11^{th} Week

Basics of Quantum Information

Synopsis.

- Quantum Information
- Quantum Computation
- Quantum Circuits
- Quantum State Identity Testing

June 18, 2018. 23:59

Course Schedule: 16 Weeks

Subject to Change

- Week 1: Basic Computation Models
- Week 2: NP-Completeness, Probabilistic and Counting Complexity Classes
- Week 3: Space Complexity and the Linear Space Hypothesis
- Week 4: Relativizations and Hierarchies
- Week 5: Structural Properties by Finite Automata
- Week 6: Stype-2 Computability, Multi-Valued Functions, and State Complexity
- Week 7: Cryptographic Concepts for Finite Automata
- Week 8: Constraint Satisfaction Problems
- Week 9: Combinatorial Optimization Problems
- Week 10: Average-Case Complexity
- Week 11: Basics of Quantum Information
- Week 12: BQP, NQP, Quantum NP, and Quantum Finite Automata
- Week 13: Quantum State Complexity and Advice
- Week 14: Quantum Cryptographic Systems
- Week 15: Quantum Interactive Proofs
- Week 16: Final Evaluation Day (no lecture)

YouTube Videos

- This lecture series is based on numerous papers of T. Yamakami. He gave conference talks (in English) and invited talks (in English), some of which were video-recorded and uploaded to YouTube.
- Use the following keywords to find a playlist of those videos.
- YouTube search keywords:

  Tomoyuki Yamakami conference invited talk playlist

Conference talk video

Main References by T. Yamakami

- ✎ T. Yamakami. A foundation of programming a multi-tape quantum Turing machine. In Proc. of MFCS 1999, LNCS, Vol. 1672, pp. 430-441 (1999)
- ✎ T. Yamakami. Analysis of quantum functions. International Journal of Foundations of Computer Science 14, 815-852 (2003)
- ✎ M. Kada, H. Nishimura, T. Yamakami. The efficiency of quantum identity testing of multiple states. Journal of Physics A: Mathematical and Theoretical Vol. 41, No.395309 (13pp), 2008.
- ✎ H. Kobayashi, K. Matsumoto, and T. Yamakami. Quantum Merlin-Arthur proof systems: are multiple Merlins more helpful to Arthur? Chicago Journal of Theoretical Computer Science, Vol. 2009, Article 3 (2009)

I. Basics of Quantum Information Theory

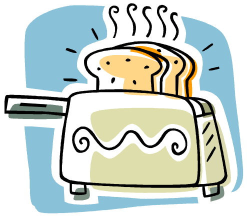
1. Why Do We Need Quantum?
2. What can a Quantum Computer Do?
3. What is a Quantum Bit?
4. Physical Representation of a Qubit
5. How Do We Obtain Quantum Information?
6. Projection Measurements
7. What is Quantum Entanglement?
8. Entangled States: EPR Pair
9. Bra Notation

Why Do We Need Quantum Information?

- Limitations of the existing computers
  - The existing computer will face physical difficulty in making computer chips smaller.
  - The existing computer may not efficiently solve a large number of important problems.
- Looking into physics
  - Fundamentally, a computer is a physical object.
  - The existing computer is based on classical physics whereas Nature obeys quantum mechanics.
  - Realization of the fact that information is physical.

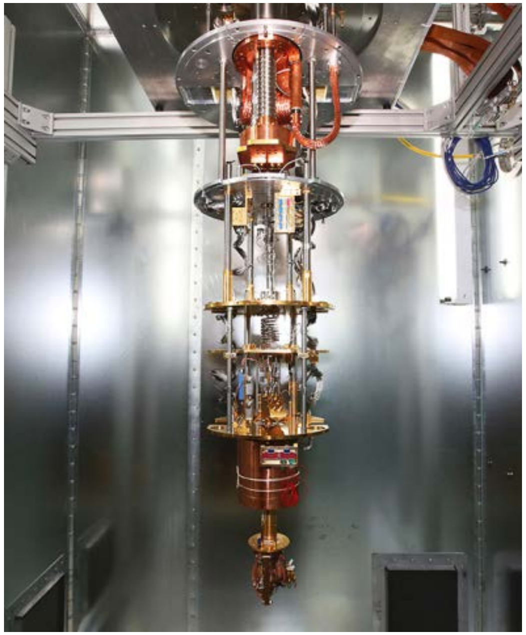
What can a Quantum Computer Do?

- A quantum computer can:
  - ✓ do factoring faster.
  - ✓ break the RSA cryptosystem.
  - ✓ do database search faster.
- Quantum communication can do:
  - ✓ quantum teleportation.
  - ✓ quantum dense coding.
- Quantum cryptography can:
  - ✓ establish secure communication.
  - ✓ build secure cryptosystems.



Currently Developing Quantum Computers I

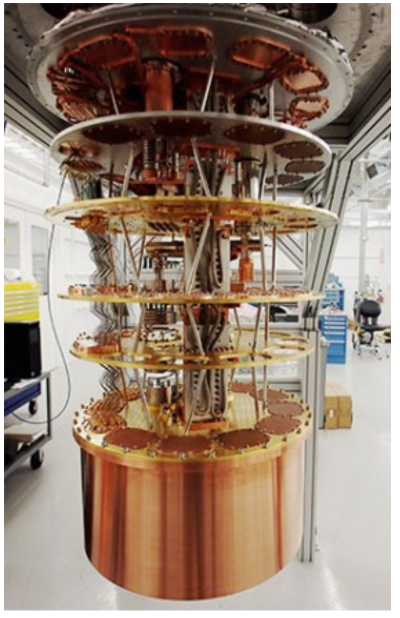
- A number of companies have been trying to build quantum computers.



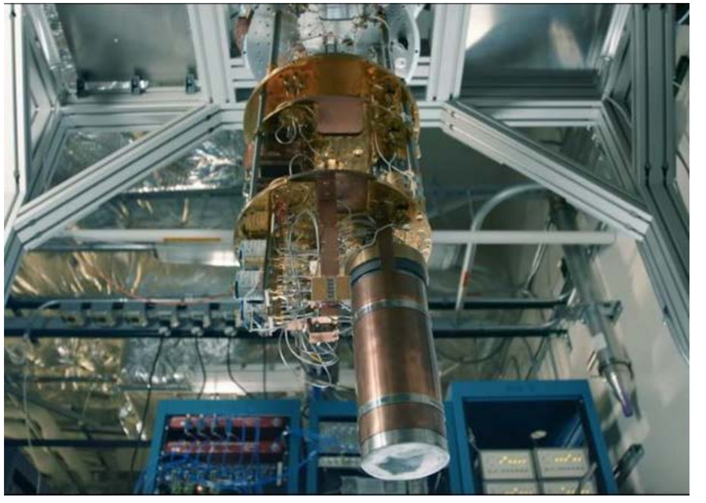
D-Wave’s quantum computer

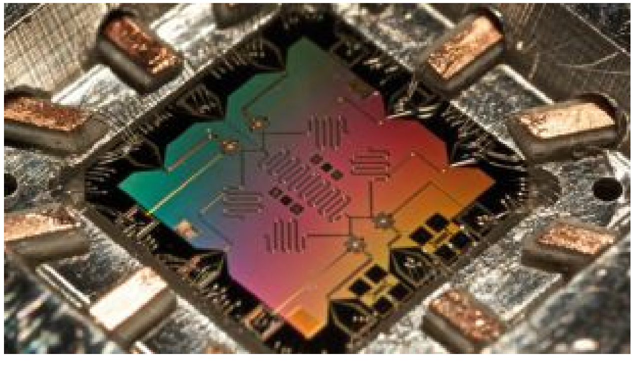
Currently Developing Quantum Computers II

Google's quantum computer



IBM's quantum computer



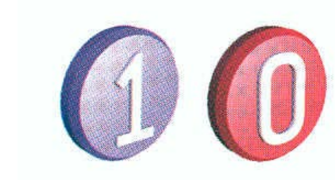


Microsoft's quantum computer

NTT's quantum computer

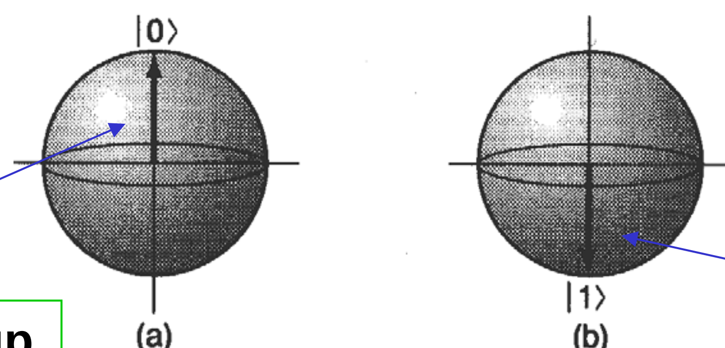
What is a Qubit?

Unit of Quantum Information



- The elementary unit of classical information is bit.

- Quantum bit (qubit) is used in quantum information theory.
- Dirac's ket notation, $|\psi\rangle$, is used to describe those "qubits."
    - Conventionally, we write $|0\rangle$ for bit 0 and $|1\rangle$ for bit 1.



$|0\rangle$ - spin head up

$|1\rangle$ - spin head down

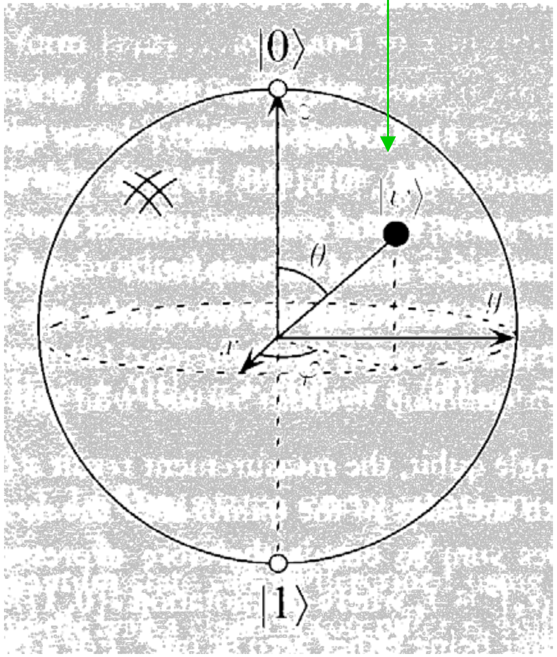
Bloch Sphere Representation of a Qubit I

A quantum bit (qubit) is a quantum analogue of a classical bit.

1 qubit $$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

A qubit is a linear combination of $|0\rangle$ and $|1\rangle$ s.t. $|\alpha|^2+|\beta|^2 = 1$.

The numbers θ and φ define a point in the Bloch sphere.



