量子信息与量子通信

Quantum information and quantum communication

李小飞 光电科学与工程学院 2022 年 4 月 2 日







1. 逻辑门的可逆性

2. 单量子比特逻辑门

3. 多量子比特逻辑门





所有类型的计算都是加法,二进制加法是逻辑运算,逻辑门是实现各种逻辑运算的基础性元件。

● 例-1. 设计一个加法器,实现两整数之间的求和:

解: 对于小于 2^n 的正整数 M, N 可表示为:

$$M = \sum_{i=0}^{n-1} a_i 2^i, \qquad N = \sum_{i=0}^{n-1} b_i 2^i$$

Table 1: 加法器真值表, 其中 s_i, c_{i+1} 分别是求和位和进位

a_i	b_{i}	s_i	c_{i+1}
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

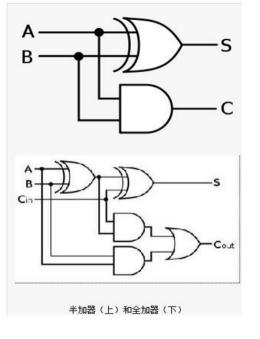
- a_i, b_i 不同时, s_i 置"1", 否则置"0": 逻辑"异或"XOR
- ullet a_i , b_i 都是 1 时, c_{i+1} 置"1",否则置"0": 逻辑"与"AND

$$s_i = a_i \oplus b_i$$

$$s_i = a_i \oplus b_i$$

$$c_{i+1} = a_i \wedge b_i$$





方氣方之

□可逆性

考察发现: 经典 XOR 门和 AND 门都是不可逆的! 不可逆过程有深刻的物理内含:

- ullet 不可逆过程熵增加 $S=k_B \ln \Omega$
- 不可逆过程信息丢失 $\Delta S = k_B \ln 2$
- 不可逆过程消耗能量
- 不可逆过程不是幺正变换

当前通用的图灵机都是不可逆的!

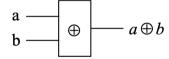
量子计算机通过酉操作(幺正变换)来实现信息处理,要求所有的逻辑门都是可逆的!

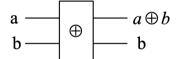
✓ Bennett 证明

所有不可逆的计算机都可以改造为可逆计算机

● 例-2. 试把不可逆的异或门,改造为可逆的异或门:

解: 改造方法如图

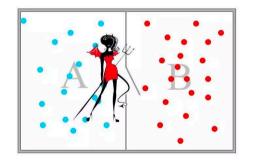




可逆源于所有信息被保留, 信息的擦除消耗能量增加熵, 导致不可逆。

■ 麦克斯韦妖佯谬-1871

绝热容器分成两格,中间是由"妖"控制的一扇"门",分子作无规则热运动时会向门上撞击,"门"可以选择性的将速度较快的分子放入一格,较慢的分子放入另一格,这样,体系的熵在减少!



1981年,Bennett 证明"妖"必须去除前面分子的信息,这消耗能量并导致 $k_{\rm P}\ln 2$ 的熵增。

6/33

基本结论:

- 微观过程是可逆的
- 微观过程服从量子力学原理
- 演化过程是幺正的
- 基于幺正变设计的量子逻辑门是可逆的
- 如果有一套普适的量子逻辑门,发展量子计算机是可行的

大氣大為



1. 逻辑门的可逆性

2. 单量子比特逻辑门

3. 多量子比特逻辑门



□ 单量子比特逻辑门

● 分析: 单量子比特波函数

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$
, $(|\alpha|^2 + |\beta|^2 = 1)$

矩阵:

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

因此,

- (1) 单比特逻辑门是操作 C^2 空间的 2×2 的矩阵,
- (2) 单比特逻辑门必须是幺正 (酉) 矩阵 (可逆性要求)



☑量子非门 (X-Gate) -比特反转门

经典非门: $0 \rightarrow 1$, $1 \rightarrow 0$

量子非门: $\alpha |0\rangle + \beta |1\rangle \rightarrow \alpha |1\rangle + \beta |0\rangle$

● 例-2. 试证明 σ₂ 矩阵就是单比特量子非门:

$$X \equiv \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$$

证明: (1) 量子非, 对于 $|\psi\rangle=\alpha\,|0\rangle+\beta\,|1\rangle$, 有

$$X | \psi \rangle = X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} = \beta | 0 \rangle + \alpha | 1 \rangle = \alpha | 1 \rangle + \beta | 0 \rangle$$

(2) 幺正性

$$X^{\dagger} = (X_{ij}^*)^T = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$
$$X^{\dagger}X = XX^{\dagger} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = I$$

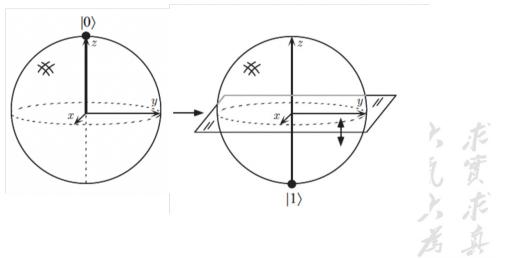
证毕!

