<table>
<thead>
<tr>
<th>Title</th>
<th>Primitive extensions of rank 3 of the finite projective special linear groups $\text{PSL}(n,q)$, $q=2^f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Bannai, Eiichi</td>
</tr>
<tr>
<td>Citation</td>
<td>Osaka Journal of Mathematics. 9(1) P.57–P.73</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1972</td>
</tr>
<tr>
<td>Text Version</td>
<td>publisher</td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://doi.org/10.18910/10249">https://doi.org/10.18910/10249</a></td>
</tr>
<tr>
<td>DOI</td>
<td>10.18910/10249</td>
</tr>
<tr>
<td>rights</td>
<td></td>
</tr>
</tbody>
</table>

Osaka University Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/repo/ouka/all/

Osaka University
0. Introduction

Let $P$ be the set of the points of $(m-1)$-dimensional projective space defined over a finite field $F_q$ with $q$ elements. The projective special linear group $PSL(n, q)$ acts doubly transitively on the set $P$ via the natural action. In [14], H. Zassenhaus completely determined transitive extensions (=primitive extensions of rank 2) of the permutation groups $(PSL(n, q), P)$. (Cf. [1].) In this note we will completely determine primitive extensions of rank 3 of the permutation groups $(PSL(n, q), P)$ in the case where $q$ are even. Our main result is the following

Theorem 1. Let $(n, f)= (2, 1)$ and $(2, 2)$. Then the permutation groups $(PSL(n, 2^f), P)$, $n \geq 2$, have no primitive extensions of rank 3.

We hope to treat the remaining cases where $q$ are odd in the next paper.

The paper [11] by T. Tsuzuku which determined primitive extensions of rank 3 of the natural representation of the symmetric group was useful to the author in setting about this work. After the most part of this work was accomplished, the paper [8] by S. Montague has been published, which uses a similar strategy as ours but the obtained results are different from ours.

In concluding the introduction we give a brief sketch of the proof of Theorem 1: if $(\mathcal{G}, \Omega)$ is a primitive extension of rank 3 of the permutation group $(PSL(n, q), P)$, then $\mathcal{G}_a$ $(a \in \Omega)$ has three orbits $\{a\}$, $\Delta(a)$ and $\Gamma'(a)$, and we may assume that $(PSL(n, q), P) \simeq (\mathcal{G}_a, \Delta(a))$ as a permutation group. In § 1 we derive some numerical relations (most of which are due to D. G. Higman) which must be satisfied by $k=|\Delta(a)|$ and $l=|\Gamma'(a)|$ (see Propositions 1.1~1.6). After the consideration of some subgroups of $PSL(n, q)$, we prove in § 2 that $L=\mathcal{G}_{a,b}$ $(b \in \Gamma'(a))$ must be of very restricted type, that is, only one of the Cases 1~6 stated at the beginning of § 3 must hold for $n \geq 5$. In § 3, for $n \geq 5$, we derive
a contradiction for every $L$ in Cases 1~6, either by using the numerical relations given in § 1 or by calculating the number of elements in $\mathfrak{G}$ which are conjugate to an elation $\tau$, in $\text{PSL}(n, q)$, and we complete the proof of Theorem 1 for $n \geq 5$. Finally for $n \leq 4$, we also complete the proof of Theorem 1 by using the similar method as in the case of $n \geq 5$ together with some additional adhoc considerations.

1. Preliminary results

A) Results on primitive permutation groups of rank 3.

Here we collect for the later use some results on primitive permutation group of rank 3 due to D. G. Higman [4] and [5].

The following notation will be fixed throughout the present note. Let $(\mathfrak{G}, \Omega)$ be a primitive extension of rank 3 of the permutation group $(\text{PSL}(n, q), \mathcal{P})$. That is to say,

1) $\mathfrak{G}$ is primitive of rank 3 on the set $\Omega$, and
2) there exists an orbit $A(\alpha)$ of the stabilizer $\mathfrak{G}_\alpha (\alpha \in \Omega)$, and that $(\mathfrak{G}_\alpha, \Delta(\alpha))$ is faithful and isomorphic to $(\text{PSL}(n, q), \mathcal{P})$ as a permutation group.

Let $k$ be the length of the orbit $\Delta(\alpha)$, and let $l$ be the length of another nontrivial orbit $\Gamma(\alpha)$ of $\mathfrak{G}_\alpha$. Clearly $k=(q^n-1)/(q-1)$. Let $\lambda, \mu$ be the intersection numbers for $\mathfrak{G}$ defined by

$$ |\Delta(\alpha) \cap \Delta(\beta)| = \begin{cases} \lambda & \text{if } b \in \Delta(\alpha) \\ \mu & \text{if } b \in \Gamma(\alpha). \end{cases} $$

Then the relation $\mu l=k(k-\lambda-1)$ holds.

Now, the following Propositions 1.1~1.4 are immediately obtained from [4], [5] and the theorem of W. A. Manning [13, Th. 17.7], by noting that $(\mathfrak{G}_\alpha, \Delta(\alpha))$ is doubly transitive. (Here we assume that $q$ is an arbitrary power of any prime).

**Proposition 1.1.** $\lambda=0$.

**Proposition 1.2.** $k \leq l \leq k(k-1)$ and $l \mid k(k-1)$.

**Proposition 1.3.** $l=k(k-1)$ implies $k=2, 3, 7$ or 57, and this implies $(n, q)=(2, 2), (3, 2), \text{ or } (3, 7)$.

**Proposition 1.4.** $d=(\lambda-\mu)^2+4(k-\mu)=4k+\mu^2-4\mu$ is a square, and $\sqrt{d}$ divides $b=2k+(\lambda-\mu)(k+l)=2k-\mu k-\mu l$.

Moreover we easily have the following propositions.

