Notes on Representation Theory

1 Definitions and first theorems

1.1 Definitions and examples

Definition 1.1 (Two equivalent definitions)**.** A linear representation of a group G can be defined equivalently as:

- a **morphism** π from G to $GL(V)$ for some vector space V.
- an **action** of G on some vector space V, such that for any two vectors u and v in V, and for all $g \in G$, we have $g \cdot (u + v) = g \cdot u + g \cdot v$.

From the "morphism" point of view, the representation is generally denoted (V, π) or simply π, or even V when there is no ambiguity.

Remark 1.2. We will only consider vector spaces over $\mathbb{C}$ or $\mathbb{R}$. Representations over finite fields are also interesting, but slightly trickier [1], and we won't be needing them.

Example 1.3 (Trivial representation). A trivial representation of a group G on some vector space V is the morphism that sends every group element to the identity linear map on V.

Example 1.4 (A representation of the general linear group $GL_n(\mathbb{R})$). Let $G = GL(\mathbb{R}^n)$, $V = \mathbb{R}^n$. Then the identity $\rho : G \to GL(\mathbb{R}^n)$ defines a representation of $GL(\mathbb{R}^n)$.

Exercise 1.5 (A representation of the symmetric group S_n). Let $G = S_n$ and define for every permutation $\sigma \in S_n$ the matrix $\rho(\sigma)$ such that $\rho(\sigma)_{ij} = \delta_{i,\sigma(j)}$. Check that ρ defines a morphism $G \to GL_n(\mathbb{R})$. Composition with the morphism $GL_n(\mathbb{R}) \to GL(\mathbb{R}^n)$ associated to the canonical basis yields a representation of S_n.

The easiest way of building a representation is to take the direct sum of two representations, which can be thought of as "sticking them side by side".

Definition 1.6 (Direct sum of representations)**.** If (ρ, V) and (η, W) are two representations of a group G, then the direct sum of ρ and η is the representation $\rho \oplus \eta : G \to V \oplus W = V \times W$ defined by:

$$\forall g \in G, (\rho \oplus \eta)(g) : (v, w) \mapsto (\rho(g)[v], \eta(g)[w])$$

1.2 Subrepresentations, irreducibility

Definition 1.7 (Subrepresentation)**.** Let $\rho : G \to GL(V)$ be a linear representation of G. Suppose W is a subspace of V that is stable by G, *i.e.* such that $\forall g \in G, \rho(g)W \subseteq W$. We can therefore consider the morphism $\eta : G \to GL(W)$ such that for every $g \in G$, $\eta(g)$ and $\rho(g)$ coincide on W. Then (η, W) is also a representation of G. We call it a **subrepresentation** of (ρ, V).

[1] to be more specific, not all representations can be decomposed into a direct sum of irreducible representations

In particular, if (ρ, V) is a representation, then the trivial representation on V and ρ itself are subrepresentations of (ρ, V).

Definition 1.8 (Irreducible representations)**.** Let $\rho : G \to GL(V)$ be a linear representation of G. If the only subrepresentations of (ρ, V) are the trivial representation on V and ρ itself, then (ρ, V) is said to be an **irreducible representation**.

Exercise 1.9 (A representation of the symmetric group S_n). By considering the orthogonal of $\mathbb{R}\mathbf{1}$, where $\mathbf{1}$ is the constant vector with all coordinates equal to 1, show that the representation of S_n defined in the previous exercise is not irreducible.

1.3 Decomposition

Our goal in this section is to show that the irreducible representations of a group are the elementary building blocks that make up other representations. We start with a motivating example.

Example 1.10. Let A be a unitary $n \times n$-matrix: A can be viewed as a representation π of $\mathbb{Z}$ on $V = \mathbb{C}^n$, namely the morphism that sends every $k \in \mathbb{Z}$ to the linear map represented by A^k in the usual basis of $\mathbb{C}^n$.

By the fundamental theorem of algebra, we know that the characteristic polynomial of A has at least one root, meaning that A has at least an eigenvalue. Therefore there exists a complex line that is left invariant by A. Since A is unitary, it also preserves the orthogonal complement of this line. By induction, we deduce that A is diagonalizable.

In terms of the representation of $\mathbb{Z}$, this implies that π can be decomposed into a direct sum of irreducible subrepresentations of dimension 1, in such a way that the multiplicity of each irreducible representation is equal to the multiplicity of the corresponding eigenvalue of A.

