Quantum Computing

Chao Liang

School of Computer Science
Wuhan University

Review: Lecture 5

- **Composite Systems**
  - Tensor Product
    - Tensor product allows parallel action
  - Assembling System
    - Tensor product of states and acts, graphs and matrices
  - Assembling Quantum System
    - Assembling of independent quantum systems have the tensor product as its state space

Lecture 6: Quantum Gates

1 Bits and Qubits

- Definitions: bit and qubit
- Relation between bit and qubit
- Definitions: byte and qubyte
- Vector representation of qubits

2 Classical Gates

- NOT gate
- AND gate
- OR gate
- NAND gate
- 功能完备与通用门
- Sequential and Parallel Operations

3 Reversible Gates

- Motivation
- Controlled-NOT gate
- Toffoli gate
- Fredkin gate

4 Quantum Gates

- Definition
- Geometric representation
- Phase shift gate
- Controlled-U gate
- Deutsch gate
- No-Clone Theorem

1. Bits and Qubits

- Definition: bit
  - A bit is a unit of information describing a two-dimensional classical system
    - a bit is a way of describing a system whose set of states is of size 2
    - A bit can be either in state $|0\rangle$ or in state $|1\rangle$, i.e., a 2-by-1 binary matrix

$$|0\rangle = \begin{matrix} \mathbf{0} \\ \mathbf{1} \end{matrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{matrix} \mathbf{0} \\ \mathbf{1} \end{matrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

1. Bits and Qubits

- Definition: qubit
  - A quantum bit or a qubit is a unit of information describing a two dimensional quantum system
    - We shall represent a qubit as a 2-by-1 matrix with complex numbers

$$\begin{matrix} \mathbf{0} \\ \mathbf{1} \end{matrix} \begin{bmatrix} c_0 \\ c_1 \end{bmatrix},$$

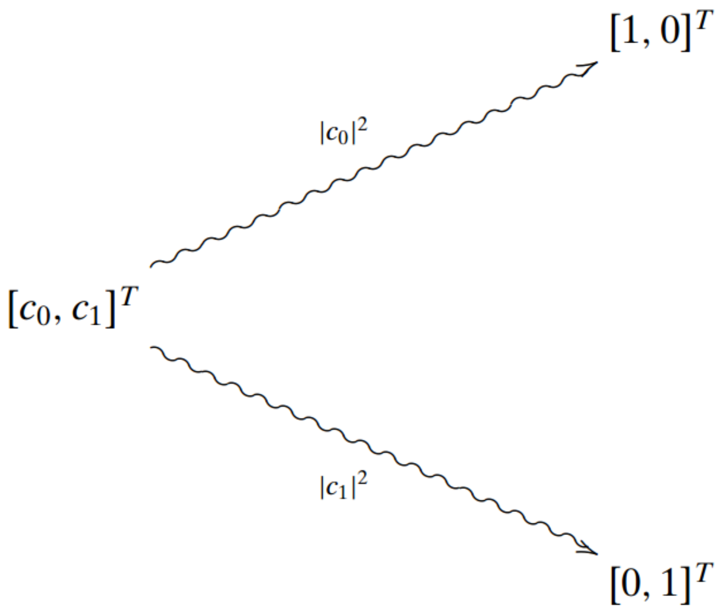
where $|c_0|^2 + |c_1|^2 = 1$

The probability that the qubit will be found in state $|1\rangle$ after measurement

（感谢弘毅学堂2020级王骏峣同学纠正英文语法错误）

1. Bits and Qubits

- Relation between bit and qubit



$$\begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = c_0 \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} + c_1 \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = c_0|0\rangle + c_1|1\rangle$$

will be found in state $|1\rangle$. Whenever we measure a qubit, it automatically becomes a bit. So we shall never "see" a general qubit. Nevertheless, they do exist and are the

1. Bits and Qubits

- Byte and Qubyte
  - 8 bits: 01101011
  - Vector representation of bits

$$\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}$$

  - Tensor product representation

$$|0\rangle \otimes |1\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle \otimes |1\rangle$$

    - An element of $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$

1. Bits and Qubits

- Byte
  - 8 bits together

$$\begin{array}{l} 00000000 \\ 00000001 \\ \vdots \\ 01101010 \\ 01101011 \\ 01101100 \\ \vdots \\ 11111110 \\ 11111111 \end{array} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix}$$

8 binary numbers to indicate a byte

VS

- Qubyte
  - 8 qubits together

$$\begin{array}{l} 00000000 \\ 00000001 \\ \vdots \\ 01101010 \\ 01101011 \\ 01101100 \\ \vdots \\ 11111110 \\ 11111111 \end{array} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{106} \\ c_{107} \\ c_{108} \\ \vdots \\ c_{254} \\ c_{255} \end{bmatrix}$$

where $\sum_{i=0}^{255} |c_i|^2 = 1.$

2^8=256 complex numbers to indicate a qubyte

1. Bits and Qubits

- A qubit pair （two qubits）
  - Ket notation $|0\rangle \otimes |1\rangle$ or $|0 \otimes 1\rangle$
  - Vector representation
    - 4-by-1 matrix

$$\begin{matrix} \mathbf{00} \\ \mathbf{01} \\ \mathbf{10} \\ \mathbf{11} \end{matrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

  - Linear combination
    - $|\psi\rangle = c_{0,0}|00\rangle + c_{0,1}|01\rangle + c_{1,0}|10\rangle + c_{1,1}|11\rangle$

2. Classical Gates

- Classical logical gates
  - Ways of manipulating bits
    - Binary matrices

$$(2^m\text{-by-}2^n) \star (2^n\text{-by-}1) = (2^m\text{-by-}1)$$

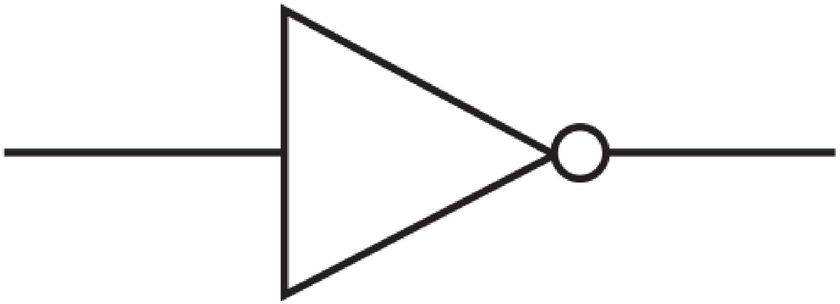
Logical gate

n input bits

m output bits

2. Classical Gates

- NOT gate

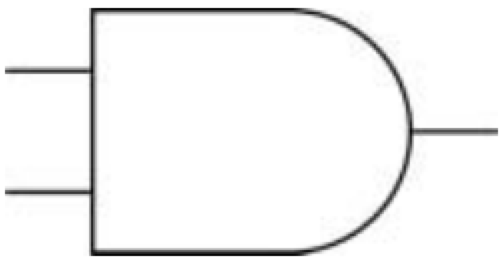


$$\mathrm{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

2. Classical Gates

- AND gate



$$\text{AND} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$\text{AND}|11\rangle = |1\rangle$