**Proposition 1.5.** $b^2 = \frac{1}{4} k^2 + \left( -\frac{1}{16} \mu^2 + \frac{12}{16} \mu - \frac{24}{16} \right) k^2 + \frac{1}{64} (\mu-2)^2 (\mu-6)^2$. 
\[
+ \frac{1}{256} \frac{\mu(\mu - 4)(\mu - 2)(\mu - 6)^2 - \frac{1}{4} \frac{\mu^4(\mu - 4)^2(\mu - 2)^2(\mu - 6)^2}{4k + \mu^2 - 4\mu}}{b + \sqrt{d}}
\]

Hence, to prove that \( \frac{b}{\sqrt{d}} \) is not an integer, we have only to prove that \( \frac{b^2}{d} \) is not an integer, and moreover we have only to prove that
\[
\alpha = \frac{\mu^2(\mu - 4)^2(\mu - 2)^2(\mu - 6)^2}{4k + \mu^2 - 4\mu}
\]

is not an integer.

**Proposition 1.6.** If we set \( u = \frac{1}{k} \left( \frac{k - 1}{\mu} \right) \), then
\[
d = \frac{k^2 + (4u^2 - 4u - 2)k + 4u + 1}{u^2}
\]

**B) Results on some subgroups of the group** \( \text{PSL}(n, q) \) **and** \( \text{PGL}(n, q) \). (Here \( q \) need not be even.)

The following Proposition 1.7 has been proved in E. Bannai [2, Lemma 1]. The proof depends heavily on the papers [9 and 10] by F. C. Piper which characterizes the group \( \text{PSL}(n, q) \) from a geometric viewpoint.

**Proposition 1.7.** Let \( H \) be a proper subgroup of index \( m \) of the group \( \text{PSL}(n, q) \) with \( n \geq 4 \), and let \( q^{n-2} \nmid m \). Then \( H \) fixes some complete subspace of the projective space \( \mathcal{P}(n-1, q) \).

By slightly modifying the proof in [2], we immediately have the following

**Proposition 1.8.** Let \( H \) be a subgroup of index \( m \) of the group \( \text{PGL}(n, q) \) with \( n \geq 4 \), and let \( q^{n-2} \nmid m \). Then either \( H \supseteq \text{PSL}(n, q) \) or \( H \) fixes some complete subspace of the projective space \( \mathcal{P}(n-1, q) \).

Now let us consider subgroups of the group \( \text{PGL}(2, 2^f) \). Note that \( \text{PGL}(2, 2^f) = \text{PSL}(2, 2^f) \).

**Proposition 1.9.** (due to L. E. Dickson and others.) (For the proof, see [6] page 213.) If \( H \) is a maximal subgroup of \( \text{PGL}(2, 2^f) \), then \( H \) is conjugate to one of the following subgroups \( A, B, C, D_j \) or \( Z_3 \):

1) \( A = \left\{ x; x \in \text{GL}(2, 2^f), x = \begin{pmatrix} * & 0 \\ 0 & \end{pmatrix} \right\} \). (\( A \) is a semi-direct product of an elementary abelian group of order \( 2^f \) by a cyclic group of order \( 2^f - 1 \).)
2) \( B = \left\{ x; x \in \text{GL}(2, 2^f), x = \begin{pmatrix} 0 & * \\ 0 & \end{pmatrix} \text{ or } x = \begin{pmatrix} * & 0 \\ 0 & \end{pmatrix} \right\} \). (\( B \) is a dihedral group of order \( 2(2^f - 1) \)).
3) \( C = \text{dihedral group of order } 2(2^f + 1), \text{ for } f \geq 1 \).
4) \( D_j = \left\{ \bar{x}; x \in \text{GL}(2, 2^f) \subseteq \text{GL}(2, 2^f) \right\} \). (\( D_j \approx \text{PGL}(2, 2^j) \)).

1) Strictly speaking, all \( D_j \) are not maximal.
2) \( x \rightarrow \bar{x} \) denotes the natural projection mapping \( \text{GL}(2, q) \rightarrow \text{PGL}(2, q) \).
5) \( Z_3 \) (cyclic group of order 3), only for \( f=1 \).

As an easy corollary of Proposition 1.9 we have the following

**Proposition 1.10.** Let \( H \) be a subgroup of \( PGL(2, 2^f) \) whose index \( m \) divides \( 2^f(2^f+1) \) and is smaller than it. Then \( H \) is conjugate to one of the following subgroups:

1) \( PGL(2, 2^f), m=1 \),  
2) \( A, m=2^f+1 \),  
3) \( B, m=2^f(2^f+1)/2 \),  
4) \( D_{2^f} \) (only for \( f \) even), \( m=2^{f+1}(2^f+1) \),  
5) \( Z_3 \) (only for \( f=1 \)), \( m=2 \).

We omit the proof of Proposition 1.10, since it is straightforward and easy.

Now let us consider subgroups of the groups \( PSL(3, 2^f) \) and \( PGL(3, 2^f) \).

**Proposition 1.11.** (due to R. W. Hartley.) If \( H \) is a maximal subgroup of the group \( PSL(3, 2^f) \), then \( H \) is conjugate to one of the following subgroups\(^3\) listed in 1)~6):

1) stabilizers of a point,  
2) stabilizers of a line,  
3) stabilizers of a triangle,  
4) \( PSL(3, 2^f), j|f \) and \( j<f \).  
5) \( PSU(3, 2^f) \), \( 2j|f \) and \( 2j|f \).  
6) \( A_o \), for \( f \geq 2 \).

For the proof, see R. W. Hartley [3].

As a corollary of Proposition 1.11, we have the following

**Proposition 1.12.** Let \( H \) be a subgroup of the group \( PGL(3, q) \) with \( q=2^f \) whose index \( m \) divides \( (q^2+q+1)(q^2+q) \) and is smaller than it. Then either \( H \supseteq PSL(3, 2^f) \) or \( H \) stabilizes a point or a line of the projective space \( \mathbb{P}(2, q) \).

Proof. If a conjugate of \( H \cap PSL(3, 2^f) \) is contained in a maximal subgroup of \( PSL(3, 2^f) \) which is in one of the cases 3)~6) in Proposition 1.11, then \( 2^{f+1} \) \( | \) \( |PGL(3, 2^f)| \) \( H \) \( | \) \( |PSL(3, 2^f)| \) \( PSL(3, 2^f) \) \( H \), and this is a contradiction. Moreover, we easily have the assertion.

2. **Structures of some subgroups of the group \( PSL(n, q) \)**

A) Definition of some subgroups of \( PSL(n, q) \).

Before setting about the proof of Theorem 1, we fix some notations for subgroups of \( PSL(n, q) \).

