Quantum Algorithms, Spring 2022: Lecture 9 Scribe

Nithish Raja, Shodasakshari Vidya

February 21, 2022

1 Recap

1.1 Previously seen quantum algorithms

Algorithm	Classical query complexity	Quantum query complexity
Deutsch	2	1
Deutsch - Jozsa	$O(1)$	1
Bernstein - Vazirani	$O(n)$	1
Simon's algorithm	$O(2^{n/2})$	$O(n)$

Table 1: Comparing query complexity of quantum algorithms and their classical counterparts

1.2 Quantum Fourier transform

$$|j\rangle \xrightarrow{F_N} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{jk} |k\rangle \tag{1}$$

Probability of observing state K after QFT:

$$\langle k| F_N |j\rangle = \frac{\omega^{jk}}{\sqrt{N}}$$

Applying QFT on an arbitrary quantum state, we get

$$\sum_{j=0}^{N-1} \alpha_j |j\rangle \xrightarrow{F_N} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} \alpha_j \omega^{jk} |k\rangle \tag{2}$$

Above equation can be written in short as

$$\sum_{j=0}^{N-1} \alpha_j |j\rangle \xrightarrow{F_N} \sum_{k=0}^{N-1} \beta_k |k\rangle \text{, where } \beta_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \alpha_j \omega^{jk}$$

QFT is calculated by applying the following unitary transform on the quantum state

$$F_N = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \dots & \omega^{(N-1)^2} \end{bmatrix}_{N \times N}$$

Unlike DFT, QFT outputs a quantum state. Because of this, measurement yeilds a random state $|k\rangle$ with some probability $\|\beta_k\|^2$. Using this we can perform fourier sampling.

2 Useful properties of QFT

2.1 QFT is shift invariant

Consider an arbitrary quantum state $|\psi\rangle = \sum_{j=0}^{N-1} \alpha_j |j\rangle$, applying QFT to it, we get

$$F_N(\sum_{j=0}^{N-1} \alpha_j |j\rangle) = \sum_{k=0}^{N-1} \beta_k |k\rangle \text{ , where } \beta_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \alpha_j \omega^{jk}$$

Now consider applying QFT where each state has been shifted by a constant value s

$$\begin{aligned}\sum_{j=0}^{N-1} \alpha_j |j+s\rangle &\xrightarrow{F_N} \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \alpha_j \sum_{k=0}^{N-1} \omega^{(j+s)k} |k\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{sk} \sum_{j=0}^{N-1} \alpha_j \omega^{jk} |k\rangle \\ &= \sum_{k=0}^{N-1} \omega^{sk} \beta_k |k\rangle\end{aligned}$$

Probablity to observe state $|k\rangle$ is still $\|\beta_k\|^2$. Therefore, shifting of initial state by a constant value does not change the output state after applying QFT i.e., QFT is shift invariant.

2.2 QFT maps a periodic superposition to another periodic superposition

Consider a periodic superposition as given below,

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{A-1} |kr\rangle \qquad (A = \tfrac{N}{r}\text{, assuming } r|N)$$

Applying QFT to state $|\psi\rangle$, we get

$$\begin{aligned}\frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |kr\rangle &\xrightarrow{F_N} \frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \omega^{krl} |l\rangle \\ &= \frac{1}{\sqrt{AN}} \sum_{k=0}^{A-1} \sum_{l=0}^{N-1} \omega^{krl} |k\rangle\end{aligned}$$

$$\text{Amplitude of state } |l\rangle = \frac{1}{\sqrt{NA}} \sum_{k=0}^{A-1} (\omega^{rl})^k$$

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

Given that $A = \frac{N}{r}$, consider amplitude of states where $l = \frac{jN}{r}$

$$\begin{aligned}\omega^{lr} &= 1 \\ \alpha_{\frac{jN}{r}} &= \frac{1}{\sqrt{r}} \qquad (\forall j \epsilon \{0, 1, \ldots, r-1\})\end{aligned}$$

Therefore,

$$\sqrt{\frac{r}{N}} \sum_{k=0}^{\frac{N}{r}-1} |kr\rangle \xrightarrow{F_N} \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |\frac{jN}{r}\rangle \tag{3}$$

Sum of probability of above states add up to 1. Therefore, probability of states where $A \neq \frac{N}{r}$ is zero.

