量子信息与量子计算

WANG LH

2025-10-28

目录

Chapter 1

基本概念

1.1 量子比特

量子比特 (quantum bit, qubit)是量子计算的基本单元。在经典计算中, 比特是最小的信息单元, 只能取 0 或 1 两个值。而量子比特则可以处于叠加态, 即同时处于 0 和 1 两个状态。这种叠加态的性质使得量子计算机能够在某些情况下比经典计算机更快地完成一些任务。

对于用作量子比特的双态量子系统, 常将状态 $|0\rangle$ 等同于矢量 $(1,0)^\intercal$, 状态 $|1\rangle$ 等同于矢量 $(0,1)^\intercal$。

比特和量子比特的区别在于, 量子比特的状态可以落在 $|0\rangle$ 和 $|1\rangle$ 之外, 即量子比特可以是状态的线性组合, 常称为叠加态, 如

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.1.1}$$

其中 α 和 β 是复数, 尽管许多时候把它们当作实数也不会有太大问题。换句话说, 量子比特的状态是二维复矢量空间中的矢量。特殊的 $|0\rangle$ 和 $|1\rangle$ 状态称为**计算基态 (computational basis state)**, 是构成这个矢量空间的一组正交基。

量子比特的一个有用的图像是如下的几何表示, 因为 $|\alpha|^2 + |\beta|^2 = 1$,式 (1.1.1) 可改写为

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle, \tag{1.1.2}$$

其中 θ 和 ϕ 是实数。这种表示称为 **Bloch 球面 (Bloch sphere)**[1], 是一个单位球面, 量子比特的状态对应于球面上的一个点, 如图 1.1 所示。

[1] 布洛赫, Felix Bloch, 1905.10.23—1983.09.10, 瑞士物理学家。

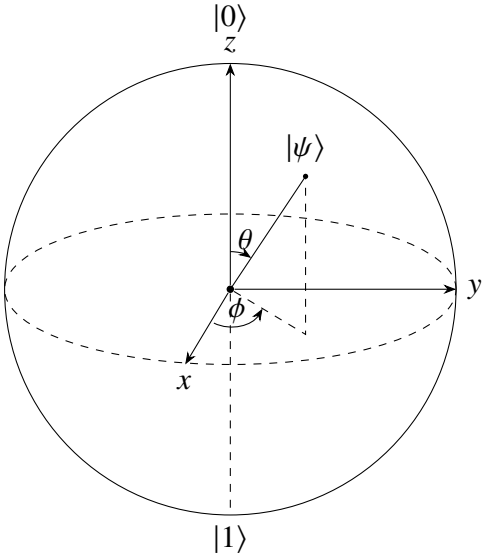


图 1.1: 量子比特的 Bloch 球面表示

1.1.1 多量子比特

假设有两个量子比特, 有四个基态 $|00\rangle$、$|01\rangle$、$|10\rangle$ 和 $|11\rangle$。状态为

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle, \tag{1.1.3}$$

其中

$$\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1. \tag{1.1.4}$$

单独测量第一个量子比特, 得 0 的概率为 $|\alpha_{00}|^2 + |\alpha_{01}|^2$, 测量后的状态为

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}. \tag{1.1.5}$$

1.2 量子计算

1.2.1 单量子比特门

在量子计算中, 各种形式的幺正矩阵被称作**量子门 (quantum gate)**。量子门是作用于量子比特的基本电路单元, 每个量子门对应于一个线性映射, 相应地对应于计算基底下的一个幺正矩阵。因此, 量子门作用于量子比特对应于一个幺正矩阵乘以量子比特态矢。

所有的量子门都是可逆的。所有的单量子比特门都对应着 Bloch 球面上的绕不同轴旋转任意角度的旋转操作。

1.2.2 Pauli 矩阵

Pauli 矩阵 (Pauli matrices)是一组重要的矩阵, 定义为

$$\sigma_0 \coloneqq I \coloneqq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 \coloneqq \sigma_x \coloneqq X \coloneqq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{1.2.1}$$

$$\sigma_2 \coloneqq \sigma_y \coloneqq Y \coloneqq \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \quad \sigma_3 \coloneqq \sigma_z \coloneqq Z \coloneqq \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.2.2}$$

