Study on the Representation Theory of Finite Groups with an Application

KAMESH ROUT

May 11, 2025

IIT PALAKKAD

Outline

Basics of Representation Theory

- A group representation is a homomorphism $\phi : G \to \mathrm{GL}(V)$
- Finite-dimensional vector spaces
- Examples: permutation representation, regular representation

$\mathrm{D}_4 = \langle a, b : a^4 = b^2 = e, b^{-1}ab = a^{-1} \rangle,$ *consider* $\phi : D_4 \to GL(2, R)$

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$\phi : a^i b^j \to A^i B^j$

Subrepresentations and Morphisms

Subrepresentation:

Let $\phi : G \to \mathrm{GL}(V)$ be a representation of a group G.

A subspace $W \subseteq V$ is G-**invariant** if:

1. $\phi_g(w) \in W$ for all $w \in W$ and $g \in G$
2. The restriction $\phi_g|_W \in \mathrm{GL}(W)$

Morphism (Intertwiner):

Let $\phi : G \to \mathrm{GL}(V)$ and $\psi : G \to \mathrm{GL}(W)$ be two representations of G.

A linear map $T : V \to W$ is a **morphism** if:

$$T \circ \phi_g(v) = \psi_g \circ T(v) \quad \forall g \in G,\, v \in V$$

Equivalent Representations:

Representations (V, ϕ) and (W, ψ) are **equivalent** if there exists an isomorphism $T : V \to W$ such that:

$$\phi_g = T^{-1} \circ \psi_g \circ T \quad \forall g \in G$$

Types of Representations

Irreducible Representation:
A representation $\phi : G \to \mathrm{GL}(V)$ is **irreducible** if the only G-invariant subspaces of V are $\{0\}$ and V itself.
Example: Every degree 1 representation $\phi : G \to \mathbb{C}^*$ is irreducible.

Decomposable Representation:
A representation $\phi : G \to \mathrm{GL}(V)$ is **decomposable** if there exist nonzero G-invariant subspaces V_1, V_2 such that:

$$V = V_1 \oplus V_2$$

Completely Reducible Representation:
A representation $\phi : G \to \mathrm{GL}(V)$ is **completely reducible** if:

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_n$$

where each V_i is a G-invariant subspace and the restriction $\phi|_{V_i}$ is irreducible.

Maschke's Theorem and Schur's Lemma

Maschke's Theorem: Every representation of a finite group is completely reducible (semi simple).

Schur's Lemma: Let $\phi : G \to GL(V)$ and $\psi : G \to GL(W)$ be two irreducible representation and $T \in Hom_G(V, W)$ Then T is either invertible or a zero map.

Schur's Orthogonality Relation

Let $\phi : G \to GL_n(C)$ and $\psi : G \to GL_m(C)$ be two irreducible representation then

(1) $\langle \phi_{(i,l)}, \psi_{(k,j)} \rangle = 0 \ \forall i, l, k, j$

(2) $\langle \phi_{(i,l)}, \phi_{(k,j)} \rangle = \frac{1}{n} \delta_{ij} \delta_{lk} = \begin{cases} \frac{1}{n} & \text{if } i = j \text{ and } l = k, \\ 0 & \text{otherwise.} \end{cases}$

Proposition Let $\phi : G \to GL(V)$ and $\psi : G \to GL(W)$ be two representation of G , let $T : V \to W$ be a linear map then

- $T_0 = \frac{1}{|G|} \sum_{t \in G} \psi_{t^{-1}} T \phi_t \in Hom_G(V, W)$
- If $T \in Hom_G(V, W)$ then $T_0 = T$

Proposition Let $\phi : G \to GL(V)$ and $\psi : G \to GL(W)$ be irreducible representation of G and $T : V \to W$ be a linear map then

- If $\phi \nsim \psi$ then $T_0 = 0$
- If $\phi = \psi$ then $T_0 = \frac{Trace(T)}{deg\phi}.I$

Proposition Let $\phi : G \to GL_n(\mathbb{C})$ and $\psi : G \to GL_m(\mathbb{C})$ be two Unitary irreducible representation of a group G . Let $A = E_{k,i} \in M_{m\times n}(\mathbb{C})$, (k, i) th entry is 1 others are 0. Then $A'_{j,l} = \langle \phi_{(i,l)}, \psi_{(k,j)} \rangle$

Proof of Schur's Orthogonality Relation

- If $i \neq k$, then $\langle \phi_{(i,l)}, \psi_{(k,j)} \rangle = 0$, since $Trace(E_{k,i}) = 0$
- If $l \neq j$, then $\langle \phi_{(i,l)}, \psi_{(k,j)} \rangle = 0$, because $I_{(l,j)} = 0$
- If $i = k$ and $l = j$ then $\langle \phi_{(i,l)}, \psi_{(k,j)} \rangle = \frac{1}{n}$ since $Trace(E_{k,i}) = 1$

Group Characters

- Definition of character $\chi(g) = \mathrm{Tr}(\phi(g))$
- Orthogonality relations

Let ϕ and ψ two irreducible representation of a group G , then

$$\langle \chi_\phi, \chi_\psi \rangle = \begin{cases} 1 & \text{if } \phi \sim \psi \\ 0 & \text{if } \phi \nsim \psi \end{cases}$$

