CS 682: Quantum Computing	Lecture 11: August 22, 2008
Lecturer: Piyush P. Kurur	*Scribe: Lovy Singhal*

11.1 Characters of finite abelian groups

We will now develop some pre-requisite mathematics required to understand Shor's famous algorithm.

Let $(A, +)$ be a finite abelian group of order n, with the identity being denoted by 0 and $-a$ denoting the inverse of an element a. The set $L^2(A)$ of all functions $f : A \to \mathbb{C}$ is a Hilbert space, with the vector addition and scalar multiplication defined as follows:

$$\begin{aligned} f + g : &\quad a \mapsto f(a) + g(a) \\ \alpha f : &\quad a \mapsto \alpha f(a) \end{aligned}$$

For every $a \in A$, there is a natural correspondence with the vector $|a\rangle \in L^2(A)$ which stands for the point function f_a given by

$$\begin{aligned} f_a(a) &= 1 \\ f_a(b) &= 0 \quad \forall\, b \neq a \end{aligned}$$

The set $\{|a\rangle \mid a \in A\}$ forms a *point basis* of $L^2(A)$ such that any $f \in L^2(A)$ is expressible as

$$f = \sum_{b \in A} f(b)\,|b\rangle$$

We now move on to define the inner product on the above mentioned basis elements of $L^2(A)$. For all $x, y \in A$, the inner product $\langle\ ,\ \rangle$ is defined as

$$\langle x|y\rangle = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{otherwise} \end{cases}$$

The above definition can be extended sesquilinearly to the whole of the Hilbert space $L^2(A)$, such that for any $|\psi\rangle = \sum_{x \in A} \alpha_x\,|x\rangle\,, |\phi\rangle = \sum_{x \in A} \beta_x\,|x\rangle \in L^2(A)$, the inner product $\langle\psi|\phi\rangle$ is given by $\sum_{x \in A} \overline{\alpha_x}\beta_x$.

It is easy to see that $L^2(A)$ is an n-dimensional Hilbert space with the basis elements indexed by A instead of the usual $\{\,1, 2,\ \ldots, n\,\}$.

Definition 11.1.1. *A **character** of a finite abelian group A is a group homomorphism $\chi : A \to \mathbb{C}^\times = (\mathbb{C}\backslash\{0\}, \times)$.*

Example 11.1. The trivial character given by $\chi(a) = 1,\ \forall\ a \in A$, where A is a finite abelian group.

Example 11.2. Let $A = (\frac{\mathbb{Z}}{2\mathbb{Z}}, +)$. A non-trivial character of A is given by $\chi(0) = 1,\ \chi(1) = -1$. It can be easily checked that χ is a homomorphism.

Example 11.3. Let $A = (\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$ and ζ be an n-th root of unity. $\chi(x) = \zeta^x$ is a character of A.

χ is a character, i.e., χ is a group homomorphism from A to $\mathbb{C}^\times$. Let $\chi(1) = \omega$. This implies

$$\chi(a) = \chi\big(\overbrace{1 + 1 + \cdots + 1}^{a \text{ times}}\big) = \overbrace{\chi(1) \cdot \chi(1) \cdots \chi(1)}^{a \text{ times}} = \omega^a, \quad a \in \frac{\mathbb{Z}}{n\mathbb{Z}}$$

since χ is a homomorphism. Also,

$$\chi(0) = \big(\overbrace{1 + 1 + \cdots + 1}^{n \text{ times}}\big) = \omega^n = 1.$$

since any group homomorphism maps identity to identity. Hence, we see that χ is a character of $\frac{\mathbb{Z}}{n\mathbb{Z}}$ only if $\chi(1) = \omega$ is an an n-th root of unity. Since there are exactly n distinct n-th roots of unity for 1 to be mapped to under χ and the value of $\chi(1)$ completely determines the homomorphism as argued above, *the cyclic group $\frac{\mathbb{Z}}{n\mathbb{Z}}$ has exactly n characters.*

11.1.1 The character group

Let A be a finite abelian group and let $\underline{1}$ denote the trivial character of A. We define the multiplication of two characters of A as follows:

$$(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a), \quad \forall\ a \in A$$

Under the above-defined multiplication operation, the characters of A form an abelian group, with the trivial character $\underline{1}$ being the identity element.

$$\chi \cdot \underline{1}(a) = \chi(a) \cdot \underline{1}(a) = \chi(a) \cdot 1 = \chi(a)$$

and the inverse χ^{-1} of χ given by

$$\chi^{-1}(a) = \frac{1}{\chi(a)}.$$

Note that χ^{-1} exists as $\chi(a) \neq 0$ for any $a \in A$.