Random Walks on Finite Groups

Rashmi Jain

A dissertation submitted for the partial fulfilment
of BS-MS dual degree in Science

Indian Institute of Science Education and Research Mohali
April 2016

Certificate of Examination

This is to certify that the dissertation titled **"Random Walks on Finite Groups"** submitted by **Ms. Rashmi Jain** (Reg. No. MS11059) for the partial fulfilment of BS-MS dual degree programme of the Institute, has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends the report be accepted.

Dr. Chandrakant S. Aribam Dr. Lingaraj Sahu Dr. Amit Kulshrestha
(Supervisor)

Dated: April 22, 2016

Declaration

The work presented in this dissertation has been carried out by me under the guidance of Dr. Amit Kulshrestha at the Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved every effort is made to indicate this clearly with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of work done by me and all sources listed within have been detailed in the bibliography.

Rashmi Jain
(Candidate)
Dated: April 22, 2016

In my capacity as the supervisor of the candidate's project work, I certify that the above statements by the candidate are true to the best of my knowledge.

Dr. Amit Kulshrestha
(Supervisor)

Acknowledgement

I take this opportunity with immense pleasure to thank all the people who have helped me in successful completion of my master's thesis. First of all I would like to express my gratitude to Dr. Amit Kulshrestha for providing me the opportunity to work under his guidance and for giving me timely advice to understand my goals.

I would like to express my sincere thanks to my family for being constant support and invaluable guidance. I would also like to thank my friends Arpit, Harshita, Devwrat and Ruchika at IISER Mohali for lifting up my mood whenever required.

Finally, I would like to thank Indian Institute of Science Education and Research, Mohali for providing me with such a great work culture and environment and DST India for providing me INSPIRE fellowship.

Rashmi Jain

List of Figures

Contents

Part I

Representation Theory

Chapter 1

Basic Representation Theory

Representation Theory studies group via its action on vector spaces and by studying these actions one can obtain more information on finite groups. The goal of this chapter is to introduce the readers to the basics of Representation Theory along with examples.

1.1 Definitions and Examples

Definition 1.1.1 *Let G be a group. A* **representation** *of G is a homomorphism $\rho : G \longrightarrow GL(V)$, where V is some finite dimensional vector space. We call the dimension of V as the* **degree** *of the representation, φ.*

We will write ρ_g for $\rho(g)$ and $\rho_g(v)$ or $\rho_g v$ for the action of ρ_g on $v \in V$. Following are a few basic examples of representations.

Example 1.1.2 The first example is that of a **Trivial Representation**. The trivial representation of a group G is the homomorphism $\varphi : G \longrightarrow \mathbb{C}^*$ defined as $\varphi(g) = 1$ for all $g \in G$. This is a degree one representation as $GL(\mathbb{C})$ can be identified with $\mathbb{C}^*$. Trivial representation is possessed by every group.

Example 1.1.3 $\varphi : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{C}^*$ defined as

$$\varphi(\overline{m}) = (-1)^m$$

is clearly a representation.

Example 1.1.4 Another example of a degree one representation can be for $G = \mathbb{Z}/4\mathbb{Z}$, $\varphi : G \longrightarrow \mathbb{C}^*$ given by $\varphi(\overline{m}) = i^m$ is a representation.

Example 1.1.5 In general one can say that, $\varphi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{C}^*$ given by $\varphi(\overline{m}) = e^{(2\pi im)/n}$ is a representation as $\mathbb{C}^*$ is group under multiplication. Next, is the example of a representation for Symmetric Group S_n on n variables.

Example 1.1.6 Let $\varphi : S_n \longrightarrow GL_n(\mathbb{C})$ be a map defined on the standard basis of $\mathbb{C}^n$ by $\varphi_\sigma(e_i) = e_{\sigma(i)}$. It can be easily checked that it is a homomorphism as it is defined on the basis elements and therefore is a representation of S_n of degree n.
In particular, when $n = 3$, we have

$$\varphi_{(12)} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \varphi_{(123)} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

These matrices are the matrix of linear transformation $T : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ defined as above.

Next, we will define the concept of equivalence of representations.

Definition 1.1.7 *Let $\rho : G \longrightarrow GL(V)$ and $\psi : G \longrightarrow GL(W)$ be two representations of G. They are called* **equivalent** *if there exists an isomorphism $T : V \longrightarrow W$ such that $\psi_g = T\rho_g T^{-1} \forall g \in G$ or equivalently $\psi_g T = T\rho_g \forall g \in G$.*

In this case one writes $\rho \sim \psi$. In particular ρ and ψ have same degrees. In pictures, the following diagram commutes.

$$\begin{array}{ccc} V & \xrightarrow{\rho_g} & V \\ \downarrow{\scriptstyle T} & & \downarrow{\scriptstyle T} \\ W & \xrightarrow{\psi_g} & W \end{array}$$

Definition 1.1.8 *Let G be a group and $\rho : G \longrightarrow GL(V)$ be a representation of G. Let W be a subspace of V. W is said to be $G-$invariant if one has $\rho_g w \in W$, for all $w \in W$ and $g \in G$.*

Example 1.1.9 Notice that in Example 1.1.6 of representation of S_n,

$$\varphi_\sigma(e_1 + e_2 + \ldots + e_n) = e_{\sigma(1)} + e_{\sigma(2)} + \ldots + e_{\sigma(n)} = e_1 + e_2 + \ldots + e_n$$

Here, the first equality is true because φ is a homomorphism and the second equality holds because σ is an element in S_n and also addition of e_i's is commutative. Thus, one can observe that $\mathbb{C}(e_1 + e_2 + \ldots + e_n)$ is a $S_n - invariant$ subspace of $\mathbb{C}^n$. Infact it is identity for all permutations, $\sigma \in S_n$.

Definition 1.1.10 *Let the representations $\rho^{(1)} : G \longrightarrow GL(V_1)$ and $\rho^{(2)} : G \longrightarrow GL(V_2)$ of a group G be given. Then one can define the* **direct sum**

$$\rho^{(1)} \oplus \rho^{(2)} : G \longrightarrow GL(V_1 \oplus V_2)$$

as follows

$$(\rho^{(1)} \oplus \rho^{(2)})_g(v_1, v_2) = (\rho_g^{(1)}(v_1), \rho_g^{(2)}(v_2)).$$

One can understand it better when it is written in terms of matrices. For that, let $\rho^{(1)} : G \longrightarrow GL_n(\mathbb{C})$ and $\rho^{(2)} : G \longrightarrow GL_m(\mathbb{C})$ be the given representations of G. Then

$$\rho^{(1)} \oplus \rho^{(2)} : G \longrightarrow GL_{m+n}(\mathbb{C})$$

has the following block matrix form

$$(\rho^{(1)} \oplus \rho^{(2)})_g = \begin{bmatrix} \rho_g^{(1)} & 0 \\ 0 & \rho_g^{(2)} \end{bmatrix}$$

Example 1.1.11 Define the representation $\varphi^{(1)} : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{C}^*$ by $\varphi^{(1)}_{(\overline{m})} = e^{(2\pi i m)/n}$ and $\varphi^{(2)} : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{C}^*$ by $\varphi^{(2)}_{(\overline{m})} = e^{(-2\pi i m)/n}$. Then

$$\left(\varphi^{(1)} \oplus \varphi^{(2)}\right)_{\overline{m}} = \begin{bmatrix} e^{(2\pi i m)/n} & 0 \\ 0 & e^{(-2\pi i m)/n} \end{bmatrix}$$

Definition 1.1.12 *Let G be a group and $\rho : G \longrightarrow GL(V)$ be a representation of G. Let $W \leq V$ be a G-invariant subspace, then one may restrict ρ to get another representation $\rho|_W : G \longrightarrow GL(W)$ defined as $(\rho|_W)_g(w) = \rho_g(w)$ for $w \in W$. We will always have $\rho_g(w) \in W$ because W is G-invariant space. Then one says $\rho|_W$ is* **subrepresentation** *of ρ.*

In mathematics, one generally tries to find some kind of factorization into irreducibles or primes, so now we will define such elements for representation theory.

Definition 1.1.13 *Let G be a group and $\varphi : G \longrightarrow GL(V)$ be a representation of G. φ is said to be* **irreducible** *if 0 and V are the only G-invariant subspaces of V.*

Example 1.1.14 Every degree 1 representation of a group $G, \varphi : G \longrightarrow \mathbb{C}^*$ is irreducible because there are no proper non-zero subspaces of $\mathbb{C}$. Let us see an example of a representation which is not irreducible.

Example 1.1.15 The representation of S_n from Example 1.1.6 is not irreducible because we have seen that $\mathbb{C}(e_1 + e_2 + \ldots + e_n)$ is a $S_n - invariant$ subspace of $\mathbb{C}^n$.

Definition 1.1.16 *Let G be a group and $\rho : G \longrightarrow GL(V)$ be a representation of G. Then ρ is said to be* **completely reducible** *if V can be written as $V = V_1 \oplus V_2 \oplus \ldots \oplus V_n$ such that V_i are G-invariant subspaces and $\rho|_{V_i} : G \longrightarrow GL(V_i)$ are irreducible representations for all $i = 1, \ldots, n$.*

Definition 1.1.17 *Let G be a group and $\rho : G \longrightarrow GL(V)$ be a representation of G. ρ is said to be* **decomposable** *if $V = V_1 \oplus V_2$ and V_1, V_2 are non-zero G-invariant subspaces. Else, it is said to be* **indecomposable**.

We will now establish the fact that the above notions of decomposability, irreducibility and complete reducibility are dependent only on the equivalence class of a representation.

Lemma 1.1.18 *Let G be a group such that $\varphi : G \longrightarrow GL(V)$ is a representation and $\psi : G \longrightarrow GL(W)$ is a decomposable representation of G and $\varphi \sim \psi$. Then φ is also decomposable.*

Proof It is given that $\varphi \sim \psi$ which implies that there exists a vector space isomorphism $T : V \longrightarrow W$ such that $\varphi_g = T^{-1}\psi_g T$. Now assume that $W = W_1 \oplus W_2$ with W_1, W_2 being non-zero G-invariant subspaces of W. This can be done because W is decomposable.
Let $V_1 = T^{-1}(W_1)$ and $V_2 = T^{-1}(W_2)$. Let us first show that $V = V_1 \oplus V_2$.
Indeed if $v \in V_1 \cap V_2$ then $Tv \in W_1$ and $Tv \in W_2$i.e., $Tv \in W_1 \cap W_2 = 0$, which

implies $Tv = 0$. But T is injective and hence $v = 0$. If $v \in V$, then $Tv = w_1 + w_2$ for some $w_1 \in W_1$ and $w_2 \in W_2$. Then $v = T^{-1}w_1 + T^{-1}w_2 \in V_1 + V_2$. Thus $V + V_1 \oplus V_2$. Next we need to verify that V_1 and V_2 are G-invariant. If $v \in V_i$, then $\varphi_g v = T^{-1}\psi_g Tv$. But $Tv \in W_i$ implies that $\psi_g Tv \in W_i$ since W_i is G-invariant. This implies that $\varphi_g v = T^{-1}\psi_g Tv \in T^{-1}(W_i) = V_i$. Thus V_1 and V_2 are G-invariant subspaces of V such that $V = V_1 \oplus V_2$ making V decomposable as required. □ There are similar results for irreducible and completely reducible representations.

Lemma 1.1.19 *Let G be a group such that $\varphi : G \longrightarrow GL(V)$ is a representation and $\psi : G \longrightarrow GL(W)$ is an irreducible representation of G and $\varphi \sim \psi$. Then φ is also irreducible.*

Lemma 1.1.20 *Let G be a group such that $\varphi : G \longrightarrow GL(V)$ is a representation and $\psi : G \longrightarrow GL(W)$ is a complete reducibility representation of G and $\varphi \sim \psi$. Then φ is also complete reducibility.*

1.2 Complete Reducibility and Maschke's Theorem

Definition 1.2.1 *Let G be a group and V be an inner product space. A representation $\rho : G \longrightarrow GL(V)$ is called* **unitary** *if ρ_g is unitary for all $g \in G$, i.e.,*

$$\langle \rho_g(v), \rho_g(w) \rangle = \langle v, w \rangle$$

for all $v, w \in V$. Also one can say that ρ is a map from $G \longrightarrow U(V$, where $U(V)$ is the set of all unitary maps from V to V, i.e., $T : V \longrightarrow V$ such that $TT^* = I$.

Proposition 1.2.2 *Let G be a group and $\rho : G \longrightarrow GL(V)$ be a unitary representation of G. Then ρ is either decomposable or irreducible.*

Proof Let us assume that ρ is not irreducible which implies that there exists a non-zero proper subspace, W of V such that it is $G - invariant$. Then, the orthogonal complement $W^{\perp}$ of W is also non-zero such that $V = W \oplus W^{\perp}$. Now, the only thing left to show is that $W \perp$ is a $G - invariant$ subspace of V.

Let $v \in W\perp$ and $w \in W$, then

$$\begin{aligned}\langle \rho_g v, w\rangle &= \langle \rho_{g^{-1}}\rho_g v, \rho_{g^{-1}}w\rangle \\ &= \langle v, \rho_{g^{-1}}w\rangle \\ &= 0\end{aligned}$$

Here, the first equality holds as ρ is unitary and the second equality holds because $v \in W^{\perp}$ and $\rho_{g^{-1}}w \in W($ as W is $G-invariant)$.
Hence, $\rho_g v \in W^{\perp}$ for $v \in W^{\perp}$. Therefore, $W\perp$ is a $G-invariant$ subspace of V and ρ is decomposable.

Proposition 1.2.3 *Let G be a finite group. Then, every representation of G is equivalent to a unitary representation.*

Proof Let $\rho : G \longrightarrow GL(V)$ be a representation of G of degree n. Now, choose a basis B for V and let $T : V \longrightarrow \mathbb{C}^*$ be the isomorphism taking coordinates w.r.t B. Set $\varphi_g = T\rho_g T^{-1}$ for $g \in G$. This leads to a representation, $\varphi : G \longrightarrow GL_n(\mathbb{C})$ equivalent to ρ.
Let $\langle .,. \rangle$ be the standard inner product on $\mathbb{C}^n$. Next we will define a new inner product $(.,.)$ on $\mathbb{C}^n$ with the help of averaging trick. Define

$$(v, w) = \sum_{g\in G} \langle \varphi_g v, \varphi_g w\rangle .$$

Let us verify that it is indeed an inner product-
First, let us see bilinearity

$$\begin{aligned}(c_1v_1 + c_2v_2, w) &= \sum_{g\in G} \langle \varphi_g(c_1v_1 + c_2v_2, \varphi_g w\rangle \\ &= \sum_{g\in G} \langle (c_1\varphi_g v_1 + c_2\varphi_g v_2, \varphi_g w\rangle \\ &= c_1 \sum_{g\in G} \langle \varphi_g v_1, \varphi_g w\rangle + c_2 \sum_{g\in G} \langle \varphi_g v_2 \varphi_g v_2, \varphi_g w\rangle \\ &= c_1(v_1, w) + c_2(v_2, w)\end{aligned}$$

Next,

$$\begin{aligned}(w,v) &= \sum_{g\in G}\langle \varphi_g w, \varphi_g v\rangle \\ &= \sum_{g\in G}\overline{\langle \varphi_g v, \varphi_g w\rangle} \\ &= \overline{\sum_{g\in G}\langle \varphi_g v, \varphi_g w\rangle} \\ &= \overline{(v,w)}\end{aligned}$$

Now,

$$\begin{aligned}(v,v) &= \sum_{g\in G}\langle \varphi_g v, \varphi_g v\rangle \\ &\geq 0\end{aligned}$$

because each term $\langle \varphi_g v, \varphi_g v\rangle \geq 0$. If $(v,v) = 0$, then

$$0 = \sum_{g\in G}\langle \varphi_g v, \varphi_g v\rangle$$

which implies that

$$\begin{aligned}\langle \varphi_g v, \varphi_g v\rangle = 0 \forall g \in G \\ \Rightarrow \langle \varphi_1 v, \varphi_1 v\rangle = 0 \\ = \langle v, v\rangle = 0 \\ \Rightarrow v = 0\end{aligned}$$

Hence, we have verified that $(.,.)$ is the inner product.

We now wish to check that φ is unitary w.r.t. inner product $(.,.)$.

$$\begin{aligned}(\varphi_h v, \varphi_w) &= \sum_{g\in G}\langle \varphi_g\varphi_h v, \varphi_g\varphi_h\rangle \\ &= \sum_{g\in G}\langle \varphi_{gh} v, \varphi_{gh}\rangle\end{aligned}$$

Let $x = gh$, then

$$\begin{aligned}(\varphi_h v, \varphi_w) &= \sum_{x\in G}\langle \varphi_x v, \varphi_x w\rangle \\ &= (v,w)\end{aligned}$$

□

Corollary 1.2.4 *Let G be a finite group and $\rho : G \longrightarrow GL(V)$ be a representation of group G. Then ρ is either decomposable or irreducible.*

Proof From Proposition 1.2.3, one can see that there exists a unitary representation φ such that $\rho \sim \varphi$. Now using proposition 1.2.2, φ is either irreducible or decomposable and so is ρ (By Lemma 1.1.18 and Lemma 1.1.19). □

The theorem that we are now going to state and prove is a very important result of this chapter.

Theorem 1.2.5 (Maschke) *Let G be a finite group, then for any representation $\varphi : G \longrightarrow GL(V)$ of G it is possible to write V as $V = V_1 \oplus V_2 \oplus \ldots \oplus V_n$ such that V_i are G-invariant subspaces and $\varphi|_{V_i} : G \longrightarrow GL(V_i)$ are irreducible representations for all $i = 1, \ldots, n$, i.e., it is completely reducible.*

Proof Let $\varphi : G \longrightarrow GL(V)$ be a representation of G. We will prove the above statement by applying induction on dimension of V.
Let $\dim(V) = 1$, but then φ is itself irreducible as V cannot have any non-zero proper subspace, so we have proved the statement for $\dim(V) = 1$.
Next, assume that the statement holds true for any vector space having $\dim(V) \leq n$. Now, let $\varphi : G \longrightarrow GL(V)$ be a representation of degree $n + 1$. If φ is irreducible then we are through. Else, φ must be decomposable (Corollary 1.2.4) which implies the existence of non-zero G-invariant subspaces V_1, V_2 of V such that $V = V_1 \oplus V_2$.
It is clear that $\dim V_1$ and $\dim V_2 < \dim V$ and we can apply induction on V_1 and V_2. Therefore, $\varphi|_{V_1}$ and $\varphi|_{V_2}$ are completely reducible and V_1 can be written as $V_1 = V_{11} \oplus V_{12} \oplus \ldots \oplus V_{1s}$ and $V_2 = V_{21} \oplus V_{22} \oplus \ldots \oplus V_{2r}$ where V_{1i}, V_{2j} are G-invariant subspaces and $\varphi|_{V_{1i}}$, $\varphi|_{V_{2j}}$ are irreducible subrepresentations of φ for all $1 \leq i \leq s; 1 \leq j \leq r$.
Then

$$V = V_{11} \oplus V_{12} \oplus \ldots \oplus V_{1s} \oplus V_{21} \oplus V_{22} \oplus \ldots \oplus V_{2r}$$

Therefore, φ is completely reducible.

Chapter 2

Character Theory and Orthogonality Relations

2.1 Morphisms and Schur's Lemma

Definition 2.1.1 *A* **morphism** *from the representation* $\rho : G \longrightarrow GL(V)$ *to the representation* $\varphi : G \longrightarrow GL(W)$ *is a linear map* $T : V \longrightarrow W$ *such that* $T\rho_g = \varphi_g T \ \forall g \in G$ *, or equivalently the diagram below commutes.*

$$\begin{array}{ccc} V & \xrightarrow{\rho_g} & V \\ \downarrow T & & \downarrow T \\ W & \xrightarrow{\varphi_g} & W \end{array}$$

The set of morphisms from ρ to φ is denoted by $Hom_G(\rho, \varphi)$.
One can observe that $Hom_G(\rho, \varphi) \subseteq Hom(V, W)$.

