MINIMAL PERMUTATION REPRESENTATIONS FOR
GL$_2$(F$_q$)

NEELIMA BORADE AND RAMIN TAKLOO-BIGHASH

Abstract. In this paper we determine all minimal permutation representations of GL$_2$(F$_q$).

1. Introduction

The purpose of this note is to determine the size and the structure of the minimal permutation representations of the group GL$_2$(F$_q$), for an odd prime power q. Theorem 3.7 of [2] claims to have determined at least the size of the minimal permutation representation, but there is a typo in the answer, and it appears to us that the proof presented is not correct. The proof we present here is inspired by the results and techniques of [1, 2].

To state the theorem we need a couple of pieces of notation. Given a natural number n, we can write $n = 2^r \prod_p p^{e_p}$. We set $n_2 = 2^r$ and $T(n) = \sum_p p^{e_p}$. Also given a finite group G we let $p(G)$ be the size of the faithful minimal permutation of G, i.e., the size of the smallest set $A$ on which G has a faithful action. We will be proving the following result:

**Theorem 1.1.** If $q \geq 3$ is an odd prime power, then

$$p(\text{GL}_2(F_q)) = p(\text{SL}_2(F_q)) + T(q-1) = (q+1)(q-1)_2 + T(q-1).$$

In fact we prove a much stronger theorem, Theorem 3.13, where we identify all minimal faithful sets for GL$_2$(F$_q$). The equality $p(\text{SL}_2(F_q)) = (q+1)(q-1)_2$ is Theorem 3.6 of [1]. To prove our theorem we first construct a faithful permutation representation of size $p(\text{SL}_2(F_q)) + T(q-1)$ and then we proceed to find all minimal faithful representations of GL$_2$(F$_q$) by trying to beat this bound. The proof, though elementary, is rather subtle.

The second author is partially supported by a Collaboration Grant from the Simons Foundation. We wish to thank Roman Bezrukavnikov.

Date: May 26, 2020.
and Annette Pilkington who independently simplified our first step of the proof of Lemma 3.7. We used numerical computations carried out using \texttt{sagemath} to convince us of the validity of Lemma 3.9.

2. A FAITHFUL COLLECTION

We start with some definition. The standard reference for minimal permutation representations of finite groups is Johnson’s classical paper [6]. In order to construct a faithful permutation representation of a group $G$ we need to construct a collection of subgroups \{$H_1, \ldots, H_l$\} such that $\text{core}_G(H_1 \cap \cdots \cap H_l) = \{e\}$. Recall that for a subgroup $H$ of $G$, $\text{core}_G(H)$ is the largest normal subgroup of $G$ contained in $H$, i.e.,

$$\text{core}_G(H) = \bigcap_{x \in G} xHx^{-1}.$$  

We call a collection \{$H_1, \ldots, H_l$\} of subgroups of $G$ \textit{faithful} if $\text{core}_G(H_1 \cap \cdots \cap H_l) = \{e\}$. In this case the left action of $G$ on the disjoint union $A = G/H_1 \cup \cdots \cup G/H_l$ is faithful. Note that $|A| = \sum_i |G/H_i|$. A collection \{$H_1, \ldots, H_l$\} is called \textit{minimal faithful} if

1. $\text{core}_G(H_1 \cap \cdots \cap H_l) = \{e\}$,
2. $\sum_i |G/H_i|$ is minimal among all collections of subsets satisfying (1). In this case, $\sum_i |G/H_i|$ is denoted by $p(G)$.

The papers [5,6] and the thesis [4] contain many examples of explicit computations of $p(G)$ for various groups $G$.

In the remainder of this section we construct a faithful collection for $\text{GL}_2(\mathbb{F}_q)$ which we will eventually prove to be minimal. Let $\varpi$ be a generator of the cyclic group $\mathbb{F}_q^\times$. For $t \mid q - 1$, set $A_t = \langle \varpi^t \rangle$. The set $A_t$ is the unique subgroup of $\mathbb{F}_q^\times$ of size $(q - 1)/t$. If $(q - 1)/2 = 2^r$, then $A_{2^r}$ is the largest subgroup of $\mathbb{F}_q^\times$ which has odd order. Note that if $s, t$ are divisors of $q - 1$, then $A_s \cap A_t = A_{\text{lcm}(s,t)}$. Let

$$D_t = \left\{ \begin{pmatrix} a \\ 1 \end{pmatrix} \mid a \in A_t \right\},$$

$$Z_t = \left\{ \begin{pmatrix} a \\ a^t \end{pmatrix} \mid a \in A_t \right\}.$$  

We usually denote $Z_1$ by $Z$. Note that any subgroup of $Z$ is of the form $Z_t$ for some $t \mid q - 1$. In fact, $Z_t$ is the unique subgroup of $Z$ of order $(q - 1)/t$. For $s, t$ divisors of $q - 1$ we have

$$Z_s \cap Z_t = Z_{\text{lcm}(s,t)}.$$  

(2.1)
Let

$$\text{GL}_2(\mathbb{F}_q)^t = \{ g \in \text{GL}_2(\mathbb{F}_q) \mid \det g \in A_t \}.$$ 

