Hidden Subgroups and Quantum Computation

Lecture 06

Dheeran E. Wiggins

Summer 2025
Illinois Mathematics and Science Academy

July 25, 2025

Overview

1. Representations
2. Characters
3. Abelian Groups
4. Outlook

Today we will work through the essentials of the complex representation theory of finite groups.

Representation theory is beautiful in its own right, but it is also incredibly powerful in mathematical and physical applications. In particular, it allows us to define a QFT for arbitrary finite groups G.

I will be omitting proofs, as I did when discussing the rudiments of groups and vector spaces, for the sake of time. I highly recommend working through some of the claimed results on your own time–most are just computational.

Let G be a finite group. Let $\mathcal{V}$ be a finite dimensional $\mathbb{C}$-linear space.

Denote by $\mathrm{Aut}(\mathcal{V})$ the group of all vector space isomorphisms

$$\varphi : \mathcal{V} \to \mathcal{V}.$$

We call such φ the automorphisms of $\mathcal{V}$. When discussing representation theory, it is a bit more common to write $\mathrm{GL}(\mathcal{V})$ for the group $\mathrm{Aut}(\mathcal{V})$.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

A representation of G is a group homomorphism $\rho : G \to \mathrm{GL}(\mathcal{V})$.

Since $\dim(\mathcal{V}) = n$ is finite, we know that for all $g \in G$, $\rho(g)$ is effectively a matrix in $\mathbb{M}_n(\mathbb{C})$. We will take for granted that we can choose our basis in such a way that ρ is a unitary matrix, i.e.,

$$\rho(g)^\dagger \rho(g) = \rho(g)\rho(g)^\dagger = I.$$

An isomorphism of representations $\rho : G \to \mathrm{GL}(\mathcal{V})$ and $\tau : G \to \mathrm{GL}(\mathcal{W})$ is a linear isomorphism $\varphi : \mathcal{V} \to \mathcal{W}$ such that for all $g \in G$ and $v \in \mathcal{V}$,

$$\rho(g)v = \tau(g)\varphi(v).$$

An irreducible representation $\rho : G \to \mathrm{GL}(\mathcal{V})$ is one for which whenever a subspace $\mathcal{W} \subseteq \mathcal{V}$ admits $\rho(G)(\mathcal{W}) \subseteq \mathcal{W}$, we either have $\mathcal{W} = \mathcal{V}$ or $\mathcal{W} = 0$.

Given a nonzero, proper subspace $\mathcal{W} \subseteq \mathcal{V}$ such that $\rho(G)\mathcal{W} \subseteq \mathcal{W}$, then there exists a subspace $\mathcal{W}'$ such that $\mathcal{V} = \mathcal{W} \oplus \mathcal{W}'$ and $\rho(G)\mathcal{W}' \subseteq \mathcal{W}'$.

We have restricted representations $\rho_1 : G \to \mathrm{GL}(\mathcal{W})$ and $\rho_2 : G \to \mathrm{GL}(\mathcal{W}')$ such that

$$\rho = \rho_1 \oplus \rho_2.$$

This can be continued until $\rho = \rho_1 \oplus \cdots \oplus \rho_k$, where ρ_j is irreducible for all $1 \le j \le k$.

The decomposition into irreducibles is unique up to representation isomorphism and reordering.

Write $d_\rho = \dim(\mathcal{V})$ for the dimension of a representation $\rho : G \to \mathrm{GL}(\mathcal{V})$.

Up to representation isomorphism, each finite group G has a finite number of irreducible representations ρ. The set of all such ρ, up to isomorphism, is denoted $\widehat{G}$. Note that the order

$$|G| = \sum_{\rho \in \widehat{G}} d_\rho^2.$$

A character of a representation ρ is a homomorphism $\chi_\rho : G \to \mathrm{GL}(\mathbb{C}) = \mathbb{C}^\times$ given by $g \mapsto \mathrm{tr}(\rho(g))$.

Equivalently, we could define a **character** to be a general group homomorphism $\chi : G \to \mathbb{C}^\times$.

Let $x, y \in G$. We say x and y are conjugate if there exists a $g \in G$ so that $gxg^{-1} = y$.

The subset of G of all conjugates of an element $x \in G$ is called the conjugacy class $\mathrm{Cl}(x) \subseteq G$.

Observe that if χ is a character, then χ is fixed on the conjugacy class $\mathrm{Cl}(x)$ for all $x \in G$:

$$\chi(gxg^{-1}) = \chi(g)\chi(x)\chi(g^{-1}) = \chi(x).$$

Let $f_1, f_2 : G \rightrightarrows \mathbb{C}$ be two functions. Then, there is an "inner product"

$$\langle f_1, f_2 \rangle_G = \frac{1}{|G|} \sum_{g \in G} f_1(g) f_2(g)^*.$$

Let $\rho : G \to \mathrm{GL}(\mathcal{V})$ be a representation. Let $\chi_\rho : G \to \mathbb{C}^\times$ be its character. Likewise, let ρ' be an irreducible representation with character $\chi_{\rho'}$. Then, $\langle \chi_\rho, \chi_{\rho'} \rangle_G$ tells us the number of times ρ' is in the decomposition $\rho = \rho_1 \oplus \cdots \oplus \rho_k$ of irreducibles.

