Quantum Fourier Transform

Quantum Algorithm Workshop
Lecturer: Zhengyi Han
Spring 2023

1 Fourier Analysis on Abelian Groups

1.1 Character Theory

In this subsection, we consider **Locally Compact Abelian Group (LCA)**.

Example 1. $\mathbb{R}, \mathbb{Z}, \mathbb{T} := \mathbb{R}/\mathbb{Z} \simeq \{e^{2\pi i\theta}\}$ are all LCA. Furthermore, $\mathbb{Z}$ is discrete, and $\mathbb{T}$ is compact.

There is a **unique** and **canonical** (Harr) measurement on LCA (up to a scalar). So we can do integration on such groups, such as the finite sum.

Definition 1. A character of a LCA G is a continuous function $\gamma : G \to \mathbb{C}^\times$, such that,

1. $|\gamma(g)| = 1$,
2. $\gamma(a+b) = \gamma(a)\gamma(b)$.

We denote all such functions by $\mathrm{Hom}(G, \mathbb{T})$ or $\hat{G}$. Actually, $\mathrm{Hom}(G, \mathbb{T})$ is also LCA. The multiplication of the group is defined by the multiplication point-wise. We call $\hat{G}$ is the dual group of G. That is to say that,

Theorem 1. The dual group of an LCA is also an LCA.

Example 2. $\hat{\mathbb{R}} = \mathbb{R}$, $\hat{\mathbb{Z}} = \mathbb{T}$, $\hat{\mathbb{T}} = \mathbb{Z}$, $\widehat{\mathbb{Z}/n\mathbb{Z}} = \mathbb{Z}/n\mathbb{Z}$

1.2 Fourier Transform of Abelian Groups

1.3 Quantum Fourier Transform on Finite Abelian Groups

Let's focus on the quantum Fourier transform on an arbitrary finite abelian group G.
Actually, G is isomorphic to $\hat{G}$. (By the fundamental structure theorem of finite abelian groups and the duality of $\mathbb{Z}/n\mathbb{Z}$) The quantum Fourier transform is:

$$F_G := \frac{1}{\sqrt{|G|}} \sum_{x\in G} \sum_{y\in \hat{G}} \chi_y(x) \, |y\rangle \langle x| \tag{1}$$

Definition 2. Hidden Subgroup Problem (HSP): Given a finite Abelian group G, a function $f : G \to \mathbb{C}$, such that $f(x) = f(y) \Leftrightarrow x - y \in H$, H is a subgroup of G, find the hidden subgroup H.

Example 3. Factoring and discrete logarithm problem are also HSP. It equals finding the size of a cyclic subgroup.

Let's see the standard procedure of HSP:

$$|G\rangle := \frac{1}{\sqrt{G}} \sum_{x \in G} |x\rangle |0\rangle \tag{2}$$

Apply the black-box f oracle:

$$|G\rangle = \frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle |f(x)\rangle \tag{3}$$

We now define the coset state:

$$|x + H\rangle := \frac{1}{\sqrt{|H|}} \sum_{h \in H} |x + h\rangle \tag{4}$$

Then we measure the second register and discard it, we get a random pure state: $|x + H\rangle$. The distribution is uniform on all cosets. Or equivalently, the state can be described as a mixed state:

$$\rho_H := \frac{1}{|H|} \sum_{x \in G} |x + H\rangle \langle x + H| \tag{5}$$

Let's say what happened after applying QFT:

$$|x \hat{+} H\rangle := F_G |x + H\rangle \tag{6}$$

After some calculation:

$$|x \hat{+} H\rangle = \sqrt{\frac{|H|}{|G|}} \sum_{y \in \hat{G}} \chi_y(x) \chi_y(H) |y\rangle \tag{7}$$

here, $\chi(H) = \frac{1}{|H|} \sum_{h \in H} \chi(h)$. We want to argue that, characters only trivial on the subgroup H will count. By the orthogonality of characters:

$$\langle \chi_y, \chi_{y^*} \rangle = \delta_{y,y^*} \tag{8}$$

Let's take χ_{y^*} as a trivial character on H. Then:

$$|x \hat{+} H\rangle = \sqrt{\frac{|H|}{|G|}} \sum_{y \in \hat{G}} \chi_y(x) \sum_{h \in H} \chi_y(h) \chi_{y^*}(h) |y\rangle \tag{9}$$

$$= \sqrt{\frac{|H|}{|G|}} \sum_{y : \chi_y(H) = 1} \chi_y(x) |y\rangle \tag{10}$$

