量子计算基础

比特与量子比特

经典计算机中，经典比特的状态是确定的，只有 `0`,`1` 两种可能。物理实现上需要介质能稳定保存两种可区分的物理状态（如 “高 / 低电压”“有 / 无电流”“正 / 反磁极”）。

量子比特突破了“非 0 即 1” 的限制，`叠加态` 与 `纠缠态` 的存在赋予了量子计算算力优势。

其物理实现目前没有统一的最优方案，超导、离子阱等技术路线都各有优劣。

叠加态与纠缠态

对于一个量子比特，虽然我们在观测前无法确定其具体取值，但我们可以用概率描述它：$\vec{v}=\begin{bmatrix}p_0\\p_1\end{bmatrix}$
p_0 是比特为 `0` 的概率，p_1 是比特为 `1` 的概率，也就是说比特可能处于 `0` 与 `1` 的混合状态，即**叠加态。**

对于多个量子比特，它们的状态可以相互关联，处于量子纠缠，即**纠缠态。**

对于两个处于纠缠态的量子比特，它们可以被描述为：$\vec{v}=\begin{bmatrix}p_{00}\\p_{01}\\p_{10}\\p_{11}\end{bmatrix}$。

张量积与狄拉克符号

张量积:
假如有矩阵A,B，并且:

$$A=\begin{bmatrix}a_{11} & a_{12} & \cdots & a_{1m}\\ a_{21} & a_{22} & \cdots & a_{2m}\\ \vdots & \vdots & \ddots & \vdots\\ a_{n1} & a_{n2} & \cdots & a_{nm}\end{bmatrix}$$

那么A与B的张量积$A\otimes B$:

$$A\otimes B=\begin{bmatrix}a_{11}B & a_{12}B & \cdots & a_{1m}B\\ a_{21}B & a_{22}B & \cdots & a_{2m}B\\ \vdots & \vdots & \ddots & \vdots\\ a_{n1}B & a_{n2}B & \cdots & a_{nm}B\end{bmatrix}$$

对于刚刚提到的多量子状态描述，$\vec{v}=\vec{v_1}\otimes\vec{v_2}\otimes\cdots$。

狄拉克符号

狄拉克符号是向量的简化表示，分为左矢和右矢，分别对应行向量和列向量。

右矢：$|\psi\rangle$，左矢 $\langle\psi|$。

定义基态（n 个量子比特取值确定）。

$n=1$ 时有 $|0\rangle=\begin{bmatrix}1\\0\end{bmatrix},|1\rangle=\begin{bmatrix}0\\1\end{bmatrix}$。

$n=2$ 时，基态由 $n=1$ 时基态做张量积得到：$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$。

任意叠加态 $|\psi\rangle = \sum_i c_i |v_i\rangle$。

概率振幅与概率

事实上，叠加态向量的元素对应的并不是概率，而是一个复数：**概率振幅**。

若振幅为 α，其对应概率为 $|\alpha|^2$。

自然，整个向量应该要满足**归一化条件**，即概率总和为 1。

观测与局部观测

对于整个量子比特系统观测，得到的结果符合狄拉克符号里的概率分布。

对于若干个量子比特单独观测，系统会坍缩一些状态，仍满足归一化条件，振幅会等比缩放。

量子门

类比经典门操作，量子门可以操纵量子比特的状态。

与经典门不同的是，量子门 U 作为一个矩阵必须满足**幺正性**。

$U^\top U = I$，确保作用 U 后仍满足归一化条件。

单量子门

X 门：$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$，反转量子比特。

Z 门：$\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$，反转相位。

R_θ 门：$\begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix}$，旋转相位。

哈达玛变换 H 门：$\dfrac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$，使计算基态转变为等概率叠加态。

多量子门

由单量子门做张量积可以得到一些多量子门，意义是对多个量子系统实现这些单量子门操作。

然而许多多量子门无法简单的通过单量子门扩展得到。

受控非门 CNOT 门：当控制比特为 `0` 时不对受控比特操作，当控制比特为 `1` 时反转受控比特。

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