Remark For an invertible $T \in Hom_G(\rho, \varphi)$ the equivalence, $\rho \sim \varphi$ holds and T is an isomorphism. Also $T : V \longrightarrow V \in Hom_G(\rho, \rho)$ if and only if $T\rho_g = \rho_g T \forall g \in G$, i.e., T is commutative with $\rho(G)$.

Proposition 2.1.2 *Let* $T : V \longrightarrow W$ *be an element in* $Hom_G(\varphi, \rho)$*. Then* $\ker(T)$ *is a* $G-$*invariant subspace of* V *and* $T(V) = Im(T)$ *is a* $G-$*invariant subspace of* W*.*

Proof To prove that $\ker(T)$ is a $G-$invariant subspace of V, we need to show that for $w \in \ker(T)$, $\varphi_g w \in \ker(T) \ \forall g \in G$.

So let $v \in \ker(T)$ and $g \in G$, then $T\varphi_g v = \rho_g T v = 0$ as $v \in \ker(T)$. This implies that $\varphi_g w \in \ker(T) \forall g \in G$. Hence, $\ker(T)$ is a $G-$invariant subspace of V.
Similarly, if $w \in \text{Im}(T)$ and $g \in G$, then $w = Tv$ for some $v \in V$. Then $\rho_g w = \rho_g T v = T\varphi_g v \in T$. Therefore, $\rho_g w \in \text{Im}(T)$ and hence $G-$invariant. □

Lemma 2.1.3 (Schur's Lemma) *Let φ, ρ be two irreducible representations of G and $T \in Hom_G(\varphi, \rho)$ then either T is invertible or $T = 0$. Equivalently-*

1. *If $\varphi \nsim \rho$, then $Hom_G(\varphi, \rho) = 0$.*
2. *If $\varphi = \rho$, then $T = \lambda I$ with $\lambda \in \mathbb{C}$.*

Remark Given two equivalent irreducible representations φ, ρ of G, the $\dim Hom_G(\varphi, \rho) = 1$, because then all linear maps from φ to ρ are scalar multiples of I.

Corollary 2.1.4 *For an abelian group G, any irreducible representation has degree 1.*

Corollary 2.1.5 *Let $\rho : G \longrightarrow GL_n(\mathbb{C})$ be a representation of a finite abelian group G. Then there exists an invertible matrix T such that $T^{-1}\varphi_g T$ is a diagonal matrix $\forall g \in G$.*

2.2 Orthogonality Relations

From now onwards we will assume that G is always finite. If $\rho : G \longrightarrow GL_n(\mathbb{C})$ is a representation of G, then $\varphi_g = (\varphi_{ij}(g))$, where $\varphi_{ij}(g) \in \mathbb{C}$ for $1 \leq i, j \leq n$. Therefore there are n^2 functions.

Proposition 2.2.1 *Let $\rho : G \longrightarrow GL(V)$ and $\varphi : G \longrightarrow GL(W)$ be representations of G and $T : V \longrightarrow W$ is a linear map. Then:*

1. $T^1 := \frac{1}{|G|} \sum_{g \in G} \varphi_{g^{-1}} T \rho_g \in Hom_G(\rho, \varphi)$
2. *If $T \in Hom_G(\rho, \varphi)$, then $T^1 = T$.*

3. *The map* $P : Hom_G(V,W) \longrightarrow Hom_G(\rho,\varphi)$ *defined by* $P(T) = T^1$ *is an onto linear transformation.*

Theorem 2.2.2 *Let* G *be a finite group and* $\varphi : G \longrightarrow GL(V), \rho : G \longrightarrow GL(W)$ *be irreducible representations of* G *let* $T : V \longrightarrow W$ *be a linear transformation, then*

1. *If* $\varphi \nsim \rho$ *then* $T_1 = 0$.

2. *If*$\varphi = \rho$ *then* $T_1 = \frac{Tr(T)}{deg(\varphi)} I$

Theorem 2.2.3 (Schur's Orthogonality Relations) *Let* $\rho : G \longrightarrow U_n(\mathbb{C})$ *and* $\varphi : G \longrightarrow U_m(\mathbb{C})$ *be irreducible representations of* G *that are both inequivalent and irreducible. Then*

1. $\langle \rho_{ij}, \varphi_{kl} \rangle = 0$

2. $\langle \rho_{ij}, \rho_{kl} \rangle = \begin{cases} \frac{1}{n} & \text{if } i = k \text{ and } k = l; \\ 0 & \text{Otherwise.} \end{cases}$

Corollary 2.2.4 *For an irreducible unitary representation of* G, ρ *of degree* d, *the* d^2 *functions* $\{\sqrt{d}\rho_{ij} : 1 \leq i, j \leq d\}$ *makes an orthonormal set.*

2.3 Class Functions and Characters

Definition 2.3.1 *Let* G *be a finite group and let* $L(G) := \{f : G \longrightarrow \mathbb{C}\}$. *Then* $L(G)$ *is called* **Group Algebra** *of* G *and is also denotes as* $\mathbb{C}^G$. *It forms an inner product space with operations as pointwise addition and multiplication.*
Inner product on $L(G)$ *is defined as* $\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g)\overline{f_2(g)}$

Definition 2.3.2 *Let* G *be a group and* $\varphi : G \longrightarrow GL(V)$ *be a representation of* G. *We define the* **character**, $\chi_\varphi : G \longrightarrow \mathbb{C}$ *of* φ *as* $\chi_\varphi(g) = Tr(\varphi_g)$. *We call the character of an irreducible representation as* **irreducible character**.

Remark For any degree one representation, $\varphi : G \longrightarrow \mathbb{C}^*$ of G, the character is same as the representation, i.e, $\chi_\varphi = \varphi$. This is true because $\chi_\varphi : G \longrightarrow \mathbb{C}$ such that $\chi_\varphi(g) = Tr(\varphi_g) = \varphi(g) \forall g \in G$ and hence,

$$\chi_\varphi = \varphi$$

So we will assume that for a degree one representation it's character and representation is same.

Next are a few properties of character that can be proved easily using the definition.

Proposition 2.3.3 *Let G be a group and $\varphi : G \longrightarrow GL(V)$ be a representation of G. Then $\chi_\varphi(1) = \deg \varphi$.*

Proposition 2.3.4 *If $\varphi \sim \rho$, then $\chi_\varphi = \chi_\rho$.*

Proposition 2.3.5 *Let G be a group and φ be a representation of G. Then $\chi_\varphi(g) = \chi_\varphi(hgh^{-1}) \forall g, h \in G$.*

Definition 2.3.6 *Let $f : G \longrightarrow \mathbb{C}$ be a function. f is said to be a* **class function** *if $f(g) = f(hgh^{-1}) \forall g, h \in G$. Also, one can say that f is a constant function over conjugacy classes of G. We use $Z(L(G))$ to denote the space of class functions.*

Remark It can be easily seen that character, χ of a representation lies in $Z(L(G))$.

Proposition 2.3.7 *$Z(L(G))$ forms a vector subspace of $L(G)$*

We now want to find out the dimension of $Z(L(G))$.

For that let $Cl(G)$ denote the set of conjugacy classes of G. For a conjugacy class $C \in Cl(G)$, we define the function $\delta_C : G \longrightarrow \mathbb{C}$ as

$$\delta_C(g) = \begin{cases} 1 & \text{if } g \in C; \\ 0 & \text{Otherwise.} \end{cases}$$

Proposition 2.3.8 *Let $B = \{\delta_C : C \in Cl(G)\}$ be a set of functions defined as above. Then B forms a basis for $Z(L(G))$. Hence* $\dim(Z(L(G)) = |Cl(G)|$.

Proof Since δ_C attains the constant value 1 on conjugacy class C, it is a class function. Therefore, $\delta_C \in Z(L(G))$. We next need to show that B spans $Z(L(G))$. If $f \in Z(L(G))$, then $f = \sum_{C \in Cl(G)} f(C)\delta_C$. Indeed, because left hand side evaluated at $g \in G$ equals $f(g)$ while right hand side equals $\sum_{C \in Cl(G)} f(C)\delta_C(g)$. Now, if C' is the conjugacy class of g then right hand side becomes $f(C')$ (from the definition of δ_C). Since $g \in C', f(C') = f(g)$.

So,the only thing left to prove is that B is a linearly independent set. For that assume,

$$\sum_{C \in Cl(G)} \alpha_C \delta_C = \sum_{C \in Cl(G)} \beta_C \delta_C$$

$\Longrightarrow$

$$\sum_{C \in Cl(G)} \alpha_C(\delta_C)(g) = \sum_{C \in Cl(G)} \beta_C(\delta_C)(g)$$

$\Longrightarrow$

$$\sum_{C \in Cl(G)} (\alpha_C - \beta_C)\delta_C(g) = 0$$

If $g \in C'$, then

$$\alpha_{C'} = \beta_{C'} \forall C \in Cl(G)$$

Therefore, B is a linearly independent set of class functions that spans $Z(L(G))$.

To check that B is an orthonormal set of non zero vectors, consider that $C, C' \in Cl(G)$, then

$$\langle \delta_C, \delta_{C'} \rangle = \frac{1}{|G|} \sum_{g \in G} \delta_C(g)\overline{\delta_{C'}(g)} = \begin{cases} \frac{|G|}{|G|} & \text{if } C = C'; \\ 0 & \text{Otherwise.} \end{cases}$$

Also $|B| = |Cl(G)| = \dim Z(L(G))$. Hence, proved. □

Now we come to one of the important results of this chapter, i.e., First Orthogonality Relation.

Theorem 2.3.9 (First Orthogonality Relation) *Let G be a group and φ, ρ be irreducible representations of G. Then*

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

Thus the set of irreducible characters of G forms an orthonormal set of class functions.

Corollary 2.3.10 *For a group G, there are at most $|Cl(G)|$ equivalence classes of irreducible representations.*

Let us define a notation. For a vector space, V, a representation φ and $m > 0$, we write

$$mV = \underbrace{V \oplus V \oplus \ldots \oplus V}_{\text{m copies}} \quad ; m\varphi = \underbrace{\varphi \oplus \varphi \oplus \ldots \oplus \varphi}_{\text{m copies}}$$

.

We also set $\{\varphi^{(1)}, \ldots, \varphi^{(s)}\}$ as the complete set of irreducible unitary representations of G and $d_i = \deg \varphi^{(i)}$

Definition 2.3.11 *Let ρ be a representation of a group G s.t $\rho \sim m_1\varphi^{(1)} \oplus \ldots \oplus m_s\varphi^{(s)}$, then the number m_i is called the* **multiplicity** *of $\varphi^{(i)}$ in ρ. It can be easily seen that deg $\rho = \sum_{i=1}^{s} m_i d_i$*

Lemma 2.3.12 *Let φ, ρ, ψ be representations of a group G such that $\varphi = \rho \oplus \psi$. Then $\chi_\varphi = \chi_\rho + \chi_\psi$.*

Theorem 2.3.13 *Let G be a group and $\{\varphi^{(1)}, \ldots, \varphi^{(s)}\}$ be the complete set of representatives of the equivalence classes of irreducible representations of G. If $\varphi \sim m_1\varphi^{(1)} \oplus \ldots \oplus m_s\varphi^{(s)}$ Then $m_i = \left\langle \chi_\varphi, \chi_\varphi^{(i)} \right\rangle$. Also, this decomposition of φ into irreducible constituents is unique and φ is determined by its character upto equivalence.*

Proof The main idea used in the proof is that equivalence of representations is an equivalence relation. Given $\varphi \sim m_1\varphi^{(1)} \oplus \ldots \oplus m_s\varphi^{(s)}$, $\chi_\varphi = m_1\chi_{\varphi^{(1)}} + \ldots + m_s\chi_{\varphi^{(s)}}$

$$\left\langle \chi_\varphi, \chi_{\varphi^{(i)}} \right\rangle = m_1 \left\langle \chi_{\varphi^{(1)}}, \chi_{\varphi^{(i)}} \right\rangle + \ldots + m_s \left\langle \chi_{\varphi^{(s)}}, \chi_{\varphi^{(i)}} \right\rangle$$

Each

$$\left\langle \chi_\varphi^{(j)}, \chi_\varphi^{(i)} \right\rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & i \neq j \end{cases}$$

$\left\langle \chi_\varphi, \chi_\varphi^{(i)} \right\rangle = m_i \forall 1 \leq i \leq s$, because $\varphi^{(j)} \nsim \varphi^{(i)}$ otherwise they would have been in same equivalence class which is not the case.

From Lemma 2.3.12, the decomposition of φ into irreducible constituents is unique otherwise if there would have been some other decomposition, say $\varphi \sim m_1'\psi^{(1)} \oplus \ldots \oplus m_s'\psi^{(s)}$

$$m_1\chi_{\varphi^{(1)}} + \ldots + m_s\chi_{\varphi^{(s)}} = m_1'\chi_{\psi^{(1)}} + \ldots + m_s'\chi_{\psi^{(s)}}$$

Then $\psi^{(i)} \sim \varphi^{(i)} \forall i$ $\square$

Corollary 2.3.14 *Let G be a group and φ be a representation of G. Then φ is irreducible if and only if $\langle \chi_\varphi, \chi_\varphi \rangle = 1$.*

Theorem 2.3.15 *Let G be a group and $\{\varphi^{(1)}, \ldots, \varphi^{(s)}\}$ be the complete set of irreducible representations of G such that $d_i = deg\varphi^{(i)}$, then $|G| = d_1^2 + d_2^2 + \ldots + d_s^2$.*

Theorem 2.3.16 *Let G be a group and $\varphi_i, d_i, 1 \leq i \leq s$ be the same as above. Then the set $B = \{\sqrt{d_k}\varphi_{ij}^{(k)} : 1 \leq k \leq s, 1 \leq i, j \leq d_k\}$ forms an orthonormal basis for the Group algebra, $L(G)$.*

So far, we have already seen a basis for the set of class functions, namely $\{\delta_C : C \in Cl(G)\}$. Next, we would like to look at another basis of $Z(L(G))$ but it is orthonormal.

Theorem 2.3.17 *Let G be a group and $Z(L(G))$ be set of class functions. Then the set $B = \{\chi_1, \chi_2, \ldots, \chi_s\}$ forms an othonormal basis for $Z(L(G))$.*

Proof We will use the same notation as above for this proof. It is clear from first orthogonality relations (Theorem 2.3.9) that irreducible characters forms an orthonormal set of class functions. We now need to show that the set B spans $Z(L(G))$. For that, let $f \in Z(L(G))$. From the previous theorem, f can be written as

$$f = \sum_{i,j,k} c_{ij}^{(k)} \varphi_{ij}^{(k)}$$

for some constants $c_{ij}^{(k)} \in \mathbb{C}$. Here $1 \leq k \leq s, 1 \leq i, j \leq d_k$. Also because f is a class function, for any $x \in G$,

$$\begin{aligned}
f(x) &= \frac{1}{|G|} \sum_{x \in G} f(g^{-1}xg) \\
&= \frac{1}{|G|} \sum_{x \in G} \sum_{i,j,k} c_{ij}^{(k)} \varphi_{ij}^{(k)}(g^{-1}xg) \\
&= \sum_{i,j,k} c_{ij}^{(k)} \frac{1}{|G|} \sum_{x \in G} \varphi_{ij}^{(k)}(g^{-1}xg) \\
&= \sum_{i,j,k} c_{ij}^{(k)} \left[\frac{1}{|G|} \sum_{x \in G} \varphi_{g^{-1}}^{(k)} \varphi_x^{(k)} \varphi_g^{(k)} \right]_{ij} \\
&= \sum_{i,j,k} c_{ij}^{(k)} \left[(\varphi_x^{(k)})^1 \right]_{ij} \\
&= \sum_{i,j,k} c_{ij}^{(k)} \frac{Tr(\varphi_x^{(k)})}{deg\varphi^{(k)}} I_{ij} \\
&= \sum_{i,k} c_{ii}^{(k)} \frac{1}{d_k} \chi_k(x)
\end{aligned}$$

Notation $(\varphi_x^{(k)})^1$ is same as in Proposition 2.2.1. Therefore,

$$f = \sum_{i,k} c_{ii}^{(k)} \frac{1}{d_k} \chi_k$$

which in a linear combination of elements in B. Hence, this shows that B forms an orthonormal basis for $Z(L(G))$. □

Corollary 2.3.18 *Let G be a group. The number of conjugacy classes of G is equal to the number of equivalence classes of irreducible representations of G.*

Proof Clearly from the above theorem we have $\dim(Z(L(G))) = s$ and also from Proposition 2.3.8, $\dim(Z(L(G))) = |Cl(G)|$.
Therefore, $s = |Cl(G)|$. □

Corollary 2.3.19 *Let G be a finite group. G is abelian if and only if number of irreducible representations of G is equal to number of equivalence classes of G.*

Proof It is a well known fact that a finite group G is abelian if and only if the number of conjugacy classes of G is equal to $|G|$. Therefore, from the above corollary, G is

abelian if and only if it has $|G|$ many equivalence classes of irreducible representations.

□

Theorem 2.3.20 (Second Orthogonality Relations) *Let C, C' be conjugacy classes of a finite group G and let $g \in C$ and $h \in C'$. Then*

$$\sum_{i=1}^{s} \chi_i(g)\overline{\chi_i(h)} = \begin{cases} \frac{|G|}{|C|} & \text{if } C = C' \\ 0 & C \neq C' \end{cases}$$

Definition 2.3.21 *For a finite group G, let $\chi_1, \ldots, \chi_s$ and $C_1, \ldots, C_s$ be the irreducible characters and conjugacy classes of G respectively. Define X to be a $s \times s$ matrix such that $(X)_{ij} = \chi_i(C_j)$. The matrix X is called the* **character table of G**.

Chapter 3

Induced Representations

This chapter deals with studying representations of $GL_2(\mathbb{F}_q)$. Representations on $GL_2(\mathbb{F}_q)$ are constructed by inducing representations of Borel subgroup, B of $GL_2(\mathbb{F}_q)$.

3.1 Basics

Definition 3.1.1 *For a subgroup H of a group G let (π, V) be a given representation of H. Define a representation of G as (π^G, V^G) where*

$$V^G = \{f : G \to V : f(hg) = \pi(h)f(g) \text{ for all } h \in H, g \in G\}$$

and

$$(\pi^G(g)f)(x) = f(xg).$$

(π^G, V^G) *is known as* **induced representation of G from π.**

Definition 3.1.2 *Given two representations (τ, U) and $\pi, V)$ of G, a linear map $\phi : U \longrightarrow V$ is called an* **interwiner** *or a homomorphism of G-modules if*

$$\phi\left(\tau\left(g\right)\left(u\right)\right) = \pi\left(g\right)\left(\phi(u)\right) \text{ for all } u \in U$$

We will now describe the relation between two induced representations. For that, let G be a finite group and H_1, H_2 be two subgroups of G with representations (π_1, V_1) and (π_2, V_2) respectively. For functions $f :\to V_1$ and $\Delta : G \to Hom_{\mathbb{C}}\left(V_1, V_2\right)$, define a convolution $\Delta * f : G \to V_2$ by

$$\left(\Delta * f\right)\left(g\right) = \frac{1}{|G|}\sum_{x \in G} \Delta(gx^{-1})(f\left(x\right))$$

Denote by D the set of all functions $\Delta : G \to Hom_{\mathbb{C}}(V_1, V_2)$ which satisfy

$$\Delta(h_2 g h_1) = \pi_2(h_2) \circ \Delta(g) \circ \pi(h_1)$$

for all $h_1 \in H_1, h_2 \in H_2$ and $g \in G$.

