Problem 1 (r is power of 2)

(a)

- if exist $r \in \mathbb{Z}_{2^t}$ s.t. $f(r) = 5^r \bmod 39 \equiv 1$;

then, $\begin{cases} f(x-r) = 5^x \cdot 5^{-r} \bmod 39 \equiv 5^x \bmod 39 = f(x) \\ f(x+r) = 5^x \cdot 5^r \bmod 39 \equiv 5^x \bmod 39 = f(x) \end{cases}$ $\Rightarrow f(x)$ is periodic.

- Furthermore, $f(4) = 5^4 = 625 \equiv 1 \bmod 39$ (and $f(1), f(2), f(3) \not\equiv 1$), $\underline{r = 4.}$

(b)

$x \to f(x)$: $0, 4, \dots, 2044 \to 1$
$1, 5, \dots, 2045 \to 5$
$2, 6, \dots, 2046 \to 25$
$3, 7, \dots, 2047 \to 8$

$\Rightarrow \underline{f(x) = \frac{1}{2}(|1\rangle + |5\rangle + |25\rangle + |8\rangle)}$ #

(c)

if $z = 8$, $|\alpha\rangle = \frac{1}{\sqrt{2^9}}(|3\rangle + |7\rangle + |11\rangle + \dots + |2047\rangle)$

$= \underline{\frac{1}{\sqrt{2^9}} \sum_{j=0}^{2^9-1} |3 + j \cdot 4\rangle}$, $r = 4$.

(d)

$QFT_{2^{11}} : |x\rangle \to \frac{1}{\sqrt{N}} \sum_{y \in \mathbb{Z}_N} w^{xy} |y\rangle$, $N \triangleq 2^{11}$

$\frac{1}{\sqrt{2^9}} \sum_{j=0}^{2^9-1} |3+4j\rangle \to \frac{1}{\sqrt{2^9}} \frac{1}{\sqrt{N}} \sum_{j=0}^{2^9-1} \sum_{y \in \mathbb{Z}_N} w^{(3+4j)y} |y\rangle$

$= \frac{1 \cdot 1}{\sqrt{2^9} \cdot \sqrt{N}} \sum_{y \in \mathbb{Z}_N} w^{3y} \left(\sum_{j=0}^{2^9-1} w^{4jy} \right) |y\rangle$

$= \frac{1}{\sqrt{2^9}\sqrt{N}} \sum_{l=0}^{3} w^{3 \cdot 2^9 l} \cdot 2^9 \cdot |2^9 \cdot l\rangle$

$= \frac{1}{2} \sum_{l=0}^{3} w^{3 \cdot 2^9 l} |2^9 l\rangle \to$ measure result : $\begin{cases} 0 : 25\% \\ 2^9 : 25\% \\ 2^{10} : 25\% \\ 3 \cdot 2^9 : 25\% \end{cases}$

(e) $\frac{2^9 \cdot l}{2^{11}} = \frac{l}{4} \to$ $\boxed{50\%}$: if $l = 1, 3$, $\frac{l}{4}$ has denominator 4, $f(x) = f(x+4)$, $r = 4$

$\searrow$ 50% : if $l = 0, 2$, $\frac{l}{4}$ has denominator 1/2, $f(x) \neq f(x+1), f(x+2)$, failed.

(f) $5^4 - 1 = (5^2-1)(5^2+1) \bmod 39 \equiv 0$

$\because 5^2 + 1 \bmod 39 \neq 0$ $\therefore$ Shor's algo holds, $\gcd(5^2-1, 39) = 3$, $\underline{3 \cdot 13 = 39}$ #
$\gcd(5^2+1, 39) = 13$

Problem 2 (r is not power of 2.)

(a) $t=9,\ 2^t=512$

(b)

- $\frac{c}{N}=\frac{427}{512}=\frac{1}{1+\frac{85}{427}}=\frac{1}{1+\frac{1}{5+\frac{2}{85}}}=\frac{1}{1+\frac{1}{5+\frac{1}{42+\frac{1}{2}}}}=[1,5,42,2]$.

- Restriction: $\left|\frac{c}{N}-\frac{l}{r}\right|\le\frac{1}{2N^2}=\frac{1}{882}\rightarrow 0.83285\le\frac{l}{r}\le 0.83512$

$[1]=1$, ×××

$[1,5]=\frac{1}{1+\frac{1}{5}}=\frac{5}{6}=0.83333$, √√ $\Rightarrow \underline{\underline{r=6}}$

$[1,5,42]=\frac{1}{1+\frac{1}{5+\frac{1}{42}}}=\frac{47}{89}$, $r>N=21$, ×.

(c)

$$\begin{cases} f(x)=2^6=64 \bmod 21\equiv 1 \\ f(x+r)=f(x)=f(x-r)\rightarrow \text{periodic} \end{cases}$$

$\because f(1), f(2), f(3), f(4), f(5)\neq 1 \quad \therefore$ period is $\underline{r=6}$.

$2^6-1=(2^3+1)(2^3-1) \bmod 21=0$

$\because 2^3+1 \bmod 21\neq 0$

$\therefore$ Shor's algo holds, $\gcd(2^3+1,21)=3$, $\underline{3\cdot 7=21}$. #

$\gcd(2^3-1,21)=7$

Problem 3.

(a) let $y = \log_g(x)$, $g^y = x$ and $k = \log_g(c)$, $g^k = c$, then

$$f(a,b)=c \leftrightarrow g^a \cdot g^{-by} \equiv g^k \bmod p \leftrightarrow g^{a-(by+k)} \equiv 1 = g^{p-1} \bmod p \leftrightarrow a-(by+k) \equiv 0 \bmod p-1 \quad \#$$

(b)

$$\frac{1}{p-1}\sum_{a,b\in\mathbb{Z}_{p-1}} |a\rangle|b\rangle|f(a,b)\rangle \xrightarrow[C_0]{\text{measure result}} \frac{1}{\sqrt{p-1}}\sum_{b\in\mathbb{Z}_{p-1}} |by+k\rangle|b\rangle = \frac{1}{\sqrt{y}}\sum_{b\in\mathbb{Z}_m} |by+k\rangle|b\rangle. \quad \#$$

if d is min s.t. $x^d \equiv 1 \bmod p$
then $x^d = g^{dy} = 1 = g^{p-1} \bmod p$.
$y \mid p-1$, $m \triangleq \frac{p-1}{y}$

(c) $QFT_{p-1}: |x\rangle \to \frac{1}{\sqrt{p-1}}\sum_{u\in\mathbb{Z}_{p-1}} w^{xu}|u\rangle$.

$$|\psi\rangle \to \frac{1}{\sqrt{y}}\sum_{b\in\mathbb{Z}_m}\left(\frac{1}{\sqrt{p-1}}\sum_{u\in\mathbb{Z}_{p-1}} w^{(by+k)u}|u\rangle\right)\left(\frac{1}{\sqrt{p-1}}\sum_{v\in\mathbb{Z}_{p-1}} w^{bv}|v\rangle\right)$$

$$= \frac{1}{\sqrt{y}}\left(\frac{1}{\sqrt{p-1}}\sum_{u\in\mathbb{Z}_{p-1}} w^{ku}\left(\sum_{b\in\mathbb{Z}_m} w^{byu}\right)|u\rangle\right)\left(\frac{1}{\sqrt{p-1}}\sum_{v\in\mathbb{Z}_{p-1}}\left(\sum_{b\in\mathbb{Z}_m} w^{bv}\right)|v\rangle\right)$$

$$= \left(\frac{1}{\sqrt{y}}\sum_{\ell=0}^{y-1} w^{k\ell m}|\ell m\rangle\right)\left(|0\rangle\right)$$

$\xrightarrow{\text{measure result}}$ $(0, \ell m)$ with $\ell = 0, 1, \dots, y-1$; each probability $= \frac{1}{y} = \frac{m}{p-1}$

(d). we have: $\frac{\ell m}{p-1} = \frac{\ell}{y}$ ... obtain denominator y in $O(\log^3(p))$ time by Continued fraction algo.