If A satisfies $A^d = 1$ for some $d \in \mathbb{N}$, then π can be seen as a representation of the finite group $\mathbb{Z}/d\mathbb{Z}$, and the same reasoning shows that this representation can be split into its irreducible parts.

In what follows, we shall show a generalization of this result. Notice that in the example, it was key that A be a unitary matrix: this way the orthogonal complement of an invariant line is also invariant. To generalize this, we introduce the notion of a **unitary representation**.

Definition 1.11 (Unitary representation)**.** If V is a Hilbert space, and if π maps G to the unitary group of V (those elements of $GL(V)$ that preserve the scalar product), then the representation is called **unitary**.

Theorem 1.12 (Representations of a finite group can be made unitary)**.** *If (ρ, V) is a representation of a finite group G, then there is an inner product $\langle -, - \rangle_G$ such that:*

$$\forall g \in G, \forall (u, v) \in V^2, \langle \rho(g)u, \rho(g)v \rangle_G = \langle u, v \rangle_G$$

Said otherwise, V can be equipped with an inner product in such a way that (ρ, V) is a unitary representation.

Proof. Let $\langle -, - \rangle$ be an inner product on V. Define the new inner product $\langle -, - \rangle_G$ as:

$$\forall (u, v) \in V^2, \langle u, v \rangle_G = \frac{1}{|G|} \sum_{g \in G} \langle u, v \rangle$$

Then for every $h \in G$, $\langle \rho(h)u, \rho(h)v \rangle_G = \frac{1}{|G|} \sum_{g \in G} \langle \rho(g)\rho(h)u, \rho(g)\rho(h)v \rangle$ by definition of $\langle -, - \rangle_G$. Taking $g' = gh$ yields $\frac{1}{|G|} \sum_{g' \in G} \langle \rho(g')u, \rho(g')v \rangle$ which is equal to $\langle u, v \rangle_G$. □

Theorem 1.13 (Invariant complement)**.** *Let* (η, W) *be a subrepresentation of some unitary representation* (ρ, V)*. Then there exists another subrepresentation* (η^0, W^0) *of* (ρ, V) *such that* $V = W \oplus W^0$ *and* $\rho = \eta \oplus \eta^0$*.*

Proof. Define W^0 as the orthogonal complement of W. It suffices to show that W^0 is stable under the action of G. Let $g \in G$ and $u \in W^0$. Since ρ is unitary: $\forall w \in W, \langle \rho(g)u, w\rangle = \langle u, \rho(g)w\rangle$.

Moreover, W is stable under the action of G, so u and $\rho(g)w$ are orthogonal, which concludes the proof. □

The following theorem follows immediately by induction:

Theorem 1.14 (Decomposition of unitary representations)**.** *Every unitary representation can be split into a* ***direct sum of irreducible representation****. In particular, every representation of a finite group is a direct sum of irreducible representation.*

2 Intertwiners and Schur's lemma

2.1 Intertwiners and Equivalence

Definition 2.1 (Representation homomorphisms)**.** Let (ρ_1, V_1) and (ρ_2, V_2) be two linear representations of a group G. A linear map $f : V_1 \to V_2$ is called a **representation homomorphism** if it **intertwines** ρ_1 and ρ_2, namely:

$$\forall g \in G, f \circ \rho_1(g) = \rho_2 \circ f$$

This is equivalent to the commutation of the following square, for every $g \in G$:

$$\begin{array}{ccc} V_1 & \xrightarrow{f} & V_2 \\ \downarrow{\scriptstyle \rho_1(g)} & & \downarrow{\scriptstyle \rho_2(g)} \\ V_1 & \xrightarrow{f} & V_2 \end{array}$$

The set of representation homomorphisms from (ρ_1, V_1) to (ρ_2, V_2) is denoted by $\mathrm{Hom}_G(V_1, V_2)$.

Equivalence is the natural notion of equality from the point of view of representation theory. We will treat equivalent representations as equal in much the same way that we treat isomorphic vector spaces as equal.

Definition 2.2 (Equivalent representations)**.** Two linear representations (ρ_1, V_1) and (ρ_2, V_2) of a group G are said to be **equivalent** when there exists an intertwining linear map $f \in \mathrm{Hom}_G(V_1, V_2)$ that is an isomorphism.