Theorem 3.1.3 (Mackey) *The space $Hom_G(V_1^G, V_2^G)$ is isomorphic to D as a vector space. In particular, for a function $\Delta \in D$, the corresponding element $L_\Delta \in Hom_G(V_1^G, V_2^G)$ is given $L_\Delta(f_1) = \Delta * f_1$ for $f_1 \in V_1^G$.*

Proof Given a $\Delta \in D$ and $f_1 \in V_1^G$, it clearly follows from the definitions that $\Delta * f_1 \in V_2^G$ and L_Δ is an interwiner defined as $L_\Delta(f_1) = \Delta * f_1$. Therefore, we have a linear map $D \longrightarrow Hom_G(V_1^G, V_2^G)$.
Conversely, we will construct an inverse map $Hom_G(V_1^G, V_2^G) \longrightarrow D$. Define a collection, $f_{g,v}$ of elements in V_1^G, indexed by $v \in V$ and $g \in g$, defined as

$$f_{g,v}(x) = \begin{cases} \pi_1(h)v & \text{if } x = hg, h \in H_1 \\ 0 & \text{if } x \notin H_1 g \end{cases}$$

Also, for $v \in V_1$

$$\Delta(g)(v) = [G : H_1] L_\Delta(f_{g^{-1},v})(1)$$

To see this we will solve right hand side by using the definition of $L_\Delta(f_{g^{-1},v})$

$$\begin{aligned}
[G : H_1] L_\Delta(f_{g^{-1},v})(1) &= [G : H_1] \left(\Delta * f_{g^{-1},v}\right)(1) \\
&= \frac{[G : H_1]}{|G|} \sum_{x \in G} \Delta(x^{-1}) f_{g^{-1},v}(x) \\
&= \frac{1}{|H_1|} \sum_{h \in H_1} \Delta(gh^{-1}) \pi_1(h)(v) \\
&= \frac{1}{|H_1|} \sum_{h \in H_1} \pi_2(1) \Delta(gh^{-1}) \pi_1(h)(v) \\
&= \frac{1}{|H_1|} \sum_{h \in H_1} \Delta(1 g h^{-1} h)(v) \\
&= \Delta(g)(v)
\end{aligned}$$

Therefore, from the proof above given any $L_\Delta \in Hom_G(V_1^G, V_2^G)$ one can define an element of D and it is clear that the two maps defined above are inverses of each other. $\square$

Lemma 3.1.4 *Let G be a group such that $H \leq G$ and $\{g_1, g_2, \ldots, g_s\}$ be the set of coset representatives of H in G. Let (π, V) and (π^G, V^G) be the representations of H and G respectively as mentioned above. Let $\{v_1, v_2, \ldots, v_n\}$ be the basis of V. Then basis of V^G is given by the functions*

$$\{\delta_{g_i,v_j} : G \to V, 1 \leq i \leq s, 1 \leq j \leq n\}$$

defined as

$$\delta_{g_i,v_j}(gh) = \begin{cases} \pi(h)v_j & \text{if } g = g_i \\ 0 & \text{else} \end{cases}$$

In particular, the $\dim V^G = \dim V \times [G : H]$.

Proof First, we shall show that δ_{g_i,v_j}'s are linearly independent. That is

$$\sum_{i=1}^{s}\sum_{j=1}^{n} \alpha_{i,j}\delta_{g_i,v_j} = 0 \Leftrightarrow \alpha_{i,j} = 0 \qquad \forall i, j$$

which implies,

$$\sum_{i=1}^{s}\sum_{j=1}^{n} \alpha_{i,j}\delta_{g_i,v_j}(x) = 0 \qquad \forall x \in G$$

In particular if $x = g_k h$ for some $h \in H$,

$$\begin{aligned} \sum_{i=1}^{s}\sum_{j=1}^{n} \alpha_{i,j}\delta_{g_i,v_j}(g_k h) &= \sum_{j=1}^{n} \alpha_{k,j}\pi(h)v_j \\ &= \pi(h)\left(\sum_{j=1}^{n} \alpha_{k,j}v_j\right) \qquad \forall h \in H \end{aligned}$$

Therefore,

$$\sum_{j=1}^{n} \alpha_{k,j}v_j = 0 \Longleftrightarrow \alpha_{k,j} = 0 \qquad \forall 1 \leq j \leq n.$$

Next, we will check that δ_{g_i,v_j}'s span V^G, that is, for any $f \in V^G$, one should be able to find $\alpha_{i,j}$ such that

$$f = \sum_{i=1}^{s}\sum_{j=1}^{n} \alpha_{i,j}\delta_{g_i,v_j}$$

Now if the above holds, then it is true for all $g \in G$, that is,

$$f(g_{i_0}h) = \sum_{i=1}^{s}\sum_{j=1}^{n} \alpha_{i,j}\delta_{g_i,v_j}(g_{i_0}h)$$

$$\pi(h) f(g_{i_0}) = \sum_{j=1}^{n} \alpha_{i_0,j}\pi(h)v_j$$

$$= \pi(h)\left(\sum_{j=1}^{n} \alpha_{i_0,j}v_j\right)$$

$$f(g_{i_0}) = \sum_{j=1}^{n} \alpha_{i_0,j}v_j$$

Therefore, each f can be written in terms of $\{\delta_{g_i,v_j} : 1 \leq i \leq s, 1 \leq j \leq n\}$ and hence it forms a basis for V^G. Clearly, $\dim V^G = \dim V \times [G : H]$. □

3.2 Representations of $GL_2(\mathbb{F}_q)$

3.2.1 Conjugacy Classes in $GL_2(\mathbb{F}_q)$

$G = GL_2(\mathbb{F}_q)$ is a group of 2×2 invertible matrices with entries in $\mathbb{F}_q$. In this section we will look at conjugacy classes of G.

Clearly, $|G| = (q^2 - q)(q^2 - 1) = q(q-1)^2(q+1)$.

Two matrices $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and $\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$ are conjugates only when $\{a, c\} = \{a', c'\}$ because conjugate matrices have same eigenvalues. With this fact in mind we can see that there are four families of conjugacy classes of G, listed as follows-

1. The matrices
$$\alpha I = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$$
for $\alpha \in \mathbb{F}_q^*$ belong to the centre of G and hence giving $q - 1$ conjugacy classes of 1.

2. Consider the matrices
$$u_\alpha = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$$
for $\alpha \in \mathbb{F}_q^*$. If
$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is an element of G, then

$$gu_\alpha = \begin{pmatrix} a\alpha & a+b\alpha \\ c\alpha & c+d\alpha \end{pmatrix}$$

and

$$u_\alpha g = \begin{pmatrix} a\alpha & d+b\alpha \\ c\alpha & d\alpha \end{pmatrix}$$

so g is in the centralizer of u_α if and only if $c = 0$ and $a = d$. Thus, $u_\alpha(\alpha \in \mathbb{F}_q^*)$ results in $q-1$ conjugacy classes and the order of centralizer is $q(q-1)$, so, each conjugacy class contains $q^2 - 1$ elements.

3. Let

$$d_{\alpha,\beta} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \in G \text{ and } (\alpha, \beta \in \mathbb{F}_q^*)$$

Also one can see that

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} d_{\alpha,\beta} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = d_{\beta,\alpha}$$

Now, if $\alpha \neq \beta$, then $gd_{\alpha,\beta} = d_{\alpha,\beta}g$ if and only if $b = c = 0$. Therefore, the matrices $d_{\alpha,\beta}$, for $\alpha, \beta \in \mathbb{F}_q^*$ and $\alpha \neq \beta$ gives us $(q-1)(q-2)/2$ conjugacy classes. Also the order of the centralizer is $(q-1)^2$, so each conjugacy class has $q(q+1)$ elements.

4. Consider,

$$\nu_s = \begin{pmatrix} 0 & 1 \\ -s^{1+q} & s+s^q \end{pmatrix} (s \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q)$$

Since s^{1+q} and $(s+s^q)$ are elements of $\mathbb{F}_q, \nu_s \in G$.The characterisctic polynomial of ν_s is

$$det(\lambda I - \nu_s) = \lambda(\lambda - (s+s^q)) + s^{1+q} = (\lambda - s)(\lambda - s^q).$$

So ν_s has eigenvalues, (s^{1+q}) and $(s+s^q)$. As $s \notin \mathbb{F}_q$, ν_s does not belong to any of the conjugacy classes constructed earlier.

Observe that

$$g\nu_s = \begin{pmatrix} -bs^{1+q} & a+b(s+s^q) \\ -ds^{1+q} & c+d(s+s^q) \end{pmatrix}$$

and

$$\nu_s g = \begin{pmatrix} c & d \\ -as^{1+q} + c(s+s^q) & -bs^{1+q} + d(s+s^q) \end{pmatrix}$$

Therefore, $\nu_s g = g\nu_s$ only when $c = -bs^{1+q}$ and $d = a + b(s+s^q)$. If this holds, then

$$ad - bc = a^2 + ab(s+s^q) + b^2 s^{1+q} = (a+bs)(a+bs^q)$$

Since $(a,b) \neq (0,0)$ and $s, s^q \notin \mathbb{F}_q, (a+bs)$ and $(a+bs^q)$ are non-zero. So, $g \in$ centralizer of (ν_s) if and only if

$$g = \begin{pmatrix} a & b \\ -bs^{1+q} & a + b(s+s^q) \end{pmatrix}$$

Thus, the order of the centralizer of ν_s is q^2-1, and the conjugacy class containing ν_s has size $q^2 - q$. Also, the matrix ν_r has eigenvalues r and r^q, so it is not conjugate to ν_s unless $r = s$ or $r = s^q$. Therefore, $\mathbb{F}_{q^2} \setminus \mathbb{F}_q)$ can be partitioned into subsets $\{s, s^q\}$, each of which gives a conjugacy class representative ν_s and different subsets gives representatives of different conjugacy classes.

3.2.2 Parabolically induced representations for $GL_2(\mathbb{F}_q)$

Let $B \leq GL_2(\mathbb{F}_q)$ which consists of the invertible upper triangular matrices, i.e.,

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : ac \neq 0, a, b, c \in \mathbb{F}_q \right\}.$$

B is also called standard Borel subgroup of G. Let T be a subgroup of $GL_2(\mathbb{F}_q)$ which consists of invertible upper triangular matices with $1's$ along diagonal, i.e.,

$$N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_q \right\}.$$

Also, denote by T the subgroup of G consisting of invertible diagonal matrices.
For χ_1 and χ_2, characters of $\mathbb{F}_q^*$, one can define character $\chi : T \longrightarrow \mathbb{C}^*$ of T as

$$\chi \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix} = \chi_1(x_1)\,\chi_2(x_2)$$

Now, this character can be extended to a character χ of B such that N lie in the kernel. Therefore,

$$\chi \begin{pmatrix} x_1 & x \\ 0 & x_2 \end{pmatrix} = \chi_1(x_1)\,\chi_2(x_2)$$

We will now construct representations, say $I(\chi_1, \chi_2)$ of $GL_2(\mathbb{F}_q)$ induced from the character of B defined above.

Proposition 3.2.1 *For the characters χ_1, χ_2, μ_1 and μ_2 of $\mathbb{F}_q^*$, we have*

$$\dim Hom_{GL_2(\mathbb{F}_q)}(I(\chi_1, \chi_2), I(\mu_1, \mu_2)) = e_1 + e_2$$

where,

$$e_1 = \begin{cases} 1 & \text{if } \chi_1 = \mu_1 \text{ and } \chi_2 = \mu_2, \\ 0 & \text{otherwise} \end{cases}$$

and

$$e_2 = \begin{cases} 1 & \text{if } \chi_1 = \mu_2 \text{ and } \chi_2 = \mu_1, \\ 0 & \text{otherwise} \end{cases}$$

Theorem 3.2.2 *For the characters χ_1, χ_2, μ_1 and μ_2 of $\mathbb{F}_q^*$, representation $I(\chi_1, \chi_2)$ of $GL_2(\mathbb{F}_q)$ is irreducible of degree $q+1$ unless $\chi_1 = \chi_2$. For $\chi_1 = \chi_2$, $I(\chi_1, \chi_2)$ is a direct sum of two irreducible representations of degrees 1 and q. So*

$$I(\chi_1, \chi_2) \sim I(\mu_1, \mu_2)$$

if and only if either

$$\chi_1 = \mu_1 \text{ and } \chi_2 = \mu_2$$

or else

$$\chi_1 = \mu_2 \text{ and } \chi_2 = \mu_1$$

Proof On applying Proposition 3.2.1 with $\chi_1 = \mu_1$ and $\chi_2 = \mu_2$, we can see that

$$\begin{aligned} \dim Hom_{GL_2(\mathbb{F}_q)}(I(\chi_1, \chi_2), I(\mu_1, \mu_2)) &= \dim End_{GL_2(\mathbb{F}_q)}(I(\chi_1, \chi_2)) \\ &= \begin{cases} 1 & \text{if } \chi_1 \neq \chi_2, \\ 2 & \text{if } \chi_1 = \chi_2 \end{cases} \end{aligned}$$

Also, if (π, V) is a representation of G and V is a direct sum of distinct irreducible representations $\pi_1, \pi_2, \ldots, \pi_s$ with multiplicities, $m_1, m_2, \ldots, m_s$ then $\dim End_G(V) =$

$\sum m_i^2$.

Therefore, $I(\chi_1, \chi_2)$ is an irreducible representation if $\chi_1 \neq \chi_2$. Else in the case when $\chi_1 = \chi_2$, it is a direct sum of two irreducible representations as $2 = 1^2 + 1^2$ is the only way to write 2 as a sum of nonzero squares.

By Lemma 3.1.4, dimension of $I(\chi_1, \chi_2) = \dim \mathbb{C} \times [GL_2(\mathbb{F}_q) : B] = q + 1$. If $\chi_1 = \chi_2$, the representation of $GL_2(\mathbb{F}_q)$, one have an irreducible representation of degree 1, namely one dimensional invariant subspace generated by the function $f(g) = \chi_1(det(g))$. It clearly satisfies $f(hg) = \chi(h)f(g)$ for all $h \in B$ and $g \in G$, hence lies in the space of $I(\chi_1, chi_2)$ resulting in the one dimensional representation of $GL_2(\mathbb{F}_q)$. The other component then is q dimensional.

If $\chi_1 \neq \chi_2$ then as mentioned earlier, $I(\chi_1, \chi_2)$ is irreducible. By proposition 6.3.1, there is a non-zero element in $Hom_{GL_2(\mathbb{F}_q)}(I(\chi_1, \chi_2), I(\mu_1, \mu_2))$ if and only if $\chi_1 = \mu_1$ and $\chi_2 = \mu_2$ or $\chi_1 = \mu_2$ and $\chi_2 = \mu_1$. Since, they are irreducible these homomorphisms must be isomorphisms. □

Let $\chi = (\chi_1, \chi_2)$ be a character of B. We have thus far constructed the following representations of $GL_2(\mathbb{F}_q)$:

1. When $\chi_1 \neq \chi_2$, the irreducible representation of $GL_2(\mathbb{F}_q)$ is of degree $q + 1$. Since the representations corresponding to the character (χ_1, χ_2) and (χ_2, χ_1) are isomorphic, we have $\frac{1}{2}(q-1)(q-2)$ irreducible representations of degree $q + 1$.

2. When $\chi_1 = \chi_2$, there are two irreducible representations of degrees 1 and q of $GL_2(\mathbb{F}_q)$. All these are pairwise non-isomorphic, hence we have $q - 1$ representations of degree 1 and $q - 1$ representations of degree q.

We know that the number of irreducible representations is equal to the number of conjugacy classes in a group and we have looked at

$$(q-1) + (q-1) + \frac{(q-1)(q-2)}{2}$$

irreducible representations, and there are $q^2 - 1$ conjugacy classes of $GL_2(\mathbb{F}_q)$. So, we are left to look at $\frac{1}{2}(q^2 - q)$ irreducible representations.

Also, if $\{\pi_1, \pi_2, \ldots, \pi_s\}$ forms a complete set of irreducible representations of degrees

$d_1, d_2, \ldots, d_s$ with multiplicities $m_1, m_2, \ldots, m_s$ of a group G, then

$$|G| = \sum_{i=1}^{s} m_i d_i^2.$$

On applying above to $GL_2(\mathbb{F}_q)$, we get

$$\frac{1}{2}(q-1)(q-2)(q+1)^2 + (q-1) + (q-1)q^2$$

and using the above equation, we get the difference as $\frac{1}{2}(q^2-q)(q-1)^2$. Therefore, $\frac{1}{2}(q^2-q)$ many representations left are of degree $q-1$ each.

3.3 Representations of Frobenius Group

Let q be a power of a prime number and let

$$F_{q,q-1} = \left\{ \begin{bmatrix} 1 & b \\ 0 & a \end{bmatrix} : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q \right\}$$

$F_{q,q-1}$ is a Frobenius group of order $q(q-1)$.

It can also be easily verified that $F_{q,q-1}$ is isomorphic to the set of affine functions, $\{f : \mathbb{F}_q \longrightarrow \mathbb{F}_q : f(x) = ax + b, a \in \mathbb{F}_q^*, b \in \mathbb{F}_q\}$.

Let

$$H = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in \mathbb{F}_q \right\}$$

Clearly, $|H| = q$ and $H \cong \mathbb{F}_q$. Also H is a normal subgroup of the Frobenius group $F_{q,q-1}$. A complete set of coset representatives of H in $F_{q,q-1}$ is

$$C = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix} : a \in \mathbb{F}_q^* \right\}$$

Now we will define a representation of H and will then induce it to write representations of $F_{q,q-1}$.

Let $\rho : H \longrightarrow \mathbb{C}^*$ be given by

$$\rho\left(\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \right) = e^{2\pi i b/q}$$

To check that a given induced representation is irreducible or not we have Mackey's Criterion . Below is the version of Mackey's Criterion for a normal subgroup H of G.

Theorem 3.3.1 (Mackey's Criterion) *Let H be a normal subgroup of G and $\varphi : H \longrightarrow GL_d(\mathbb{C})$ be an irreducible representation. Then the induced representation of φ on G is also irreducible if and only if for some $s \notin H$ the representation $\varphi^s : H \longrightarrow GL_d(\mathbb{C})$ defined as $\varphi^s(h) = \varphi(s^{-1}hs)$ does not have φ as an irreducible constituent.*

So to check that the induced representation of ρ on $F_{q,q-1}$, say $\rho^{F_{q,q-1}}$ is irreducible or not, let $s = \begin{bmatrix} 1 & 0 \\ 0 & a^{-1} \end{bmatrix}$ be such that $a \neq 1$, then

$$\rho^s\left(\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}\right) = \rho\left(\begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix}\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & a^{-1} \end{bmatrix}\right) = \rho\left(\begin{bmatrix} 1 & ba^{-1} \\ 0 & 1 \end{bmatrix}\right) = e^{2\pi iba^{-1}/q}$$

Therefore, ρ and ρ^s are inequivalent irreducible characters of H. So, from Mackey's Criterion $\rho^{F_{q,q-1}}$ is an irreducible representation of degree $[F_{q,q-1} : H] = q - 1$ (from Lemma 3.1.4). Hence,

$$\rho^{F_{q,q-1}} : F_{q,q-1} \longrightarrow GL_{q-1}(\mathbb{C}).$$

Also, from Theorem 2.3.15,

$$(q-1) + (q-1)(q-1) = (q-1)(1+q-1) = q(q-1) = |F_{q,q-1}|$$

Now, we are left with $q - 1$ degree 1 representations of $F_{q,q-1}$. Given a character $\chi : \mathbb{F}_q^* \longrightarrow \mathbb{C}^*$ we have

$$\chi^{F_{q,q-1}} : F_{q,q-1} \longrightarrow \mathbb{C}^*$$

defined as

$$\chi^{F_{q,q-1}}\left(\begin{bmatrix} 1 & b \\ 0 & a \end{bmatrix}\right) = \chi(a)$$

Part II

Fourier Analysis and Random Walks

Chapter 4

Fourier Analysis on Finite Groups

This chapter introduces the reader with the concept of Fourier transform and Fourier Inversion on Finite Abelian as well as non-Abelian Groups. We will also introduce an algebraic structure on $L(G)$ which comes from the convolution product. The applications of which we will see in later chapters.

4.1 The Convolution Product

In this section we define the concept of convolution product in $L(G)$, which then will explain the name, Group Algebra for $L(G)$.

