Quantum Algorithms, Spring 2022: Lecture 10 Scribe

Sravani Yanamandra, Srikar Kale

February 21, 2022

1 Recap

1.1 Properties of QFT:

1. **Invariance under shift:** Suppose,

$$\sum_j \alpha_j |j\rangle \xrightarrow{QFT} \sum_k \beta_k |k\rangle$$

then,

$$\sum_j \alpha_j |j+s\rangle \xrightarrow{QFT} \sum_k \omega^{sk} \beta_k |k\rangle$$

2. **QFT maps a periodic superposition to a period superposition:**

Let,

$$|\psi\rangle = \frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |kr\rangle$$

such that

$$A = \frac{N}{r}\ ,\ r|N$$

then,

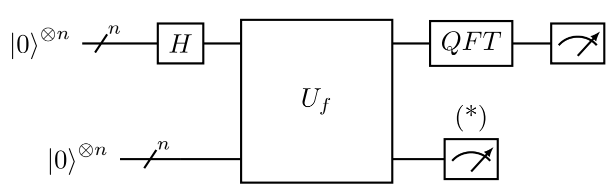
$$QFT\,|\psi\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |\frac{jN}{r}\rangle$$

1.2 Quantum period finding:

1. **Problem statement:**

Given a blackbox U_f for some boolean function $f : \{0,1\}^n \to \{0,1\}^m$ such that f is a periodic function with $r << \sqrt{N}$ where $N = 2^n$ i.e, $f(x) = f(y) \Leftrightarrow y = x(mod \text{ r})$. How many queries to U_f are required to find r?

2. **Circuit:**



3. **Equations:**

Hadamard gate applied to first register:

$$|0\rangle^{\otimes n} |0\rangle^{\otimes n} \xrightarrow{H^{\otimes n} \otimes I} \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle$$

U_f applied to both registers

$$\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

Measuring 2nd register and observe $f(x_0)$:

$$\frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |x_0 + kr\rangle$$

Using the shift in variance property discussed in *Section* 1.1 (property 1)

$$\frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |x_0 + kr\rangle = \frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |kr\rangle$$

Applying QFT on the remaining qubits

$$\frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |kr\rangle \xrightarrow{QFT} \frac{1}{\sqrt{AN}} \sum_{l=0}^{N-1} \sum_{k=0}^{A-1} (\omega^{rl})^k |l\rangle$$

4. **Amplitude of $|l\rangle$:**

$$\alpha_l = \frac{1}{\sqrt{AN}} \sum_{k=0}^{A-1} (\omega^{rl})^k$$

$$\alpha_l = \begin{cases} \sqrt{\frac{A}{N}} & \text{if } \omega^{rl} = 1 \\ \frac{1}{\sqrt{NA}} \frac{(1-\omega^{rlA})}{(1-\omega^{rl})} & \text{if } \omega^{rl} \neq 1 \end{cases}$$

5. **We have 2 cases:**

   (a) Case 1:

   $$r|N \implies A = \frac{N}{r}$$

   (b) Case 2:

   $$r \nmid N \implies A = \left\lceil \frac{N}{r} \right\rceil \; or \; \left\lfloor \frac{N}{r} \right\rfloor \; , \; A - 1 \leq \frac{N}{r} \leq A + 1$$

6. **We had already discussed Case 1 in the previous class and analysed it as follows:**

$$r|N \implies A = \frac{N}{r}$$

$$\sqrt{\frac{r}{N}} \sum_{k=0}^{\frac{N}{r}-1} |kr\rangle \rightarrow \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |\frac{jN}{r}\rangle$$

   (a) Measuring the first register gives $s_1 \frac{N}{r}$

   (b) Repeating $k = \theta(1)$ times we have $\{s_1 \frac{N}{r}, s_2 \frac{N}{r}, s_3 \frac{N}{r}, ..., s_k \frac{N}{r}\}$

   (c) With very high probability, S_i's are relatively co prime

   (d) $\gcd\{s_1 \frac{N}{r}, s_2 \frac{N}{r}, s_3 \frac{N}{r}, ..., s_k \frac{N}{r}\} = \frac{N}{r}$ which gives us r as N is known.