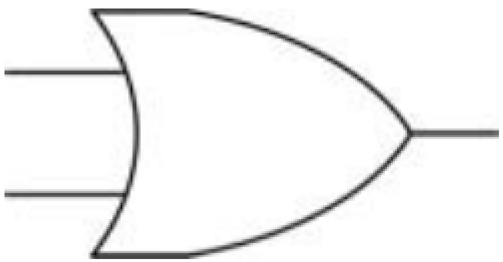
$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$\text{AND}|01\rangle = |0\rangle$

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

2. Classical Gates

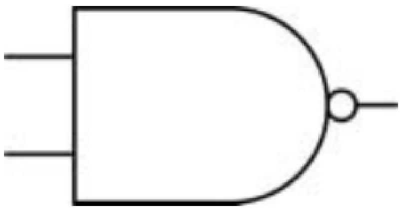
- OR gate



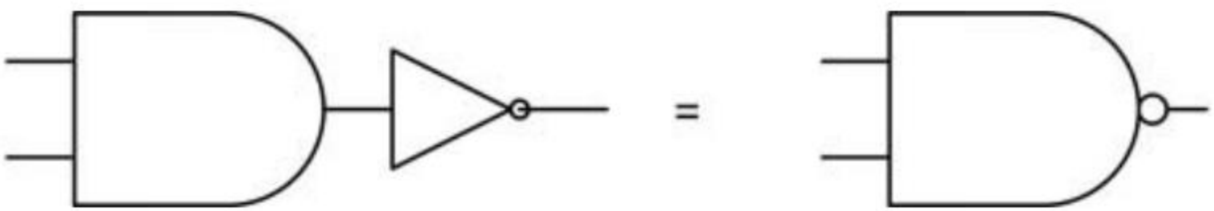
$$\mathrm{OR} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

2. Classical Gates

- NAND gate



$$\mathrm{NAND} = \begin{array}{c} \\ \mathbf{0} \\ \mathbf{1} \end{array} \begin{array}{c} \begin{array}{cccc} \mathbf{00} & \mathbf{01} & \mathbf{10} & \mathbf{11} \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$



$$NOT \star AND = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \star \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} = \mathrm{NAND}$$

补充材料：功能完备与通用门

- 逻辑等价

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

P	Q	$\neg P$	$\neg Q$	$\neg P \wedge \neg Q$	$\neg(\neg P \wedge \neg Q)$
T	T	F	F	F	T
T	F	F	T	F	T
F	T	T	F	F	T
F	F	T	T	T	F

$$P \vee Q \equiv \neg(\neg P \wedge \neg Q)$$

- 这意味着任何“或”都可以被“与”和“非”替代

来源于：《人人可懂的量子计算》，Chris Bernhardt著，邱道文等译，机械工业出版社，2020年

补充材料：功能完备与通用门

■ 逻辑等价

P	Q	$P \oplus Q$
T	T	F
T	F	T
F	T	T
F	F	F

$$P \oplus Q \equiv (P \wedge \neg Q) \vee (\neg P \wedge Q)$$

$$P \vee Q \equiv \neg(\neg P \wedge \neg Q)$$

$$P \oplus Q \equiv \neg(\neg(P \wedge \neg Q) \wedge (\neg(\neg P \wedge Q)))$$

- 这意味着“异或”也可以被“与”和“非”替代

来源于：《人人可懂的量子计算》，**Chris Bernhardt著，邱道文等译，机械工业出版社，2020年**

补充材料：功能完备与通用门

- 布尔函数

P	Q	R	$f(P,Q,R)$
T	T	T	
T	T	F	
T	F	T	
T	F	F	
F	T	T	
F	T	F	
F	F	T	
F	F	F	

需要填充 8 个值。对每个值，我们有两种选择，总计 2^8 种函数。我们会展示不管如何选择函数，都能找到仅用函数 $\neg$ 和 $\wedge$ 的等价表示。

来源于：《人人可懂的量子计算》，Chris Bernhardt著，邱道文等译，机械工业出版社，2020年

补充材料：功能完备与通用门

■ 功能完备性

P	Q	R	$f(P,Q,R)$
T	T	T	F
T	T	F	F
T	F	T	T
T	F	F	F
F	T	T	F
F	T	F	T
F	F	T	F
F	F	F	T

$$f(P,Q,R) \equiv (P\wedge\neg Q\wedge R)\vee(\neg P\wedge Q\wedge\neg R)\vee(\neg P\wedge\neg Q\wedge\neg R)$$

$$P\vee Q \equiv \neg(\neg P\wedge\neg Q)$$

$$f(P,Q,R) \equiv \neg(\neg(P\wedge\neg Q\wedge R)\wedge\neg(\neg P\wedge Q\wedge\neg R))\vee(\neg P\wedge\neg Q\wedge\neg R)$$

$$P\vee Q \equiv \neg(\neg P\wedge\neg Q)$$

$$\neg(\neg[\neg(\neg(P\wedge\neg Q\wedge R)\wedge\neg(\neg P\wedge Q\wedge\neg R))]\wedge\neg[\neg P\wedge\neg Q\wedge\neg R])$$

- ｛“非”，　“与”｝是一个功能完备的布尔运算集

来源于：《人人可懂的量子计算》，Chris Bernhardt著，邱道文等译，机械工业出版社，2020年

补充材料：功能完备与通用门

■ 功能完备性

- "与非" $P\uparrow Q = \neg(P \wedge Q)$

P	$P \wedge P$	$\neg(P \wedge P)$
T	T	F
F	F	T

$$P\uparrow P \equiv \neg P$$

"非"可以表示为"与非"

P	Q	$P\uparrow Q$
T	T	F
T	F	T
F	T	T
F	F	T

$$P \wedge Q \equiv \neg\neg(P \wedge Q)$$

$$\neg(P \wedge Q) \equiv P\uparrow Q$$

$$P \wedge Q \equiv \neg(P\uparrow Q)$$

$$P \wedge Q \equiv (P\uparrow Q)\uparrow(P\uparrow Q)$$

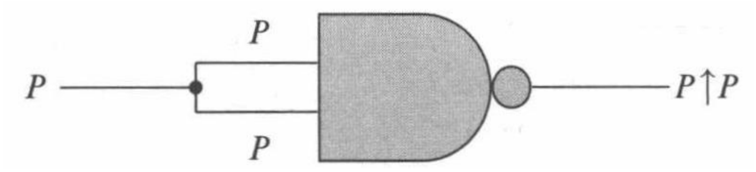
"与"可以表示为"与非"

- {"与非"}也是一个功能完备的布尔运算集

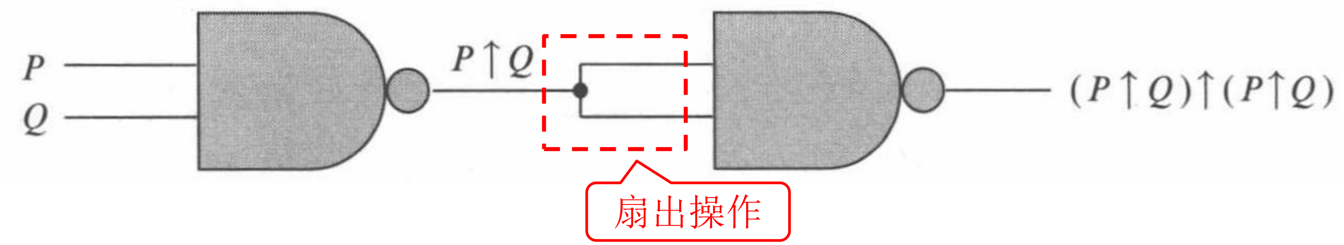
来源于：《人人可懂的量子计算》，Chris Bernhardt著，邱道文等译，机械工业出版社，2020年