Geometric representation $i = \sqrt{-1}$

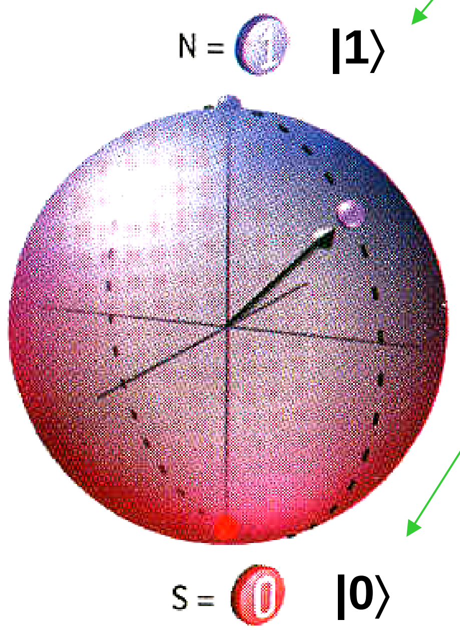
$$|\psi\rangle = e^{i\gamma}\left(\cos\tfrac{\theta}{2}|0\rangle + e^{i\varphi}\sin\tfrac{\theta}{2}|1\rangle\right)$$

If a phase factor $e^{i\gamma}$ is ignored, we can write $|\psi\rangle$ effectively as:

$$|\psi\rangle = \cos\tfrac{\theta}{2}|0\rangle + e^{i\varphi}\sin\tfrac{\theta}{2}|1\rangle$$

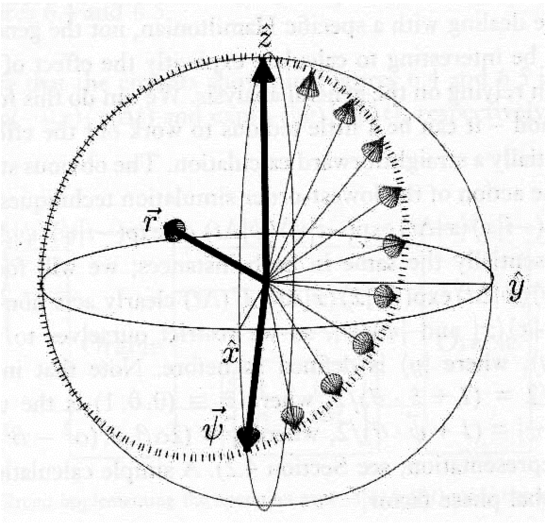
Bloch Sphere Representation of a Qubit II

$|0\rangle$ represents classical bit 0
$|1\rangle$ represents classical bit 1



$|1\rangle$

$|0\rangle$

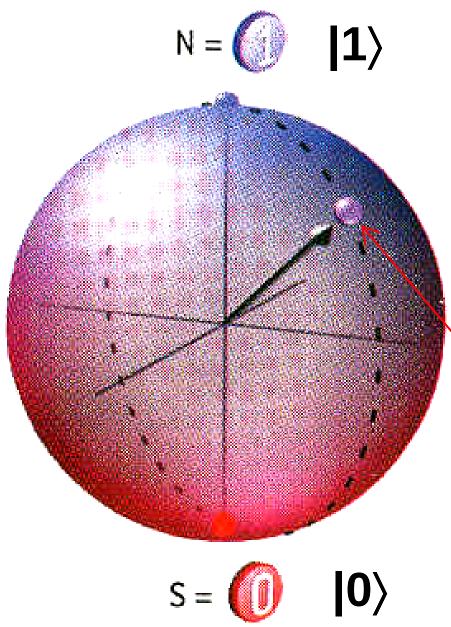


$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$

A qubit is a linear combination of $|0\rangle$ and $|1\rangle$ s.t. $|\alpha|^2+|\beta|^2 = 1$.

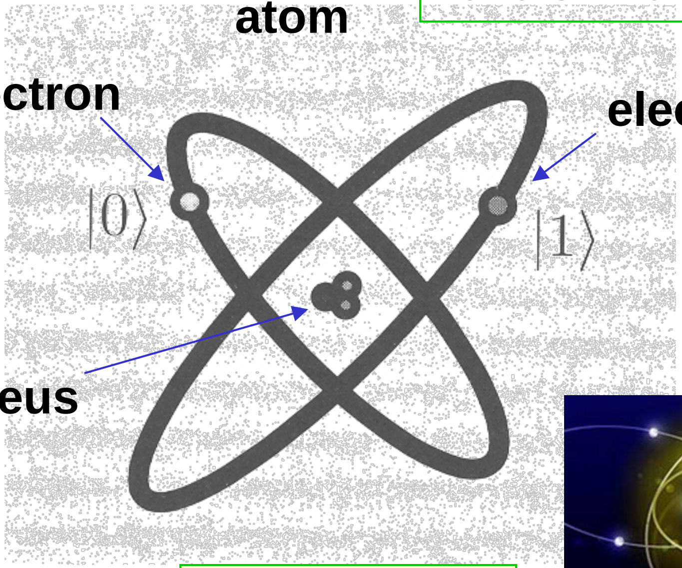
Physical Representation of Qubits

$|0\rangle$ represents classical bit **0**
$|1\rangle$ represents classical bit **1**

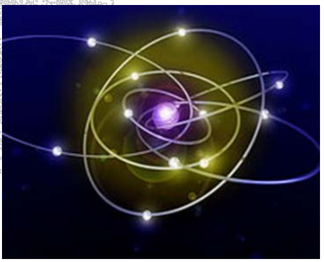


$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$

Two electronic levels in an atom

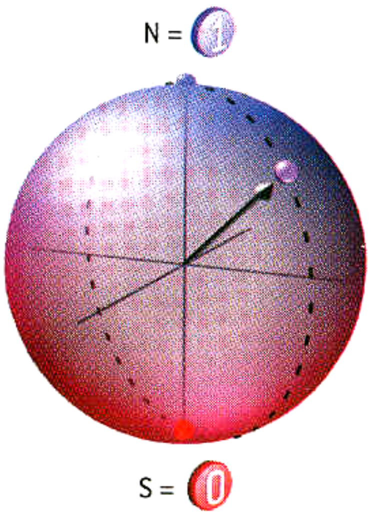


An electron exists in a superposition



A Quantum State over n Qubits

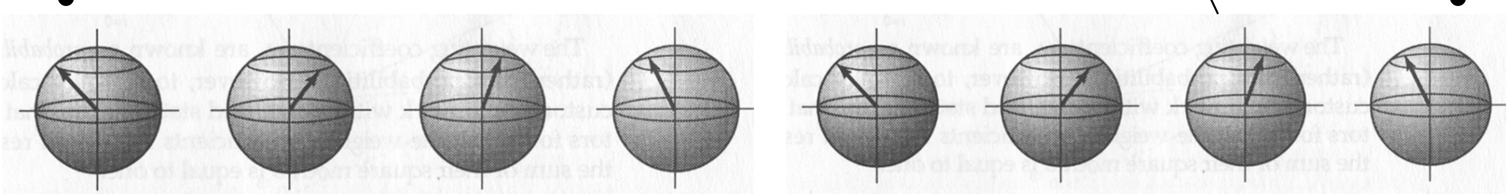
One qubit can be extended to a system of n qubits.



Note that each qubit in $|\boldsymbol{\varphi}\rangle$ may not independent.

one qubit / each

$$|\boldsymbol{\varphi}\rangle = |\boldsymbol{\varphi}_1\rangle|\boldsymbol{\varphi}_2\rangle \cdots |\boldsymbol{\varphi}_n\rangle$$



1 $|\boldsymbol{\varphi}_1\rangle$ **2** $|\boldsymbol{\varphi}_2\rangle$ **3** $|\boldsymbol{\varphi}_3\rangle$ **……..** ***n*** $|\boldsymbol{\varphi}_n\rangle$

Mathematical Definition of a Qubit

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

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

superposition

$$|\varphi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$$

α,β are called amplitudes

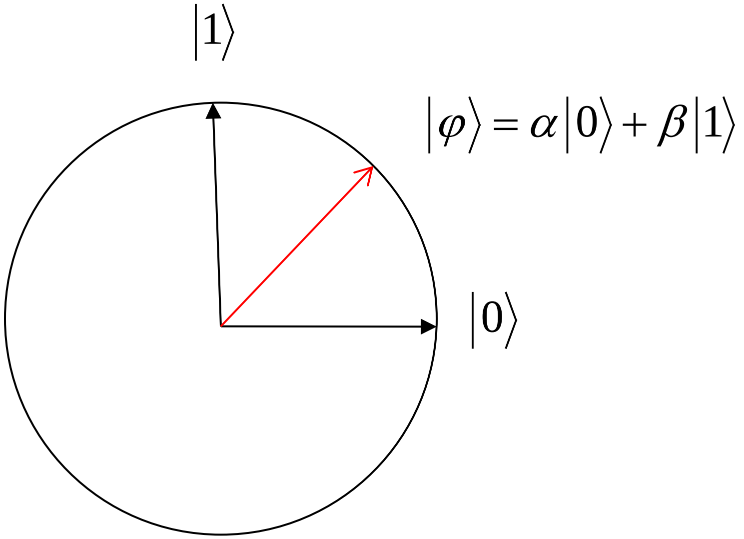
A qubit $|\varphi\rangle$ is a linear combination of $|0\rangle$ and $|1\rangle$ (called a superposition) of the vector form:

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

where $\alpha,\beta \in C$ with $|\alpha|^2+|\beta|^2=1$.

Computational Basis of 1 Qubit System

- A quantum state of 1 qubit can be expressed by using two orthnormal basis states.
- To express 1 qubit systems, we use B = { $|0\rangle$, $|1\rangle$ }, which is called the computational basis.

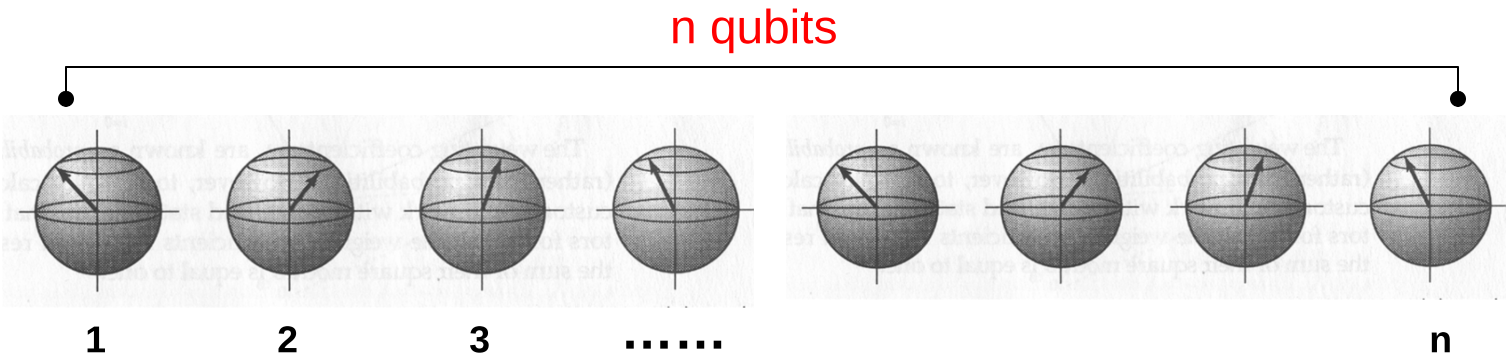


A standard coordinate system

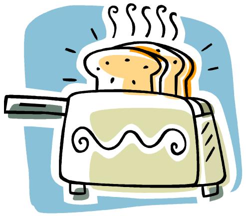
Quantum Information vs Classical Information

How much information can we store in a quantum state?