3 Quantum period finding algorithm

Let $f : \{0,1\}^n \rightarrow \{0,1\}^m$ be a periodic function with period r. r is a positive number satisfying $1 << r << \sqrt{2^n}$

$$f(x) = f(x + kr) \qquad (x, x + kr \epsilon \{0, 1, \ldots, N-1\})$$

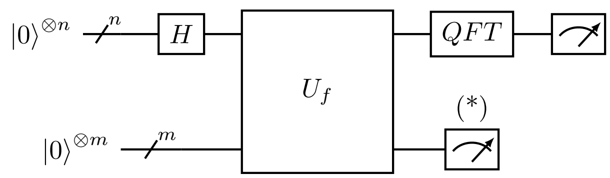
$$f(x) = f(x + kr) \iff f(x) = f(y) \qquad (\text{iff } y = x \mod r)$$

Therefore, for a given x_0,

$$f(x_0) = f(x_0 + r) = f(x_0 + 2r) = \cdots = f(x_0 + (A-1)r)$$

If $r|N$, then $A = \frac{N}{r}$ else $A = \lfloor \frac{N}{r} \rfloor$ or $A = \lceil \frac{N}{r} \rceil$.

The quantum circuit for quantum period finding algorithm is given below



$$|0^{\otimes n}\rangle |0^{\otimes m}\rangle \xrightarrow{H^{\otimes n} I} \frac{1}{\sqrt{N}} \sum_{x \epsilon \{0,1\}^n} |x\rangle |0\rangle^{\otimes m} \xrightarrow{U_f} \sum_{x \epsilon \{0,1\}^n} |x\rangle |f(x)\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_x \frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |x + kr\rangle |f(x)\rangle$$

After measurement in second register, the state collapses into

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

Ignoring the value in second register,

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

We know that QFT is shift invariant, therefore the above state can be written as

$$\frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |kr\rangle \xrightarrow{F_N} \sum_l \alpha_l |l\rangle$$

$$\alpha_l = \frac{1}{\sqrt{NA}} \sum_{k=0}^{A-1} (\omega^{rl})^k = \begin{cases} \sqrt{\dfrac{A}{N}}, & \text{if } \omega^{rl} = 1 \\ \dfrac{1}{\sqrt{NA}} \dfrac{(1 - \omega^{rlA})}{(1 - \omega^{rl})}, & \text{if } \omega^{rl} \neq 1 \end{cases}$$

Case 1: $r|N$ i.e., $A = \frac{N}{r}$ From 3, we know that

$$\frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |kr\rangle \xrightarrow{F_N} \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |\frac{jN}{r}\rangle$$

At this point, we make a measurement and observe some $\frac{s_1 N}{r}$, $s_1 \epsilon \{0, 1, \ldots, r-1\}$.
Making multiple runs of the circuit, we get $\{\frac{s_1 N}{r}, \frac{s_2 N}{r}, \ldots, \frac{s_k N}{r}\}$. If $s_1, s_2, \ldots, s_N$ are coprimes, then the GCD of $\{\frac{s_1 N}{r}, \frac{s_2 N}{r}, \ldots, \frac{s_k N}{r}\}$ will be $\frac{N}{r}$. Using euclid's algorithm, GCD can be calculated in $\log N$ time.
We know N, therefore the value of r can be calculated.

3.1 Probability that k randomly selected numbers are co-primes

Consider $s_i \epsilon \{1, 2, \dots, n\}$. Let p be a prime number s.t. $p|s_i$ and $\frac{s_i}{p} = q$, where $q \epsilon \{1, 2, \dots, \frac{n}{p}\}$.

$$Pr[p|s_i] < \frac{\frac{n}{p} + 1}{n} \sim \frac{1}{p} + \frac{1}{n}$$

$$Pr[p|s_i] \sim \frac{1}{p}$$

$$Pr[\text{k randomly selected numbers are all divisible by p}] \sim \frac{1}{p^k}$$

$$Pr[\text{Atleast 1 among k randomly selected numbers is not divisible by p}] \sim 1 - \frac{1}{p^k}$$

$$Pr[\text{k randomly selected numbers are co-primes}] = \prod_{p \epsilon PRIMES} (1 - \frac{1}{p^k}) = \frac{1}{\zeta(k)}$$

Here, $\zeta(k)$ represents the reimann zeta function. The value of $\frac{1}{\zeta(k)}$ approaches 1 very quickly. Therefore, for large values of k, the value of Pr[k randomly selected numbers are coprimes] is very close to 1.