   (e) The additional cost here is $O(logN)$ from Euclid's GCD algorithm

   (f) If the S_i's are not relatively co prime, we wont be able to detect the mistake in the next step. To overcome this we can take k to be large enough such that the probability is extremely high or repeat the algo and verify r in the subsequent iteration.

   (g) These are not deterministic algorithm's

2 Things to know for this class:

2.1 Properties of sin(x):

1. For $x \in \mathbb{R}$, $\theta < \frac{|sin(x)|}{|x|} < 1 \implies sin^2(x) < x^2$, this can be derived using the Mean Value Theorem
2. For $0 \leq |x| \leq \frac{\pi}{2}, |sin(x)| \geq \frac{2|x|}{\pi}$
   This is because $\frac{|sin(x)|}{|x|}$ is a decreasing function for the interval $0 \leq |x| \leq \frac{\pi}{2}$. Let $g(|x|) = \frac{|sin(x)|}{|x|}$ *then* $g(|x|) \geq g(\frac{\pi}{2})$ (for decreasing functions only)
3. $sin^2(\pi q \pm \theta) = sin^2(\theta)\ as\ sin(\pi q \pm \theta) = \pm sin(\theta)\ when\ q \in \mathbb{N}_0$

2.2 Continued fractions

The idea of the continued fractions method is to describe real numbers in terms of integers alone. A finite simple continued fraction is defined by a finite collection $a_0, ..., a_N$ of positive integers as

$$[a_0, a_1, ..., a_N] = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{... + \frac{1}{a_N}}}}$$

We define the nth convergent $(0 \leq n \leq N)$ to this continued fraction to be $[a_0, ..., a_n]$.
Suppose we are trying to decompose 31/13 as a continued fraction.

The first step of the continued fractions algorithm is to **split** 31/13 into its integer and fractional part,

$$\frac{31}{13} = 2 + \frac{5}{13}$$

Next we **invert** the fractional part, obtaining

$$\frac{31}{13} = 2 + \frac{1}{\frac{13}{5}}$$

And we keep on going forward with the **split and invert** procedure, we would end up with

$$\frac{31}{13} = 2 + \cfrac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}$$

1. It's clear that the continued fractions algorithm terminates after a finite number of 'split and invert' steps for any rational number, since the numerators which appear are strictly decreasing.
2. The continued fractions algorithm provides an unambiguous method for obtaining a continued fraction expansion of a given rational number.
3. The only possible ambiguity comes at the final stage, because it is possible to split an integer in two ways, either $a_N = a_N$, or as $a_N = (a_N - 1) + 1/1$, giving two alternate continued fraction expansions.
4. This ambiguity is actually useful, since it allows us to assume without loss of generality that the continued fraction expansion of a given rational number has either an odd or even number of convergent, as desired.
5. How quickly does this termination occur? It follows that if $x = \frac{p}{q}$ is a rational number, p & q are L bit integers, then the continued fraction expansion for x can be computed using $O(L^3)$ operations – $O(L)$ 'split and invert' steps, each using $O(L^2)$ gates for elementary arithmetic.

2.3 Useful claim 1:

Claim 2.1. 2 distinct rational numbers with denominators $\leq r$ are atleast $\frac{1}{r^2}$ apart

Proof. Let $Z = \frac{X}{Y}$ and $Z' = \frac{X'}{Y'}$ with $(Y, Y') \leq r$ then

$$|Z - Z'| = |\frac{XY' - X'Y}{YY'}|$$

The numerator will be ≥ 1 while the denominator will be $\leq r^2$ so we can say

$$|Z - Z'| \geq \frac{1}{r^2}$$

□

2.4 Useful claim 2

Claim 2.2. Let $p, q \in Z^+$, and $x \in Q$ that satisfy the following:

$$|x - \frac{p}{q}| \leq \frac{1}{2q^2}$$

Also let $c = (c_0, c_1, ..., c_m)$ be the continued fraction expansion of x then there exists some $Q \in \{0, 1, 2, ...M\}$ such that the Q^{th} convergent $C_Q = (c_0, c_1, ..., c_Q)$ is exactly $\frac{p}{q}$. Further more choosing $M = O(logN)$ suffices, where p & q are $logN$ bit integers.

