1. Implementing the Square root of a unitary

(a) $V = P_0 + iP_1$

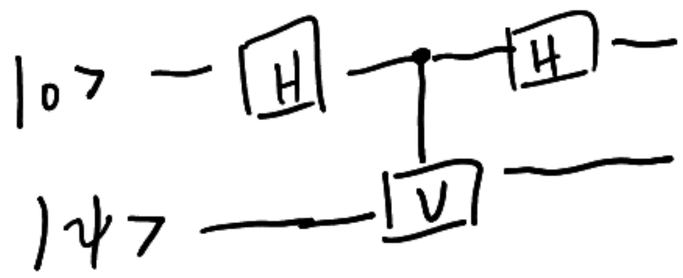
$V^2 = (P_0+iP_1)(P_0+iP_1) = P_0^2 + iP_1P_0 + iP_0P_1 - P_1^2$

Let $V = V_1 \perp V_{-1}$, where V_1 is the $+1$ eigenspace and V_{-1} is the -1 eigenspace

Then $V|\psi\rangle = U(P_0|\psi\rangle + P_1|\psi\rangle) = P_0|\psi\rangle - P_1|\psi\rangle$

$V|\psi\rangle = P_0^2|\psi\rangle + iP_1P_0|\psi\rangle + iP_0P_1|\psi\rangle - P_1^2|\psi\rangle = P_0|\psi\rangle - P_1|\psi\rangle$ #

(b). 使用 Hadamard test:

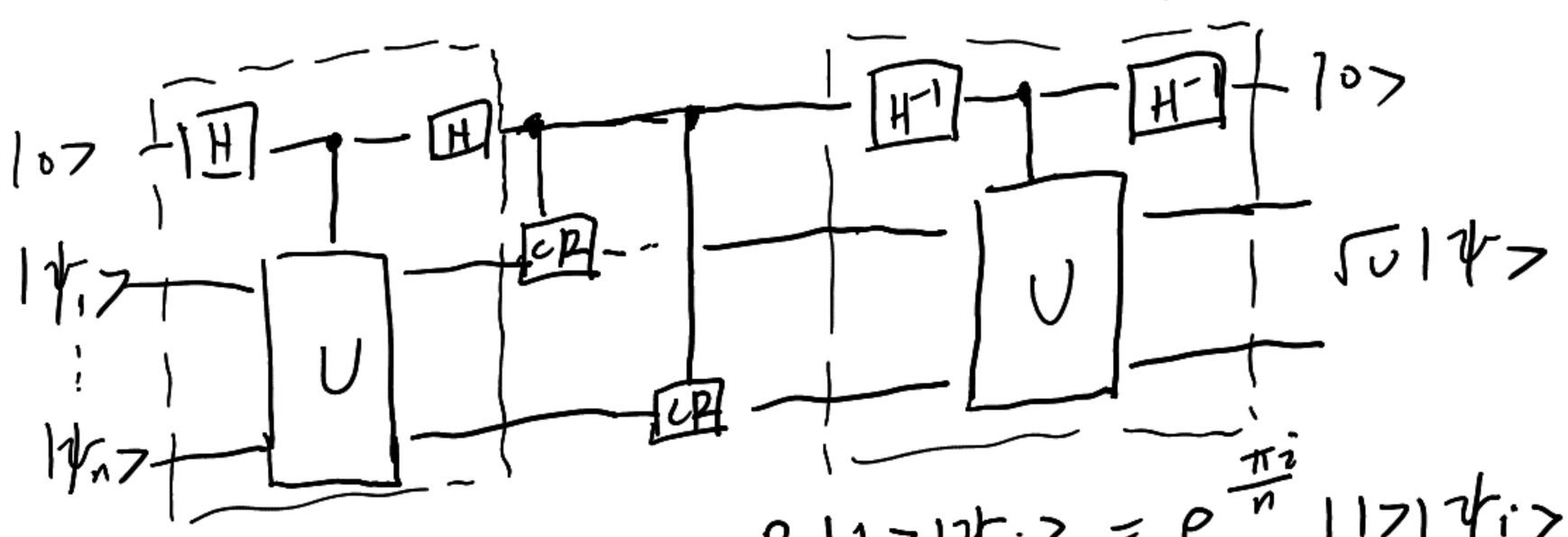


$|0\rangle|\psi\rangle \xrightarrow{(H\otimes I)} \xrightarrow{\text{Controled-}V} \xrightarrow{H\otimes I} \left(\frac{1+e^{i\theta}}{2}|0\rangle + \frac{1-e^{i\theta}}{2}|1\rangle\right)|\psi\rangle$

其中 $V|\psi\rangle = e^{i\theta}|\psi\rangle$ $\theta=0$ 时, $V|\psi\rangle = |\psi\rangle$, 得到 $|0\rangle|\psi\rangle$