补充材料：功能完备与通用门

- 与非门是一个通用门
  - “非门”的“与非门”表示



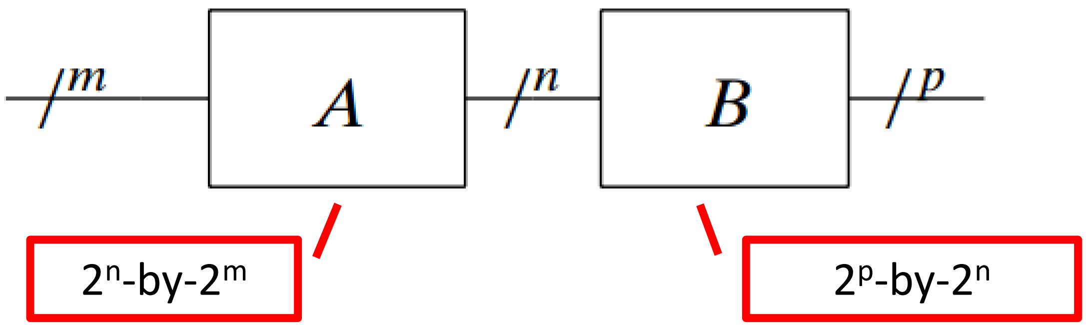
  - “与门”的“与非门”表示



来源于：《人人可懂的量子计算》，Chris Bernhardt著，邱道文等译，机械工业出版社，2020年

2. Classical Gates

- Sequential operation

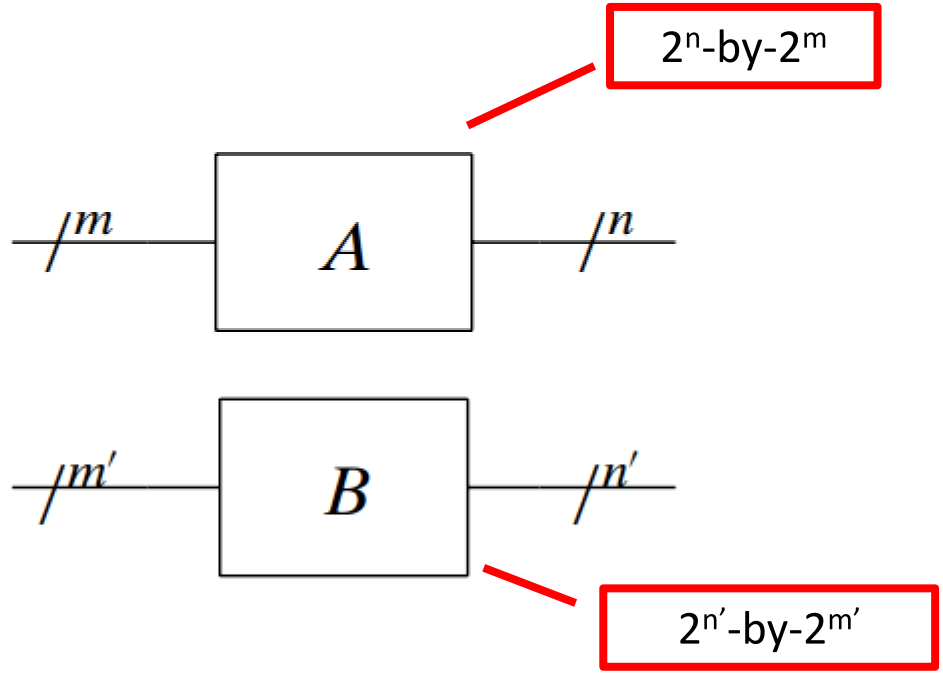


$B \star A$, which is a $(2^p\text{-by-}2^n) \star (2^n\text{-by-}2^m) = (2^p\text{-by-}2^m)$ matrix

$$\otimes: \ \mathbb{C}^{m\times m'} \times \mathbb{C}^{n\times n'} \to \mathbb{C}^{mn\times m'n'}$$

2. Classical Gates

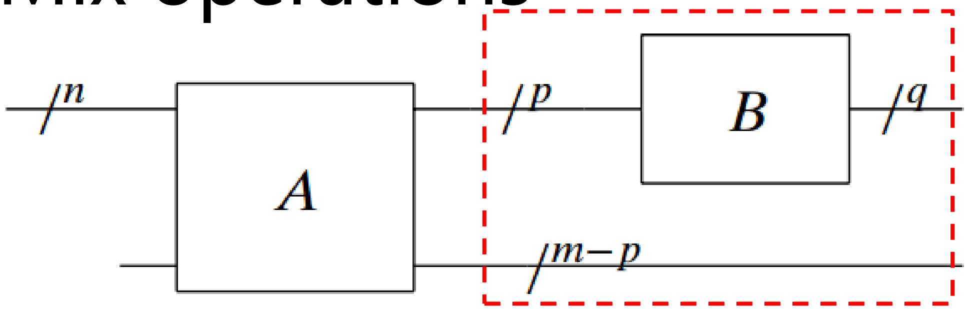
- Parallel operation



$$A \otimes B \text{ is of size } 2^n 2^{n'} = 2^{n+n'}\text{-by-}2^m 2^{m'} = 2^{m+m'}$$

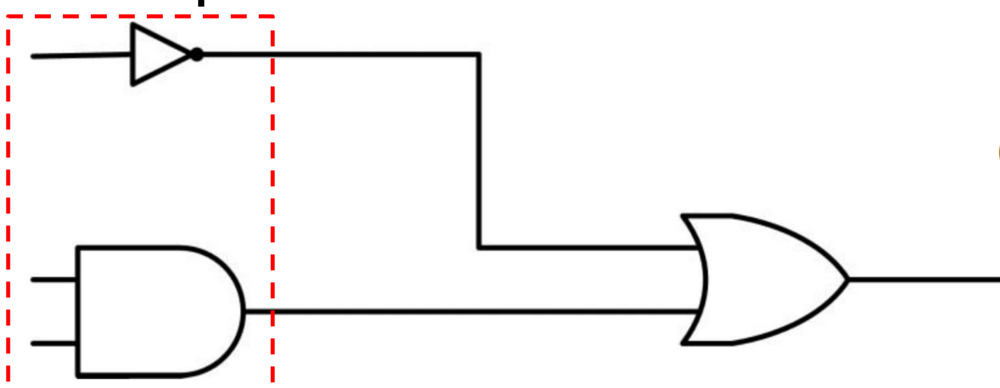
2. Classical Gates

- Mix operations



$$(B \otimes I_{m-p}) \star A$$

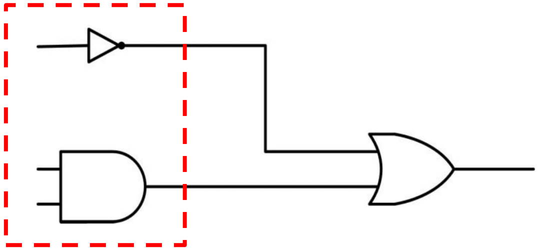
- Example



$$\text{OR} \star (\text{NOT} \otimes \text{AND})$$

2. Classical Gates

- Example 1
  - $\text{OR} \star (\text{NOT} \otimes \text{AND})$



$$\text{NOT} \otimes \text{AND} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}. \tag{5.51}$$