- Question: How many classical bits can *n* qubits encode?
- Quick Answers:
  - Holevo's Theorem says *n* bits.
  - Dense coding with quantum teleportation encodes *2n* bits.
  - Quantum fingerprinting encodes $2^{O(n)}$ bits.
  - Complex amplitudes encode infinitely many bits.



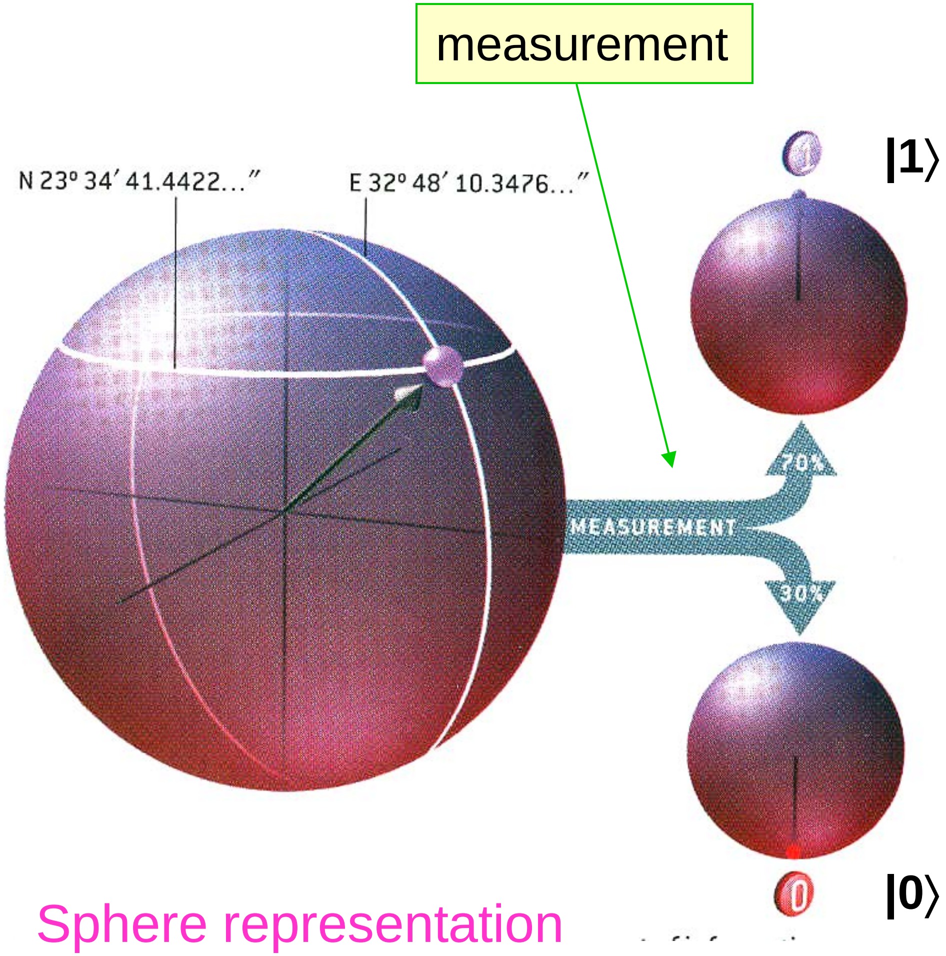
Multi Qubits



- To express multiple qubit systems, we use the notation of ⊗ (tensor product).
- For example, $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, and $|1\rangle \otimes |1\rangle$.
- For convenience, we often write $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$ instead.
- Qubit $|01\rangle$, for example, can be calculated as follows:

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

How Do We Obtain Quantum Information?



Sphere representation

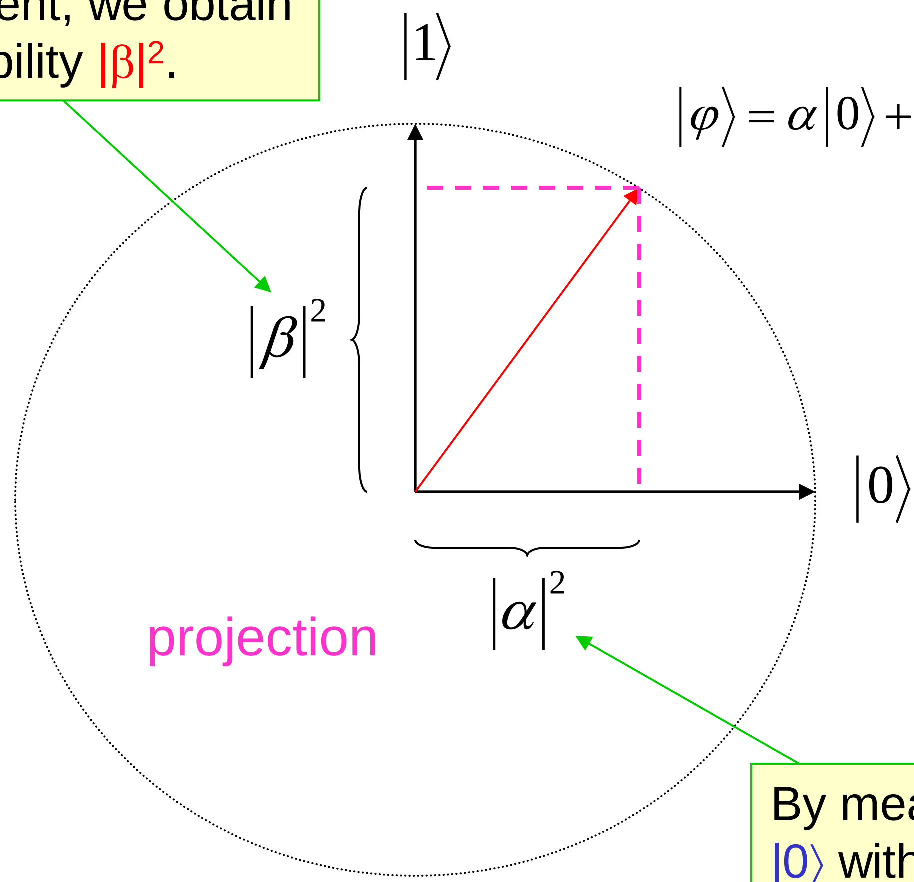
- The measurement is the way to find out what is going on inside the quantum system.
- When a qubit is measured, quantum mechanics requires the result to be always a classical bit.

Projection Measurements

By measurement, we obtain $|1\rangle$ with probability $|\beta|^2$.

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha \\ \beta\end{pmatrix}$$

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



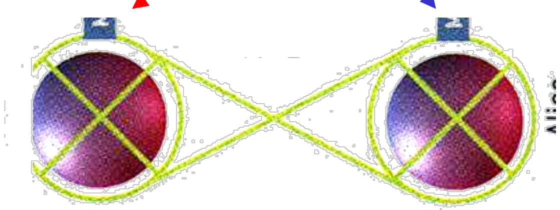
By measurement, we obtain $|0\rangle$ with probability $|\alpha|^2$.

What is Quantum Entanglement?

- In certain 2-qubit systems, two qubits can be strongly correlated.
- Such correlation is called quantum entanglement.

An Bell pair $|\psi\rangle$

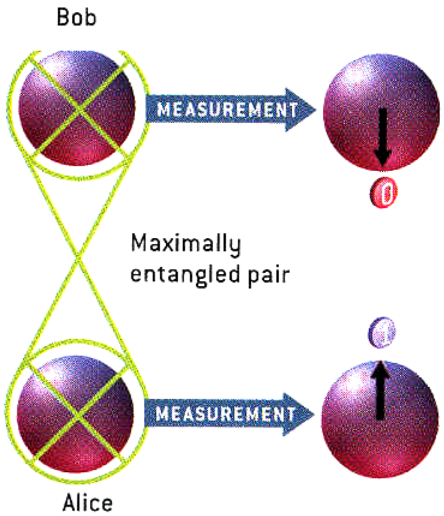
$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle + |1\rangle|0\rangle\right)$$



Bob's qubit

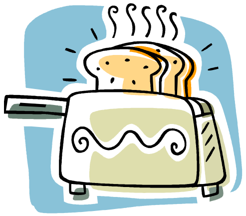
Alice's qubit

If Bob measures $|\psi\rangle$ and obtain $|0\rangle$, then Alice must obtain $|1\rangle$ after measurement.



If Bob measures $|\psi\rangle$ and obtain $|1\rangle$, then Alice must obtain $|0\rangle$ after measurement.

Entangled States: EPR Pair



- Consider the EPR pair $|\varphi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$
- This quantum state can be expressed as:

$$|\varphi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\0\end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix}0\\0\\0\\1\end{bmatrix} = \begin{bmatrix}1/\sqrt{2}\\0\\0\\1/\sqrt{2}\end{bmatrix}$$

- The EPR pair will be discussed later in conducting quantum teleportation.

Bra Notation

- Given a matric A, we write A^+ (dagger) for the transposed conjugate of A.
- Since $|\varphi\rangle$ is expressed as a column vector, we can consider $(|\varphi\rangle)^+$, which we express as $\langle\varphi|$ (bra notation).
- The inner product between $|\varphi\rangle$ and $|\psi\rangle$ is expressed as $\langle\varphi|\psi\rangle$.
- The outer product is expressed as $|\varphi\rangle\langle\psi|$, which is a matrix.