$\theta=\pi$ 时, $V|\psi\rangle = -|\psi\rangle$, 得到 $|1\rangle|\psi\rangle$

(c)



其中 $cR|0\rangle|\psi_i\rangle = |0\rangle|\psi_i\rangle$, $cR|1\rangle|\psi_i\rangle = e^{\frac{\pi i}{n}}|1\rangle|\psi_i\rangle$

$|0\rangle|\psi\rangle = |0\rangle P_0|\psi\rangle + |0\rangle P_1|\psi\rangle \xrightarrow{H\otimes I} \xrightarrow{\text{Controled-}U} \xrightarrow{H\otimes I} |0\rangle P_0|\psi\rangle + |1\rangle P_1|\psi\rangle$

$\xrightarrow{cR^{\otimes n}} |0\rangle P_0|\psi\rangle + i|1\rangle P_1|\psi\rangle \xrightarrow{H^{-1}\otimes I} \xrightarrow{\text{Controled-}V} \xrightarrow{H^{-1}\otimes I} |0\rangle P_0|\psi\rangle + i|0\rangle P_1|\psi\rangle$

$= |0\rangle(P_0+iP_1)|\psi\rangle$ 由(a)即证 #

(2个虚线 box 互为逆算子, 因为 $U^2 = I$, $U^{-1} = U$)

2. Factoring 21

(a) $2^1 \equiv 2 \bmod 21$ $2^2 \equiv 4 \bmod 21$ $2^3 \equiv 8 \bmod 21$ $2^4 \equiv 16 \bmod 21$ $2^5 \equiv 11 \bmod 21$

$2^6 \equiv 1 \bmod 21 \Rightarrow \mathrm{Ord}_{21}(2) = 6.$

(b) 根据 Shor 算法，从 0 ~ 5 随机选出 k，输出 $\frac{k}{r} = \frac{k}{6}$ 在 n 精度相位估计结果

而 $P_r(k,y) = \frac{1}{2^{2n}} \frac{\sin^2\left(\left(\frac{k}{6} - \frac{y}{2^n}\right)2^n\pi\right)}{\sin^2\left(\left(\frac{k}{6} - \frac{y}{2^n}\right)\pi\right)}$，$k = 1, 2, 4, 5$

$P_r(0,y) = \begin{cases} 1 & y=0 \\ 0 & y\neq 0 \end{cases}$ $P_r(3,y) = \begin{cases} 1 & y=32 \\ 0 & y\neq 32 \end{cases}$

对 $t = 0, 1, \cdots 2^n - 1$

$$P_r(t) = \frac{1}{6}\left(\sum_{k=1,2,4,5} \frac{1}{2^{2n}} \frac{\sin^2\left(\left(\frac{k}{6} - \frac{y}{2^n}\right)2^n\pi\right)}{\sin^2\left(\left(\frac{k}{6} - \frac{y}{2^n}\right)\pi\right)} + 1_{y=0} + 1_{y=32}\right)$$

(c) 见邮件中文件．（(b)代入 n=7 即可）

(d) $\gcd(21, a^{\frac{r}{2}} - 1) = \gcd(21, 7) = 7$

$\gcd(21, a^{\frac{r}{2}} + 1) = \gcd(21, 9) = 3$

这确定 21 (所有) 2个素因子．因此求出 r 即可求出 21 所有素因子

(e) (a'): $\mathrm{Ord}_{21}(5) = 6$

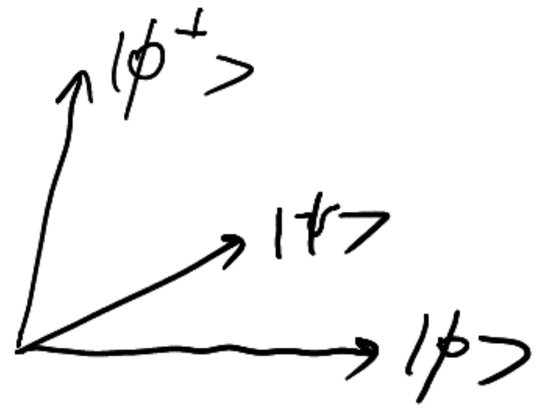
(b')(c'): 由于仅与 r, n 有关，故结果不变

(d'): $\gcd(21, a^{\frac{r}{2}} - 1) = 1$

$\gcd(21, a^{\frac{r}{2}} + 1) = 21$ 与 21 质因子不同．得不出结果

3. Searching for a quantum state

(a) $|\phi^\perp\rangle = \dfrac{e^{i\lambda}|\psi\rangle - \sin\theta|\phi\rangle}{\cos\theta}$



$\frac{2}{128} \approx \frac{5}{6}$

$|\psi\rangle = e^{i\lambda}\cos\theta|\phi^\perp\rangle + e^{i\lambda}\sin\theta|\phi\rangle$