---

\(^3\) Strictly speaking, all these subgroups are not maximal.
Let $GL(n, q)$ be the group of invertible $n \times n$ matrices whose coefficients lie in the finite field $F_q$, $q$ being a power of an arbitrary prime $p$ ($q = p^r$). Let us set $SL(n, q) = \{ x \in GL(n, q); \det x = 1 \}$, and

$$Z = \left \{ x \in GL(n, q); x = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \right \},$$

$$Z^{(i, n-i)} = \left \{ x \in GL(n, q); x = \begin{pmatrix} \alpha I_i & 0 \\ 0 & \beta I_{n-i} \end{pmatrix} \right \}^i \text{ where } I_i \text{ denotes the } i \times i \text{ identity matrix.}$$

Let us set

$$PGL(n, q) = GL(n, q)/Z,$$

$$PSL(n, q) = SL(n, q)/SL(n, q) \cap Z.$$ 

We denote by $\bar{x}$ the homomorphic image of $x \in GL(n, q)$ by the above natural homomorphism $GL(n, q) \to PGL(n, q)$. As is well known, the groups $PGL(n, q)$ and $PSL(n, q)$ naturally act doubly transitively on the set of the points of the projective space $\mathbb{P}(n-1, q)$. The orders of these groups are given as follows:

$$|GL(n, q)| = q^{n^2/2(n-1)} (q^n-1)(q^{n-1}-1) \cdots (q-1)(q-1),$$

$$|SL(n, q)| = |PGL(n, q)| = \frac{1}{q-1} |GL(n, q)|,$$

$$|PSL(n, q)| = \frac{1}{(n, q-1)} |PGL(n, q)|,$$

where $(n, q-1)$ denotes the $G.C.D.$ of $n$ and $q-1$.

Now let us set

$$G^{(i, n-i)} = \left \{ \bar{x}; x \in SL(n, q), x = \begin{pmatrix} * & 0 \\ * & \end{pmatrix} \right \}^i \text{ n-i},$$

$$P^{(i, n-i)} = \left \{ \bar{x}; x \in SL(n, q), x = \begin{pmatrix} I_i & 0 \\ * & I_{n-i} \end{pmatrix} \right \}^i \text{ n-i},$$

$$K^{(i, n-i)} = \left \{ \bar{x}; x \in SL(n, q), x = \begin{pmatrix} 0 & 0 \\ 0 & * \end{pmatrix} \right \}^i \text{ n-i}.$$ 

Then we have $G^{(i, n-i)} = K^{(i, n-i)} P^{(i, n-i)} P^{(i, n-i)}$, $K^{(i, n-i)} \cap P^{(i, n-i)} = 1$, and $G^{(i, n-i)}$ is an maximal subgroup of $PSL(n, q)$ consisting of all the elements which fix an $(i-1)$-dimensional complete subspace of the projective space $\mathbb{P}(n-1, q)$. We denote by $\chi^{(i, n-i)}$ the natural homomorphism $G^{(i, n-i)} \to K^{(i, n-i)}$.

Let us set
E. Bannai

\[ \tilde{K}^{(i,n-i)} = \left\{ x; x \in SL(n, q), x = \left( \begin{array}{c} \ast \\ 0 \\ \ast \end{array} \right) n-i \right\} . \]

Since \( \tilde{K}^{(i,n-i)} \cap Z \subseteq \tilde{K}^{(i,n-i)} \cap Z^{(i,n-i)} \subseteq \tilde{K}^{(i,n-i)} \), we have naturally a homomorphism

\[ \tilde{K}^{(i,n-i)}/\tilde{K}^{(i,n-i)} \cap Z \xrightarrow{\rho^{(i,n-i)}} \tilde{K}^{(i,n-i)}/\tilde{K}^{(i,n-i)} \cap Z^{(i,n-i)} \cong \text{PGL}(i, q) \times \text{PGL}(n-i, q). \]

Note that if \( q=2^n \) and \( i=1 \) or 2, then

\[ \tilde{K}^{(i,n-i)}/\tilde{K}^{(i,n-i)} \cap Z^{(i,n-i)} = \text{PGL}(i, q) \times \text{PGL}(n-i, q). \]

B) The stabilizer subgroup of the permutation group \((\mathfrak{G}_a, \Gamma(a))\). From now on we always assume that \( q \) is a power of 2 (i.e., \( q=2^n \)) and that \( n \geq 4 \), unless the contrary is stated.

Let \( L \) be the stabilizer of a point of the permutation group \((\mathfrak{G}_a, \Gamma(a))\), where \( \mathfrak{G}_a \simeq \text{PSL}(n, q) \) and is simple from the assumption that \( n \geq 4 \). Thus the index of \( L \) in \( \mathfrak{G}_a \) is equal to \( l \), the length of \( \Gamma(a) \).

**Proposition 2.1.** Let \( n \geq 4 \). Then a conjugate of \( L \) is contained in either \( G^{(1,n-1)}, G^{(2,n-2)}, G^{(n-2,2)} \) or \( G^{(n-1,1)} \).

**Proof.** By Proposition 1.2, \( l \) is not divisible by \( q^n-1 \), hence from Proposition 1.7. \( L \) fixes some complete subspace of dimension, say \( s \). Hence a conjugate of \( L \) is contained in the group \( G^{(s+1,n-s-1)} \). (Here, note that \( \text{PSL}(n, q) \) is transitive on the set of all \( s \)-dimensional complete subspaces of \( \mathfrak{P}(n-1, q) \), where \( 0 \leq s \leq n-2 \).) But \( s+1 \) must be either 1, 2, \( n-2 \) or \( n-1 \), since otherwise the index \( l \) of \( L \) in \( \text{PSL}(n, q) \) which is a multiple of \( |\text{PSL}(n, q)|: G^{(s+1,n-s-1)}| \) does not divides \( k(k-1) \), and it contradicts Proposition 1.2. (Here, \( q \) need not be a power of 2.)

