量子计算理论基础与软件系统

理论作业二 量子测量与量子算法

redacted

理论作业二 量子测量与量子算法

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。

   - H: 进行谱分解得到 $H = \sum_{i=1}^{2} \lambda_i \, |e_i\rangle\langle e_i|$

     $\lambda_1 = 1, |e_1\rangle = \frac{|0\rangle + \left(\sqrt{2}-1\right)|1\rangle}{\sqrt{4-2\sqrt{2}}}$

     $\lambda_2 = -1, |e_2\rangle = \frac{|0\rangle + \left(-\sqrt{2}-1\right)|1\rangle}{\sqrt{4+2\sqrt{2}}}$

     因此使用酉算子 H 测量 $|1\rangle$ 的结果为 $|\varphi_1\rangle = |e_1\rangle$ 的概率为 $P(\varphi_1) = \langle 1|e_1\rangle\langle e_1|1\rangle = \frac{3-2\sqrt{2}}{4-2\sqrt{2}}$；为 $|\varphi_2\rangle$ 的概率为 $P(\varphi_2) = \langle 1|e_2\rangle\langle e_2|1\rangle = \frac{3+2\sqrt{2}}{4+2\sqrt{2}}$。

   - X: 本征值 $\lambda = \pm 1$，本征向量 $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

     得到 $|+\rangle$ 概率为 $p_1 = |\langle 1|+\rangle|^2 = \frac{1}{2}$，得到 $|-\rangle$ 概率为 $p_2 = |\langle 1|-\rangle|^2 = \frac{1}{2}$

   - $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$: 实本征值 $\lambda = 1$，对应本征态 $|0\rangle$；虚本征值 $\lambda = i$，对应本征态 $|1\rangle$。

     得到 $|0\rangle$ 概率为 $p_1 = |\langle 1|0\rangle|^2 = 0$，得到 $|1\rangle$ 概率为 $p_2 = |\langle 1|1\rangle|^2 = 1$

   - $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$: 实本征值 $\lambda = 1$，对应本征态 $|0\rangle$；虚本征值 $\lambda = e^{i\frac{\pi}{4}}$，对应本征态 $|1\rangle$。

     得到 $|0\rangle$ 概率为 $p_1 = |\langle 1|0\rangle|^2 = 0$，得到 $|1\rangle$ 概率为 $p_2 = |\langle 1|1\rangle|^2 = 1$

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。

   - 证明：记 Oracle 搜索的目标基矢态组成的等权叠加态为 $|\beta\rangle$，与其正交的非目标基矢态组成的等权叠加态为 $|\alpha\rangle$。算法制备初始量子态为 $|\psi_0\rangle = \cos\left(\frac{\theta}{2}\right)|\alpha\rangle + \sin\left(\frac{\theta}{2}\right)|\beta\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$，其中 $\sin\left(\frac{\theta}{2}\right) = \sqrt{\frac{M}{N}}, \cos\left(\frac{\theta}{2}\right) = \sqrt{\frac{N-M}{N}}$，$M$ 为目标态个数，N 为总态数。
   - 由 Grover 算法，算子 $G = DO$，其中 O 为 Oracle 算子，$D = 2\,|\psi_0\rangle\langle\psi_0| - I$，试证明 G 作用 k 次后的量子态为 $|\psi_k\rangle = \cos\left((2k+1)\frac{\theta}{2}\right)|\alpha\rangle + \sin\left((2k+1)\frac{\theta}{2}\right)|\beta\rangle$。
     - $k = 0$ 时，直接成立。
     - 由归纳假设有 $|\psi_{k+1}\rangle = G\,|\psi_k\rangle = DO\,|\psi_k\rangle = D\left(\cos\left((2k+1)\frac{\theta}{2}\right)|\alpha\rangle - \sin\left((2k+1)\frac{\theta}{2}\right)|\beta\rangle\right)$
     - 定义 $|\psi_0^\perp\rangle = \sin\left(\frac{\theta}{2}\right)|\alpha\rangle - \cos\left(\frac{\theta}{2}\right)|\beta\rangle$，则 $|\alpha\rangle = \cos\left(\frac{\theta}{2}\right)|\psi_0\rangle + \sin\left(\frac{\theta}{2}\right)|\psi_0^\perp\rangle$，$|\beta\rangle = \sin\left(\frac{\theta}{2}\right)|\psi_0\rangle - \cos\left(\frac{\theta}{2}\right)|\psi_0^\perp\rangle$
     - 易得，$D\,|\psi_0\rangle = |\psi_0\rangle, D\,|\psi_0^\perp\rangle = -|\psi_0^\perp\rangle$，那么 $D\,|\alpha\rangle = \cos\left(\frac{\theta}{2}\right)|\psi_0\rangle - \sin\left(\frac{\theta}{2}\right)|\psi_0^\perp\rangle = \cos(\theta)\,|\alpha\rangle + \sin(\theta)\,|\beta\rangle$，$D\,|\beta\rangle = \sin\left(\frac{\theta}{2}\right)|\psi_0\rangle + \cos\left(\frac{\theta}{2}\right)|\psi_0^\perp\rangle = \sin(\theta)\,|\alpha\rangle - \cos(\theta)\,|\beta\rangle$
     - 代入归纳式，即得 $|\psi_{k+1}\rangle = \cos\left((2(k+1)+1)\frac{\theta}{2}\right)|\alpha\rangle + \sin\left((2(k+1)+1)\frac{\theta}{2}\right)|\beta\rangle$，归纳成立。
   - 那么，每次作用算子 G 时，量子态均旋转角度 θ。