Observe that $\mathrm{Hom}_G(V_1, V_2)$ is a vector subspace of $\mathrm{Hom}(V_1, V_2)$. More precisely it is the subspace of invariant vectors under the following linear action of G: $\pi(g)(f) = \rho_2(g) \circ f \circ \rho_1(g^{-1})$. Observe that π is a linear representation of G. The natural projection onto the subspace of invariant vectors of π is defined as

$$T(f) := \frac{1}{|G|} \sum_{g \in G} \pi(g)(f).$$

We immediately deduce the following useful lemma.

Lemma 2.3. *The following map defines a projection from* $\mathrm{Hom}(V_1, V_2)$ *onto* $\mathrm{Hom}_G(V_1, V_2)$*:*

$$T(f) = \frac{1}{|G|} \sum_{g \in G} \rho_2(g) \circ f \circ \rho_1(g^{-1}).$$

Exercise 2.4. Exhibit a scalar product on $\mathrm{Hom}(V_1, V_2)$ for which T is an orthogonal projection.

2.2 Schur's Lemma

Theorem 2.5 (Schur's lemma)**.** *Let (ρ_1, V_1) and (ρ_2, V_2) be two irreducible representations of a group G, and $T \in \mathrm{Hom}_G(V_1, V_2)$.*

1. *if ρ_1 and ρ_2 are not equivalent, then $f = 0$*
2. *if $\rho_1 = \rho_2 = \rho$ and $V_1 = V_2 = V$, then f is a constant times the identity id_V*

Proof. Let $x \in \mathrm{Ker}\, f$ and $g \in G$: since f is intertwining, $f(\rho_1(g)x) = \rho_2(g)f(x) = 0$. Therefore $\mathrm{Ker}\, f$ is stable under the action of G. If ρ_1 and ρ_2 are not equivalent, T cannot be an isomorphism, so $\mathrm{Ker}\, f \neq 0$. Since ρ_1 is irreducible, necessarily $\mathrm{Ker}\, f = V_1$ and $f = 0$, hence the first part of Schur's lemma.

If $\rho_1 = \rho_2 = \rho$ and $V_1 = V_2 = V$, then if $f \neq 0$, then f has a non-zero eigenvalue λ. $f - \lambda \mathrm{id}_V$ is also in $\mathrm{Hom}_G(V, V)$, and $\mathrm{Ker}\,(f - \lambda \mathrm{id}_v) \neq 0$: the first part of the proof show that $\mathrm{Ker}\,(f - \lambda \mathrm{id}_v) = V$, so that $f = \lambda \mathrm{id}_V$. If $f = 0$ then the result is also true, which concludes the proof of Schur's lemma. □

3 Uniqueness of the decomposition in irreducible representations

A first impressive consequence of Schur's lemma is the following result.

Theorem 3.1. *Let (V, π) be a representation of a finite group G. There exists a* ***unique orthogonal decomposition***

$$V = \oplus_\rho W_\rho,$$

where for each isomorphism class of irreducible representation ρ, the subspace W_ρ is $\pi(G)$-invariant and if non-zero, (W_ρ, π) is isomorphic to a direct sum of copies of ρ (we call it a multiple of ρ).

Proof. Existence has already been established in Theorem 1.14. To prove uniqueness, we shall need the following lemma.

Lemma 3.2. *Two non-equivalent irreducible subrepresentations of a unitary representation are in orthogonal direct sum.*

Proof. This is an almost immediate consequence of the Schur Lemma. Indeed, assume V_1 and V_2 are invariant subspaces, such that (V_1, π) and (V_2, π_2) are isomorphic to two non-isomorphic irreducible representations of G. The restriction of orthogonal projection on V_2 to V_1 interwines these two irreducible representations. So by the Schur lemma, this linear map must equal 0. □

Let us now finish proving the uniqueness of the orthogonal decomposition of a representation: assume $V = \bigoplus_\rho W_\rho = \bigoplus_\rho W'_\rho$ are two such decompositions, where the restriction of π to W_ρ (resp. W'_ρ) is isomorphic to a multiple of ρ. Let $V_\rho \subset W_\rho$ be an invariant subspace, whose restriction of π is isomorphic to ρ. Then by the previous lemma, V_ρ is orthogonal to every $W'_{\rho'}$, for $\rho' \neq \rho$. So it follows that V_ρ is contained in W'_ρ. Therefore $W_\rho \subset W'_\rho$, and by symmetry of the argument, they must be equal, so we are done. □

