CS 506: An Introduction to Quantum Computing

University of Illinois Chicago

(Class Note)

Student: Kazi Shahrukh Omar

Date: October 29, 2025

To begin with:

$$|\phi\rangle = \frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} |x_0 + zr\rangle$$

where

$$m = \left\lfloor \frac{2^n}{r} \right\rfloor, \quad N = 2^n, \quad n = \log_2 N.$$

Now:

$$|\psi_1\rangle = QFT_{2^n} |\phi\rangle = \sum_{y=0}^{2^n-1} \left(\frac{1}{\sqrt{2^n m}} \sum_{z=0}^{m-1} e^{2\pi i (x_0+zr)y/2^n} \right) |y\rangle .$$

Equivalently, this can be written in terms of $N = 2^n$ as:

$$|\psi_1\rangle = QFT_N |\phi\rangle = \sum_{y=0}^{N-1} \left(\frac{1}{\sqrt{Nm}} \sum_{z=0}^{m-1} e^{2\pi i (x_0+zr)y/N} \right) |y\rangle .$$

The Quantum Fourier Transform requires $O(n^2)$ gates, i.e., $= O(n_0^2)$ gates.

$$\Pr\left[y_0 \text{ is obtained when } |\psi_1\rangle \text{ is observed}\right] = \left| \frac{1}{\sqrt{Nm}} \sum_{z=0}^{m-1} e^{2\pi i z r y_0/N} \right|^2 = \frac{1}{Nm} \left| \sum_{z=0}^{m-1} e^{2\pi i z r y_0/N} \right|^2 .$$

We have already seen that if $\frac{2^n}{r}$ is an integer, then $m = \frac{2^n}{r}$, and

$$P_m[y_0 = km] = \frac{1}{r},$$

while all other probabilities are zero, where k is an integer in $\{0, 1, 2, \ldots, r-1\}$.

When $\frac{2^n}{r}$ is not an integer, we have to verify that the obtained r is correct. Verifying

$$f(x) = f(x+a) \quad \text{for any } x \text{, in polynomial time.}$$

Old condition:

$$N = 2^n, \quad 1 \le r \le 2^n = N, \quad N \ge r$$

Now, lets assume

$$r \le 2^{n_0}, \quad n_0 = O(\log r)$$

and select n such that

$$2^n = 2^{2n_0+1} \Rightarrow n = 2n_0 + 1 = O(n_0).$$

The running time of the algorithm should thus be polynomial in n_0 and $\log r$, i.e., in n and $\log r$.

This ensures results from continued fraction theory can be applied.

$$P_r[y_k \text{ observed}] = \frac{1}{2^n m}\left|\sum_{z=0}^{m-1} e^{2\pi i r z \frac{y_k}{2^n}}\right|^2$$

Let

$$y_k = k\frac{2^n}{r} + \delta_k,$$

where δ_k (small) adjusts y_k to be an integer.

Then,

$$\frac{y_k}{2^n} = \frac{k}{r} + \frac{\delta_k}{2^n} \quad \Rightarrow \quad r\frac{y_k}{2^n} = k + r\frac{\delta_k}{2^n}.$$

Geometric Series Simplification:

$$\sum_{z=0}^{m-1} e^{2\pi i z(k+\frac{r\delta_k}{2^n})} = \sum_{z=0}^{m-1} e^{2\pi i z k} e^{2\pi i z\frac{r\delta_k}{2^n}}.$$

Since $e^{2\pi i z k} = 1$,

$$\sum_{z=0}^{m-1} e^{2\pi i z\frac{r\delta_k}{2^n}} = \frac{e^{2\pi i m\frac{r\delta_k}{2^n}} - 1}{e^{2\pi i\frac{r\delta_k}{2^n}} - 1}.$$

Using $e^{ix} - e^{-ix} = 2i\sin x$,

$$\frac{e^{2\pi i m\frac{r\delta_k}{2^n}} - 1}{e^{2\pi i\frac{r\delta_k}{2^n}} - 1} = \frac{e^{\pi i r\delta_k\frac{m}{2^n}}\left(e^{\pi i r\delta_k\frac{m}{2^n}} - e^{-\pi i r\delta_k\frac{m}{2^n}}\right)}{e^{\pi i r\delta_k/2^n}\left(e^{\pi i r\delta_k/2^n} - e^{-\pi i r\delta_k/2^n}\right)}$$

$$= \frac{2i\sin\left(\pi r\delta_k\frac{m}{2^n}\right)}{2i\sin(\pi r\delta_k/2^n)} \cdot \frac{e^{\pi i r\delta_k\frac{m}{2^n}}}{e^{\pi i r\delta_k/2^n}}$$

Thus,

$$P_r[y_k \text{ observed}] = \frac{1}{2^n m}\left|\frac{e^{i\pi r\delta_k\frac{m}{2^n}}}{e^{i\pi r\delta_k\frac{1}{2^n}}}\right|^2\left(\frac{\sin\left(\pi r\delta_k\frac{m}{2^n}\right)}{\sin\left(\pi r\delta_k\frac{1}{2^n}\right)}\right)^2$$

$$= \frac{1}{2^n m}\underbrace{\left|e^{i\theta}\right|^2}_{=1}\left(\frac{\sin\left(\pi r\delta_k\frac{m}{2^n}\right)}{\sin\left(\pi r\delta_k\frac{1}{2^n}\right)}\right)^2$$

$$= \frac{1}{2^n m}\left(\frac{\sin\left(\pi r\delta_k\frac{m}{2^n}\right)}{\sin\left(\pi r\delta_k\frac{1}{2^n}\right)}\right)^2.$$

When δ_k is small:

$$\frac{r}{2^n} \leq \frac{2^{n_0}}{2^{2n_0+1}} \approx 0$$

When a is small:

$$\sin(a) \approx a.$$

Hence,

$$P_r[y_k \text{ observed}] \approx \frac{1}{2^n m}\left(\frac{\sin(\pi r\delta_k m/2^n)}{\pi r\delta_k/2^n}\right)^2 = \frac{2^{2n}}{\pi^2 r^2 2^n m\delta_k^2} = \frac{2^n}{\pi^2 r^2 m\delta_k^2}.$$

$$|\delta_k| < 1, \quad |\delta_k| \leq \frac{1}{2}, \quad |\pi r\delta_k| \leq \frac{\pi}{2}.$$

For $0 \leq |x| \leq \frac{\pi}{2}$:

$$\frac{\sin x}{x} \geq \frac{2}{\pi}.$$

Thus,

$$\frac{1}{\pi^2 r^2 \delta_k^2} \sin^2(\pi r \delta_k) \geq \frac{1}{r^2} \left(\frac{2}{\pi}\right)^2.$$

Therefore,

$$P_r[y_k \text{ observed}] \geq \frac{1}{r} \left(\frac{4}{\pi^2}\right) \approx \frac{1}{r} \times 0.4.$$

Possible values of k:

$$k \in \{0, 1, 2, \ldots, r-1\}.$$

Hence, the total probability of observing some y_k corresponding to one of these values is:

$$P_r[\text{some } y_k \text{ observed for } k \in \{0, 1, \ldots, r-1\}] \geq r \cdot \frac{1}{r} \cdot \frac{4}{\pi^2} = \frac{4}{\pi^2} \approx 0.4.$$