Examples

- We show some examples of how to use the bra notion.

$$|0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \qquad |1\rangle\langle 0| = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \qquad |0\rangle\langle 1| = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \qquad |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Let $|\varphi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$ and $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$

$$\langle\varphi|\psi\rangle = \frac{1}{2}\left(\langle 0| + \langle 1|\right)\left(|0\rangle - |1\rangle\right) = \frac{1}{2}\left(\langle 0|0\rangle - \langle 0|1\rangle + \langle 1|0\rangle - \langle 1|1\rangle\right)$$

$$= \frac{1}{2}\left(1 - 0 + 0 - 1\right) = 0$$

inner product

$$|\varphi\rangle\langle\psi| = \frac{1}{2}\left(|0\rangle + |1\rangle\right)\left(\langle 0| - \langle 1|\right) = \frac{1}{2}\left(|0\rangle\langle 0| - |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\right)$$

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

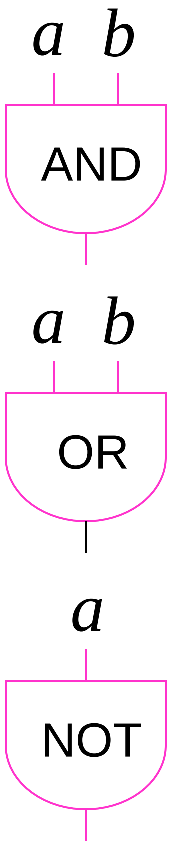
outer product

II. Quantum Computation

1. Logical gates and Quantum Gates
2. Examples of Qubit Quantum Gates
3. What is a Quantum Circuit?
4. No-Cloning Theorem
5. Proof of the No-Cloning Theorem
6. Sets of Universal Quantum Gates
7. Uniform families of Quantum Circuits
8. Polynomial-Time Quantum Computation

Logical Gates and Logical Circuits

Logical gates

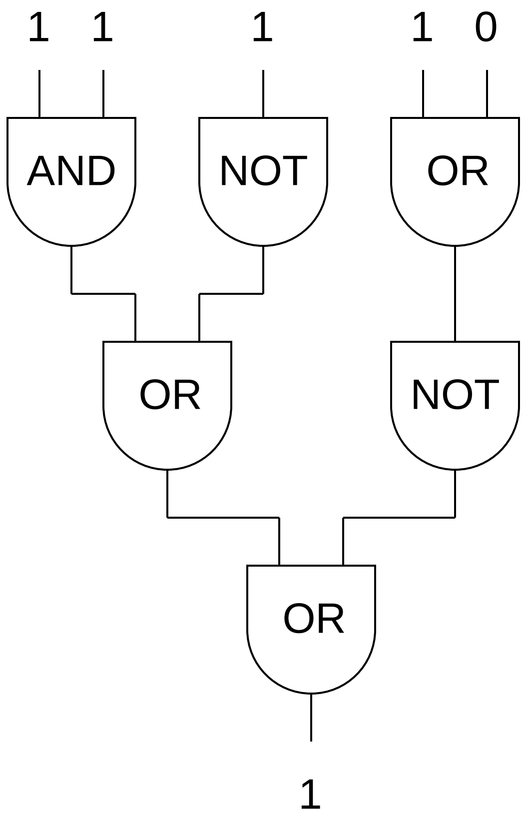


$$\color{red}{AND}: (a,b) \to \min\{a,b\}$$

$$\color{red}{OR}: (a,b) \to \max\{a,b\}$$

$$\color{red}{NOT}: a \to 1-a$$

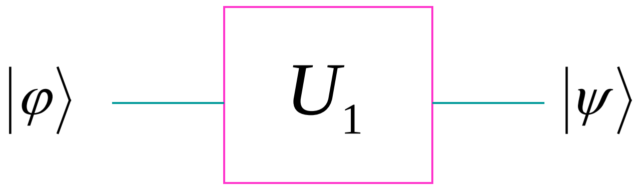
Logical circuit



What are Quantum Gates?

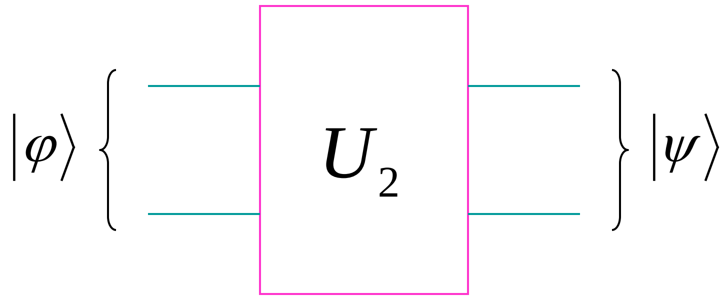
1-qubit quantum gates

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix}$$



$$U_1 = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$$

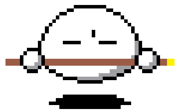
2-qubit quantum gates



$$U_2 = \begin{pmatrix}a_{11} & a_{12} & a_{13} & a_4\\ a_{21} & a_{22} & a_{23} & a_{24}\\ a_{31} & a_{32} & a_{33} & a_{34}\\ a_{41} & a_{42} & a_{43} & a_{44}\end{pmatrix}$$

$$U_1|\varphi\rangle = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha\begin{pmatrix}a\\c\end{pmatrix} + \beta\begin{pmatrix}b\\d\end{pmatrix} = \alpha\cdot U_1|0\rangle + \beta\cdot U_1|1\rangle$$

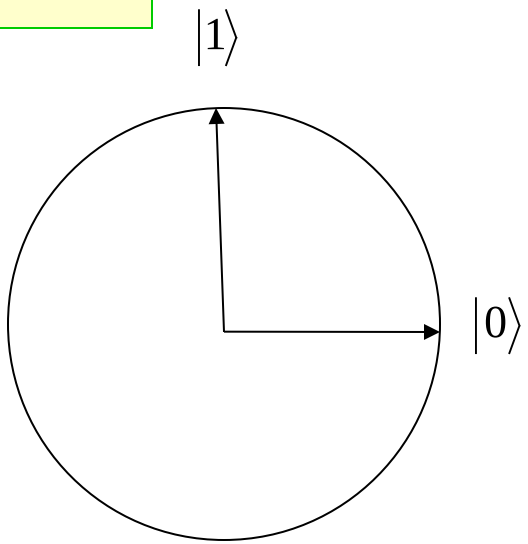
Examples of 1-Qubit Quantum Gates I



- Here are two examples of simple quantum gates that handle one qubit:
  - I (identity)
  - NOT (negation)

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad I : \begin{cases} |0\rangle \rightarrow |0\rangle \\ |1\rangle \rightarrow |1\rangle \end{cases}$$

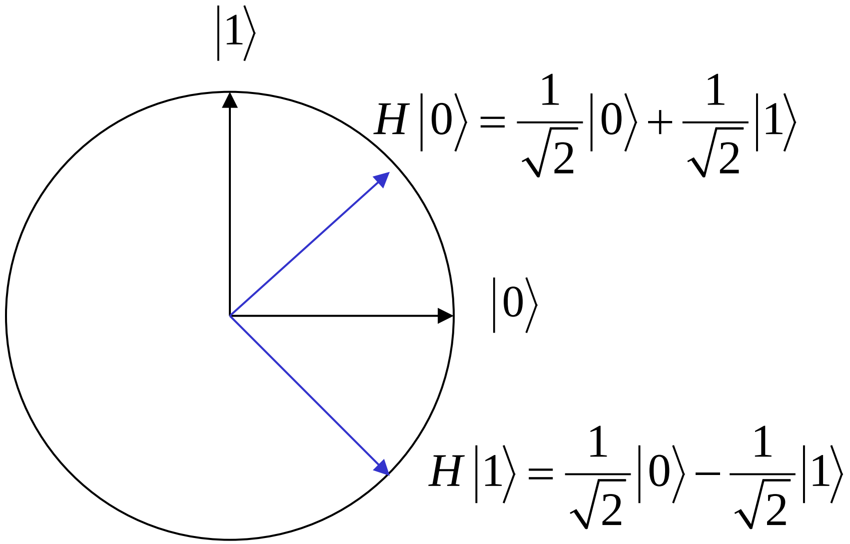
$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad NOT : \begin{cases} |0\rangle \rightarrow |1\rangle \\ |1\rangle \rightarrow |0\rangle \end{cases}$$



Examples of 1-Qubit Quantum Gates II

H: Walsh-Hadamard Gate

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



$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Examples of 1-Qubit Quantum Gates III

Phase Shift: S

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$S|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$i = \sqrt{-1}$$

$$S|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ i \end{pmatrix} = i|1\rangle$$

Rotations: $R_x(\theta), R_y(\theta), R_z(\theta)$

$$R_x(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \quad R_y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \quad R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$$

Examples of 1-Qubit Quantum Gates IV

Phase Shift: $Z_{1,\theta}$, $Z_{2,\theta}$

$$i = \sqrt{-1}$$

$$Z_{1,\theta} = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & 1 \end{pmatrix} \qquad Z_{1,\theta} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

We then obtain:

$$R_z(2\theta) = Z_{1,\theta} Z_{2,\theta}$$

$$S = Z_{2,\pi/2}$$

Examples of 2-Qubit Quantum Gates

Controlled-NOT: CNOT

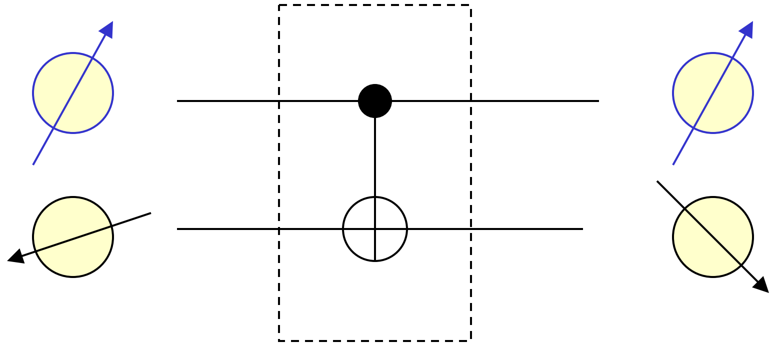
$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$CNOT\,|0\rangle|a\rangle = |0\rangle|a\rangle$$

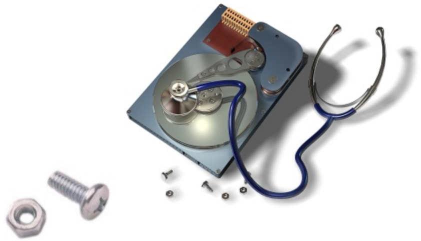
$$CNOT\,|1\rangle|a\rangle = |1\rangle|1-a\rangle$$

$$a \in \{0,1\}$$

$|\varphi\rangle$

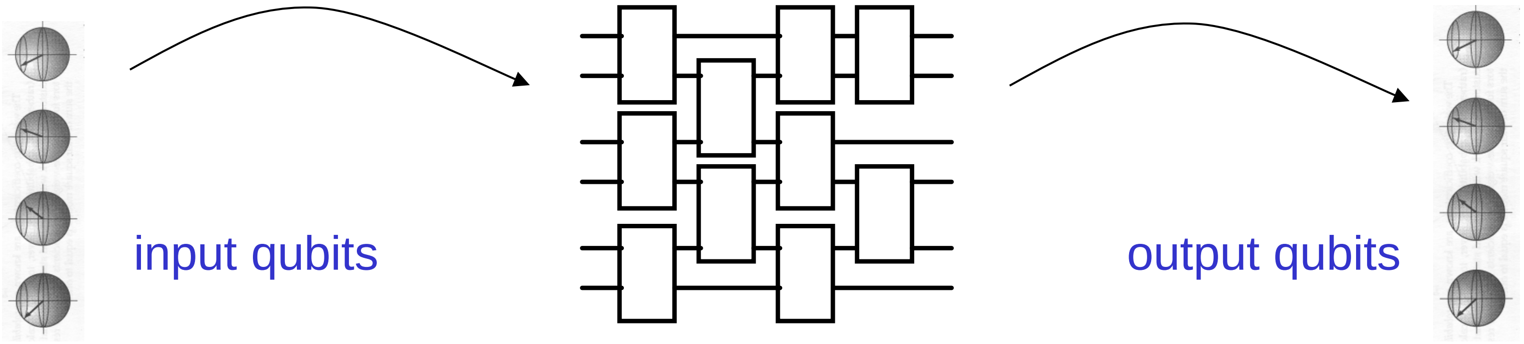


Controlled bit



What is a Quantum Circuit?