- Choosing g, g must be co-prime to $p-1$

→ we must run $O(\log\log(p))$ times to achieve a constant level prob q ... [week 8 ppt, P38]

Given ε → For n repetition, successful prob $= (1-q)^n \geq (1-\varepsilon)$, take $n = \lceil \log_{1-q}(1-\varepsilon) \rceil$. #

This part need $O(\log\log(p) \cdot \lceil \log_{(1-q)}(1-\varepsilon) \rceil)$ times.

. QFT_{p-1} need $O(\text{poly}(\log p))$ times.

⇒ total time is $O(\text{poly}(\log p))$ times. #

Problem 4.

(a) PVM

- $\begin{cases} Pr(H_0 = |+_0\rangle) = \frac{1}{2} \\ Pr(H_1 = |+_1\rangle) = \frac{1}{2} \end{cases}$, let $\Pi_0 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\Pi_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ by unambiguous discrimination

- $\begin{cases} Pr(\text{outcome is } 0 \mid H_0 = |+_0\rangle) = \langle 0|\Pi_0|0\rangle \cdot \frac{1}{2} = \frac{1}{2}|a) \\ Pr(\text{outcome is } 1 \mid H_1 = |+_1\rangle) = \langle +|\Pi_1|+\rangle \cdot \frac{1}{2} = 0 \end{cases}$

- $4 \cdot P_S = a + 0 = a \leq 1 \Rightarrow P_S \leq \frac{1}{4}$

(b) POVM

- $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +| = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix} = \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix}$

- $\left.\begin{array}{l} Pr(\text{outcome } 0) = Tr(\rho\Pi_0) \\ Pr(\text{outcome } 1) = Tr(\rho\Pi_1) \\ Pr(\text{outcome } *) = Tr(\rho\Pi_*) \end{array}\right\} Tr(\rho\Pi_0) + Tr(\rho\Pi_1) + Tr(\rho\Pi_*) = Tr(\rho I) = 1.$

- Take $\Pi_* = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $\Pi_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\Pi_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$; $Pr(\text{outcome } *) = \frac{1}{4}$, $P_S = \frac{1 - \frac{1}{4}}{2} = \underline{\frac{3}{8}}$ #

(c) Since $P_S = \frac{1 - Tr(\rho\Pi_*)}{2}$ and $Tr(\rho\Pi_*) \geq 0$. When $\Pi_* = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $\underline{P_S \text{ has max value} = \frac{1}{2}}$ #

(d) Yes! In 4-dim, $\Pi_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}$, $\Pi_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix}$, $\Pi_* = I - \Pi_0 - \Pi_1$.

Then, $P_S = \frac{1}{4}(\langle 0|\Pi_0|0\rangle + \langle +|\Pi_1|+\rangle)$

$= \frac{1}{4}(1 + \frac{1}{2}) = \frac{1}{4} \cdot \frac{3}{2} = \frac{3}{8} > \frac{1}{4}$ #.

Problem 5.

(a). $Tr(I\sigma_x) = Tr(I\sigma_y) = Tr(I\sigma_z) = 0$

$Tr(\sigma_x\sigma_y) = Tr\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = 0$, $Tr(\sigma_x\sigma_z) = Tr\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = 0$, $Tr(\sigma_y\sigma_z) = Tr\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = 0$.

• $Tr(\rho\sigma_\lambda) = Tr\left(\frac{1}{2}r_\lambda\sigma_\lambda\cdot\sigma_\lambda\right) = \frac{2}{2^2}Tr(I) = r_\lambda$, $\lambda = x, y, z$. #

(b)

$$\rho = \frac{1}{2}\left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & r_x \\ r_x & 0 \end{pmatrix} + \begin{pmatrix} 0 & -ir_y \\ ir_y & 0 \end{pmatrix} + \begin{pmatrix} r_z & 0 \\ 0 & -r_z \end{pmatrix}\right] = \frac{1}{2}\begin{pmatrix} 1+r_z & r_x - ir_y \\ r_x + ir_y & 1-r_z \end{pmatrix}$$