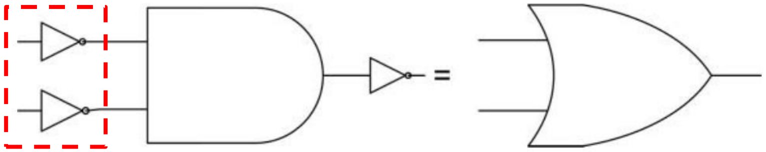
And so we get

$$\text{OR} \star (\text{NOT} \otimes \text{AND}) = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{5.52}$$

□

2. Classical Gates

- Example 2



  - $\text{NOT} \star \text{AND} \star (\text{NOT} \otimes \text{NOT}) = \text{OR}$

$$\text{NOT} \otimes \text{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}. \qquad (5.54)$$

This DeMorgan's law corresponds to the following identity of matrices:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \star \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \star \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}. \qquad (5.55)$$

3. Reversible Gates

- Motivation
  - Landauer's principle (1960s)
    - erasing information, as opposed to writing information, is what causes energy loss and heat
    - writing information is a reversible procedure while erasing is not

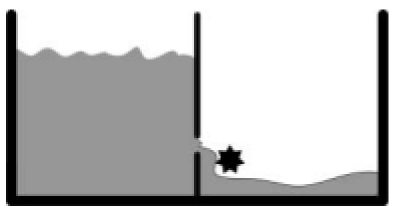


Figure 5.3. State |0⟩ dissipating and creating energy.

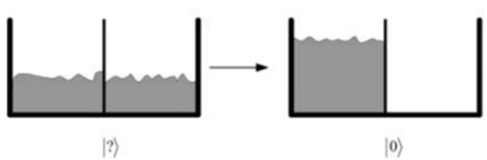


Figure 5.4. Reversibility of writing.

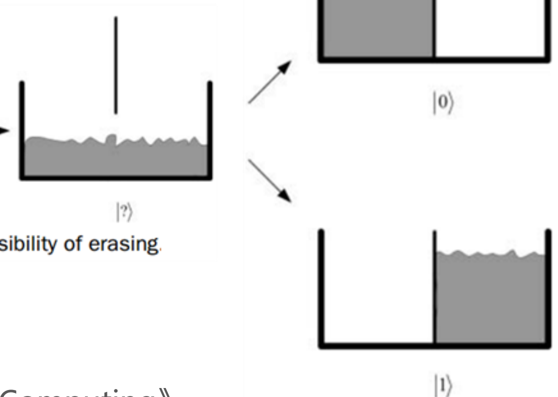
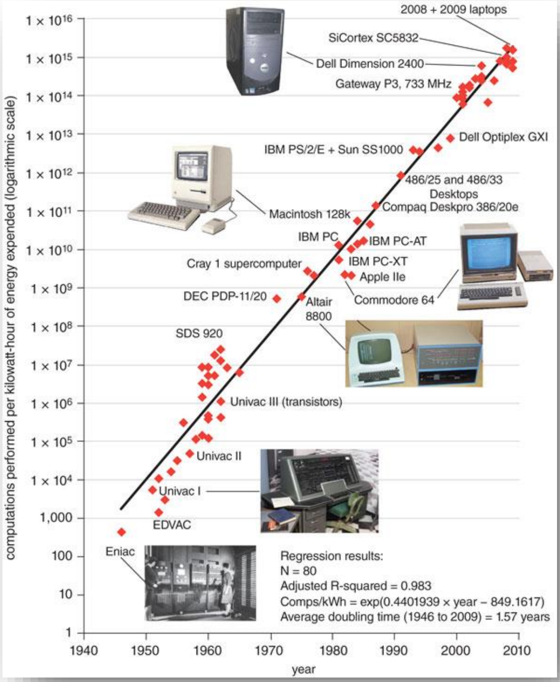


Figure 5.5. Irreversibility of erasing.

3. Reversible Gates

- Motivation
  - Bennett's thought (1970s)
    - Irreversible->erasing->energy loss
    - Reversible->no energy loss
  - Reversible circuits and programs
    - Examples: NOT, controlled-NOT, Toffoli, Fredkin, …
    - Note: AND, OR gates are irreversible



Source: https://www.americanscientist.org/article/computers-that-can-run-backwards

补充材料：可逆门

■ 门与布尔函数

与门

输入		输出
0	0	0
0	1	0
1	0	0
1	1	1

半加器

输入		输出	
		数字	进位
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

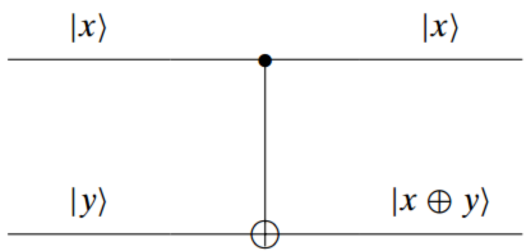
■ 可逆门与可逆函数

- 给定一组输出，是否可以确定输入？

来源于：《人人可懂的量子计算》，Chris Bernhardt著，邱道文等译，机械工业出版社，2020年

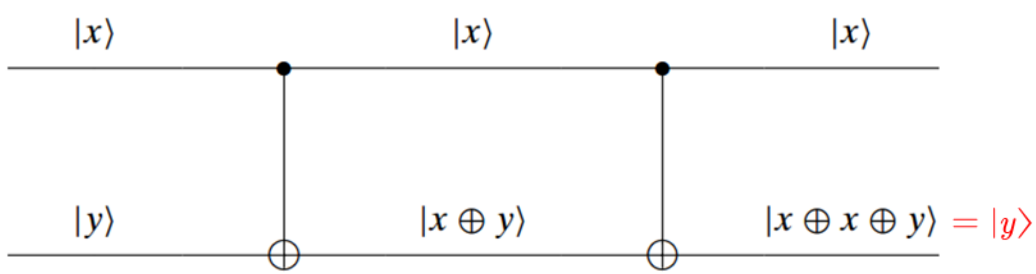
3. Reversible Gates

- Controlled-NOT gate
  - $|x,\ y\rangle \mapsto |x,\ x \oplus y\rangle$



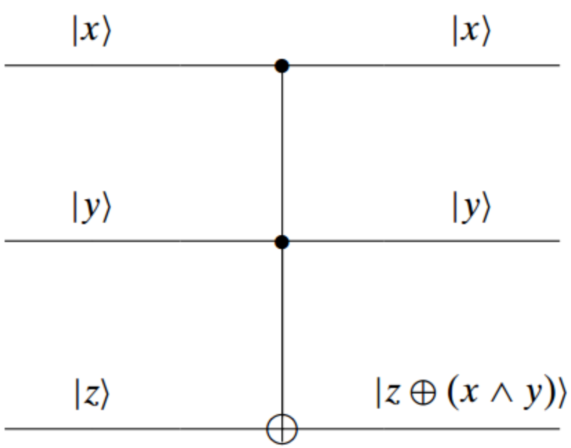
	00	**01**	**10**	**11**
00	1	0	0	0
01	0	1	0	0
10	0	0	0	1
11	0	0	1	0