Considering the mixed state ρ_H before applying the Fourier transform, we denote it as $\hat{\rho_H}$ then. After some calculation, we can find that

$$\hat{\rho}_H = \frac{|H|}{|G|} \sum_{y : \chi_y(H) = 1} |y\rangle \langle y| \tag{11}$$

That is to say, $\hat{\rho}_H := F_G \rho_H F_G^\dagger$ is diagonal. (Circulant matrix can be diagonalized by Fourier transform.) So we can measure the state under the computational basis without losing any information.

Once we get the result χ_y after measuring, we can calculate its kernal $\ker(\chi_y)$. It's clearly that $H < \cap\ker(\chi_y)$. So the problem is how many times should we measure to get the hidden subgroup H? Suppose after some measuring, we get $K := \cap\ker(\chi_y)$. If $K \not< \ker(\chi_y)$, $|K \cap \ker(\chi_y)| \leq |K|/2$. So the size decreased to its half. What's probability that we get such χ_y? It's greater than $1/2$ by Lagarange's theorem.

2 Fourier Analysis on Finite Non-Abelian Groups

2.1 Representation Theory

We need to list some basic results of representation of finite groups. A representation is a homomorphism $\sigma : G \to GL(V)$, $d_\sigma := \dim(V)$. The chatacter of a representation is a function:$\chi_\sigma(g) := \mathrm{Tr}(\sigma(g))$.

1. χ is a conjugate class function.
2. Given two representations, they are isomorphic if they have the same character.
3. For characters of irreducible representations, $\langle \chi, \chi \rangle = 1$, $\langle \chi, \chi' \rangle = 0$ if they are not isomorphic.
4. Given two irreducible representations ϕ, ψ,
   - $\langle \phi_{ij}, \psi_{kl} \rangle = 0$
   - $\langle \phi_{ij}, \psi_{kl} \rangle = 1/n$ if $i = k, j = l$. Otherwise 0.
5. For all irreducible representations $\sigma_1, \cdots, \sigma_m$ of G, $\sum \sigma_i^2 = |G|$.
6. $L \simeq \bigoplus(\sigma \otimes I_{d_\sigma})$, $R \simeq \bigoplus(I_{d_\sigma}) \otimes \sigma^*$

2.2 Fourier Transform on Finite Non-Abelian Groups

The Fourier transform on finite Abelian groups is a ring isomorphism $F : (L(G), +, *) \to (L(\hat{G}), +, \cdot)$ (Convolution Theorem). In Non-Abelian cases, we need to transform the function to matrixes.

By Schur's Orthogonality, $L(G) \simeq \mathbb{C}^{|G|}$. Let $\phi^{(1)}, \cdots, \phi^{(m)}$ be all irreducible representations, $\sqrt{d_k}\phi_{ij}^{(k)}$ form an orthonormal basis for $L(G)$. So we can define the Fourier transform.

Definition 3. We define the Fourier transform $F : L(G) \to M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})$ by $F(f) = (\hat{f}(\phi^{(1)}), \cdots, \hat{f}(\phi^{(m)}))$, where

$$\hat{f}(\phi^{(k)})_{ij} = |G| \langle f, \phi_{ij}^{(k)} \rangle = \sum f(g)\overline{\phi_{ij}^{(k)}}(g)$$

Such transform is an isomorphism of vector space. Furthermore, it's a ring isomorphism.