它们都是幺正矩阵和厄米矩阵。后三个矩阵称为 Pauli-X 门、Pauli-Y 门和 Pauli-Z 门。

性质 1.1

$$\sigma_0^2 = \sigma_1^2 = \sigma_2^2 = \sigma_3^2 = I, \tag{1.2.3}$$

$$\sigma_1\sigma_2 = \mathrm{i}\sigma_3, \quad \sigma_2\sigma_3 = \mathrm{i}\sigma_1, \quad \sigma_3\sigma_1 = \mathrm{i}\sigma_2, \tag{1.2.4}$$

或

$$\sigma_i\sigma_j = \delta_{ij}I + \mathrm{i}\varepsilon_{ijk}\sigma_k. \tag{1.2.5}$$

性质 1.2 反对易关系

$$\left[\sigma_i, \sigma_j\right]_+ = 2\delta_{ij}I. \tag{1.2.6}$$

Pauli-X 门也称为**量子非门 (quantum NOT gate)**, 是量子计算中的基本门之一, 它将 $|0\rangle$ 状态变为 $|1\rangle$ 状态, 将 $|1\rangle$ 状态变为 $|0\rangle$ 状态, 即

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \tag{1.2.7}$$

或

$$X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle. \tag{1.2.8}$$

Pauli-X 门能交换观测到 $|0\rangle$ 和 $|1\rangle$ 的概率, 会让球面上的点绕 x 轴旋转 180 度。对于量子态 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = (\alpha, \beta)^\intercal$, Pauli-X 门的作用是

$$X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta|0\rangle + \alpha|1\rangle. \tag{1.2.9}$$

Pauli-Y 门的作用是绕 y 轴旋转 180 度, 即

$$\begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \mathrm{i} \end{pmatrix}, \quad \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\mathrm{i} \\ 0 \end{pmatrix}, \tag{1.2.10}$$

或

$$Y|0\rangle = \mathrm{i}|1\rangle, \quad Y|1\rangle = -\mathrm{i}|0\rangle. \tag{1.2.11}$$

对于量子态 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = (\alpha, \beta)^\intercal$, Pauli-Y 门的作用是

$$Y|\psi\rangle = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} -\mathrm{i}\beta \\ \mathrm{i}\alpha \end{pmatrix} = -\mathrm{i}\beta|0\rangle + \mathrm{i}\alpha|1\rangle . \tag{1.2.12}$$

Pauli-Z 门的作用是绕 z 轴旋转 180 度, 即

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix}, \tag{1.2.13}$$

或

$$Z|0\rangle = |0\rangle , \quad Z|1\rangle = -|1\rangle . \tag{1.2.14}$$

对于量子态 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = (\alpha, \beta)^\intercal$, Pauli-Z 门的作用是

$$Z|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix} = \alpha|0\rangle - \beta|1\rangle . \tag{1.2.15}$$

1.2.3 Hadamard 门

Hadamard 门 (Hadamard gate)[2]是量子计算中的一个重要门, 简称 H 门, 作用是

$$H|0\rangle \coloneqq \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad H|1\rangle \coloneqq \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{1.2.16}$$

其中

$$H \coloneqq \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{1.2.17}$$

它将两个基矢量变换成了两个等概率叠加态。对于量子态 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = (\alpha, \beta)^\intercal$, H 门的作用是

$$H|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix} = \frac{\alpha + \beta}{\sqrt{2}}|0\rangle + \frac{\alpha - \beta}{\sqrt{2}}|1\rangle . \tag{1.2.18}$$

H 门在量子线路中的作用就是用于创建叠加态, 它通常用在量子线路的最前端。从 Bloch 球面上来看, H 门的效果是使得 Bloch 球面上的点先绕 y 轴旋转 90 度, 然后绕 x 轴旋转 180 度, 也即绕 z 轴与 x 轴之间的倾斜 45 度的轴旋转 180 度。

1.2.4 多量子比特门：CNOT 门

受控非门 (controlled-NOT gate)是量子计算中的一个重要门, 也称 CNOT 门或 CX 门, 作用是

$$|00\rangle \mapsto |00\rangle , \quad |01\rangle \mapsto |01\rangle , \quad |10\rangle \mapsto |11\rangle , \quad |11\rangle \mapsto |10\rangle , \tag{1.2.19}$$

[2]阿达玛, Jacques Salomon Hadamard, 1865.12.08—1963.10.17, 法国数学家。

即双量子比特的第一个量子比特是控制位, 第二个量子比特是目标位, 当控制位为 1 时, 目标位取反。CNOT 门的矩阵表示为

$$U_{\mathrm{CN}} \coloneqq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{1.2.20}$$