  - controlled-NOT gate can be reversed by itself



3. Reversible Gates

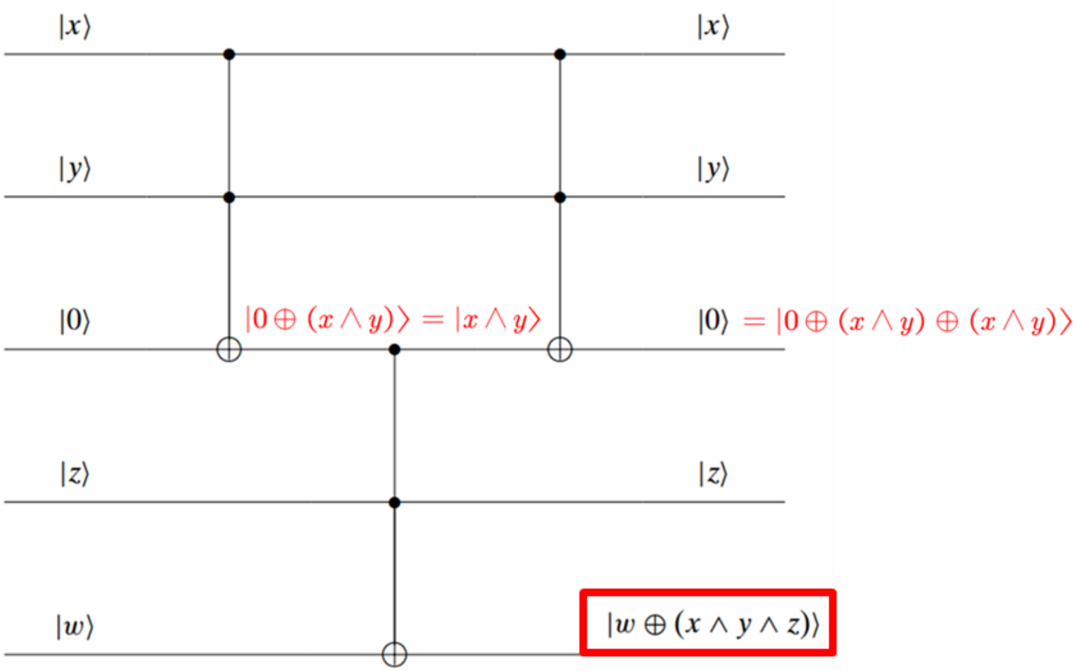
- Toffoli gate / doubly-controlled gate
  - $|x,\ y,\ z\rangle \mapsto |x,\ y,\ z \oplus (x \wedge y)\rangle$



	000	001	010	011	100	101	110	111
000	1	0	0	0	0	0	0	0
001	0	1	0	0	0	0	0	0
010	0	0	1	0	0	0	0	0
011	0	0	0	1	0	0	0	0
100	0	0	0	0	1	0	0	0
101	0	0	0	0	0	1	0	0
110	0	0	0	0	0	0	0	1
111	0	0	0	0	0	0	1	0

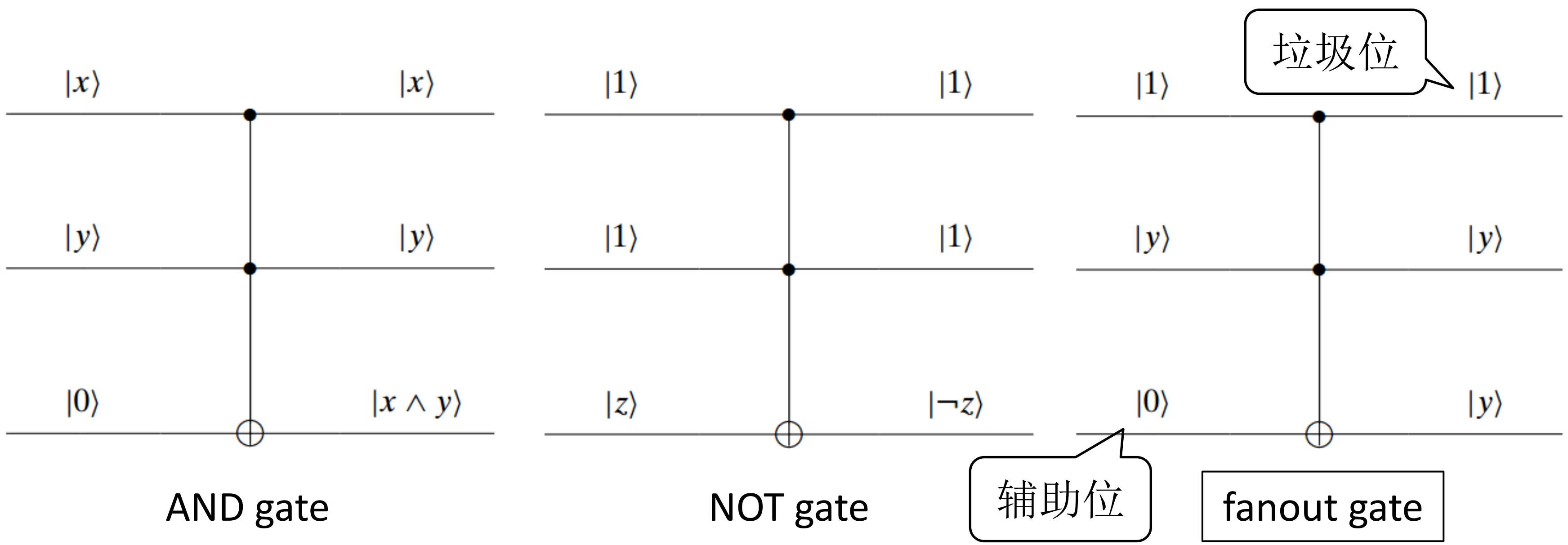
3. Reversible Gates

- Toffoli gate
  - A gate with three controlling bits



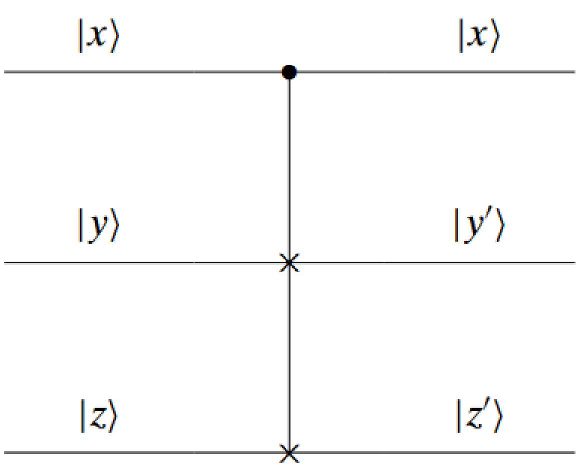
3. Reversible Gates

- Toffoli gate
  - Toffoli gate is universal（通用门）



3. Reversible Gates

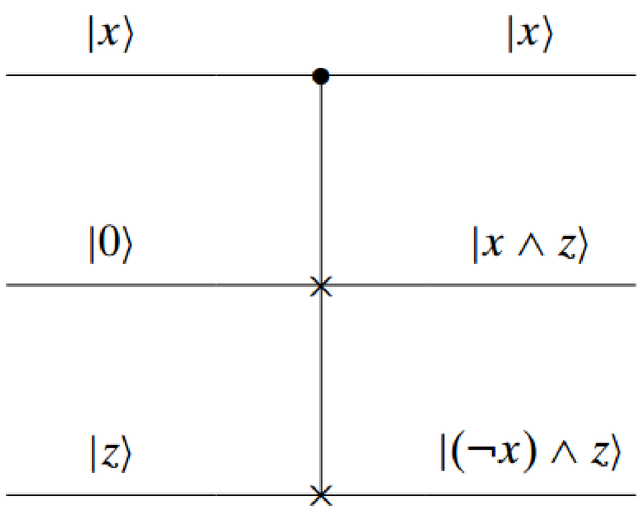
- Fredkin gate / controlled swap gate
  - $|0,\ y,\ z\rangle \mapsto |0,\ y,\ z\rangle$ and $|1,\ y,\ z\rangle \mapsto |1,\ z,\ y\rangle$