- To manipulate quantum information, we use unitary operations, which are realized by quantum circuits made of a finite set of “simple” quantum gates.
- In particular, we use quantum circuits whose circuitry can be “efficiently” designed in a reasonable amount of time (say, polynomial time).
- Such a quantum circuit transforms qubits as follows:

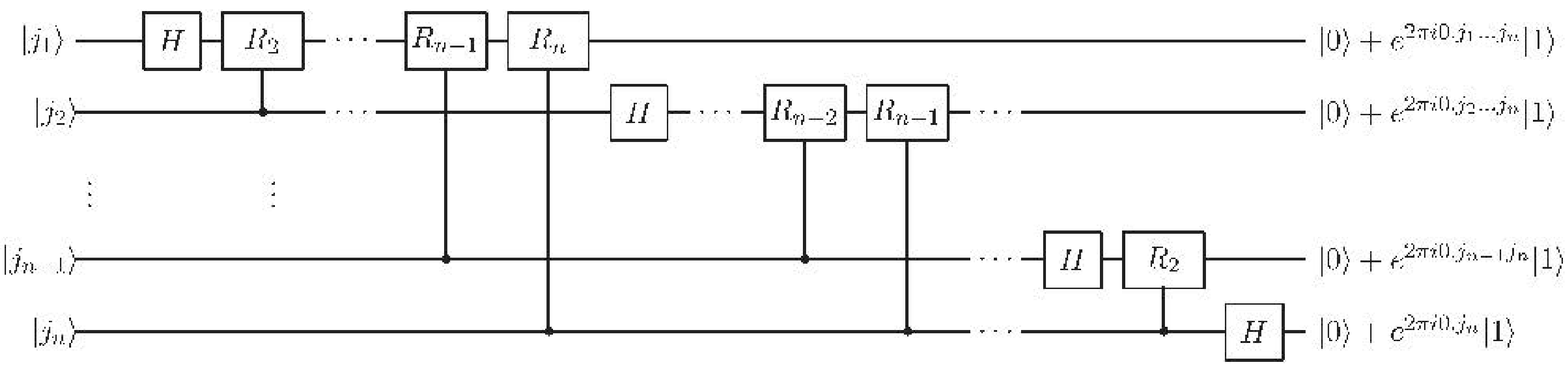


A quantum circuit

Quantum Fourier Transform (QTF)

- We show one example of quantum circuit, which computes the quantum Fourier transform (QTF).

$$QTF\,|\,j\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j k/2^n} \,|k\rangle, \text{ where } 0 \le j \le 2^n - 1$$



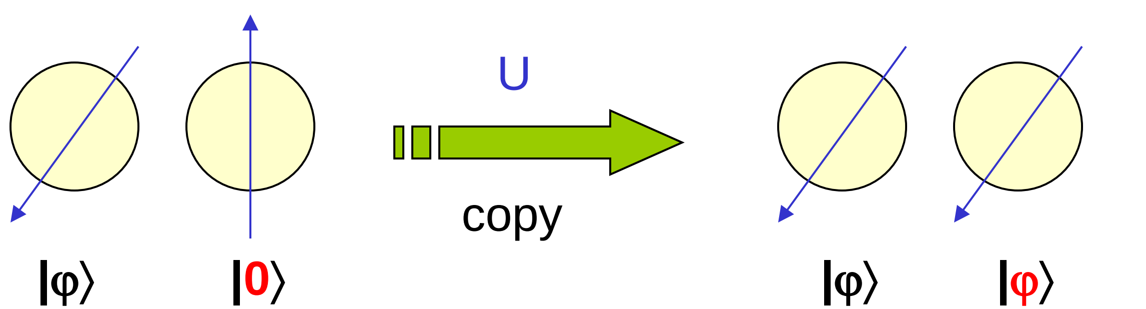
$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix} \qquad H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

No-Cloning Theorem

- The no-cloning theorem gives a significant limitation to quantum computation.

> **No-Cloning Theorem:**
> No quantum algorithm makes an exact copy of any quantum state.

- “Making an exact copy” means that a certain unitary transformation U satisfies $U|\varphi\rangle|0\rangle = |\varphi\rangle|\varphi\rangle$ for any $|\varphi\rangle$.



Proof of the No-Cloning Theorem

- Theorem: There is no quantum computation U such that, for any quantum state $|\varphi\rangle$, $U|\varphi\rangle|0\rangle = |\varphi\rangle|\varphi\rangle$.

❑ Proof:

- Assume that there exists a unitary operator U such that $U|\varphi\rangle|0\rangle = |\varphi\rangle|\varphi\rangle$ for any $|\varphi\rangle$.
- Consider two unit vectors $|\varphi\rangle$ and $|\psi\rangle$ satisfying $0<|\langle\varphi|\psi\rangle|<1$. Obviously, $|\langle\varphi|\psi\rangle|^2<|\langle\varphi|\psi\rangle|$.
- Since U is unitary, we obtain:

$$\langle\varphi|\psi\rangle = \langle\varphi,0|\psi,0\rangle = \langle U\varphi 0|U\psi 0\rangle = \langle\varphi,\varphi|\psi,\psi\rangle = |\langle\varphi|\psi\rangle|^2.$$

- This is clearly a contradiction.

QED

Sets of Universal Quantum Gates

- There are infinitely many quantum gates to consider.
- However, it is possible to take a fixed set of quantum gates in order to realize all the other quantum gates in an approximate way.
- A set of those specific quantum gates is called universal.

- Examples of sets of universal gates:

  1) CNOT + all 1-qubit gates
  2) Walsh-Hadamard + CNOT + $Z_{2,\pi/4}$

     [Boykin-Mor-Pulver-Roychowdhury-Vatan (1999)]

Uniform Families of Quantum Circuits

- We fix a finite family of universal quantum gates: for example,

  Walsh-Hadamard gate + CNOT gate + $Z_{2,\pi/4}$ gate.

- We then consider appropriate encoding of these gates. We consider families $\{C_n\}_{n\in N}$ of quantum circuits, where each C_n takes n inputs.

- We say that a family $\{C_n\}_{n\in N}$ of quantum circuits is called P-uniform if there exists a polynomial-time DTM M with an output tape such that, for every index $n\in N$, M on input 1^n produces an encoding of C_n.

$$M: \ 1^n \rightarrow \ \text{description } \langle C_n \rangle \text{ of circuit } C_n$$

Polynomial-Time Quantum Computation

- A decision problem (or a language) L is said to be polynomial-time solvable if there exists a P-uniform family $\{C_n\}_{n\in N}$ of polynomial-size quantum circuits such that, for each $n\in N$ and any $x\in\Sigma^n$,
  1. if $x \in L \leftrightarrow C_n(x) = 1$ with probability $\geq 2/3$, and
  2. if $x \notin L \leftrightarrow C_n(x) = 0$ with probability $\geq 2/3$.

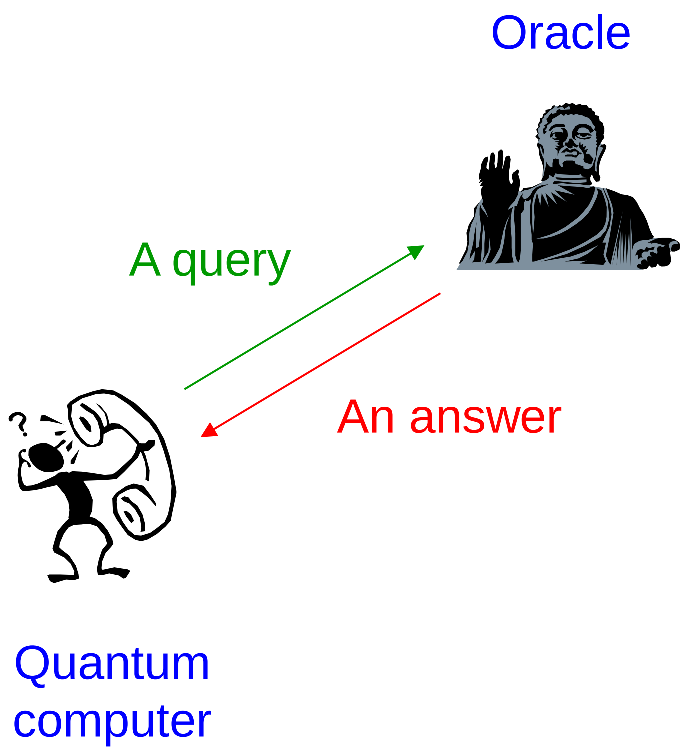
- A function $f : \Sigma^* \to \Sigma^*$ is polynomial-time computable if there exists a P-uniform family $\{C_n\}_{n\in N}$ of polynomial-size quantum circuits with outputs such that, for each $n\in N$ and any input $x\in\Sigma^n$, C_n outputs exactly $f(x)$ with probability $\geq 2/3$.

