REPRESENTATION THEORY OF PSL$_2(q)$

YAQIAO LI

Following are notes from book [1]. The aim is to show the quasirandomness of PSL$_2(q)$, i.e., the group has no low dimensional representation.

1. Representation Theory of Finite Groups

Let $G$ be a finite group, in the following we recall some elementary representation theory for $G$. Say $(\pi, V)$ is a representation of $G$ we mean $V$ is a (finite-dimensional) complex vector space and $\pi: G \to \text{GL}(V)$ is a group homomorphism. The dimension of the representation $(\pi, V)$ is just the dimension of $V$ over $\mathbb{C}$, we consider only finite dimensional representation in this note. Say a representation $(\pi, V)$ is irreducible if $V$ has no nontrivial $G$-invariant subspace, for example 1-dimensional representations are all irreducible. Say the representation is faithful if $\pi$ is injective, for example all nontrivial representations for simple groups are faithful.

A first result is the Schur’s Lemma. Let $(\pi, V)$ and $(\rho, W)$ be two representations of $G$, and $\text{Hom}_G(\pi, \rho)$ be the vector space of interwiners $T$, that is, $T: V \to W$ is a linear map and $\rho(g) \circ T = T \circ \pi(g)$ holds for every $g \in G$. Say $\pi \cong \rho$ if there exists an invertible $T \in \text{Hom}_G(\pi, \rho)$.

Lemma 1.1 (Schur). Let $(\pi, V)$ and $(\rho, W)$ be two finite-dimensional and irreducible representations of $G$, then

$$\dim \text{Hom}_G(\pi, \rho) = \begin{cases} 0, & \pi \not\cong \rho; \\ 1, & \pi \cong \rho. \end{cases}$$

Proof. Consider the kernel and image of $T \in \text{Hom}_G(\pi, \rho)$, use the irreducibility. To show the dimension equals 1 when $\pi \cong \rho$, is equivalent to show all $T \in \text{Hom}_G(\pi, \rho)$ are just scalars, hence we should consider the eigenvalue $\lambda$ of $T$, then it's equivalent to show $T - \lambda I = 0 \iff \text{Ker}(T - \lambda I) = V$. \hfill \Box

Next we give some standard operations of representations, enabling us to construct new representations from given representations. The direct sum and tensor product is defined in the anticipated way as follows,

$$(\pi \oplus \rho)(g)(v, w) = (\pi(g)v, \rho(g)w), \quad (\pi \otimes \rho)(g)(v \otimes w) = \pi(g)v \otimes \rho(g)w,$$

acting on spaces $V \oplus W$ and $V \otimes W$, respectively. The conjugate representation $(\pi^*, V^*)$ (recall $V^* = \text{Hom}(V, \mathbb{C})$ is the dual space of $V$) is defined as

$$(\pi^*(g)f)(v) = f(\pi(g^{-1})v), \quad f \in V^*.$$

Note that we can identify the tensor space $W \otimes V^*$ with $\text{Hom}(V, W)$ naturally by identifying a tensor $w \otimes f$ as a linear map from $V$ to $W$ as $(w \otimes f)(v) = f(v)w$, and both of these two spaces have dimension $\dim(V) \times \dim(W)$, hence it's easy to see the following useful fact.

Lemma 1.2 (Equivalence of two representations). We have the following two representations are equivalent

$$(\sigma, \text{Hom}(V, W)) \cong (\rho \otimes \pi^*, W \otimes V^*),$$

where $\sigma(g)(T) = \rho(g)T\pi(g^{-1})$ for $T \in \text{Hom}(V, W)$.

Date: May 21, 2015.

McGill University, yaqiao.li@mail.mcgill.ca.
An extremely important and useful notion in representation theory of finite groups is the characters. The character of representation \((\pi, V)\) is the complex valued function \(\chi_\pi : G \to \mathbb{C}\) defined as \(\chi_\pi(g) = \text{tr}(\pi(g))\), the trace of \(\pi(g)\).

