理论作业二　量子测量与量子算法

李瀚轩　3220106039

2024 年 11 月 18 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。

Solution. 我们可以得到 H 的本征值为 $1, -1$, 对应本征态为 $|\lambda_1\rangle = \frac{\sqrt{2+\sqrt{2}}}{2}|0\rangle + \frac{\sqrt{2-\sqrt{2}}}{2}|1\rangle$ 和 $|\lambda_2\rangle = \frac{\sqrt{2-\sqrt{2}}}{2}|0\rangle - \frac{\sqrt{2+\sqrt{2}}}{2}|1\rangle$。
接下来我们进行测量，可以得到测量结果的概率

$$p_1 = |\langle\lambda_1|1\rangle|^2 = \frac{2-\sqrt{2}}{4}, p_2 = |\langle\lambda_2|1\rangle|^2 = \frac{2+\sqrt{2}}{4}$$

接下来几个算子的结果同理，X 的本征值为 $1, -1$，对应本征态 $|\lambda_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ 和 $|\lambda_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$。进行测量，可以得到测量结果的概率

$$p_1 = |\langle\lambda_1|1\rangle|^2 = \frac{1}{2}, p_2 = |\langle\lambda_2|1\rangle|^2 = \frac{1}{2}$$

T 的本征值为 $1, e^{i\frac{\pi}{4}}$，对应本征态 $|\lambda_1\rangle = |0\rangle$ 和 $|\lambda_2\rangle = |1\rangle$。进行测量，可以得到测量结果的概率

$$p_1 = |\langle\lambda_1|1\rangle|^2 = 0, p_2 = |\langle\lambda_2|1\rangle|^2 = 1$$

S 的本征值为 $1, i$, 对应本征态为 $|\lambda_1\rangle = |0\rangle$ 和 $|\lambda_2\rangle = |1\rangle$。进行测量，可以得到测量结果的概率

$$p_1 = |\langle\lambda_1|1\rangle|^2 = 0, p_2 = |\langle\lambda_2|1\rangle|^2 = 1$$

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。

Solution. 假设作用 k 次 G 算子之后量子态为

$$G^k|\psi\rangle = \cos(\frac{2k+1}{2}\theta)|\alpha\rangle + \sin(\frac{2k+1}{2}\theta)|\beta, \quad \theta = 2\arccos\sqrt{\frac{N-M}{N}}$$

我们使用数学归纳法来证明：

1. 当 $k=0$ 时，显然符合条件。
2. 假设对于 k 成立，即 $G^k|\psi\rangle = \cos(\frac{2k+1}{2}\theta)|\alpha\rangle + \sin(\frac{2k+1}{2}\theta)|\beta$。
3. 接下来我们证明对于 $k+1$ 也成立。对量子态作用 Oracle，$O(G^k|\psi\rangle) = \cos(\frac{2k+1}{2}\theta)|\alpha\rangle - \sin(\frac{2k+1}{2}\theta)|\beta$。之后作用扩散算子，我们有:

