科学计算中的量子算法：量子力学与量子算法基础 1

安冬

北京大学北京国际数学研究中心（BICMR）

andong@bicmr.pku.edu.cn

25-26 学年第 2 学期

大纲

- 量子力学的基本原理和数学表达方法
- 量子态、量子比特、门、变换、测量、量子电路等基本概念
- Deutsch-Jozsa 算法

量子力学的基本原理

- **状态空间假设**（State space postulate）
- **演化假设**（Evolution postulate）
- **量子测量假设**（Quantum measurement postulate）
- **复合系统假设**（Composite system postulate）

量子力学的基本原理：状态空间假设

公设 1: 任意一个孤立的物理系统都与一个称为系统状态空间的复内积向量空间相联系。系统完全由状态向量来描述，它是系统状态空间里的一个单位向量。

经典比特：0 或 1

量子比特（qubit）：$|0\rangle$ 和 $|1\rangle$ 的叠加（superposition）

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

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2$$

- 测量（measure）一个量子比特：$|\alpha|^2$ 概率变为 0，$|\beta|^2$ 概率变为 1

$$|\alpha|^2 + |\beta|^2 = 1, \quad \langle\psi|\psi\rangle = 1.$$

单量子比特

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad |\alpha|^2 + |\beta|^2 = 1.$$

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle\right), \quad \gamma \in [0, 2\pi), \theta \in [0, \pi), \phi \in [0, 2\pi).$$

- γ：**全局相位**（global phase）
- Bloch **球**：$(\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)^T$

量子力学的基本原理：演化假设

公设 2: 封闭量子系统的演化可用酉变换来描述。

$$|\psi'\rangle = U|\psi\rangle\,.$$

$$U \in \mathbb{C}^{2\times 2}, \quad U^\dagger U = I.$$

单量子比特下，U 也被称为单量子比特门

单量子比特门

Pauli 门:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Hadamard 门:

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

相位门:

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

T 门:

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}.$$

单量子比特门

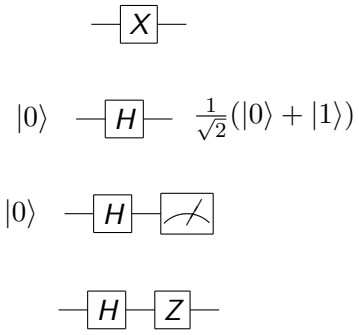
Pauli 旋转门：

$$R_X(\theta) = e^{-iX\theta/2} = \begin{pmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{pmatrix},$$

$$R_Y(\theta) = e^{-iY\theta/2} = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix},$$

$$R_Z(\theta) = e^{-iZ\theta/2} = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}.$$

量子线路（Quantum circuit）



量子力学的基本原理：复合系统假设

公设 4：复合物理系统的状态空间是分物理系统的状态空间的张量积。

$$A = \mathbb{C}^p = \mathrm{span}\left\{e_A\right\}, \quad B = \mathbb{C}^q = \mathrm{span}\left\{e_B\right\}, \quad A \otimes B = \mathrm{span}\left\{e_A \otimes e_B\right\} \cong \mathbb{C}^{pq}$$

双量子比特

$$|00\rangle = |0\rangle \otimes |0\rangle = |0\rangle\,|0\rangle\,, |01\rangle\,, |10\rangle\,, |11\rangle$$

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

注：我们有时也记 $|k\rangle = |(k)_2\rangle\,, 0 \leq k \leq 3$，**称为计算基**（Computational basis）

$$|0\rangle = |00\rangle\,, |1\rangle = |01\rangle\,, |2\rangle = |10\rangle\,, |3\rangle = |11\rangle\,.$$

双量子比特

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \in \mathbb{C}^4, \quad \sum |\alpha_{ij}|^2 = 1.$$