Then it is clear that $D_t$, $Z_t$, and $\text{GL}_2(\mathbb{F}_q)^t$ are subgroups of $\text{GL}_2(\mathbb{F}_q)$, and that $\text{GL}_2(\mathbb{F}_q)^t = D_t \cdot \text{SL}_2(\mathbb{F}_q)$. We note that for $t \mid q - 1$,

$$[\text{GL}_2(\mathbb{F}_q) : \text{GL}_2(\mathbb{F}_q)^t] = t. \quad (2.2)$$

The following lemma is a consequence of the Lattice Isomorphism Theorem:

**Lemma 2.1.** If $H$ is a subgroup of $\text{GL}_2(\mathbb{F}_q)$ which contains $\text{SL}_2(\mathbb{F}_q)$, then there is $t \mid q - 1$ such that $H = \text{GL}_2(\mathbb{F}_q)^t$.

The following lemma is important:

**Lemma 2.2.** We have

$$Z \cap \text{GL}_2(\mathbb{F}_q)^t = \begin{cases} Z_{t/2} & \text{if } t \text{ is even;} \\ Z_t & \text{if } t \text{ is odd.} \end{cases}$$

**Proof.** We observe that $Z \cap \text{GL}_2(\mathbb{F}_q)^t$ is a subgroup of $Z$, so it must be of the form $Z_s$ for some $s \mid (q - 1)$. We need to determine the diagonal elements of the form $\begin{pmatrix} z & \vphantom{\frac{1}{2}} \\ \frac{1}{x} & \vphantom{\frac{1}{2}} \end{pmatrix}$ that can be written in the form

$$\begin{pmatrix} \omega^{kt} \\ 1 \end{pmatrix} \begin{pmatrix} a^{-1} \\ a \end{pmatrix} = \begin{pmatrix} \omega^{kt}a^{-1} \\ a \end{pmatrix}$$

for some integer $0 \leq k < (q - 1)/t$ and $a \in \mathbb{F}_q^\times$. This means $\omega^{kt}a^{-1} = a$, i.e., $\omega^{kt} = a^2$. Two cases:

If $t$ is even, then $a = \pm \omega^{k \frac{t}{2}}$, for any $0 \leq k < (q - 1)/t$. This means there are $2(q - 1)/t$ possibilities for $a$, and that means that $Z \cap \text{GL}_2(\mathbb{F}_q)^t = Z_{t/2}$.

If $t$ is odd, then $a = \pm \omega^{k t}$ whenever $0 \leq k < (q - 1)/t$ is even. Since $(q - 1)/t$ is even, there are $(q - 1)/t$ possibilities for $a$, and we have $Z \cap \text{GL}_2(\mathbb{F}_q)^t = Z_t$. □

We also recall the construction of the minimal faithful representation of $\text{SL}_2(\mathbb{F}_q)$ from [1]. Write $q - 1 = 2^r \cdot m$ with $m$ odd. Set

$$H_{\text{odd}} = \left\{ \begin{pmatrix} a & \vphantom{\frac{1}{2}} \\ \frac{1}{x} & \vphantom{\frac{1}{2}} \end{pmatrix} \begin{pmatrix} 1 \\ x \end{pmatrix} \mid a \in A_{2^r}, x \in \mathbb{F}_q \right\}. \quad (2.3)$$
Then Theorem 3.6 of \cite{1} says that $H_{\text{odd}}$ is a corefree subgroup of $\text{SL}_2(\mathbb{F}_q)$ of minimal index, i.e., the action of $\text{SL}_2(\mathbb{F}_q)$ on $\text{SL}_2(\mathbb{F}_q)/H_{\text{odd}}$ is a minimal faithful representation. Also, it is easy to see that 

$$[\text{SL}_2(\mathbb{F}_q) : H_{\text{odd}}] = (q - 1)2(q + 1).$$

Set 

$$GH_{\text{odd}} = D_1 \cdot H_{\text{odd}}.$$ 

Then $GH_{\text{odd}}$ is a subgroup of $\text{GL}_2(\mathbb{F}_q)$, and we have 

$$[\text{GL}_2(\mathbb{F}_q) : GH_{\text{odd}}] = (q - 1)2(q + 1).$$

**Lemma 2.3.** We have 

$$\text{core}_{\text{GL}_2(\mathbb{F}_q)}(GH_{\text{odd}}) = Z_{2^r}.$$ 

**Proof.** Any normal subgroup of $\text{GL}_2(\mathbb{F}_q)$ which does not contain $\text{SL}_2(\mathbb{F}_q)$ is a subgroup of $Z$, so we just need to show $Z \cap GH_{\text{odd}} = Z_{2^r}$. For $a \in A_{2^r}$ we have 

$$\begin{pmatrix} a^2 & 1 \\ 1 & a \end{pmatrix} \cdot \begin{pmatrix} a^{-1} \\ a \end{pmatrix} = \begin{pmatrix} 1 & \ast \\ \ast & 1 \end{pmatrix}.$$ 

□

We can now give a construction of a faithful permutation representation which we will later prove to be minimal.