Some examples are as follows. Consider the following\[V^G := \{ v \in V : \pi(g)v = v, \ \forall \ g \in G\},\]which is the subspace of \(V\) fixed by \(G\). We show the following

**Lemma 1.3** (The sum of a character on \(G\)). We have\[\sum_{g \in G} \chi_\pi(g) = |G| \dim V^G.\]

**Proof.** Consider the “average operation” \(A_\pi := \frac{1}{|G|} \sum_{g \in G} \pi(g)\) on \(V\); clearly it’s idempotent, i.e., \(A_\pi^2 = A_\pi\). Recall that as an idempotent matrix we have \(r(A_\pi) = \text{tr}(A_\pi)(\text{this can be seen by that idempotent matrix is diagonalizable and has eigenvalues only 0 and 1})\) where \(r(A_\pi)\) is the rank of \(A_\pi\), note \(r(A_\pi) = \dim \text{Im} A_\pi\), and it’s easy to see that \(\text{Im} A_\pi = V^G\), hence \(\dim V^G = \text{tr}(A_\pi)\) which reduces to the desired equality. 

As a second example consider the left regular representation \((\lambda_G, V = CG)\) defined as \((\lambda(g)f)(x) = f(g^{-1}x)\) for \(g, x \in G\). In this case it’s easy to see \(\dim V^G = 1\) (since \(V^G\) consists only of constant functions on \(G\)), hence we have \(\sum_{g \in G} \chi_{\lambda_G}(g) = |G| \dim(V^G) = |G|\). But clearly we have \(\chi_{\lambda_G}(e) = |G|\), hence \(\chi_{\lambda_G}(g) = 0\) for all other \(g \neq e\).

Following are some easy-to-verify facts about characters.

**Lemma 1.4** (Properties of characters). Let \((\pi, V)\) and \((\rho, W)\) be two representations of \(G\),
- character and dimension \(\chi_\pi(e) = \dim V\);
- we have (by considering \(G\)-invariant inner product) \(\chi_\pi(g^{-1}) = \chi_\pi(g)\), \(\chi_\pi(hgh^{-1}) = \chi_\pi(g)\) \(\forall \ h \in G\);
- if \(\pi \cong \rho\) then \(\chi_\pi = \chi_\rho\);
- the characters after operations, \(\chi_{\pi \circ \rho} = \chi_\pi \cdot \chi_\rho\).

One remark about above properties: the \(G\)-invariant inner product \(\langle \cdot, \cdot \rangle\) on \(V\) can be constructed by applying the Weyl unitary trick on any given inner product \(\langle \cdot, \cdot \rangle\) as follows, \[\langle u, v \rangle = \sum_{g \in G} (\pi(g)u, \pi(g)v).\]

Now we turn to an important fact. The inner product of complex valued functions on \(G\) is defined as usual, hence we can consider the inner product of characters.

**Theorem 1** (Orthogonality). Let \((\pi, V)\) and \((\rho, W)\) be two irreducible representations of \(G\), then\[\langle \chi_\pi, \chi_\rho \rangle = \begin{cases} 0, & \pi \not\cong \rho; \\ 1, & \pi \cong \rho. \end{cases}\]

**Proof.** By Schur’s lemma, it’s equivalent to show \(\langle \chi_\pi, \chi_\rho \rangle = \dim \text{Hom}_G(\pi, \rho)\). To keep notation consistence, we compute \(\langle \chi_\rho, \chi_\pi \rangle\) instead, as follows,
\[
\langle \chi_\rho, \chi_\pi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g)\overline{\chi_\pi(g)} = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g)\chi_\pi^*(g) = \frac{1}{|G|} \sum_{g \in G} \chi_{\rho \circ \pi^*}(g)
\]
\[
= \frac{1}{|G|} \sum_{g \in G} \chi_\sigma(g) = \dim \text{Hom}(V, W)^G = \dim \text{Hom}_G(\pi, \rho).
\]
Note in the above computation, we have successively used Lemma 1.4, 1.2 and 1.3. The last equality follows by observing that $\text{Hom}(V, W)^G = \text{Hom}_G(\pi, \rho)$.