可以把 CNOT 门看作是经典异或门的量子版本, 作用可总结为 $|a,b\rangle \mapsto |a,a\oplus b\rangle$, 其中 $\oplus$ 表示异或运算 (模 2 加法)。CNOT 门的电路图如图 1.2 所示。

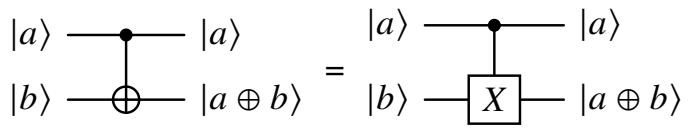


图 1.2: CNOT 门

1.2.5 其他基态的选择

对于量子比特, 态 $|0\rangle$ 和 $|1\rangle$ 是计算基态, 但并不是唯一的基态。在量子计算中, 可以选择任意一组正交归一的基作为计算基态。例如, 对于单量子比特, 可以选择 Hadamard 门的作用下的基态作为计算基态, 即

$$|+\rangle \coloneqq H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle \coloneqq H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{1.2.21}$$

任意态可以写成

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle. \tag{1.2.22}$$

1.2.6 量子线路

量子线路是描述量子计算的一种图形化表示方法。量子线路由量子比特和量子门组成, 量子比特用线表示, 量子门用方框表示。量子线路从左到右表示时间的流动, 即从左到右的量子门作用于从左到右的量子比特。量子线路的输入是初始量子态, 输出是最终量子态。

对换门 (swap gate)是一种重要的多量子比特门, 作用是交换两个量子比特的状态, 如图 1.3 所示。

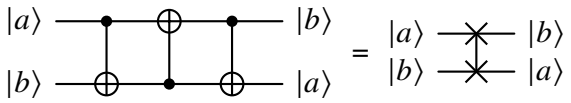


图 1.3: 对换门

可以由

$$\begin{aligned} |a,b\rangle &\mapsto |a,a\oplus b\rangle \\ &\mapsto |a\oplus(a\oplus b),a\oplus b\rangle = |b,a\oplus b\rangle \\ &\mapsto |b,(a\oplus b)\oplus b\rangle = |b,a\rangle, \end{aligned} \tag{1.2.23}$$

简单验证对换门的作用是交换两个量子比特的状态。对换门的矩阵表示为

$$U_{\text{swap}} \coloneqq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{1.2.24}$$

引入**受控 U 门 (controlled-U gate)**, 其中 U 门是任意的单量子比特门, 电路图如图 1.4 所示。当 $U = X$ 时, 受控 X 门就是 CNOT 门。

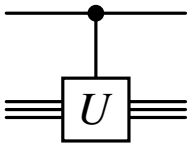


图 1.4: 受控 U 门

测量也是量子线路中的一种操作, 如图 1.5 所示, 将单量子比特态转化为一个经典比特 M, 双线代表经典电子线路, 单线代表量子比特线路。

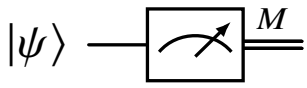


图 1.5: 表示测量的量子线路符号

1.2.7 量子比特复制电路

使用 CNOT 门可以实现量子比特 $|0\rangle$ 和 $|1\rangle$ 的复制, 如图 1.6 所示, 将待复制的 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, 与初始化的 $|0\rangle$ 量子比特进行 CNOT 门操作, 记为

$$[\alpha|0\rangle + \beta|1\rangle]|0\rangle = \alpha|00\rangle + \beta|11\rangle. \tag{1.2.25}$$

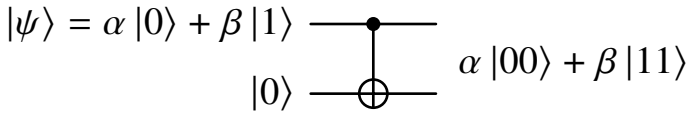


图 1.6: 量子比特复制电路

对于除 $|0\rangle$ 和 $|1\rangle$ 之外的态, 有

$$|\psi\rangle|\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle, \tag{1.2.26}$$

这说明, 除 $|0\rangle$ 和 $|1\rangle$ 之外的态不可能通过量子线路复制。这是由于量子态的线性叠加性质, 使得复制一个未知量子态会破坏原有的态。这个结论被称为**不可克隆定理 (no-cloning theorem)**。

