理论作业二　量子测量与量子算法

杨亿酬　3230105697

2025 年 11 月 12 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。

解：$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}, X=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}, T=\begin{bmatrix}1 & 0\\ 0 & e^{\frac{i\pi}{4}}\end{bmatrix}, S=\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$

H：先对 H 作谱分解

(1) 特征值：

$det(H-\lambda I)=0 \Rightarrow det\begin{pmatrix}\frac{1}{\sqrt{2}}-\lambda & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}-\lambda\end{pmatrix}=0 \Rightarrow \lambda=\pm 1$

(2) 特征向量：

对 $\lambda=1$，解 $(H-I)v=0$

$\begin{bmatrix}\frac{1}{\sqrt{2}}-1 & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}-1\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix}=0 \Rightarrow y=(\sqrt{2}-1)x$

取 $x=1, y=\sqrt{2}-1$，归一化因子 $N_1=\frac{1}{\sqrt{x^2+y^2}}=\frac{1}{\sqrt{4-2\sqrt{2}}}$

$|e_1\rangle=\frac{|0\rangle+(\sqrt{2}-1)|1\rangle}{\sqrt{4-2\sqrt{2}}}$

同理对 $\lambda=-1, |e_2\rangle=\frac{|0\rangle+(-\sqrt{2}-1)|1\rangle}{\sqrt{4+2\sqrt{2}}}$

用 H 对 $|1\rangle$ 进行测量，有 p_i 的概率得到态 $|\psi_i\rangle, i=1,2$

$$p_1=\langle\psi|e_1\rangle\langle e_1|\psi\rangle=(\langle 1|e_1\rangle)^2=(\frac{\sqrt{2}-1}{\sqrt{4-2\sqrt{2}}})^2=\frac{3-2\sqrt{2}}{4-2\sqrt{2}}, |\psi_1\rangle=\frac{|e_1\rangle\langle e_1|\psi\rangle}{\sqrt{p_1}}=|e_1\rangle$$

$$p_2=\langle\psi|e_2\rangle\langle e_2|\psi\rangle=\frac{3+2\sqrt{2}}{4+2\sqrt{2}}, |\psi_2\rangle=\frac{|e_2\rangle\langle e_2|\psi\rangle}{\sqrt{p_2}}=|e_2\rangle$$

X:$\lambda_1=1$, 对应 $e_1=\frac{|0\rangle+|1\rangle}{\sqrt{2}}$,$\lambda_2=-1$, 对应 $e_2=\frac{|0\rangle-|1\rangle}{\sqrt{2}}$

$$p_1=\langle\psi|e_1\rangle\langle e_1|\psi\rangle=\frac{1}{2}, |\psi_1\rangle=\frac{|e_1\rangle\langle e_1|\psi\rangle}{\sqrt{p_1}}=|e_1\rangle$$

$$p_2=\langle\psi|e_2\rangle\langle e_2|\psi\rangle=\frac{1}{2}, |\psi_2\rangle=\frac{|e_2\rangle\langle e_2|\psi\rangle}{\sqrt{p_2}}=|e_2\rangle$$

T:$\lambda_1=1$, 对应 $e_1=|0\rangle$,$\lambda_2=e^{\frac{i\pi}{4}}$, 对应 $e_2=|1\rangle$

$$p_1=\langle\psi|e_1\rangle\langle e_1|\psi\rangle=0, |\psi_1\rangle=\frac{|e_1\rangle\langle e_1|\psi\rangle}{\sqrt{p_1}}=|e_1\rangle$$

$$p_2=\langle\psi|e_2\rangle\langle e_2|\psi\rangle=1, |\psi_2\rangle=\frac{|e_2\rangle\langle e_2|\psi\rangle}{\sqrt{p_2}}=|e_2\rangle$$

S:$\lambda_1=1$, 对应 $e_1=|0\rangle$,$\lambda_2=i$, 对应 $e_2=|1\rangle$

$$p_1=\langle\psi|e_1\rangle\langle e_1|\psi\rangle=0, |\psi_1\rangle=\frac{|e_1\rangle\langle e_1|\psi\rangle}{\sqrt{p_1}}=|e_1\rangle$$

$$p_2=\langle\psi|e_2\rangle\langle e_2|\psi\rangle=1, |\psi_2\rangle=\frac{|e_2\rangle\langle e_2|\psi\rangle}{\sqrt{p_2}}=|e_2\rangle$$