The orthogonality, as usual, enables us to decompose any representation $(\pi, V)$ into a sum of irreducible representations. Specifically we have the following structure theorem.

**Theorem 2** (Decomposition of a representation into irreducibles). Let $(\pi_i, W_i), i = 1, \ldots, k$ be all the distinct irreducible representations of $G$, then every representation $(\pi, V)$ can be decomposed uniquely as

$$\pi = \sum_{i=1}^{k} m_i \pi_i,$$

where $m_i = \langle \chi_\pi, \chi_{\pi_i} \rangle$ is the number of representations equivalent to $\pi_i$ in the decomposition of $\pi$. In particular, we have the degree formula,

$$|G| = \sum_{i=1}^{k} (\dim W_i)^2.$$

**Proof.** The decomposition is clear. Apply it to the left regular representation $(\lambda_G, \mathbb{C}G)$, recall previously we have seen that $\chi_{\lambda_G}(e) = |G|$ and $\chi_{\lambda_G}(g) = 0$ for all other $g \neq e$, hence

$$m_i = \langle \chi_{\lambda_G}, \chi_{\pi_i} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{\lambda_G}(g) \chi_{\pi_i}(g) = \chi_{\pi_i}(e) = \dim W_i.$$

Evaluating $\lambda_G$ through the decomposition formula on the identity gives the degree formula. $\square$

As a quick application we describe the irreducible representations of abelian groups.

**Corollary 1** (Irreducible representations of abelian groups). If $G$ is a finite abelian group, then it has exactly $|G|$ distinct irreducible representations, all of which are of dimension one.

**Proof.** By the degree formula, it suffices to show if $(\pi, V)$ is an irreducible representation of $G$, then $\dim V = 1$. Clearly the representation $(\pi, V)$ is equivalent to itself $(\pi, V)$, hence by Schur Lemma 1.1, we have $\dim \text{Hom}_G(\pi, \pi) = 1$, and actually we have seen that $\text{Hom}_G(\pi, \pi)$ is a set of scalars. Now $G$ is abelian implies that $\pi(g) \in \text{Hom}_G(\pi, \pi)$ for every $g \in G$, hence every $\pi(g)$ is a scalar. As a result, every 1-dimensional subspace of $V$ is $G$-invariant, but $(\pi, V)$ is irreducible, hence $V$ is itself of dimension one. $\square$

Clearly in this case (i.e., when $G$ is abelian) these $|G|$ distinct irreducible representations form an orthonormal basis for $\mathbb{C}G$. For example when $G = \mathbb{Z}_n$, let $\omega = e^{2\pi i/n}$, then these $n$ distinct irreducible representations are described by $\chi_k : \mathbb{Z}_n \rightarrow \mathbb{C}^\times$ for $k = 0, 1, \ldots, n-1$ where $\chi_k(r) := \omega^{kr}$ for $r \in \mathbb{Z}_n$. For general (non-abelian) finite groups, it can be shown that the number of irreducible representations equals to the number of conjugacy classes of $G$.

Now we give a construction of an irreducible representation which will be useful in the next section. A finite set $X$ is said to be a $G$-space if $G$ acts on $X$, specifically, if there is a homomorphism from $G$ to $\text{Sym}(X)$, that is each element in $G$ can be viewed as a permutation on $X$. Let $X$ be a $G$-space, we can consider the permutation representation $(\lambda_X, \mathbb{C}X)$ of $G$ as defined by

$$(\lambda_X(g) f)(x) = f(g^{-1}x)$$

where $f \in \mathbb{C}X$. If we choose the characteristic functions of $\mathbb{C}X$ as a basis, then it’s easy to see that $\lambda_X(g)$ are just permutation matrices for all $g \in G$. In particular we see that $\chi_{\lambda_X} : G \rightarrow \mathbb{C}$ is actually $\chi_{\lambda_X} : G \rightarrow \mathbb{N}$. It’s also easy to see that $\dim(\mathbb{C}X)^G$ equals the number of orbits of $X$.