**Proposition 2.4.** Write $q - 1 = 2^r \cdot p_1^{e_1} \cdots p_k^{e_k}$ with $p_1, \ldots, p_k$ distinct odd primes, and $e_1, \ldots, e_k \geq 1$. Then the collection of subgroups 

$$\{GH_{\text{odd}}, \text{GL}_2(\mathbb{F}_q)^{p_1^{e_1}}, \ldots, \text{GL}_2(\mathbb{F}_q)^{p_k^{e_k}}\}$$

is a faithful collection. The corresponding faithful permutation representation has size $p(\text{SL}_2(\mathbb{F}_q)) + T(q - 1)$.

**Proof.** We need to show that the subgroup $U = GH_{\text{odd}} \cap \text{GL}_2(\mathbb{F}_q)^{p_1^{e_1}} \cap \cdots \cap \text{GL}_2(\mathbb{F}_q)^{p_k^{e_k}}$ is corefree. By Lemma 2.3 $\text{core}_{\text{GL}_2(\mathbb{F}_q)}(GH_{\text{odd}})$ is a subset of $Z$, so the core of $U$ is a subgroup of $Z$. Since any subgroup of $Z$ is normal, we just need to compute the intersection $U \cap Z$. Lemmas 2.2 and 2.3 implies that this intersection is $Z_{2^r} \cap Z_{p_1^{e_1}} \cap \cdots Z_{p_k^{e_k}}$. As $\text{lcm}(2^r, p_1^{e_1}, \ldots, p_k^{e_k}) = q - 1$, Equation (2.1) says

$$Z_{2^r} \cap Z_{p_1^{e_1}} \cap \cdots Z_{p_k^{e_k}} = Z_{q - 1} = \{e\}.$$ 

This means that the collection is faithful. The size of the corresponding permutation representation is equal to 

$$[\text{GL}_2(\mathbb{F}_q) : GH_{\text{odd}}] + [\text{GL}_2(\mathbb{F}_q) : \text{GL}_2(\mathbb{F}_q)^{p_1^{e_1}}] + \cdots + [\text{GL}_2(\mathbb{F}_q) : \text{GL}_2(\mathbb{F}_q)^{p_k^{e_k}}].$$
\[ = (q - 1)_2(q + 1) + p_1^{e_1} + \cdots + p_k^{e_k} \]

after using Equations (2.5) and (2.2). This finishes the proof of the proposition. \hfill \Box

**Corollary 2.5.** We have

\[ p(\text{GL}_2(\mathbb{F}_q)) \leq (q - 1)_2(q + 1) + T(q - 1). \]

**Remark 2.6.** It might have been tempting to use the results of [3], especially Lemma 2.3, to compute \( p(\text{GL}_2(\mathbb{F}_q)) \). Unfortunately, however, this result is wrong. Lemma 2.3 of [3] states that if \( G \ltimes \varphi H \) is a semi-direct product of groups such that \( \varphi \) is injective, and if \( G \) has a minimal faithful collection given by a subgroups that are invariant under the conjugation action of \( H \), then \( p(G \ltimes \varphi H) = p(G) \). The proof of this lemma proceeds by claiming that if \( \{H_1, \ldots, H_l\} \) is a faithful collection of \( G \) consisting of subgroups invariant under the conjugation action of \( H \), then \( \{H_1H, \ldots, H_lH\} \) is a faithful collection of \( G \ltimes \varphi H \). As we saw in Lemma 2.3 this is not true for \( G = \text{SL}_2(\mathbb{F}_q), H = D_1, H_1 = H_{\text{odd}}. \) Also by Theorem 3.13 below, \( p(\text{GL}_2(\mathbb{F}_q)) \neq p(\text{SL}_2(\mathbb{F}_q)) \).

### 3. Minimal faithful collections

We start with a lemma. This lemma should be compared with Lemma 3.1 of [2].

**Lemma 3.1.** Let \( H \) be a subgroup of \( \text{GL}_2(\mathbb{F}_q) \). Then

\[ [H : H \cap \text{SL}_2(\mathbb{F}_q)] = \frac{|H \cdot \text{SL}_2(\mathbb{F}_q)|}{|\text{GL}_2(\mathbb{F}_q)|} \cdot (q - 1). \]

**Proof.** We observe that \( H \cdot \text{SL}_2(\mathbb{F}_q) \) is a subgroup of \( \text{GL}_2(\mathbb{F}_q) \). We have

\[ |H \cdot \text{SL}_2(\mathbb{F}_q)| = \frac{|H| \cdot |\text{SL}_2(\mathbb{F}_q)|}{|H \cap \text{SL}_2(\mathbb{F}_q)|}. \]