4 Character of a representation

4.1 Definition and basic properties

Definition 4.1 (Character of a representation)**.** Let (ρ, V) be a representation of a finite group G. The character of (ρ, V) is the group morphism $\chi_\rho : G \to \mathbb{C}$ defined by:

$$\forall g \in G, \chi_\rho(g) = \mathrm{Tr}[\rho(g)]$$

Proposition 4.2 (Elementary properties of characters). *Let (ρ, V) be a representation of a finite group G, and χ_ρ be the character of ρ. Then:*

1. $\chi_\rho(e_G) = \dim(V)$
2. $\forall g, h \in G, \chi_\rho(gh) = \chi_\rho(hg)$
3. $\forall g \in G, \chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$

Proposition 4.3 (Additivity). *Assume $\rho = \rho_1 \oplus \rho_2$ then $\chi_\rho = \chi_{\rho_1} + \chi_{\rho_2}$.*

4.2 Orthogonality of coefficients and of characters

Definition 4.4 (Scalar product on $\ell^2(G)$). If G is a finite group, we can turn the vector space $\mathbb{C}^G$ of functions $G \to \mathbb{C}$ into a Hilbert space by equipping it with the inner form $\langle , \rangle$ defined as follows:

$$\forall f, h \in \mathbb{C}^G, \langle f, h \rangle = \frac{1}{|G|} \sum_{g \in G} f(g)\overline{h(g)}$$

The corresponding Hilbert space is sometimes denoted by $\ell^2(G)$.

Definition 4.5 (Coefficient of a representation). Let (ρ, V) be a unitary representation of dimension $n \in \mathbb{N}$ and $(e_i)_{1 \le i \le n}$ be an orthogonal basis of V. A **coefficient** of the representation (ρ, V) is some function $r^\rho_{ij} : G \to \mathbb{C}$ of the form $r^\rho_{ij} : g \mapsto \langle \rho(g)e_i, e_j \rangle$.

Said otherwise, the coefficient r^ρ_{ij} is the function sending every $g \in G$ to the entry of position (i, j) in the matrix in the basis $(e_i)_{1 \le i \le n}$ of the linear map $\rho(g)$.

Proposition 4.6 (Orthogonality of coefficients). *The (matrix) coefficients of distinct irreducible representations are orthogonal. Moreover, if ρ is irreducible, then distinct matrix coefficients are orthogonal, and the square norm of a matrix coefficient is the inverse of the dimension.*

1. *Let (ρ_1, V_1) and (ρ_2, V_2) be distinct irreducible representations of respective dimensions n_1 and n_2. If $1 \le i, j \le n_1$ and $1 \le k, l \le n_2$, then the functions $r^{\rho_1}_{ij} \in \mathbb{C}^G$ and $r^{\rho_2}_{kl} \in \mathbb{C}^G$ are orthogonal.*
2. *Let (ρ, V) be an irreducible representation of dimension n, and $1 \le i, j, k, l \le n$ such that $(i, j) \ne (k, l)$. Then the functions $r^\rho_{ij} \in \mathbb{C}^G$ and $r^\rho_{kl} \in \mathbb{C}^G$ are orthogonal, and $\langle r_{ij}, r_{ij} \rangle = \frac{1}{\dim(\rho)}$.*

Proof. We equip V_1 and V_2 with orthonormal bases $(e_i)_{1 \le i \le n_1}$ and $(b_j)_{1 \le j \le n_2}$. Let (e^*_i) and (b^*_j) be dual bases of respectively (e_i) and (b_j).

In the first case, consider for every $1 \le k \le n_1$ and $1 \le l \le n_2$ the linear map $h_{kl} : V_1 \to V_2$ sending e_k to b_l, and e_m to 0 if $m \ne k$. In other words, $h_{kl} = b_l e^*_k$.