Consider the $G$-space $X \times X$ by extending the action of $G$ on $X$ to $X \times X$ naturally, say a $G$-space $X$ is $2$-transitive if for any two ordered pairs $(x_1, y_1), (x_2, y_2) \in X \times X$ with $x_i \neq y_i$ for $i = 1, 2$, there exists an element $g \in G$ such that $g(x_1, y_1) = (gx_1, gy_1) = (x_2, y_2)$. Then $X$
is 2-transitive implies that $X \times X$ has exactly two orbits: the diagonal, and the rest. Hence $\dim(\mathbb{C}(X \times X))^G = 2$.

**Lemma 1.5** (An irreducible representation). Consider the $G$-invariant co-dimension one subspace of $\mathbb{C}X$,

$$W = \{ f \in \mathbb{C}X : \sum_{x \in X} f(x) = 0 \},$$

then $X$ is 2-transitive implies $\lambda_X|_W$ is an irreducible representation of $G$.

**Proof.** If we consider the two representations $(\lambda_X \otimes \lambda_X, \mathbb{C}(X \times X))$ and $(\lambda_X, \mathbb{C}X \otimes \mathbb{C}X)$, it is not hard to see that they are actually equivalent, hence $\chi_{\lambda_X \times \lambda_X}(g) = \chi_{\lambda_X \otimes \lambda_X}(g) = \chi_{\lambda_X}(g)^2$.

Also since $W$ is $G$-invariant and codimension one, the complement subspace $V$ of $W$ is just the constant functions, hence $\lambda_X|_V$ is the trivial representation, therefore $\lambda_X = 1 + \lambda_X|_W$.

Applying Lemma [1.3] we have

$$|G| \dim(\mathbb{C}(X \times X))^G = \sum_{g \in G} \chi_{\lambda_X \times \lambda_X}(g) = \sum_{g \in G} \chi_{\lambda_X}(g)^2 = \sum_{g \in G}(1 + \chi_{\lambda_X|_W}(g))^2.$$ 

Applying the integer-valued property of $\chi_{\lambda_X|_W}$ and $\dim(\mathbb{C}(X \times X))^G = 2$ gives that $\langle \chi_{\lambda_X|_W}, \chi_{\lambda_X|_W} \rangle = 1$, or equivalently, $\lambda_X|_W$ is irreducible.

In fact, the converse is also true, hence $X$ is 2-transitive is equivalent to $\lambda_X|_W$ is irreducible.

2. **Quasirandomness of $PSL_2(q)$**

Given a finite field $K = \mathbb{F}_q$ of order $q$, recall that the group $PSL_2(q)$ is defined to be

$$PSL_2(q) := SL_2(q)/\{I, -I\}$$

where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The order of related groups are $|GL_2(q)| = q(q - 1)(q^2 - 1)$, $|SL_2(q)| = |PGL_2(q)| = q(q^2 - 1)$ and

$$|PSL_2(q)| = \begin{cases} q(q^2 - 1), & q \text{ is even;} \\ q(q^2 - 1)/2, & q \text{ is odd.} \end{cases}$$

By elementary group theory, it can be shown that $PSL_2(2) \cong S_3$ the symmetric group of order 3, and $PSL_2(3) \cong A_4$ the alternating group of order 4, hence both are not simple. Jordan showed in 1861 that $PSL_2(q)$ are all simple groups for $q \geq 4$.

Consider now $q \geq 5$ and $q$ is odd, then we know that $PSL_2(q)$ is a simple group of order $q(q^2 - 1)/2$. A group $G$ is said to be $k$-quasirandom if its every nontrivial unitary representation has dimension at least $k$. Such quasirandomness are useful as demonstrated in [2] and [3]. Our aim in this section is to show that $PSL_2(q)$ is quasirandom.

