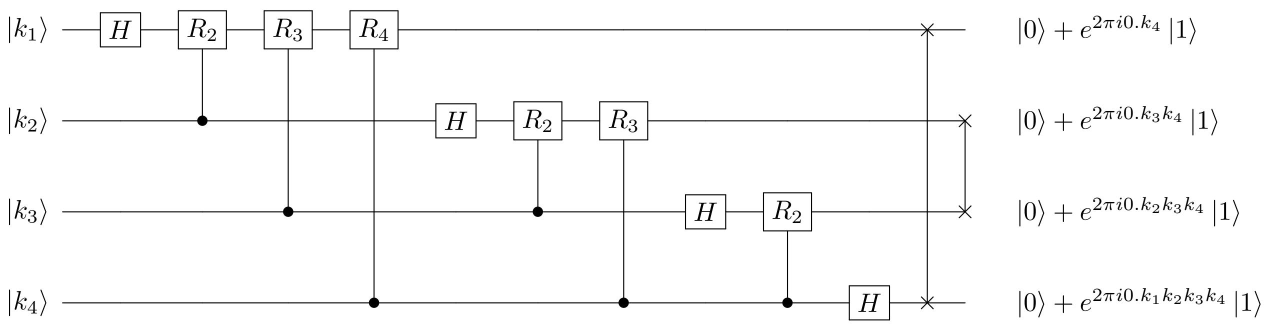
Homework 10
Quantum Information

Cheng-Ching Lin

June 24, 2018

1 QFT I

1.1



1.2

We can write down the general form of DFT.

$$\hat{x}_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-i\frac{2\pi}{N}kj} x_k = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{kj} x_k$$

Assume r divides N, and also assume that

$$x_k = \begin{cases} 1, & \text{if} \quad k = 0 \mod r \\ 0, & \text{otherwises} \end{cases}$$

Therfore, the entries $\hat{x}_j$ of the vector Ux is

$$\hat{x}_j = \frac{1}{\sqrt{N}} \sum_{k=0 \mod r}^{N-r} e^{-i\frac{2\pi}{N}kj} = \frac{1}{\sqrt{N}} \sum_{k=0 \mod r}^{N-r} \omega_N^{kj}$$

In this case, the largest magetude is

$$\frac{1}{\sqrt{N}} \sum_{k=0 \mod r}^{N-r} e^{-i\frac{2\pi}{N}kj} = \frac{1}{\sqrt{N}} \frac{N}{r} = \frac{\sqrt{N}}{r}$$

If $N = 100$ and $r = 20$, the result will be Figure 1.

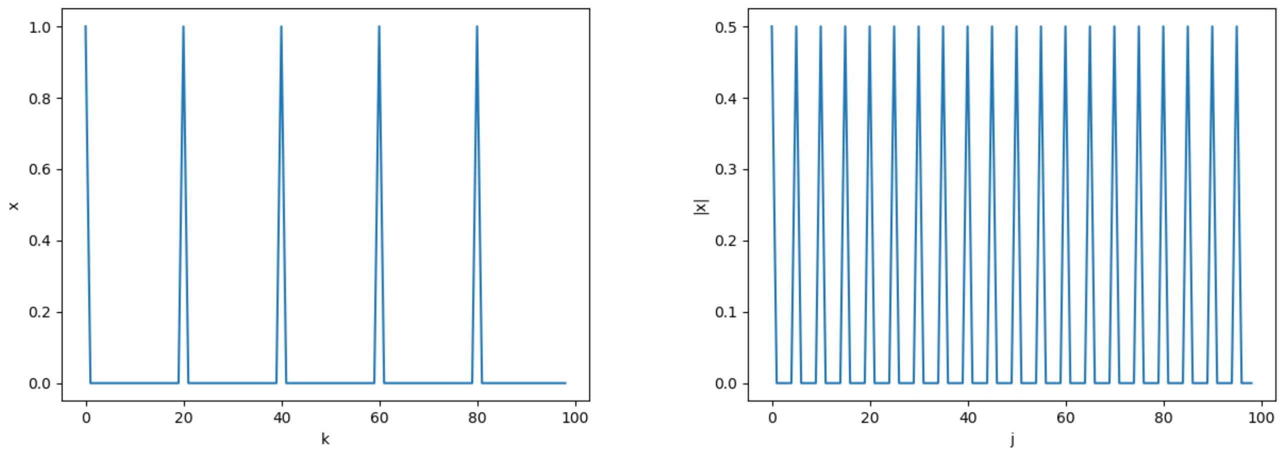
2 QFT II

2.1

$$\|A\| = \frac{\|A|\psi\rangle\|}{\||\psi\rangle\|} = \frac{\sqrt{\langle\psi| A^\dagger A |\psi\rangle}}{\sqrt{\langle\psi|\psi\rangle}}$$

