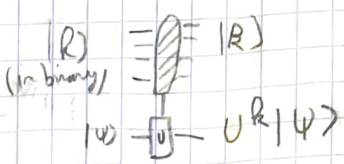
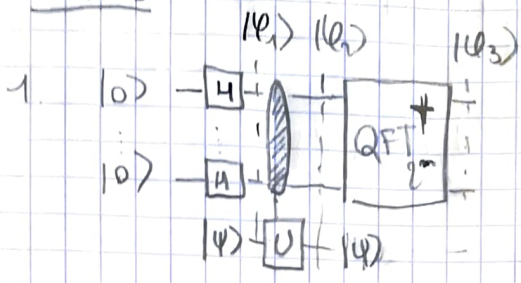
TD 5

1. HW 5:



1.



$$|\varphi_1\rangle = \sum_{k \in \{0,1\}^m \,(\text{ie } k \in [2^m])} \frac{|k\rangle}{\sqrt{2^m}} \otimes |\psi\rangle$$

$$|\varphi_2\rangle = \frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} \left(\frac{|k\rangle}{\sqrt{2^m}} \otimes e^{2i\pi k\theta} |\psi\rangle \right)$$

$$= \left(\frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} e^{2i\pi k\theta} |k\rangle \right) \otimes \underbrace{|\psi\rangle}_{\text{we can leave it alone.}}$$

Focus on m first qubits: $QFT_{2^m}^{\dagger} |k\rangle = \frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} e^{-2i\pi k j 2^{-m}} |j\rangle$

So $$|\varphi_3\rangle = \frac{1}{2^m} \sum_{j=0}^{2^m-1} \left(\sum_{k=0}^{2^m-1} e^{2i\pi k[\theta - j2^{-m}]} \right) |j\rangle .$$

2. $p_j = \mathbb{P}(\text{Outcome} = j) = \left| \sum_{k=0}^{2^m-1} e^{2i\pi k[\theta - j2^{-m}]} \right|^2 / 4^m$

$$= \left| \sum_{k=0}^{2^m-1} \left(e^{2i\pi(\theta - j2^{-m})} \right)^k \right|^2 / 4^m$$

⇒ This is the sum of a geometric series with $e^{2i\pi(\theta - j2^{-m})} \neq 1$ (since θ not of the form $\frac{j}{2^m}$)

So $$\boxed{p_j = \frac{1}{4^m} \left| \frac{1 - e^{2i\pi(\theta 2^m - j)}}{1 - e^{2i\pi(\theta - j2^{-m})}} \right|^2}$$

3. Suppose that j is a wrong answer, ie $|\theta - j2^{-m}| > 2^{-t-1}$ and $|\theta - j2^{-m}| > 1-2$

Then $P_j = \left(\frac{1}{2^m}\right)^2 \frac{|1-e^{2i\pi(\theta 2^m - j)}|^2}{|1-e^{2i\pi(\theta - j2^{-m})}|^2} \leq \left(\frac{1}{2^m}\right)^2 \frac{4}{|1-e^{i[2\pi(\theta-j2^{-m})]}|^2}$

↳ since $|1-e^{i\delta}| \leq 2$

Case ① $|\theta - j2^{-m}| \leq \frac{1}{2}$

Then $|2\pi(\theta - j2^{-m})| \leq \pi$. We can apply the claimed inequality:

$$\leq \left(\frac{1}{2^m}\right)^2 \frac{4}{\left(\frac{2}{\pi}|2\pi(\theta - j2^{-m})|\right)^2} \leq \left(\frac{1}{2^m}\right)^2 \frac{1}{4(2^{-t-1})^2} \quad \text{since } |\theta - j2^{-m}| > 2^{-t-1}$$

$$= 2^{2t-2m}$$

So $\mathbb{P}(\text{We get a wrong } j) \leq \underbrace{2^m}_{\text{all possible } j\text{'s}} \times \underbrace{2^{2t-2m}}_{\text{previous result}} = 2^{2t-m}$

So $\boxed{\mathbb{P}(\text{Correct answer}) \geq 1 - 2^{2t-m}}$

So for t fixed and $m \to +\infty$, $1 - 2^{2t-m} \to 1$ QED

Case ②: $|\theta - j2^{-m}| > \frac{1}{2}$

Case 2.1: $\theta - j2^{-m} > \frac{1}{2}$: Then take $j' = j - 2^m$.

Then $e^{2i\pi(\theta - j2^{-m})} = e^{2i\pi(\theta - j'2^{-m})}$ by 2π-periodicity of $e^{2i\pi(\cdot)}$

And $\theta - j'2^{-m} > \frac{1}{2} - 1 = -\frac{1}{2}$

and $\theta - j'2^{-m} = \theta - j2^{-m} - 1 \leq 1 - 1 = 0$

so $|\theta - j'2^{-m}| < \frac{1}{2}$: we can apply the ineq:

get $P_j \leq \left(\frac{1}{2^m}\right)^2 \frac{4}{\left(\frac{2}{\pi}|2\pi(\theta - j'2^{-m})|\right)^2} \leq \left(\frac{1}{2^m}\right)^2 \frac{1}{4(2^{-t-1})^2}$ since $|\theta - j'2^{-m}| > 2^{-t-1}$