Hence,

\[ [H : H \cap \text{SL}_2(\mathbb{F}_q)] = \frac{|H|}{|H \cap \text{SL}_2(\mathbb{F}_q)|} = \frac{|\text{GL}_2(\mathbb{F}_q)|}{|\text{GL}_2(\mathbb{F}_q) : H \cdot \text{SL}_2(\mathbb{F}_q)|} \cdot \frac{1}{|\text{SL}_2(\mathbb{F}_q)|} \cdot \frac{q - 1}{|\text{GL}_2(\mathbb{F}_q) : H \cdot \text{SL}_2(\mathbb{F}_q)|}, \]

as claimed. \hfill \Box

The following lemma is a strengthening of Lemma 3.2 of [2].
Lemma 3.2. Let $H$ be a subgroup of $GL_2(\mathbb{F}_q)$ such that $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \not\in H$. Then

$$[GL_2(\mathbb{F}_q) : H] \geq p(SL_2(\mathbb{F}_q)) \cdot [GL_2(\mathbb{F}_q) : H \cdot SL_2(\mathbb{F}_q)].$$

Proof. Since $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \not\in H$, $H \cap SL_2(\mathbb{F}_q)$ is a corefree subgroup of $SL_2(\mathbb{F}_q)$. Hence

(3.1) $$[SL_2(\mathbb{F}_q) : H \cap SL_2(\mathbb{F}_q)] \geq p(SL_2(\mathbb{F}_q)).$$

Next,

$$[GL_2(\mathbb{F}_q) : H] = \frac{[GL_2(\mathbb{F}_q) : H \cap SL_2(\mathbb{F}_q)]}{[H : H \cap SL_2(\mathbb{F}_q)]}.$$

By Lemma 3.1 this expression is equal to

$$= \frac{[GL_2(\mathbb{F}_q) : H \cap SL_2(\mathbb{F}_q)]}{q - 1} \cdot [GL_2(\mathbb{F}_q) : H \cdot SL_2(\mathbb{F}_q)]$$

$$= [SL_2(\mathbb{F}_q) : H \cap SL_2(\mathbb{F}_q)] \cdot [GL_2(\mathbb{F}_q) : H \cdot SL_2(\mathbb{F}_q)]$$

$$\geq p(SL_2(\mathbb{F}_q)) \cdot [GL_2(\mathbb{F}_q) : H \cdot SL_2(\mathbb{F}_q)],$$

by Equation (3.1). \qed

We also state the following elementary fact as lemma for ease of reference:

Lemma 3.3. For natural numbers $a_1, \ldots, a_k \geq 2$, at least one of which is strictly larger than 2, we have

$$\sum_i a_i < \prod_i a_i.$$

Proof. Proof is by induction, without loss of generality assume $a_1 \geq 3$. We have

$$(a_1 - 1) \cdot (a_2 - 1) \geq 2.$$ Simplifying gives $a_1 a_2 \geq a_1 + a_2 + 1$. The rest is clear. \qed

Corollary 3.4. We have

$$T(q - 1) < p(SL_2(\mathbb{F}_q)).$$

Proof. Write $q - 1 = 2^r p_1^{e_1} \cdots p_k^{e_k}$ with $p_i$’s distinct odd primes and $e_i \geq 1$. By Lemma 3.3

$$T(q - 1) \leq \frac{q - 1}{(q - 1)^2} < q - 1 < q + 1 < (q - 1)2(q + 1).$$ \qed
Now let \( C = \{ H_1, \ldots, H_\ell \} \) be a minimal faithful collection of \( \text{GL}_2(\mathbb{F}_q) \).

Since \( \begin{pmatrix} -1 & -1 \\ 1 & 1 \end{pmatrix} \) is in the center of \( \text{GL}_2(\mathbb{F}_q) \), there is an \( i \) such that \( \begin{pmatrix} -1 & -1 \\ 1 & 1 \end{pmatrix} \notin H_i \).

**Lemma 3.5.** There is exactly one \( i \) as above and \( H_i \cdot \text{SL}_2(\mathbb{F}_q) = \text{GL}_2(\mathbb{F}_q) \).

**Proof.** Suppose \( H_i, H_j \) do not contain \( \begin{pmatrix} -1 & -1 \\ 1 & 1 \end{pmatrix} \). Then by Lemma 3.2 \( [\text{GL}_2(\mathbb{F}_q) : H_i] + [\text{GL}_2(\mathbb{F}_q) : H_j] \) is larger than or equal to \( \geq ([\text{GL}_2(\mathbb{F}_q) : H_i \cdot \text{SL}_2(\mathbb{F}_q)] + [\text{GL}_2(\mathbb{F}_q) : H_j \cdot \text{SL}_2(\mathbb{F}_q)]) \cdot \text{p}(\text{SL}_2(\mathbb{F}_q)) \) which is at least \( 2\text{p}(\text{SL}_2(\mathbb{F}_q)) \). By Corollary 3.3 we have \( 2\text{p}(\text{SL}_2(\mathbb{F}_q)) > \text{p}(\text{SL}_2(\mathbb{F}_q)) + T(q - 1) \), and this latter quantity, by Corollary 2.5, is larger than or equal to \( \text{p}(\text{GL}_2(\mathbb{F}_q)) \). Consequently, if \( H_i \neq H_j \) or if \( H_i \cdot \text{SL}_2(\mathbb{F}_q) \neq \text{GL}_2(\mathbb{F}_q) \),

\[ [\text{GL}_2(\mathbb{F}_q) : H_i] + [\text{GL}_2(\mathbb{F}_q) : H_j] > \text{p}(\text{GL}_2(\mathbb{F}_q)) \]

This contradicts the assumption that \( C \) is a minimal faithful collection. \( \square \)

Without loss of generality let \( i = 1 \).