• 很明显, 这是比特反转

$$X \left| 0 \right\rangle = \left| 1 \right\rangle, \qquad X \left| 1 \right\rangle = \left| 0 \right\rangle$$



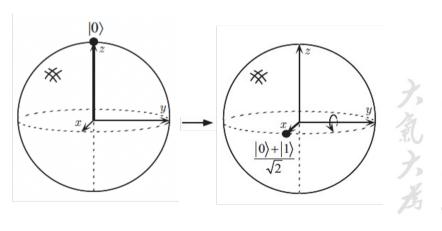
比特反转的物理图像



11/33

∠ 基矢变换门 (H-Gate)

基矢变换: $|0\rangle \to |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |1\rangle \to |-\rangle =$ 物理图像: 把 Z 方向的基矢变换成 X 方向的基矢



● 例-4. 试证明如下矩阵就是基矢变换门:

$$H \equiv \frac{1}{\sqrt{2}}(X+Z) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1\\ 1 & -1 \end{bmatrix}$$

证明: (1) 基矢变换

证明: (1) 基务变换
$$H |0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle$$

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

(2) 幺正性

$$H^{\dagger}H = HH^{\dagger} = I$$

证毕!

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

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

统一表示为: (x,z 分别取 ○ 或 1)

$$H|x\rangle = \frac{\sum_{z} (-1)^{xz} |z\rangle}{\sqrt{2}}$$



● 很明显 H 是自共轭矩阵, 有:

$$H^{\dagger} = H \rightarrow H^2 = I$$

● 例-5. 试证明 H 可以完成反向变换:

$$H\left|+\right\rangle = \left|0\right\rangle, \qquad H\left|-\right\rangle = \left|1\right\rangle$$

证明:

$$H |0\rangle = |+\rangle$$
, $H |0\rangle = |-\rangle$
 $HH |0\rangle = H |+\rangle$, $HH |0\rangle = H |-\rangle$
 $|0\rangle = H |+\rangle$, $|0\rangle = H |-\rangle$

证毕!



■相位反转门 (Z-Gate)

相位反转: $\alpha |0\rangle + \beta |1\rangle \rightarrow \alpha |0\rangle - \beta |1\rangle$

● 例-3. 试证明 σ₂矩阵就是相位反转门:

$$Z \equiv \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = -i \, |0\rangle\langle 1| + i \, |1\rangle\langle 0|$$

证明: (1) 相位反转

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

(2) 幺正性

$$Z^{\dagger}Z = ZZ^{\dagger} = I$$

证毕! • 很明显 $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle = e^{i\pi}|1\rangle$



/ 旋转门

既然态矢都在 Block 球面,相位反转 (Z-Gate) 就是绕 Z 轴旋转 180 度 (π) (为什么?)

• 绕 Z 轴旋转 90 度 $(\frac{\pi}{2})$ 的门是 S-Gate.

$$Z |1\rangle = e^{i\pi} |1\rangle$$

 $S |1\rangle = e^{i\pi/2} |1\rangle$

解得:

$$S \equiv \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{2}} \end{bmatrix}$$

由于 $i = \sqrt{-1}$, 也称 S-Gate 为 \sqrt{Z} -Gate



绕 Z 轴旋转 45 度的门为 T-Gate, 也称 π/8-Gate

$$T \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix} = e^{\frac{i\pi}{8}} \begin{bmatrix} e^{\frac{-i\pi}{8}} & 0 \\ 0 & e^{\frac{i\pi}{8}} \end{bmatrix}$$

• 绕 Z 轴旋转任意角度 (φ) 的门为旋转门 $R_z(\varphi)$ -Gate

$$R_z(\varphi) \equiv \begin{bmatrix} e^{-i\varphi/2} & 0 \\ 0 & e^{i\varphi/2} \end{bmatrix}$$



● 不失一般性, 存在各方向的旋转门

$$\begin{split} R_z(\theta) &\equiv e^{-i\theta Z/2} \\ R_y(\theta) &\equiv e^{-i\theta Y/2} \\ R_x(\theta) &\equiv e^{-i\theta X/2} \\ R_{\hat{n}}(\theta) &\equiv e^{-i\theta \hat{n}\cdot \sigma/2} \end{split}$$