Then by Lemma 2.3, $f_{kl} = \frac{1}{|G|} \sum_{g \in G} \rho_2(g) h_{kl} \rho_1(g^{-1}) \in \mathrm{Hom}_G(V_1, V_2)$. Since (ρ_1, V_1) and (ρ_2, V_2) are not equivalent, the first statement of the Schur's lemma implies that $f_{kl} = 0$. Consider the matrix of f_{kl} with respect to (e_i) and (b_j): all its entries are zero. In other words, for all $1 \le i \le n_1$ and $1 \le j \le n_2$,

$$\begin{aligned}
0 &= b^*_j \circ f_{kl}(e_i) \\
&= \frac{1}{|G|} \sum_{g \in G} b^*_j \circ \rho_2(g) \circ h_{kl} \rho_1(g^{-1})(e_i) \\
&= \frac{1}{|G|} \sum_{g \in G} b^*_j(\rho_2(g)(b_l)) e^*_k(\rho(g^{-1})(e_i)) \\
&= \frac{1}{|G|} \sum_{g \in G} r^{\rho_2}_{jl}(g) \overline{r^{\rho_1}_{ki}(g)} \\
&= \langle r^{\rho_1}_{jl}, r^{\rho_2}_{ki} \rangle.
\end{aligned}$$

This proves the first part of the proposition. For the second part of the proposition, we define $h_{ij} = e_j e_i^*$, for all $1 \leq i, j \leq n_1$. The second statement of the Schur lemma implies that $f_{ij} = \frac{1}{|G|} \sum_{g \in G} \rho_1(g) h_{ij} \rho_1(g^{-1})$ is a constant times the identity. Observe that $\text{Tr}(f_{ij}) = \text{Tr}(h_{ij})$, which therefore equals 0 if $i \neq j$ and 1 if $i = j$. Hence, $f_{ij} = 0$ if $i \neq j$ and $\frac{1}{n_1}\text{id}$ if $i = j$. The second statement of the proposition now follows by computing the matrix coefficients of f_{ij} as above. □

Theorem 4.7 (Orthogonality of characters)**.** *Characters of irreducible representations form an orthonormal family of functions in $\ell^2(G)$.*

Proof. Orthogonality follows from the first item of the previous proposition and the fact that characters are unit vectors is a straightforward consequence of the second item. □

5 The regular representation

5.1 Definition, examples and main properties

Definition 5.1 (Regular representation)**.** Let G be a finite group: consider the Hilbert space $l^2(G) = \mathbb{C}^G$ introduced above. The **regular representation** λ of G sends every group element $g \in G$ to the unique linear map $\lambda(g) : l^2(G) \to l^2(G)$ defined on the basis elements $(\mathbf{1}_h)_{h \in G}$ by:

$$\forall h \in G, \lambda(g)(\mathbf{1}_h) = \mathbf{1}_{gh}$$

The regular representation of a group is a special case of a more general kind of representations: *quasiregular* representations.

Definition 5.2 (Quasiregular representation)**.** Let G be a finite group acting on a set X. The associated **quasiregular representation** of G is the morphism sending every element $g \in G$ to the endomorphism of $l^2(X) = \mathbb{C}^X$ defined on the basis elements $(\mathbf{1}_x)_{x \in X}$ by:

$$\forall x \in X, \lambda(g)(\mathbf{1}_x) = \mathbf{1}_{g \cdot x}$$

Proposition 5.3 (Characters of the regular representation)**.** *Consider the regular representation λ_G of a group G of identity element e_G. Then $\chi_{\lambda_G}(e_G) = Card(G)$, and for every $g \in G$ such that $g \neq e_G$, $\chi_{\lambda_G}(g) = 0$.*

Corollary 5.4. *Let G be a finite group. Every irreducible representation of G is contained in the regular one, with multiplicity equal to its dimension.*

Proof. We have just seen that the character of the regular representation equals $|G|$ at the neutral element and 0 elsewhere. Hence we have for every irreducible representation ρ, that its multiplicity equals

$$m_\rho = \langle \chi_\lambda, \chi_\rho \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_\lambda(g) \chi_\rho^*(g) = \chi_\rho^*(1) = d,$$

where d is the dimension of ρ. □

5.2 Space of central functions

Two elements s and t of a group G are said to be **conjugate** if usu^{-1} for some u in G. Thus in an abelian group each conjugacy classe has exactly one element, so that the number of conjugacy classes equals $|G|$. A function f on G that is constant on conjugacy classes is called a **class function**.