**Lemma 3.6.** The \( H_1 \cap \text{SL}_2(\mathbb{F}_q) \) is a conjugate of \( H_{\text{odd}} \) in \( \text{SL}_2(\mathbb{F}_q) \), with \( H_{\text{odd}} \) defined by Equation (2.3).

**Proof.** Since \( \begin{pmatrix} -1 & -1 \\ 1 & 1 \end{pmatrix} \notin H_1 \), \( H_1 \cap \text{SL}_2(\mathbb{F}_q) \) will have odd order. By Lemma 3.5 of [1], up to conjugation, we have the following possibilities for \( H_1 \cap \text{SL}_2(\mathbb{F}_q) \):

(A) a cyclic subgroup of odd order dividing \( q \pm 1 \);

(B) a subgroup of odd order of the upper triangular matrices

\[ T(2, q) = \left\{ \begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{F}_q^\times, x \in \mathbb{F}_q \right\} \].

In case (A), since \( |H_1 \cap \text{SL}_2(\mathbb{F}_q)| = (q \pm 1)/t \) is odd, and \( q \pm 1 \) are even numbers, we must have \( t \geq 2 \). By the proof of Lemma 3.2 and the statement of Lemma 3.5

\[ [\text{GL}_2(\mathbb{F}_q) : H_1] = [\text{SL}_2(\mathbb{F}_q) : H_1 \cap \text{SL}_2(\mathbb{F}_q)] \cdot [\text{GL}_2(\mathbb{F}_q) : H_1 \cdot \text{SL}_2(\mathbb{F}_q)] \]

\[ = [\text{SL}_2(\mathbb{F}_q) : H_1 \cap \text{SL}_2(\mathbb{F}_q)] = \frac{|\text{SL}_2(\mathbb{F}_q)|}{|H_1 \cap \text{SL}_2(\mathbb{F}_q)|} \]
\[ \frac{q(q + 1)(q - 1)}{q + 1} \cdot t \geq 2 \frac{q(q + 1)(q - 1)}{q + 1}. \]

We determine the cases where \( \frac{q(q+1)(q-1)}{q+1} \geq (q - 1) \cdot (q + 1). \) We need \( \frac{q(q-1)}{q+1} \geq (q - 1) \). We have two cases:

- If the denominator is \( q - 1 \), then we need \( q \geq (q - 1) \), which is obviously true.

- If the denominator is \( q + 1 \), then we want \( q(q - 1) \geq (q + 1)(q - 1) \). For this write \( q - 1 = 2^r m \) with \( m \) odd, then we need \( (2^r m + 1)2^r m \geq 2^r m + 2^r \), or what is the same, \( (2^r m + 1)m \geq 2^r m + 2 \). If \( m \geq 3 \), then this last inequality is definitely satisfied, but if \( m = 1 \), it is not true.

This discussion means that unless \( q = 2^r + 1 \), \( [\text{GL}_2(\mathbb{F}_q) : H_1] \geq 2p(\text{SL}_2(\mathbb{F}_q)) \) which by Corollary 3.4 is strictly bigger than \( p(\text{SL}_2(\mathbb{F}_q)) + T(q - 1) \). This last statement, by Corollary 2.5, contradicts the minimality of \( C \).

Now we examine the case where \( q = 2^r + 1 \). Note that in this case \( T(q - 1) = 0 \) as \( q - 1 \) has no odd prime factors. One easily checks that

\[ \frac{2q(q + 1)(q - 1)}{q + 1} > (q - 1)(q + 1). \]

This means that \( [\text{GL}_2(\mathbb{F}_q) : H_1] > p(\text{SL}_2(\mathbb{F}_q)) + T(q - 1) \) which again, by Corollary 2.5, contradicts the minimality of \( C \).