**Theorem 3** (Quasirandomness of $PSL_2(q)$). Let $q \geq 5$ and $q$ is odd, then the group $PSL_2(q)$ is $(q - 1)/2$-quasirandom, that is, every nontrivial representation of $PSL_2(q)$ has dimension at least $(q - 1)/2$.

For simplicity, denote $K := \mathbb{F}_q$ to be the field. Consider a subgroup $H \leq PSL_2(q)$ of order $|H| = q(q - 1)/2$ given as follows

$$H = \left\{ A = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} : a \in K^\times, b \in K \right\} / \{I, -I\}.$$

Let $G \leq GL_2(q)$ be the subgroup

$$G = \left\{ A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in K^\times, b \in K \right\}.$$
It’s easy to see that $H$ is isomorphic to a subgroup of $G$ consisting of matrices of the form $\begin{pmatrix} a^2 & ab \\ 0 & 1 \end{pmatrix}$. The isomorphism is given by mapping $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$ to $\begin{pmatrix} a^2 & ab \\ 0 & 1 \end{pmatrix}$, using this isomorphism we view $H \leq G$. Hence alternatively we can view $H$ as

$$H = \left\{ A = \begin{pmatrix} a^2 & ab \\ 0 & 1 \end{pmatrix} : a \in K^\times, b \in K \right\}.$$

To prove theorem 3 we will determine the list of irreducible representations of group $H$, and to achieve this, we first present an irreducible representation of $G$ of high dimension using Lemma 1.5. Observe that $G$ can be viewed as the group of affine transformations on $K$ as follows: given $x \in K$, we have

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} ax + b \\ 1 \end{pmatrix},$$

hence we have the affine transform action of $G$ on $K$ given by

$$A : K \to K, \quad x \mapsto ax + b,$$

where $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$. Therefore $K$ can be viewed as a $G$-space. Let $(\lambda_K, \mathbb{C}K)$ be the permutation representation of $G$. As usual, let

$$W = \{ f \in \mathbb{C}K : \sum_{x \in K} f(x) = 0 \}.$$

be the subspace of $\mathbb{C}K$ of co-dimension one.

**Lemma 2.1.** The representation $(\lambda_K|_W, W)$ is an irreducible representation of $G$.

**Proof.** By Lemma 1.5 it suffices to show $K$ is 2-transitive. As $K$ is a field, view $(x_1, y_1)$ and $(x_2, y_2)$ as two points, then the matrix which maps $(x_1, y_1)$ to $(x_2, y_2)$ is given by the corresponding line equation. \hfill \Box

Using this fact next we determine the irreducible representations of $H \leq G$.

**Lemma 2.2** (List of irreducible representations of $H$). The list of irreducible representations of $H$ is given as follows

- $(q - 1)/2$ distinct representations $\rho_j, j = 1, 2, \ldots, (q - 1)/2$, all of dimension one;
- two distinct representations $\rho^+, \rho^-$, both of dimension $(q - 1)/2$.

**Proof.** First by degree formula in theorem 2 and using the fact that $|H| = q(q - 1)/2$ we see the list is complete.

We first give all the 1-dimensional representations. Let $K^{\times 2} := \{ x^2 : x \in K^\times \} \leq K^\times$ be the subgroup of squares in $K^\times$, we have $|K^{\times 2}| = (q - 1)/2$. Since $K^{\times 2}$ is an abelian group, Corollary 1 says it has exactly $(q - 1)/2$ distinct 1-dimensional irreducible representations, let $\phi_j : K^{\times 2} \to \mathbb{C}^\times, j = 1, 2, \ldots, (q - 1)/2$ be these representations. Observe that there is a natural homomorphism $\varphi : H \to K^{\times 2}$ given by $\varphi(A) = a^2$ for $A = \begin{pmatrix} a^2 & ab \\ 0 & 1 \end{pmatrix} \in H$, then $\rho_j := \phi_j \circ \varphi$ gives the desired 1-dimensional representations.