Note

$$\langle \chi_\phi, \chi_\psi \rangle \ = \tfrac{1}{|G|} \textstyle\sum_{g \in G} \chi_\phi(g) \overline{\chi_\psi(g)} = \tfrac{1}{|G|} \sum_{g \in G} \sum_{i=1}^{n} \phi_{ii}(g) \overline{\sum_{j=1}^{m} \psi_{jj}(g)}$$
$$= \textstyle\sum_{i=1}^{n} \sum_{j=1}^{m} \tfrac{1}{|G|} \sum_{g \in G} \phi_{ii}(g) \overline{\psi_{jj}(g)}$$
$$= \textstyle\sum_{i=1}^{n} \sum_{j=1}^{m} \langle \phi_{ii}(g), \psi_{jj}(g) \rangle$$

Private Information Retrieval (PIR)

Definition

A PIR protocol allows a user to retrieve an entry x_i from a database $x = (x_1, \ldots, x_n)$ without revealing the index i to the server.

- Goal: minimize communication while preserving user privacy.
- Communication: number of bits exchange between user and server
- Trivial solution: send the whole database (n bits).
- Focus: Two-server and Linear PIR schemes.

Two-Server PIR and Linearity

Two-Server PIR Protocol

User generates queries (q_1, q_2) and sends them to servers (S_1, S_2), receives answers (a_1, a_2), and reconstructs x_i.

- Servers respond with vectors over a field $\mathbb{F}_q$
- User computes dot product of server responses
- Final result x_i is extracted from $\langle \text{Answer}_1, \text{Answer}_2 \rangle$

Linear PIR

Answer function $A(j, x, q_j)$ is linear in x.

Definition: A **Generalized Latin Square** $\mathrm{GLS}[n, T]$ is a $T \times T$ matrix Q over $[n] \cup \{*\}$

Example: $G = \mathbb{Z}_3 = \{0, 1, 2\}$ (under addition mod 3), and $S = \{0, 1\}$.

$$Q = \begin{bmatrix} 1 & 2 & * \\ * & 1 & 2 \\ 2 & * & 1 \end{bmatrix}$$

Each entry $Q_{a,b} = i$ if $a - b \equiv s_i \mod 3$; otherwise $Q_{a,b} = *$.

Construction from Group: Let $G = \{g_1, g_2, \ldots, g_T\}$ be a finite group, and let $S = \{s_1, \ldots, s_n\} \subseteq G$. Define $Q_S^G \in ([n] \cup \{*\})^{T \times T}$ by:

$$Q_{g_1,g_2} = \begin{cases} i & \text{if } g_1 g_2^{-1} = s_i \text{ for some } i \in [n] \\ * & \text{otherwise} \end{cases}$$

Respecting Group Structure: A matrix $M \in [q]^{T \times T}$ respects G if:

$$g_1 g_2^{-1} = g_3 g_4^{-1} \Rightarrow M_{g_1,g_2} = M_{g_3,g_4}$$

Algebraic Formulation

- Group algebra $\mathbb{F}_q[G]$ is a vector space of dimension $|G|$.
- A representation is a homomorphism $\phi : G \to \mathrm{GL}_r(\mathbb{F}_q)$.
- Each r-dimensional $\mathbb{F}_q[G]$-module corresponds to such a representation.

Regular Representation

$$\phi(g)_{g_1,g_2} = \begin{cases} 1 & \text{if } g_1 g_2^{-1} = g \\ 0 & \text{otherwise} \end{cases}$$

Matrix Interpretation and Rank

- The representation ϕ maps group algebra elements to matrices.
- Used to model PIR matrices and analyze structure
- $N(q, G, r)$: Number of $|G| \times |G|$ matrices over $\mathbb{F}_q$ respecting G and of rank at most r.

$$q^n \leq N(q, G, r)$$

Bounding Representations and Modules

- Number of r-dimensional modules $\leq q^{r^2 \log_2 |G|}$.
- Uses generators $g_1, \ldots, g_s$ for G where $s \leq \log_2 |G|$.
- Each representation determined by images of these generators in $\mathrm{GL}_r(\mathbb{F}_q)$.
- For an arbitrary finite group G and arbitrary values of q and r , $N(q, G, r) \leq q^{O(r^2 \log |G|)}$

Conclusion

- If $q^n \leq q^{O(r^2 \log |G|)}$, then $n \leq O(r^2 \log |G|)$
- Total communication $= \log |G| + r$
- Therefore: $\Omega(n^{1/3})$ communication required

Let $Q \hookrightarrow H_r$ be a bilinear group-based PIR scheme over a group G. Let $t = \log |G|$ denote the query length and r denote the answer length then $n \leq O(tr^2)$.
In particular the total communication of any such scheme is $\Omega(n^{\frac{1}{3}})$.

References

- W. Fulton, J. Harris, Representation Theory: A First Course, Springer, 1991.
- J.-P. Serre, Linear Representations of Finite Groups, Springer, 1977.
- Representation Theory of Finite Groups (Benjamin Steinberg)
- Alexander A. Razborov and Sergey Yekhanin.
  An $\Omega(n^{1/3})$ *Lower Bound for Bilinear Group-Based Private Information Retrieval*.
  Theory of Computing, Volume 3 (2007), pp. 221–238.
  Available at: `http://theoryofcomputing.org/articles/main/v003/a012`

Thank You