Definition 4.1.1 *For a finite group G and $f_1, f_2 \in L(G)$ the convolution product of f_1 and f_2 is a function, $f_1 * f_2 : G \longrightarrow \mathbb{C}$ defined by*

$$f_1 * f_2(x) = \sum_{y \in G} f_1(xy^{-1}) f_2(y).$$

We would now like to show that convolution product provides a ring structure on $L(G)$.

So, to each $g \in G$, associate the delta function δ_g defined as

$$\delta_g(x) = \begin{cases} 1 & \text{if } x = g \\ 0 & \text{otherwise} \end{cases}$$

Proposition 4.1.2 *Let $g, h \in G$, then $\delta_g * \delta_h = \delta_{gh}$.*

Proof Let * be the convolution, then

$$\delta_g * \delta_h(x) = \sum_{y \in G} \delta_g(xy^{-1})\delta_h(y)$$

and the only non-zero term on right hand side is when $xy^{-1} = g$ and $h = y$ i.e., $g = xh^{-1}$ which implies $x = gh$. Therefore, $\delta_g * \delta_h = \delta_{gh}$. □

Now if $f_1, f_2 \in L(G)$, then

$$f_1 = \sum_{g \in G} f_1(g)\,\delta_g, f_2 = \sum_{g \in G} f_2(g)\delta_g$$

Theorem 4.1.3 *Let G be a finite group and $L(G)$ denotes it's Group Algebra. Then $L(G)$ forms a ring with pointwise addition and convolution as multiplication. Also, the multiplicative identity of $L(G)$ is δ_1.*

Proof Firstly, we need to show that it is an additive abelian group. Clearly, it is closed under addition. Also the identity element exists, i.e., the zero function, say $f_0 : G \longrightarrow \mathbb{C}$ defined by $f_0(x) = 0 \forall x \in G$. Inverse of every function f is $-f$ which is in $L(G)$ such that $f + (-f) = f_0$. Also for $f_1, f_2 \in L(G), (f_1 + f_2)(x) = f_1(x) + f_2(x) = f_2(x) + f_1(x) = (f_2 + f_1)(x) \forall x \in G$ Therefore, it is an abelian additive group.

Next we need to show that convolution is associative and distributive. For associativity, let $f_1, f_2, f_3 \in L(G)$. Then,

$$\begin{aligned}[(f_1 * f_2) * f_3](x) &= \sum_{y \in G} [f_1 * f_2(xy^{-1})] f_3(y) \\ &= \sum_{y \in G} \sum_{z \in G} f_1(xy^{-1}z^{-1} f_2(z) f_3(y)\end{aligned}$$

Let $u = zy \Rightarrow y^{-1}z^{-1} = u^{-1} \Rightarrow z = uy^{-1}$. Then,

$$\begin{aligned}[(f_1 * f_2) * f_3](x) &= \sum_{y \in G} \sum u \in G f_1(xu^{-1}) f_2(uy^{-1}) f_3(y) \\ &= \sum_{u \in G} f_1(xu^{-1}) \sum y \in G f_2(uy^{-1}) f_3(y) \\ &= \sum_{u \in G} f_1(xu^{-1})[f_2 * f_3](u) \\ &= [f_1 * (f_2 * f_3)](x)\end{aligned}$$

Hence convolution product on $L(G)$ is associative.

To see that it distributes over addition, let $f_1, f_2, f_3 \in L(G)$, then

$$\begin{aligned}(f_1 + f_2) * f_3(x) &= \sum_{y\in G} (f_1 + f_2)\,(xy^{-1}) f_3(y) \\ &= \sum_{y\in G} f_1(xy^{-1}) f_2(y) + \sum_{y\in G} f_2(xy^{-1}) f_3(y) \\ &= (f_1 * f_3)\,(x) + (f_2 * f_3)\,(x)\end{aligned}$$

Similarly, one can check that $f_1 * (f_2 + f_3) = f_1 * f_2 + f_1 * f_3$.

So $L(G)$ forms a ring with pointwise addition and convolution product as multiplication. Next, let's check the multiplicative identity. Let $a \in L(G)$, then

$$a * \delta_1(x) = \sum_{y\in G} a(xy^{-1})\delta_1(y) = a(x)$$

The equality holds because $\delta_1(y)$ will be nonzero only when $y = 1$. Similarly,

$$\begin{aligned}\delta_1 * a(x) &= \sum_{y\in G} \delta_1(xy^{-1}) a(y) \\ &= a(x) \forall x \in G\end{aligned}$$

Equality holds because $\delta_1(xy^{-1})$ is non zero only when $y = x$. □

In the previous chapter, we denoted the space of class functions by $Z(L(G))$. We know that for a ring $R, Z(R)$ is used for the center of the ring so next we will explain the notation $Z(L(G))$ for the ring $L(G)$.

Proposition 4.1.4 *Let G be a group then the set of class functions $Z(L(G))$ forms the center of G.*

Proof We need to show that a function $f : G \longrightarrow \mathbb{C}$ is a class function if and only if $f * a = a * f$ for all $a \in L(G)$

First, let f be a class function and let $a \in L(G)$. Then,

$$\begin{aligned}a * f(x) &= \sum_{y\in G} a(xy^{-1}) f(y) \\ &= \sum_{y\in G} a(xy^{-1}) f(yxy^{-1})\end{aligned}$$

The first equality holds because f is a class function. Now, let $z = xy^{-1}$

$$\begin{aligned} a * f(x) &= \sum_{z \in G} a(z) f(xz^{-1}) \\ &= \sum_{z \in G} f(xz^{-1}) a(z) \\ &= f * a(x) \end{aligned}$$

Hence, $a * f = f * a$. Conversely, let $f \in$ center of $L(G)$.

Claim $f(gh) = f(hg)$ for all $h, g \in G$

Justification

$$\begin{aligned} f(gh) &= \sum_{y \in G} f(gy^{-1}) \delta_{h^{-1}}(y) = f * \delta_{h^{-1}}(g) \\ &= \delta_{h^{-1}} * f(g) = \sum_{y \in G} \delta_{h^{-1}}(gy^{-1}) f(y) \\ &= f(hg) \end{aligned}$$

The last equality holds because $\delta_{h^{-1}} \neq 0 \Leftrightarrow gy^{-1} = h^{-1} \Leftrightarrow y = hg$.

Hence, $f(ghg^{-1}) = f(hg^{-1}g) = f(h)$ showing that f is class function. □

4.2 Fourier Analysis on Finite Abelian Groups

For a finite abelian group G, the set of class functions is same as $L(G)$. Clearly, $Z(L(G)) \subseteq L(G)$. Now for any function $f \in L(G), f(g) = f(gh^{-1}h) = f(hgh^{-1})$ for all $g, h \in G$. So $f \in Z(L(G))$

Hence, $L(G)$ forms a **commutative ring** when G is an abelian group.

Definition 4.2.1 *For a finite abelian group G, we define the the dual group of G as the set of all irreducible characters, $\chi : G \longrightarrow \mathbb{C}^*$ It is denoted by $\hat{G}$.*

Proposition 4.2.2 *For a finite abelian group G and $\chi, \theta \in \hat{G}$, define a product on $\hat{G}$ as $(\chi.\theta)(g) = \chi(g)\theta(g)$. Then $\hat{G}$ forms an abelian group with respect to the above defined product and $|\hat{G}| = |G|$.*

Proof Let $\chi, \theta \in \hat{G}$, then

$$\begin{aligned}\chi.\theta(g_1g_2) &= \chi(g_1g_2)\theta(g_1g_2)\\ &= \chi(g_1)\chi(g_2)\theta(g_1)\theta(g_2)\\ &= \chi(g_1)\theta(g_1)\chi(g_2)\theta(g_2)\\ &= (\chi.\theta)(g_1).(\chi.\theta)(g_2)\end{aligned}$$

Hence, $\hat{G}$ is closed under the defined product. Also, the product is commutative as well as associative. The trivial character $\chi_1(g) = 1$ for all $g \in G$ is the identity for $\hat{G}$. Also, $\chi^{-1}(g) = \chi(g)^{-1} = \overline{\chi(g)}$ is the inverse. Indeed, $\chi.\chi^{-1} = \chi_1$. Therefore, $\hat{G}$ forms an abelian group.

It is known that the number of irreducible characters of an abelian group G is $|G|$, so $|\hat{G}| = |G|$. □

Definition 4.2.3 *Let G be a finite abelian group and $f \in L(G)$. Then the* **Fourier transform** *of f is the function $\hat{f} : \hat{G} \longrightarrow \mathbb{C}$ defined as*

$$\hat{f}(\chi) = |G| \langle f, \chi \rangle = \sum_{g \in G} f(g)\overline{\chi(g)}$$

The numbers $|G| \langle f, \chi \rangle$ are known as the Fourier coefficients of f.

Example 4.2.4 If $\theta_1, \theta_2 \in \hat{G}$, then

$$\hat{\theta_1}(\theta_2) = |G| \langle \theta_1, \theta_2 \rangle = \begin{cases} |G| & \text{if } \theta_1 = \theta_2 \\ 0 & \text{else} \end{cases}$$

by the orthogonality relations. So, $\hat{\theta_1} = |G|\delta_{\theta_1}$

Theorem 4.2.5 (Fourier Inversion Theorem) *For a finite abelian group G and the function $f \in L(G)$,*

$$f = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi.$$

Proof It is just an easy computation.

$$\begin{aligned} f &= \sum_{\chi \in \hat{G}} \langle f, \chi \rangle \chi \\ &= \frac{1}{|G|} \sum_{\chi \in \hat{G}} |G| \langle f, \chi \rangle \chi \\ &= \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi \end{aligned}$$

□

Next, we will show that Fourier transform of a function is a linear transformation.

Proposition 4.2.6 *For a finite abelian group G, the map $T : L(G) \longrightarrow L(\hat{G})$ defined as $T(f) = \hat{f}$ is invertible and linear.*

Proof Let G be such that $|G| = n$. From the definition, $T(c_1 f_1 + c_2 f_2) = c_1 \widehat{f_1 + c_2} f_2$

$$\begin{aligned} c_1 \widehat{f_1 + c_2} f_2(\chi) &= n \langle c_1 f_1 + c_2 f_2, \chi \rangle \\ &= c_1 n \langle f_1, \chi \rangle + c_2 n \langle f_2, \chi \rangle \\ &= c_1 \hat{f}_1(\chi) + c_2 \hat{f}_2(\chi) \qquad \forall \chi \in \hat{G} \end{aligned}$$

Therefore, $c_1 \widehat{f_1 + c_2} f_2 = c_1 \hat{f}_1 + c_2 \hat{f}_2$. We need to check T is bijective. Let's first check injectivity. Let

$$\begin{aligned} \hat{f}_1 &= \hat{f}_2 \\ \hat{f}_1(\chi) &= \hat{f}_2(\chi) \qquad \forall \chi \in \hat{G} \\ |G| \langle f_1, \chi \rangle &= |G| \langle f_2, \chi \rangle \\ \langle f_1, \chi \rangle &= \langle f_2, \chi \rangle \\ \langle f_1 - f_2, \chi \rangle &= 0 \qquad \forall \chi \in \hat{G} \\ f_1 &= f_2 \end{aligned}$$

So, it is injective and also $\dim L(G) = n = \dim L(\hat{G})$. Therefore, T is an invertible linear transformation. □

One can also define a ring structure on $L(G)$ using pointwise multiplication defined as $(f.g)(x) = f(x)g(x)$. And it can be easily checked that if δ_1 is the multiplicative identity of $L(G)$ under convolution, the map $\mathbb{I} : G \longrightarrow \mathbb{C}$ defined by $\mathbb{I}(g) = 1$ for all $g \in G$ is the identity of $L(G)$ under pointwise multiplication.

One can establish an isomorphism between both these rings as done in the next theorem.

Theorem 4.2.7 *Let G be a finite abelian group and $f_1, f_2 \in L(G)$. Then the Fourier transform satisfies*

$$\widehat{f_1 * f_2} = \hat{f}_1 . \hat{f}_2.$$

So, the linear map $T : L(G) \longrightarrow L(\hat{G})$ defined as $Tf = \hat{f}$ gives an isomorphism between the rings $(L(G), +, *)$ and $(L(\hat{G}), +, .)$.

Proof From Proposition 4.2.6, one already knows that T is an isomorphism of vector spaces. So it is enough to show that $T(f_1 * f_2) = Tf_1.Tf_2$, i.e.,

$$\widehat{f_1 * f_2} = \hat{f}_1.\hat{f}_2$$

Let $|G| = n$.

$$\begin{aligned}
\widehat{f_1 * f_2}(\chi) &= n \langle f_1 * f_2, \chi \rangle \\
&= n.\frac{1}{n}\sum_{x\in G}(f_1 * f_2)(x)\overline{\chi(x)} \\
&= \sum_{x\in G}\overline{\chi(x)}\sum_{y\in G} f_1(xy^{-1})f_2(y) \\
&= \sum_{y\in G} f_2(y)\sum_{x\in G} f_1(xy^{-1})\overline{\chi(x)}
\end{aligned}$$

We will now change the variable z, i.e, $z = xy^{-1}$

$$\begin{aligned}
\widehat{f_1 * f_2}(\chi) &= \sum_{y\in G} f_2(y)\sum_{z\in G} f_1(z)\overline{\chi(zy)} \\
&= \sum_{y\in G} f_2(y)\overline{\chi}(y)\sum_{z\in G} f_1(z)\overline{\chi}(z) \\
&= \sum_{z\in G} f_1(z)\overline{\chi}(z)\sum_{y\in G} f_2(y)\overline{\chi}(y) \\
&= n \langle f_1, \chi \rangle .n \langle f_2, \chi \rangle \\
&= \hat{f}_1(\chi).\hat{f}_2(\chi) \qquad\qquad \forall \chi \in \hat{G}
\end{aligned}$$

Therefore,

$$\widehat{f_1 * f_2} = \hat{f}_1.\hat{f}_2$$

□

Example 4.2.8 This exapmle is the summary of whatever we have seen so far for the case when $G = \mathbb{Z}/n\mathbb{Z}$. Let $f, g : \mathbb{Z} \longrightarrow \mathbb{C}$ be two periodic functions with period n, i.e., $f(x + n) = f(x)$ for all $x \in \mathbb{Z}$. It can be clearly observed that periodic functions with period n are in one one to correspondence with elements of $L(\mathbb{Z}/n\mathbb{Z})$. The convolution product is defined as

$$f_1 * f_2(j) = \sum_{k=0}^{n-1} f_1(j-k)f_2(k)$$

And the Fourier transform of a function $f_1 \in L(\mathbb{Z}/n\mathbb{Z})$ is

$$\hat{f}_1(j) = \sum_{k=0}^{n-1} f_1(k) e^{(-2\pi ijk)/n}$$

By Theorem 4.2.5,

$$f_1(j) = \frac{1}{n} \sum_{k=0}^{n-1} \hat{f}_1(k) e^{(-2\pi ikk)/n}$$

Next, we need a lemma on eigenvector and eigenvalues of the convolution operator on $L(G)$.

Lemma 4.2.9 *For an abelian group G and $f \in L(G)$, define the convolution operator $M_f : L(G) \longrightarrow L(G)$ by $M_f(f_1) = f * f_1$. Then M_f is a linear map and χ is an eigenvector of M_f with eigenvalue as $\hat{f}(\chi)$ for all $\chi \in \hat{G}$*

Proof To check that M_f is linear, for $f_1, f_2 \in L(G)$ and $c_1, c_2 \in \mathbb{C}$, consider

$$\begin{aligned} M_f(c_1 f_1 + c_2 f_2) &= M_f * (c_1 f_1 + c_2 f_2) \\ &= f * c_1 f_1 + f * c_2 f_2 \\ &= c_1 f * f_1 + c_2 f * f_2 \\ &= c_1 M_f(f_1) + c_2 M_f(f_2) \end{aligned}$$

Next, let $|G| = n$ and $\chi \in \hat{G}$. Then

$$\widehat{f * \chi} = \hat{f}.\hat{\chi} = \hat{f}.n\delta_\chi$$

The equality holds as $\hat{\chi} = n \langle \chi, \theta \rangle = \begin{cases} n & \text{if } \chi = \theta \\ 0 & \text{else} \end{cases}$

Therefore, $\hat{\chi} = n\delta_\chi$

$$(\hat{f}.n\delta_\chi)(\theta) = \begin{cases} \hat{f}(\theta)n & \text{if } \chi = \theta \\ 0 & \text{else} \end{cases}$$

for some $\theta \in \hat{G}$. So $\hat{f}.n\delta_\chi = \hat{f}(\chi)n\delta_\chi$ Therefore,

$$\widehat{f * \chi} = \hat{f}(\chi)n\delta_\chi$$

Now applying the Fourier Inversion Theorem and using $\hat{\chi} = n\delta_\chi$

$$\begin{aligned} f * \chi &= \frac{1}{n} \sum_{\theta \in \hat{G}} \widehat{f * \chi}(\theta)\theta \\ &= \frac{1}{n} \sum_{\theta \in \hat{G}} \hat{f}(\chi) n\delta_\chi(\theta)\theta \end{aligned}$$

The only term that will survive is when $\theta = \chi$. Therefore, $M_f(\chi) = f * \chi = \hat{f}(\chi)\chi$. So χ is an eigenvector with eigenvalue as $\hat{f}(\chi)$

4.3 Fourier Analysis on non-abelian Groups

Given a non-abelian group G, it is clear that $Z(L(G)) \neq L(G)$ and hence $L(G)$ becomes a non commutative ring. Therefore, one can't find a Fourier transform that turns convolution into pointwise multiplication.
Let us look at another interpretation of Theorem 4.2.7 which will lead us in understanding the notion of Fourier transform for a non-abelian group:
Let G be a finite abelian group of order n and $\chi_1, \chi_2, \ldots, \chi_n$ be the irreducible characters. Then for each $f \in L(G)$, define $T : L(G) \longrightarrow \mathbb{C}^n$ as

$$T(f) = (n\langle f, \chi_1\rangle, n\langle f, \chi_2\rangle, \ldots, n\langle f, \chi_n\rangle) = (\hat{f}(\chi_1), \hat{f}(\chi_2), \ldots, \hat{f}(\chi_n)).$$

It is easy to verify that T is an isomorphism of vector spaces. Indeed, it is linear (Prop. 4.2.6). Since $\dim L(G) = n = \dim \mathbb{C}^n$ it only remains to show that T is injective which is also true because of the Fourier inversion theorem as one can recover $\hat{f}$ and f from Tf. Therefore,

Theorem 4.3.1 *For a finite abelian group G of order n, $L(G) \cong \mathbb{C}^n$.*

Also, this suggests that for an abelian group all irreducible representations are degree one and for a non-abelian group $\mathbb{C}$ should be replaced by matrix rings over $\mathbb{C}$.
For a finite group G of order n, let $\{\varphi^{(1)}, \varphi^{(2)}$ denote the complete set of irreducible unitary representations of G such that $d_k = deg\varphi^{(k)}$. Each entry of the matrix of representation is a function $\varphi_{ij}^{(k)} : G \longrightarrow \mathbb{C}$ given by $\varphi_g^{(k)} = \left(\varphi_{ij}^{(k)}(g)\right)$. Now let us define Fourier transform for a finite group.

Definition 4.3.2 *For a finite group G define $T : L(G) \longrightarrow M_{d_1}(\mathbb{C}) \times \ldots \times M_{d_s}(\mathbb{C})$ by*

$$Tf = (\hat{f}(\varphi^{(1)}), \ldots, \hat{f}(\varphi^{(s)}))$$

where, $\hat{f}(\varphi^{(1)})_{ij} = n\left\langle f, \varphi_{ij}^{(k)}\right\rangle = \sum_{g\in G} f(g)\varphi_{ij}^{(k)}(g)$. Tf is known as the **Fourier transform of** *f.*

Next is the Fourier inversion theorem for a non-abelian group G.

