CS 593/MA 592 - Intro to Quantum Computing
Spring 2024
Thursday, February 22 - Lecture 7.2

Today's scribe: Jun Kil [Note: not proofread by Eric]

Reading:
Agenda:

1. Group Algebra
2. Irreps of $\mathbb{Z}/n\mathbb{Z}$
3. Fourier Transform on $\mathbb{Z}/n\mathbb{Z}$
4. Quantum Fourier Transform (QFT)

1 Group Algebra

Note: Within the branch of math called algebra, there is a specific type of algebraic structure called an "algebra". An "algebra" is a vector space with a distributive vector multiplication.

Let G be any finite group. Define $\mathbb{C}G$ to be the Hilbert space with an orthonormal basis given by:

$$|g\rangle, g \in G$$

$$dim(\mathbb{C}G) = |G|$$

$\mathbb{C}G$ is not just a Hilbert space: We can multiply vectors in $\mathbb{C}G$ by extending the group multiplication linearly.

$$|g\rangle \cdot |h\rangle = |gh\rangle$$

$$(\sum_{g\in G} bg\,|g\rangle)(\sum_{h\in G} ch\,|h\rangle) = \sum_{g,h} bgch\,|gh\rangle$$

$\mathbb{C}G$ with this multiplication is called the group algebra of G. The group algebra has an obvious representation of G on it:

$$\rho : G \to GL(\mathbb{C}G), g \mapsto Lg$$

where

$$Lg : \mathbb{C}G \to \mathbb{C}G, |h\rangle \mapsto |gh\rangle$$

This is called the (left) regular representation of G.
We can think of a general vector $|\psi\rangle \in \mathbb{C}G$

$$|\psi\rangle = \sum \psi_g\,|g\rangle$$

as a function $\psi : G \to \mathbb{C}, g \mapsto \psi_g$
Roughly: $\mathbb{C}G = \bigoplus_{\rho\in \mathrm{Irrep}(G)} (\mathbb{C}G)_\rho$ where $(\mathbb{C}G)_\rho$ is the set of functions $G \to \mathbb{C}$ that are "ρ periodic".
Fourier transform is essentially a way of decomposing a function $\psi : G \to \mathbb{C}$into its "ρ periodic pieces". Making this precise for non-abelian groups ought to be done with "character theory". Instead, now we will prove this directly for $G = A = \mathbb{Z}/N\mathbb{Z}$, where A is an abelian group.

2 Irreps of $\mathbb{Z}/n\mathbb{Z}$

Last time: Irreps of A are the same thing as 1-dim representation which we might as well assume it is unitary, so, the irreps of A are given by $\hat{A} := \{\rho : A \to U(1) | \rho \text{ a homomorphism}\}$, with $A = \mathbb{Z}/N\mathbb{Z} = \{0, 1, ..., N-1\}$.
(Note: we use '+' notation for A not '$\cdot$' notation whereas $\hat{A}$ is multiplicative)
Since $A = \mathbb{Z}/N\mathbb{Z}$ is cyclic and generated by 1, every representation $\rho : A \to U(1)$ is determined by $\rho(1)$. On the other hand, $U(1) = \{e^{2\pi i\theta} | 0 \leq \theta < 1\}$. Given ρ, write $\rho(1) = e^{2\pi i\theta}$for some $0 \leq \theta_1 < 1$.
Since $\rho$is a homomorphism, $\rho(k) = \rho(1)^k = e^{2\pi i\theta_1 k}$. Moreover, $e^{2\pi i\theta_1 0} = \rho(0) = \rho(N) = \rho(1)^N = e^{2\pi i\theta_1 N}$. Thus $\theta_1 \in \{\frac{0}{N}, \frac{1}{N}, \frac{2}{N}, ..., \frac{N-1}{N}\}$.
In fact, every such theta gives a valid representation $\rho : A \to U(1)$. Equivalently, every irrep of $\mathbb{Z}/N\mathbb{Z}$ is of the form $\rho_k : \mathbb{Z}/N\mathbb{Z} \to U(1), j \mapsto e^{2\pi ikj/N}$.

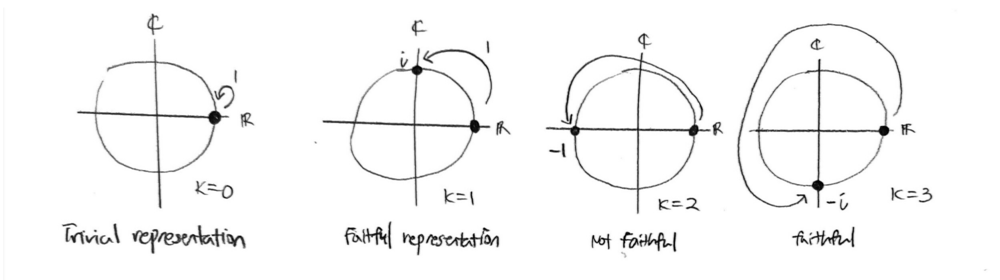


Figure 1: Ex. $\mathbb{Z}/N\mathbb{Z}$ 4 Irreps

What is $\otimes$ of representation?

