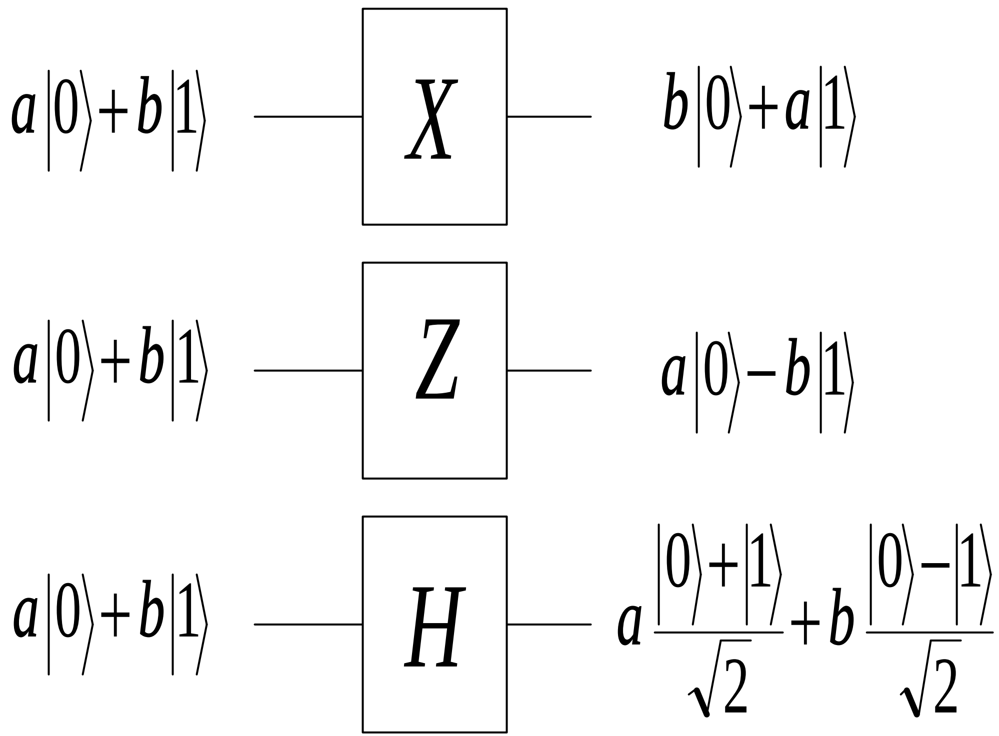
$$a\,|0> + b\,|1> \;\rightarrow\; a\,|1> + b\,|0>$$