$$\|UA\| = \frac{\sqrt{\langle\psi| A^\dagger U^\dagger U A |\psi\rangle}}{\sqrt{\langle\psi|\psi\rangle}} = \frac{\sqrt{\langle\psi| A^\dagger A |\psi\rangle}}{\sqrt{\langle\psi|\psi\rangle}} = \|A\|$$

$$\|AU\| = \frac{\sqrt{\langle\psi| U^\dagger A^\dagger A U |\psi\rangle}}{\sqrt{\langle\psi|\psi\rangle}} = \frac{\sqrt{\langle\psi| U U^\dagger A^\dagger A U U^\dagger |\psi\rangle}}{\sqrt{\langle\psi|\psi\rangle}} = \frac{\sqrt{\langle\psi| A^\dagger A |\psi\rangle}}{\sqrt{\langle\psi|\psi\rangle}} = \|A\|$$



(a) x_k v.s. k

(b) $\hat{x}_j$ v.s. j

Figure 1: In the case of $N = 100$ and $r = 20$.

2.2

$$\begin{aligned}\|U - \mathbb{1}\| &= \sqrt{\langle\psi|(U^\dagger - \mathbb{1})(U - \mathbb{1})|\psi\rangle} = \sqrt{\langle\psi| U^\dagger U - U^\dagger - U + \mathbb{1} |\psi\rangle} \\ &= \sqrt{\langle\psi| - U^\dagger - U + 2\mathbb{1} |\psi\rangle} = \sqrt{\langle\psi| - \begin{pmatrix}1 & 0 \\ 0 & e^{-i\phi}\end{pmatrix} - \begin{pmatrix}1 & 0 \\ 0 & e^{i\phi}\end{pmatrix} |\psi\rangle + 2} \\ &= \sqrt{-2 - 2\cos\phi + 2} \approx \sqrt{\phi^2} = \mathcal{O}(\phi)\end{aligned}$$

2.3

Let $U_j = A$, $U_> = U_L \cdots U_{j+1}$, and $U_< = U_{j-1} \cdots U_1$, so

$$\|U - U'\| = \|U_> A U_< - U_> U_<\|$$

From 2.1, we can rewrite the formula into

$$\|U_> A U_< - U_> U_<\| = \|A - \mathbb{1}\| = \|U_j - \mathbb{1}\|$$

2.4

Let $U_a = U_L \cdots U_{j+1}$, $U_b = U_{j-1} \cdots U_{k+1}$, and $U_c = U_{k-1} \cdots U_1$, thus

$$\begin{aligned}\|U - U''\| &= \|U_j U_b U_k - Ub\| \\ = \|U_j U_b U_k - U_b U_k + U_b U_k - Ub\| &\leq \|(U_j - \mathbb{1}) U_b U_k\| + \|U_b(U_k - \mathbb{1})\| \leq \|U_j - \mathbb{1}\| + \|U_k - \mathbb{1}\|\end{aligned}$$

2.5

The phase gate $R_s = \begin{pmatrix}1 & 0 \\ 0 & e^{2i\pi/2^s}\end{pmatrix}$ will be close to identity if s is large. It doesn't too much change when $s \gg \log n$. Thus, we will take out $\mathcal{O}(\log n)$ gates which $s \gg \log n$. We only keep $\mathcal{O}(\log n)$ gates for each qubit, $\mathcal{O}(n \log n)$ gates in the quantum circuits.

We suppose U is the quantum circuit with $\mathcal{O}(n \log n)$ gates, and also we suppose $s \geq \log n^2$, therefore

$$\|U_{FT^{(n)}} - U\| \geq n \| \begin{pmatrix}1 & 0 \\ 0 & e^{i2\pi/2^{\log n^2}}\end{pmatrix} - \mathbb{1}\| = n \| \begin{pmatrix}1 & 0 \\ 0 & e^{i2\pi/n^2}\end{pmatrix} - \mathbb{1}\| = \mathcal{O}(\frac{1}{n})$$

3 Finding the period in the "hard" case

3.1

Because $0 \leq k < r$, and $j \in 0, 1, \cdots, L-1$, by pigeonhole principle, every k must have at least one j such that

$$|j - k\frac{L}{r}| \leq \frac{1}{2}$$

Therefore, there are at least r goof j's that satisfied the condition.

