Mohammad Reza Darafsheh; Yaghoub Farjami; M. Khademi; Ali Reza Moghaddamfar
Some results on the recognizability of the linear groups over the binary field

Commentationes Mathematicae Universitatis Carolinae, Vol. 46 (2005), No. 4, 589--600

Persistent URL: http://dml.cz/dmlcz/119552

Terms of use:
© Charles University in Prague, Faculty of Mathematics and Physics, 2005

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these Terms of use.
Some results on the recognizability of the linear groups over the binary field

M.R. Darafsheh, Y. Farjami, M. Khademi, A.R. Moghaddamfar

Abstract. In this paper, we first find the set of orders of all elements in some special linear groups over the binary field. Then, we will prove the characterizability of the special linear group $\text{PSL}(13, 2)$ using only the set of its element orders.

Keywords: element order, prime graph, projective special linear group

Classification: 20D05

1. Introduction

Let $G$ be a finite group and $\pi_e(G)$ be the set of orders of all elements in $G$. Clearly, $\pi_e(G)$ is a subset of the set of natural numbers, also $\pi_e(G)$ is closed and partially ordered by the divisibility relation. Hence, $\pi_e(G)$ is uniquely determined by $\mu(G)$, the set of elements that are maximal under the divisibility relation. If $\Omega$ is a subset of natural numbers, then $h(\Omega)$ denotes the number of non-isomorphic finite groups $G$ such that $\pi_e(G) = \Omega$. It is clear that $h(\pi_e(G)) \geq 1$, for any group $G$. Following W.J. Shi, we say that a finite group $G$ is non-distinguishable if $h(\pi_e(G)) = \infty$; and distinguishable if $h(\pi_e(G)) < \infty$. Moreover, a distinguishable group $G$ is called $k$-distinguishable if $h(\pi_e(G)) = k$ $(k < \infty)$. Usually, a 1-distinguishable group $G$ is called a recognizable (or characterizable) group.

To every finite group $G$ we associate a graph known as its prime graph denoted by $\Gamma(G) = (V(G), E(G))$. For this graph we have $V(G) = \pi_e(G)$, the set of all prime divisors of the order of $G$, and for two vertices $p, q \in V(G)$ we have $\{p, q\} \in E(G)$ if and only if $pq \in \pi_e(G)$. Denote the connected components of $\Gamma(G)$ by $\pi_i(G) = \pi_i$, $i = 1, 2, \ldots, t(G)$, where $t(G)$ is the number of connected components. If $2 \in \pi_i(G)$ we set $2 \in \pi_1$.

By [8] we have

$$t(\text{PSL}(n, 2)) = \begin{cases} 1 & \text{if } n \neq p, p + 1; \\ 2 & \text{if } n = p \text{ or } p + 1, \end{cases}$$

where $p$ is an odd prime number. When $n = p$ or $p + 1$, PSL($n, 2$) has two components, one of them is

$$\pi_1 = \pi(2 \prod_{i=1}^{p-1} (2^i - 1)), \quad (\text{resp. } \pi_1 = \pi(2(2^{p+1} - 1) \prod_{i=1}^{p-1} (2^i - 1)))$$
and the other in any case is

\[ \pi_2 = \pi(2^p - 1). \]

Characterization of finite groups through their element orders is one of the most interesting problems in finite group theory. This problem was first introduced by W.J. Shi in [15]. There are some results in the literature showing that certain groups are characterizable (see references and Table 1 in [12]). In particular, it was proved that the following simple groups are characterizable: PSL\( (n, 2) \) for \( n = 3, 4, 5, 6, 7, 8 \) (see [17], [13], [3], [16], [4], [5]). About simple groups PSL\( (9, 2) \) and PSL\( (10, 2) \), the problem is still open. In fact, since the prime graphs of these groups are connected, the problem is more difficult. Moreover, in [3], Darafsheh and Moghaddamfar put forward the following conjecture:

**Conjecture.** For all positive integers \( n \geq 3 \), the simple groups PSL\( (n, 2) \) are characterizable.

In this paper, we will prove that the conjecture is correct for the special linear group PSL\( (13, 2) \). Finally we will prove that:

**Main Theorem.** Let \( G \) be a finite group. Then \( G \cong \text{PSL}(13, 2) \) if and only if \( \pi_e(G) = \pi_e(\text{PSL}(13, 2)) \).

In the following, groups considered are finite and simple groups are non-abelian. We also use the notation PSL\( (n, q) \) or \( L_n(q) \) for the projective special linear group. It is clear that PSL\( (n, 2) = \text{GL}(n, 2) \).