(b) $U_\phi|\phi\rangle = -|\phi\rangle \quad U_\phi|\phi^\perp\rangle = |\phi^\perp\rangle$

起至 span$\{|\phi\rangle, |\phi^\perp\rangle\}$ 为 U_ϕ 矩阵 $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$

$V|\phi\rangle = 2|\psi\rangle\langle\psi|\phi\rangle - |\phi\rangle = 2e^{i\lambda}\sin\theta|\psi\rangle - |\phi\rangle = 2\sin^2\theta|\phi\rangle + \sin 2\theta|\phi^\perp\rangle - |\phi\rangle = -\cos 2\theta|\phi\rangle + \sin 2\theta|\phi^\perp\rangle$

$V|\phi^\perp\rangle = 2|\psi\rangle\langle\psi|\phi^\perp\rangle - |\phi^\perp\rangle = 2e^{-i\lambda}\cos\theta|\psi\rangle - |\phi^\perp\rangle$

$= 2\cos^2\theta|\phi^\perp\rangle + \sin 2\theta|\phi\rangle - |\phi^\perp\rangle = \sin 2\theta|\phi\rangle + \cos 2\theta|\phi^\perp\rangle$

V 矩阵 $\begin{pmatrix} -\cos 2\theta & \sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix}$

(c) $VU_\phi = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{pmatrix}$

用归纳法易知 $(VU_\phi)^k = \begin{pmatrix} \cos 2k\theta & \sin 2k\theta \\ -\sin 2k\theta & \cos 2k\theta \end{pmatrix}$

(d) 在 span$\{|\phi\rangle, |\phi^\perp\rangle\}$ 下计算, $(VU_\phi)^k|\psi\rangle = \begin{pmatrix} \cos 2k\theta & \sin 2k\theta \\ -\sin 2k\theta & \cos 2k\theta \end{pmatrix}\begin{pmatrix} e^{i\lambda}\sin\theta \\ e^{i\lambda}\cos\theta \end{pmatrix}$

$= e^{i\lambda}\begin{pmatrix} \sin(2k+1)\theta \\ \cos(2k+1)\theta \end{pmatrix}$

$\langle\phi|(VU_\phi)^k|\psi\rangle = (1 \quad 0)\, e^{i\lambda}\begin{pmatrix} \sin(2k+1)\theta \\ \cos(2k+1)\theta \end{pmatrix} = e^{i\lambda}\sin(2k+1)\theta$

(e) $\langle\phi|\psi\rangle = e^{i\lambda}\sin\theta \quad |\langle\phi|\psi\rangle|$ small $\Rightarrow \theta$ small

需要让 $|\langle\phi|(VU_\phi)^k|\psi\rangle|^2$ 尽量大, 即 $\sin^2(2k+1)\theta$ 大, 让 $(2k+1)\theta \approx \frac{\pi}{2}$

$k \approx \frac{\pi}{4\theta} - \frac{1}{2} \approx \frac{\pi}{4\sin\theta} - \frac{1}{2} = \frac{\pi}{4|\langle\phi|\psi\rangle|} - \frac{1}{2}$ #

4. The collision problem

(a) $f(1)\cdots f(k)$ 需要 k 次 query 考虑最坏情况

之后找过程可形式化：

记 $H(x)=1$ iff $\exists x_0\in\{1,\cdots k\}$, $H(x)=H(x_0)$ 且 $x\notin\{1,\cdots k\}$

为求 $H(x)=1$ 的解

而 $\#\{x\in\{1,\cdots n\}\mid H(x)=1\}=k$

故此步用 $O(\sqrt{\frac{n}{k}})+k=O(k+\sqrt{\frac{n}{k}})$ 次 query

总共用 $O(k+\sqrt{\frac{n}{k}})$ 次query

(b) 由平均值不等式. $k+\sqrt{\frac{n}{k}}=k+\frac{1}{2}\sqrt{\frac{n}{k}}+\frac{1}{2}\sqrt{\frac{n}{k}}\geq 3\sqrt[3]{\frac{1}{4}n}$

取等当且仅当 $k=(\frac{1}{2})^{\frac{2}{3}}\sqrt[3]{n}=\Theta(\sqrt[3]{n})$

(c) 问题下界是 $\Omega(n^{\frac{1}{3}})$ 说明此个算法对 query 的次数是渐近意义下最好的 (因为此个算法就是 $\Omega(n^{\frac{1}{3}})$ 的)