**Proposition 2.2.** Let \( n \geq 5 \). If \( L \) is contained in \( G^{(2,n-2)} \), then one of the following cases occurs:

1) \( L = G^{(2,n-2)}, \mu = q(q+1), \)

2) \( L \) is conjugate to

\[ M_1 = \left\{ \bar{x}; x \in SL(n, q), x = \left( \begin{array}{cc} \ast & 0 \\ \ast & 0 \end{array} \right) n-2 \right\}, \mu = q, \]

3) \( L \) is conjugate to
FINITE PROJECTIVE SPECIAL LINEAR GROUPS

\[ M_2 = \left\{ x; x \in SL(n, q), x = \begin{pmatrix} 2 & n-2 \\ \ast & 0 \\ 0 & \ast \end{pmatrix} \right\} \text{ or } \]

\[ x = \begin{pmatrix} 0 & 0 \\ \ast & \ast \end{pmatrix} \right\}^{n-2}, \mu = 2. \]

4) \( L \) is conjugate to

\[ M_3 = \left\{ x; x \in SL(n, 2f), x = \begin{pmatrix} 2 & n-2 \\ \ast & \ast \end{pmatrix} \right\}, \mu = 2. \]

\( \left(\begin{array}{cc}
 a & b \\
 c & d
\end{array}\right) \in PGL(2, 2^{2f}) \subseteq PGL(2, 2f) \right\} \text{ for } f \text{ even}, \mu = \sqrt{q} = 2^{f/2}. \]

Proof. Since (1) \( k < l < k(k-1) \) and (2) \( l \mid k(k-1), |PGL(2, q) \times PGL(n-2, q)| = \rho_{(2,n-2),\pi_{(2,n-2)}}(L) \) must be a divisor of \( q(q+1)-2(2f+1) \), since \( PGL(2, q) \times PGL(n-2, q) \) is the homomorphic image of \( G_{(2,n-2)} \) by \( \rho_{(2,n-2),\pi_{(2,n-2)}} \). Thus \( |I_2 \times PGL(n-2, q)| = \rho_{(2,n-2),\pi_{(2,n-2)}}(L) \cap (I_2 \times PGL(n-2, q)) \) must also a divisor of \( q(q+1) \) and less than \( q(q+1) \), since \( I_2 \times PGL(n-2, q) \) is normal in \( PGL(2, q) \times PGL(n-2, q) \). (Here, \( I_i \) denotes the identity subgroup of \( PGL(i, q) \). Thus by Proposition 1.8 and Proposition 1.12, \( I_2 \times PGL(n-2, q) \subseteq \rho_{(2,n-2),\pi_{(2,n-2)}}(L) \). (Here, note that \( q+1, q-1=1 \) since \( q=2f. \) While by Proposition 1.10, \( PGL(2, q) \times I_{n-2} \) must be conjugate to one of the following subgroups \( PGL(2, q) \times I_{n-2}, A \times I_{n-2}, B \times I_{n-2}, D_{f-2} \times I_{n-2} \) (for \( f \) even) or \( Z_3 \times I_{n-2} \) (for \( f=1 \). Hence, \( \rho_{(2,n-2),\pi_{(2,n-2)}}(L) \) is conjugate to one of the following subgroups (1) \( PGL(2, q) \times PGL(n-2, q), (2) A \times PGL(n-2, q), (3) B \times PGL(n-2, q), (4) D_{f-2} \times PGL(n-2, q) \) (for \( f \) even) or (5) \( Z_3 \times PGL(n-2, q) \) (for \( f=1 \). But the last case (5) is impossible, because otherwise \( d=4k^2+\mu^2-4\mu=4\cdot2^{2^{n-2}+\cdots+2+1} \) is not a square and this contradicts Proposition 1.4. In every case (1)~(4), we have

\[ L \cap P_1 = 1, \text{ where } P_1 = \left\{ x; x \in SL(n, q), x = \begin{pmatrix} 1 & 0 \\ \ast & \ast \end{pmatrix} \right\}, \text{ and } \]

\[ L \cap P_2 = 1, \text{ where } P_2 = \left\{ x; x \in SL(n, q), x = \begin{pmatrix} 1 & 0 \\ \ast & \ast \end{pmatrix} \right\}. \]
Clearly in every case (1)~(4), \( \pi^{(5,n-2)}(L) \) is transitive on the set of non-identity elements of \( P_1 \) (resp. \( P_2 \)). Hence \( L \supseteq P^{(5,n-2)} \), and we have the assertion of the proposition.

Similar argument proves the following

**Proposition 2.3.** Let \( n \geq 5 \). If \( L \) is contained in \( G^{(n-2,2)} \), then one of the following cases occurs:

1) \( L = G^{(n-2,2)} \), \( \mu = q(q+1) \),

2) \( L \) is conjugate to

\[
M'_1 = \left\{ x; x \in SL(n, q), x = \begin{pmatrix} * & 0 \\ * & 0 \\ * & 0 \end{pmatrix} \begin{pmatrix} n-2 & 2 \\ 0 & 2 \end{pmatrix} \right\}, \quad \mu = q,
\]

3) \( L \) is conjugate to

\[
M'_2 = \left\{ x; x \in SL(n, q), x = \begin{pmatrix} * & 0 \\ * & 0 \\ * & 0 \end{pmatrix} \begin{pmatrix} n-2 & 2 \\ 0 & 2 \end{pmatrix} \right\}, \quad \mu = 2,
\]

4) \( L \) is conjugate to

\[
M'_2 = \left\{ x; x \in SL(n, q), x = \begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix} \begin{pmatrix} n-2 & 2 \\ 0 & 2 \end{pmatrix} \right\}, \quad \mu = q,
\]

\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PGL(2, 2^{(f)}) \subseteq PGL(2, 2^f) \cdot \text{for } f \text{ even, } \mu = \sqrt{q} = 2^{f/2}.
\]

**Proposition 2.4.** Let \( n \geq 4 \). If \( L \) is contained in \( G^{(1,n-1)} \), then one of the following cases occurs:

1) \( u = |G^{(1,n-1)}: L| \) is a divisor of \( (q-1)(q-1, n-1)/(q-1, n) \) and more than 1.