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。

证明：设某次迭代初始态为 $|\psi\rangle$，其与 $|\alpha\rangle$ 呈 $\theta/2$ 角，作用 Oracle 后得到 $O|\psi\rangle$,$O|\psi\rangle$ 与 $|\psi\rangle$ 关于 $|\alpha\rangle$ 对称，则 $<|\psi\rangle,|\alpha\rangle>=<|\alpha\rangle,O|\psi\rangle>=\theta/2, <|\psi\rangle,O|\psi\rangle>=\theta$

Grover 算法中的算子 G 可写作 $DO=(2|\psi\rangle\langle\psi|-I)O, \forall|v\rangle=p|\psi\rangle+q|\psi\rangle_\perp$

$G|v\rangle=(2|\psi\rangle\langle\psi|-I)|v\rangle=2p|\psi\rangle\langle\psi||\psi\rangle-p|\psi\rangle+2q|\psi\rangle\langle\psi||\psi\rangle_\perp-q|\psi\rangle_\perp=p|\psi\rangle-q|\psi\rangle_\perp$

设 $|\psi'\rangle=G(O|\psi\rangle)$, 则 $|\psi'\rangle$ 与 $O|\psi\rangle$ 关于 $|\psi\rangle$ 对称

$\therefore <|\psi'\rangle,|\psi\rangle>=<|\psi\rangle,O|\psi\rangle>=\theta$, 即作用算子 G 使量子态向 $|\beta\rangle$ 旋转了角度 θ

另证：Grover 算法的初始量子态

$$\begin{aligned}|\psi_0\rangle&=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle\\&=\cos(\theta/2)|\alpha\rangle+\sin(\theta/2)|\beta\rangle\end{aligned}$$

$$cos(\theta/2)=\sqrt{\frac{N-M}{N}}$$

下归纳证明，算子 G 作用 k 次的量子态为

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

(1) 当 $k=0$ 时，$|\psi_0\rangle=cos(\frac{\theta}{2})|\alpha\rangle+sin(\frac{\theta}{2})|\beta\rangle$ 显然成立

(2) 假设 k 时成立，则 $k=k+1$ 时

$$\begin{aligned}|\psi_{k+1}\rangle&=G|\psi_k\rangle\\&=DO(cos(\frac{2k+1}{2}\theta)|\alpha\rangle+sin(\frac{2k+1}{2}\theta)|\beta\rangle)\\&=D(cos(\frac{2k+1}{2}\theta)|\alpha\rangle-sin(\frac{2k+1}{2}\theta)|\beta\rangle)\end{aligned}$$

对 $\left|\psi_0^\perp\right\rangle = sin(\frac{\theta}{2})\left|\alpha\right\rangle - cos(\frac{\theta}{2})\left|\beta\right\rangle$, 有

$$\left|\alpha\right\rangle = cos(\frac{\theta}{2})\left|\psi_0\right\rangle + sin(\frac{\theta}{2})\left|\psi_0^\perp\right\rangle$$
$$\left|\beta\right\rangle = sin(\frac{\theta}{2})\left|\psi_0\right\rangle - cos(\frac{\theta}{2})\left|\psi_0^\perp\right\rangle$$

由 $D = 2\left|\psi_0\right\rangle\left\langle\psi_0\right| - I$,

$$D\left|\psi_0\right\rangle = 2\left|\psi_0\right\rangle\left\langle\psi_0|\psi_0\right\rangle - I\left|\psi_0\right\rangle = \left|\psi_0\right\rangle$$
$$D\left|\psi_0^\perp\right\rangle = 2\left|\psi_0\right\rangle\left\langle\psi_0\middle|\psi_0^\perp\right\rangle - I\left|\psi_0^\perp\right\rangle = -\left|\psi_0^\perp\right\rangle$$

$$\begin{aligned}
D\left|\alpha\right\rangle &= cos(\frac{\theta}{2})\left|\psi_0\right\rangle - sin(\frac{\theta}{2})\left|\psi_0^\perp\right\rangle \\
&= cos(\frac{\theta}{2})(cos(\frac{\theta}{2})\left|\alpha\right\rangle + sin(\frac{\theta}{2})\left|\beta\right\rangle) \\
&- sin(\frac{\theta}{2})(sin(\frac{\theta}{2})\left|\alpha\right\rangle - cos(\frac{\theta}{2})\left|\beta\right\rangle) \\
&= cos\theta\left|\alpha\right\rangle + sin\theta\left|\beta\right\rangle \\
D\left|\beta\right\rangle &= sin\theta\left|\alpha\right\rangle - cos\theta\left|\beta\right\rangle
\end{aligned}$$