Now we examine case (B). In this case, if we write \( q - 1 = 2^r m \), there is a divisor \( m_0 \) of \( m \) such that

\[ H_1 \cap \text{SL}_2(\mathbb{F}_q) = \left\{ \begin{pmatrix} a & x \\ a^{-1} & 1 \end{pmatrix} \mid a \in A_{2^r m_0}, x \in \mathbb{F}_q \right\}. \]

(Note that this is up to conjugation only, but with a change of basis, we may assume it to be true.) Then

\[ [\text{SL}_2(\mathbb{F}_q) : H_1 \cap \text{SL}_2(\mathbb{F}_q)] = [\text{SL}_2(\mathbb{F}_q) : H_{odd}] \cdot [H_{odd} : H_1 \cap \text{SL}_2(\mathbb{F}_q)] = m_0 \cdot p(\text{SL}_2(\mathbb{F}_q)). \]

By the proof of Lemma 3.2 we have

\[ [\text{GL}_2(\mathbb{F}_q) : H_1] = [\text{SL}_2(\mathbb{F}_q) : H_1 \cap \text{SL}_2(\mathbb{F}_q)] \cdot [\text{GL}_2(\mathbb{F}_q) : H_1 \cdot \text{SL}_2(\mathbb{F}_q)] = m_0 \cdot p(\text{SL}_2(\mathbb{F}_q)), \]

upon using Lemma 3.3. Again as before if \( m_0 > 1 \), we conclude \( [\text{GL}_2(\mathbb{F}_q) : H_1] \geq 2 \), and we get a contradiction. \( \square \)
Without loss of generality we may assume \( H_1 \cap \text{SL}_2(\mathbb{F}_q) = H_{\text{odd}} \).

For \( n, 0 \leq n < q - 1 \), define a subgroup \( D(n) \subset \text{GL}_2(\mathbb{F}_q) \) by
\[
D(n) = \left\{ \begin{pmatrix} a^{n+1} & a^{-n} \\ a^{-n} & 1 \end{pmatrix} \mid a \in \mathbb{F}_q^\times \right\}.
\]

Set
\[
G \! H(n) = D(n) \cdot H_{\text{odd}}.
\]
The subgroup \( G \! H(0) \) is what we had called \( G \! H_{\text{odd}} \) in Equation (2.4).

**Lemma 3.7.** There is an \( n, 0 \leq n < q - 1 \), such that \( H_1 = G \! H(n) \).

**Proof.** The proof of this lemma is in two steps. In the first step we show that \( H_1 \) is a subgroup of upper triangular matrices in \( \text{GL}_2(\mathbb{F}_q) \), and then we identify it explicitly. The simple argument we give for the first step was suggested independently by Roman Bezrukavnikov and Annette Pilkington. We start with the observation that \( H_1 \cap \text{SL}_2(\mathbb{F}_q) \) is normal in \( H_1 \). By Lemma 3.6, \( H_1 \cap \text{SL}_2(\mathbb{F}_q) \) consists of upper triangular matrices and contains all upper triangular unipotent matrices. Suppose \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H_1 \), and let \( \begin{pmatrix} 1 & x \\ 1 & 1 \end{pmatrix} \) be an arbitrary upper triangular unipotent matrix. Then since the matrix
\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & x \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} * & * \\ \frac{c^2x}{ad-bc} & * \end{pmatrix}
\]
for all \( x \), we must have \( c = 0 \).

Now we proceed to identify \( H_1 \) explicitly. By the proof of Lemma 3.2 and the statements of Lemmas 3.5 and 3.6 we have
\[
[\text{GL}_2(\mathbb{F}_q) : H_1] = [\text{SL}_2(\mathbb{F}_q) : H_{\text{odd}}].
\]
This means \( |H_1| = (q - 1) \cdot |H_{\text{odd}}| \). So we need to find \( (q - 1) \) representatives for the quotient \( H_1/H_{\text{odd}} \). By Lemma 3.5, the determinant \( \det : H_1 \to \mathbb{F}_q^\times \) is surjective. In particular, if \( \varpi \) is a generator of \( \mathbb{F}_q^\times \), there is a matrix \( X \) in \( H_1 \), upper triangular by the first part, such that \( \det X = \varpi \). Since by Lemma 3.6, \( H_1 \) contains all upper triangular unipotent matrices, we may assume that \( X \) is diagonal. Since \( \varpi \) is a generator of \( \mathbb{F}_q^\times \), we may write \( X = \begin{pmatrix} \varpi^{n+1} & \varpi^m \\ \varpi^m & \varpi^n \end{pmatrix} \). Since \( \varpi = \det X = \varpi^{n+m+1} \), we conclude \( n+m \equiv 0 \mod (q-1) \), or \( m \equiv -n \).
So if we let \( X_n = \begin{pmatrix} \varpi^{n+1} & \varpi^{-n} \\ \varpi^{-n} & \varpi^{-1} \end{pmatrix} \), then \( X_n \in H_1 \) and \( \det X_n = \varpi \). The elements \( \{ X_n^i \mid 0 \leq i < q - 1 \} \) provide the \( (q - 1) \) representatives for \( H_1/H_{\text{odd}} \) that we need. \( \square \)
Corollary 3.8 (From the proof). We have
\[ [\text{GL}_2(\mathbb{F}_q) : H_1] = p(\text{SL}_2(\mathbb{F}_q)). \]

Proof. This is Equation 3.2. \(\square\)

Lemma 3.9. We have
\[ \text{core}_{\text{GL}_2(\mathbb{F}_q)}(H_1) = Z_{2^r}. \]