III. Quantum Algorithms

1. Black-Box Model of Quantum Computation
2. Deutsch's XOR Problem
3. A Quantum Algorithm for Deutsch's Problem
4. Analysis of the Quantum Algorithm
5. Quantum state Identity Testing
6. Quantum Algorithm for QSITP
7. Important Quantum Algorithms

Black-Box Model of Quantum Computation I

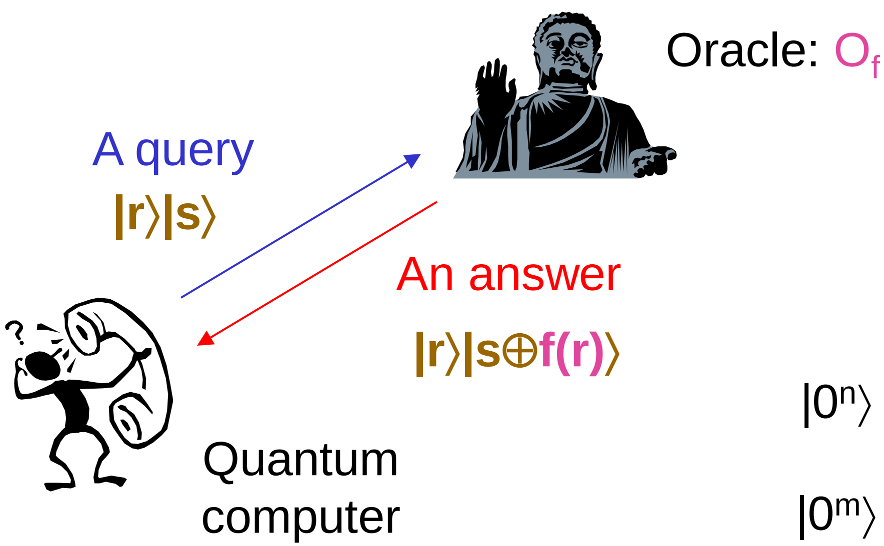
- Unlike the model of quantum circuits, we discuss a black-box model of quantum computation.
- In this mode, input information is given by way of queries to an external source, called an oracle.
- We are concerned about how many times a computation accesses the input information.



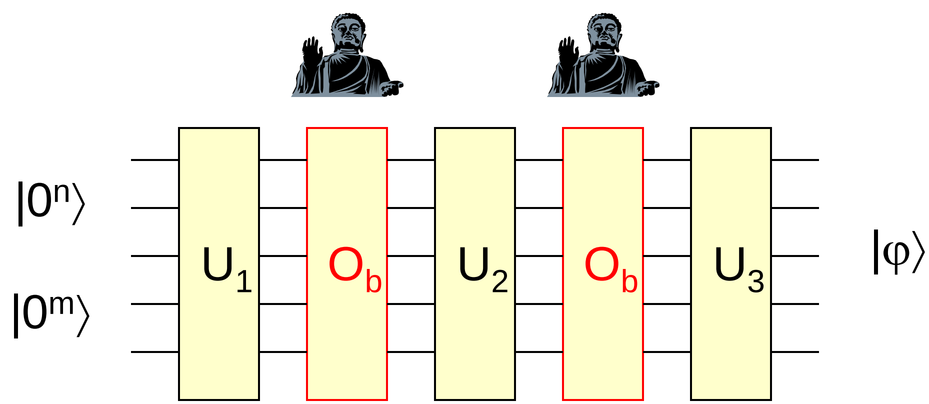
Black-Box Model of Quantum Computation II

Let f be any function from $\{0,1\}^n$ to $\{0,1\}^l$.

Oracle O_f is used to represent this function f.



An oracle computation proceeds as a chain of unitary operations and oracle queries.



Instead of starting standard input x, the input information is given through oracle queries.

Deutsch's XOR Problem

- A function f: $\{0,1\} \to \{0,1\}$ is
  - balanced if $|f^{-1}(0)|=|f^{-1}(1)|$ (i.e., $f(0)\oplus f(1)=1$)
  - constant if either $|f^{-1}(0)|=2$ or $|f^{-1}(1)|=2$ (i.e., $f(0)\oplus f(1)=0$)

There are four possibilities.

$f(0)=0$ $f(1)=0$	$f(0)=0$ $f(1)=1$	$f(0)=1$ $f(1)=0$	$f(0)=1$ $f(1)=1$
constant	balanced	balanced	constant

How many times should we access f?

Deutsch's XOR problem

Input: a function $f : \{0,1\} \to \{0,1\}$

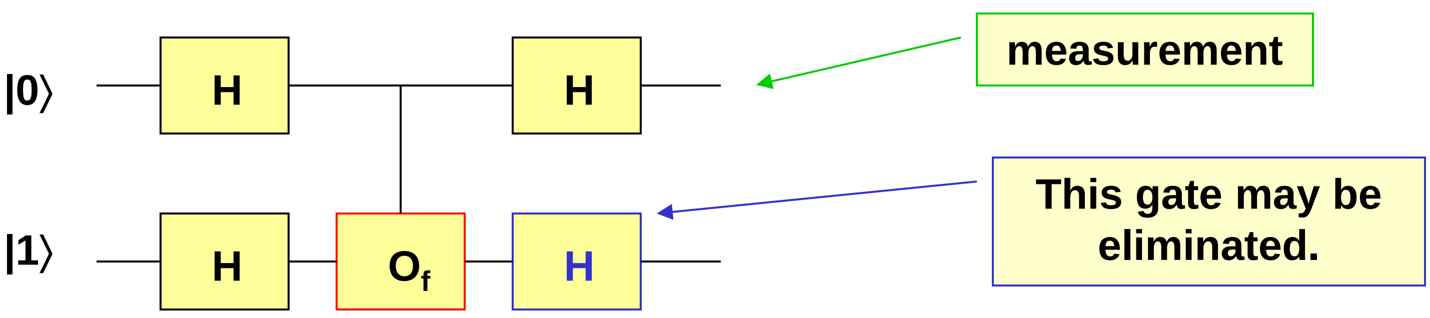
Question: Is f balanced?

A Quantum Algorithm for Deutsch's Problem

✓ Here is a quantum algorithm of Cleve, Ekert, Macchiavello, and Mosca (1998)

1. Initially, prepare $|0\rangle|1\rangle$.
2. Apply $H \otimes H$.
3. Apply O_f.
4. Apply $H \otimes H$.
5. Observe the first register w.r.t. computational basis $\{|0\rangle, |1\rangle\}$.
6. If 1 is observed, then output YES, or else NO.

We query only once!



Analysis of the Quantum Algorithm I

Step 2

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

$$=\frac{1}{2}\left(|0\rangle|0\rangle+|1\rangle|0\rangle-|0\rangle|1\rangle-|1\rangle|1\rangle\right)=\frac{1}{2}\left[|0\rangle\left(|0\rangle-|1\rangle\right)+|1\rangle\left(|0\rangle-|1\rangle\right)\right]$$

Step 3

oracle query/answer

$$O_f(H\otimes H)|0\rangle|1\rangle=\frac{1}{2}\left[|0\rangle\left(|0\oplus f(0)\rangle-|1\oplus f(0)\rangle\right)+|1\rangle\left(|0\oplus f(1)\rangle-|1\oplus f(1)\rangle\right)\right]$$

oracle query/answer

$$=\frac{1}{2}\left[(-1)^{f(0)}|0\rangle+(-1)^{f(1)}|1\rangle\right]\left(|0\rangle-|1\rangle\right)$$

Analysis of the Quantum Algorithm II

Step 4

$$(H \otimes H) O_f (H \otimes H)|0\rangle|1\rangle = \frac{1}{2}\Big[(-1)^{f(0)} H|0\rangle + (-1)^{f(1)} H|1\rangle\Big] \otimes \big[H|0\rangle - H|1\rangle\big]$$

$$= \frac{1}{4}\Big[(-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle)\Big] \otimes \Big[(|0\rangle + |1\rangle) - (|0\rangle - |1\rangle)\Big]$$

$$= \frac{1}{2}\Big[\Big((-1)^{f(0)} + (-1)^{f(1)}\Big)|0\rangle + \Big((-1)^{f(0)} - (-1)^{f(1)}\Big)|1\rangle\Big] \otimes |1\rangle$$

$$= (-1)^{f(0)}|f(0) \oplus f(1)\rangle|1\rangle$$

Measurement

Step 5

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

Quantum State Identity Testing

- Let us consider the problem of determining if given two (classical) binary strings s and t are identical.
- How can we solve this question?
- A simple solution is to look at these strings and check each pair of corresponding bits are exactly the same.
- What if we are given two unknown quantum states instead of the two binary strings?
- Unfortunately, we cannot physically look at the quantum states because the observation destroys the original quantum states!

Quantum State Identity Testing Problem

- Is there any way to check the identity of two unknown quantum states without looking at them?
- More specifically, let us consider the following promise problem.

- Quantum State Identity Testing Problem (2QSITP)
  - Input: two quantum states $|\varphi\rangle$ and $|\psi\rangle$ of the same dimension.
  - Promise: $|\varphi\rangle$ and $|\psi\rangle$ are either equal or orthogonal
  - Question: are $|\varphi\rangle$ and $|\psi\rangle$ identical?

- In the next slide, we will give a simple quantum algorithm that solves this 2QSITP.

SWAP TEST Algorithm for 2QSITP I

- The following SWAP TEST algorithm solves 2QSITP.

➢ SWAP TEST

1. Start with the three registers that contain $|0\rangle \otimes |\varphi\rangle \otimes |\psi\rangle$.
2. Apply H to the first register.
3. Conditionally swap the second and third registers; namely, if the first register contains 1, then swap the two registers; otherwise, do nothing. We do not need to look at the quantum states!
4. Apply H again to the first register.
5. Measure the first register. If we observe 0, then output 1 (YES); otherwise, output 0 (NO).

SWAP TEST Algorithm for 2QSITP II

- SWAP TEST algorithm enjoys the following properties.
- Proposition: [Kada-Nishimura-Yamakami (2008)]

  For any YES instance to 2QSITP, SAWP TEST outputs YES with certainty and, for any NO instance, it outputs NO with error probability exactly 1/2.
- One-sided error requirement says that, for any YES instance to 2QSITP, a given algorithm must output YES (1) with certainty (i.e., probability 1).
- Proposition: [Kobayashi-Matsumoto-Yamakami (2009)]

  Under the one-sided error requirement, SWAP TEST is an optimal operation to solve 2QSITP.

Analysis of SAWP TEST Ⅰ

- To show the first proposition, we give a close analysis of SAWP TEST algorithm.