$$\begin{bmatrix} b \\ a \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

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

Single Bit and Single Qubit Gates





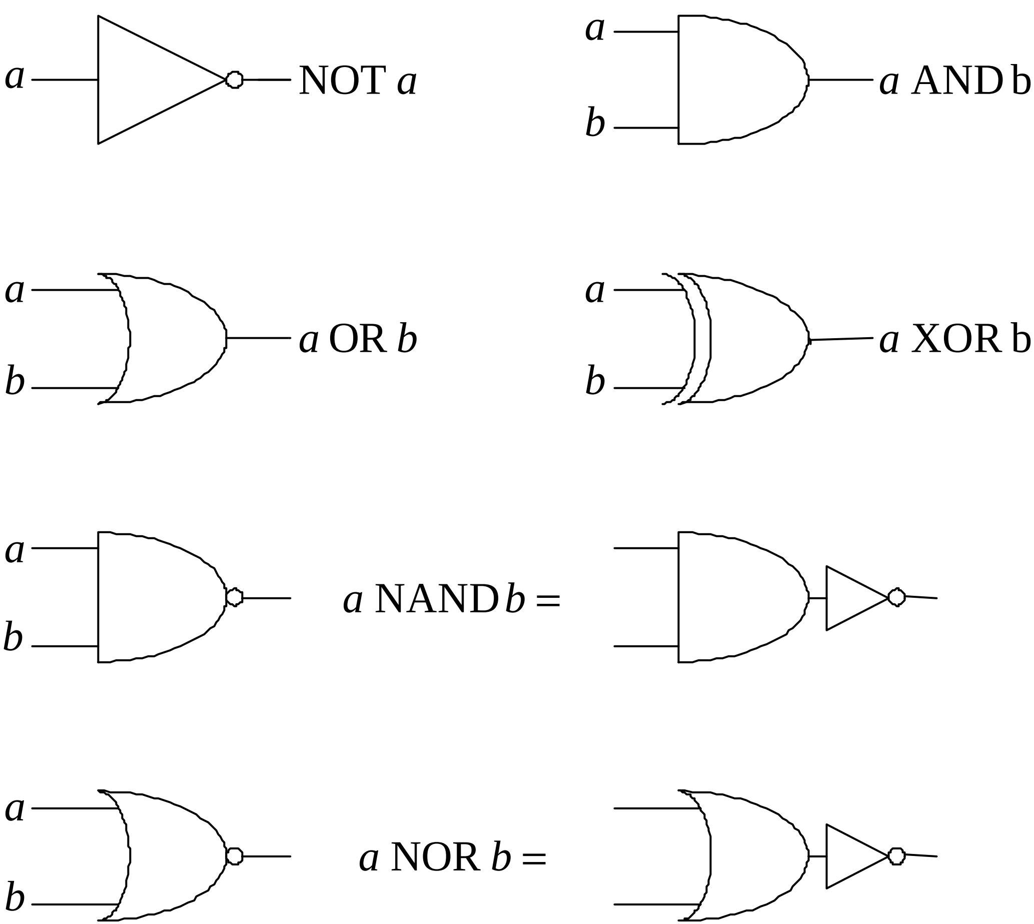
A Generic Single Qubit Gate

- A unitary operator U on a qubit

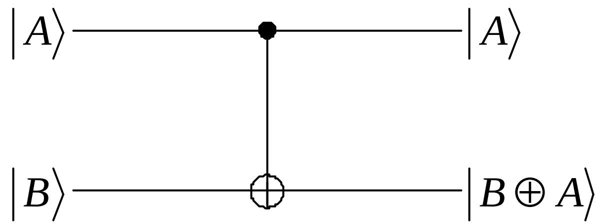
$$U^H U = U U^H = I$$

- U^H : the Hermitian of U
  - Conjugate transpose of U

Multiple Bit and Qubit Gates



controlled - NOT



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

Controlled-NOT Gate U_{CN}

- A control qubit
- A target qubit
- The two output qubits are entangled
- A unitary operator on a four-dimensional Hilbert space

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

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

An n Qubit Gates

- A Unitary operator on n qubits
- Any multiple qubit gate can be composed from CNOT gates and single qubit gates

A Simple Circuit : Swapping

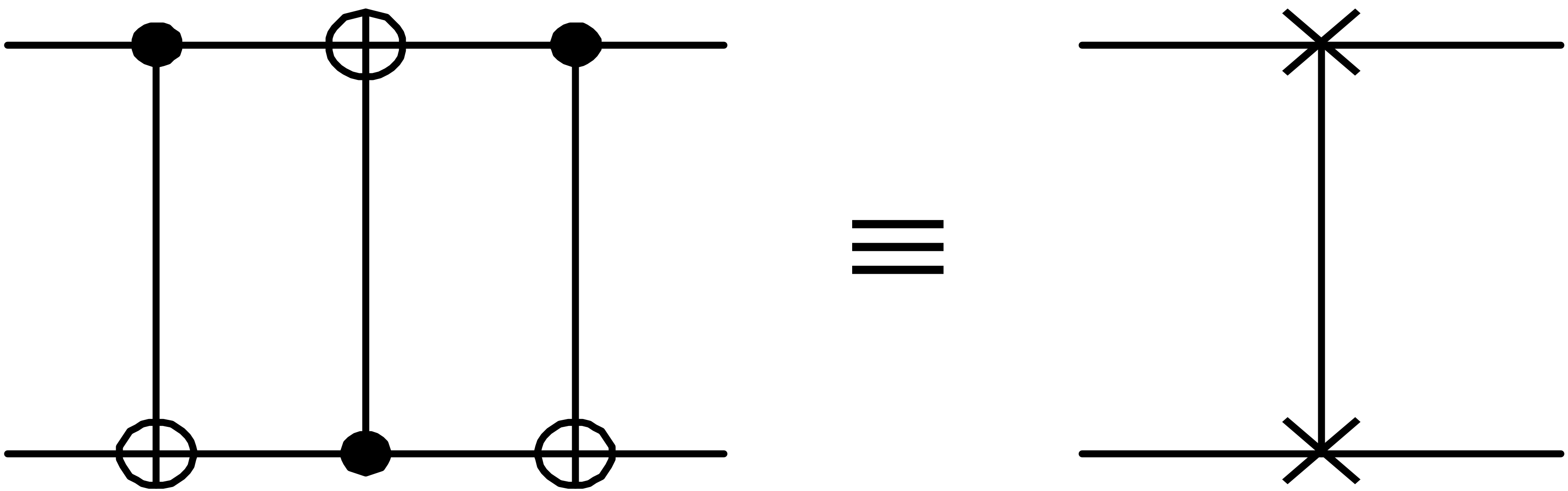
- Circuit diagram is read from left to right
- A wire corresponds to the passage of time or a physical particle moving from one location to another through space

