理论作业二　量子测量与量子算法

王晓宇　3220104364

2024 年 11 月 7 日

---

1. 假设有初始化为 $|1\rangle$ 态的量子寄存器若干，给出分别使用酉算子 H、X、T、S 进行测量的结果。

i. 使用 H 算子进行测量。

$$|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

ii. 使用 X 算子进行测量。

$$|1\rangle \xrightarrow{X} |0\rangle$$

iii. 使用 T 算子进行测量。

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

$$|1\rangle \xrightarrow{T} e^{i\frac{\pi}{4}}|1\rangle$$

iv. 使用 S 算子进行测量。

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

$$|1\rangle \xrightarrow{S} i|1\rangle$$

2. 证明 Grover 算法中的算子 G 每次作用时使量子态向 $|\beta\rangle$ 方向旋转角度 θ。

初始状态为 $|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle = \cos(\frac{\theta}{2})|\alpha\rangle + \sin(\frac{\theta}{2})|\beta\rangle$

其中 N 为待检验的解个数，M 为可行解的数量。

这里为了简便表示 $|\psi\rangle$, 我们将系数表示为 $\cos(\frac{\theta}{2})$ 和 $\sin(\frac{\theta}{2})$，其中 $\frac{\theta}{2}$ 为初始态与正解轴 α 之间的夹角。

我们将 Grover 算法中的算子 G 作用按照课上所讲分为两个部分，即 Oracle 和 Combined(2、3、4 步骤结合的酉矩阵)。

i. Orcale 作用：改变正解相位

$$|x\rangle \stackrel{Orcale}{\longrightarrow} (-1)^{f(x)}|x\rangle$$

平面作用：以 $|\alpha\rangle$ 为轴做对称操作，在 $|\alpha\rangle$ 上的投影不变，即 $|\alpha\rangle$ 不变，$|\beta\rangle$ 上的投影翻转。即：

$$|x\rangle = p|\alpha\rangle + q|\beta\rangle \stackrel{Orcale}{\longrightarrow} p|\alpha\rangle - q|\beta\rangle$$

ii. Combined 我们这里表示 $|x\rangle$ 时更换基：$|x\rangle = p|\psi\rangle + q|\psi\rangle_\perp$，其中 $|\psi\rangle_\perp$ 为与 $|\psi\rangle$ 正交的向量。作用：将 $|\psi\rangle$ 向 $|\beta\rangle$ 方向旋转

$$|x\rangle \stackrel{Combined}{\longrightarrow} (2|\psi\rangle\langle\psi| - I)\,|x\rangle$$

平面作用：以 $|\psi\rangle$ 为轴做对称操作

$$|x\rangle = p|\psi\rangle + q|\psi\rangle_\perp \stackrel{Combined}{\longrightarrow} p|\psi\rangle - q|\psi\rangle_\perp$$

我们证明的目标是证明 Grover 算法中的算子 G 每次作用时使量子态向 $|\beta\rangle$ 方向旋转角度 θ。这里可以用数学归纳法证明：

(1) 归纳奠基

证明 G 算子作用到初态上时成立：

$$|x\rangle = |\psi\rangle = \cos(\frac{\theta}{2})|\alpha\rangle + \sin(\frac{\theta}{2})|\beta\rangle$$

$$|x\rangle \stackrel{Orcale}{\longrightarrow} \cos(\frac{\theta}{2})|\alpha\rangle - \sin(\frac{\theta}{2})|\beta\rangle$$

$$\cos(\frac{\theta}{2})|\alpha\rangle - \sin(\frac{\theta}{2})|\beta\rangle \stackrel{Combined}{\longrightarrow} (2|\psi\rangle\langle\psi| - I)\left(\cos(\frac{\theta}{2})|\alpha\rangle - \sin(\frac{\theta}{2})|\beta\rangle\right)$$

$$\longrightarrow \begin{bmatrix} 2\cos^2(\frac{\theta}{2}) - 1 & 2\cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) \\ 2\cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) & 2\sin^2(\frac{\theta}{2}) - 1 \end{bmatrix} \begin{bmatrix} \cos(\frac{\theta}{2})|\alpha\rangle \\ -\sin(\frac{\theta}{2})|\beta\rangle \end{bmatrix}$$

$$\longrightarrow \cos(\frac{3\theta}{2})|\alpha\rangle + \sin(\frac{3\theta}{2})|\beta\rangle$$