4. $\det(\rho - \lambda I) = (1-2\lambda+r_z)(1-2\lambda-r_z) - (r_x+\lambda r_y)(r_x-\lambda r_y)$

$= (1-2\lambda)^2 - r_z^2 - r_x^2 - r_y^2 = (1-2\lambda)^2 - \|r\|^2 = 0 \Rightarrow \lambda = \frac{1 \pm \|r\|}{2}$

ρ is density operator $\leftrightarrow$ eigenvalue $\lambda_0, \lambda_1 \geq 0 \leftrightarrow \frac{1+\|r\|}{2}, \frac{1-\|r\|}{2} \geq 0 \leftrightarrow 1 \geq \|r\|$. #.

(c). $Tr(\rho\sigma) = \frac{1}{2}\left[Tr(I\sigma) + r_x Tr(\sigma_x\sigma) + r_y Tr(\sigma_y\sigma) + r_z Tr(\sigma_y\sigma)\right]$

$= \frac{1}{2}(1 + r_x s_x + r_y s_y + r_z s_z) = \frac{1}{2}(1 + \vec{r}\cdot\vec{s})$. #.

• ρ is orthogonal to $\sigma \leftrightarrow 0 = Tr(\rho\sigma) = \frac{1}{2}(1+\vec{r}\cdot\vec{s}) \leftrightarrow \vec{r}\cdot\vec{s} = -1$ ... 向量平行，反方向
球面上的兩端，組成線

(d) $P(\text{outcome is } 0) = Tr(\rho|\psi_0\rangle\langle\psi_0|) \overset{by(c)}{=\!=} \frac{1}{2}(1+\vec{r}\cdot\vec{r}_0)$

$P(\text{outcome is } 1) = Tr(\rho|\psi_1\rangle\langle\psi_1|) \overset{by(c)}{=\!=} \frac{1}{2}(1+\vec{r}\cdot\vec{r}_1)$. #

(e). $\sum_{a,b} \Pi_{(a,b)} = \frac{6+\sigma_x+\sigma_y+\sigma_z-\sigma_x-\sigma_y-\sigma_z}{6} = I$.

• $\Pi_{(a,b)}$ are positive semi-definite Hermitian matrices;

$Tr(\Pi_{(a,b)}) = \frac{1}{6}[2+(-1)^b\cdot 0] = \frac{1}{3}$

$\Pi_{(a,b)}\Pi_{(a,b)}^\dagger = \frac{I+(-1)^b\overline{\sigma a^T}}{6} = \frac{I+(-1)^b\sigma a}{6} = \Pi_{(a,b)}$. #

(f) $P_r(a,b) = Tr(\rho\Pi_{(a,b)}) = \frac{1}{2}\left[Tr(I\Pi_{(a,b)}) + r_x Tr(\sigma_x\Pi_{(a,b)}) + r_y Tr(\sigma_y\Pi_{(a,b)}) + r_z Tr(\sigma_z\Pi_{(a,b)})\right]$

$= \frac{1}{2}\left[\frac{2}{6} + r_a Tr\left(\sigma_a\cdot\frac{I+(-1)^b\sigma_a}{6}\right)\right]$

$= \frac{1}{2}\left[\frac{2}{6} + r_a Tr\left(\frac{\sigma_a+(-1)^b I}{6}\right)\right] = \frac{1}{2}\left[\frac{2}{6} + r_a\cdot 2\cdot(-1)^b\right] = \frac{1+(-1)^b r_a}{6}$

#

(g) Given each copy ρ, we can use $\Pi_{(a,0)}$ to get $\frac{1+r_a}{6} \triangleq V$, and $r_a = 6V-1$ to get r_a.
In this case, ρ is 2×2 matrix, has r_x, r_y, r_z; we need 3 copy to obtain $r = (r_x, r_y, r_z)$.
[If ρ is $n\times n$ matrix, we need n^2-1 copy $\leftrightarrow$ n^2-1 freedom #]