2) \( L \) is conjugate to

\[
M'_1 = \left\{ x; x \in SL(n, q), x = \begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix} \begin{pmatrix} 2 & n-2 \\ 0 & 2 \end{pmatrix} \right\}, \quad \mu = q,
\]
3) \(L\) is conjugate to

\[ M_\mu = \{ x; x \in SL(n, q), x = \begin{pmatrix} \star & 0 & \cdots & 0 \\ \star & \star & \ddots & \vdots \\ \star & \star & \ddots & 0 \\ \star & \star & \cdots & \star \end{pmatrix} n-2 \}, \ \mu = q. \]

Proof. Note that \(\rho^{(1, n-1)}\pi^{(1, n-1)}(G^{(1, n-1)}) = PGL(1, q) \times PGL(n-1, q) (\cong 1 \times PGL(n-1, q))\). Since \(l\) satisfies the relations (1) \(k < l < k(k-1)\) and (2) \(l \mid k (k-1)\) by Proposition 1.2, \(|PGL(1, q) \times PGL(n-1, q): \rho^{(1, n-1)}\pi^{(1, n-1)}(L)|\) must be a divisor of \(k-1 = 2(2^{(n-2)} + \cdots + 2^{l} + 1)\). Then, by Propositions 1.8 and 1.12, either \(\rho^{(1, n-1)}\pi^{(1, n-1)}(L)\) contains \(PGL(1, q) \times PSL(n-1, q)\) or fixes a complete subspace of the projective subspace \(P(n-2, q) = \{(x_1, \cdots, x_{n}) \in \mathcal{P}(n-1, q); x_1 = 0\}\). Here, the dimension of the fixed complete subspace must be either 0 or \(n-3\), since otherwise \(|PGL(1, q) \times PSL(n-1, q): \rho^{(1, n-1)}\pi^{(1, n-1)}(L)|\) does not divide \(k(k-1)\), and this is a contradiction.

1) Let us assume that \(\rho^{(1, n-1)}\pi^{(1, n-1)}(L) \cong PGL(1, q) \times PSL(n-1, q)\). We have \(L \cap P^{(1, n-1)} = 1\). While \(\pi^{(1, n-1)}(L)\) acts transitively on the set of non-identity elements of \(P^{(1, n-1)}\). Noting that

\[
\begin{pmatrix} a & 0 & \cdots & 0 \\ b_2 & a_2 & \cdots & b_n \\ \vdots & \vdots & \ddots & \vdots \\ b_n & b_n & \cdots & a_n \\ \end{pmatrix} \begin{pmatrix} \star & \star & \cdots & \star \\ \star & \star & \cdots & \star \\ \vdots & \vdots & \ddots & \vdots \\ \star & \star & \cdots & \star \\ \end{pmatrix} = \begin{pmatrix} \star & \star & \cdots & \star \\ \star & \star & \cdots & \star \\ \vdots & \vdots & \ddots & \vdots \\ \star & \star & \cdots & \star \\ \end{pmatrix}
\]

with \(b_2 + A \cdot \begin{pmatrix} b_2 \\ \vdots \\ b_n \\ \end{pmatrix} = 0\), we immediately conclude that \(L \cong P^{(1, n-1)}\), and clearly the case 1) in the assertion of the proposition holds.

2) Let us assume that \(\rho^{(1, n-1)}\pi^{(1, n-1)}(L)\) fixes a complete subspace of dimension 0 (i.e., a point) of the \(\mathcal{P}(n-2, q)\). Choosing a suitable conjugate \(L^x\) of \(L\), we have

\[ L^x \subseteq \{ x; x \in SL(n, q), x = \begin{pmatrix} \star & 0 & \cdots & 0 \\ \star & \star & \cdots & \vdots \\ \star & \star & \cdots & \star \\ \star & \star & \cdots & \star \end{pmatrix} n-2 \}. \]

Since \(L^x \subseteq G^{(2, n-2)}\), from Proposition 2.3, a conjugate of \(L^x\) is equal to the subgroup \(M_\mu\).

3) Let us assume that \(\rho^{(1, n-1)}\pi^{(1, n-1)}(L)\) fixes a complete subspace of dimension \(n-3\) (i.e., a hyperplane) of the \(\mathcal{P}(n-2, q)\). Choosing a suitable conjugate \(L^x\) of \(L\), we have
Now let us use the following notation:

\[ L^* \subseteq \{ x; \ x \in SL(n, q), \ x = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & I_{n-2} & \cdots & 0 \\ 0 & 0 & \cdots & 1 \end{pmatrix} \} \]

Then \( J = UV \cup U \) and \( U \cap V = 1 \). We denote by \( \tau \) the natural homomorphism \( J \to V \). Since \( |M_2; L^*| \) is a divisor of \( q \) and less than \( q \), \( |J; \pi^{(1, n-1)}(L^*)| \) and \( |V; \tau \cdot \pi^{(1, n-1)}(L^*)| \) must also be a divisor of \( q \) and less than \( q \). Therefore, by Propositions 1.8, 1.10 and 1.12, \( \tau \cdot \pi^{(1, n-1)}(L^*) = V \), because of \( (q, q) = 1 \). Moreover a similar argument as in the proof of Proposition 2.2 shows that \( J = \pi^{(1, n-1)}(L^*) \) and that \( L = \pi^{(1, n-1)} J = M_4 \). Hence the assertion of the proposition is completely proved.

A similar argument as in Proposition 2.4 proves the following

**Proposition 2.5.** Let \( n \geq 4 \). If \( L \) is contained in \( G^{(n-1, 1)} \), then one of the following cases occurs:

1) \( u = |G^{(n-1, 1)}; L| \) is a divisor of \( (q-1)(q-1, n-1)/(q-1, n) \) and is more than 1.

2) \( L \) is conjugate to

\[ M_4 = \{ x; x \in SL(n, q), x = \begin{pmatrix} \ast & 0 & \cdots & 0 \\ 0 & \ast & \cdots & 0 \\ \ast & \ast & \cdots & \ast \end{pmatrix} \} \]

3) \( L \) is conjugate to \( M_4, \mu = q \).

3. **Proof of Theorem 1 for the case \( n \geq 5 \)**

In this section we always assume that \( q = 2^k \) and that \( n \geq 5 \).