2. On set of orders of elements in PSL\( (n, 2) \)

In this section, we first introduce some notation which are taken from [7]. Then we continue to find some properties of the set \( \pi_e(\text{PSL}(n, 2)) \), whose proof is based on examining the structure of PSL\( (n, 2) \) and on several arithmetic arguments. Finally, we calculate the set of orders of elements of the projective special linear groups PSL\( (n, 2) \) where \( n = 9, 10, 11, 12, 13 \).

**Notation.** Let \( f(x) = x^m - a_{m-1}x^{m-1} - \ldots - a_0 \) be a polynomial over GF\( (q) \) of degree \( m \). Using Green’s notation ([7]), let

\[
U(f) = U_1(f) := \begin{bmatrix}
0 & 1 & 0 & 0 & \ldots & 0 \\
0 & 0 & 1 & 0 & \ldots & 0 \\
0 & 0 & 0 & 1 & \ldots & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & \ldots & 1 \\
a_0 & a_1 & a_2 & a_3 & \ldots & a_{m-1}
\end{bmatrix}
\]
Some results on the recognizability of the linear groups over the binary field

Denote its companion matrix. We also set

$$U_l(f) := \begin{bmatrix} U(f) & 1_m & 0 & 0 & \ldots & 0 \\ 0 & U(f) & 1_m & 0 & \ldots & 0 \\ 0 & 0 & U(f) & 1_m & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & U(f) \end{bmatrix},$$

with \(l\) diagonal blocks \(U(f)\), where \(1_m\) is the identity matrix.

If \(\lambda = \{l_1, l_2, \ldots, l_p\}\) is a partition of a positive integer \(k\) whose \(p\) parts are written in descending order i.e.

$$l_1 \geq l_2 \geq \ldots \geq l_p > 0,$$

then we set

$$U_\lambda(f) := \text{diag}\{U_{l_1}(f), U_{l_2}(f), \ldots, U_{l_p}(f)\}.$$

We denote by \(c(n, q)\) the number of conjugacy classes of \(\text{GL}(n, q)\). In general, there is a generating function for \(c(n, q)\) as follows:

$$\sum_{n=0}^{\infty} c(n, q)x^n = \prod_{m=1}^{\infty} p(x^m)^{w(m, q)},$$

where

$$w(m, q) = \frac{1}{m} \sum_{k|m} \mu(k)q^{m/k}$$

is the number of irreducible polynomials \(f(x)\) of degree \(m\) over \(\text{GF}(q)\). We recall that in equations (1) and (2)

$$p(x) = \frac{1}{(1-x)(1-x^2)\ldots} = \sum_{d=0}^{\infty} p_d x^d$$

is the partition function (in this power series the coefficient \(p_d\) is the number of partitions of \(d\)), and \(\mu\) is the Möbius function.

By definition the order of \(f(x) \in \text{GF}(q)[x]\), \(f(0) \neq 0\), is the smallest natural number \(e\) such that \(f(x)|x^e - 1\), denoted by \(\text{ord}(f)\). If \(A\) is an element of \(\text{GL}(n, q)\) with minimal polynomial \(f(x)\), then it is known that the order of \(A\) in \(\text{GL}(n, q)\) is equal to the order of \(f(x)\). Therefore finding the orders of polynomials over
where $f$ is conjugate to one of the matrices of the form $A$ in $\text{GL}(n, \text{GF}(t))$ respectively. In this case, we denote the conjugacy class $c$ by the symbol $c = (f_{\nu_1}^{m_{\nu_1}} f_{\nu_2}^{m_{\nu_2}} \cdots f_{\nu_s}^{m_{\nu_s}})$. Furthermore, if $B$ is conjugate to $\text{diag}\{U_{k_1}(f_{m_1}), U_{k_2}(f_{m_2}), \ldots, U_{k_s}(f_{m_s})\}$, then we have

$$o(B) = \text{l.c.m.} \{o(U_{k_1}(f_{m_1})), o(U_{k_2}(f_{m_2})), \ldots, o(U_{k_s}(f_{m_s}))\}. \quad (4)$$

Hence, among all elements of $\text{GL}(n, \text{GF}(2))$ having the same characteristic polynomial $f_{m_1}^{k_1} f_{m_2}^{k_2} \cdots f_{m_s}^{k_s}$, $o(B)$ is maximal.

If $w(d, 2) = k$, then it means that there are $k$ irreducible polynomials of degree $d$ over $\text{GF}(2)$, say, $g_1, g_2, \ldots, g_k$. Certainly $o(U_1(g_i)) = \text{ord}(g_i)$ divides $2^d - 1$, and also there exist $g_j$, $1 \leq j \leq k$, such that $o(U_1(g_j)) = \text{ord}(g_j) = 2^d - 1$.