- 全部测量：以 $|\alpha_{00}|^2$ 概率变为 00，以此类推
- 部分测量：只测量第一个量子比特，以 $|\alpha_{00}|^2 + |\alpha_{01}|^2$ 概率变为 0，测量后的量子态变为

$$\frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} = |0\rangle \left(\frac{\alpha_{00}|0\rangle + \alpha_{01}|1\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} \right)$$

双量子比特

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle, \quad \sum |\alpha_{ij}|^2 = 1.$$

- 并非所有的双比特量子态都可以写成张量积的形式
- 贝尔态/EPR 对:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- 量子纠缠（Quantum entanglement）

多量子比特

n 个量子比特：$|i_0 i_1 \cdots i_{n-1}\rangle = |i_0\rangle \otimes |i_1\rangle \otimes \cdots \otimes |i_{n-1}\rangle \in \mathbb{C}^{2^n}, i_j \in \{0,1\}$

记

$$|k\rangle = |(k)_2\rangle \in \mathbb{C}^{2^n}, \quad 0 \le k \le 2^n - 1$$

$$|\psi\rangle = \sum_{k=0}^{2^n-1} \alpha_k |k\rangle \in \mathbb{C}^{2^n} = (\alpha_0, \cdots, \alpha_{2^n-1})^T, \quad \| |\psi\rangle \| = 1.$$

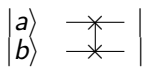
n 个量子比特可以表示 2^n 维单位向量，指数加速？

- 构造：量子态制备
- 读取信息

多量子比特门

交换门（SWAP）：

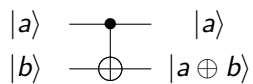
$$\mathrm{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$



多量子比特门

控制非门（CNOT）：

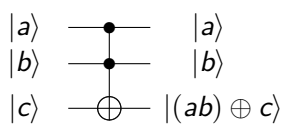
$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$



多量子比特门

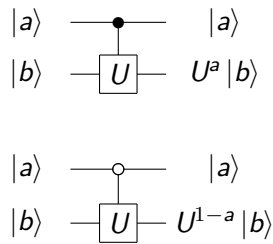
Toffoli 门:

$$\mathrm{CCNOT} = \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & 1 \\ & & & & & & 1 & \end{pmatrix}.$$



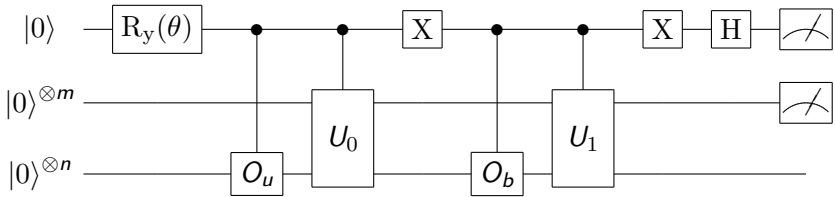
多量子比特门

控制酉变换：



一条线路也可以代表多个量子比特：寄存器（register）

量子算法

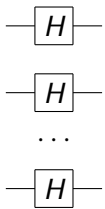


- 张量积
- 量子“并行”
- 振幅相干相消

Walsh-Hadamard 変換

$$H_0 = 1, \quad H_m = \frac{1}{\sqrt{2}} \begin{pmatrix} H_{m-1} & H_{m-1} \\ H_{m-1} & -H_{m-1} \end{pmatrix}.$$

$$H_m \in \mathbb{C}^{2^m \times 2^m}, \quad H_m = H^{\otimes m}$$



$$H_m |0\rangle^{\otimes m} = \frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} |k\rangle$$

$$|0\rangle^{\otimes m} \text{ — } \boxed{H^{\otimes m}} \text{ — } \frac{1}{\sqrt{2^m}} \sum_k |k\rangle$$

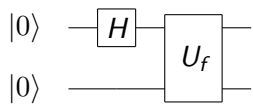
量子“并行”

函数 $f(x) : \{0,1\} \to \{0,1\}$

- **经典**：$x \mapsto f(x)$
- **量子**：$|x\rangle \mapsto |f(x)\rangle$?