Proposition 5.5. *Let f be a class function on G. Let $\rho : G \to GL(V)$ be an irreducible representation of G. Then $\hat{f}(\rho) = \lambda * I$ with*

$$\lambda = \frac{1}{\rho_p}\Sigma f(t)\chi_\rho(t) = \frac{|G|}{d_\rho}\left(f|\chi_\rho^*\right)$$

Proof.

$$\rho_s\hat{f}(\rho)\rho_s^{-1} = \Sigma f(t)\rho(t)\rho(s^{-1}) = \Sigma f(t)\rho(sts^{-1}) = \hat{f}(\rho)$$

Using Schur's lemma, one may conclude that $\hat{f}_\rho = \lambda I$. Then take traces on both side to obtain λ. □

Theorem 5.6 (Basis of the space of central functions)**.** *The characters of the irreducible representations: $\chi_1, .., \chi_h$ form an orthonormal basis of the space of class functions $G \to \mathbb{C}$.*

Proof. Characters are class class functions. Moreover it has been proved above that they are orthonormal. It remains to show that they are enough. Suppose that $\left(f|\chi_\rho^*\right) = 0$ for all ρ irreductible. The previous proposition gives $\hat{f}(\rho) = 0$ for all ρ. Thus one obtain $f = 0$.

□

Theorem 5.7 (Number of irreducible representations)**.** *The number of irreducible representations of G is equal to the number of conjugacy classes in G.*

Proof. The number h of irreducible representations is also the dimension of the space of class functions. The number of conjugacy classes equals the dimension of class functions (the value of a class function on each conjugate classe can be defined arbitrary). □

Proposition 5.8. *The following properties are equivalent*

1. *G is Abelian*
2. *All irreducible representation of G have degree 1*

Proof. We have $\Sigma d_{rho}^2 = |G|$. If G is abelian, there are $|G|$ conjugate classes, for all ρ, $d_\rho = 1$. If all $d_\rho = 1$, then there must be $|G|$ conjugate classes, thus for all s, t, $sts^{-1} = t$. G is abelian.

□

6 The Fourier Transform

6.1 Definition and examples

Definition 6.1 (Fourier transform)**.** Let $f : G \to \mathbb{C}$ be a function, with G a finite group and ρ a representation of G. The **Fourier transform** $\hat{f}(\rho)$ of f at ρ is the linear map defined by:

$$\hat{f}(\rho) = \sum_{g \in G} f(g)\rho(g)$$

Definition 6.2 (Convolution)**.** Let $f_1 : G \to \mathbb{C}$ and $f_2 : G \to \mathbb{C}$ be two functions in $l^2(G)$. Then the **convolution** $f_1 * f_2 : G \to \mathbb{C}$ of f_1 and f_2 is the function:

$$(f_1 * f_2) : g \mapsto \frac{1}{|G|}\sum_{h \in G} f_1(gh^{-1})f_2(h)$$

One of the advantages of Fourier transforms is that they behave well with respect to convolution:

Proposition 6.3 (Fourier transforms and convolution)**.** *Let $f_1 : G \to \mathbb{C}$ and $f_2 : G \to \mathbb{C}$ be two functions in $l^2(G)$, of respective Fourier transforms $\hat{f}_1(\rho)$ and $\hat{f}_2(\rho)$ with ρ a representation of G. Then:*

$$(f_1 \hat{*} f_2)(\rho) = \hat{f}_1(\rho) \circ \hat{f}_1(\rho)$$

6.2 Plancherel and the inverse Fourier transform

Theorem 6.4. *Let f and h be functions on G. Then we have*

- *The Inverse Fourier formula:*

$$f(g) = \frac{1}{|G|} \sum_{\rho} d_\rho \cdot \mathrm{Tr}(\rho(g^{-1})\hat{f}(\rho)),$$

  where the sum is taken over all irreducibles.

- *The Plancherel formula:*

$$\sum_{g \in G} f(g^{-1})h(g) = \frac{1}{|G|} \sum_{\rho} d_\rho \cdot \mathrm{Tr}(\hat{f}(\rho)\hat{h}(\rho)).$$

Proof. Both being linear in f, it suffices to prove it for f equal the Dirac at an element k. In this case $\hat{f}(\rho) = \rho(k)$. The right-hand term is

$$\frac{1}{|G|} \sum_{\rho} d_\rho \mathrm{Tr}(\rho(g^{-1}k),$$

which equals 0 if $k \neq g$ and $\frac{1}{|G|} \sum_\rho d_\rho^2 = 1$ (by Theorem 5.4) if $g = k$. □

7 The upper bound lemma

This section shows how representation theory can be used to bound the total variation distance between a probability distribution and the uniform distribution, thereby allowing us to prove cutoff behaviours.