1.2.8 Bell 态

Bell 态 (Bell state)是一种特殊的量子态, 是两个量子比特的纠缠态, 也称为 **EPR 对 (EPR pair)**。E, P 和 R 分别是 Einstein、Podolsky 和 Rosen 的姓氏首字母。Bell 态的电路图如图 1.7 所示。

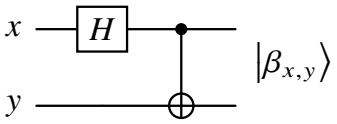


图 1.7: 制备 Bell 态的量子线路

Bell 态有四种, 分别为

$$|\beta_{00}\rangle = \left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \tag{1.2.27}$$

$$|\beta_{10}\rangle = |\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right), \tag{1.2.28}$$

$$|\beta_{01}\rangle = \left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right), \tag{1.2.29}$$

$$|\beta_{11}\rangle = |\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right). \tag{1.2.30}$$

或

$$\left|\beta_{x,y}\right\rangle := \frac{1}{\sqrt{2}}\left(|0, y\rangle + (-1)^x |1, \overline{y}\rangle\right), \tag{1.2.31}$$

其中 $x, y \in \{0, 1\}$, $\overline{y} = 1 - y$ 是 y 的取反。Bell 态是一种纠缠态, 其中两个量子比特之间的关系是不可分割的, 即对一个量子比特的测量会立即影响另一个量子比特的状态。

1.2.9 量子隐形传态

量子隐形传态 (quantum teleportation)是一种量子通信协议, 可以实现量子比特的传输, 但并不是传统意义上的传输, 而是通过量子态的交换实现的, 双方没有量子通信信道连接都能实现量子比特的传输。

Alice 和 Bob 各持有 EPR 对的一个量子比特。现在, Alice 想要传输一个量子比特 $|\psi\rangle$ 给 Bob。首先, Alice 令 $|\psi\rangle$ 与她持有的一个量子比特相互作用, 然后对她手上的这两个比特进行测量, 得 4 种经典结果 00、01、10 和 11 之一。Bob 根据 Alice 的测量结果对他现在手上的量子比特进行操作, 恢复成 $|\psi\rangle$。该量子隐形传态的电路图如图 1.8 所示。

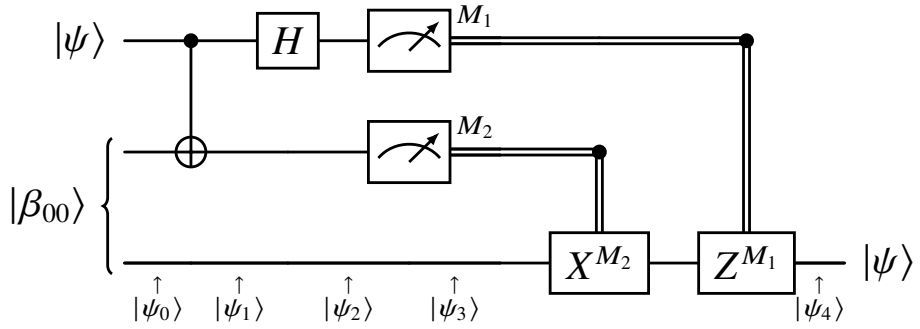


图 1.8: 隐形传态电路。前两个比特是 Alice 的, 第三个比特是 Bob 的

将要进行隐形传态的态是 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$。线路的输入态为

$$\begin{aligned}|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle &= \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)], \end{aligned} \tag{1.2.32}$$

经过 CNOT 门, 得

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)], \tag{1.2.33}$$

再经过 H 门, 得

$$\begin{aligned}|\psi_2\rangle &= \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)] \\ &= \frac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)]. \end{aligned} \tag{1.2.34}$$

上式分为四项, 可以在给定 Alice 测量结果的情况下, 读出 Bob 的量子态, 即

$$00 \mapsto |\psi_3(00)\rangle \coloneqq [\alpha|0\rangle + \beta|1\rangle], \tag{1.2.35}$$
$$01 \mapsto |\psi_3(01)\rangle \coloneqq [\alpha|1\rangle + \beta|0\rangle], \tag{1.2.36}$$
$$10 \mapsto |\psi_3(10)\rangle \coloneqq [\alpha|0\rangle - \beta|1\rangle], \tag{1.2.37}$$
$$11 \mapsto |\psi_3(11)\rangle \coloneqq [\alpha|1\rangle - \beta|0\rangle]. \tag{1.2.38}$$

