# Quantum Computing (Fall 2013) Instructor: Shengyu Zhang.

# Lecture 3 Hidden Subgroup Problem 1: Group Representations

Studies of Hidden Subgroup Problem for non-Abelian groups often need knowledge of group representations, which is the subject of this lecture.

## Linear representation of finite groups

Suppose that is a vector space over . The *general linear group* is the group of invertible linear operators from to itself. Here we only consider the case . The group can also be identified with the group of invertible matrices in .

For a finite group , a linear representation is a *homomorphism* . The dimension of is called the *degree* of , denoted by . (Homomorphism: The map is a *homomorphism* if .) Note that this implies that , and where is the identify element of the group .

*Example* 1. *Trivial representation*: . Here the degree .

*Example* 2. *Regular representation*: . The left regular representation is defined by , and the right regular representation is defined by . Here the degree

Two representations and are *isomorphic* if there is an invertible linear operator s.t. . Intuitively, it means that the two representations are the same up to a change of basis.

For a representation , a subspace of is called *-invariant* if

**Claim**. If is -invariant, then there is another subspace s.t. , and is also -invariant.

See [Ser77] for two proofs. By this result, we know that if there is a -invariant subspace , then for a subspace , and the representation can also be decomposed into the direct sum of two *subrepresentations*, namely . In matrix form, is a block diagonal matrix .

If doesn’t have any nontrivial -invariant subspace, we call *irreducible*. We use to denote the set of irreducible representations of . We sometimes use “irrep” as a shorthand for “irreducible representation”.

**Fact**. Every representation is isomorphic to a direct sum of irreducible representations.

An important result about irreducible representations is the following Schur’s lemma.

**Theorem** (Schur’s lemma). For two irreducible representations and with degree and , respectively, assume that there is a matrix s.t. . If is not isomorphic to , then . If and , then for some real number .

*Proof*. See [Ser77].

This lemma can be used to prove the following fundamental orthogonality theorem.

**Theorem**. For any two different irreducible representations and in matrix form, and any , , it holds that  
When and take unitary matrices, then the above equality changes to *Proof*. See [Ser77]

## Character theory

For a representation , its character is simply a function defined by , where is the trace---sum of eigenvalues. Note that . A character is *irreducible* if it is the character of an irreducible representation.

The following theorem is a simple corollary of the orthogonality of irreducible representations.

**Theorem**. Different irreducible characters and are orthogonal: .

Two elements and are called *conjugate* if s.t. . It’s an equivalent relation and thus partitions into *conjugacy classes*. *Class functions* are constant for members of the same conjugacy class. It is not hard to see that characters are class functions.

For two complex-valued functions and on , define two inner products

and

where the superscript \* is the complex conjugate. These two inner products are the same if one of the functions is a character, due to the following fact.

**Fact**. For a character of , .

*Proof*. , where ’s are the eigenvalues of .

## Regular representation and Fourier transform

Recall the left regular representation and the right regular representation . The following equalities hold.

and . (1)

In fact, these hold for the same isomorphism, which is the *Fourier transform* over . Formally, define the Fourier transform by the following.

, where .

In other words, the Fourier transform is  
Note that depends on the choice of basis for each irrep of dimension greater than 1.

**Theorem**. The Fourier transform simultaneously decomposes the left and right regular representations and into their irreducible components.

Proof. We verify for left regular representation, and the case for is similar.



The identity Eq.(1) also implies the following basic fact.

**Fact**. .

## Abelian groups

For a cyclic group , the irreps are for . The Fourier transform is . For a finite Abelian group, suppose it is isomorphic to , then the irreps are where , and the Fourier transform is

For Abelian groups, all irreps are one-dimensional. The converse is also true: Any non-Abelian group has an irrep with degree strictly larger than 1.

One can also note that Abelian groups have the property that , which non-Abelian groups do not enjoy.

## Note

A good (and concise) reference for group representation is [Ser77]. [CvD10] also has an appendix for some basic knowledge about group representation, though it takes a matrix (instead of operator) view. For general introduction of algebra, see [Art10]. For more extensive introduction of abstract algebra, a standard textbook is [DF03].

## Reference

[Art10] Michael Artin, Algebra, 2nd edition, *Pearson*, 2010.

[CvD10] Andrew M. Childs and Wim van Dam, Quantum algorithms for algebraic problems, *Reviews of Modern Physics*, Volume 82, January–March 2010.

[DF03] David S. Dummit and Richard M. Foote, Abstract Algebra, Wiley, 2003.

[Ser77] Jean-Pierre Serre, Linear representations of finite groups, Springer-Verlag, 1977.

## Exercise

1. Prove that characters are class functions, namely . Also prove another property: .
2. Check that the Fourier transform defined is unitary.