$$a, b > -- >| a, a \oplus b >$$

$$-- >| a \oplus (a \oplus b), a \oplus b >=| b, a \oplus b >$$

$$-- >| b, (a \oplus b) \oplus b >=| b, a >$$

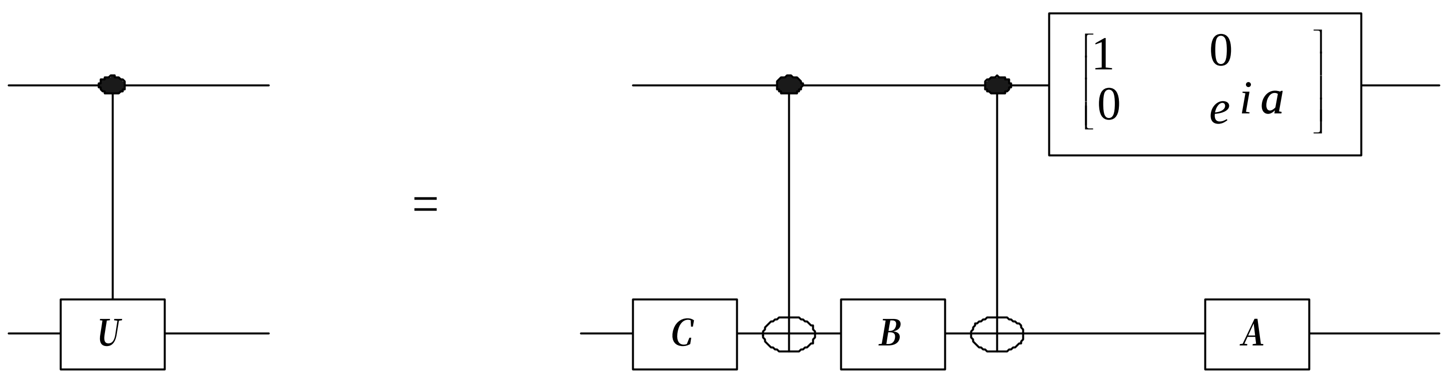
The Swapping Circuit



Single qubit controlled-U Operatior

- U, A, B, C : single-qubit gates

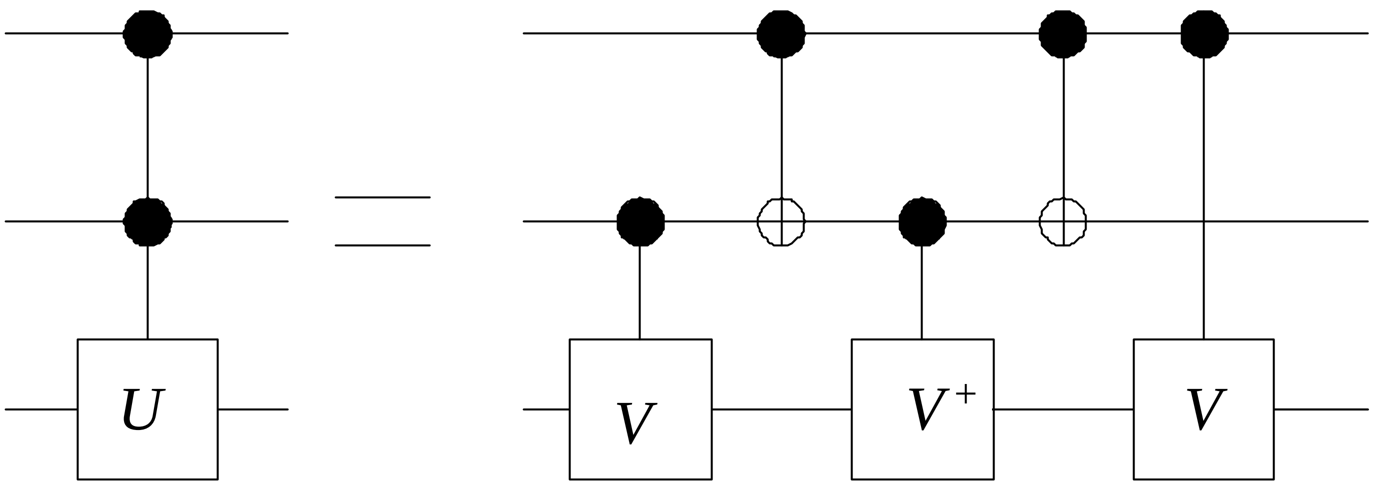
$$U = e^{ia} AXBXC, \quad \text{and} \quad ABC = I$$



Two-Qubit Controlled-U Gate

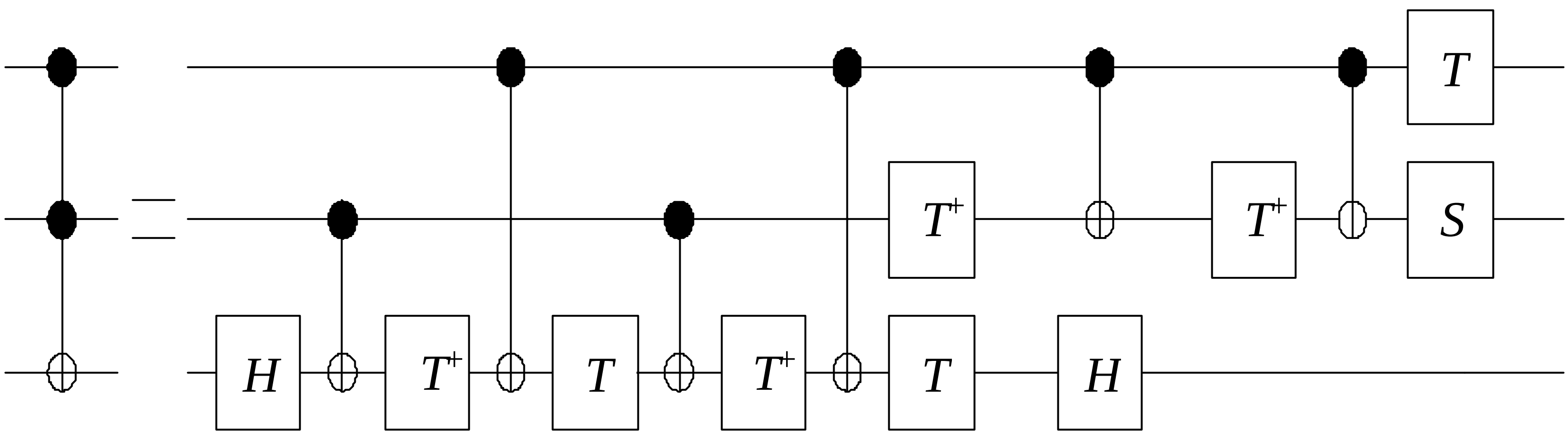
- U : single qubit operator
- V : single qubit operator $U = V^2$