As we have seen in Proposition 2.1, we may assume that a conjugate of \( L \) is contained in either \( G^{(1, n-1)} \), \( G^{(3, n-2)} \), \( G^{(n-2, 2)} \) or \( G^{(n-1, 1)} \). In the first place we assume that a conjugate of \( L \) is contained in either in \( G^{(1, n-1)} \) or \( G^{(3, n-2)} \).
From Propositions 2.2 and 2.4, one of the following cases occurs:

**Case 1.** $u(=l/k)$ is a divisor of $(q-1)(q-1, n-1)/(q-1, n)$ and is more than 1.

**Case 2.** $L$ is conjugate to the subgroup $G^{2,n-2}$, $\mu=q(q+1)$.

**Case 3.** $L$ is conjugate to the subgroup $M_1$, $\mu=q$.

**Case 4.** $L$ is conjugate to the subgroup $M_2$, $\mu=q$.

**Case 5.** $L$ is conjugate to the subgroup $M_3$, $\mu=2$.

**Case 6.** $L$ is conjugate to the subgroup $M_4$, $\mu=2^{(f/2)}=\sqrt{q}$ (for $f$ even).

Now we will show that the above 6 cases are all impossible.

Firstly, let us recall some elementary properties concerning involutions (elements of order 2) in $PSL(2, 2^f)$.

Let us set

\[
\tau_j = \begin{pmatrix}
1 & 1 \\
0 & 1 \\
\vdots & \vdots \\
0 & \vdots \\
1 & 0 \\
1 & 0 \\
\end{pmatrix}
\text{j blocks}
\begin{pmatrix}
1 & 1 \\
0 & 1 \\
\vdots & \vdots \\
0 & \vdots \\
1 & 0 \\
1 & 0 \\
\end{pmatrix}
\begin{pmatrix}
j=1, \ldots, \left[\frac{n}{2}\right].
\end{pmatrix}
\]

Then every involution of $PSL(n, 2^f)$ is conjugate to some $\tau_j(j=1, 2, \ldots, \left[\frac{n}{2}\right])$, and that $\tau_i$ and $\tau_j$ are not conjugate to each other if $i \neq j$. The number of element of $PSL(n, q)$ which are conjugate to $\tau_i$ is $(q^n-1)(q^n-1)/(q-1)$.

Let us denote by $\psi_1$ the permutation character of the permutation group $(\mathbb{S}_n, \Delta(a))$ and by $\psi_2$ the permutation character of $(\mathbb{S}_n, \Gamma(a))$. Clearly we have $\psi_1(\tau_j)=q^{n-j-1}+\cdots+1$, and so $\psi_1(\tau_i) > \psi_1(\tau_j)$ for every $j=2, \ldots, \left[\frac{n}{2}\right]$.

**Proposition 3.1.** The case 1 does not hold.

Proof. If $n$ is sufficiently large, $d=\frac{k^2+(4u^2-4u-2)k+4u+1}{u^3}$ is not a square, because $(k+(2u^2-2u-1))^2>k^2+(4u^2-4u-2)k+4u+1>(k+(2u^2-2u-1)-1)^2$ for $u>2$ and in this case $u$ is never equal to 2, and it contradicts Proposition 1.4. For small values of $n$, we can practically derive a contradiction to Proposition 1.4.

**Proposition 3.2.** The case 2 does not hold.

Proof. Let $q=2$. Then $\mu=6$ and $d=8(2^n-1)\cdots+2^3+3)$ is not a square, and it contradicts Proposition 1.4. Let $q\neq2$. Then $\mu=q(q+1)$, and if $n$ is sufficiently large, $\alpha=\frac{u^2(\mu-4)(\mu-2)(\mu-6)}{4k+\mu^2-4\mu}$ is clearly not an integer, hence $d$
is not an integer by Proposition 1.5, and this contradicts Proposition 1.4. For small values of \( n \), we can practically derive a contradiction to Proposition 1.4, by computing the value \( \alpha \).

**Remark.** An alternative proof of Proposition 3.2 is also possible, which banishes the troublesome calculations in the case of small \( n \). That is to say, under the assumptions of Proposition 3.2, \((\mathfrak{G}, \Gamma(\alpha)) \cong PSL(n, q)\) acting on the set of lines of the projective space \( P \). Thus \((\mathfrak{G}, \Gamma(\alpha))\) is primitive and rank 3, and the subdegrees are 1, \( q\Omega_{2}Q_{n-2}^{|\mathfrak{G}_{n-3}/Q_{2}|} \), where \( Q_{j} = (q^{j} - 1)/(q - 1) \). Thus the stabilizer of a point of the permutation group \((\mathfrak{G}, \Gamma(\alpha))\) has no union of orbits whose total length is \( k - \mu \), and this is a contradiction. (Cf. D. Wales, Uniqueness of the graph of a rank three group, Pacific J. of Math. 30 (1969), 271–276, Theorem 1. This assertion is immediate from the existence of an element \( g \in \mathfrak{G} \) interchanging \( a \) and \( d \in \Gamma(\alpha) \).)

**Proposition 3.3.** The case 3 does not hold.

**Proof.** Let \( q \neq 2 \) and \( q \neq 4 \). Then \( \mu = q \) and \( \alpha = \mu^{2}(\mu - 4)^{2}(\mu - 2)^{2}(\mu - 6)^{2} \)

\[ 4k + \mu^{2} - 4\mu 

is never an integer for \( n \geq 7 \), and so \( d \) is never an integer and it contradicts Proposition 1.4. For \( n \leq 6 \), we can also derive a contradiction to Proposition 1.4 by actually computing the value \( \alpha \). Let \( q = 4 \). Then we can regard \((\mathfrak{G}, \Gamma(\alpha)) \cong (PSL(n, q), PSL(n, q)/M)\) as the group of permutations of \( \mathfrak{G}(\cong PSL(n, q)) \) on the set of incident point-line pairs in the projective space \( \mathcal{P}(n-1, q) \). Noting that the involution \( \tau_{1} \) is an elation, we immediately have that \( \psi_{s}(\tau_{1}) = (q^{*2} + \cdots + q + 1)(q^{*3} + \cdots + q + 1) + q^{*1} \). As is easily verified, \( \psi_{s}(\tau_{1}) > \psi_{s}(\tau_{j}) \) for every \( j = 2, \ldots, \left[ \frac{n}{2} \right] \). Let us denote by \( \psi \) the permutation character of \((\mathfrak{G}, \Omega) \). Then \( \psi = 1 + \psi_{1} + \psi_{2} \) on \( \mathfrak{G} \). Since \( \psi(\tau_{1}) > \psi(\tau_{j}) \) for every \( j = 2, \ldots, \left[ \frac{n}{2} \right] \), every element of \( \mathfrak{G} \), which is conjugate to \( \tau_{1} \) in \( \mathfrak{G} \) is already conjugate to \( \tau_{1} \) in \( \mathfrak{G}_{n} \), and there exist \((q^{*1} - 1)(q^{*1} - 1)/(q - 1) \) such elements. Hence, the number \( \beta \) of element of \( \mathfrak{G} \) which are conjugate to \( \tau_{1} \) is given as follows (cf. [1]):

\[ \beta = \frac{\psi(1)(q^{*1} - 1)(q^{*1} - 1)}{\psi(\tau_{1})} = \frac{64X^{2} + 28X + 7}{4X^{2} + 16X + 7}, \text{ where } X = 4^{n-2}. \]