Proof. The proof of this claim is available in the Quantum Computation and Quantum Information textbook by Michael A. Nielsen & Isaac L. Chuang, Appendix: Number Theory. □

3 Main crux of lecture 10:

3.1 Quantum period finding, Case 2:

We know,

$$r \nmid N \implies A = \left\lceil \frac{N}{r} \right\rceil \ or \left\lfloor \frac{N}{r} \right\rfloor \ , \ A - 1 \leq \frac{N}{r} \leq A + 1$$

Let

$$\alpha_l = \frac{1}{\sqrt{NA}} \frac{(1 - \omega^{rlA})}{(1 - \omega^{rl})}, \omega = e^{\frac{i2\pi}{N}}$$

In this case, we will argue that l is still very close to some $\frac{jN}{r}$

$$|\alpha_l|^2 = \frac{1}{NA} \frac{|1 - e^{\frac{2irlA\pi}{N}}|^2}{|1 - e^{\frac{2irl\pi}{N}}|^2}$$

We know that

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

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

Which implies,

$$|1 - e^{i\theta}|^2 = 4sin^2(\frac{\theta}{2})$$

Coming back to α_l

$$|\alpha_l|^2 = \frac{1}{NA} \frac{sin^2(\frac{rlA\pi}{N})}{sin^2(\frac{rl\pi}{N})}$$

So the probability of observing some l is given by $|\alpha_l|^2$ which is $\frac{1}{NA}\frac{sin^2(\frac{rlA\pi}{N})}{sin^2(\frac{rl\pi}{N})}$.
What is the probability of l being close to some multiple of $\frac{N}{r}$?
Consider, $l = \frac{mN}{r} + \delta_m$ where $m \in \{0, 1, ..., r-1\}$, δ_m is a very small value. We know that $|\delta_m| < 0.5$ (we want this kind of accuracy, rather). The intuition behind this is that the nearest integer from $\frac{mN}{r}$ would be less than 0.5 distance away.
We now plug in the value of l

$$\frac{rlA\pi}{N} = \frac{\pi rA}{N}(\frac{mN}{r} + \delta_m)$$
$$\frac{rlA\pi}{N} = \pi mA + \frac{\pi rA\delta_m}{N}$$

Similarly

$$\frac{rl\pi}{N} = \pi m + \frac{\pi r\delta_m}{N}$$

Using the property 3 from *Section* 2.1 and plugging the above information into $|\alpha_l|^2$,

$$|\alpha_l|^2 = \frac{1}{NA}\frac{sin^2(\frac{rlA\pi}{N})}{sin^2(\frac{rl\pi}{N})}$$

$$|\alpha_l|^2 = \frac{1}{NA}\frac{sin^2(\frac{\pi rA\delta_m}{N})}{sin^2(\frac{r\pi\delta_m}{N})}$$

So to get a lower bound on $|\alpha_l|^2$ we use property 2 to the numerator and property 1 to the denominator *present in Section* 2.1.
We get

$$|\alpha_l|^2 \geq \frac{4A}{\pi^2 N}$$
$$|\alpha_l|^2 \geq const.\frac{A}{N}$$

To be able to apply the property for the numerator we need to show $0 \leq |\frac{rlA\pi}{N}| \leq \frac{\pi}{2}$, we know that

$$A - 1 \leq \frac{N}{r} \leq A + 1$$

$$\frac{N}{r} - 1 \leq A \leq \frac{N}{r} + 1$$

$$1 - \frac{r}{N} \leq \frac{Ar}{N} \leq 1 + \frac{r}{N}$$

By assumption $r << \sqrt{N}$, $\frac{rA}{N} \simeq 1$, $\frac{r}{N} \simeq o(\frac{1}{\sqrt{N}})$
So,

$$\frac{\pi r\delta_m A}{N} \simeq \pi\delta_m$$
$$0 \leq \frac{\pi r\delta_m A}{N} \leq \frac{\pi}{2} \pm O(\frac{r}{N})$$