If $\rho(g)$ and $\rho'(g)$ are unitary for all $g \in G$, then we have the nice form

$$\langle \chi_\rho, \chi_{\rho'} \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \chi_{\rho'}(g^{-1}).$$

Fix $x \in G$. Then, χ_ρ is fixed on $\mathrm{Cl}(x)$, taking only the value $\chi_\rho(x)$. Then,

$$\sum_{\rho \in \widehat{G}} |\chi_\rho(x)|^2 = \frac{|G|}{|\mathrm{Cl}(x)|}.$$

Consider a $\mathbb{C}$-linear space $\mathcal{V} \simeq \mathbb{C}^{|G|}$. Fix an ordering $G = \{g_1, \ldots, g_n\}$, so that we can write down a basis β of $\mathcal{V}$ given by $\beta = \{e_{g_1}, \ldots, e_{g_n}\}$.

The regular representation $\rho_G : G \to \mathrm{GL}(\mathcal{V})$ is the homomorphism given by $g \mapsto (\rho_G(g) : e_h \mapsto e_{gh})$.

That is, we are just G-permuting the basis.

If $\widehat{G} = \{\rho_1, \ldots, \rho_k\}$, then

$$\rho_G = \rho_1^{\oplus d_{\rho_1}} \oplus \cdots \oplus \rho_k^{\oplus d_{\rho_k}}.$$

The regular character, denoted χ_G, is the character χ_{ρ_G}, which is

$$\chi_G(g) = \sum_{\rho \in \widehat{G}} d_\rho \chi_\rho(g) = \begin{cases} 0, & g \neq e \\ |G|, & g = e. \end{cases}$$

Let G be finite and abelian. Then, it is certainly finitely generated.

Recall that by the fundamental theorem of finitely generated abelian groups, we know that

$$G \simeq \mathbb{Z}^r \oplus \mathbb{Z}/p_1 \oplus \cdots \oplus \mathbb{Z}/p_k.$$

Further, since $|G|$ is finite, we do not have any of the $\mathbb{Z}$ summands.

Thus, we have a form

$$G \simeq \mathbb{Z}/p_1 \oplus \cdots \oplus \mathbb{Z}/p_k.$$

Show that all irreducible representations of G are 1-dimensional.
That is, for all $\rho \in \widehat{G}$, the dimension $d_\rho = 1$.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Observe that for any character χ,

$$\chi(0, \ldots \underbrace{, 1,}_{j\,\mathrm{th}} \ldots, 0) = \zeta_{p_j}^{h_j},$$

for some $h_j \in \{0, 1, \ldots, p_j - 1\}$.

Thus, any character χ is precisely given by a tuple $(h_1, \ldots, h_k)$, in bijective correspondence with elements $h \in G$.

For all $g \in G$, define a character $\chi_g : G \to \mathbb{C}^\times$ by

$$h \mapsto \prod_{j=1}^{k} \zeta_{p_j}^{g_j h_j}.$$

It is easy to see that for all $g, h \in G$,

$$\chi_g(h) = \chi_h(g)$$

and

$$\chi_g(-h) = \frac{1}{\chi_g(h)}.$$

Write $\chi(G)$ for the set of all such χ_g. This is a group, taking the operation $\chi_g \chi_h = \chi_{g+h}$. The identity is $\chi_e : G \mapsto 1$.

It is a brief check to show that $\chi(G) \simeq G$.

Let $X \subseteq G$. An element $g \in G$ is orthogonal to X if $\chi_g(x) = 1$ for all $x \in X$.

Let $H \leq G$ be a subgroup. Then, there is the orthogonal subgroup

$$H^{\perp} = \{g \in G : \chi_g(x) = 1 \text{ for all } x \in H\}.$$

If H is a normal subgroup, then $G/H \simeq H^{\perp}$. Also, $(H^{\perp})^{\perp} = H$.

The abelian QFT is the operator

$$F_G = \frac{1}{\sqrt{|G|}} \sum_{g,h \in G} \chi_g(h) \, |g\rangle\langle h| \, .$$

Of use will be the translation operator

$$\tau_h = \sum_{g \in G} |h + g\rangle\langle g|$$

and the phase operator

$$\varphi_h = \sum_{g \in G} \chi_g(h) \, |g\rangle\langle g| \, .$$

By brute force, if we write

$$|H\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |h\rangle \, ,$$

then $F_G \, |H\rangle = \, |H^{\perp}\rangle$.

Finally, observe the following useful relation:

$$F_G \tau_h = \varphi_h F_G.$$

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Next time we will discuss

(i) the finite abelian HSP.

(ii) standard algorithm like those of Simon and Shor.

After this, we will take a glance at progress on the nonabelian HSP.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN