QUANTUM COMPUTATION

Lecture 4

Nilava Metya
nilavam@cmi.ac.in

1 August 2020

1 Some group theory

We let G be a group. We look at the following two sets related to the group G.

Definition 1.1. The vector space of complex valued functions on the group G is

$$L^2(G) := \{f : G \to \mathbb{C}\}$$

The dual group or character group of G is defined as

$$\hat{G} := \left\{\varphi : G \to S^1 \subseteq \mathbb{C} \mid \varphi \text{ is a homomorphism}\right\}$$

Exercise 1
Find the dual group of the cyclic group $\mathbb{Z}_n$ for $n \in \mathbb{N}, n \geq 2$.

Exercise 2
Prove the following:

1. $L^2(G) \cong \mathbb{C}^{|G|}$ for any group G.
2. $\hat{G}$ is a group.
3. Let G be a finite group. $L^2(G)$ is an inner product space with respect to the inner product

$$\langle f|h\rangle = \frac{1}{|G|}\sum_{x\in G}\overline{f(x)}h(x)$$

   for $f, h \in L^2(G)$.

We will be looking at finite abelian groups G for a very special reason which is brought out in the following theorem and the subsequent claims.

Theorem 1.2 (Fundamental theorem of finite abelian groups)**.** *A finite abelian group G is isomorphic to the direct product of cyclic groups of prime-power orders. This decomposition is unique up to the order in which the factors are written.*

Corollary 1.3. *If G is a finite abelian group then $G \cong \hat{G}$.*

Proposition 1.4. *Let G be a finite abelian group. Then:*

1. $\chi \in \hat{G} \implies |\chi(g)| = 1 \ \forall \ g \in G$.
2. *For* $\chi_1, \chi_2 \in \hat{G}$
$$\langle \chi_1 | \chi_2 \rangle = \begin{cases} 1 & \chi_1 = \chi_2 \\ 0 & \textit{otherwise} \end{cases}$$
3. $\hat{G}$ *is an orthonormal basis of* $L^2(G)$.

2 The (discrete) Fourier Transform

Let G be a finite abelian group of order N (we will make this assumption throughout this section). We have already seen that $G \cong \hat{G}$ in that case. Note that this isomorphism is not unique. We fix one and name it $x \mapsto \chi_x$, that is, the character corresponding to $x \in G$ is $\chi_x \in \hat{G}$.

Definition 2.1. For $f \in L^2(G)$ define $\hat{f} \in L^2(G)$ as

$$\hat{f}(g) = \frac{1}{\sqrt{N}} \sum_{x \in G} \overline{\chi_g(x)} f(x)$$

The function $F : L^2(G) \to L^2(G)$ given by $f \overset{F}{\mapsto} \hat{f}$ is called the Fourier Transform.

Proposition 2.2 (Fourier inversion). $f(g) = \dfrac{1}{\sqrt{N}} \displaystyle\sum_{x \in G} \chi_x(g) \hat{f}(x)$

For quantum computation, we will use the cyclic group $G = \mathbb{Z}_N$ with $N = 2^n$. Since any $f \in L^2(\mathbb{Z}_N)$ can be identified with a vector in $\mathbb{C}^N$, in order to find the Fourier transform of a function (that is a vector in $\mathbb{C}^N$) is is enough to look at the action (of Fourier transform) on the vectors in the (canonical) basis $\mathcal{B} = \{|j\rangle\}_{j=0}^{N-1}$ of $\mathbb{C}^N$. Note that this is possible because the Fourier transform is a linear map. This transformation F is given by

$$F|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left\{\frac{2\pi i}{N} jk\right\} |k\rangle$$

If we execute it naively, the time complexity to find all the transforms will be $O(N^2)$.

2.1 Fast Fourier Transform

The best (in terms of time complexity) known classical algorithm is the Fast Fourier Transform which is a slight modification of the Fourier Transform. This uses divide and conquer to bring down the time complexity to $O(N \lg N)$. This will be evident from the following:

$$
\begin{aligned}
F\left|j\right\rangle &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left\{\frac{2\pi i}{N} jk\right\} \left|k\right\rangle \\
&= \frac{1}{\sqrt{2}} \left[\frac{1}{\sqrt{N/2}} \sum_{k=0}^{N/2-1} \exp\left\{\frac{2\pi i}{N/2} jk\right\} \left|2k\right\rangle + \frac{1}{\sqrt{N/2}} \sum_{k=0}^{N/2-1} \exp\left\{\frac{2\pi i}{N} j(2k+1)\right\} \left|2k+1\right\rangle\right] \\
&= \frac{1}{\sqrt{2}} \left[\frac{1}{\sqrt{N/2}} \sum_{k=0}^{N/2-1} \exp\left\{\frac{2\pi i}{N/2} jk\right\} \left|2k\right\rangle + \frac{\exp\left\{\frac{2\pi i j}{N}\right\}}{\sqrt{N/2}} \sum_{k=0}^{N/2-1} \exp\left\{\frac{2\pi i}{N/2} jk\right\} \left|2k+1\right\rangle\right]
\end{aligned}
$$

The above is popularly known as the Danielson-Lanczos Lemma. This procedure can be applied recursively, and treating the even and odd parts separately in each step helps to avoid redundant calculations thus reducing the time complexity.

2.2 Quantum Fourier Transform

Exercise 3
Verify that the above transformation F is unitary and its matrix with respect to the basis $\mathcal{B}$ is given by $F = (F_{j,k})_{N\times N}$ where $F_{jk} = \frac{1}{\sqrt{N}} \exp\left\{\frac{2\pi i}{N} jk\right\}$.

Proposition 2.3. *Consider the Hilbert space $H = \mathbb{C}^N = C^{2^n} \cong \left(\mathbb{C}^2\right)^{\otimes n}$. And take the basis element $\left|j\right\rangle$ where $j = \sum_{t=1}^{n} j_t 2^{n-t}$ (because $j \in \{0, 1, \ldots, 2^n - 1\}$). Then the Fourier transform F has the following representation:*

$$
F\left|j\right\rangle = F\left|j_1 \ldots j_n\right\rangle = \frac{1}{2^{\frac{n}{2}}} \bigotimes_{l=1}^{n} \left(\left|0\right\rangle + \exp\left\{2\pi i \left(\overline{0.j_{n-(l-1)} \ldots j_n}\right)_2\right\} \left|1\right\rangle\right)
$$

where $\left(\overline{0.j_l \ldots j_n}\right)_2 = \sum_{t=1}^{n-(l-1)} \frac{j_{t+l-1}}{2^t}$.

Proof. Every $\left|k\right\rangle \in \mathcal{B}$ can be expressed as $k = \left(\overline{k_1 \ldots k_n}\right)_2$ as the base-2 expansion. Varying $\left|k\right\rangle \in \mathcal{B}$ is same as varying each $k_t \in \{0, 1\}$.

$$
\begin{aligned}
F\left|j\right\rangle &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left\{\frac{2\pi i}{N} jk\right\} \left|k\right\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \cdots \sum_{k_n=0}^{1} \exp\left\{2\pi i j \sum_{l=1}^{n} \frac{k_l}{2^l}\right\} \left|k_1 \ldots k_n\right\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{k_1, k_2, \ldots, k_n} \bigotimes_{l=1}^{n} \exp\left\{\frac{2\pi i j k_l}{2^l}\right\} \left|k_l\right\rangle \\
&= \frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} \left(\left|0\right\rangle + \exp\left\{\frac{2\pi i j}{2^l}\right\} \left|1\right\rangle\right)
\end{aligned}
$$

Now $\frac{j}{2^l} = \left\lfloor \frac{j}{2^l} \right\rfloor + \frac{j_{n-(l-1)}}{2} + \cdots + \frac{j_{n-1}}{2^{l-1}} + \frac{j_n}{2^l} = \left\lfloor \frac{j}{2^l} \right\rfloor + \left(\overline{0.j_{n-(l-1)} \cdots j_n}\right)_2$. And so we can ignore the integer part in the above (because an integer power of $\exp\{2\pi i\}$ evaluates to 1). Hence, we finally get

$$F\,|j\rangle = \frac{1}{2^{\frac{n}{2}}} \bigotimes_{l=1}^{n} \left(|0\rangle + \exp\left\{2\pi i \left(\overline{0.j_{n-(l-1)} \cdots j_n}\right)_2\right\} |1\rangle\right)$$

$\square$

The quantum circuit to implement the above algorithm is as follows.

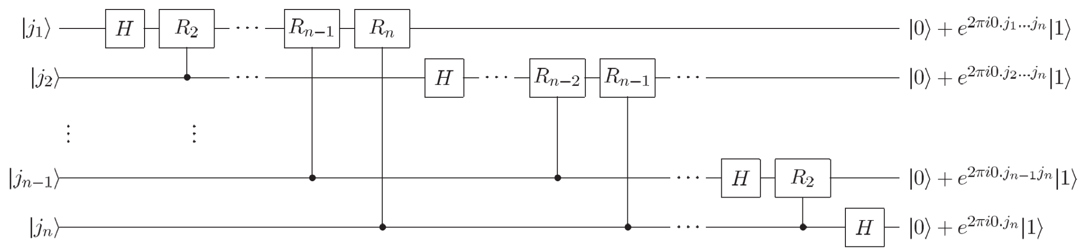

Figure 1: Quantum circuit for Quantum Fourier Transform

The diagram has been taken from the book *Quantum Computation and Quantum Information* by Nielsen and Chuang. The gate H represents the Hadamard gate (though, we have used $\mathcal{H}$ throughout the seminar) and R_k is the gate $R_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp\{\frac{2\pi i}{k}\} \end{bmatrix}$.