Proof. By Lemma 3.7 it suffices to prove \(\text{core}_{\text{GL}_2(\mathbb{F}_q)}(GH(n)) = Z_{2^r}\) for each \(n\), and that means we need to determine \(Z \cap GH(n)\). Suppose we have an element of the form
\[ t = \left( \begin{array}{c} a^{n+1} \\ a^{-n} \end{array} \right) \cdot \left( \begin{array}{c} b^{-1} \\ b \end{array} \right), \quad a \in \mathbb{F}_q^\times, b \in A_{2^r} \]
and suppose \(t \in Z\). This means \(a^{2n+1} = b^2\). Write \(a = \varpi^i, b = \varpi^{2r \cdot j}\). Then we have
\[ (2n + 1)i \equiv 2^{r+1}j \mod (q - 1). \]
Let \(g = \gcd(2n + 1, q - 1)\). Then \(j = gu\) for some \(u\). Then if \(k\) is a multiplicative inverse of \((2n + 1)/g\) modulo \((q - 1)/g\), we have
\[ i \equiv k \cdot 2^{r+1} \cdot u \mod \frac{q - 1}{g}, \]
or
\[ i = k \cdot 2^{r+1} \cdot u + \frac{q - 1}{g}s \]
for some \(s\). So if for any \(u, s\) we set \(a = \varpi^i, b = \varpi^{2r \cdot j}\) with \(i, j\) satisfying
\[ \begin{cases} i = k \cdot 2^{r+1} \cdot u + \frac{q - 1}{g}s \\ j = u \end{cases}, \]
then \(a^{2n+1} = b^2\). Now we examine the matrix \(t\). We see that \(a^{-n} \cdot b\) is equal to \(\varpi\) raised to the power
\[ -n(k \cdot 2^{r+1} \cdot u + \frac{q - 1}{g}s) + u \cdot g \cdot 2^r \]
\[ = (-2nk + g)2^r \cdot u - n \cdot \frac{q - 1}{g} \cdot s \]
\[ = 2^r \cdot \left\{ (-2nk + g) \cdot u - n \cdot \frac{q - 1}{2^r \cdot g} \cdot s \right\}. \]
We will show that
\[ \gcd(2nk - g, n \cdot \frac{q - 1}{g}) = 1. \]
Let us first look at $\gcd(2nk - g, n)$. This is equal to $\gcd(g, n)$ which is equal to 1, as $g \mid 2n + 1$ and $\gcd(n, 2n + 1) = 1$. This means

$$\gcd(2nk - g, n \cdot \frac{q - 1}{g}) = \gcd(2nk - g, \frac{q - 1}{g})$$

$$= \gcd((2n + 1)k - k, \frac{q - 1}{g})$$

$$= \gcd(g \left\{ \frac{2n + 1}{g} \cdot k - 1 \right\} - k, \frac{q - 1}{g})$$

$$= \gcd(-k, \frac{q - 1}{g})$$

$$= 1.$$  

In the above computation we have used the fact that $k$ is multiplicative inverse of $(2n + 1)/g$ modulo $(q - 1)/g$, so $k \cdot (2n + 1)/g - 1$ is divisible by $(q - 1)/g$. Now that we have established Equation (3.3) we observe that since $-2nk + g$ is odd we have

$$\gcd(-2nk + g, -n \cdot \frac{q - 1}{2r \cdot g}) = 1.$$ 

This means that there are integers $s, u$ such that the corresponding $a, b$ satisfy $a^{-n}b = a^{n+1}b^{-1} = \varpi^{2r}$, and that whenever $a^{-n}b = a^{n+1}b^{-1}$ for $a \in \mathbb{F}_q^\times, b \in A_{2r}$, then the common value is of the form $\varpi^{f \cdot 2r}$ for some integer $f$. This finishes the proof of the lemma. □

Now that we have identified the possibilities for $H_1$ and its core, we optimize the choices of $H_2, \ldots, H\ell$. Define natural numbers $t_2, \ldots, t\ell$ by setting

$$Z \cap H_i = Z_{t_i}, \quad 2 \leq i \leq \ell.$$ 

We can pick each $t_i$ to be a divisor of $q - 1$. By Equation (2.1) and Lemma 3.9, the statement

$$\text{core}_{\text{GL}_2(\mathbb{F}_q)}(H_1 \cap \cdots \cap H\ell) = \{e\}$$

is equivalent to

$$\text{lcm}(2^r, t_2, \ldots, t\ell) = q - 1.$$ 

Our goal is to minimize

$$[\text{GL}_2(\mathbb{F}_q) : H_2] + \cdots + [\text{GL}_2(\mathbb{F}_q) : H\ell].$$

We need a lemma.
Lemma 3.10. Suppose $t | q - 1$, and $t \neq q - 1$. Let $H(t)$ be the subgroup of $\text{GL}_2(\mathbb{F}_q)$ with minimal $[\text{GL}_2(\mathbb{F}_q) : H]$ among the subgroups that satisfy $Z \cap H = Z_t$. Then

$$H(t) = \begin{cases} \text{GL}_2(\mathbb{F}_q)^t & t \text{ odd}; \\ \text{GL}_2(\mathbb{F}_q)^{2t} & t \text{ even}. \end{cases}$$