We are now ready for the first result.

**Lemma 1.** Let $n = k_1 m_1 + k_2 m_2 + \cdots + k_s m_s$, where $k_1, k_2, \ldots, k_s, m_1, m_2, \ldots, m_s$ are positive integers and $n \geq 3$. Let $e = \text{l.c.m.} (2^{m_1} - 1, 2^{m_2} - 1, \ldots, 2^{m_s} - 1)$ and $t$ be the smallest integer with $2^t \geq \max(k_1, k_2, \ldots, k_s)$. Then $2^t e \in \pi_e(\text{PSL}(n, 2))$.

**Proof:** Let $A \in \text{PSL}(n, 2) \cong \text{GL}(n, 2)$ have characteristic polynomial $f = f_{m_1}^{k_1} f_{m_2}^{k_2} \cdots f_{m_s}^{k_s}$, where $f_{m_i}$ is an irreducible polynomial over $\text{GF}(2)$ of degree $m_i$ and $o(U_1(f_{m_i})) = \text{ord}(f_{m_i}) = 2^{m_i} - 1$. Now, if $A$ is conjugate to $\text{diag}\{U_{k_1}(f_{m_1}), U_{k_2}(f_{m_2}), \ldots, U_{k_s}(f_{m_s})\}$, then by (4) and Theorem 3.8 in [10], we obtain that

$$o(A) = \text{l.c.m.} \{o(U_{k_1}(f_{m_1})), o(U_{k_2}(f_{m_2})), \ldots, o(U_{k_s}(f_{m_s}))\}$$

$$= \text{l.c.m.} \{2^{t_1} \text{ord}(f_{m_1}), 2^{t_2} \text{ord}(f_{m_2}), \ldots, 2^{t_s} \text{ord}(f_{m_s})\}$$

$$= 2^t \times \text{l.c.m.} \{\text{ord}(f_{m_1}), \text{ord}(f_{m_2}), \ldots, \text{ord}(f_{m_s})\}$$

$$= 2^t \times \text{l.c.m.} \{2^{m_1} - 1, 2^{m_2} - 1, \ldots, 2^{m_s} - 1\},$$

where $t_i$ is the smallest integer with $2^{t_i} \geq k_i$, and $t = \max(t_1, t_2, \ldots, t_s)$. \qed
Corollary 1. The following statements hold.

(a) For $i \geq 1$ we have $\pi_e(\text{PSL}(i, 2)) \subseteq \pi_e(\text{PSL}(i + 1, 2))$. In particular, for every $1 \leq i \leq n$, $2^i - 1$ belong to $\pi_e(\text{PSL}(n, 2))$.

(b) $(q^n - 1)/d(q - 1)$ and $(q^{n-1} - 1)/d$ belong to $\mu(L_n(q))$, where $d = (n, q - 1)$. In particular, $2^{n-1} - 1$ and $2^n - 1$ belong to $\mu(L_n(2))$.

(c) $2^s \in \mu(\text{PSL}(n, 2))$, where $s$ is the smallest integer with $2^s \geq n$.

(d) $2^n - 1$ is the maximal number in $\mu(\text{PSL}(n, 2))$.

(e) $k(2^{n-2} - 1) \in \pi_e(\text{PSL}(n, 2))$ if and only if $k = 1, 2$ or 3. Moreover $2(2^{n-2} - 1)$ is the maximal even number in $\mu(\text{PSL}(n, 2))$.

(f) Assume that

\[
A \in \text{PSL}(n, 2) \quad \text{and} \quad \text{for every} \quad i, j = 1, 2, \ldots, s, \quad (m_i, m_j) = 1.
\]

Then $\prod_{i=1}^{s} (2m_i - 1) \in \mu(\text{PSL}(n, 2))$.

PROOF: (a) Evidently, $\text{PSL}(i, 2) \rightarrow \text{PSL}(i + 1, 2)$ for every $i \geq 1$, and so $\pi_e(\text{PSL}(i, 2)) \subseteq \pi_e(\text{PSL}(i + 1, 2))$. Moreover, $\text{PSL}(i, 2)$ contains a Singer cycle of order $2^i - 1$. This proves part (a).

(b) These facts are quite well-known, see for instance [9].

(c) Take $A \in c = (f^n)$, where $f_1$ is irreducible polynomial over GF(2) of degree 1. Then the result follows from Lemma 1.