Second let us give the two irreducible representations of dimension $(q - 1)/2$, which come from irreducible representation $(\lambda_K|_W, W)$ of $G$. Consider the restriction of $\lambda_K|_W$ to the subgroup $H \leq G$, denote it by $\rho$, hence $(\rho, W)$ is a representation of $H$. For $A \in H$, recall that the representation $\rho$ is defined by $(\rho(A)f)(x) = f(A^{-1}x)$ where $f \in W, x \in K$. Since $K$ is abelian, a basis of $\mathbb{C}K$ is given by the $q$ characters $\chi_m : K \to \mathbb{C}^\times, m = 0, 1, \ldots, q - 1$ defined by $\chi_m(x) = a^m$.
where \( \omega = e^{2\pi i/q} \). Clearly \( \{ \chi_1, \chi_2, \ldots, \chi_q \} = \{ \chi_m : m \in K^\times \} \) is a basis for \( W \leq \mathbb{C}^K \). Let us compute the representation \( (\rho, W) \) of \( H \) as follows: since \( A^{-1} = \begin{pmatrix} a^{-2} & -a^{-1}b \\ 0 & 1 \end{pmatrix} \), we have

\[
(\rho(A)\chi_m)(x) = \chi_m(A^{-1}x) = \chi_m(a^{-2}x - a^{-1}b) = \chi_m(-a^{-1}b)\chi_{m/a^2}(x).
\]

If \( m \in K^{x^2} \), then \( m/a^2 \in K^{x^2} \), and vice versa. Hence the two subspaces

\( W^+ = \text{span}\{\chi_m : m \in K^{x^2}\} \), \( W^- = \text{span}\{\chi_m : m \in K^x - K^{x^2}\} \),

are both \( H \)-invariant. It’s then easy to verify (by calculating the inner product of characters) that \( (\rho^+ = \rho|_{W^+}, W^+) \) and \( (\rho^- = \rho|_{W^-}, W^-) \) are both irreducible. Clearly they are of dimension \( (q - 1)/2 \).

Now we are ready to prove theorem 3.

**Proof.** Let \( (\pi, V) \) be an \( n \)-dimensional nontrivial representation of \( \text{PSL}_2(q) \), we will show \( n \geq (q - 1)/2 \). Consider the restriction of \( \pi \) to the subgroup \( H \leq \text{PSL}_2(q) \), denote it by \( \rho \), we get a representation \( (\rho, V) \) of group \( H \). Applying theorem 2 and Lemma 2.2 we have

\[
\rho = m_+ \rho^+ \oplus m_- \rho^- \oplus \sum_{j=1}^{(q-1)/2} m_j \rho_j,
\]

where \( m_+, m_-, m_- \) are the number of representations equivalent to \( \rho_j, \rho^+, \rho^- \), respectively. It then suffices to show \( m_+ + m_- \geq 1 \).

Since \( H \) is non-abelian, its commutator subgroup \( [H, H] \) is nontrivial. Clearly the restriction of \( \rho_j \) on \( [H, H] \) are all trivial because they are all 1-dimensional representations (which are just homomorphisms from \( H \) to \( \mathbb{C}^\times \)). Now as \( q \geq 5 \) we know \( \text{PSL}_2(q) \) is a simple group, hence \( \pi \) is faithful, hence \( \rho(A) \neq I_n \) for all \( I \neq A \in H \). In particular this holds for \( I \neq A \in [H, H] \). As we already seen all the 1-dimensional representations are trivial on \( [H, H] \), hence at least one of \( \rho^+ \) or \( \rho^- \) must appear in the decomposition of \( \rho \), i.e., \( m_+ + m_- \geq 1 \) as desired.

**References**