证明确实向 $|\beta\rangle$ 方向旋转了 θ 角度。

(2) 归纳假设证明假设 G 算子作用到第 k-1 次时成立：

$$|x\rangle = \cos(\frac{(2k-1)\theta}{2})|\alpha\rangle + \sin(\frac{(2k-1)\theta}{2})|\beta\rangle$$

现证明 G 算子作用到第 k 次时成立：

$$|x\rangle = \cos(\frac{(2k-1)\theta}{2})|\alpha\rangle + \sin(\frac{(2k-1)\theta}{2})|\beta\rangle$$

$$|x\rangle \xrightarrow{Orcale} \cos(\frac{(2k-1)\theta}{2})|\alpha\rangle - \sin(\frac{(2k-1)\theta}{2})|\beta\rangle$$

$$\cos(\frac{(2k-1)\theta}{2})|\alpha\rangle - \sin(\frac{(2k-1)\theta}{2})|\beta\rangle$$

$$\xrightarrow{Combined} (2|\psi\rangle\langle\psi| - I)\left(\cos(\frac{(2k-1)\theta}{2})|\alpha\rangle - \sin(\frac{(2k-1)\theta}{2})|\beta\rangle\right)$$

$$\longrightarrow \begin{bmatrix} 2\cos^2(\frac{\theta}{2})-1 & 2\cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) \\ 2\cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) & 2\sin^2(\frac{\theta}{2})-1 \end{bmatrix} \begin{bmatrix} \cos(\frac{(2k-1)\theta}{2})|\alpha\rangle \\ -\sin(\frac{(2k-1)\theta}{2})|\beta\rangle \end{bmatrix}$$

$$\longrightarrow \cos(\frac{(2k+1)\theta}{2})|\alpha\rangle + \sin(\frac{(2k+1)\theta}{2})|\beta\rangle$$

证明确实向 $|\beta\rangle$ 方向旋转了 θ 角度。

根据数学归纳法，我们证明了 Grover 算法中的算子 G 每次作用时使量子态向 $|\beta\rangle$ 方向旋转角度 θ。

3. 根据 Grover 算法中 M、N 的定义，令 $\gamma = M/N$，证明在 $|\alpha\rangle$、$|\beta\rangle$ 基下，Grover 算法中的算子 G 可以写为 $\begin{bmatrix} 1-2\gamma & -2\sqrt{\gamma-\gamma^2} \\ 2\sqrt{\gamma-\gamma^2} & 1-2\gamma \end{bmatrix}$。

由上一道题的证明，我们知道 Grover 算法中的算子 G 可以分为两步：

i. Orcale

$$|x\rangle = p|\alpha\rangle + q|\beta\rangle \xrightarrow{Orcale} p|\alpha\rangle - q|\beta\rangle$$

ii. Combined

$$|x\rangle = p|\alpha\rangle + q|\beta\rangle = (2|\psi\rangle\langle\psi| - I)(p|\alpha\rangle + q|\beta\rangle)$$

我们将两个酉矩阵相乘，即：

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \times \begin{bmatrix} 2\cos^2(\frac{\theta}{2})-1 & 2\cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) \\ 2\cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) & 2\sin^2(\frac{\theta}{2})-1 \end{bmatrix} = \begin{bmatrix} 2cos(\frac{\theta}{2})^2-1 & 2\cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) \\ -2\cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) & 1-2\sin^2(\frac{\theta}{2}) \end{bmatrix}$$

$$= \begin{bmatrix} 1-2sin^2(\frac{\theta}{2}) & -2\cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) \\ 2\cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) & 1-2\sin^2(\frac{\theta}{2}) \end{bmatrix}$$