(d) Let $A \in \text{PSL}(n, 2)$ have characteristic polynomial $f = f_{m_1}^{k_1}f_{m_2}^{k_2} \cdots f_{m_s}^{k_s}$, where $f_{m_i}$ is irreducible polynomial over GF(2) of degree $m_i$. Assume that $t$ and $e$ are as in Lemma 1. Clearly $o(A)$ divides $2^te$, and by noticing that $\sum_{i=1}^{n} m_i k_i = n$, we conclude that

\[
o(A) \leq 2^e \leq 2^t (2^{m_1} - 1)(2^{m_2} - 1) \cdots (2^{m_s} - 1) \leq 2^{t + \sum_{i=1}^{s} m_i} - 1 \leq 2^n - 1,
\]

completing the part (d).

(e) Assume that $A \in \text{PSL}(n, 2)$. Evidently $A \in c = (f^n - 2f^k)$ if and only if $(i, k) = (1, 2)$ or $(2, 1)$. Using (4), in the first case we have $o(A) = 2(2^{n-2} - 1)$, and in the latter case we have

\[
o(A) = \begin{cases} 
2^{n-2} - 1 & \text{if } n \text{ is even}, \\
3(2^{n-2} - 1) & \text{if } n \text{ is odd}.
\end{cases}
\]

Hence $k(2^{n-2} - 1) \in \pi_e(\text{PSL}(n, 2))$ if and only if $k = 1, 2$ or 3. Now, with the same argument as in (d) we may prove that $2(2^{n-2} - 1)$ is the maximal even number in $\pi_e(\text{PSL}(n, 2))$, which implies that $2(2^{n-2} - 1) \in \mu(\text{PSL}(n, 2))$.

(f) Assume that $A \in c = (f_{m_1}, f_{m_2}, \ldots, f_{m_s})$, where $f_{m_i}$ is irreducible polynomial over GF(2) of degree $m_i$, and $o(U_1(f_{m_i})) = 2^{m_i} - 1$. Now by Lemma 1, it is easy to see that

\[
o(A) = \text{l.c.m.}(2^{m_1} - 1, 2^{m_2} - 1, \ldots, 2^{m_s} - 1) = \prod_{i=1}^{s} (2^{m_i} - 1),
\]
since \((2^{m_i} - 1, 2^{m_j} - 1) = 2^{(m_i, m_j)} - 1 = 1\).

Now, we show that \(o(A) \in \mu(\text{PSL}(n, 2))\). Assume that \(\text{PSL}(n, 2)\) contains an element, say, \(B\), such that \(o(A)\) divides \(o(B)\). Suppose that \(B \in (f_{d_1}^{k_1} f_{d_2}^{k_2} \cdots f_{d_z}^{k_z})\), where \(f_{d_j}, 1 \leq j \leq z\), is an irreducible polynomial over \(\text{GF}(2)\) of degree \(d_j\), \(\sum_{j=1}^{z} k_j d_j = n\) and \(o(U_1(f_{d_j})) = 2^{d_j} - 1\). From Lemma 1, we have \(o(B) = 2^t\), where \(t\) is the least positive integer such that \(2^t \geq \max(k_1, k_2, \ldots, k_z)\) and \(e = \text{l.c.m.}(2^{d_1} - 1, 2^{d_2} - 1, \ldots, 2^{d_z} - 1)\). Since \(o(A)\) divides \(o(B)\), for each \(i\) there is a \(j(i)\) such that \(m_i \mid d_{j(i)}\), \(1 \leq i \leq s\). Hence \(m_i \leq d_{j(i)}\) implying \(\sum_{i=1}^{s} m_1 \leq \sum_{i=1}^{s} d_{j(i)}\).

On the other hand, since \(k_i \geq 1\), we obtain

\[
\sum_{j=1}^{z} d_j \leq \sum_{i=1}^{z} k_j d_j = \sum_{i=1}^{s} m_1 \leq \sum_{i=1}^{s} d_{j(i)}.
\]

Therefore equality holds, which implies \(s = z, k_i = 1\) and \(d_{j(i)} = m_i\), for all \(i, 1 \leq i \leq s\). Hence \(A = B\), and the result follows. \(\square\)

**Lemma 2.** Let \(G = \text{PSL}(n, 2)\), where \(n = 9, 10, 11, 12, 13\). Then \(\mu(G)\) is given as in Table 4.

**Proof:** First of all, using (2) and (3) we calculate the values of \(w(n, 2)\) and \(p_n\) where \(1 \leq n \leq 13\), and list them in Table 1.