$$\rho : G \to GL(v)$$
$$\rho' : G \to GL(w)$$
$$\Rightarrow \rho \otimes \rho' : G \to GL(v \otimes w), g \mapsto \rho(g) \otimes \rho(g').$$

3 Fourier transform on $\mathbb{Z}/N\mathbb{Z}$ (Discrete 1-dim Fourier transform)

Write A=$\mathbb{Z}/N\mathbb{Z}$. The group algebra $\mathbb{C}A$ is a representation of A. $\mathbb{C}A$ has a standard basis $\{|a\rangle \, | a \in A\}$. As a function, what is $|a\rangle$?

$$|a\rangle : A \to \mathbb{C}, b \mapsto 1 \text{ if } b = a, 0 \text{ otherwise. i.e.} |a\rangle = \delta_{aix}$$

On the other hand, $\mathbb{C}A = \bigoplus_{\rho \in \hat{A}} (\mathbb{C}A)_\rho$, where $(\mathbb{C}A)_\rho \subseteq \mathbb{C}A$ consisting "ρ periodic" functions $A \to \mathbb{C}$. A priori, $(\mathbb{C}A)_\rho$ could be multidimensional (for non-abelian G, there's always an irrep ρ such that $(\mathbb{C}G)_\rho$ is greater than 1 dimensional).
In fact, $(\mathbb{C}A)_\rho$ can be identified in our case by an elementary observation: $\hat{A} \subset \mathbb{C}A$. That is, every irrep $\rho : A \to U(1) \subseteq \mathbb{C}$ is an element of $\mathbb{C}A$. Intuition: ρ is a "discretized cosine with frequency ρ".

Lemma: $\hat{A}$is an orthogonal basis of $\mathbb{C}A$.
Proof:
Pick $\rho_k, \rho_l \in \hat{A}, |\rho_k\rangle = \sum_{a \in A} \rho_k(a) |a\rangle = \sum_{a \in A} e^{2\pi ika/N} |a\rangle$
Likewise $|\rho_l\rangle = \sum_{b \in A} e^{2\pi ikb/N} |b\rangle$
$\langle \rho_l | \rho_k \rangle = \sum_a e^{2\pi ia(k-l)/N}$.
If $k = l, \langle \rho_l | \rho_k \rangle = \sum_{a \in A} 1 = |A| = N$.
If $k \neq l, \langle \rho_l | \rho_k \rangle = 0$ by symmetry.

Definition: The Fourier basis of $\mathbb{C}A$ is the (ordered) Orthonormal Basis

$$\frac{1}{\sqrt{N}}\left|\rho_0\right\rangle, \frac{1}{\sqrt{N}}\left|\rho_1\right\rangle, \ldots, \frac{1}{\sqrt{N}}\left|\rho_{N-1}\right\rangle$$

The above lemma is saying that every function $\psi : A \to \mathbb{C}$ is a unique linear combination of these periodic functions.

Definition: The Fourier transform $\mathcal{F}$ of $\mathbb{C}\mathbb{Z}/N\mathbb{Z}$ is the unitary transformation $\mathbb{C}\mathbb{Z}/N\mathbb{Z} \to \mathbb{C}\mathbb{Z}/N\mathbb{Z}, |a\rangle \mapsto \frac{1}{\sqrt{N}}\left|\rho_a\right\rangle$

$$\mathcal{F}_{\mathbb{Z}/2\mathbb{Z}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \mathrm{H}$$

$$\mathcal{F}_{\mathbb{Z}/4\mathbb{Z}} = \frac{1}{\sqrt{4}}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

4 Quantum Fourier Transform (QFT)

The QFT is a realization of $\mathcal{F}_{\mathbb{Z}/2\mathbb{Z}}$ as a quantum circuit on n qubits. This is sensible because $\mathbb{C}\mathbb{Z}/2^n\mathbb{Z} \to (\mathbb{C}^2)^{\otimes n}$.

$|a\rangle \mapsto |a_1, a_2, ..., a_n\rangle$ (binary representation of a, where $a \in \{0, ..., 2^{n-1}\}$ and $a = a_1 a_2 ... a_n$ is binary rep of such an integer.