3.2

If $\exp(i2\pi rj/L) = 1$, then $c_j = m$

$$Prob(j) = \frac{|c_j|^2}{mL} = \frac{m^2}{mL} = \frac{m}{L}$$

On the other side, if $\exp(i2\pi rj/L) \neq 1$, then

$$c_j = \frac{1 - \exp(i2\pi rmj/L)}{1 - \exp(i2\pi rj/L)}$$

Also because

$$|1 - e^{i\theta}| = | - 2ie^{i\theta/2}\sin(\theta/2)| = |2\sin(\theta/2)|$$

Thus,

$$Prob(j) = \frac{|c_j|^2}{mL} = \frac{1}{mL}|\frac{1 - \exp(i2\pi rmj/L)}{1 - \exp(i2\pi rj/L)}|^2 = \frac{1}{mL}|\frac{\sin(\pi rmj/L)}{\sin(\pi rj/L)}|^2$$

3.3

Suppose good j can be written as

$$j = k\frac{L}{r} + h$$

For $|h| \leq \frac{1}{2}$. All good j's need to be satisfy this condition:

$$|j - k\frac{L}{r}| \leq \frac{1}{2}$$

$$\Rightarrow |k\frac{L}{r} + h - k\frac{L}{r}| = |h| \leq \frac{1}{2}$$

Therefore, we can always write good j's as $k\frac{L}{r} + h$. In order words, for every good j, there exists an integer $0 \leq k < r$ and $|h| \leq \frac{1}{2}$ such that

$$j = k\frac{L}{r} + h$$

3.4

if $h = 0$, $j = k\frac{L}{r}$ and then

$$\exp(i2\pi rj/L) = \exp(ik2\pi) = 1$$

It means that

$$Prob(j) = \frac{m}{L} \geq \frac{\frac{L}{r}}{L} = \frac{1}{r}$$

3.5

If $h \neq 0$, $j = k\frac{L}{r} + h$ and then

$$\exp(i2\pi rj/L) = \exp(i2\pi rh/L) \neq 1$$

Therefore,

$$Prob(j) = \frac{1}{mL}|\frac{1 - \exp(i2\pi rmj/L)}{1 - \exp(i2\pi rj/L)}|^2 = \frac{1}{mL}|\frac{1 - \exp(i2\pi rmh/L)}{1 - \exp(i2\pi rh/L)}|^2 = \frac{1}{mL}|\frac{\sin(\pi rmh/L)}{\sin(\pi rh/L)}|^2$$

3.6

We know that $0 \leq |h| \leq \frac{1}{2}$ and $0 < \frac{r}{L} \leq 1$. Because m equals to $\lfloor \frac{L}{r} \rfloor$ or $\lceil \frac{L}{r} \rceil$, we rewrite the range of m as

$$\frac{L}{r} - \frac{1}{2} \leq m \leq \frac{L}{r} + \frac{1}{2}$$

Now we times $\frac{r}{L}$.

$$1 - \frac{r}{2L} \leq m\frac{r}{L} \leq 1 + \frac{r}{2L}$$

$$\Rightarrow \frac{1}{2} \leq m\frac{r}{L} \leq \frac{3}{2}$$

Finally, we times $|h|$.

$$\Rightarrow 0 \leq m\frac{r}{L}|h| \leq \frac{3}{4} < \frac{4}{5}$$

We can rewrite the range as

$$0 \leq \frac{r}{L}|h| < m\frac{r}{L}|h| \leq \frac{3}{4} = \frac{1}{2} + \frac{1}{4} < \frac{4}{5}$$

It means that $\sin\left(m\pi\frac{r}{L}|h|\right) = \sin\left(\pi(m\frac{r}{L}|h| - \frac{1}{2})\right) \leq \sin\left(\frac{\pi}{4}\right)$ Therefore, the range of $Prob(j)$ is

$$\frac{1}{mL}|\frac{\frac{3\pi mhr}{4L}}{\frac{\pi hr}{L}}|^2 < \frac{1}{mL}|\frac{\sin(\pi rmh/L)}{\sin(\pi rh/L)}|^2 < \frac{1}{mL}|\frac{\frac{\pi mhr}{L}}{\frac{3\pi hr}{4L}}|^2$$
$$\Rightarrow \frac{1}{mL}|\frac{3m}{4}|^2 < \frac{1}{mL}|\frac{\sin(\pi rmh/L)}{\sin(\pi rh/L)}|^2 < \frac{1}{mL}|\frac{4m}{3}|^2$$
$$\Rightarrow \frac{9m}{16L} < \frac{1}{mL}|\frac{\sin(\pi rmh/L)}{\sin(\pi rh/L)}|^2 < 1 < \frac{16m}{9L}$$