Furthermore,

$$[\text{GL}_2(\mathbb{F}_q) : H(t)] = \begin{cases} t & t \text{ odd}; \\ 2t & t \text{ even}. \end{cases}$$

Proof. By Lemma 2.2 there is a subgroup $H$ containing $\text{SL}_2(\mathbb{F}_q)$ which satisfies the conditions of the lemma. If $t$ is odd, there are the two subgroups $\text{GL}_2(\mathbb{F}_q)^t$ and $\text{GL}_2(\mathbb{F}_q)^{2t}$ that have the same intersection $Z_t$ with $Z$. Of these two, $\text{GL}_2(\mathbb{F}_q)^t$ has smaller index. If $t$ is even, the only subgroup that has intersection $Z_t$ with $Z$ is $\text{GL}_2(\mathbb{F}_q)^{2t}$. The last assertion follows from Equation (2.2).

To finish the proof of Theorem 1.1 we have to solve the following optimization problem for $n = q - 1$.

Problem 3.11. Suppose a natural number $n = 2^r m$ with $m$ odd is given. For a natural number $t$, set $\epsilon(t) = (3 + (-1)^t)/2$. Find natural numbers $t_2, \ldots, t_\ell$ such that

- $\text{lcm}(2^r, t_2, \ldots, t_\ell) = n$;
- $\sum_{i=2}^\ell \epsilon(t_i)t_i$ is minimal.

We call $(t_2, \ldots, t_\ell)$ the optimal choice for $n$.

Lemma 3.12. Write $n = 2^r p_1^{e_1} \cdots p_k^{e_k}$ with $p_i$’s distinct odd primes. Then the optimal choice for $n$ is $(p_1^{e_1}, \ldots, p_k^{e_k})$.

Proof. Suppose $(t_2, \ldots, t_\ell)$ is an optimal choice for $n$. If some $t_i$ is even, say equal to $2s$, replacing $t_i$ by $s$ does not change the lcm in the statement Problem 3.11 but decreases the value of $\sum \epsilon(t_i)t_i$. Since $(t_2, \ldots, t_\ell)$ is optimal for $n$, this means that all of the $t_i$’s have to be odd. Next, write each $t_i$ as the product of prime powers $\pi_1^{m_1} \cdots \pi_v^{m_v}$. By Lemma 3.3, $\sum \frac{m_j}{\pi_j^v} \leq t_i$ with equality only when $v = 1$. Again, since $(t_2, \ldots, t_\ell)$ is optimal, this means each $t_i$ is a prime power. It is also clear that if $i \neq j$, then $(t_i, t_j) = 1$, because otherwise $t_i, t_j$ will be powers of the same prime, and we can throw away the one with smaller exponent.

Putting everything together we have proved the following theorem:
Theorem 3.13. We have
\[ p(\text{GL}_2(\mathbb{F}_q)) = p(\text{SL}_2(\mathbb{F}_q)) + T(q - 1). \]
Up to conjugacy we have \( q - 1 \) classes of minimal faithful sets for \( \text{GL}_2(\mathbb{F}_q) \) and the representatives \( C_n, 0 \leq n \leq q - 2 \), are described as follows: For \( 0 \leq n \leq q - 2 \) set
\[ C_n = \{ GH(n), \text{GL}_2(\mathbb{F}_q)^{p_1^{e_1}}, \ldots, \text{GL}_2(\mathbb{F}_q)^{p_k^{e_k}} \}. \]

REFERENCES

[1] H. Behravesh, Quasi-permutation representations of \( \text{SL}(2,q) \) and \( \text{PSL}(2,q) \), Glasgow Mathematical Journal, October 1999.
[2] M. R. Darafsheh, M. Ghorbany, A. Daneshkhah, and H. Behravesh, Quasi-permutation representations of the group \( \text{GL}_2(q) \), Journal of Algebra 243, 142–167, 2001.
[3] D. Easdown, and M. Hendriksen, Minimal permutation representations of semidirect products of groups. J. Group Theory 19 (2016), no. 6, 1017–1048.
[4] B. Elias, Minimally faithful group actions and \( p \)-groups, 2005, Princeton University Senior Thesis.
[5] B. Elias, L. Silberman, and R. Takloo-Bighash, Minimal permutation representations of nilpotent groups. Experiment. Math. 19 (2010), no. 1, 121–128.
[6] D. L. Johnson, Minimal permutation representations of finite groups, Amer. J. Math. 93(1971), 857–866.

DEPARTMENT OF MATHEMATICS, STATISTICS, AND COMPUTER SCIENCE, UNIVERSITY OF ILLINOIS AT CHICAGO, 851 S. MORGAN STR, CHICAGO, IL 60607, USA

E-mail address: nborad2@uic.edu
E-mail address: rtakloo@math.uic.edu