与 Simon 问题的联系：

Simon 问题 $f:\{0,1\}^n\to\{0,1\}^n$

$f(x)=f(y)\Leftrightarrow x=y$ or $x\oplus y=s$, $s\neq 0^n$

是一个条件强得多的 2-to-1 function

故 query 次数也可得为：只需 $\Omega(\log n)$ 次

但 Simon 问题条件太强，其首在理论上分开 BPP 和 BQP

而 Collison 问题对 f 假设弱得多，有更的实用价值

5. Spectrum of a product of reflections

(a) $A: \mathbb{C}^a \to \mathbb{C}^{n\times a}$ $\quad B: \mathbb{C}^b \to \mathbb{C}^{n\times b}$

$A = \sum_{j=1}^{a} |\psi_j\rangle\langle j|$ $\quad B = \sum_{j=1}^{b} |\phi_j\rangle\langle j|$

$A^\dagger A = \sum_{j=1}^{a}\sum_{k=1}^{a} |j\rangle\langle\psi_j|\psi_k\rangle\langle k| = \sum_{j=1}^{a} |j\rangle\langle j| = I_a$

$AA^\dagger = \sum_{j=1}^{a}\sum_{k=1}^{a} |\psi_j\rangle\langle j|k\rangle\langle\psi_k| = \sum_{j=1}^{a} |\psi_j\rangle\langle\psi_j| = \Pi$

同理 $B^\dagger B = I_b$ $\quad BB^\dagger = \sum$

由SVD, $D = \sum_{i=1}^{r} \sigma_i |\alpha_\sigma\rangle\langle\beta_\sigma|$, $D|\beta\rangle = \sigma|\alpha\rangle$ $\quad D^\dagger|\alpha\rangle = \sigma|\beta\rangle$

$A^\dagger B = \sum_{j=1}^{a}\sum_{k=1}^{b} |j\rangle\langle\psi_j|\phi_k\rangle\langle k| = D$

$B^\dagger A = \sum_{j=1}^{b}\sum_{k=1}^{a} |j\rangle\langle\phi_j|\psi_k\rangle\langle k| = D^\dagger$

$U|A\psi\rangle = (2AA^\dagger - I_n)(2BB^\dagger - I_n)A|\psi\rangle = (2AA^\dagger - I_n)(2BB^\dagger A|\psi\rangle - A|\psi\rangle)$

$= 4AA^\dagger BB^\dagger A|\psi\rangle - 2BB^\dagger A|\psi\rangle - A|\psi\rangle$

$= 4\sigma^2 A|\psi\rangle - 2BB^\dagger A|\psi\rangle - A|\psi\rangle$

$= (4\sigma^2 - 1)A|\psi\rangle - 2BD^\dagger|\psi\rangle = (4\sigma^2-1)A|\psi\rangle - 2\sigma B|\beta\rangle$

$U|B\beta\rangle = (2AA^\dagger - I_n)(2BB^\dagger - I_n)B|\beta\rangle = (2AA^\dagger - I_n)B|\beta\rangle$

$= (2AA^\dagger B - B)|\beta\rangle = 2AD|\beta\rangle - B|\beta\rangle$

$= 2\sigma A|\alpha\rangle - B|\beta\rangle$ 故 U 不变

(b) $U|_{\mathrm{span}\langle A|\psi\rangle, B|\beta\rangle\rangle}$ 写成矩阵为 $\begin{pmatrix} 4\sigma^2-1 & -2\sigma \\ 2\sigma & -1 \end{pmatrix} = (v_1\ v_2)\begin{pmatrix} \lambda_1 & \\ & \lambda_2 \end{pmatrix}\begin{pmatrix} v_1^T \\ v_2^T \end{pmatrix}$

特征值 $\lambda_{1,2} = 2\sigma^2 - 1 \pm 2\sigma\sqrt{1-\sigma^2}\,i$

当 $\sigma \neq 1$ 得到两个特征值，$\sigma = 1$ 得到一个特征值

特征向量 $v_{1,2} = (\sigma \mp \sqrt{1-\sigma^2}\,i, 1)^T$

(c) 见(b)

(d) 设 D 的 r 个 singular value 有 t 个为 1

对称到 $t+2(r-t)$ 个特征向量

记 $V_i = \mathrm{span}\langle A|\alpha_i\rangle, B|\beta_i\rangle\rangle$ V_i 为 U 一不变子空间

$\mathbb{C}^n = \bigoplus_{i=1}^{r} V_i + V_0$, V_0 为 $\bigoplus_{i=1}^{r} V_i$ 的正交补空间

记 $C(A)$, $C(B)$ 为 $A\cdot B$ 列空间

我们有在 $C(A)^{\perp} \cap C(B)^{\perp}$ 上 $U=I$

在 $V_{>2} = C(A) \cap C^{\perp}(B)$ 及 $C^{\perp}(A) \cap C(B)$ 上 $U=-I$

直接给出了其余特征值与特征向量

(见 Quantum speed-up of Markov Chain based algorithms, M. Szegedy, in FCS 2004 中 Theorem 1 (specterd Lemma)) #