Theorem 4.3.3 *For a non-abelian group G of order n let $G :\longrightarrow \mathbb{C}$ be a function. Then*

$$f = \frac{1}{n}\sum_{i,j,k} d_k \hat{f}(\varphi^{(k)})_{ij}\varphi_{ij}^{(k)}.$$

Proof The computation is carried using the fact that $\sqrt{d_k}\varphi_{ij}^{(k)}$ forms an orthonormal basis of $L(G)$.

$$\begin{aligned} f &= \sum_{i,j,k} \left\langle f, \sqrt{d_k}\varphi_{ij}^{(k)} \right\rangle \sqrt{d_k}\varphi_{ij}^{(k)} \\ &= \frac{1}{n}\sum_{i,j,k} d_k n \left\langle f, \varphi_{ij}^{(k)} \right\rangle \varphi_{ij}^{(k)} \\ &= \frac{1}{n}\sum_{i,j,k} d_k \hat{f}(\varphi^{(k)})_{ij}\varphi_{ij}^{(k)} \end{aligned}$$

Hence, proved. □

Proposition 4.3.4 *Let G be a finite group and $T : L(G) \longrightarrow M_{d_1}(\mathbb{C}) \times \ldots \times M_{d_s}(\mathbb{C})$ be the Fourier transform then T is a vector space isomorphism.*

Proof It is an easy check that T is a linear map. Also, injectivity of T is ensured by Fourier inversion theorem and

$$\dim L(G) = |G| = d_1^2 + d_2^2 + \ldots + d_s^2 = \dim M_{d_1}(\mathbb{C}) \times \ldots \times M_{d_s}(\mathbb{C}).$$

Therefore, T is an isomorphism of vector spaces. □

Theorem 4.3.5 (Wedderburn) *Let G be a finite group and*

$$T : L(G) \longrightarrow M_{d_1}(\mathbb{C}) \times \ldots \times M_{d_s}(\mathbb{C})$$

be the Fourier transform then T is a ring isomorphism.

Chapter 5

Random Walk on Finite Groups

The most famous analogy to a **random walk** is that of a drunkard wandering off a village with no particular direction. So one can assume the village to be a graph where the intersection of streets represent vertices and the streets represent the edges. Whenever the drunkard reaches to one of the vertices, i.e., intersection, he randomly decides which way to go and continues on his path. Natural questions that can be asked includes the deunkard's probability to reach a certain point after say, n steps? amongst many more questions. It doesn't seem very useful to study an ambling drunkard, rather on ecan think of the random walker as a particle involved in the diffusion process. Or may be one can think of vertices representing the configuration of a deck of cards and edges representing the transformation from one configuration to other. Then the random walk represents the change of one configuration to the other.

5.1 Probability on Finite Group

One can define the probability distribution function on a Group. This section deals with defining a few probabilistic concepts with respect to a finite group. Also a notion of distance and convergence will be introduced for probabilities.

5.1.1 Basics

Definition 5.1.1 *A* **random variable** *is a G-valued function $X : \Omega \longrightarrow G$ where Ω is a probability space.*

Definition 5.1.2 *The* **probability distribution of a random variable** X *is a function* $P : G \longrightarrow [0,1]$ *defined as*

$$P(g) := Prob[X = g]$$

such that the following holds

$$\sum_{g \in G} P(g) = 1.$$

Also, if we have a subset $A \subseteq G$*, we put*

$$P(A) := \sum_{g \in A} P(g).$$

Definition 5.1.3 *Define the set*

$$supp(P) = \{g \in G : P(g) \neq 0\}.$$

This set is called **support of the probability** P*.*

Let us consider a few examples of probability distribution functions.

Example 5.1.4 Consider the set $G = \frac{\mathbb{Z}}{2\mathbb{Z}}$ and let $P(\overline{0}) = \frac{1}{2}$ and $P(\overline{1}) = \frac{1}{2}$. Then P is the probability for which $\overline{0}$ and $\overline{1}$ are equally probable.

Example 5.1.5 Let G be a finite group. We define the uniform distribution, U on G as

$$U(g) = \frac{1}{|G|} \qquad \forall g \in G$$

Usually it is thought as being unbiased.

Example 5.1.6 Let G be a finite group. Then, for any $g \in G$, we define a probability distribution δ_g as

$$\delta_g(h) = \begin{cases} 1 & \text{if } h = g \\ 0 & \text{else} \end{cases}$$

5.1.2 Convolution Product on Probabilities

One can observe that $P \in L(G)$ and hence one can define convolution product on probabilities and this product has got a probabilistic interpretation as well. Let G be a group. Let P and Q be two probabilities on G with X and Y as associated random variables, respectively. Now we want to look at the quantity $Prob[XY = g]$. For $XY = g$ to occur and $Y = x$ we must have $X = gx^{-1}$. Thus, the probability that these two occur simultaneously is $P(gx^{-1})Q(x)$. But x can have as many as $|G|$ choices. Therefore,

$$Prob[XY = g] = \sum_{x \in G} P(gx^{-1})Q(x) = P * Q(g).$$

Hence, one can think convolution product of probabilities as the probability distribution of XY whenever X and Y are themselves independent random variables with respect to the probabilities P and Q respectively.

It still remains to show that the convolution product of probabilities is also a probability.

Proposition 5.1.7 *Let G be a finite group and let P and Q be probabilities on G, then $P * Q$ is also a probability distribution on G. Moreover, $supp(P * Q) = supp(P).supp(Q)$.*

Proof Clearly, one can see that

$$0 \leq \sum_{h \in G} P(gh^{-1})Q(h) \leq \sum_{h \in G} Q(h) = 1$$

Therefore, $P * Q(g) \in [0, 1] \ \ \forall g \in G$. Next,

$$\begin{aligned} \sum_{g \in G} P * Q(g) &= \sum_{g \in G} \sum_{x \in G} P(gx^{-1})Q(x) \\ &= \sum_{x \in G} Q(x) \sum_{g \in G} P(gx^{-1}) \\ &= \sum_{x \in G} Q(x) \\ &= 1 \end{aligned}$$

The third equality holds because gx^{-1} runs through every element of G exactly once as g does when x^{-1} remains fixed. Therefore, $P * Q$ is a probability on G.
Moving onto the second part of the theorem, we can see that $P*Q(g) \neq 0$ if and only if there exists $x \in G$ such that $P(gx^{-1}) \neq 0$ and $Q(x) \neq 0$.
Let $a = gx^{-1}$ and $b = x$. One can now conclude that $P * Q(g) \neq 0$ if and only if there exists $a \in supp(P)$ and $b \in supp(Q)$ such that $ab = g$. Hence, $Supp(P * Q) = Supp(P).Supp(Q)$ □

5.1.3 Norm on Probabilities

There are a few notions of distance between the probabilities, so here we will introduce them and also establish the relations between them.

Definition 5.1.8 *Let G be a finite group. $L^1 - norm$ on $L(G)$ is defined as*

$$\|f\|_1 := \sum_{g \in G} |f(g)| \quad \text{for } 1f \in L(G)$$

One can observe that if $P \in L(G)$, then $\|P\|_1 = 1$. Next are a few properties of $L^1 - norm$.

Proposition 5.1.9 *If $f_1, f_2 \in L(G)$ and $c \in \mathbb{C}$, then the following holds-*

1. $\|f_1\|_1 = 0$ *if and only if* $f_1 \equiv 0$;
2. $\|cf_1\|_1 = |c|.\|f_1\|_1$;
3. $\|f_1 + f_2\|_1 \leq \|f_1\|_1 + \|f_2\|_1$ *(the triangle inequality);*
4. $\|f_1 * f_2\|_1 \leq \|f_1\|_1.\|f_2\|_1$.

Proof

1. First, let $\|f_1\|_1 = 0$. Then by the definition,

$$\|f_1\|_1 = \sum_{g \in G} |f_1(g)| = 0$$

Since each term is positive and sum of positive terms can be zero if and only if each term, i.e., $|f_1(g)| = 0$. Hence $f_1 \equiv 0$ on G.

Converse is obvious by the definition.

2. Consider $f_1 \in L(G)$ and $c \in \mathbb{C}$. Then again using the definition,

$$\begin{aligned}\|cf_1\|_1 &= \sum_{g\in G} |cf_1(g)| \\ &= \sum_{g\in G} |c|.|f_1(g)| \\ &= |c| \sum_{g\in G} |f_1(g)| \\ &= |c|.\|f_1\|_1\end{aligned}$$

3. Let $f_1, f_2 \in L(G)$, then

$$\begin{aligned}\|f_1 + f_2\|_1 &= \sum_{g\in G} |(f_1 + f_2)(g)| \\ &= \sum_{g\in G} |f_1(g) + f_2(g)| \\ &\leq \sum_{g\in G} |f_1(g)| + \sum_{g\in G} |f_2(g)| \\ &= \|f_1\|_1 + \|f_2\|_1\end{aligned}$$

4. Consider $f_1, f_2 \in L(G)$, then

$$\begin{aligned}\|f_1 * f_2\|_1 &= \sum_{g\in G} |f_1 * f_2(g)| \\ &= \sum_{g\in G} \left| \sum_{h\in G} f_1(gh^{-1}) f_2(h) \right| \\ &\leq \sum_{g\in G} \sum_{h\in G} |f_1(gh^{-1})||f_2(h)| \\ &= \sum_{h\in G} |f_2(h)| \sum_{g\in G} |f_1(gh^{-1})| \\ &= \|f_1\|_1.\|f_2\|_1\end{aligned}$$

The last equality holds because gh^{-1} runs over all elements of G.

We will now define yet another notion of distance between probabilities, i.e., total variation distance.

Definition 5.1.10 *Let P and Q be probabilities on a group G. The* **total variation** *distance between P and Q is defined as*

$$\|P - Q\|_{TV} := \max_{A\subseteq G} |P(A) - Q(A)|$$

In other words, the two probabilities differ by little with respect to the total variation distance if they are close enough on every subset of G.

There is a close relation between $L_1 - norm$ and *total variation distance.* To establish it, we require the following lemma.

Lemma 5.1.11 *Let G be a group and P and Q be probability distributions on it. Let $A = \{g \in G : \ P(g) \geq Q(g)\}$ and $B = \{g \in G : \ Q(g) \geq P(g)\}$ Then*

$$\|P - Q\|_{TV} = P(A) - Q(A) = Q(B) - P(B).$$

Proposition 5.1.12 *Let P and Q be probabilities on a finite group G. Then the following equality always holds:*

$$\|P - Q\|_{TV} = \frac{1}{2}\|P - Q\|_1.$$

Proof By Lemma 5.1.11

$$\begin{aligned}
\|P - Q\|_{TV} &= \frac{1}{2}\left(P(A) - Q(A) + Q(B) - P(B)\right) \\
&= \frac{1}{2}\left[\sum_{g\in A}\left(P(g) - Q(g)\right) + \sum_{g\in B}\left(Q(g) - P(g)\right)\right] \\
&= \frac{1}{2}\sum_{g\in G}|P(g) - Q(g)| \\
&= \frac{1}{2}\|P - Q\|_1
\end{aligned}$$

□

Since we have defined distance between the probabilities, there is also the notion of convergence.

Definition 5.1.13 *Let $\{P_n\}_{n\geq 1}$ be the sequence of probabilities on G. The sequence $\{P_n\}_{n\geq 1}$ is said to be* **convergent** *to a probability P if for given $\varepsilon > 0$, there exists $k > 0$ such that $\|P_n - P\|_{TV} < \varepsilon$ whenever $n \geq k$.*

5.2 Random Walks on Finite Groups

For a probability P on a group G, we will write P^{*k} for the k^{th} convolution power of P.

Definition 5.2.1 *Let G be a finite group and P be a probability distribution function on it. The sequence of probability distributions $\{P^{*k}\}_{k\geq 1}$ is called the* **random walk on G driven by P.**

Let us look at this in simple words. Suppose the walk starts at identity and then an element of G is chosen according to P, say g_1 and the walker moves to g_1. Then he chooses another element g_2 according to P and moves to g_2g_1 and so on.

Definition 5.2.2 *Let G be a finite group. Let S be a subset of G such that:*

1. $1 \notin S$;
2. *$s \in S$ implies $s^{-1} \in S$.*

A subset S of G satisfying above properties is called a **symmetric subset of G.** *Given a symmetric subset S of G, one can define the* **Cayley Graph** *of G with respect to S as a graph for which the vertex set is G and there is an edge $\{g, h\}$ connecting g and h if $gh^{-1} \in S$, or $hg^{-1} \in S$.*

A random walk on a Cayley Graph of a group G, say Γ can be thought of as a random walk on G.

Example 5.2.3 Let G be a group such that S is a symmetric subset of G. Given G and S, let Γ be the Cayley graph of the group G w.r.t symmetric subset S. Then one can define a **simple random walk** on Γ as a random walk on G which is driven by the probability $(P_S = 1/|S|).\delta_S$. Here again, the walk starts at the identity of G. Now, if after the k^{th} step of the walk, the walker is at the vertex $g \in G$, he randomly choses an element $s \in S$ according to P_S and the walker moves to the vertex sg. This is equivalent to the walk of an ambling drunkard through the graph Γ.

Example 5.2.4 Let p and q be numbers between 0 and 1 such that $p+q = 1$. Let's assume that one has a particle which is moving on a regular $n-$gon. The particle

moves one step anti-clockwise with probability q and clockwise with probability p. Then this forms a random walk on the group $\mathbb{Z}/n\mathbb{Z}$ which is driven by the probability $p\delta_{\overline{1}} + q\delta_{-\overline{1}}$.

Next we have the model of the diffusion process known as Ehrenfest's Urn model.

Example 5.2.5 Consider two urns, say A and B and let urn A contain n numbered balls. Now, the balls from urn A are chosen at random (with equal probability) and transferres to urn B. With this as the process one can label the configuration space by elements of the group $(\mathbb{Z}/2\mathbb{Z})^n$. For instance, if $v = (c_1, c_2, \ldots, c_n) \in (\mathbb{Z}/2\mathbb{Z})^n$, then the correspponding configuration is that the i^{th} ball is in urn A if $c_i = \overline{0}$ and it is in urn B if $c_i = \overline{1}$. Hence, the initial configuration would be $(\overline{0}, \overline{0}, \ldots, \overline{0})$, i.e, all the balls are in urn A. Consider e_i to be the vector for which the only nonzero position is i^{th} position and it's value is $\overline{1}$. The configuration $e_i + v$ is obtained from v by switching the position of the i^{th} ball. Thus this process of exchanging the balls in between urns corresponds to a random walk on group $(\mathbb{Z}/2\mathbb{Z})^n$ which is driven by the probability

$$P_S = \frac{1}{n}(\delta_{e_1} + \delta_{e_2} + \ldots + \delta_{e_n})$$

This can also be thought of as a simple random walk on $(\mathbb{Z}/2\mathbb{Z})^n$ w.r.t $S = \{e_1, e_2, \ldots, e_n\}$. Now we will look at an example related to card shuffling.

Example 5.2.6 This example can be considered as a random walk on the Symmetric group S_n. For example the permutation $(3, 2, 1)$ takes the top card to the third position, second one to the first position and the third card to the second position, while the remaining deck is as it is. Let us look at random transpositions.
Suppose that there is a dealer who randomly chooses a card from the deck with each of his hands (the cards can be same also) and then swaps the two cards. Given the positions i and j s.t. $i \neq j$, there are exactly two ways in which the dealer can pick a pair, i.e., i with left hand and j with right hand or vice versa. So the probability of performing the transposition $(i, j) = \frac{2}{n^2}$. Also, the probability that the dealer picks the same position, say i with both hands is $\frac{1}{n^2}$. However, the resulting permutation of positions remains identity for all i and the probability of performing identity is $\frac{1}{n}$. Therefore, one can model this random transpositions shuffle as a random walk on S_n

which is driven by P according as-

$$P(\sigma) = \begin{cases} \frac{1}{n} & \text{if } \sigma = \text{ identity} \\ \frac{2}{n^2} & \text{if } \sigma = \text{ transposition} \\ 0 & \text{else} \end{cases}$$

One can view a random walk on a group G as a way that randomly generates an element of G and generally one would like the result to be unbiased, i.e., all the elements of G to be equally likely. So an interesting question is, does the sequence $\{P^{*k}\}_{k\geq 1}$ converges to U, the uniform probability distribution on G

5.3 Spectrum and Upper Bound Lemma

Let G be a finite group (throughout this section) and P be a probability distribution on G. When we analyze the random walk on G, it leads us to analyzing and understanding the convolution powers of P. So for that matter one can associate the convolution operator to P defined as

$$M : L(G) \longrightarrow L(G) \text{ such that } M(f_1) := P * f_1$$

In particular $M^k(\delta_1) = P^{*k}$.

Definition 5.3.1 *Let G be a finite group. For a random walk on G driven by P, one can define* **spectrum of the walk** *to be the set of all eigenvalues, with multiplicities, of the linear convolution operator, M. Spectrum of the walk is denoted by $Spec(P)$.*

Consider

$$\begin{aligned} P * U(g) &= \sum_{h\in G} P(gh^{-1})U(h) \\ &= \frac{1}{|G|}\sum_{h\in G} P(gh^{-1}) \\ &= \frac{1}{|G|} = U(g) \end{aligned}$$

One can easily see that U, uniform distribution is an eigenvector of M with eigenvalue 1, i.e., $P * U = U$. The eigenvalue 1 is called trivial.

Lemma 5.3.2 *Let $\lambda \in Spec(P)$. Then $|\lambda| \leq 1$ for all eigenvalues in $Spec(P)$.*

Proof Let $\lambda \in Spec(P)$, then

$$P * f = \lambda f \Longrightarrow |P * f(g)| = |\lambda|.|f(g)|$$
$$|\lambda|.|f(g)| = \left|\sum_{h\in G} P(gh^{-1})f(h)\right|$$
$$\leq \sum_{h\in G} |P(gh^{-1}||f(h)|$$

Summing both sides of the equation over all elements of G

$$|\lambda|.\sum_{g\in G}|f(g)| \leq \sum_{g\in G}\sum_{h\in G}|P(gh^{-1})||f(h)|$$
$$= \sum_{h\in G}|f(h)|\sum_{g\in G}|P(gh^{-1})|$$
$$= \sum_{h\in G}|f(h)|$$
$$|\lambda|.\sum_{g\in G}|f(g)| \leq \sum_{h\in G}|f(h)|$$

Therefore, $|\lambda| \leq 1$, or equivalently $Spec(P) \subseteq \{z \in \mathbb{C} : |z| \leq 1\}$. □

In case of an abelian group, it is quite easy to understand the spectrum via Fourier analysis.

Theorem 5.3.3 *Let P be a probability distribution on a finite abelian group G and $\hat{P}$) denote Fourier transform of P. Then $Spec(P) = \{\hat{P}(\chi) : \chi \in \hat{G}\}$, and the multiplicity of an eigenvalue $\lambda \in Spec(P)$ is the equal to the number of characters χ for which $\hat{P}(\chi) = \lambda$.*

Proof This is a special case of Lemma 4.2.9 □

Let us compute spectrum for some of the random walks that we have already seen.