But we can easily show that the \( \beta \) is not an integer, and this is a contradiction. To be more precise, the G.C.D. of \( 64X^{2} + 28X + 7 \) and \( 4X^{2} + 16X + 7 \) divides \(-228X - 105 \), and the G.C.D. of \( 64X^{2} - 20X + 1 \) and \( 4X^{2} + 16X + 7 \) divides \((-92X - 37) \cdot 3 \). Thus in order to \( \beta \) being an integer, \((-228X - 105)(-92X - 37) \)

\[ \frac{4X^{2} + 16X + 7} \]
must also be an integer. Since the G.C.D. of \((-228X-105)(-92X-37)\) and 
\(4X^2+16X+7\) divides \(65808X+32823\), we can conclude that 
\(4X^2+16X+7\) must be also an integer. But we can easily show that this is impossible for any 
\(X=4^{n-2}\). This kind of argument will be used repeatedly in the following

REMARK. An alternative proof of Proposition 3.2 for the case \(q=4\) is also possible. This is done by making use of the following Propositions A and B.

**Proposition A** (W. Ljunggren). The diophantine equation \(\frac{x^n-1}{x-1}=y^p, n>2, |x|, |y| > 1\), has no integral solution except for the two cases (i) \(n=4, x=7\), and
(ii) \(n=5, x=3\).

(For the proof see W. Ljunggren, Noen setninger om ubestemte linkninger av formen \(\frac{x^n-1}{x-1}=y^p\) (Norwegian), Norsk Math. Tidsskr. 25 (1943), 17–20.
Cf. Math. Review Vol. 8, 315.)

From Proposition A we immediately have the following

**Proposition B.** \(\mu=2\) and \(\mu=4\) are impossible.

Because if \(\mu=2\) then \(d=4k-4=4q\cdot\frac{q^n-1}{q-1}\) is not a square, and if \(\mu=4\) then \(d=4k-4\cdot\frac{q^n-1}{q-1}\) is not a square, for \(q\) a power of 2.

From Proposition B the assertion of Proposition 3.2 for the case \(q=4\) is clear.

(Moreover, Proposition A gives an affirmative answer to the question left open in S. Montague [8], page 519 lines 21–30.)

**Proposition 3.4.** The case 4 does not hold.

Proof. Let \(q\neq4\). Then \(\mu=q\), and this is a contradiction as we have seen in the proof of Proposition 3.3. Let \(q=4^\alpha\). Then we can regard \((\mathfrak{S}_a, \Gamma(a)) (\cong (PSL(n, q), PSL(n, q)/M_4))\) as the group of permutations of \(\mathfrak{S}_a (\cong PSL(n, q))\) on the set of incident point-hyperplane pairs of the projective space \(\mathcal{P}(n-1, q)\). Moreover we have

\[\varphi_2(\tau)= (q^{n-2}+\cdots+1)^2+ (q^{n-2}+\cdots+q)(q^{n-2}+\cdots+q+1) \geq \varphi_2(\tau)\]

for every

4) Proposition B in Remark following Proposition 3.3 gives an alternative (calculation free) proof of this assertion.
70 E. BANNAI

\[ j = 2, \ldots, \left[ \frac{n}{2} \right], \text{ and } \psi(\tau_i) \neq \psi(\tau_j) \text{ for every } j = 2, \ldots, \left[ \frac{n}{2} \right]. \] Hence the number \( \beta \) of elements of \( \mathcal{G} \) which are conjugate to \( \tau_i \) is given as follows:

\[
\beta = \frac{\psi(1)(q^n - 1)(q^{n-1} - 1)}{\psi(\tau_i)} = \frac{64X^2 + 28X + 7 \cdot 64X^2 - 20X + 1}{20X^2 - 4X + 11}, \text{ where } X = 4^{n-2}.
\]

But we can easily show that the \( \beta \) is never an integer, and this is a contradiction.

**Proposition 3.5**. *The case 5 does not hold.*

Proof. \( \mu = 2 \). Thus the assertion is clear from Proposition B in Remark following Proposition 3.3. (In the original manuscript, the author proved Proposition 3.5 by showing that the number of elements of \( \mathcal{G} \) which are conjugate to the element \( \tau_i \) is not an integer, as in the proof of Proposition 3.3.)

**Proposition 3.6**. *The case 6 does not hold.*

Proof. Let \( q \neq 16 \). (Note that \( q \neq 4 \), since otherwise \( \mu = 2 \) and this is a contradiction as we have already seen.) Then \( \mu = \sqrt[4]{q} \), and \( \alpha = q\sqrt{(q-4)^4(q-2)^2(q-6)^2} \) is not an integer, hence \( \alpha \) is not an integer and this contradicts Proposition 1.4. Let \( q = 16 \). Then \( \mu = 4 \) and the assertion is clear from Proposition B in Remark following Proposition 3.3. (In the original manuscript, the author proved Proposition 3.6 by showing that the number of elements of \( \mathcal{G} \) which are conjugate to the element \( \tau_i \) is not an integer, as in the proof of Proposition 3.3.)