$$C^2(U)\,|c_1c_2>|t> \;=\; |c_1c_2>U^{c_1c_2}\,|t>$$



The Toffoli Gate

- A universal set of gates : CNOT, Hadamard gate H , phase gate S and $p/8$ gate T



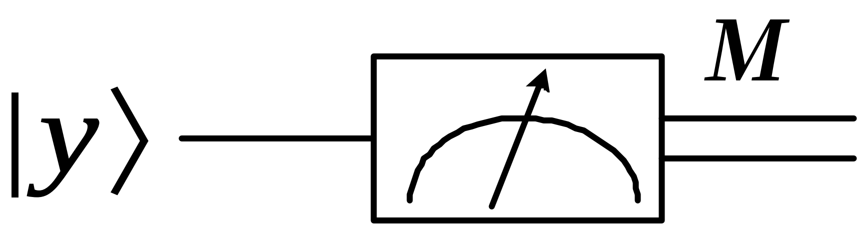
Quantum Circuit Symbol for Measurement

- Converting a single qubit state

$$|y\rangle = a\,|0\rangle + b\,|1\rangle$$

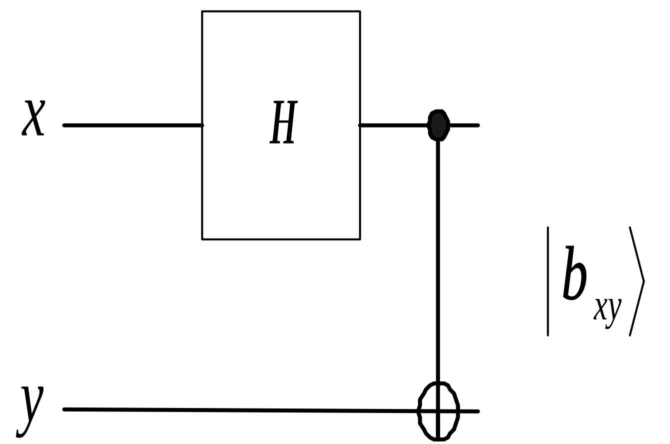
  to a classical bit M

  - M=0 with probability $|a|^2$
  - M=1 with probability $|b|^2$



Creating Bell States or EPR Pairs

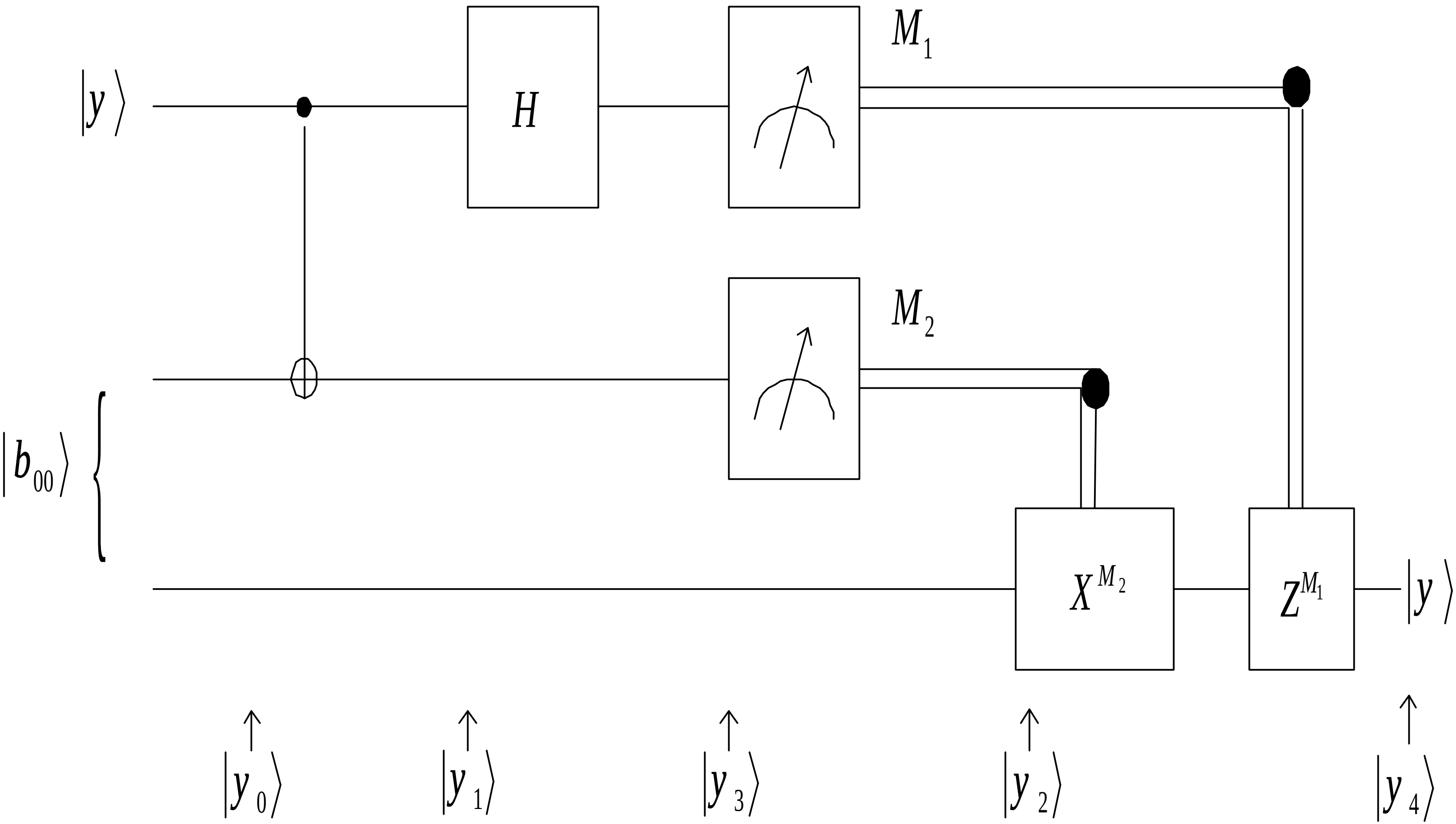
In	Out
$\vert 00\rangle$	$(\vert 00\rangle + \vert 11\rangle)/\sqrt{2} \equiv \vert b_{00}\rangle$
$\vert 01\rangle$	$(\vert 01\rangle + \vert 10\rangle)/\sqrt{2} \equiv \vert b_{01}\rangle$
$\vert 10\rangle$	$(\vert 00\rangle - \vert 11\rangle)/\sqrt{2} \equiv \vert b_{10}\rangle$
$\vert 11\rangle$	$(\vert 01\rangle + \vert 10\rangle)/\sqrt{2} \equiv \vert b_{11}\rangle$



Quantum Teleportation

- Alice and Bob met long ago but now live far apart
- When together, they prepared an EPR pair and each took one qubit when separated
- Now Alice wants to deliver a qubit to Bob
- Alice can only send classical information to Bob