小结: 常用单比特量子门

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

Pauli- X $-X$ $-\frac{1}{\sqrt{2}}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Pauli- Y $-\frac{1}{\sqrt{2}}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Pauli- Z $-\frac{1}{\sqrt{2}}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

Phase $-\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Phase $-\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
 $\pi/8$ $-\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$

方気が



1. 逻辑门的可逆性

2. 单量子比特逻辑门

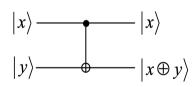
3. 多量子比特逻辑门



☑ 多量子比特逻辑门

1. 控制非门 (Controlled-Not-Gate)

$$C - NOT \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



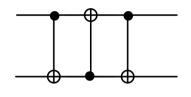


输入	输出
$ x\rangle y\rangle$	$ x\rangle x\oplus y\rangle$
$ 00\rangle$	$ 00\rangle$
$ 01\rangle$	$ 01\rangle$
$ 10\rangle$	$ 11\rangle$
$ 11\rangle$	$ 10\rangle$

控制位 (x) 置位时,对目标位 (y) 做非操作

六氯六萬

2. 交换门 (Switch-Gate)



输入
$$|a,b\rangle$$
 \rightarrow 输出 $|b,a\rangle$

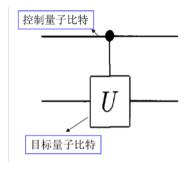
证明:

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

证毕!



3. 控制 U 门 $(U_0:I,U_1:X,U_2:Y,U_3:Z,\cdots)$



功能: U 是单量子比特的任意酉算子。如果控制位置位,则 U 作用到目标位上,否则目标位不变。

$$|c\rangle |t\rangle \rightarrow |c\rangle U^c |t\rangle$$

显然, 当 U=X 时, 就是控制非门 (CNOT)

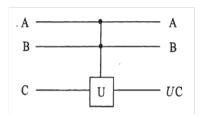
 \bullet 通过设计一系列的控制 U 门,我们可以控制系统的初态向目标态的演化!

依据: 量子力学的演化假设, 薛定谔方程与酉变换等价, 有:

$$ig| ar{m{x}} ar{m{x}} ig
angle = \prod_i U_i ig| m{n}$$
 态 $ig
angle$

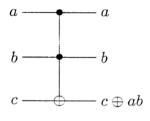
六氯六五

4. 双控制位的控制 U 门 $(C^2(U))$



功能:只有当两个控制位都置位时,U才作用到目标位上,否则目标位不变。显然,当U=X时,就是控制非门 (CNOT)

例. 下面的 Toffoli 门, 就是双控制位的控制非 (X) 门



Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

六氣六為

27/33

□ 深刻意义

Toffoli 门是可逆门,是实现普适计算的基础。可以证 明: 经典条件下一位两位可逆门不足以实现 Toffoli 门。而量子条件下由 H, CNOT, S和T门可以任意 精度地近似任意酉操作。也就是说,只有在量子条 件下,才可以实现普适的可逆计算!

构建普适门

任意的酉算子 可以用仅非平凡的作用在 由两个计算基态张成的 子空间的酉算子的乘积 精确描述

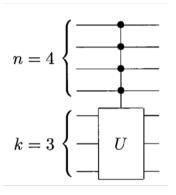
> 任意酉矩阵可以用 单量子位门和CNOT门精确描述

单量子位操作 可以用Hadamard,相位门和 π/8门近似到任意精度。 设光子偏振态与计算基矢态有如下关系:

试设计普适计算所必须的 H, CNOT, S和T门

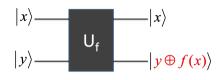


5. 多控制位多目标位的控制 U 门 $(C^n(U_k))$



功能:只有当所有控制位都置位时, U 才作用到目标位上, 否则目标位不变。

6. 经典函数的量子门阵列实现

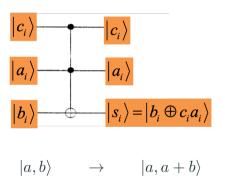


- ullet 任意经典函数都可以转化成二进位形式下的一系列逻辑运算,这些逻辑运算由量子门阵列 U_f 实现
- 输入位 $|x\rangle$, 经 U_f 运算后,得到函数值 f(x)
- f(x) 要么是 0 要么是 1,只有当 f(x)=1 时,才对目标位 (y) 做非操作,否则目标位不变。

$$U_f \left| x,y \right\rangle \qquad \rightarrow \qquad \left| x,y \oplus f(x) \right\rangle$$



这是一个量子加法器



试给出真值表

六氯六



Thanks for your attention!

A & Q

方氯方名