$$
\begin{aligned}
G^{k+1}|\psi\rangle &= (2|\psi\rangle\langle\psi| - I)O(G^k|\psi\rangle) && (1)\\
&= 2\cos(\frac{2k+1}{2}\theta)|\psi\rangle\langle\psi|\alpha\rangle - 2\sin(\frac{2k+1}{2}\theta)|\psi\rangle\langle\psi|\beta\rangle - O(G^k|\psi\rangle) && (2)\\
&= 2\left(\cos\frac{2k+1}{2}\theta\cos\frac{1}{2}\theta - \sin\frac{2k+1}{2}\theta\sin\frac{1}{2}\theta\right)|\psi\rangle - O(G^k|\psi\rangle) && (3)\\
&= 2\cos(\frac{2k+2}{2}\theta)|\psi\rangle - \cos(\frac{2k+1}{2}\theta)|\alpha\rangle + \sin(\frac{2k+1}{2}\theta)|\beta\rangle && (4)\\
&= \left(2\cos\frac{2k+2}{2}\theta\cos\frac{1}{2}\theta - \cos\frac{2k+1}{2}\theta\right)|\alpha\rangle && (5)\\
&+ \left(2\cos\frac{2k+2}{2}\theta\sin\frac{1}{2}\theta + \sin\frac{2k+1}{2}\theta\right)|\beta\rangle && (6)\\
&= \left(\cos\frac{2k+3}{2}\theta + \cos\frac{2k+1}{2}\theta - \cos\frac{2k+1}{2}\theta\right)|\alpha\rangle && (7)\\
&+ \left(\sin\frac{2k+3}{2}\theta - \sin\frac{2k+1}{2}\theta + \sin\frac{2k+1}{2}\theta\right)|\beta\rangle && (8)\\
&= \cos(\frac{2k+3}{2}\theta)|\alpha\rangle + \sin(\frac{2k+3}{2}\theta)|\beta\rangle && (9)
\end{aligned}
$$

因此对于 $k+1$ 也成立，归纳假设成立。

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 $\begin{bmatrix} 1-2\gamma & -2\sqrt{\gamma-\gamma^2} \\ 2\sqrt{\gamma-\gamma^2} & 1-2\gamma \end{bmatrix}$。

Solution. 我们假设被作用的态为 $|\phi\rangle = a|\alpha\rangle + b|\beta\rangle$，作用 G 之后得到

$$G|\phi\rangle = (2a\cos^2\frac{\theta}{2} - 2b\sin\frac{\theta}{2}\cos\frac{\theta}{2} - a)|\alpha\rangle + (2a\sin\frac{\theta}{2}\cos\frac{\theta}{2} - 2b\sin^2\frac{\theta}{2} + b)|\beta\rangle$$

因此我们可以写出矩阵：

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

我们有 $\cos\theta = 1-2\gamma, \sin\theta = 2\sqrt{\gamma-\gamma^2}$，代入矩阵中得证。

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

Solution. RSA 算法的加密过程如下：

1. 选择两个不同的大素数 p 和 q，计算 $n = pq$。
2. 计算 $\varphi(n) = (p-1)(q-1)$。
3. 选择一个整数 e，使得 $1 < e < \varphi(n)$ 且 e 与 $\varphi(n)$ 互质。
4. 计算 d，使得 $ed \equiv 1 \pmod{\varphi(n)}$。
5. 公钥是 (n, e)，私钥是 (n, d)。
6. 加密明文 a，计算密文 $c = a^e \pmod{n}$。
7. 解密密文 c，计算明文 $a = c^d \pmod{n}$。

接下来我们给出证明：由于 $ed \equiv 1 \pmod{\varphi(n)}$，因此存在整数 k 使得 $ed = 1 + k\varphi(n)$.

如果 $(a, n) = 1$，根据费马小定理，$a^{\varphi(n)} \equiv 1 \pmod{n}$，因此 $a^{cd} \equiv a^{k\varphi(n)+1} \equiv a \pmod{n}$。

如果 $(a, n) \neq 1$, 因为 $n = p_1 p_2$ 并且 $a < n$，所以 a 一定是 p_1 或者 p_2 的倍数。我们设 $a = mp_1$，这时有 $(a, p_2) = 1$，因此 $a^{\varphi(p_2)} \equiv 1 \pmod{p_2}$，即 $a^{k\varphi(p_2)} \equiv 1 \pmod{p_2}$。

因此我们有：

$$(a^{k\varphi(p_2)})^{\varphi(p_1)} \equiv 1^{\varphi(p_1)} \equiv 1 \pmod{p_2}$$

即，

$$a^{k\varphi(n)} = 1 + bp_2$$

两边同乘 a 得到：

$$a^{k\varphi(n)+1} = a + nbm \equiv a \pmod{n}$$

因此 $a \equiv C^d \mod n$ 得证。