Step 1

$$|0\rangle \otimes |\varphi\rangle|\psi\rangle$$

Step 2

$$\left(H \otimes I^2\right)|0\rangle|\varphi\rangle|\psi\rangle = H|0\rangle \otimes |\varphi\rangle|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes |\varphi\rangle|\psi\rangle$$

$$= \frac{1}{\sqrt{2}}|0\rangle|\varphi\rangle|\psi\rangle + \frac{1}{\sqrt{2}}|1\rangle|\varphi\rangle|\psi\rangle.$$

Step 3

$$CSWAP\left(H \otimes I^2\right)|0\rangle|\varphi\rangle|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|\varphi\rangle|\psi\rangle + \frac{1}{\sqrt{2}}|1\rangle\overbrace{|\psi\rangle|\varphi\rangle}^{\text{Swap}}.$$

Analysis of SAWP TEST II

Step 4

$$\left(H \otimes I^2\right) CSWAP \left(H \otimes I^2\right) |0\rangle |\varphi\rangle |\psi\rangle$$

$$= \frac{1}{2}\left[|0\rangle + |1\rangle\right] \otimes |\varphi\rangle |\psi\rangle + \frac{1}{2}\left[|0\rangle - |1\rangle\right] \otimes |\psi\rangle |\varphi\rangle$$

$$= \frac{1}{2}|0\rangle\left[|\varphi\rangle|\psi\rangle + |\psi\rangle|\varphi\rangle\right] + \frac{1}{2}|1\rangle\left[|\varphi\rangle|\psi\rangle - |\psi\rangle|\varphi\rangle\right].$$

Step 5

Measurement

Measurement

$$= \begin{cases} |0\rangle|\varphi\rangle|\psi\rangle & \text{if} \quad |\varphi\rangle = |\psi\rangle, \\ \frac{1}{2}|0\rangle\left[|\varphi\rangle|\psi\rangle + |\psi\rangle|\varphi\rangle\right] + \frac{1}{2}|1\rangle\left[|\varphi\rangle|\psi\rangle - |\psi\rangle|\varphi\rangle\right] & \text{if} \quad |\varphi\rangle \neq |\psi\rangle. \end{cases}$$

- If $\langle\varphi|\psi\rangle=0$ (orthogonal), it follows that $\||\varphi\rangle|\psi\rangle-|\psi\rangle|\varphi\rangle\|=\sqrt{2}$. Thus, 1 is observed with probability $(\sqrt{2} / 2)^2 = 1/2$.

Identity Testing of n Objects

- Kada, Nishimura, and Yamakami (2008) studied the identity testing of n objects, where $n \geq 2$.

- n Quantum State Identity Testing Problem (nQSITP)
  - Input: n quantum states $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_n\rangle$ of the same dimension
  - Promise: any pair of the quantum states is either equal or orthogonal
  - Question: are all of $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_n\rangle$ identical?

- Kada, Nishimura, and Yamakami (2008) proposed several quantum algorithms to solve this nQSITP.

PERMUTATION TEST

- Here is one of quantum algorithms proposed by Kada, Nishimura, and Yamakami (2008) to solve nQSITP for any $n \geq 2$.

➢ PERMUTATION TEST

1. Start with the n+1 registers that contain $|0\rangle \otimes |\varphi_1\rangle \otimes \ldots \otimes |\varphi_n\rangle$.
2. Apply QFT $F_{n!}$ over n! elements to $|0\rangle$.
3. Apply a controlled-σ operator; i.e., if the first register is $i \in \{0,1,\ldots,n!-1\}$, transform $|\varphi_1\rangle \otimes \ldots \otimes |\varphi_n\rangle$ to $|\varphi_{\sigma i(1)}\rangle \otimes \ldots \otimes |\varphi_{\sigma i(n)}\rangle$, where σ_i is the i-th permutation over n! elements.
4. Apply $(F_{n!})^{-1}$ to the first register.
5. Measure the first register. If we observe 0, then output 1 (YES); otherwise, output 0 (NO).

CIRCLE TEST

- We see another quantum algorithm of Kada, Nishimura, and Yamakami (2008) for nQSITP.

➢ CIRCLE TEST

1. Start with the n+1 registers that contain $|0\rangle\otimes|\varphi_1\rangle\otimes\ldots\otimes|\varphi_n\rangle$.
2. Apply QFT F_n over n elements to $|0\rangle$.
3. Apply a controlled-σ operator; i.e., if the first register is $i\in\{0,1,\ldots,n-1\}$, transform $|\varphi_1\rangle\otimes\ldots\otimes|\varphi_n\rangle$ to $|\varphi_{\sigma i(1)}\rangle\otimes\ldots\otimes|\varphi_{\sigma i(n)}\rangle$, where $\sigma(k)=k+1$ and $\sigma(n)=1$ for all $k\in[n-1]$, and σ^i is obtained by the i applications of σ.
4. Apply $(F_n)^{-1}$ to the first register.
5. Measure the first register. If we observe 0, then output 1 (YES); otherwise, output 0 (NO).

Efficiency of the Quantum Algorithms

- Proposition: [Kada-Nishimura-Yamakami (2008)]

  Let $n \geq 2$. For any YES instance to nQSITP, PERMUTATION TEST outputs YES with certainty and, for any NO instance, it outputs NO with error probability at most $1/n$.

- Proposition: [Kada-Nishimura-Yamakami (2008)]

  Let n be any prime number. For any YES instance to nQSITP, PERMUTATION TEST outputs YES with certainty and, for any NO instance, it outputs NO with error probability at most $1/n$.

- Proposition: [Kada-Nishimura-Yamakami (2008)]

  Under the one-sided error requirement, PERMUTATION TEST is an optimal operation to solve nQSITP for $n \geq 2$.

Important Quantum Algorithms

- Shor's integer factorization algorithm
  - Find all factors of each given natural number.
  - The fastest classical algorithm (so far) requires exponential time.
  - A quantum algorithm takes $O(n^2 log^2 n)$ time.

- Grover's database search algorithm
  - Find a unique key in database of *N* locations.
  - The classical algorithm needs *N-1* accesses in worst case.
  - A quantum algorithm needs $(\pi/4)\sqrt{N}$ accesses.

What is Integer Factorization Problem?

Integer Factorization Problem (IFP)

Input: nonnegative integer n

Output: all prime factors of n

Example:

Let n = 33957.

The prime factors are {3,7,11} because $33957 = 3^2 \times 7^3 \times 11$.

Unfortunately, the Integer Factorization Problem seems very difficult to solve; there is no known fast classical algorithm that solves the problem.

Why is Factorization Difficult?

Computational Problem: Find all the prime factors of the following number.

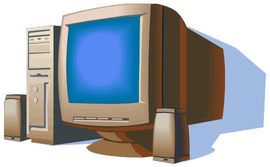
2799783391122132787082946763872260162107044678
6955428537560009929326128400010760934567105295
5360856061822351910951365788637105954482006576
7750985805576135790987349501441788631789462951
8723786922182398 3

$=$

3532461934402770121272604 9781984643686711974001976 2502364930346877612125367 9423200058547956528088349	$\times$	7925869954478333033347085 8414800596877379758573642 1996073433034145576787281 8152135381409304740185467

We needed to run 80 computers for 3 months to obtain the above factors.

How Fast does Factoring Go?



Classical Case

Future factoring times on networks of 1000 classical workstations (whose power increases by Moore's law).

number of bits	1024	2048	4096
factoring in 2006	10^5 years	5×10^{15} years	3×10^{29} years
factoring in 2024	38 years	10^{12} years	7×10^{25} years
factoring in 2042	3 days	3×10^{8} years	2×10^{22} years

Quantum Case

Factoring on quantum computers with minimal clock speed of 100MHz.

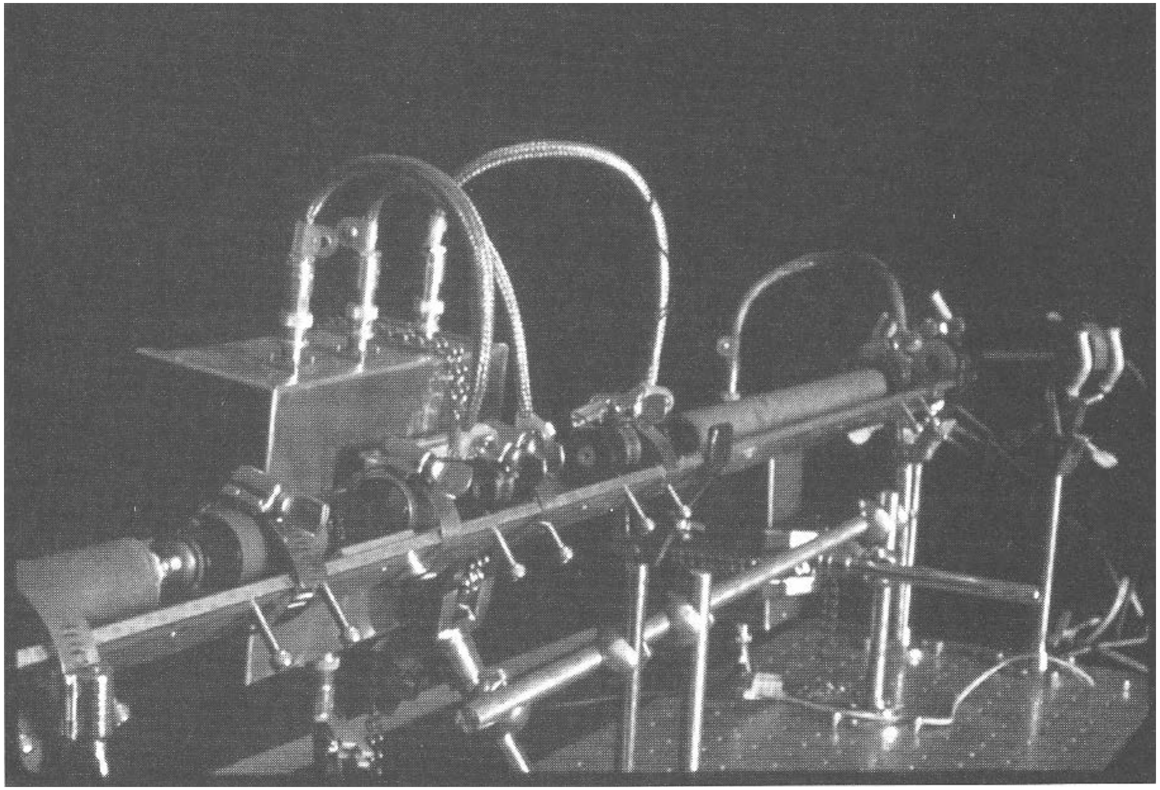
size in bits	1024	2048	4096
number of qubits	5124	10244	20484
number of gates	3×10^{9}	2×10^{11}	2×10^{12}
factoring time	4.5 min.	36 min.	4.8 hours

IV. Quantum Teleportation

1. First Quantum Crypto Machine
2. Quantum Teleportation Basics
3. A Quantum Teleportation Circuit
4. Analysis of Quantum Circuit
5. Another Teleportation Circuit

First Quantum Crypto Machine

The first quantum cryptography machine built by IBM in 1989.



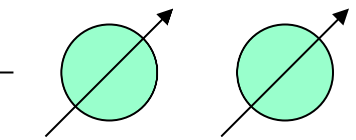
Quantum Teleportation Basics

Quantum teleportation is a way of sending quantum information without actually sending qubits.