Example 5.3.4 **Lazy Random Walk** on $\mathbb{Z}/n\mathbb{Z}$ is a walk on $\mathbb{Z}/n\mathbb{Z}$ driven by the probability

$$P = \frac{1}{2}\delta_{\overline{0}} + \frac{1}{4}\delta_{\overline{1}} + \frac{1}{4}\delta_{-\overline{1}}$$

As usual we will define,

$$\chi_k(\overline{m}) = e^{(2\pi ikm)/n}$$

From the above theorem, $Spec(P) = \{\hat{P}(\chi) : \chi \in \hat{G}\}$, so we need to compute $\hat{P}(\chi_k)$.

$$\begin{aligned}\hat{P}(\chi_k) &= |G| \langle P, \chi_k \rangle \\ &= \frac{n}{n} \sum_{r \in G} P(r) \overline{\chi_k(r)} \\ &= \frac{1}{2} + \frac{1}{4} e^{(-2\pi ik)/n} + \frac{1}{4} e^{(2\pi ik)/n}\end{aligned}$$

The last equality comes from substituting the expression for P and the fact that the only terms surviving will be when $r = 0, 1, -1$

Example 5.3.5 Ehrenfest's Urn Model As seen earlier it is the random walk on $G = (\mathbb{Z}/2\mathbb{Z})^n$ which is driven by $P = \frac{1}{n}(\delta_{e_1} + \delta_{e_2} + \ldots + \delta_{e_n})$. To calculate the spectrum we have to look at the irreducible characters of G. Consider $v = (c_1, \ldots, c_n) \in G$ and define $\alpha(v) = \{i : \ c_i = \overline{1}\}$. Given $Y \subseteq \{1, 2, \ldots, n\}$, define $\chi_Y : G \longrightarrow \mathbb{C}$ by

$$\chi_Y(v) = (-1)^{|\alpha(v) \cap Y|}$$

Then $\hat{G} = \{\chi_Y : \ Y \subseteq \{1, 2, \ldots, n\}\}$. Clearly, $|\hat{G}| = |G| = 2^n$ and also each χ_Y is an irreducible character of G because $\langle \chi_Y, \chi_Y \rangle = 1 \, \forall Y \subseteq \{1, 2, \ldots, n\}$. Now,

$$\begin{aligned}\hat{P}(\chi_Y) &= |G| \langle P, \chi_Y \rangle \\ &= \frac{|G|}{|G|} . \left[\frac{1}{n} \sum_{g \in G} (\delta_{e_1} + \delta_{e_2} + \ldots + \delta_{e_n})(g) \chi_Y(g) \right]\end{aligned}$$

The only terms that will be surviving in the above equation will be that corresponding to $g \in \{e_1, \ldots, e_n\}$. So let us calculate $\chi_Y(e_i)$, i.e.,

$$\chi_Y(e_i) = \begin{cases} -1 & \text{if } i \in Y \\ 1 & \text{else} \end{cases}$$

So, $|Y|$ elements of $\{e_1, \ldots, e_n\}$ will contribute a value of $-1/n$ and the rest $n - |Y|$ will contribute a value of $1/n$. Therefore,

$$\hat{P}(\chi_Y) = 1 - \frac{2|Y|}{n}$$

and the multiplicity of each eigenvalue will be $\binom{n}{|Y|}$ because this is the number of subsets Y with $|Y|$ elements.

We will now define the norm that comes from the inner product on $L(G)$ and establish it's relation with L^1-norm. For $f \in L(G)$

$$\|f\| = \sqrt{\langle f, f \rangle}$$

It can be easily checked that it satisfies all the properties of norm.

Lemma 5.3.6 *For a finite group G and $f \in L(G)$ we have $\|f\|_1 \leq |G|.\|f\|$.*

Proof Let χ_1 be the trivial character of G, then $\chi_1(g) = 1 \; \forall g \in G$. We will write $|f|$ for the function defined as $|f|(g) := |f(g)|$ for $g \in G$. Then

$$\|f\|_1 = \sum_{g \in G} |f(g)| = \sum_{g \in G} |f|(g)\chi_1(g) = |G|.\langle |f|, \chi_1 \rangle \leq |G|.\|f\|.\|\chi_1\| = |G|.\|f\|$$

where the inequality is the Cauchy-Schwarz inequality, i.e, $|\langle v, w \rangle| \leq ||v||.||w||$ and the fact that $||\chi_1|| = 1$. □

Next comes a very important formula that relates the original norm of a function to the norm of it's Fourier transform.

Theorem 5.3.7 (Plancherel Formula) *Let G be a finite abelian group and $f_1, f_2 \in L(G)$. Then*

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \left\langle \hat{f}_1, \hat{f}_2 \right\rangle$$

Consequently, $\|f\|^2 = \frac{\|\hat{f}\|^2}{|G|}$.

Proof Using Theorem 4.2.5 for f_1 and f_2 gives

$$f_1 = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}_1(\chi)\chi$$

$$f_2 = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}_2(\chi)\chi$$

Then,

$$\begin{aligned}
\langle f_1, f_2 \rangle &= \left\langle \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}_1(\chi)\chi, \frac{1}{|G|} \sum_{\theta \in \hat{G}} \hat{f}_2(\theta)\theta \right\rangle \\
&= \frac{1}{|G|^2} \sum_{\chi \in \hat{G}} \hat{f}_1(\chi)\overline{\hat{f}_2(\chi)} \\
&= \frac{1}{|G|} \left\langle \hat{f}_1, \hat{f}_2 \right\rangle
\end{aligned}$$

The second equality holds because of the first orthogonality relation and the third equality holds due to the fact that $G \cong \hat{G}$. The second part of the theorem is proved once we subsitute $f_1 = f_2$ above. □

The following inequality was derived by Persi Diaconis and Mehrdad Shahshahani in 1981.

Theorem 5.3.8 (Upper Bound Lemma) *Let G be a finite group and Q be a probability on G. Then*

$$\|Q - U\|_{TV}^2 \leq \frac{1}{4} \sum_{\rho} d_\rho Tr(\hat{Q}(\rho)\hat{Q}(\rho)^*)$$

where the sum is over all non-trivial irreducible representations ρ of G and d_ρ is the degree of ρ.

Lemma 5.3.9 (Upper bound lemma for abelian groups) *Let G be a finite abelian group and let $\hat{G}^*$ be the set of non-trivial irreducible characters of G. Let Q be a probability on G. Then*

$$\|Q - U\|_{TV}^2 \leq \frac{1}{4} \sum_{\chi \in \hat{G}^*} |\hat{Q}(\chi)|^2$$

Proof Applying Proposition 5.1.12 and Lemma 5.3.6, one can see that

$$\|Q - U\|_{TV}^2 = \frac{1}{4}\|Q - \|_1^2 \leq \frac{1}{4}|G|\|Q - U\|^2 \tag{5.1}$$

By Plancherel formula (Theorem 5.3.7 and the fact that Fourier transform is a linear map,

$$\begin{aligned} |G|^2\|Q - U\|^2 = |G|.\|\widehat{Q - U}\|^2 = |G|.\|\hat{Q} - \hat{U}\|^2 \\ = |G| \left[\left\langle \hat{Q}, \hat{Q} \right\rangle - 2 \left\langle \hat{Q}, \hat{U} \right\rangle + \left\langle \hat{U}, \hat{U} \right\rangle \right] \end{aligned}$$

So let us evaluate $\left\langle \hat{Q}, \hat{Q} \right\rangle, \left\langle \hat{Q}, \hat{U} \right\rangle$ and $\left\langle \hat{U}, \hat{U} \right\rangle$.

$$\hat{U}(\chi) = |G| \langle U, \chi \rangle = \langle \chi_1, \chi \rangle = \begin{cases} 1 & \text{if } \chi = \chi_1 \\ 0 & \text{else} \end{cases}$$

So,

$$\hat{U} = \delta_{\chi_1} \Longrightarrow \left\langle \hat{U}, \hat{Q} \right\rangle = \left\langle \delta_{\chi_1}, \hat{Q} \right\rangle = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \delta_{\chi_1}(\chi)\overline{\hat{Q}(\chi)} = \frac{\hat{Q}(\chi_1)}{|G|} = \frac{1}{|G|}$$

$$\langle U, U\rangle = \frac{1}{|G|}\sum_{\chi\in\hat{G}}\hat{U}(\chi)\hat{U}(\chi) = \frac{1}{|G|}\sum_{\chi\in\hat{G}}\delta_{\chi_1}(\chi)\delta_{\chi_1}(\chi) = \frac{1}{|G|}$$

$$\left\langle \hat{Q}, \hat{Q}\right\rangle = \frac{1}{|G|} + \frac{1}{|G|}\sum_{\chi\in\hat{G}^*}\hat{Q}(\chi)\overline{\hat{Q}(\chi)}$$

On substituting the above calculated values in $\|Q-U\|^2$

$$\|Q-U\|^2 = \frac{1}{|G|} + \frac{1}{|G|}\sum_{\chi\in\hat{G}^*}\hat{Q}(\chi)\overline{\hat{Q}(\chi)} + \frac{1}{|G|} - \frac{2}{|G|} = \frac{1}{|G|}\sum_{\chi\in\hat{G}^*}\hat{Q}(\chi)\overline{\hat{Q}(\chi)}$$

Substituting the above in eq. 5.1 gives

$$\|Q-U\|_{TV}^2 \le \frac{1}{4}|G|\left(\frac{1}{|G|}\sum_{\chi\in\hat{G}^*}|\hat{Q}(\chi)|^2\right) = \frac{1}{4}\left(\sum_{\chi\in\hat{G}^*}|\hat{Q}(\chi)|^2\right)$$

□

Corollary 5.3.10 *For a finite abelian group G and a probability distribution P on G, we have*

$$\|P^{*k}-U\|_{TV}^2 \le \frac{1}{4}\sum_{\chi\in\hat{G}^*}|\hat{P}(\chi)|^{2k}.$$

One can obtain bounds on the rate of convergence for a variety of random walks. These can be obtained by applying upper bound lemma.

Theorem 5.3.11 *Let*

$$P_S = \frac{1}{n+1}\left(\delta_{(0,0,\ldots,0)} + \delta_{e_1} + \ldots + \delta_{e_n}\right)$$

be the probability distribution on the group $(\mathbb{Z}/2\mathbb{Z})^n$, where e_i is the vector with 1 in the i^{th} position and 0 in all other coordinates. Let c be a positive constant. Then for $k \ge (n+1)(\log n + c)/4$ the inequality

$$\|P_S^{*k}-U\|_{TV}^2 \le \frac{1}{2}\left(e^{e^{-c}}-1\right)$$

holds.

And if $k \le (n+1)(\log n - c)/4$ where $0 < c < \log n$ and n is sufficiently large then

$$\|P_S^{*k}-U\|_{TV}^2 \ge 1 - 20e^{-c}$$

holds.

Before proving it let us analyze it. It can be observed that $\sqrt{\frac{e^{e^{-c}}-1}{2}} \longrightarrow 0$ extremely fast as $c \longrightarrow \infty$ whereas $1-20e^{-c}$ goes to 1 very quickly. If $c = 10,$ then $\sqrt{\frac{e^{e^{-c}}-1}{2}} \approx 0.004765$ and $1-20e^{-c} \approx 0.999092$.

Roughly speaking, theorem says that all the possible configurations of balls in two urns are almost equally likely in $(n+1)(\log n)/4$ steps but in any fewer steps it is not even close to uniform. This phenomenon of changing very rapidly to uniform behaviour is called the *cut-off phenomenon* by Diaconis.

Let us prove the theorem. For that the following inequalities are required-

1. For $0 \leq i \leq \left\lfloor \frac{n+1}{2} \right\rfloor, \binom{n}{i-1} \leq \binom{n}{i}$.

2. If $0 \leq x \leq 1, (1-x)^{2k} \leq e^{-2kx}\ \forall k \geq 0$.

Proof [Proof of Theorem 5.3.11] The characters of G are already states in Example 5.3.5, so consider $|Y| = j$ and applying the corollary to Upper bound lemma gives

$$\|P_S^{*k} - U\|_{TV}^2 \leq \frac{1}{4}\sum_{j=1}^{n}\binom{n}{j}\left[1-\frac{2j}{n+1}\right]^{2k} \tag{5.2}$$

On expanding RHS of eq. 5.2, one can observe that the first and the last term are equal and similarly one can find that the second term is greater then the second last term (using inequality 1 stated above) and so on,we obtain

$$\|P_S^{*k} - U\|_{TV}^2 \leq \frac{1}{2}\sum_{j=1}^{\left\lfloor \frac{n+1}{2} \right\rfloor}\binom{n}{j}\left[1-\frac{2j}{n+1}\right]^{2k}$$

Also,

$$\binom{n}{j} = \frac{n(n-1)\dots(n-j+1)}{j!} \leq \frac{n^j}{j!}$$

Using inequality 2, when $x = \frac{2j}{n+1}$, one would obtain

$$\|P_S^{*k} - U\|_{TV}^2 \leq \frac{1}{2}\sum_{j=1}^{\left\lfloor \frac{n+1}{2} \right\rfloor}\frac{n^j}{j!}e^{\frac{-4kj}{n+1}}$$

Suppose now that $k \geq (n+1)(\log n + c)/4$. Then

$$e^{\frac{-4kj}{n+1}} \leq e^{-j\log\, n - cj} = \frac{e^{-jc}}{n^j}$$

Therefore,

$$\begin{aligned}\|P_S^{*k} - U\|_{TV}^2 &\leq \frac{1}{2}\sum_{j=1}^{\lfloor \frac{n+1}{2} \rfloor} \frac{1}{j!} e^{-jc} \\ &\leq \frac{1}{2}\sum_{j=1}^{\infty} \frac{1}{j!}(e^{-c})^j \\ &\leq \frac{1}{2}\left(e^{e^{-c}} - 1\right)\end{aligned}$$

□

Theorem 5.3.12 *For n odd, let P_S be the probability distribution on $\mathbb{Z}/n\mathbb{Z}$ given by $P_S = 1/2.(\delta_{\overline{1}} + \delta_{-\overline{1}})$, then*

$$\|P_S^{*k} - U\|_{TV} \leq e^{\frac{-\pi^2 k}{2n^2}}$$

for $k \geq n^2$.

For $n \geq 6$ and $k \geq 0$, the inequality

$$\|P_S^{*k} - U\|_{TV} \geq \frac{1}{2} e^{\frac{-\pi^2 k}{2n^2} - \frac{\pi^4 k}{2n^4}}$$

holds.

Chapter 6

Calculations

Let G be a finite group and Q be a probability distribution on G. This chapter priovides a few examples of the calculation of $\|Q - U\|_{TV}^2$ with the help of upper bound lemma for various extraspecial groups like D_4, Q_8 and $D_4 \circ D_4$. Also we present some plots obtained from GAP simulations on $GL_2(\mathbb{F}_q)$ and $SL_2(\mathbb{F}_q)$.

6.1 Dihedral Group of order 8

Let D_4 be the dihedral group of order 8. Then $D_4 = \langle r, s : r^4 = s^2 = 1, (sr)^2 = 1\rangle$ There are 5 irreducible representations of D_4, say $\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5$ defined as following

Representation	$\varphi_i(r)$	$\varphi_i(s)$
φ_1	1	1
φ_2	1	-1
φ_3	-1	1
φ_4	-1	-1
φ_5	$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

The set of generators considered for random walk on D_4 is $S = \{1, r, s\}$ and the probability used to drive the random walk on D_4 is

$$P_S = \frac{1}{3}(\delta_1 + \delta_r + \delta_s)$$

Let $Q = P_S^{*k}$ then

$$\|Q - U\|_{TV}^2 \leq \frac{1}{4}\sum d_\rho Tr(\hat{Q}(\rho)\hat{Q}(\rho)^*)$$

equals

$$\|P_S^{*k} - U\|_{TV}^2 \leq \frac{1}{4}\sum_{i=2}^{5} d_{\varphi_i} Tr\left(\widehat{P_S^{*k}}(\varphi_i)\,\widehat{P_S^{*k}}(\varphi_i)^*\right)$$

Let us evaluate $\widehat{P_S^{*k}}(\varphi_i)$ for $i = 2, \ldots, 5$. Since $\widehat{P_S^{*k}}(\varphi_i) = \widehat{P_S}(\varphi_i)^k$, it is sufficient to evaluate $\widehat{P_S}(\varphi_i)$. Hence,

$$\begin{aligned}
\widehat{P_S}(\varphi_i) &= \sum_{g\in D_4} P_S(g)\varphi_i(g) \\
&= \sum_{g\in D_4} \frac{1}{3}(\delta_1 + \delta_r + \delta_s)(g)\,\varphi_i(g) \\
&= \frac{\varphi_i(1) + \varphi_i(r) + \varphi_i(s)}{3} \text{ for } i = 2, \ldots, 5
\end{aligned}$$

Therefore,

$$\widehat{P_S^{*k}}(\varphi_2) = \frac{1}{3^k} = \widehat{P^{*k}}(\varphi_3)$$

$$\widehat{P_S^{*k}}(\varphi_4) = \frac{-1}{3^k}$$

$$\widehat{P_S^{*k}}(\varphi_5) = \begin{bmatrix} 1+ki & k \\ k & 1-ki \end{bmatrix}$$

Now on substituting the values of $\widehat{P_S^{*k}}(\varphi_i)$ in eq. 5.1, we get

$$\begin{aligned}
\|P_S^{*k} - U\|_{TV}^2 &\leq \frac{1}{4}\left[\frac{3 + 2\times(2+4k^2)}{3^{2k}}\right] \\
&\leq \frac{7+8k^2}{4\times 3^{2k}}
\end{aligned}$$

Comparison Table for D_4		
Number of steps, k	Part of Upper Bounds	GAP Calculation
1	4.2×10^{-1}	-
2	1.20×10^{-1}	-
3	2.7×10^{-2}	2.05×10^{-2}
4	5.1×10^{-3}	3.45×10^{-3}
5	8.7×10^{-4}	4.53×10^{-4}
6	1.3×10^{-4}	6.18×10^{-5}
7	3.1×10^{-5}	1.62×10^{-5}
8	2.01×10^{-5}	2.65×10^{-6}
9	4.22×10^{-7}	2.34×10^{-7}

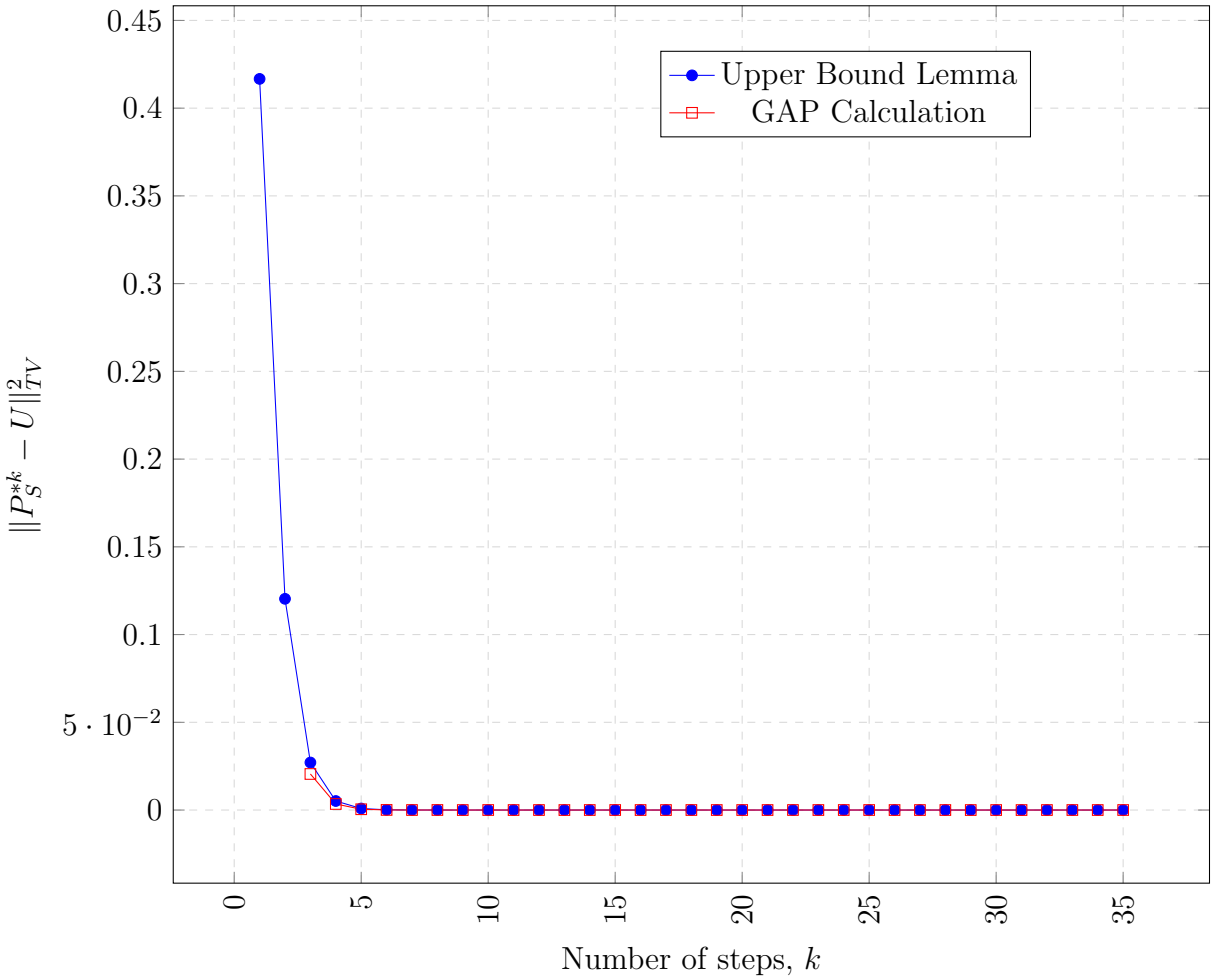

Figure 6.1: Comparison graph for D_4

6.2 Quaternion Group,Q_8

Let Q_8 be quaternion group of order 8. Then $Q_8 = \langle a, b : a^4 = 1, b^2 = a^2, bab^{-1} = a^{-1} \rangle$ There are 5 irreducible representations of Q_8, say $\psi_1, \psi_2, \psi_3, \psi_4, \psi_5$ defined as following