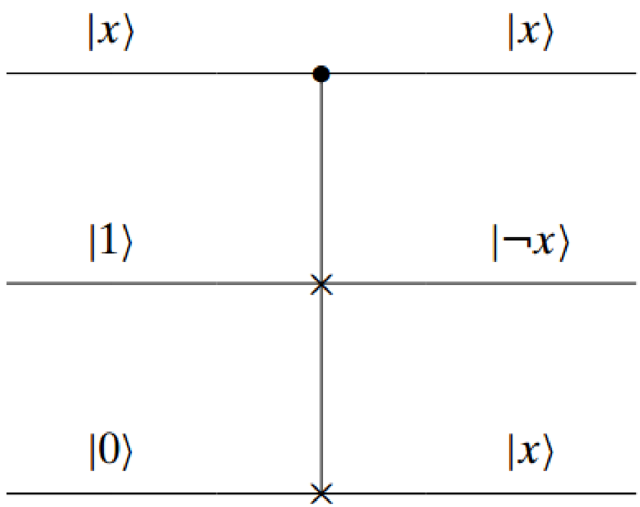
	000	001	010	011	100	101	110	111
000	1	0	0	0	0	0	0	0
001	0	1	0	0	0	0	0	0
010	0	0	1	0	0	0	0	0
011	0	0	0	1	0	0	0	0
100	0	0	0	0	1	0	0	0
101	0	0	0	0	0	0	1	0
110	0	0	0	0	0	1	0	0
111	0	0	0	0	0	0	0	1

3. Reversible Gates

- Fredkin gate
  - Fredkin gate is (also) universal



AND gate



NOT gate

4. Quantum Gates

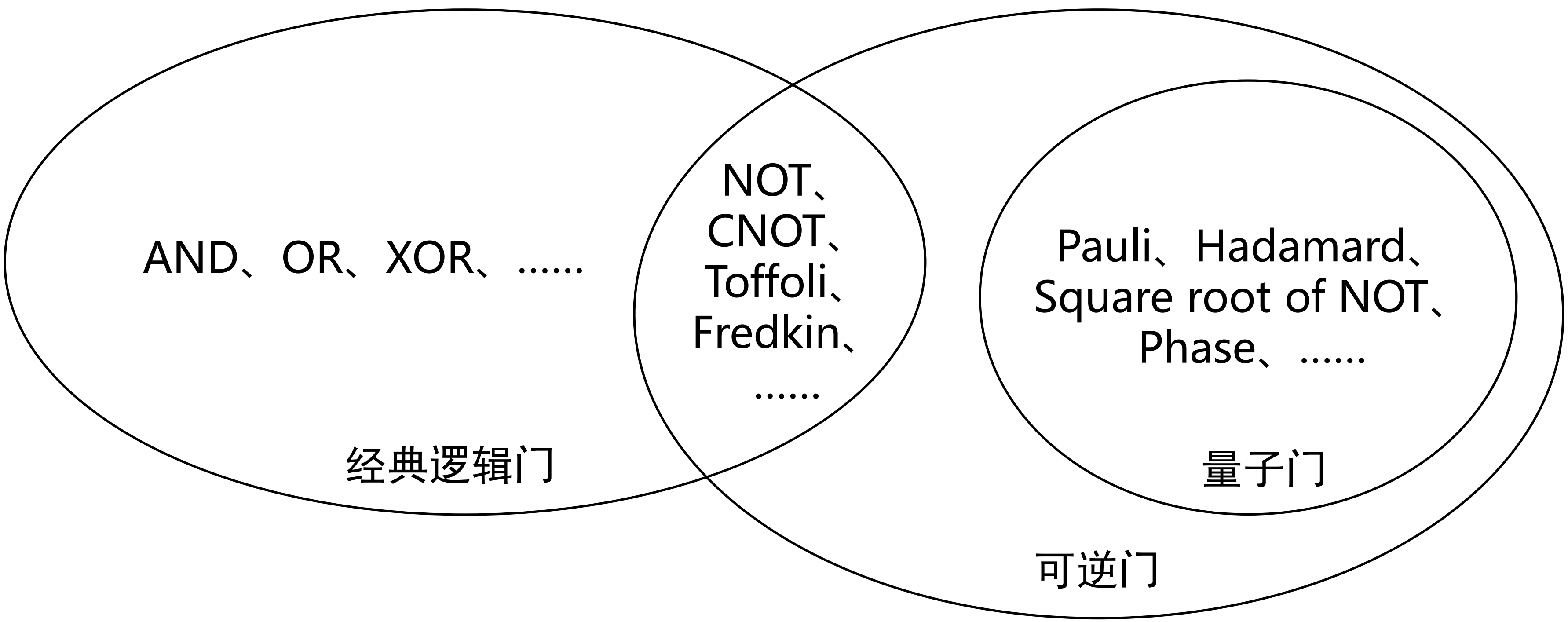
- Definition: quantum gate
  - A quantum gate is simply an operator that acts on qubits. Such operators will be represented by unitary matrices
- Remarks
  - Reversible matrix operators that work on classic bits also work on qubits, e.g., NOT, CNOT, Toffoli, and Fredkin gates
  - Some matrix operators only make sense in a quantum context, e.g., Hadamard (H) gate

4. Quantum Gates

- Examples
  - Pauli matrices: $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$
  - Square root of NOT: $\sqrt{\text{NOT}} = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$
  - Some others: $H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
  - Phase shift gate, Controlled-U gate, Deutsch gate

补充材料

■ 经典逻辑门、可逆门、量子门



Supplementary material

- Geometric representation of 1-qubit state

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle$$

- 4 real numbers -> 2 actual degrees of freedom

$$|\psi\rangle = r_0\, e^{i\phi_0}|0\rangle + r_1\, e^{i\phi_1}|1\rangle$$

- Reasons
  - Scale multiplication does not change state (4->3)

$$e^{-i\phi_0}|\psi\rangle = e^{-i\phi_0}(r_0\, e^{i\phi_0}|0\rangle + r_1\, e^{i\phi_1}|1\rangle) = r_0|0\rangle + r_1\, e^{i(\phi_1-\phi_0)}|1\rangle$$

ϕ

  - Normalization (3->2)

$$1 = |c_0|^2 + |c_1|^2 \;\Rightarrow\; r_0^2 + r_1^2 = 1$$

$r_0 = \cos(\theta)$ and $r_1 = \sin(\theta)$

（感谢弘毅学堂2019级贾祖硕同学纠正关于标量乘法不改变量子态的陈述）

Supplementary material

- Geometric representation of 1-qubit state

$$|\psi\rangle = \cos(\theta)|0\rangle + e^{i\phi}\sin(\theta)|1\rangle$$

- Latitude: $0 \leqslant \theta \leqslant \frac{\pi}{2}$
- Longitude: $0 \leqslant \phi < 2\pi$
- Problem
  - $(\theta,\ \phi)\ vs\ (\pi - \theta,\ \phi + \pi)$