Indeed $\frac{1}{2} < \theta - j2^{-m} < 1 - 2^{-t-1}$ so $-\frac{1}{2} < \theta - j'2^{-m} < -2^{-t-1}$

thus $|\theta - j'2^{-m}| > 2^{-t-1}$ & rest of proof identical

Case 2.2: Symmetrical with $j' := j + 2^m$ ■

II- 1. $x \in \{0,1,2,\dots \ell-1\}$

$x \in \mathbb{Z}_\ell^* \iff \exists\, y \in \{0,\dots,\ell-1\}$ s.t. $xy \equiv 1 \ [\ell]$

$\iff \exists\, y, k$ s.t $xy + k\ell = 1$

$\iff x \wedge \ell = 1$

So as ℓ is prime, $\mathbb{Z}_\ell^* = \{1,2,\dots,\ell-1\}$

2. By CRT, $\mathbb{Z}_N = \mathbb{Z}_p \times \mathbb{Z}_q$ as rings

$\Rightarrow \mathbb{Z}_N^* = \mathbb{Z}_p^* \times \mathbb{Z}_q^*$

$\Rightarrow |\mathbb{Z}_N^*| = |\mathbb{Z}_p^*| \cdot |\mathbb{Z}_q^*|$

$= (p-1)(q-1)$

3. $x \xleftarrow{\$} \mathbb{Z}_N$ $\quad \mathbb{P}(x \in \mathbb{Z}_N^*) = \dfrac{|\mathbb{Z}_N^*|}{|\mathbb{Z}_N|}$

$= \dfrac{(p-1)(q-1)}{pq} = 1 - \dfrac{p+q}{pq} + \dfrac{1}{pq}$

$\approx 1 - 2^{-\lambda/2}$

4. Let $w(x)$ the order of x

We have $(-x)^k = (-1)^k x^k$ so $(-x)^{w(x)} = (-1)^{w(x)}$

$\Rightarrow (-x)^{2w(x)} = 1$

$\Rightarrow w(-x) \mid 2 \cdot w(x)$ (1)

By the same argument, $w(x) \mid 2 \cdot w(-x)$ (2)

write (1) $\iff 2w(x) = v \cdot w(-x)$

(2) $\iff 2w(-x) = v \cdot w(x)$

We have $w(x)$ odd, so $2 \mid v$ $\quad v = 2v'$

$\Rightarrow w(-x) = v' w(x)$

(1) $\Rightarrow 2w(x) = v \cdot v' w(x)$

$\iff 2 = vv'$

If $v = 2$, then $2w(x) = 2w(-x)$

$\Leftrightarrow w(x) = w(-x)$

But $(-x)^{w(x)} = (-1)^{w(x)} = -1$

So it is impossible

Then $v' = 2 \Rightarrow w(-x) = 2w(x)$ □

It implies that $|\{x / w(x) \text{ odd}\}| < |\{x / w(x) \text{ even}\}|$

and hence

$$\mathbb{P}(w(x) \text{ even}) \geq 1/2$$ □

5. We have $x^r - 1 = k \cdot N$ for a certain k

$\Leftrightarrow (x^{r/2} - 1)(x^{r/2} + 1) = k \cdot N$

The condition on $x^{r/2} \pm 1$ impose that

$x^{r/2} - 1$ share a non-trivial factor with N (else: $x^{r/2} - 1 = kN$ and $x^{r/2} + 1 = 1$ - or $x^{r/2} - 1 = N$)

So return $\gcd(x^{r/2} - 1, N)$.

6. • Run Shor while obtaining odd order on random x
   • return $\gcd(x, N)$ or replay.

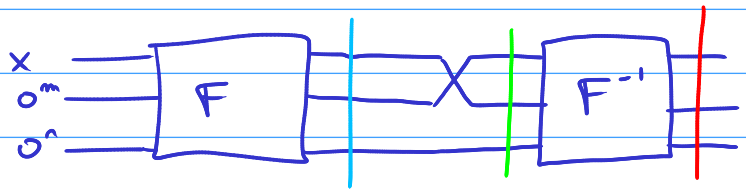
Expected run time: $O\left(\frac{1}{1-\varepsilon} \cdot 2\right)$ call to Shor

($\frac{1}{1-\varepsilon}$: proba of $x^{r/2} - 1$ bad; 2: proba of order odd)

$|F(x)\rangle|x \oplus F^{-1}(F(x))\rangle|0\rangle$
$= |F(x)\rangle|0^{n+m}\rangle$

III

1.



$|x\rangle|F(x)\rangle|0^n\rangle$

$|F(x)\rangle|x\rangle|0^n\rangle$

2. Previous question with $F_a(x) = ax$

$F_a^{-1}(x) = a^{-1}x$

3. Fast Exp(x, k, N)

If $k = 1$ return $x \bmod N$

$k = 0$ return 1

Else

if $2 \mid k$

return $Exp(x^2 \bmod N, k/2, N)$

else

return $x \cdot Exp(x^2 [N], (k-1)/2, N)$

4. Do Fast Exp with T_a gates on input x