Representation	$\varphi_i(a)$	$\varphi_i(b)$
ψ_1	1	1
ψ_2	1	-1
ψ_3	-1	-1
ψ_4	-1	1
ψ_5	$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$	$\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$

Let $S = \{1, a, b\}$ be the set of generators to be used for random walk on Q_8, and probability used to drive the random walk be

$$P_S = \frac{1}{3}\left(\delta_1 + \delta_a + \delta_b\right)$$

We need to evaluate $\widehat{P_S^{*k}}\left(\psi_i\right)$ for $i = 2, \ldots, 5$. So,

$$\begin{aligned}
\widehat{P_S}\left(\psi_i\right) &= \sum_{g \in Q_8} P_S(g)\psi_i\left(g\right) \\
&= \sum_{g \in Q_8} \frac{1}{3}\left(\delta_1 + \delta_a + \delta_b\right)\left(g\right)\psi_i\left(g\right) \\
&= \frac{\psi_i\left(1\right) + \psi_i\left(a\right) + \psi_i\left(b\right)}{3} \text{ for } i = 2, \ldots, 5
\end{aligned}$$

Therefore,

$$\widehat{P_S^{*k}}\left(\psi_2\right) = \frac{1}{3^k} = \widehat{P^{*k}}\left(\psi_3\right)$$

$$\widehat{P_S^{*k}}\left(\psi_4\right) = \frac{-1}{3^k}$$

$$\widehat{P_S^{*k}}\left(\psi_5\right) = \begin{bmatrix} \frac{(\sqrt{2}-1)(1-i\sqrt{2})^k + (\sqrt{2}+1)(1+i\sqrt{2})^k}{2\sqrt{2}} & \frac{i[(1-i\sqrt{2})^k - (1+i\sqrt{2})^k]}{2\sqrt{2}} \\ \frac{i[(1+i\sqrt{2})^k - (1-i\sqrt{2})^k]}{2\sqrt{2}} & \frac{(\sqrt{2}+1)(1-i\sqrt{2})^k + (\sqrt{2}-1)(1+i\sqrt{2})^k}{2\sqrt{2}} \end{bmatrix}$$

Now on substituting the values of $\widehat{P_S^{*k}}\left(\varphi_i\right)$ in eq. 5.1, we get

$$\begin{aligned}
\|P_S^{*k} - U\|_{TV}^2 &\leq \frac{1}{4}\left[\frac{3 + \left(4 \times 3^k\right)}{3^{2k}}\right] \\
&\leq \frac{3 + 4 \times 3^k}{4 \times 3^{2k}}
\end{aligned}$$

Comparison Table for Q_8		
Number of steps, k	Part of Upper Bounds	GAP Calculation
1	7.8×10^{-1}	-
2	1.6×10^{-1}	-
3	4.2×10^{-2}	2.06×10^{-2}
4	1.3×10^{-2}	8.7×10^{-3}
5	4.1×10^{-3}	2.5×10^{-3}
6	1.37×10^{-4}	9.14×10^{-4}
7	4.58×10^{-4}	3.05×10^{-4}
8	1.52×10^{-4}	1.23×10^{-4}
9	5.08×10^{-5}	2.98×10^{-5}

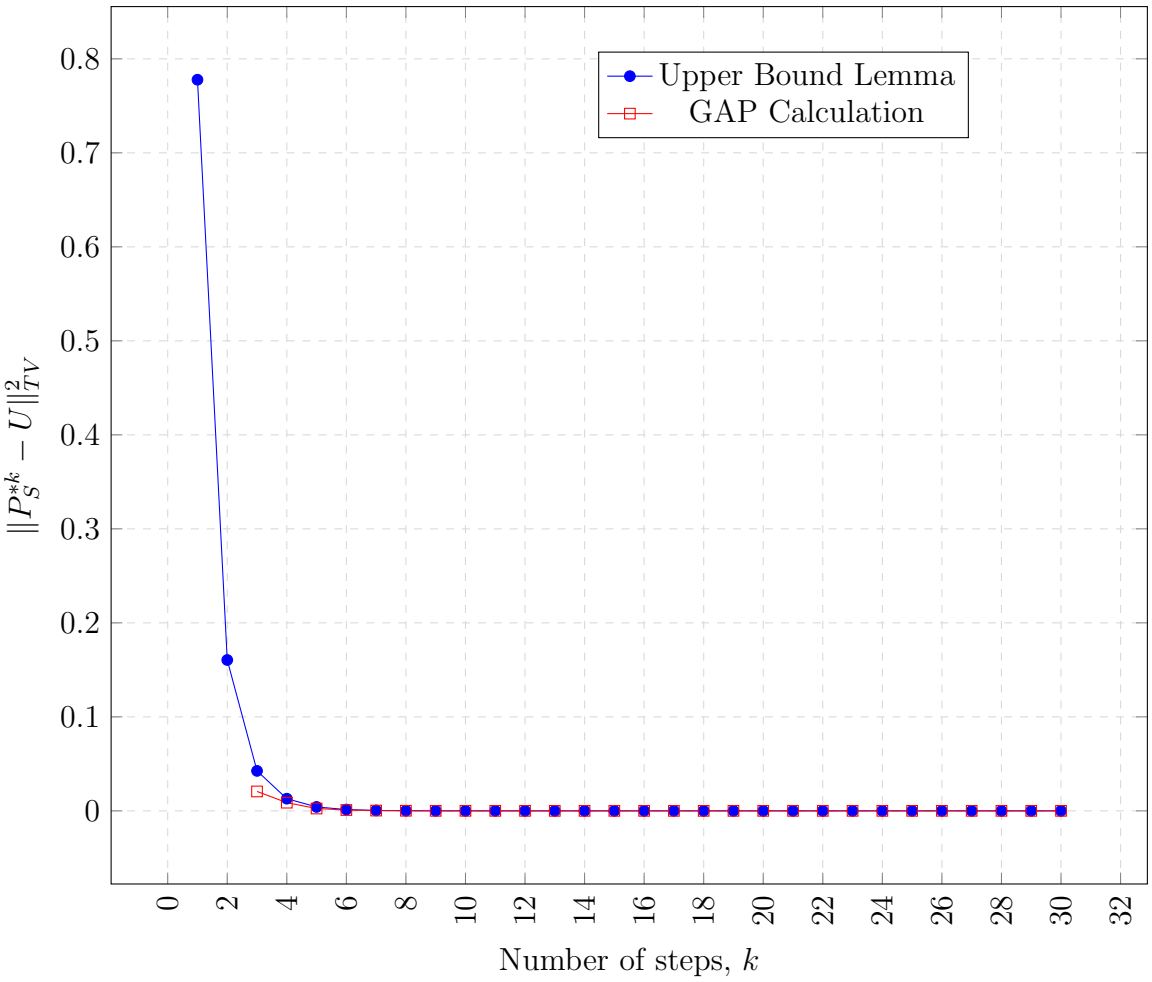

Figure 6.2: Comparison graph for Q_8

6.3 Central Product of D_4 with D_4, $D_4 \circ D_4$

There are a total of 17 representations of $D_4 \circ D_4$. The unique non linear representation is given by, $\widehat{\varphi} : D_4 \circ D_4 \longrightarrow GL(4, \mathbb{C})$ defined as $\widehat{\varphi}(\overline{(a,b)}) = \varphi(a,b)$, where $\overline{(a,b)} = (a,b)N$ and $(a,b) \in D_4 \times D_4$.
Also, $\varphi(a,b) = (\varphi_5 \otimes \varphi_5)(a,b) = \varphi_5(a) \otimes \varphi_5(b)$.

$$S = \{(1,1), (r,1), (s,1), (1,r), (1,s)\}$$

For 15 linear representations of $D_4 \circ D_4$, $\widehat{P_S^{*k}}(\varphi)(\widehat{P^{*k}})^*(\varphi) = \frac{1}{5^{2k}}$ for 10 of the representations and $\widehat{P_S^{*k}}(\varphi)(\widehat{P_S^{*k}})^*(\varphi) = \left(\frac{3}{5}\right)^{2k}$ for the rest 5 linear representations. Also,

$$\widehat{P_S^{*k}}(\widehat{\varphi}) = \begin{bmatrix} k(k+1)+1 & k^2 & k^2 & k(k-1) \\ -k^2 & -k(k-1)+1 & -k(k-1) & -k(k-2) \\ -k^2 & -k(k-1) & -k(k-1)+1 & -k(k-2) \\ k(k-1) & k(k-2) & k(k-2) & k(k-3)+1 \end{bmatrix}$$

Therefore, on substituting the above calculated values in the Upper Bound Lemma, we get

$$\begin{aligned} \|P_S^{*k} - U\|_{TV}^2 &\leq \frac{5 \times 3^{2k} + 10 + 16k^4 - 32k^3 + 32k^2 + 4}{4 \times 5^{2k}} \\ &\leq \frac{5 \times 3^{2k} + 16k^4 - 32k^3 + 32k^2 + 14}{4 \times 5^{2k}} \end{aligned}$$

Comparison Table for $D_4 \circ D_4$		
Number of steps, k	Part of Upper Bounds	GAP Calculation
1	7.5×10^{-1}	-
2	2.188×10^{-1}	-
3	7.01×10^{-2}	-
4	2.26×10^{-2}	2.16×10^{-2}
5	7.2×10^{-3}	5.84×10^{-3}
6	2.73×10^{-3}	1.9×10^{-3}
7	9.8×10^{-4}	7.29×10^{-4}
8	3.53×10^{-4}	2.47×10^{-4}
9	1.27×10^{-4}	1.04×10^{-4}

6.4 Random Walk on $GL_2(\mathbb{F}_q)$

$$GL_2(\mathbb{F}_q) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc \neq 0 \text{ and } a, b, c, d \in \mathbb{F}_q \right\}$$

The set of generators considered for random walk on $GL_2(\mathbb{F}_q)$ is

$$S = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ \mu & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix} : \lambda, \mu, d \in \mathbb{F}_q^*, d \neq 1 \right\}$$

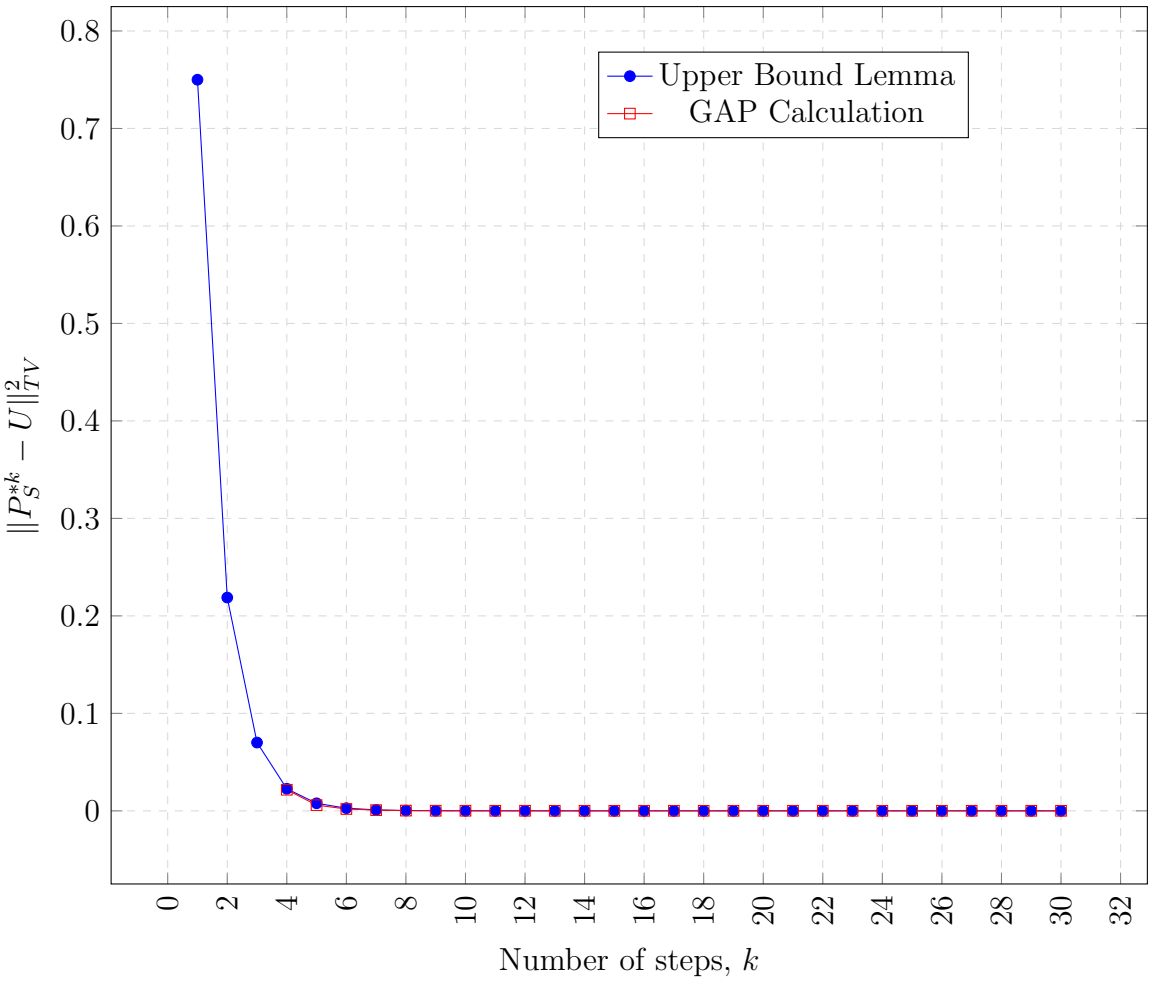

Figure 6.3: Comparison graph for $D_4 \circ D_4$

And probability used to drive the walk is

$$P_S = \frac{1}{|S|} \sum_{s \in S} \delta_S$$

6.4.1 Upper Bound for $GL_2(\mathbb{F}_3)$

Let $G := GL_2(\mathbb{F}_3)$. There are a total of 8 representations of $GL_2(\mathbb{F}_3)$ say $\varphi_1, \varphi_2, \varphi_3, \varphi_4$, $\varphi_5, \varphi_6, \varphi_7$, and φ_8 such that φ_1 is trivial and $\varphi_2 = I(\chi_1, \chi_2)$ for $\chi_1 = \chi_2$ be degree one representation and $\varphi_3 = I(\chi_1, \chi_2)$ for $\chi_1 \neq \chi_2$ be degree 4 representation (notation same as in Section 3.2). These are the only representations of G that we are considering for Upper Bound Lemma because we want to see the effect of these on upper bounds as compared to the remaining representations of G. Set of generators

considered for random walk is

$$S = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \right\}$$

We need to evaluate $\widehat{P_S^{*k}}(\varphi_i)$ for $i = 2, 3$. So,

$$\begin{aligned} \widehat{P_S}(\varphi_i) &= \sum_{g \in G} P_S(g) \varphi_i(g) \\ &= \sum_{g \in G} \frac{1}{6} (\delta_1 + \delta_a + \delta_b + \delta_c + \delta_d + \delta_e)(g) \varphi_i(g) \\ &= \frac{\varphi_i(1) + \varphi_i(a) + \varphi_i(b) + \varphi_i(c) + \varphi_i(d) + \varphi_i(e)}{6} \text{ for } i = 2, 3 \end{aligned}$$

Here, $1, a, b, c, d, e$ are the elements of S. Now,

$$\widehat{P_S}(\varphi_2) = \frac{4}{6}$$

$$\widehat{P_S}(\varphi_3) = \begin{bmatrix} 2 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{bmatrix}$$

$$\widehat{P_S^{*k}}(\varphi_2) (\widehat{P_S^{*k}})^*(\varphi_2) = \left(\frac{2}{3}\right)^{2k}$$

$$tr\left(\widehat{P_S^{*k}}(\varphi_3) (\widehat{P_S^{*k}})^*(\varphi_3)\right) = \frac{4\left(1 + 12^{2k} + 38^{2k}\right)}{60^{2k}}$$

Thus a part of Upper Bound Lemma turns out to be

$$\left(\frac{2}{3}\right)^{2k} + \frac{4\left(1 + 12^{2k} + 38^{2k}\right)}{60^{2k}}$$

Comparison table for $GL_2(\mathbb{F}_3)$		
Number of steps, k	Part of Upper Bounds	GAP Calculation
1	1.988	-
2	6.7×10^{-1}	-
3	2.61×10^{-1}	-
4	1.03×10^{-1}	8.12×10^{-2}
5	4.15×10^{-2}	4.26×10^{-2}
6	2.67×10^{-2}	2.41×10^{-2}
7	6.68×10^{-3}	1.32×10^{-2}
8	2.68×10^{-3}	7.31×10^{-3}
9	1.08×10^{-3}	4.57×10^{-3}
10	4.31×10^{-4}	2.57×10^{-3}
11	1.73×10^{-4}	1.47×10^{-3}
12	6.93×10^{-5}	7.9×10^{-4}

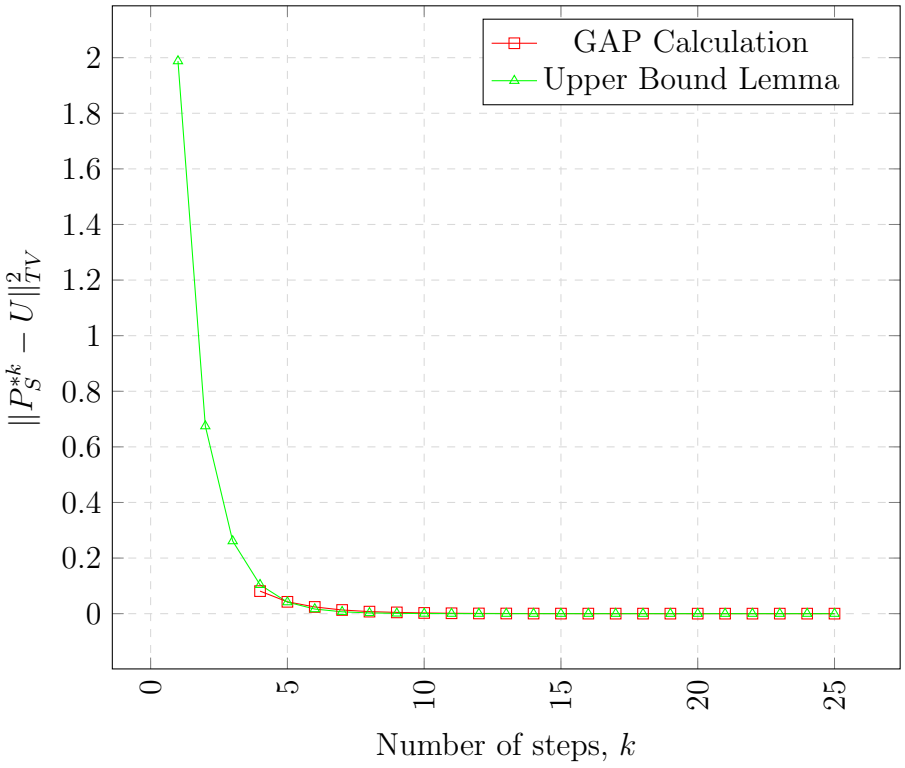

Figure 6.4: Comparison graph for $GL_2(\mathbb{F}_3)$

GAP Calculation for $GL_2(\mathbb{F}_q)$				
Number of steps, k	$q = 2$	$q = 3$	$q = 5$	$q = 7$
1	-	-	-	-
2	-	-	-	-
3	4.01×10^{-2}	-	-	-
4	1.69×10^{-2}	$8.11 \times 10^{-2}2$	-	-
5	7.48×10^{-3}	4.26×10^{-2}	0.150557	-
6	3.54×10^{-3}	2.41×10^{-2}	9.44845×10^{-2}	0.131479
7	1.48×10^{-3}	1.33×10^{-2}	5.71×10^{-2}	7.94×10^{-2}
8	7.82×10^{-4}	7.32×10^{-3}	3.382×10^{-2}	4.79×10^{-2}
9	3.10×10^{-4}	4.571×10^{-3}	2.078×10^{-2}	2.77×10^{-2}
10	1.2×10^{-4}	2.57×10^{-3}	1.19334×10^{-2}	1.711×10^{-2}
11	4.91×10^{-5}	1.472×10^{-3}	7.33×10^{-3}	1.116×10^{-2}
12	1.64×10^{-5}	7.88×10^{-4}	4.704×10^{-3}	8.37×10^{-3}
13	1.95×10^{-5}	5.9341×10^{-4}	3.10×10^{-3}	6.264×10^{-3}
14	2.33×10^{-5}	3.61×10^{-4}	2.204×10^{-3}	5.12×10^{-3}
15	2.78×10^{-5}	2.68×10^{-4}	1.76×10^{-3}	4.41×10^{-3}

6.5 Random Walk on $SL_2(\mathbb{F}_q)$

Let us first have a look at a set of generators for $SL_2(\mathbb{F}_q)$.