**Table 1.** The number of irreducible polynomials of degree \(n\) over \(\mathbb{Z}_2\), and the number of partitions of \(n\).

<table>
<thead>
<tr>
<th>(n)</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>(w(n, 2))</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>18</td>
<td>30</td>
<td>56</td>
<td>99</td>
<td>186</td>
<td>335</td>
<td>630</td>
</tr>
<tr>
<td>(p_n)</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>11</td>
<td>15</td>
<td>22</td>
<td>30</td>
<td>42</td>
<td>56</td>
<td>77</td>
<td>101</td>
</tr>
</tbody>
</table>

Next, we calculate the values of \(c(n, 2)\), where \(1 \leq n \leq 13\). In fact, using (1) we obtain

\[
\sum_{n=0}^{\infty} c(n, 2)x^n = \prod_{m=1}^{\infty} p(x^m)^{w(m, 2)} = 1 + x + 3x^2 + 6x^3 + 14x^4 + 27x^5 + 60x^6 + 117x^7 + 246x^8 + 490x^9 + 1002x^{10} + 1998x^{11} + 4031x^{12} + 8066x^{13} + \cdots.
\]

Finally, we calculate \(o(U_k(f_i))\) with \(k \geq 2\) and \(ki \leq 13\), which is given in Table 2.
Some results on the recognizability of the linear groups over the binary field

Table 2. The order of $A \in \text{GL}(ki, 2)$ having characteristic polynomial $f_1^k$, where $k > 1$ and $ki \leq 13$.

<table>
<thead>
<tr>
<th>$k$</th>
<th>$f_1$</th>
<th>$f_2$</th>
<th>$f_3$</th>
<th>$f_4$</th>
<th>$f_5$</th>
<th>$f_6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>6</td>
<td>14</td>
<td>30</td>
<td>62</td>
<td>126</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>12</td>
<td></td>
<td>28</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>12</td>
<td></td>
<td>28</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$5 \leq k \leq 6$</td>
<td>8</td>
<td>24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$7 \leq k \leq 8$</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$9 \leq k \leq 13$</td>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

First suppose $G = \text{PSL}(9, 2)$. By (5), $G$ contains 490 conjugacy classes. Now, by the previous explanations and using Lemma 1 and Table 2, we can easily list these conjugacy classes and find the maximum order for all elements in the conjugacy classes having the same characteristic polynomial, which is denoted by $m$ in the last column of Table 3. Therefore, we derive the set $\mu(G)$ from this column, as required. Note that, in Table 3, Par($k$) denotes the set of partitions of $k$. We can find $\mu(\text{PSL}(n, 2))$ for $n = 10, 11, 12$ and 13, in a similar manner. The final result is tabulated in Table 4.

Table 3. The order of elements of the simple group $\text{PSL}(9, 2)$.