于是

$$\begin{aligned}
\left|\psi_{k+1}\right\rangle &= D(cos(\frac{2k+1}{2}\theta)\left|\alpha\right\rangle - sin(\frac{2k+1}{2}\theta)\left|\beta\right\rangle) \\
&= (cos(\frac{2k+1}{2}\theta)cos\theta - sin(\frac{2k+1}{2}\theta)sin\theta)\left|\alpha\right\rangle \\
&+ (cos(\frac{2k+1}{2}\theta)sin\theta + sin(\frac{2k+1}{2}\theta)cos\theta)\left|\beta\right\rangle \\
&= cos(\frac{2k+3}{2}\theta)\left|\alpha\right\rangle + sin(\frac{2k+3}{2}\theta)\left|\beta\right\rangle
\end{aligned}$$

证毕。

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

证明:Grover 算法中,M 是待检验的解个数,N 是可行解个数,$\left|\psi\right\rangle = \sqrt{\frac{N-M}{N}}\left|\alpha\right\rangle + \sqrt{\frac{M}{N}}\left|\beta\right\rangle$
由 $\left|\alpha\right\rangle \perp \left|\beta\right\rangle, \left|\alpha\right\rangle\left\langle\beta\right| = -\left|\beta\right\rangle\left\langle\alpha\right|, \left|\alpha\right\rangle\left\langle\alpha\right| = -\left|\beta\right\rangle\left\langle\beta\right|$
$G = 2\left|\psi\right\rangle\left\langle\psi\right| - I = (2\frac{N-M}{N}\left|\alpha\right\rangle\left\langle\alpha\right| - 1) + (2\sqrt{\frac{M(N-M)}{N^2}}\left|\alpha\right\rangle\left\langle\beta\right|) + (2\sqrt{\frac{M(N-M)}{N^2}}\left|\beta\right\rangle\left\langle\alpha\right|) + (2\frac{M}{N}\left|\beta\right\rangle\left\langle\beta\right| - 1) = \begin{bmatrix} 2\frac{N-M}{N} - 1 & -2\sqrt{\frac{M(N-M)}{N^2}} \\ 2\sqrt{\frac{M(N-M)}{N^2}} & -(2\frac{M}{N} - 1) \end{bmatrix} = \begin{bmatrix} 1-2\gamma & -2\sqrt{\gamma-\gamma^2} \\ 2\sqrt{\gamma-\gamma^2} & 1-2\gamma \end{bmatrix}$
另证：利用题 2

$$G\left|\alpha\right\rangle = D\left|\alpha\right\rangle = cos\theta\left|\alpha\right\rangle + sin\theta\left|\beta\right\rangle$$
$$G\left|\beta\right\rangle = -D\left|\beta\right\rangle = -sin\theta\left|\alpha\right\rangle + cos\theta\left|\beta\right\rangle$$

而 $\gamma = M/N, cos(\frac{\theta}{2}) = \sqrt{\frac{N-M}{N}} = \sqrt{1-\gamma}, sin(\frac{\theta}{2}) = \sqrt{\gamma}$
易知 $cos\theta = 1-2\gamma, sin\theta = 2\sqrt{\gamma-\gamma^2}$
从而 G 对应的矩阵为

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

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：RSA 的过程如下：
(1). 获得大质数 p_1, p_2
(2).$n = p_1p_2, \varphi(n) = (p_1-1)(p_2-1)$
(3).Find $e, s.t. gcd(e, \varphi(n)) = 1$
(4).Find $d, s.t. ed \equiv 1(mod\varphi(n))$
加密 $C = a^e(modn)$, 下证明文 $a = C^d(modn)$
$C^d(modn) \equiv a^{ed}(modn) \overset{(4)}{\equiv} a^{k\varphi(n)+1}(modn)$
当 $gcd(a,n) = 1$ 时，由欧拉函数的性质 $a^{\varphi(n)} \equiv 1(modn), \therefore C^d(modn) \equiv a$
当 $gcd(a,n) \neq 1$ 时，因为 $0 < a < n$，且 p_1, p_2 互质，不失一般性，设 a 是 p_1 的倍数，则 a 不是 p_2 的倍数
则 $a^{ed} \equiv 0(modp_1)$, 这等价于 $a^{ed} \equiv a(modp_1)$(a 是 p_1 的倍数)
由费马小定理，$a^{p_2-1} \equiv 1(modp_2)$
$\therefore a^{\varphi(n)} \equiv a^{(p_1-1)(p_2-1)} \equiv 1^{p_1-1} \equiv 1(modp_2)$
$\therefore a^{ed} = a^{k\varphi(n)+1} \equiv a(modp_2)$
$\because a^{ed} \equiv a(modp_1), a^{ed} \equiv a(modp_2)$
$\therefore$ 由中国剩余定理 $a^{ed} \equiv a(modp_1p_2) = a(modn)$
即 $a = C^d(modn)$