在上一个问题中我们同样表示了 θ，即：$\sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle = \cos(\frac{\theta}{2})|\alpha\rangle + \sin(\frac{\theta}{2})|\beta\rangle$

$$\therefore sin(\frac{\theta}{2}) = \sqrt{\frac{M}{N}} = \sqrt{\gamma}, cos(\frac{\theta}{2}) = \sqrt{\frac{N-M}{N}} = \sqrt{1-\gamma}$$

$$\therefore G = \begin{bmatrix} 1-2sin^2(\frac{\theta}{2}) & -2\cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) \\ 2\cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) & 1-2\sin^2(\frac{\theta}{2}) \end{bmatrix} = \begin{bmatrix} 1-2\gamma & -2\sqrt{\gamma-\gamma^2} \\ 2\sqrt{\gamma-\gamma^2} & 1-2\gamma \end{bmatrix}$$

Bonus: 给出 RSA 算法加密、解密过程的证明，即证明明文为 $a \equiv C^d \mod n$。

证明目标: $a \equiv C^d \mod n$。

已知条件：

(1) 加密过程产生等式

i. 明文 a，密文 C，且 $0 \leq a < n$，因为解密一直得到小于 n 的值。

ii. $n = pq$, 其中 p, q 为素数。

iii. $\phi(n) = (p-1)(q-1)$。

iv. e 满足 $1 < e < \phi(n)$ 且 $\gcd(e, \phi(n)) = 1$。

v. $d \equiv e^{-1} \mod \phi(n)$。

vi. $C = a^e \mod n$。

(2) 数学定理

i. Theorem1_ 欧拉函数性质：对于任意素数 p, q，$n = pq$，有 $\phi(n) = (p-1)(q-1)$。

ii. Theorem2_ 欧拉定理：对于任意整数 a 和 n 互质的情况，有 $a^{\phi(n)} \equiv 1 \mod n$。

iii. Theorem3_ 模逆元：$e, \phi(n)$ 互质，存在整数 d 使得 $ed \equiv 1 \mod \phi(n)$。

证明：

$$C^d = (a^e)^d = a^{ed}$$

$$\because Theorem3: \ d \equiv e^{-1} \mod \phi(n)$$

$\therefore$ 存在整数 k:

$$C^d = a^{ed} = a^{1+k\phi(n)} = a \times (a^{\phi(n)})^k$$

分情况讨论：

i. a,n 互质，根据 Theorem2，$a^{\phi(n)} \equiv 1 \mod n$。

$$C^d = a \times (a^{\phi(n)})^k \equiv a \times \left((a^{\phi(n)})^k \mod n\right) \equiv a \times 1 \equiv a \mod n \tag{1}$$

ii. a,n 不互质

$n = pq$, 则说明 a 必然是 p, q 中一个的倍数且不是两者乘积 n 的倍数

不妨假设 a 是 p 的倍数，即 $\exists t \in \mathbb{N}, \ a = p \times t$

$$\because Theorem2$$

$$\therefore a^{\phi(q)} \equiv 1 \mod q$$

两边同时乘方操作 $a^{k\phi(p)}$, 即：

$$a^{k\phi(p)\phi(q)} \equiv 1 \mod q$$

$$\because Theorem 1 \phi(n) = (p-1)(q-1)$$

$$\therefore \exists m \in \mathbb{N} \ s.t. \ a^{k\phi(p)\phi(q)} = a^{k\phi(n)} = q \times m + 1$$

$$\therefore C^d = a^{1+k\phi(n)} = a \times (q \times m + 1) = a + a \times q \times m = a + a \times tm(p \times q) = a + a \times tmn$$

$$\therefore C^d \equiv a \mod n$$

综上所述，$a \equiv C^d \mod n$。