<table>
<thead>
<tr>
<th>Type of $c$</th>
<th>Conditions</th>
<th>Number</th>
<th>$m$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(f_1^r)$</td>
<td>$r \in \text{Par}(9)$</td>
<td>30</td>
<td>$16 = 2^4$</td>
</tr>
<tr>
<td>$(f_3^r f_1)$</td>
<td>$r \in \text{Par}(4)$</td>
<td>5</td>
<td>$12 = 2^2 \cdot 3$</td>
</tr>
<tr>
<td>$(f_2^r f_3)$</td>
<td>$r, s \in \text{Par}(3)$</td>
<td>9</td>
<td>$12 = 2^2 \cdot 3$</td>
</tr>
<tr>
<td>$(f_2^r f_1)$</td>
<td>$r \in \text{Par}(2), s \in \text{Par}(5)$</td>
<td>14</td>
<td>$24 = 2^3 \cdot 3$</td>
</tr>
<tr>
<td>$(f_2^r)$</td>
<td>$r \in \text{Par}(7)$</td>
<td>15</td>
<td>$24 = 2^3 \cdot 3$</td>
</tr>
<tr>
<td>$(f_3^r f_2 f_1)$</td>
<td>$r \in \text{Par}(2)$</td>
<td>5</td>
<td>$42 = 2 \cdot 3 \cdot 7$</td>
</tr>
<tr>
<td>$(f_3^r f_1)$</td>
<td>$r \in \text{Par}(2), s \in \text{Par}(3)$</td>
<td>15</td>
<td>$28 = 2^2 \cdot 7$</td>
</tr>
<tr>
<td>$(f_3^r)$</td>
<td>$r \in \text{Par}(3)$</td>
<td>10</td>
<td>$28 = 2^2 \cdot 7$</td>
</tr>
<tr>
<td>$(f_3^r f_2)$</td>
<td>$r \in \text{Par}(2)$</td>
<td>8</td>
<td>$42 = 2 \cdot 3 \cdot 7$</td>
</tr>
<tr>
<td>$(f_3^r f_1)$</td>
<td>$r \in \text{Par}(4)$</td>
<td>10</td>
<td>$84 = 2^2 \cdot 3 \cdot 7$</td>
</tr>
<tr>
<td>$(f_3^r f_2)$</td>
<td>$r \in \text{Par}(6)$</td>
<td>22</td>
<td>$56 = 2^3 \cdot 7$</td>
</tr>
<tr>
<td>$(f_3^r f_1)$</td>
<td>$r \in \text{Par}(2)$</td>
<td>9</td>
<td>$30 = 2 \cdot 3 \cdot 5$</td>
</tr>
<tr>
<td>$(f_3^r f_2 f_1)$</td>
<td>$r \in \text{Par}(2)$</td>
<td>6</td>
<td>$105 = 3 \cdot 5 \cdot 7$</td>
</tr>
<tr>
<td>$(f_3^r f_1)$</td>
<td>$r \in \text{Par}(2)$</td>
<td>12</td>
<td>$210 = 2 \cdot 3 \cdot 5 \cdot 7$</td>
</tr>
<tr>
<td>$(f_3^r f_2)$</td>
<td>$r \in \text{Par}(2)$</td>
<td>6</td>
<td>$30 = 2 \cdot 3 \cdot 5$</td>
</tr>
<tr>
<td>$(f_3^r f_1)$</td>
<td>$r \in \text{Par}(3)$</td>
<td>9</td>
<td>$60 = 2^2 \cdot 3 \cdot 5$</td>
</tr>
<tr>
<td>$(f_3^r f_1)$</td>
<td>$r \in \text{Par}(5)$</td>
<td>21</td>
<td>$120 = 2^3 \cdot 3 \cdot 5$</td>
</tr>
</tbody>
</table>
Table 4. The set of orders of elements of some projective special linear groups.

<table>
<thead>
<tr>
<th>$G$</th>
<th>$\mu(G)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSL(9, 2)</td>
<td>16, 56, 120, 124, 186, 210, 217, 252, 254, 255, 381, 465, 511</td>
</tr>
<tr>
<td>PSL(11, 2)</td>
<td>48, 120, 248, 315, 372, 420, 504, 508, 762, 868, 889, 930, 1020, 1022, 1023, 1533, 1785, 1905, 1953, 2047</td>
</tr>
<tr>
<td>PSL(12, 2)</td>
<td>48, 112, 504, 630, 744, 840, 868, 1016, 1020, 1302, 1524, 1533, 1785, 1778, 1860, 1905, 1953, 2044, 2046, 2047, 2667, 3255, 3937, 4095</td>
</tr>
<tr>
<td>PSL(13, 2)</td>
<td>112, 240, 504, 744, 840, 1016, 1260, 1524, 1736, 1860, 2040, 2044, 2604, 3066, 3255, 3556, 3570, 3810, 3906, 3937, 4092, 4094, 4095, 6141, 7161, 7665, 7905, 8001, 8191</td>
</tr>
</tbody>
</table>

3. Recognizing PSL(13, 2) by its order elements

Our main result of this section is the characterization of PSL(13, 2) by its order elements, in fact we prove the statement of the Main Theorem.

We begin with a well-known theorem due to Gruenberg and Kegel.

**Gruenberg-Kegel Theorem** (see [18, Theorem A]). *If G is a finite group with disconnected prime graph $\Gamma(G)$ then one of the following holds.*

1. $t(G) = 2$ and $G$ is either a Frobenius or a 2-Frobenius group.
2. $G$ is an extension of a $\pi_1(G)$-group $N$ by a group $G_1$, where $P \trianglelefteq G_1 \trianglelefteq \text{Aut}(P)$, $P$ is a non-abelian simple group and $G_1/P$ is a $\pi_1(G)$-group. Moreover $t(P) \geq t(G)$ and for every $i, 2 \leq i \leq t(G)$, there exists $j, 2 \leq j \leq t(P)$, such that $\pi_j(P) = \pi_i(G)$.
By Lemma 2, we know that $26 \notin \mu(\text{PSL}(13,2))$. Now, in the following lemma we prove that there is an outer automorphism of $\text{PSL}(13,2)$ of order 26, which certainly proves that $\pi_e(\text{PSL}(13,2)) \subseteq \pi_e(\text{Aut}(\text{PSL}(13,2)))$.