6.5.1 Transvections

Definition 6.5.1 *Let V be a vector space. A map $\tau \in GL(V)$ not equal to the identity map is called a* **transvection**, *if there exists a hyperplane W of V satisfying $\tau|_W = 1_W$ and $\tau(v) - v \in W$ for all $v \in V$. We call W as the* **fixed hyperplane of** *τ.*

Proposition 6.5.2 *Let τ be a transvection in $GL(V)$. Then τ always lie in $SL(V)$, i.e., for a given basis of V and W determinant of the matrix of τ is always 1.*

Theorem 6.5.3 *The set of transvections generate the group $SL(V)$.*

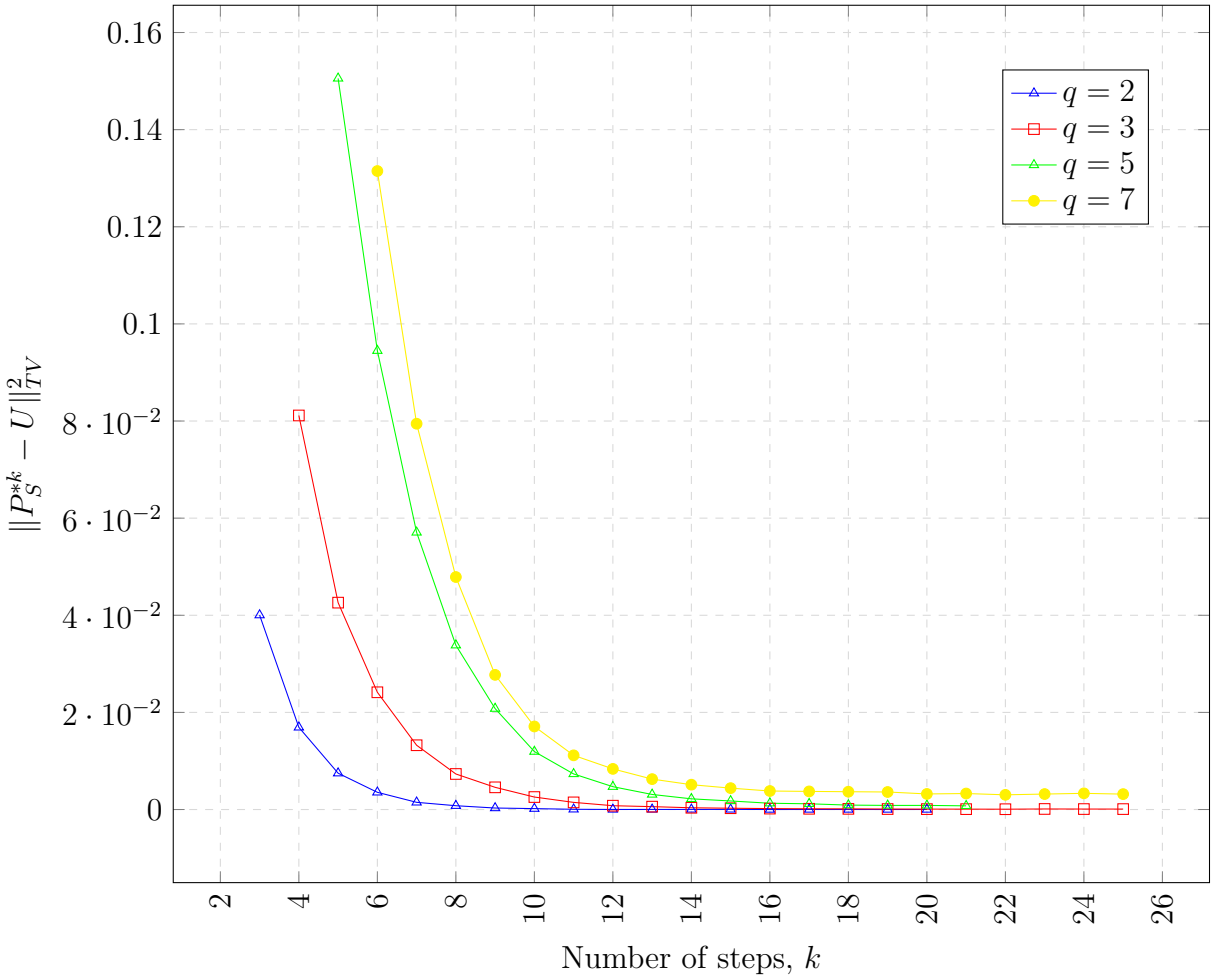

Figure 6.5: GAP Calculation for Upper Bounds of $GL_2(\mathbb{F}_q)$

Let S be the set of transvections on $V = (\mathbb{F}_q)^n$. We would like to ask as to how large k has to be for the product of k transvections to yield a uniformly random element of $SL_n(\mathbb{F}_q)$.

Theorem 6.5.4 (M. Hildebrand[Hil92]) *For sufficiently large n and all $c > 0$, where $c = k - n$, there exist positive constants A and λ such that*

$$||P_S^{*k} - U||_{TV} < Ae^{-\lambda c}$$

holds.

Given $\epsilon > 0$, there exist $c > 0$ such that for $k = n - c$ and sufficiently large n,

$$||P_S^{*k} - U||_{TV} > 1 - \epsilon$$

holds.

From above theorem one can conclude that for any $k < n$, it is not possible for the product of k transvections to be uniform on $SL_n(\mathbb{F}_q)$, and for any $k > n$, it is always possible to get close enough to the uniform distribution on $SL_n(\mathbb{F}_q)$ through transvections.

6.5.2 GAP Calculation

$$SL_2(\mathbb{F}_q) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc \neq 0, ad - bc = 1 \text{ and } a, b, c, d \in \mathbb{F}_q \right\}$$

The set of generators considered for random walk on $SL_2(\mathbb{F}_q)$ is

$$S = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ \mu & 1 \end{bmatrix} : \lambda, \mu, \in \mathbb{F}_q^* \right\}$$

And probability used to drive the walk is

$$P_S = \frac{1}{|S|} \sum_{s \in S} \delta_S$$

GAP Calculation for $SL_2(\mathbb{F}_q)$						
k	$q = 2$	$q = 3$	$q = 5$	$q = 7$	$q = 11$	$q = 13$
1	-	-	-	-	-	-
2	-	-	-	-	-	-
3	4.1×10^{-2}	-	-	-	-	-
4	1.67×10^{-2}	6.19×10^{-2}	1.16×10^{-1}	1.448×10^{-1}	1.756×10^{-1}	1.87×10^{-1}
5	7.4×10^{-3}	3.32×10^{-2}	5.634×10^{-2}	6.70×10^{-2}	7.56×10^{-2}	7.90×10^{-2}
6	3.36×10^{-3}	1.9×10^{-2}	2.61×10^{-2}	2.95×10^{-2}	3.12×10^{-2}	3.42×10^{-2}
7	1.56×10^{-3}	9.84×10^{-3}	1.324×10^{-2}	1.36×10^{-2}	1.433×10^{-2}	1.57×10^{-2}
8	6.28×10^{-4}	5.67×10^{-3}	6.613×10^{-3}	6.56×10^{-3}	7.034×10^{-3}	9.17×10^{-3}
9	3.37×10^{-4}	2.98×10^{-3}	3.03×10^{-3}	2.704×10^{-3}	4.25×10^{-3}	5.85×10^{-3}
10	1.62×10^{-4}	1.56×10^{-3}	1.50×10^{-3}	1.64×10^{-3}	3.18×10^{-3}	4.818×10^{-3}
11	8.63×10^{-4}	9.29×10^{-4}	8.65×10^{-4}	1.091×10^{-3}	2.66×10^{-3}	4.028×10^{-3}
12	5.595×10^{-5}	5.42×10^{-4}	5.27×10^{-4}	7.53×10^{-4}	2.38×10^{-3}	3.582×10^{-3}
13	3.029×10^{-5}	3.39×10^{-4}	3.161×10^{-4}	7.24×10^{-4}	2.213×10^{-3}	3.62×10^{-3}
14	8.61×10^{-6}	2.478×10^{-4}	2.27×10^{-4}	6.753×10^{-4}	2.042×10^{-3}	3.652×10^{-3}
15	1.153×10^{-5}	1.640×10^{-4}	2.023×10^{-4}	5.4×10^{-4}	2.16×10^{-3}	3.35×10^{-3}

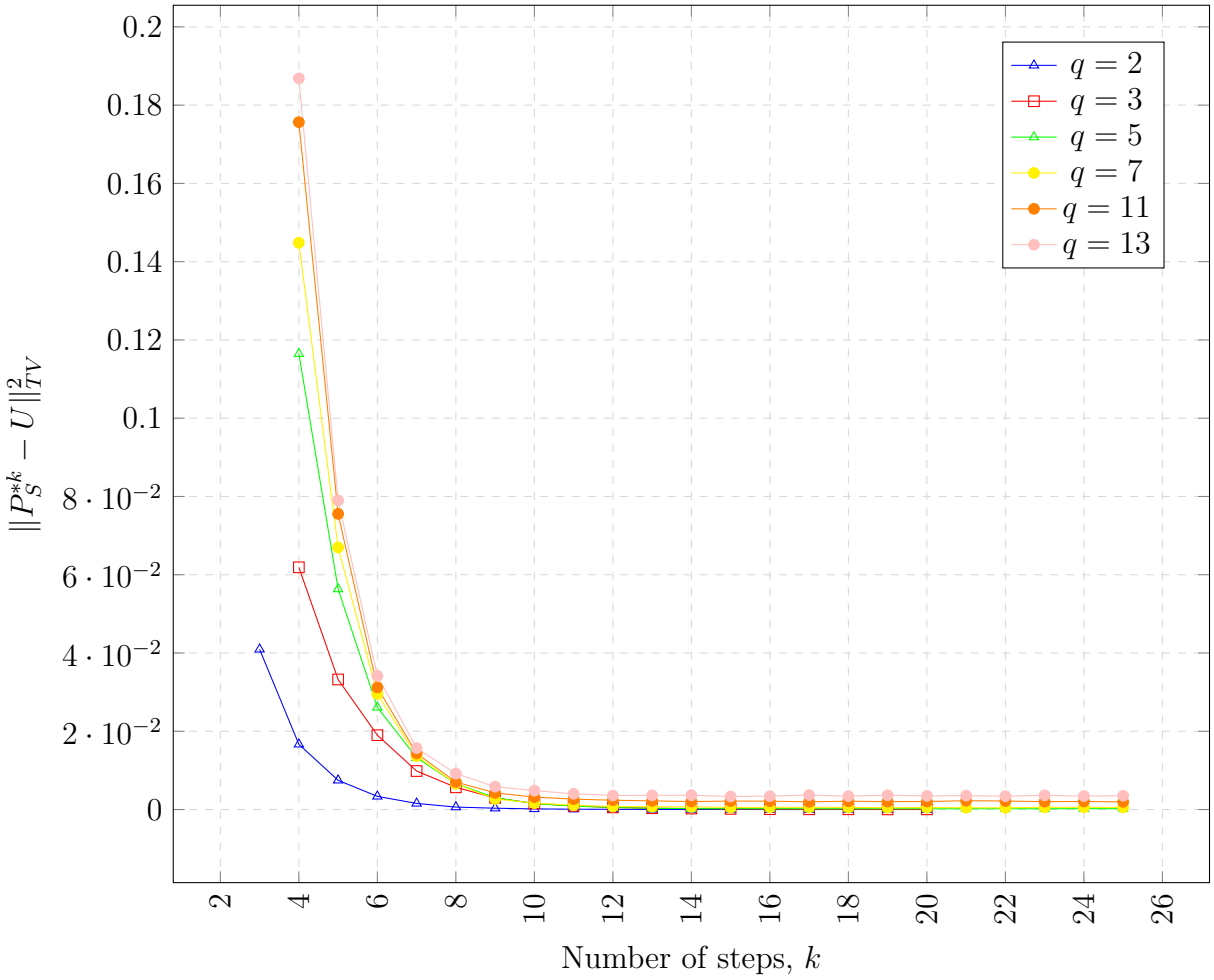

Figure 6.6: GAP Calculation for Upper Bounds of $SL_2(\mathbb{F}_q)$

6.6 Upper Bound on Frobenius Group

Let q be a prime power and

$$F_{q,q-1} = \left\{ \begin{bmatrix} 1 & b \\ 0 & a \end{bmatrix} : a \in (\mathbb{Z}/p\mathbb{Z})^*, b \in (\mathbb{Z}/p\mathbb{Z}) \right\}$$

Clearly order of $F_{q,q-1}$ is $q(q-1)$.

The set of generators considered for random walk on $F_{q,q-1}$ is

$$S = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, b = \begin{bmatrix} 1 & 0 \\ 0 & \mu \end{bmatrix} : \mu \in \mathbb{F}_q \text{ and is of order } q-1 \right\}$$

And probability used to drive the walk is

$$P_S = \frac{1}{|S|} \sum_{s \in S} \delta_S$$

6.6.1 Upper Bound for $F_{3,2}$

There are 3 representations of $F_{3,2}$ say φ_1, φ_2 and φ_3 such that φ_1 is trivial and φ_3 is the degree 2 representation. The set of generators used for random walk is

$$S = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, b = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \right\}$$

We need to evaluate $\widehat{P_S^{*k}}(\varphi_i)$ for $i = 2, 3$. Since $\widehat{P_S^{*k}}(\varphi_i) = \widehat{P_S}(\varphi_i)^k$, it is sufficient to evaluate $\widehat{P_S}(\varphi_i)$. So,

$$\begin{aligned} \widehat{P_S}(\varphi_i) &= \sum_{g \in F_{3,2}} P_S(g) \varphi_i(g) \\ &= \sum_{g \in F_{3,2}} \frac{1}{3} (\delta_1 + \delta_a + \delta_b)(g) \varphi_i(g) \\ &= \frac{\varphi_i(1) + \varphi_i(a) + \varphi_i(b)}{3} \text{ for } i = 2, 3 \end{aligned}$$

Now,

$$\widehat{P_S}(\varphi_2) = \frac{1}{3}$$

$$\widehat{P_S}(\varphi_3) = \begin{bmatrix} 1 + e^{2\pi i/3} & 1 \\ 1 & 1 + e^{4\pi i/3} \end{bmatrix}$$

$$\widehat{P_S^{*k}}(\varphi_2) (\widehat{P_S^{*k}})^*(\varphi_2) = \left(\frac{1}{3}\right)^{2k}$$

$$\widehat{P_S^{*k}}(\varphi_3) (\widehat{P_S^{*k}})^*(\varphi_3) = \begin{bmatrix} 2 & 2 + 2e^{2\pi i/3} \\ 2 + 2e^{4\pi i/3} & 2 \end{bmatrix}$$

Thus Upper Bound Lemma turns out to be

$$\begin{aligned} ||P_S^{*k} - U||_{TV}^2 &\leq \frac{1}{3^{2k}} + \frac{8}{3^{2k}} \\ &\leq \frac{1}{3^{2k-2}} \end{aligned}$$

Appendix A

GAP Program

We have written a GAP Program for simulation of a random walk on a given group G and S be set of generators. Given k, the number of steps, it also returns the total variation norm $\|P_S^{*k} - U\|_{TV}^2$.

```
#Simulation of Random Walk for any group G, with its set of
Generators, S and k is the number of steps we want to traverse.
All G, S and k are to be given by the user.


P := [];
iter := 100000;
for i in [1..iter] do
    a := Identity(G);
    for j in [1..k] do
        b := Random(S);
        a := b*a;
    od;
    Add(P,a);
od;
Q := Collected(P);
#Also this calculates ||P^*k-U||_TV for the specified group, G.
L := Concatenation(Q);
s := Length(L);
c := Order(G);
```

```
if s = 2*c then
    f := 0;
    for i in [1..c] do
        d := 2*i;
        e := Float(L[d]/iter);
        g := (e-Float(1/Order(G)));
        if SignFloat(g) = -1 then
             g := -1*g
        fi;
        f := f+g;
    od;
    f := Float((f*f)/4);
    s := s+1;
fi;
```

Bibliography

[Bum97] Daniel Bump, *Automorphic forms and representations*, Cambridge Studies in Advanced Mathematics, vol. 55, Cambridge University Press, Cambridge, 1997. MR 1431508

[Dia88] Persi Diaconis, *Group representations in probability and statistics*, Institute of Mathematical Statistics Lecture Notes—Monograph Series, 11, Institute of Mathematical Statistics, Hayward, CA, 1988. MR 964069 (90a:60001)

[Dia10] ———, *Threads through group theory*, Character theory of finite groups, Contemp. Math., vol. 524, Amer. Math. Soc., Providence, RI, 2010, pp. 33–47. MR 2731916 (2012b:60247)

[GAP16] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.8.3*, 2016.

[Hil92] Martin Hildebrand, *Generating random elements in* $\mathrm{SL}_n(\mathbb{F}_q)$ *by random transvections*, J. Algebraic Combin. **1** (1992), no. 2, 133–150. MR 1226348

[JL01] G. James and M.W. Liebeck, *Representations and characters of groups*, Cambridge mathematical textbooks, Cambridge University Press, 2001.

[KK15] Dilpreet Kaur and Amit Kulshrestha, *Characters of real special 2-groups*, J. Ramanujan Math. Soc. **30** (2015), no. 4, 375–396.

[Ser77] Jean-Pierre Serre, *Linear representations of finite groups*, Springer-Verlag, New York-Heidelberg, 1977, Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42. MR 0450380 (56 #8675)

[Ste12] Benjamin Steinberg, *Representation theory of finite groups*, Universitext, Springer, New York, 2012, An introductory approach. MR 2867444 (2012j:20028)

Index