Quantum Teleportation



In Preparation

$$|\psi_0>=|\psi>|\beta_{00}>=(a|0>+b|1>)|\beta_{00}>$$

$$=\frac{1}{\sqrt{2}}[a|0>(|00>+|11>)+b|1>(|00>+|11>)]$$

Alice Sends Her Two QUbits Through a CNOT Gate

$$|y_1>$$

$$=\frac{1}{\sqrt{2}}[a\,|0>(|00>+|11>)+b\,|1>(|10>+|01>)]$$

Alice Sends Her First Qubit Through a Hadamard Gate

$$|y_2>$$

$$= \frac{1}{2}[a(|0> + |1>)(|00> + |11>)$$

$$+ b(|0> - |1>)(|10> + |01>)]$$

$$= \frac{1}{2}[|00> (a|0> + b|1>) + |01> (a|1> + b|0>)$$

$$+ |10> (a|0> - b|1>) + |11> (a|1> - b|0>)]$$

Alice Measures Her Two Qubits

$$00 \mapsto |y_3(00)> \equiv a|0> + b|1> = |y>$$

$$01 \mapsto |y_3(01)> \equiv a|1> + b|0> = X|y>$$

$$10 \mapsto |y_3(10)> \equiv a|0> - b|1> = Z|y>$$