We can ignore the right most term and apply this property to the numerator:

$$|\alpha_l|^2 \geq \frac{4A}{\pi^2 N}$$

$$|\alpha_l|^2 \geq \frac{4}{\pi^2 r}$$

With a probability $\geq \frac{4}{\pi^2 r}$ we observe some l such that $l = \frac{mN}{r} + \delta_m$

$$|l - \frac{mN}{r}| = \delta_m$$

$$\implies |l - \frac{mN}{r}| < 0.5 \ (as\ \delta_m < 0.5) for\ m \in \{0, 1, 2, ..., r-1\}$$

Therefore, the probability of observing any such $'m'$

$$\geq \frac{4}{\pi^2 r} * r$$

$$\geq \frac{4}{\pi^2}$$

$$\geq 0.4$$

For case 1: $r|N$, we observed $\frac{mN}{r}$ exactly. If we observe some $'bad'$ value of l we still follow the same procedure and get some $'r'$ and if its erroneous, we repeat it again.
Over here, we get some $'l'$ close to $\frac{mN}{r}$ but we dont know which $\frac{mN}{r}$ it is. We need to extract this closeness multiple to $\frac{N}{r}$. Lets say we do that erroneously. We do the procedure a few times and it fails one of the time, and we dont get the correct value of $'r'$ but we are guaranteed that it will succeed with probability ≥ 0.4

So far:

1. We have observed some $'l'$ such that with a probability $\geq \frac{4}{\pi^2}$, $|l - \frac{mN}{r}| < 0.5$
2. From the above equation $|\frac{l}{N} - \frac{m}{r}| < \frac{1}{2N} < \frac{1}{r^2}\ as\ (r << \sqrt{N})$
3. $\frac{l}{N}$ & $\frac{m}{r}$ are 2 rational numbers
4. we know l & N, we dont know $m\ or\ r$

We need information about $\frac{m}{r}$. From the claim in $section$ 2.3 we can say that $\frac{m}{r}$ is the only fraction with denominator $\leq r$ that is within $\frac{1}{2r^2}$ of $\frac{l}{N}$. The reason being if any other fraction existed then that distance would be at least $\frac{1}{r^2}$ away from $\frac{m}{r}$.
Now there exists a classical procedure that allows us to exactly obtain $\frac{m}{r}$, starting from $\frac{l}{N}$ provided $|\frac{l}{N} - \frac{m}{r}| < \frac{1}{2r^2}$. This procedure is known as continued fraction expansion. This has been explained to some extent in $Section 2.2$.
Using the claim in $Section$ 2.4 Starting from $\frac{l}{N}$, we can exactly obtain $\frac{m}{r}$ in $O(logN)$ steps. After the continued fraction algorithm, we end up with $\frac{m}{r}$.
Repeat QFT algorithm and the continued fraction algorithm k times such that we get:

$$\{\frac{m_1}{r}, \frac{m_2}{r}, ..., \frac{m_k}{r}\}$$

then,

$$gcd\{\frac{m_1}{r}, \frac{m_2}{r}, ..., \frac{m_k}{r}\}\ to\ get\ r$$

where $m_1, m_2, ..., m_k$ are relatively coprime with very high probability. The GCD calculation will take $O(logN)$ steps.

3.2 Analysis of QFT period finding, case 2:

1. Query complexity: $K = \theta(1)$ to U_f
2. Additional costs:
   (a) $O(logN)$ overhead for GCD and continued fractions calculations
   (b) $logN$ number of Hadamard gates needed
   (c) QFT circuit: $O(log^2 N)$ elementary gates.