**Lemma 3.** The group $\text{Aut}(\text{PSL}(13,2))$ contains an element of order 26.

**Proof:** Let $\theta$ be an involuntary graph automorphism of $G = \text{PSL}(13,2)$. Using the notation in [2] we have $G^+ = \text{Aut}(G) = G \cdot \langle \theta \rangle = G \cup \theta G$. The conjugacy classes of $G^+$ which lie in $\theta G$ are called negative classes and by Theorem 1 in [2], $G^+$ has only one negative conjugacy class of involutions with representative $\theta I$ and we have

$$|C_{G^+}(\theta I)| = 2^{37}(2^2 - 1)(2^4 - 1) \cdots (2^{12} - 1) = 2^{37} \cdot 3^8 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 31,$$

where $I$ is the identity matrix. Now, we deduce that $2 \cdot 13 \in \pi_e(G^+)$.

**Lemma 4.** If $G$ is a simple group of Lie type such that $8191 \in \pi(G) \subseteq \pi(\text{PSL}(13,2))$, then $G$ is isomorphic to $\text{PSL}(13,2)$ or $\text{PSL}(2,8191)$.

**Proof:** Suppose $G$ is a finite simple group of Lie type over a finite field of order $q = p^n$, where $p$ is a prime and $n$ is a natural number. Evidently $p \in \pi(G)$, hence $p$ may be equal to 2, 3, 5, 7, 11, 13, 17, 23, 31, 73, 89, 127 or 8191. If $p = 2$, then it is clear that the order of 2 modulo 8191 is 13, and there is no natural number $m$ such that $2^m + 1 \equiv 0 \pmod{8191}$. Thus if $2^k - 1$ divides $|G|$ and $8191 \in \pi(2^k - 1)$, for some $k$, then $k$ must be a multiple of 13. Therefore, from Table 6 in [1], the only candidate for $G$ under our assumptions is $A_{12}(2) \cong \text{PSL}(13,2)$. Suppose $p = 3$. In this case the calculations show that the order of 3 modulo 8191 is greater than 100. Now, if $G$ is a simple group of Lie type in characteristic 3, the order of which is divisible by 8191, from Table 6 in [1], no candidates for $G$ will arise. Similarly for $p = 5, 7, 11, 13, 17, 23, 31, 73, 89, 127$, there is no group with the above property. If $p = 8191$, then $q$ must be a power of 8191 and the only possible group is $G = A_1(8191) \cong \text{PSL}(2,8191)$. The lemma is proved.

**Lemma 5.** The special linear group $\text{PSL}(13,2)$ has a Frobenius subgroup of shape $3^3 : 13$.

**Proof:** Let $F$ be the finite field with $3^3$ elements. Let $H$ be the cyclic subgroup of $F^\times$ with order 13. Then it is easy to verify that

$$G = \{ f_{a,b} : F \to F \mid f_{a,b}(x) = ax + b, \ a \in H, \ b \in F, \ \forall x \in F \}$$

is a Frobenius group with complement $H$ and kernel the additive group of $F$ which is an elementary abelian group of order $3^3$. Therefore the existence of the Frobenius group $G$ of the shape $3^3 : 13$ is established.
But from \[6, \text{p.68}\] the complex character table of the group \(G\) can be constructed. In particular, \(G\) has 13 irreducible complex characters of degree 1 and two with degree 13, apparently the characters of degree 13 are faithful. But it is well-known that the degrees of the irreducible characters of any finite group \(G\) over a field whose characteristic does not divide the order of \(G\) are the same as the degrees of ordinary irreducible characters of \(G\). Therefore the Frobenius group \(G = 3^3 : 13\) has an irreducible character of degree 13 over a field with characteristic 2 which is denoted by \(K\). Therefore we have the faithful representation \(G \to \text{GL}(13, K)\) affording the character of degree 13. But the above representation can be realized over a field with two elements. Therefore we have a monomorphism \(G \to \text{GL}(13, 2)\) proving the lemma. □

Now we are able to prove the Main Theorem of this section.

**Proof of Main Theorem:** We only need to prove the sufficiency part. Let \(G\) be a finite group for which \(\pi_e(G) = \pi_e(\text{PSL}(13, 2))\). Then \(t(G) = 2\) and the connected components of the prime graph of \(\Gamma(G)\) are:

\[
\pi_1(G) = \{2, 3, 5, 7, 11, 13, 17, 23, 31, 73, 89, 127\} \quad \text{and} \quad \pi_2(G) = \{8191\}
\]

(see [8]). We will prove that \(G\) is isomorphic to \(\text{PSL}(13, 2)\). First of all, from [11] \(G\) is non-soluble and so \(G\) is not a 2-Frobenius group. On the other hand, since \(2 \cdot 13 \notin \pi_e(G)\), by Lemma 2.7 in [3] it follows that \(G\) cannot be a Frobenius group.