因为 Bob 要知道 Alice 的测量结果才能恢复 $|\psi\rangle$, 所以隐形传态传送信息的速率是受限的, 不能超过光速。当 Alice 的测量结果为 00 时, Bob 不需要做任何事。如果 Alice 的测量结果是 01, 那么 Bob 需要用 X 门来修正量子态; 如果 Alice 的测量结果是 10, 那么 Bob 需要用 Z 门来修正量子态; 如果 Alice 的测量结果是 11, 那么 Bob 需要用 X 和 Z 门来修正量子态, 即应用变换 $Z^{M_1}X^{M_2}$。注意矩阵乘积项的顺序与时间流逝的顺序相反。

1.3 量子算法

1.3.1 Toffoli 门：量子计算的经典门

Toffoli 门 (Toffoli gate)[3]是量子计算中的一个重要门, 也称 CCX 门, 如图 1.9 所示, 前两个比特是控制位, 第三个比特是目标位, 真值表如表 1.1 所示。

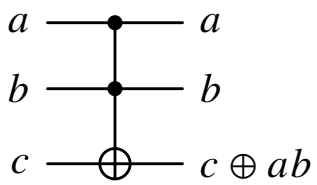
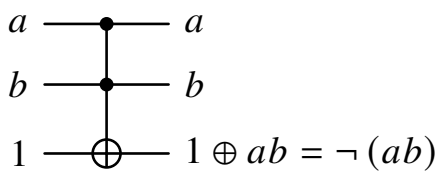


图 1.9: Toffoli 门

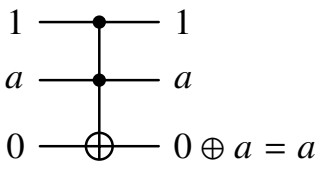
表 1.1: Toffoli 门及其作用两次的真值表

a	b	c	ab	$c \oplus ab$	$c \oplus ab \oplus ab$
0	0	0	0	0	0
0	0	1	0	1	1
0	1	0	0	0	0
0	1	1	0	1	1
1	0	0	0	0	0
1	0	1	0	1	1
1	1	0	1	1	0
1	1	1	1	0	1

作用 Toffoli 门两次又回到了原来的状态, 即可以用来模拟经典电路中的 NAND 门, 如图 1.10a 所示。



(a) 利用 Toffoli 门实现 NAND 门。第 3 个比特是辅助态。上两比特是输入, 第 3 比特是输出



(b) 利用 Toffoli 门实现扇出, 即量子比特的复制。第 1、3 比特是辅助态。第 2 比特是输入, 第 2、3 比特是输出

图 1.10

1.3.2 量子并行性

量子并行性 (quantum parallelism)是许多量子算法的基本性质, 即允许量子计算机同时计算不同 x 的函数值 $f(x)$。

考虑函数 $f(x) : \{0,1\} \mapsto \{0,1\}$, 第一个寄存器是数据寄存器, 第二个寄存器是目标寄存器。定义映射 $U_f : |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$, 这是个幺正变换, 如图 1.11 所示。

[3]托佛利, Tommaso Toffoli, 1943.06—, 意大利裔美国计算机科学家。

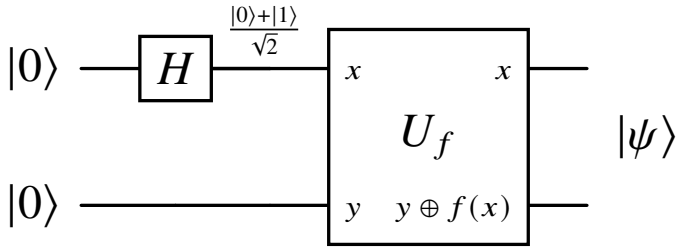


图 1.11: 同时计算 $f(0)$ 和 $f(1)$ 的量子线路

两个比特初态为 $|00\rangle$, 第一个比特经过 H 门后变为 $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, 然后和第二个比特 $|0\rangle$ 一起经过 U_f 门, 有

$$\begin{aligned}\frac{1}{\sqrt{2}}\left[|00\rangle + |10\rangle\right] &\mapsto \frac{1}{\sqrt{2}}\left[|0, 0 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle\right] \\ &= \frac{1}{\sqrt{2}}\left[|0, f(0)\rangle + |1, f(1)\rangle\right]. \end{aligned} \tag{1.3.1}$$

