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 2 月 22 日

第 3 讲： 量子信息处理-逻辑门

Contents

信息学基本原理

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：

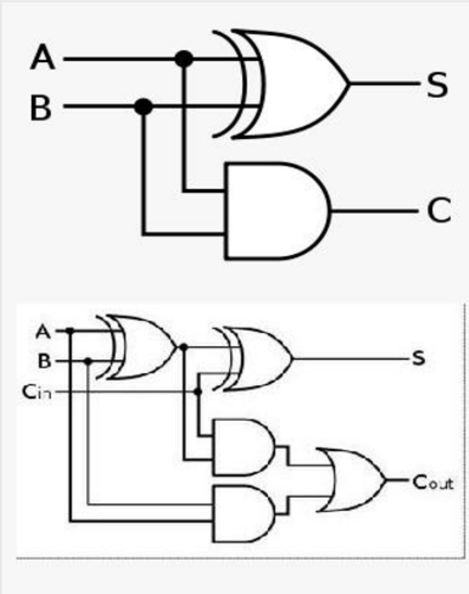
解: 对于小于 2^n 的正整数 M, N 可表示为：

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

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 $s_i = a_i \oplus b_i$
- a_i, b_i 都是 1 时，c_{i+1} 置“1”，否则置“0”: 逻辑“与”AND $c_{i+1} = a_i \wedge b_i$



半加器（上）和全加器（下）

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：

- 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！

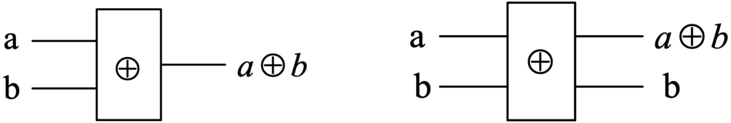
- 量子计算机通过酉操作（幺正变换）来实现信息处理，要求所有的逻辑门都是可逆的！

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：

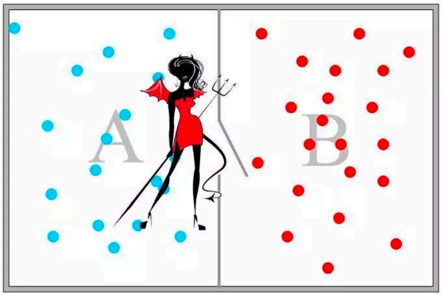
解: 改造方法如图



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 $k_B \ln 2$ 的熵增。

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

Contents

单量子比特波函数:

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

矩阵:

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

因此，单比特逻辑门是操作 C^2 空间的 2×2 的矩阵，
由于可逆性的要求，单比特逻辑门也必须是幺正（酉）矩阵。

1. 量子非门 (X-Gate)

经典非门：$0 \to 1, \qquad 1 \to 0$

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

例-2. 试证明 σ_x 矩阵就是单比特量子非门：

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

证明： (1) 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

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

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

证毕!

- 很明显，这是比特反转

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

基矢变换: $|0\rangle \to |+\rangle, \qquad |1\rangle \to |-\rangle$

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)

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

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

(2) 幺正性

$$H^\dagger H = H H^\dagger = I$$

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 0 或 1)

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

- 可以证明 H 也是自共轭矩阵，有：

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

例-5. 试证明 H 可以完成反向变换：

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

证明:

$$\begin{aligned} H|0\rangle &= |+\rangle, & H|0\rangle &= |-\rangle \\ HH|0\rangle &= H|+\rangle, & HH|0\rangle &= H|-\rangle \\ |0\rangle &= H|+\rangle, & |0\rangle &= H|-\rangle \end{aligned}$$

证毕！

3. 相位反转门 (Z-Gate)

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

例-3. 试证明 σ_z 矩阵就是相位反转门:

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

证明: (1)

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

(2) 幺正性

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

证毕!

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

4. 各种相位门

既然态矢都在 Block 球面，那相位反转 (Z-Gate) 就是绕 Z 轴旋转 180 度 (π)，当然有绕 Z 轴旋转 90 度 ($\frac{\pi}{2}$) 的门，这就是 S-Gate.

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

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

由此得:

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

所以 S-Gate=$\sqrt{Z}$-Gate

当然，也有绕 Z 轴旋转 45 度的门，称为 T-Gate，也称 $\pi/8$-Gate

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

绕 Z 轴旋转任意角度 (ϕ) 的门，则称为旋转门 R_ϕ-Gate

$$R_\phi \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$$

- 很明显 $R_\phi|0\rangle = |0\rangle, \quad R_\phi|1\rangle = e^{i\phi}|1\rangle$

Contents

Contents

求實求真
大氣大為

Contents

基于以上 4 个假定，可以从数学上在 Hilbert 空间导出整个量子力学体系，那么基于假定导出的量子力学可靠吗？

学术讨论

Thanks for your attention!

A & Q

求實求真
大氣大為