Now, we adhere to the notation of item (2) of the Gruenberg-Kegel theorem. We invoke the Classification of Finite Simple Groups to eliminate all possibilities for \(P\) (see [1]). Note that \(\pi_2(G) = \pi_j(P) = \{8191\}\) for some \(j \geq 2\). We claim that \(P \cong \text{PSL}(13, 2)\). If \(P\) is an alternating group \(A_n, n \geq 5\), then since \(8191 \in \pi(P)\), we deduce \(n \geq 8191\). But then \(19 \in \pi(G)\), which is a contradiction. Also, \(P\) cannot be a sporadic simple group, because otherwise the maximum prime in \(P\) would be 71, whereas \(8191 \in \pi(P)\), which is a contradiction. Finally, we assume that \(P\) is a simple group of Lie type. In this case, by Lemma 4, we obtain \(P \cong \text{PSL}(13, 2)\) or \(\text{PSL}(2, 8191)\). If \(P \cong \text{PSL}(2, 8191)\), then we get \(4096 \in \pi_e(P) \setminus \pi_e(G)\), which is a contradiction. Therefore, \(P \cong \text{PSL}(13, 2)\), as claimed.

Now, we show that \(N = 1\). Assume the contrary. Without loss of generality we may assume that \(N = O_r(G)\) for some prime \(r \in \pi_1(G)\). Moreover, we may assume that \(N\) is an elementary abelian subgroup and \(C_{G_1}(N) = N\). Let \(K = \langle A \rangle\) where \(A \in \text{GL}(12, 2)\) and \(o(A) = 2^{12} - 1\). Then

\[
L = \left\{ \begin{bmatrix} 1 & a_1 & a_2 & \ldots & a_{12} \\ 0 & X \\ \end{bmatrix} \bigg| X \in K, a_i \in GF(2), 1 \leq i \leq 12 \right\} \leq \text{PSL}(13, 2).
\]

We put

\[
S = \left\{ \begin{bmatrix} 1 & a_1 & a_2 & \ldots & a_{12} \\ 0 & I \\ \end{bmatrix} \bigg| a_i \in GF(2), 1 \leq i \leq 12 \right\},
\]
Some results on the recognizability of the linear groups over the binary field

and

\[ T = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & X \end{bmatrix} \mid X \in K \right\}. \]

Then we form the semi-direct product

\[ L = T \times S = 2^{12} : (2^{12} - 1) \leq \text{PSL}(13, 2) \leq G_1 \leq G/N. \]

Now, if \( r \neq 2 \), then by Lemma 6 in [14], we get \( r \cdot (2^{12} - 1) \in \pi_e(G) \), which contradicts Lemma 2. Thus, \( N \) is a non-trivial 2-subgroup. In this case, we have \( 3^3 : 13 < \text{PSL}(13, 2) \) by Lemma 5, and again by Lemma 6 in [14], we obtain \( 26 \in \pi_e(G) \), which contradicts Lemma 2. Therefore \( N = 1 \).

Finally, we claim that \( G \cong \text{PSL}(13, 2) \). Because \( N = 1 \), we obtain

\[ \text{PSL}(13, 2) \leq G \leq \text{Aut}(\text{PSL}(13, 2)). \]

Moreover, since \( |\text{Out}(\text{PSL}(13, 2))| = 2 \), it follows that \( G \cong \text{PSL}(13, 2) \) or \( G \cong \text{Aut}(\text{PSL}(13, 2)) \). However, by Lemma 3 we have \( \pi_e(G) \subsetneq \pi_e(\text{Aut}(\text{PSL}(13, 2))) \), which implies that \( G \cong \text{PSL}(13, 2) \), as claimed. \( \square \)

**References**


M.R. Darafsheh, Y. Farjami:
**DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCES, UNIVERSITY OF TEHRAN, TEHRAN, IRAN**

*E-mail: daraf@khayam.ut.ac.ir*

M. Khademi:
**ISLAMIC AZAD UNIVERSITY, TEHRAN SOUTH BRANCH, TEHRAN, IRAN**

A.R. Moghaddamfar:
**DEPARTMENT OF MATHEMATICS, K.N.T. UNIVERSITY OF TECHNOLOGY, P.O. BOX 16315-1618, TEHRAN, IRAN**

*(Received February 11, 2005, revised June 10, 2005)*