量子 Oracle：$U_f |x\rangle |0\rangle = |x\rangle |f(x)\rangle$

考虑线路：



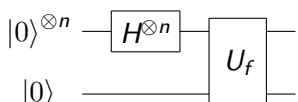
- **输出**：$\frac{1}{\sqrt{2}} \sum_{x=0}^{1} |x\rangle |f(x)\rangle$
- **一次函数访问“同时计算”两个函数值，然而信息存储在叠加态中**

量子“并行”

函数 $f(x) : [2^n] \to \{0, 1\}$ （**这里** $[N] = \{0, 1, 2, \cdots, N-1\}$）

量子 Oracle：$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$, $x \in [2^n]$

考虑线路：



- **输出**：$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$
- **一次函数访问“同时计算”** 2^n **个函数值**

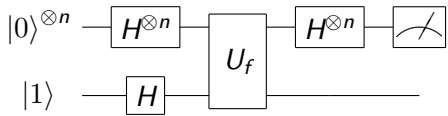
Deutsch-Jozsa 算法

函数 $f(x) : [2^n] \to \{0, 1\}$ （这里 $[N] = \{0, 1, 2, \cdots, N-1\}$）

- 黑盒
- 保证：要么 $f(x)$ 为常值函数，要么 $f(x)$ 为平衡函数（对于一半的 x 取 0，另一半取 1）

问：需要调用多少次 $f(x)$ 才能确定它是哪一种类型？

Deutsch-Jozsa 算法



$$|0\rangle^{\otimes n}|1\rangle \to \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \to \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$
$$\to \frac{1}{2^n}\sum_{z}\sum_{x}(-1)^{x\cdot z+f(x)}|z\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

- 若 $f(x)$ 为常数函数，则第一个寄存器始终为 $|0\rangle^{\otimes n}$
- 若 $f(x)$ 为平衡函数，则第一个寄存器 $|0\rangle^{\otimes n}$ 的振幅为 0

仅需一次函数访问！

Deutsch-Jozsa 算法

量子 1 次 vs 经典 $2^{n-1}+1$ 次

注:

- 尚无应用场景
- 概率经典计算也可以实现类似的效率

量子力学的基本原理：量子测量假设

公设 3：量子测量由一组测量算子描述，这些算子作用在被测量的状态空间上，可能出现不同的测量结果。

考虑厄米矩阵 M（称为可观测量），有谱分解

$$M = \sum_m \lambda_m P_m$$

- $\lambda_m \in \mathbb{R}$：特征值
- P_m：特征空间的投影算子

观测后：

- 以 $p_m = \langle\psi|P_m|\psi\rangle$ 概率输出实数 λ_m（$\{p_m\}$ 是一个离散概率分布）
- 对应的量子态变为 $\frac{P_m|\psi\rangle}{\sqrt{p_m}}$

量子力学的基本原理：量子测量假设

例子 1:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad M = |1\rangle\langle 1|$$

例子 2:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad M = X$$

量子力学的基本原理：量子测量假设

$$M = \sum_m \lambda_m P_m$$

$$\mathbb{E}_\psi(M) = \sum_m p_m \lambda_m = \sum_m \lambda_m \langle\psi|P_m|\psi\rangle = \langle\psi|(\sum_m \lambda_m P_m)|\psi\rangle = \langle\psi|M|\psi\rangle$$

- **推迟测量原理**（principle of deferred measurements）
- **隐含测量原理**（principle of implicit measurements）

其他内容与阅读

- **纯态**（pure state）**与混合态**（mixed state）、**密度矩阵**（density matrix）
- **通用量子门集合**（universal gate set）

阅读:

- LL: Chapter 1.1, 1.3, 1.5, 2.1
- NC: Section 1,2,4