$$11 \mapsto |y_3(11)> \equiv a|1> - b|0> = XZ|y>$$

Quantum Algorithms

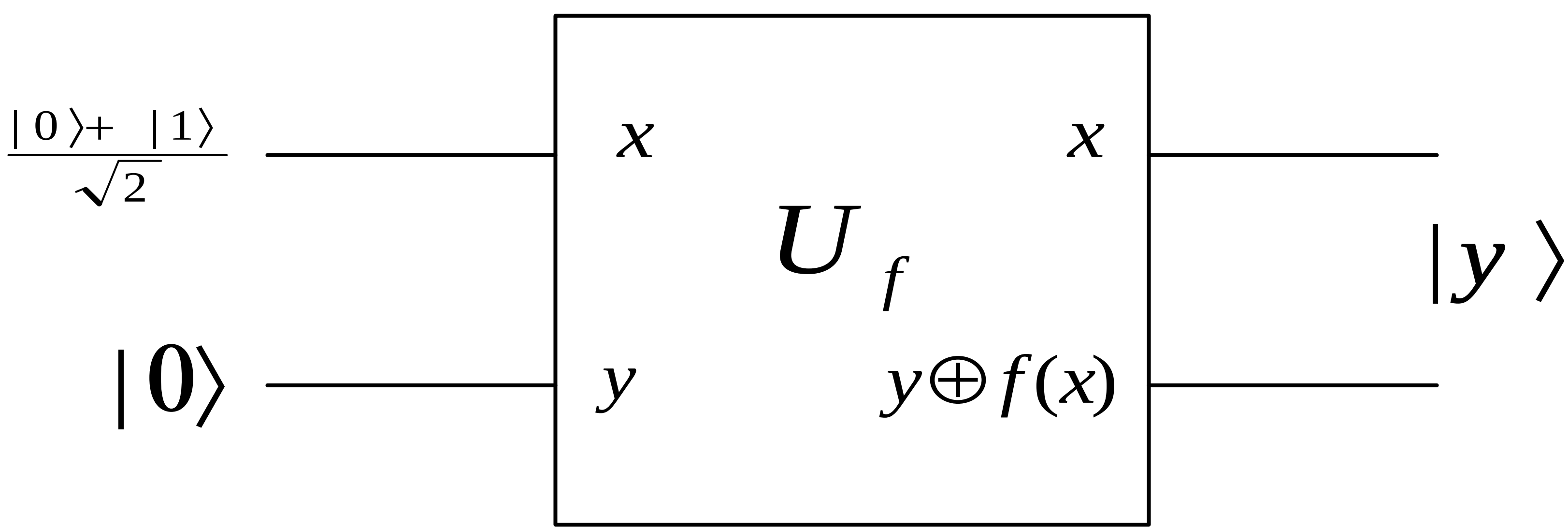
Quantum Parallelism

- A function f from {0,1} to {0,1}
- How to evaluate f(x) for different x *simultaneously* ?
  - A unitary operation U_f on two qubits

$$|x, y> \;\to\; |x, y \oplus f(x)>$$

A Quantum Parallelism Circuit

- The output state is $|y> = \dfrac{|0, f(0) > + |1, f(1) >}{\sqrt{2}}$

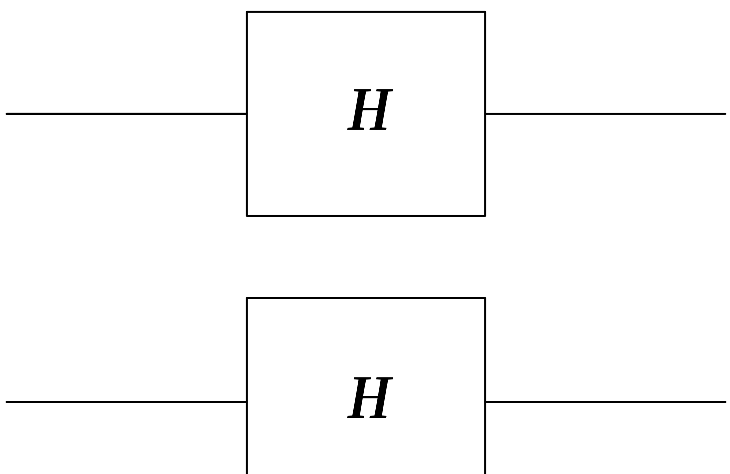


Walsh-Hadamard Transform

$$|0>|0>$$

$$\downarrow$$

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

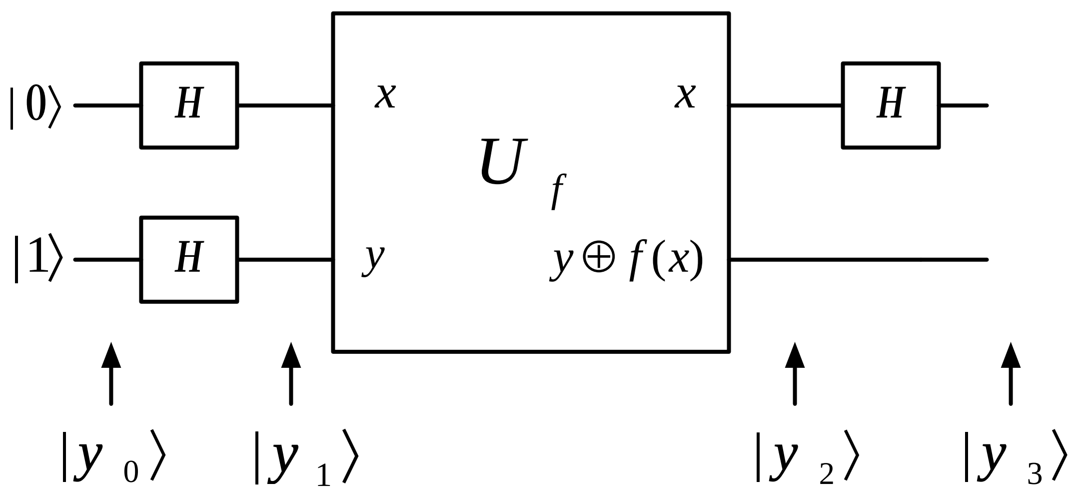


Deutsch's Algorithm

- Determine a global property of $f(x)$

$$f(0) \oplus f(1),$$

by using one evaluation of f(x)