An unknown qubit

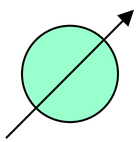
$|\varphi\rangle$

An EPR pair



$$|\psi\rangle = \tfrac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right)$$

Alice

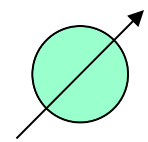


$|\varphi\rangle$

ab

4. Alice tells Bob about her measured results ab.

ab



$|\varphi\rangle$

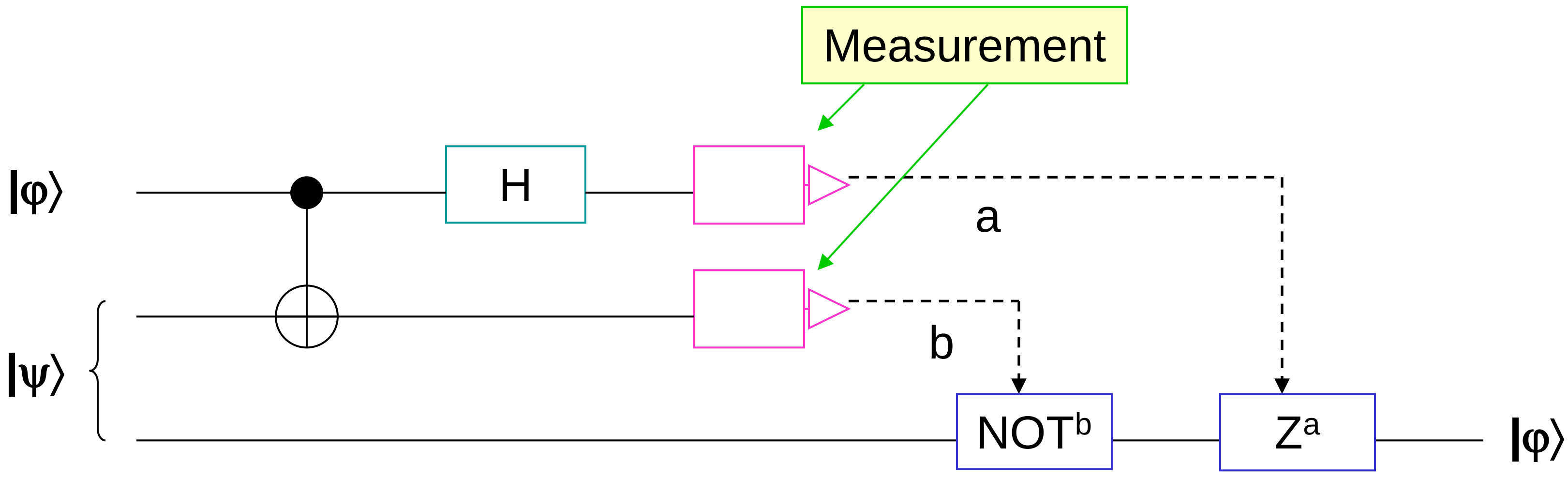
Bob

1. Alice applies CNOT.
2. Alice applies H⊗I.
3. Alice measures two qubits.

5. Bob receives two bits ab.
6. Bob applies two quantum gates.
7. Bob creates $|\varphi\rangle$.

A Quantum Teleportation Circuit

- Quantum teleportation can be realized by the following quantum circuit.



|ψ⟩ = the EPR pair

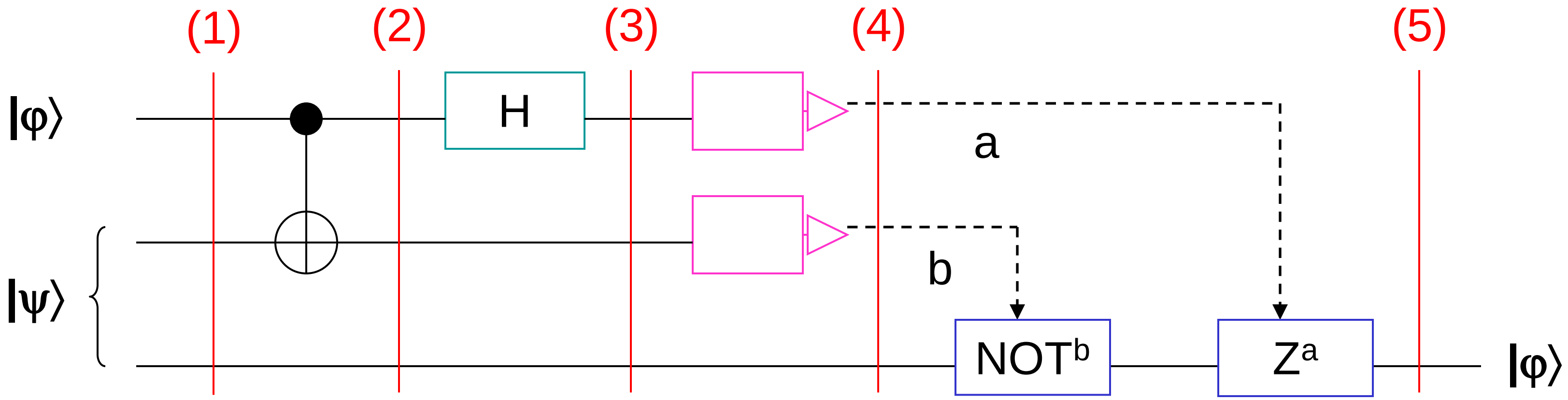
|φ⟩= unknown qubit

$$NOT^b = \begin{cases} NOT & \text{if } b = 1 \\ I & \text{if } b = 0 \end{cases} \qquad Z^a = \begin{cases} Z & \text{if } a = 1 \\ I & \text{if } a = 0 \end{cases}$$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Analysis of Quantum Circuit I

- Let us analyze the given quantum circuit.



Assume that $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$

Recall that $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$

Analysis of Quantum Circuit II

Step (1)

$$\left|\xi_1\right\rangle = \left|\varphi\right\rangle\left|\psi\right\rangle = \left(\alpha\left|0\right\rangle + \beta\left|1\right\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left(\alpha\left|000\right\rangle + \beta\left|100\right\rangle + \alpha\left|011\right\rangle + \beta\left|111\right\rangle\right)$$

Step (2)

$$\left|\xi_2\right\rangle = \left(CNOT \otimes I\right)\left|\xi_1\right\rangle = \frac{1}{\sqrt{2}}\left(\alpha\left|000\right\rangle + \beta\left|110\right\rangle + \alpha\left|011\right\rangle + \beta\left|101\right\rangle\right)$$

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

Analysis of Quantum Circuit III

Step (3)

$$
\begin{aligned}
\left|\xi_3\right\rangle &= \left(H \otimes I^{\otimes 2}\right)\left|\xi_2\right\rangle \\
&= \frac{\alpha}{2}\left(|0\rangle + |1\rangle\right)\left(|00\rangle + |11\rangle\right) + \frac{\beta}{2}\left(|0\rangle - |1\rangle\right)\left(|10\rangle + \beta|01\rangle\right) \\
&= \frac{1}{2}|00\rangle\left(\alpha|0\rangle + \beta|1\rangle\right) + \frac{1}{2}|01\rangle\left(\beta|0\rangle + \alpha|1\rangle\right) + \\
&\qquad + \frac{1}{2}|10\rangle\left(\alpha|0\rangle - \beta|1\rangle\right) + \frac{1}{2}|11\rangle\left(-\beta|0\rangle + \alpha|1\rangle\right) \\
&= \frac{1}{2}|00\rangle|\varphi\rangle + \frac{1}{2}|01\rangle \otimes NOT|\varphi\rangle + \frac{1}{2}|10\rangle \otimes Z|\varphi\rangle + \frac{1}{2}|11\rangle \otimes \left(NOT \cdot Z\right)|\varphi\rangle \\
&= \frac{1}{2}\sum_{a,b\in\{0,1\}} |ab\rangle \otimes \left(NOT^{b} \cdot Z^{a}|\varphi\rangle\right)
\end{aligned}
$$

Analysis of Quantum Circuit IV

Step (4)

- After measurement, assume that we obtain $|ab\rangle$ with probability 1/4.
- We then obtain a normalized quantum state $|\xi_4\rangle$.

$$\left|\xi_4\right\rangle = \left(NOT^b \cdot Z^a\right)\left|\varphi\right\rangle$$

Step (5)

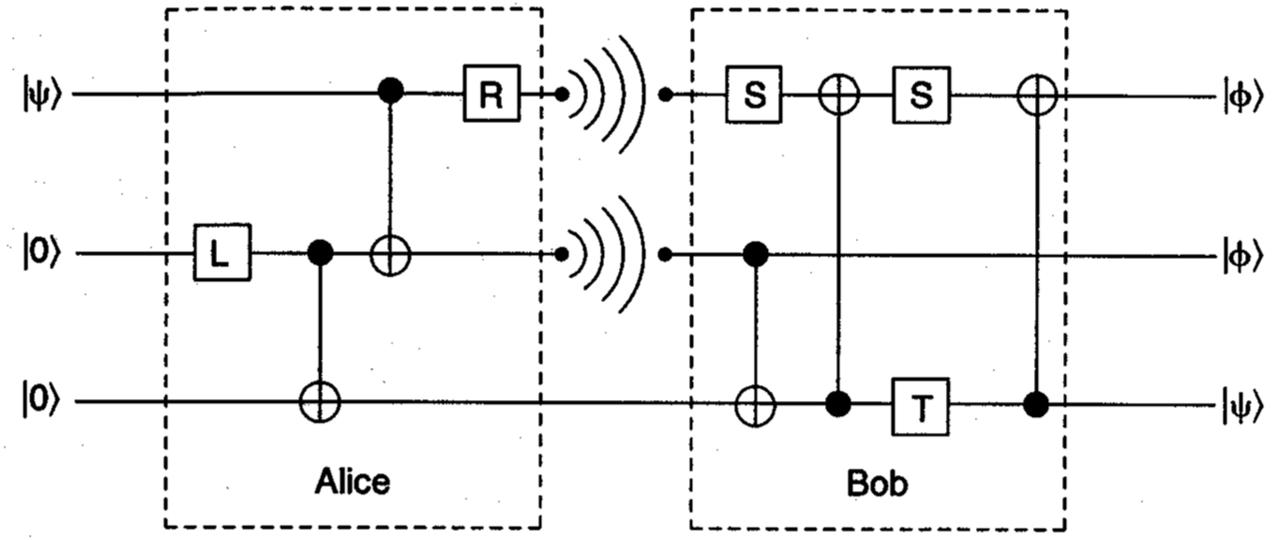
- We then apply $Z^a \cdot NOT^b$ to $|\xi_4\rangle$.
- We then obtain a quantum state $|\xi_5\rangle$.

$$\left|\xi_5\right\rangle = \left(Z^a \cdot NOT^b\right)\left|\xi_4\right\rangle$$

$$= \left(Z^a \cdot NOT^b\right)\left(NOT^b \cdot Z^a\right)\left|\varphi\right\rangle = \left|\varphi\right\rangle$$

Another Teleportation Circuit

- Here is a different quantum circuit that can teleport any unknown state from Alice to Bob.



$$L = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \qquad R = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \qquad S = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \qquad T = \begin{pmatrix} -1 & 0 \\ 0 & -i \end{pmatrix}$$

Thank you for listening

Q & A

I’m happy to take your question!

END