输出的态中, 不同的项包含 $f(0)$ 和 $f(1)$ 的信息, 看起来像是同时计算了 $f(x)$ 的两个值, 这就是量子并行性的体现。

可以把以上过程推广, 将 n 个 H 门作用在 n 个量子比特上, 记作 $H^{\otimes n}$, $\otimes$ 是张量积算符。

当 $n = 2$, 且初态制备均为 $|0\rangle$ 时, 有输出

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}. \tag{1.3.2}$$

推广到任意正整数 n, 初态制备均为 $|0\rangle$ 时, 有输出

$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle, \tag{1.3.3}$$

其中 x 是 n 位二进制数。

然后将经过 n 个 H 门后的输出和目标比特一起经过 U_f 门, 制备 $n + 1$ 比特的量子态 $|0\rangle^{\otimes n}|0\rangle$, 有输出

$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle\,|f(x)\rangle. \tag{1.3.4}$$

一次计算就可以同时得到 $f(x)$ 的所有 2^n 个值。

1.3.3 Deutsch-Jozsa 算法

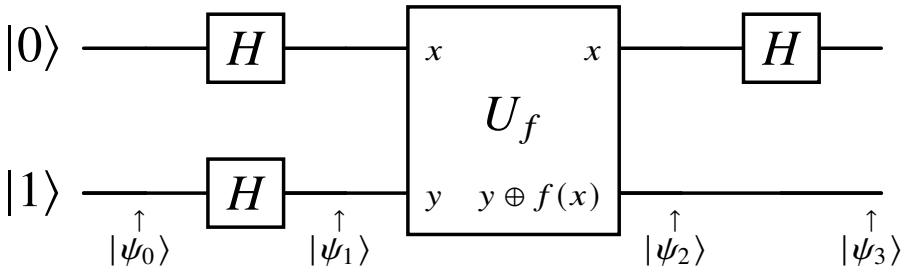


图 1.12: Deutsch 算法

对图 1.11 进行一些修改得到 **Deutsch 算法 (Deutsch algorithm)**[4], 如图 1.12 所示, 输入态为

$$|\psi_0\rangle = |01\rangle\,, \tag{1.3.5}$$

通过两个 H 门后, 有

$$|\psi_1\rangle = |+\rangle\,|-\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{1.3.6}$$

现在来看 U_f 门的作用。当 $f(x) = 0$ 时, 有

$$|x\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \oplus |0\rangle\right] = |x\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right], \tag{1.3.7}$$

当 $f(x) = 1$ 时, 有

$$|x\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \oplus |1\rangle\right] = |x\rangle\left[\frac{|1\rangle - |0\rangle}{\sqrt{2}}\right], \tag{1.3.8}$$

写在一起就是

$$|x\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \oplus |f(x)\rangle\right] = (-1)^{f(x)}\,|x\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right], \tag{1.3.9}$$

所以

$$\begin{aligned} |\psi_2\rangle &= \left[\frac{(-1)^{f(0)}\,|0\rangle + (-1)^{f(1)}\,|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \\ &= \begin{cases} \pm\left[\dfrac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right], & f(0) = f(1), \\ \pm\left[\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\left[\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right], & f(0) \neq f(1), \end{cases} \end{aligned} \tag{1.3.10}$$

[4]多伊奇, David Elieser Deutsch, 1953.05.18—, 英国物理学家。

最后第一个比特经过 H 门后, 有

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right], & f(0)=f(1), \\ \pm|1\rangle\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right], & f(0)\neq f(1), \end{cases} \tag{1.3.11}$$

注意到当 $f(0)=f(1)$ 时, $f(0)\oplus f(1)=0$, 否则为 1, 所以

$$|\psi_3\rangle = \pm|f(0)\oplus f(1)\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]. \tag{1.3.12}$$

测量第一个比特, 就可以知道 $f(0)\oplus f(1)$ 的值, 量子线路只需要计算一次 $f(x)$, 而经典计算需要计算两次 $f(x)$。这就是 Deutsch 算法的量子优势。

将 Deutsch 算法一般化, 就可得 **Deutsch-Jozsa 算法 (Deutsch-Jozsa algorithm)**[5], 它是量子计算中的一个重要算法, 用于判断一个函数是常函数还是平衡函数。平衡函数是指函数的值在 0 和 1 上均匀分布。