Thus, we have verified from Propositions 3.1–3.6 that if \( n \geq 5 \) and a conjugate of \( L \) is contained in \( G^{(n-1,n-1)} \) or \( G^{(n,n-2)} \), then the permutation group \((PSL(n, q), P)\) has no primitive extension of rank 3. A similar argument as above shows that if \( n \geq 5 \) and a conjugate of \( L \) is contained in \( G^{(n-2,n)} \) or \( G^{(n-1,1)} \), then the \((PSL(n, q), P)\) has no primitive extension of rank 3. Thus we completed the proof of Theorem 1 for the case \( n \geq 5 \).

4. Proof of Theorem 1 for the case \( n \leq 4 \)

A) The case \( n = 2 \).

**Proposition 4.1**. \((PSL(2, 2), P)\) has a unique primitive extension of rank 3 of degree 10, and this is isomorphic to \( A_5 \) acting on the set of unordered pairs of

5) This is already proved in [8], page 519.
the 10 points.

**Proposition 4.2.** \((\text{PSL}(2, 4), P)\) has a unique primitive extension of rank 3 of degree 16, and this contains a regular normal subgroup of order 16.

Proof of above two propositions are easy, and so we omit the proof. (Here, note that \(\text{PSL}(2, 2)\)\(^{\text{symmetric group on 3 letters}}\), \(\text{PSL}(2, 4)\)\(^{\text{alternating group on 5 letters}}\). Cf. T. Tsuzuku [11] and S. Iwasaki [7].)

**Proposition 4.3.** Let \(f \geq 3\). Then \((\text{PSL}(2, 2^f), P)\) has no primitive extension of rank 3.

Proof. By Proposition 1.10, \(L\) must be conjugate to either \(B\) or \(D_{f/2}\) (for \(f\) even). Let \(L\) be conjugate to \(B\). Since \(d=2f\), \(f\) must be even. The number \(\beta\) of elements of \(g\) which are conjugate to \(\tau_1\) is given as follows:

\[
\beta = \frac{1 + 2^{f-1}}{1 + 1 + 2^{f-1}} + 1 + 2^{f-1}(2^f - 1)(2^{2f} - 1).
\]

But \(\beta\) is not an integer for \(f\) even unless \(f = 4\). The case \(f = 4\) is also impossible, because there exist no natural integers \(f_1\) and \(f_2\) such that \((1+k+l) \cdot \frac{kl}{f_1 f_2}\) is a square, and it contradicts the theorem of J. S. Frame [13, Theorem 30.1]. Now let \(L\) be conjugate to \(D_{f/2}\). Then \(l = 2^{f} / (2f + 1)\) and \(\mu = 2^{f/2} \geq 4\) because \(f\) = even and \(\geq 3\), and \(\alpha = \mu^2 (\mu - 4)^2 (\mu - 2)^2 (\mu - 6)^2\) is not an integer and so is \(d\), and it contradicts Proposition 1.4.

B) The case \(n = 3\).

**Proposition 4.4.** \((\text{PSL}(3, 2^f), P)\) has no primitive extension of rank 3 for any \(f\).

Proof. From Proposition 1.12, a conjugate of \(L\) is contained in \(G^{(1,2)}\) or \(G^{(2,1)}\). First let us assume \(q = 2\) and let \(L \subseteq G^{(1,2)}\). Then \(|1 \times \text{PGL}(2, 2^f)| \rho^{(1,2)}\) \(\pi^{(1,2)}(L)|\) must be a divisor of \(q(q+1)\) and less than \(q(q+1)\). Hence, from Proposition 1.10, we have that \(\rho^{(1,2)} \pi^{(1,2)} (L)\) is conjugate to one of the subgroups \(1 \times A\), \(1 \times B\) or \(1 \times D_{f/2}\) (for \(f\) even \(\geq 4\)). The same argument as in the previous sections shows that in every above case \(L \supseteq P^{(2)}\) and \(L\) is conjugate to one of the subgroups \(M_1\), \(M_2\) or \(M_3\). If \(L\) is conjugate to \(M_1\), then \(\mu = q\) and \(\alpha = q^2 (q-4)^2 (q-2)^2 (q-6)^2\), and we can derive a contradiction to Proposition 1.4.

If \(L\) is conjugate to \(M_2\), then \(d = 4(2^f + 2^f) = 4 \cdot 2^f (2^f + 1)\) is not a square, and this is a contradiction. If \(L\) is conjugate to \(M_3\), then \(\mu = \sqrt{q}\) and \(d = 4q^2 + 5q - 4\sqrt{q} + 1\) is never a square since \((2q + 1)^2 < d < (2q + 2)^2\), and this is also a
contradiction. If $q \neq 2$ and $L \subseteq G^{(1,2)}$, then we can easily get the same conclusion. Finally let us assume $q=2$. Then $k=7$ and the theorem of Frame [13, Theorem 30.1] shows that $l=k(k-1)=42$. But this is impossible as was already verified in D. G. Higman [5]. Thus we completed the proof of the proposition.

C) The case $n=4$.

**Proposition 4.5.** $(PSL(4, 2^2), P)$ has no primitive extension of rank 3.

Proof. By Proposition 2.1, a conjugate of $L$ is contained in either $G^{(1,2)}$, $G^{(2,2)}$ or $G^{(3,1)}$. First let us assume that a conjugate of $L$ is contained in $G^{(1,2)}$. From Proposition 2.4, one of the three cases (1)~(3) in Proposition 2.4 holds. However, we can easily prove, using a similar method as in § 3, that these three cases are all impossible. If a conjugate of $L$ is contained in $G^{(3,1)}$, then we have the same conclusion, i.e., this case is also impossible. Now, let us assume that a conjugate $L'$ of $L$ is contained in $G^{(2,2)}$. Then $\rho^{(2,2); \tau^{(2,2)}}(L') \cap PGL(2, 2') \times PGL(2, 2') \times PGL(2, 2') \times PGL(2, 2') \times A)$, $B \times PGL(2, 2') \times PGL(2, 2') \times B)$, $D_{27} \times PGL(2, 2') \times PGL(2, 2') \times D_{27}$, or $Z_3 \times PGL(2, 2) \times Z_3$. As in Proposition 2.3, $L$ is conjugate to either $C^{(3,2)}, (M_1)$, $M_2(M_2)$ or $M_3(M_3)$. A similar argument as in § 3 shows that these cases are all impossible. Thus the proof of the proposition is completed.

Thus, Theorem 1 is completely proved.

---

**References**