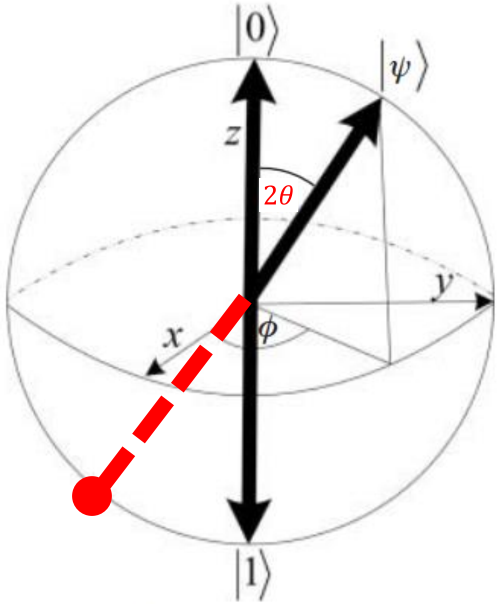


Figure 5.6. Bloch sphere.

Supplementary material

- Geometric representation of 1-qubit state
  - New Bloch sphere

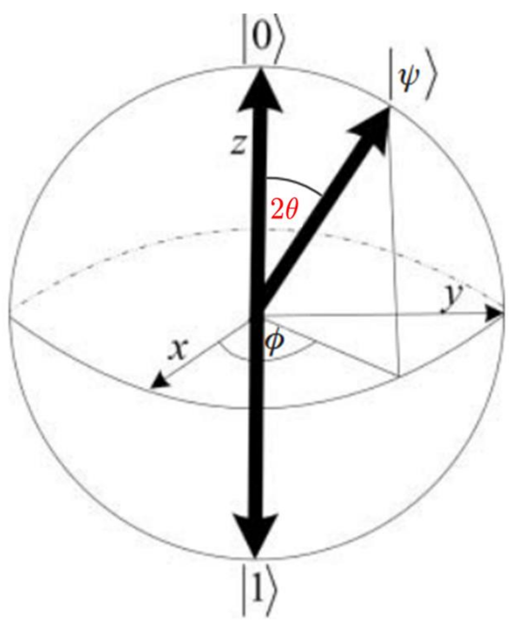


Figure 5.6. Bloch sphere.

$$|\psi\rangle = \cos(\theta)|0\rangle + e^{i\phi}\sin(\theta)|1\rangle$$

⇕

$$x = \cos\phi \sin 2\theta,$$

$$y = \sin 2\theta \sin\phi,$$

$$z = \cos 2\theta.$$

where $0 \leqslant \theta \leqslant \frac{\pi}{2}$ and $0 \leqslant \phi < 2\pi$

（感谢弘毅学堂2019级周伟贤同学纠正关于标量乘法不改变量子态的陈述）

Supplementary material

- Geometric representation of 1-qubit state
  - New Bloch sphere (cont.)

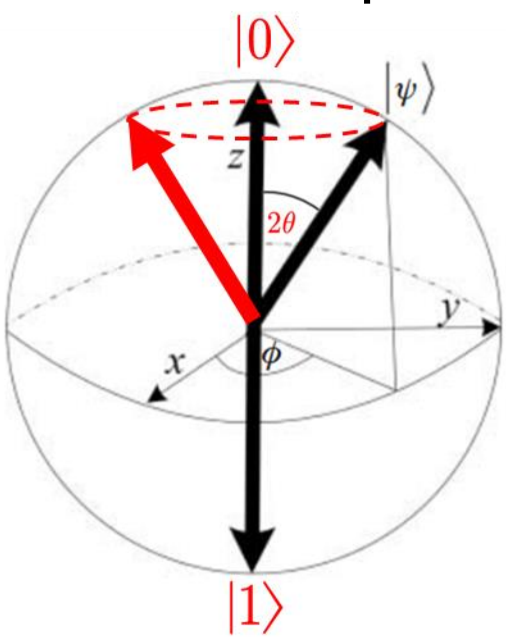


Figure 5.6. Bloch sphere.

- Bit locates in the north or south pole
- Measurement probability depends on the latitude 2θ
- Qubit on the equator has a 50-50 chance of collapsing to either $|0\rangle$ or $|1\rangle$
- Phase (longitude) shift does not affect the collapsing probability

（感谢弘毅学堂2020级杜忠璠同学纠正关于latitude单词拼写错误）

Supplementary material

- Geometric representation of operator
  - Dynamics
    - every unitary 2-by-2 matrix (i.e., a one-qubit operation) can be visualized as a way of manipulating the sphere

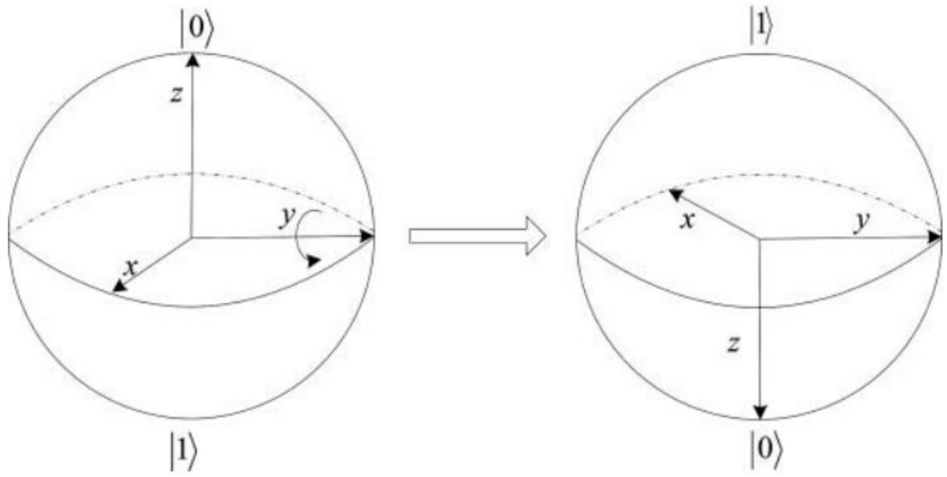
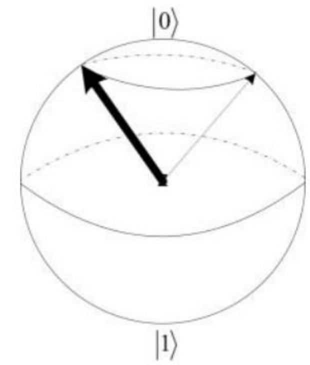


Figure 5.7. A rotation of the Bloch sphere at y.

4. Quantum Gates



- Phase shift gate

$$R(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{\theta} \end{bmatrix}. \quad \Rightarrow \quad R(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} \tag{5.95}$$

This gate performs the following operation on an arbitrary qubit:

$$\cos(\theta')|0\rangle + e^{i\phi}\sin(\theta')|1\rangle = \begin{bmatrix} \cos(\theta') \\ e^{i\phi}\sin(\theta') \end{bmatrix} \mapsto \begin{bmatrix} \cos(\theta') \\ e^{i\theta}e^{i\phi}\sin(\theta') \end{bmatrix}. \tag{5.96}$$

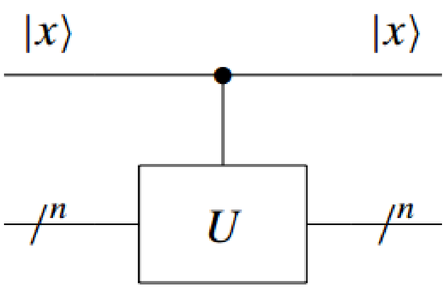
This corresponds to a rotation that leaves the latitude alone and just changes the longitude. The new state of the qubit will remain unchanged. Only the phase will change.