After Walsh-Hadamard Transform

$$|y_1> = \left(\frac{|0> + |1>}{\sqrt{2}} \right) \left(\frac{|0> - |1>}{\sqrt{2}} \right)$$

Interference after Applying U_f

$$|x>(|0>-|1>)/\sqrt{2}$$

$$\downarrow U_f$$

$$|x>(|f(x)>-|1\oplus f(x)>)/\sqrt{2}$$

$$=(-1)^{f(x)}|x>(|0>-|1>)/\sqrt{2}$$

After Applying U_f to $|y_1>$

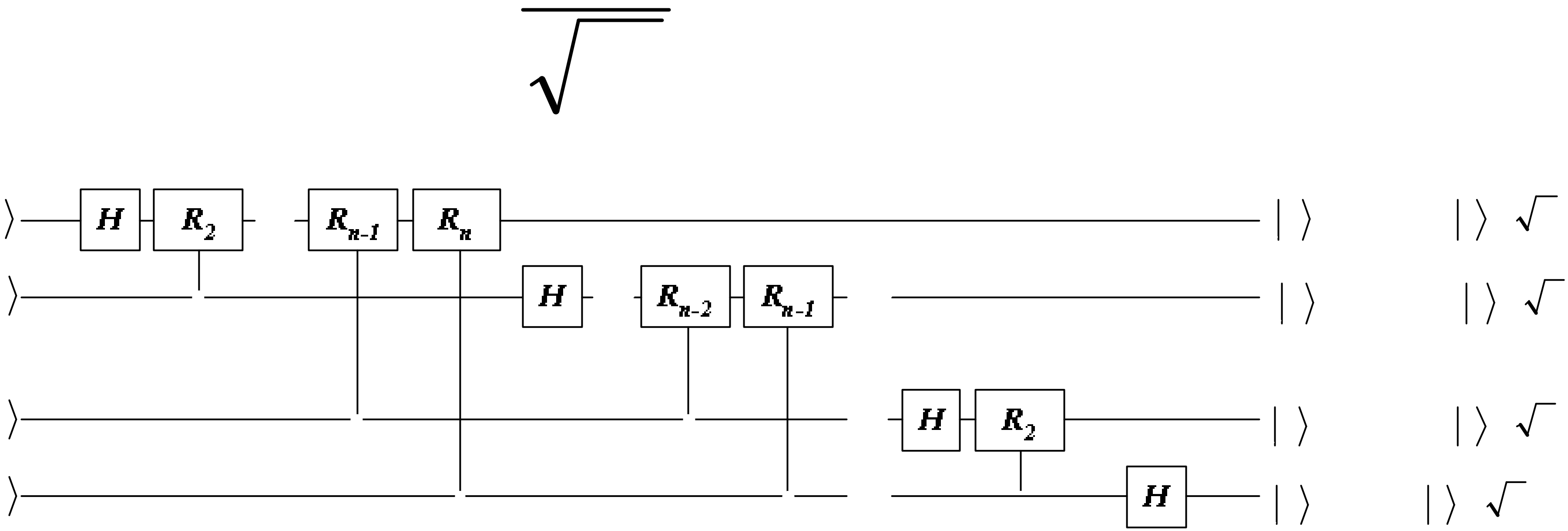
$$|y_2>=\begin{cases}\pm\left(\dfrac{|0>+|1>}{\sqrt{2}}\right)\left(\dfrac{|0>-|1>}{\sqrt{2}}\right) & \text{if } f(0)=f(1) \\ \pm\left(\dfrac{|0>-|1>}{\sqrt{2}}\right)\left(\dfrac{|0>-|1>}{\sqrt{2}}\right) & \text{if } f(0)\neq f(1)\end{cases}$$

Applying Hadamard Gate on the First Qubit

$$|y_3\rangle = \begin{cases} \pm|0\rangle\left(\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \text{if } f(0)=f(1) \\ \pm|1\rangle\left(\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \text{if } f(0)\neq f(1) \end{cases}$$