7.1 The lemma

Lemma 7.1 (Upper bound lemma)**.** *Let Q be a probability distribution on a finite group G. Then:*

$$||Q - U||_{TV}^2 \leq \frac{1}{4} \sum_{\rho \in Irr(G)} d_\rho \cdot tr(\hat{Q}(\rho)\hat{Q}(\rho)^*)$$

where:

- *the sum is over all the non-trivial irreducible representations of G*
- *d_ρ denotes the dimension of representation ρ*
- *$\hat{Q}(\rho)^*$ is the adjoint of the endomorphism $\hat{Q}(\rho)$*

Proof. We use the definition of the Total Variation Distance as half the l^1 norm:

$$\begin{aligned} ||Q - U||_{TV}^2 &= \frac{1}{4}(\sum_{g \in G} |Q(g) - 1/|G||)^2 \\ &\leq \frac{1}{4}|G| \cdot \sum_{g \in G} (Q(g) - 1/|G|)^2 \quad (Cauchy - Schwarz) \\ &\leq \frac{1}{4} \sum_{\rho \in Irr(G)} d_\rho \cdot tr[(\hat{Q} - \hat{U})(\rho)(\hat{Q} - \hat{U})^*(\rho)] \quad (Plancherel) \end{aligned}$$

For a trivial representation ρ we have $Q(\rho) = U(\rho)$: these representations therefore don't intervene in the sum. For a non-trivial representation ρ we have $\hat{U}(\rho) = \frac{1}{|G|}\sum_{g\in G}\rho(g) = 0$. Therefore:

$$||Q - U||_{TV}^2 \leq \frac{1}{4}\sum_{\rho\in Irr(G)} d_\rho \cdot tr(\hat{Q}(\rho)\hat{Q}^*(\rho))$$

□

7.2 Lower bounds

Showing that a sequence of random walks has a cutoff (or pre-cutoff) at some time τ_n entails asymptotically bounding the total variation distance both above and below. The following propositions provide lower bounds for $||Q - U||_{TV}$:

Proposition 7.2 (First lower bound). *Let Q be a probability distribution on a finite group G. Then:*

$$||Q - U||_{TV} \geq \frac{1}{2|G|}\sum_{\rho\in Irr(G)} d_\rho \cdot tr(\hat{Q}(\rho)\hat{Q}(\rho)^*)$$

Proof. We use the fact that for every $g \in G$, $-1 \leq Q(g) - 1/|G| \leq 1$. Therefore:

$$\begin{aligned} ||Q - U||_{TV} &= \frac{1}{2}\sum_{g\in G}|Q(g) - 1/|G|| \\ &\geq \frac{1}{2}\sum_{g\in G}(Q(g) - 1/|G|)^2 \\ &\geq \frac{1}{2|G|}\sum_{\rho\in Irr(G)} d_\rho \cdot tr(\hat{Q}(\rho)\hat{Q}(\rho)^*) \quad (Plancherel) \end{aligned}$$

□

Proposition 7.3 (Second lower bound). *Let Q be a probability distribution on a finite group G. Then:*

$$||Q - U||_{TV}^2 \geq \frac{1}{4|G|}\sum_{\rho\in Irr(G)} d_\rho \cdot tr(\hat{Q}(\rho)\hat{Q}(\rho)^*)$$

Proof.

$$\begin{aligned} ||Q - U||_{TV}^2 &= \frac{1}{4}(\sum_{g\in G}|Q(g) - 1/|G||)^2 \\ &\geq \frac{1}{4}\sum_{g\in G}(Q(g) - 1/|G|)^2 \\ &= \frac{1}{4|G|}\sum_{\rho\in Irr(G)} d_\rho \cdot tr(\hat{Q}(\rho)(\hat{Q}^*(\rho)) \quad (Plancherel) \end{aligned}$$

□

Despite these lemmas, most of the time finding lower bounds involves exhibiting an *ad hoc* subset of G such that $|Q(A) - U(A)|$ is large enough.

Given a random walk defined by the probability distribution Q and with a uniform invariant measure, we are interested in the total variation distance $||Q^{*k} - U||$, where Q^{*k} denotes the convolution of Q with itself, k times. Conveniently, we recall that Fourier transforms behave well with regard to convolution, so that $\hat{Q^{*k}}(\rho) = (\hat{Q})^k(\rho)$.