The trick to getting a circuit rep of $\mathcal{F}_{\mathbb{Z}/2\mathbb{Z}}$ is to use binary functions.

$$\mathcal{F}_{\mathbb{Z}/2^n\mathbb{Z}}|a\rangle = \frac{1}{2^{n/2}}\sum_{b=0}^{2^n-1} \exp(2\pi i\, ab/2^n)|b\rangle$$

want to think of this as a function in binary

$$= \frac{1}{2^{n/2}}\sum_{b_1=0}^{1}\sum_{b_2=0}^{1}\cdots\sum_{b_n=0}^{1} \exp\left[2\pi i a\left(\sum_{\ell=1}^{n} b_\ell 2^{-\ell}\right)\right]|b_1 b_2 \cdots b_\ell\rangle$$

$$= \frac{1}{2^{n/2}}\sum_{b_1=0}^{1}\cdots\sum_{b_n=0}^{1}\left[\bigotimes_{\ell=1}^{n} \exp\left(2\pi i a b_\ell/2^\ell\right)|b_\ell\rangle\right]$$

$$= \frac{1}{2^{n/2}}\bigotimes_{\ell=1}^{n}\left[\sum_{b_\ell=0}^{1} \exp(2\pi i a b_\ell/2^\ell)|b_\ell\rangle\right]$$

$$= \frac{1}{2^{n/2}}\bigotimes_{\ell=1}^{n}\left(|0\rangle + e^{2\pi i a/2^\ell}|1\rangle\right)$$

$$= \frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi i a/2^1}|1\rangle\right)\left(|0\rangle + e^{2\pi i a/2^2}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i a/2^n}|1\rangle\right)$$

Note $\exp(2\pi i a/2^\ell) = \exp(2\pi i\, a_1 a_2 \cdots a_{n-\ell} \underset{\text{decimal}}{.} a_{n-\ell+1}\cdots a_n)$

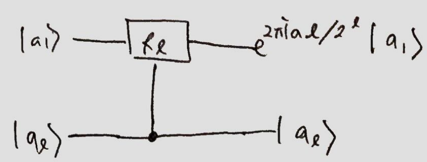
$$= \exp(2\pi i\, 0.a_{n-\ell+1}\cdots a_n)$$

$$\mathcal{F}_{\mathbb{Z}/2^n\mathbb{Z}}|a\rangle = \frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi i 0.a_n}|1\rangle\right)\otimes\left(|0\rangle + e^{2\pi i 0.a_{n-1}a_n}|1\rangle\right)\otimes \cdots \otimes\left(|0\rangle + e^{2\pi i 0.a_1\cdots a_n}|1\rangle\right)$$

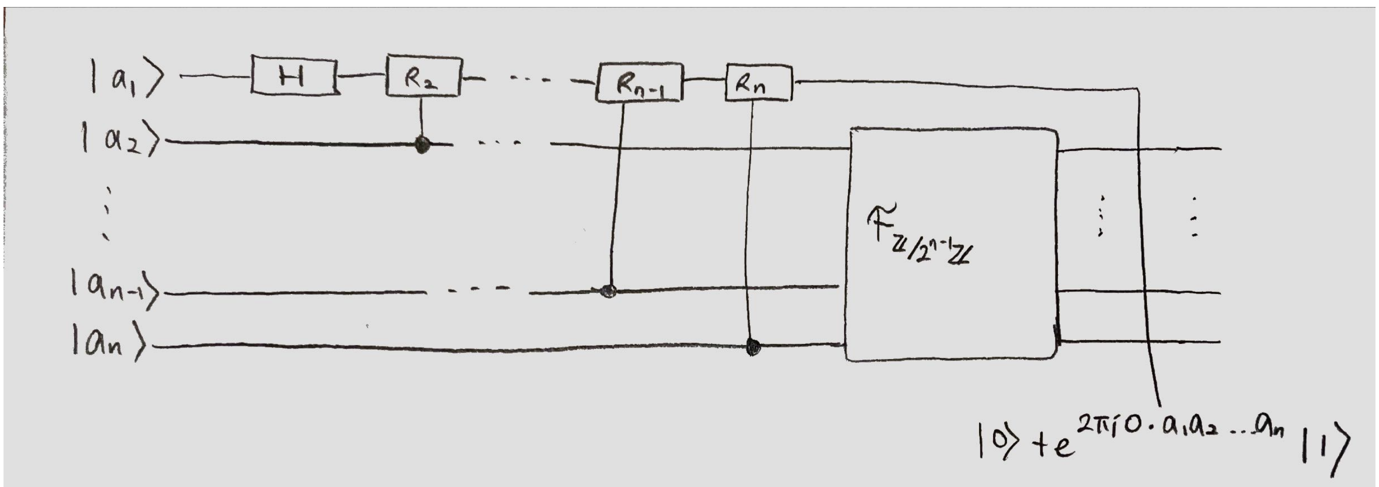
Notation: $R_\ell = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^\ell}\end{pmatrix}$

relative rotation gate.

controlled R_ℓ



6



$|a_1\rangle$
$|a_2\rangle$
$|a_{n-1}\rangle$
$|a_n\rangle$
H
R_2
R_{n-1}
R_n
$\tilde{F}_{\mathbb{Z}/2^{n-1}\mathbb{Z}}$
$|0\rangle + e^{2\pi i 0.a_1a_2\ldots a_n}|1\rangle$