3. 根据 Grover 算法中 M、N 的定义，令 $\gamma = \frac{M}{N}$，证明在 $|\alpha\rangle$、$|\beta\rangle$ 基下，Grover 算法中的算子 G 可以写为 $\begin{bmatrix} 1-2\gamma & -2\sqrt{\gamma-\gamma^2} \\ 2\sqrt{\gamma-\gamma^2} & 1-2\gamma \end{bmatrix}$。
   - 证明：由上题可知，$G|\alpha\rangle = \cos(\theta)|\alpha\rangle + \sin(\theta)|\beta\rangle, G|\beta\rangle = -\sin(\theta)|\alpha\rangle + \cos(\theta)|\beta\rangle$，其中 $\sin\left(\frac{\theta}{2}\right) = \sqrt{\frac{M}{N}}, \cos\left(\frac{\theta}{2}\right) = \sqrt{\frac{N-M}{N}}$，那么 $\sin(\theta) = 2\sin\left(\frac{\theta}{2}\right)\cos\left(\frac{\theta}{2}\right) = 2\sqrt{\gamma-\gamma^2}, \cos(\theta) = \cos^2\left(\frac{\theta}{2}\right) - \sin^2\left(\frac{\theta}{2}\right) = 1-2\gamma$。
   - 代入得到 $G|\alpha\rangle = (1-2\gamma)|\alpha\rangle + 2\sqrt{\gamma-\gamma^2}|\beta\rangle, G|\beta\rangle = -2\sqrt{\gamma-\gamma^2}|\alpha\rangle + (1-2\gamma)|\beta\rangle$，即在 $|\alpha\rangle$、$|\beta\rangle$ 基下，Grover 算法中的算子 G 可以写为 $\begin{bmatrix} 1-2\gamma & -2\sqrt{\gamma-\gamma^2} \\ 2\sqrt{\gamma-\gamma^2} & 1-2\gamma \end{bmatrix}$。

- Bonus: 给出 RSA 算法加密、解密过程的证明，即证明明文为 $a \equiv C^d \bmod n$。
  - 加密方通过 $C = a^e \bmod n$ 将明文 a 加密为密文 C。取 e 模 $\varphi(n)$ 的乘法逆元d，使得 $ed = 1 \bmod \varphi(n)$。取大素数 p、q，计算 $n = pq$，并将 (e, n) 作为公钥发布，将 d 作为私钥保密。
  - 命 $ed = k\varphi(n) + 1$，若 $\gcd(a, n) = 1$，由欧拉定理，有 $a^{\varphi(n)} = 1 \bmod n$，则 $C^d = a^{ed} \bmod n = a^{k\varphi(n)+1} \bmod n = a \bmod n$，即明文 $a \equiv C^d \bmod n$
  - 若 $\gcd(a, n) = \gcd(a, pq) \neq 1$，则 $\gcd(a, p) = p$ 或 $\gcd(a, q) = q$。不妨设 $\gcd(a, p) = p$，则 $a \equiv 0 \bmod p$，那么 $\gcd(a, q) = 1$。由欧拉定理，有 $a^{\varphi(q)} \equiv 1 \bmod q$，那么 $a^{\varphi(p)\varphi(q)} \equiv 1 \bmod q$
    - 命 $a^{\varphi(p)\varphi(q)} = mq + 1$，由于 $\varphi(n) = \varphi(p)\varphi(q)$ 那么 $C^d = a^{ed} \bmod n = a^{k\varphi(n)+1} \bmod n = a^{k\varphi(p)\varphi(q)+1} \bmod n = (mq+1)a \bmod n = a \bmod n$，即明文 $a \equiv C^d \bmod n$