We consider the quantum case. $|x\rangle$ is a basis of $L(G)$, it is mapped to the vector space $\bigoplus(\mathbb{C}^{d_\sigma} \times \mathbb{C}^{d_\sigma})$

$$|\hat{x}\rangle := \sum_\sigma \frac{d_\sigma}{\sqrt{|G|}} |\sigma, \sigma(x)\rangle \tag{12}$$

where,

$$|\sigma(x)\rangle := \sum_{j,k} \frac{\sigma(x)_{jk}}{\sqrt{d_\sigma}} |j,k\rangle \tag{13}$$

So we can write the quantum Fourier transform explicitly:

$$F_G := \sum |\hat{x}\rangle \langle x| = \sum_x \sum_\sigma \sqrt{\frac{d_\sigma}{|G|}} \sum_{j,k} \sigma(x)_{j,k} |\sigma, j, k\rangle \langle x| \tag{14}$$

Since the irreducible decompose is not unique, the Fourier transform is also not defined uniquely.

Using the orthogonality, we can verify that F_G is unitary.

In Abelian case, the regular representation $U(x)$ commutes with the density matrix ρ_H, ρ_H can be diaganolized by Fourier transform. So $U(x)$ can also be diaganolized by Fourier transform. While in the non-Abelian case, the left (right) regular representations is blocked diagnoalized.

$$\hat{L}(x) := F_G L(x) F_G^\dagger = \sum |\hat{xy}\rangle \langle \hat{y}| \tag{15}$$

$$= \sum_\sigma \sum_{j,k,l} \sigma(x)_{j,l} |\sigma, j, k\rangle \langle \sigma, l, k| \tag{16}$$

$$= \bigoplus (\sigma(x) \otimes I_{d_\sigma}) \tag{17}$$

2.3 Fourier Sampling

Let's consider HSP in non-Abelian case. The coset state $|gH\rangle := \frac{1}{\sqrt{|H|}} \sum |gh\rangle$. Since cosets are uniform, the mixed state can be described as $\rho_H := \frac{1}{|G|} \sum |gH\rangle \langle gH|$. The regular representations play an important role in the analysis of such functions. This is because:

$$|gH\rangle = \frac{1}{\sqrt{|H|}} \sum R(h) |g\rangle . \tag{18}$$

Hence we can rewrite the mixed state using the right regular representation.

$$\rho_H = \frac{1}{|G|} \sum R(h) \tag{19}$$

So according to the above study of regular representation, we kown that the density matrix ρ_H is block-diagonalized by Fourier transform.

$$\hat{\rho}_H = F_G \rho_H F_G^\dagger = \frac{1}{|G|} \bigoplus (I_{d_\sigma} \otimes \sigma(H)^*) \tag{20}$$

, where $\sigma(H) := \sum \sigma(h)$.

The probability that result is σ is:

$$\Pr(\sigma) = \frac{1}{|G|} \mathrm{Tr}(I_{d_\sigma} \otimes \sigma(H)^*) = \frac{d_\sigma}{|G|} \sum \chi_\sigma(h)^* \tag{21}$$

So how many times do we need to recover the information of H?

If H is a normal subgroup. This is similar to Abelian case. Since $gHg^{-1} = H$

$$\sigma(H) = \frac{1}{|G|} \sum \sigma(ghg^{-1}) \tag{22}$$

It commutes with $\sigma(g)$ for all $g \in G$. By Schur's Lemma, σ is proportional to identity. Hence $\hat{\rho}_H$'s blocks are all a multiple of identity. We can measure the state in the computational basis.

$$\Pr(\sigma) = d_\sigma^2 |H|/|G| (H \leq \ker\sigma). \tag{23}$$

It is similar to the Abelian case, which can be done in polynomial time. Measuring a diagonal density matrix under computational basis will reveal all information. But for non-normal cases, we can not get all information just by measuring the name register of representations.

What does this mean? Certainly, we can get the result of σ, but the probability can not be polynomially small. In normal case, its like abelian case, the probability is proportional to the ratio of the size of H and G, which might not hold for the nonabelian cases.

To get more information of the state, we need to measure more elements. Strong Fourier sampling not only measures the name of the representations, but also measure the row and column element of the matrix.