Thus,

$$Prob(j) > \frac{9m}{16L} \geq \frac{m}{2L}$$

3.7

4 Simulating Shor's algorithm

4.1

The general form of $|\psi_3\rangle$ (only consider first register) is

$$|\psi_3\rangle = \frac{1}{\sqrt{m}}\sum_{k=0}^{m-1}|kr+s\rangle$$

I use the Python to find the x of $f(x) = 9 = x^7 \mod 11$. There are 12 components satisfying this condition($m = 12$), and $r = 11$. Thus, we can write down $|\psi_3\rangle$.

$$|\psi_3\rangle = \frac{1}{\sqrt{12}}\sum_{k=0}^{11}|11k+3\rangle$$

4.2

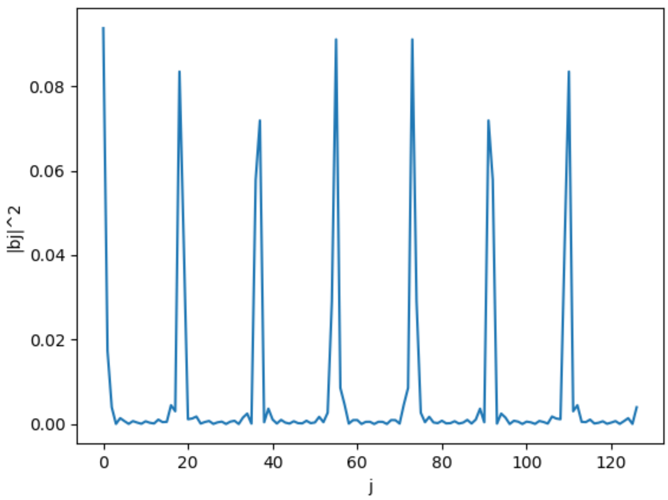


Figure 2: The figure of j v.s. $|b_j|^2$

The first four j's for which $|b_j|^2$ peaks are

$$\begin{cases} j = 0 & |b_j^2| = 0.09375 \\ j = 18 & |b_j^2| = 0.08346 \\ j = 37 & |b_j^2| = 0.07189 \\ j = 55 & |b_j^2| = 0.09109 \end{cases}$$

This is my code of DFT, and the result is $refB$.

```
def DFT():
        blist = []
        b = []
        s = 3
        r = 11
        L = 128
        m = 12
        for jdx in range(0,127):
                ansj = cmath.exp(2j*s*math.pi*jdx/L)
                ansk = 0
                for kdx in range(3,124,11):
                        ansk += cmath.exp(2j*math.pi*r*kdx*jdx/L)
                        ans = ansk*ansj/math.sqrt(L*m)
                blist.append(pow(abs(ans),2))
                if pow(abs(ans),2) >0.06:
                        print(jdx)
                        print(pow(abs(ans),2))
                b.append(jdx)
        plt.plot(b, blist)
        plt.xlabel("j")
        plt.ylabel("|bj|^2")
        plt.show()
```

4.3

To find the correct order, we use "continued fractions" to $\frac{j}{L}$. In these three cases, the continued fractions are

$$\frac{102}{128} = [0, 1, 3, 1, 12]$$

$$\frac{13}{128} = [0, 9, 1, 5, 2]$$

$$\frac{39}{128} = [0, 3, 3, 1, 1, 5]$$

The number in the bracket is partial quotients. We can find the fractions $\frac{c}{r}$ which are close to $\frac{j}{L}$ by them. the way to find it is. However, the fractions must satisfy two conditions.

$$r \leq N$$

$$|\frac{j}{L} - \frac{c}{r}| \leq \frac{1}{2L}$$

$$\Rightarrow |\frac{j}{128} - \frac{c}{r}| \leq \frac{1}{256}$$

We believe r will be the answer if above are satisfied. In our cases, there are only two fractions satisfied.

$$|\frac{102}{128} - \frac{8}{10}| = \frac{1}{320} < \frac{1}{256}$$

$$|\frac{13}{128} - \frac{1}{10}| = \frac{1}{640} < \frac{1}{256}$$

Therefore, $j = 102$ and $j = 13$ can give the correct order.