$$= \pm|f(0)\oplus f(1)\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

Quantum Fourier Transform

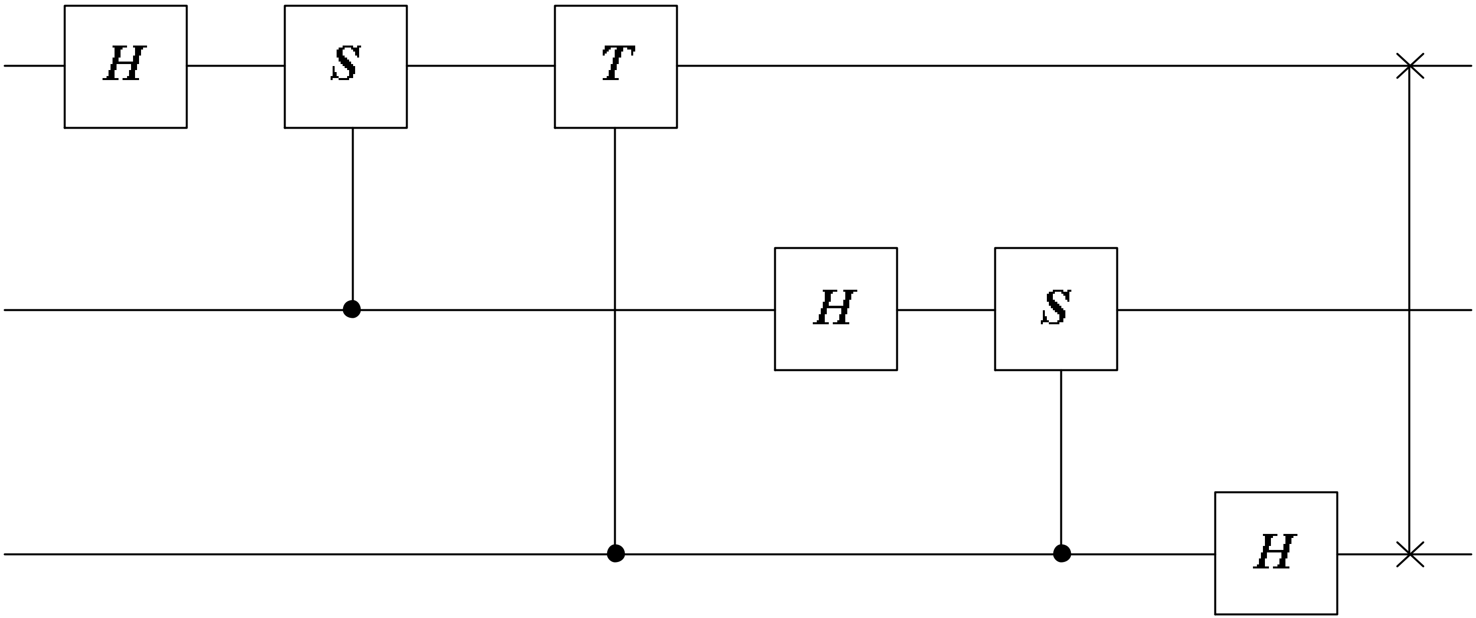


Where the Gates Are

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

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2 p i 2^{-k}} \end{bmatrix}$$

A Concrete Example – Three-Qubit



$$S = \begin{bmatrix} 1 & 0 \\ 0 & e^{2pi\,2^{-2}} \end{bmatrix} \qquad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{2pi\,2^{-3}} \end{bmatrix}$$

Complexity of 2^n -Point FFT

- Classical FFT: $O(n2^n)$ Gates
- Quantum FT: $O(n^2)$ Gates

Obstacles in Using Quantum FT

- The complex amplitudes cannot be accessed directly by measurement
- No efficient ways to prepare the original states to be Fourier transformed

Applications of Quantum Fourier Transform

- Quantum phase estimation
  - $|u>$ and e^{2pij} : an eigenvector and the associated eigenvalue of a unitary operator
- Shor's algorithm for factoring $N = pq$
  - Break unbreakable codes such as RSA
- Discrete logarithm $a^s = b \bmod N$
  - a, b : known

Quantum Search Algorithm

- M : size of data base
- Classical search: $O(M)$
- Quantum search: $O(\sqrt{M})$

Quantum Cryptography

- Quantum key distribution
  - Perfect secret key distribution over public channels

Quantum Error Correction

Decoherence

- Dynamics (evolution) of quantum systems
- Physical state of qubit decays over time
  - Environments
  - Other degrees of freedoms

Quantum Error-correcting Codes

- Code designs
  - Shor’s codes
  - Calderbank-Shor-Steane Codes
- Stabilizer codes
  - Group-theoretical basis
  - Analogous to linear block codes
  - An optimal 5-qubit single-error-correcting quantum code can be designed

Quantum Information Theory

- Classical information through quantum channels
- Quantum information through quantum channels
- Quantum distinguishability
- Creation and transformation of entanglement

Conclusion

Critical Issues

- What can quantum computation do beyond classical computation ?
- How powerful is the quantum computation ?
- How do we realized quantum computation ?
- What other possible quantum algorithms can we design ?
- What possible scenarios of quantum communications can we conceive ?

References

- C.P. Williams and S.H. Clearwater, *Exploration in Quantum Computing*. Santa Clara, CA: TELOS, 1997.
- H.-K. Lo, *Introduction to Quantum Computation and Information*. Singapore: World Scientific, 1998.
- C. Williams (ed.), *Quantum Computing and Quantum Communications: QCQC '98*. New York: Springer, 1999.
- M. Brooks, *Quantum Computing and Communications*. New York: Springer, 1999.

References (Cont')

- D. Bouwmeester, A.K. Ekert and A. Zeilinger (ed.), *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*. New York: Springer, 2000.
- C. Macchiavello, G>M. Palma and A. Zeilinger (ed.), *Quantum Computation and Quantum Information Theory*. Singapore: World Scientific, 2000.
- M. Hirvensalo, *Quantum Computing*. New York: Spring, 2001.
- G. Alber, *Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments*. New York: Springer, 2001.

Recent Papers

- At quant-ph site of Los Alamos National Laboratory, USA

Acknowledgement

- I would like to thank my graduate students who help me drawing all pictures in preparing this presentation

END