（感谢弘毅学堂 2018级韩森同学指正此页相移门矩阵表示的错误）

4. Quantum Gates

- Controlled-U gate or ^{C}U gate
  - IF-THEN statement

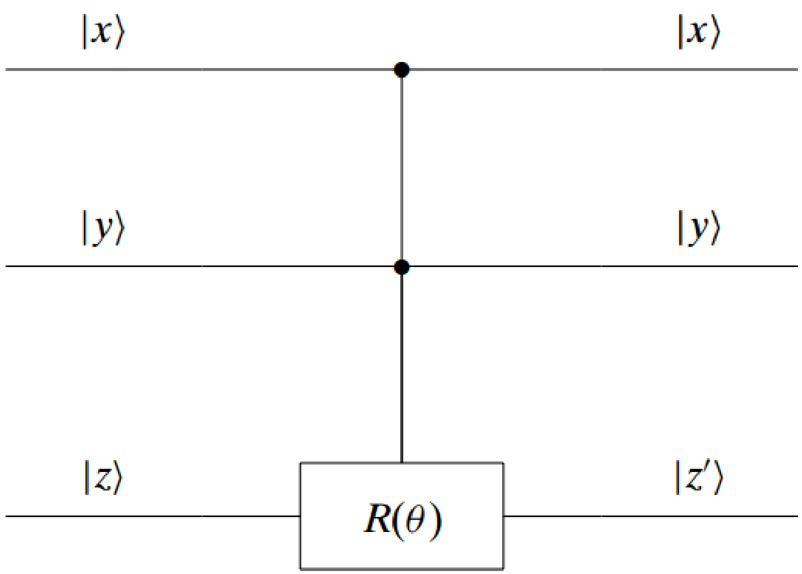
$$|0,\ y\rangle \mapsto |0,\ y\rangle \text{ and } |1,\ y\rangle \mapsto |1,\ Uy\rangle$$



$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Rightarrow {}^{C}U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{bmatrix}$$

4. Quantum Gates

- Deutsch gate $D(\theta)$
  - $|x, y, z\rangle = \begin{cases} |1, 1, R(\theta)z\rangle, \text{ if } |x\rangle = |y\rangle = |1\rangle \\ |x, y, z\rangle, \text{ otherwise} \end{cases}$



4. Quantum Gates

- Universal gates
  - Universal logic gates
    - {AND, NOT}
    - NAND
    - Toffoli
    - Fredkin
  - Universal quantum gates
    - $\left\{H, {}^{C}\mathrm{NOT}, R\left(\cos^{-1}\left(\frac{3}{5}\right)\right)\right\}$
    - $D(\theta)$

4. Quantum Gates

- Properties of quantum gates
  - Every operation must be reversible
  - No-cloning Theorem*
    - We can "cut" and "paste" a quantum state
    - We cannot "copy" and "paste" a quantum state

(* See the following supplementary material)

Supplementary material

- No-Cloning Theorem
  - Assume there is a potential cloning operation C
    - It would be a linear map (indeed unitary!)

$$C\colon \mathbb{V} \otimes \mathbb{V} \longrightarrow \mathbb{V} \otimes \mathbb{V}$$

    - To clone $|x\rangle$

$$C(|x\rangle \otimes |0\rangle) = |x\rangle \otimes |x\rangle$$

      - When $|x\rangle$ are basic states

$$C(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle \quad \text{and} \quad C(|1\rangle \otimes |0\rangle) = |1\rangle \otimes |1\rangle$$

Supplementary material

- When $|x\rangle$ are superposition state $c_0|0\rangle + c_1|1\rangle$

$$
\begin{aligned}
& C((c_0|0\rangle + c_1|1\rangle) \otimes |0\rangle) \\
= & C(c_0(|0\rangle \otimes |0\rangle) + c_1(|1\rangle \otimes |0\rangle)) \quad \text{\% Tensor product distributes over addition} \\
= & c_0 C(|0\rangle \otimes |0\rangle) + c_1 C(|1\rangle \otimes |0\rangle) \quad \text{\% } C \text{ is a linear operation} \\
= & c_0(|0\rangle \otimes |0\rangle) + c_1(|1\rangle \otimes |1\rangle) \quad \text{\% clone when } |x\rangle \text{ is basic state} \\
\neq & (c_0|0\rangle + c_1|1\rangle) \otimes (c_0|0\rangle + c_1|1\rangle) \quad \text{\% definition of clone operation}
\end{aligned}
$$

When C is a linear operation, clone is not permitted

Supplementary material

- No-Cloning Theorem
  - Consider a transporting operation T
    - It would be a linear map too

$$T\colon \mathbb{V}\otimes\mathbb{V} \longrightarrow \mathbb{V}\otimes\mathbb{V}$$

    - To transport $|x\rangle$

$$T(|x\rangle \otimes |0\rangle) = |0\rangle \otimes |x\rangle$$

      - When $|x\rangle$ are basic states

$$T(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle \quad \text{and} \quad T(|1\rangle \otimes |0\rangle) = |0\rangle \otimes |1\rangle$$

Supplementary material

- When $|x\rangle$ are superposition state $c_0|0\rangle + c_1|1\rangle$

$$
\begin{aligned}
& T\left((c_0|0\rangle + c_1|1\rangle) \otimes |0\rangle\right) \\
= & T\left(c_0(|0\rangle \otimes |0\rangle) + c_1(|1\rangle \otimes |0\rangle)\right) && \text{\% Tensor product distributes over addition} \\
= & c_0 T(|0\rangle \otimes |0\rangle) + c_1 T(|1\rangle \otimes |0\rangle) && \text{\% } T \text{ is a linear operation} \\
= & c_0(|0\rangle \otimes |0\rangle) + c_1(|0\rangle \otimes |1\rangle) && \text{\% clone when } |x\rangle \text{ is basic state} \\
= & |0\rangle \otimes (c_0|0\rangle + c_1|1\rangle) && \text{\% definition of transport operation}
\end{aligned}
$$

When T is a linear operation, transport is permitted

Conclusion

1. Bits and Qubits
   - Definitions and their relation
2. Classical Gates
   - NOT, AND, OR, and NAND gates
   - 功能完备与通用门
   - Sequential and Parallel Operations
3. Reversible Gates
   - Controlled-NOT, Toffoli, and Fredkin gates
4. Quantum Gates
   - Definition
   - Geometric representation
   - Phase shift, Controlled-U, and Deutsch gates
   - No-Clone Theorem

预告

- 下次上课讲量子算法，入门可能有点难，大家提前看两个资料：
  - Quantum Computing for Computer Scientists，Microsoft Research，2016
    https://www.bilibili.com/video/BV14W411o7G6?from=search&seid=2931728500800941075
  - 量子计算通识，zhyuzh3d，简书, 2019
    https://www.jianshu.com/p/2a23f15e4efb