Deutsch-Jozsa 算法应用于 Deutsch 问题, 问题描述是 Alice 从 0 到 2^n-1 之间的 x 中选择一个数给 Bob, Bob 计算出某个函数 $f(x):\{0,1\}^n\mapsto\{0,1\}$ 的值, Alice 想要判断 $f(x)$ 是常函数还是平衡函数。Deutsch-Jozsa 算法的量子线路如图 1.13 所示。

在经典情况下, Alice 一次只能发一个 x 给 Bob, Alice 要问 Bob 至少 $2^{n-1}+1$ 次计算才能判断 $f(x)$ 是常函数还是平衡函数, 因为在她收到第一个 1 之前可能会收到 $2^n/2$ 个 0, 从而知道 $f(x)$ 是平衡函数。而在量子情况下, Alice 只需要与 Bob 通信一次就能判断 $f(x)$ 是常函数还是平衡函数。

Deutsch-Jozsa 算法的量子线路如图 1.13 所示。

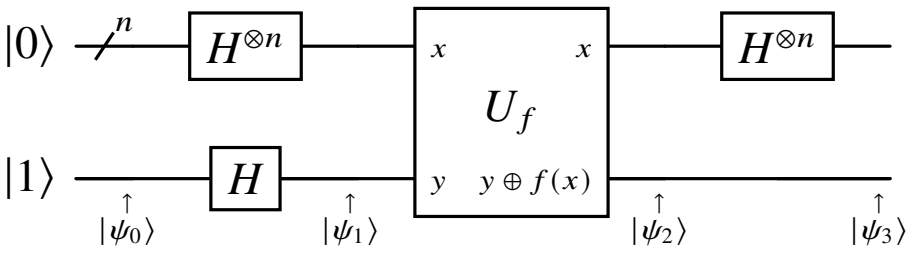


图 1.13: Deutsch-Jozsa 算法。/ 处的 n 代表有 n 个量子比特

输入态为

$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle, \tag{1.3.13}$$

经过 $H^{\otimes n}$ 门后, 有

$$|\psi_1\rangle = |+\rangle^{\otimes n}|-\rangle = \left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]^{\otimes n}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] = \sum_{x\in\{0,1\}^n}\frac{|x\rangle}{2^{n/2}}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]. \tag{1.3.14}$$

经过 U_f 门后, 有

$$|\psi_2\rangle = \sum_{x\in\{0,1\}^n}\frac{(-1)^{f(x)}|x\rangle}{2^{n/2}}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]. \tag{1.3.15}$$

[5]约扎, Richard Jozsa, 1953.11.13—, 澳大利亚数学家。

前 n 个比特经过 $H^{\otimes n}$ 门后, 有

$$H^{\otimes n}|x_1,\ldots,x_n\rangle = \sum_{z_1,\ldots,z_n} \frac{(-1)^{x_1z_1+\cdots+x_nz_n}}{2^{n/2}}|z_1,\ldots,z_n\rangle, \tag{1.3.16}$$

或更简洁地写成

$$H^{\otimes n}|x\rangle = \sum_{z=0}^{2^n-1} \frac{(-1)^{x\cdot z}}{2^{n/2}}|z\rangle, \tag{1.3.17}$$

其中 $x\cdot z$ 是 x 和 z 的二进制内积 (按位模 2)。得到

$$|\psi_3\rangle = \sum_z\sum_x \frac{(-1)^{x\cdot z+f(x)}}{2^n}|z\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]. \tag{1.3.18}$$

现在 Alice 测量前 n 个比特, 注意到态 $|0\rangle^{\otimes n}$ 的振幅是 $\sum_x \frac{(-1)^{f(x)}}{2^n}$。当 f 是常函数时, $|0\rangle^{\otimes n}$ 的振幅是 1 或 -1; 当 f 是平衡函数时, $|0\rangle^{\otimes n}$ 的振幅是 0。所以, 如果测量结果全为 0, 那么 f 是常函数; 否则 f 是平衡函数。

附录 A

参考书目

[1] Kaye PR, Laflamme R, Mosca M. An Introduction to Quantum Computing. Oxford University Press, 2007.

[2] Nielsen MA, Chuang IL. Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press, 2010.
中译本：孙晓明, 尚云, 李绿周等译. 量子计算与量子信息 (10 周年版). 电子工业出版社, 2022.

索引