Glasgow Math. J. **55** (2013) 581–590. © Glasgow Mathematical Journal Trust 2013.
doi:10.1017/S0017089512000766.

SUBGROUP PERMUTABILITY DEGREE OF $PSL(2, p^n)$

F. SAEEDI
Department of Mathematics, Mashhad Branch, Islamic Azad University, Mashhad, Iran
e-mail: saeedi@mshdiau.ac.ir

and M. FARROKHI D. G.
Department of Pure Mathematics, Ferdowsi University of Mashhad, Mashhad, Iran
e-mail: m.farrokhi.d.g@gmail.com

(Received 3 April 2012; accepted 25 July 2012; first published online 26 February 2013)

Abstract. We will compute the subgroup permutability degree of the projective special linear groups $PSL(2, p^n)$.

2000 *Mathematics Subject Classification.* Primary 20P05; Secondary 20G40, 12E20, 12F99, 12Y05.

1. Introduction. Probabilistic group theory is one of the oldest areas in group theory. It has been the centre of attention to many authors and it is studied in many directions. Among various kinds of probabilities defined to date, one can refer to the work of Gustafson [**6**] who initiated studying the commutativity degree of elements of a finite group. This concept can be generalized and modified in many directions. Two subgroups H and K of G permutes if $HK = KH$. Hence, by changing the role of elements to subgroups in a finite group, one can obtain a modification of the commutativity degree of a finite group.

Let $L(G)$ be the lattice of all subgroups of G. Then, the *subgroup permutability degree* of G is the proportion of the number of all ordered pairs (H, K) of subgroups of G by $|L(G)|^2$. In other words,

$$spd(G) = \frac{|\{(H, K) \in L(G) \times L(G) : HK = KH\}|}{|L(G)|^2}.$$

Tărnăuceanu in [**10**] introduces the subgroup permutability degree of a finite group and computes it for some classes of finite groups, namely dihedral groups D_{2n}, generalized quaternion 2-groups Q_{2^n}, quasi-dihedral groups QD_{2^n} ($n \geq 4$) and modular p-groups M_{p^n} ($n \geq 3$). These groups together with the abelian groups $\mathbb{Z}_{p^n} \times \mathbb{Z}_p$ present all finite p-groups, which have a cyclic maximal subgroup. In [**11**], he also gives many open problems concerning the subgroup permutability degree and its generalizations.

The subgroup permutability degree of finite groups has a close relationship to the problem of counting the number of factorizations of finite groups. We recall some terminologies. A finite group G is *factorized* if $G = AB$ for some subgroups A and B of G and this factorization is proper if A and B are proper subgroups of G. The number of all possible factorizations of G is called the *factorization number* of G and is denoted by $F_2(G)$. The factorization of groups has been the focus of much research in such a way that how the structure of a group is influenced by the structure of subgroups in a given

factorization. On the other hand, determination of all factorizations of a given finite group has been the interest of many authors, which helps to get, as a consequence, a better understanding of the factorizations. We remark that the factorizations of a large variety of finite simple groups are known and we may refer the reader to [**1**, **4**, **5**, **8**, **12**].

The subgroup permutability degree and factorization numbers are connected through the following formula:

$$spd(G) = \frac{1}{|L(G)|^2} \sum_{H \in L(G)} F_2(H). \tag{1}$$

We intend to compute the subgroup permutability degree of the finite simple groups $PSL(2, p^n)$. To end this, it is necessary to know the structure of subgroups of these groups, which is well-known and is stated in the following celebrated theorem of Dickson.

THEOREM 1.1 [**7**, Hauptsatz II.8.27]*(Dickson). Any subgroup of* $PSL(2, p^n)$ *is isomorphic to one of the following families of groups:*

(1) *Elementary abelian p-groups;*
(2) *Cyclic group of order m, where m is a divisor of* $(p^n \pm 1)/d$ *and* $d = \gcd(p-1, 2)$*;*
(3) *Dihedral group of order* $2m$*, where m is as defined in* (2)*;*
(4) *Alternating group* A_4 *if* $p > 2$*, or* $p = 2$ *and* $n \equiv 0 \pmod 2$*;*
(5) *Symmetric group* S_4 *if* $p^{2n} \equiv 1 \pmod{16}$*;*
(6) *Alternating group* A_5 *if* $p = 5$ *or* $p^{2n} \equiv 1 \pmod 5$*;*
(7) *A semi-direct product of an elementary abelian p-group of order* p^m *and a cyclic group of order k, where k is a divisor of* $p^m - 1$ *and* $p^n - 1$*;*
(8) *The group* $PSL(2, p^m)$ *if m is a divisor of n, or the group* $PGL(2, p^m)$ *if* $2m$ *is a divisor of n.*

Also, it is necessary to mention the following prominent structural result concerning the projective special linear groups over finite fields, which we will use frequently in the sequel.

THEOREM 1.2 [**7**, Satz II.8.5]. *If* $G = PSL(2, p^n)$*, then there exists subgroups* $\mathcal{H}$*,* $\mathcal{K}$ *and* $\mathcal{L}$ *of G such that*

$$G = \bigcup_{g \in G} \mathcal{H}^g \cup \bigcup_{g \in G} \mathcal{K}^g \cup \bigcup_{g \in G} \mathcal{L}^g,$$

$\mathcal{H}$ *is a Sylow p-subgroup of G, which is elementary abelian of order* p^n*,* $\mathcal{K}$ *is cyclic of order* $(p^n - 1)/d$ *and* $\mathcal{L}$ *is cyclic of order* $(p^n + 1)/d$*, where* $d = \gcd(p-1, 2)$*. Moreover* $[G : N_G(\mathcal{H})] = p^n + 1$*,* $[G : N_G(\mathcal{K})] = p^n(p^n + 1)/2$ *and* $[G : N_G(\mathcal{L})] = p^n(p^n - 1)/2$*.*

Note that in the above theorem, for $\mathcal{H}$, $\mathcal{K}$ and $\mathcal{L}$ we have $N_G(N_G(\mathcal{H})) = N_G(\mathcal{H})$, $N_G(N_G(\mathcal{K})) = N_G(\mathcal{K})$ and $N_G(N_G(\mathcal{L})) = N_G(\mathcal{L})$. In what follows, the centre of $SL(2, p^n)$ is denoted by $\mathcal{Z}$.

2. Factorization numbers of subgroups of $PSL(2, p^n)$**.** According to equation (1), to compute the subgroup permutability degree of the group $PSL(2, p^n)$, it is enough to compute the factorization number and the size of isomorphism classes of its subgroups. We first give the factorization number of all subgroups except those of type (7) in Theorem 1.1, which is computed by the authors in [**9**].

https://doi.org/10.1017/S0017089512000766 Published online by Cambridge University Press

THEOREM 2.1 [**9**]. *If $G = \mathbb{Z}_n$ is a cyclic group, then*

$$F_2(G) = \prod_{i=1}^{m}(2\alpha_i + 1),$$

where $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$.

The authors [**9**] gave the following recursive formula for the factorization number of finite elementary abelian p-groups.

$$F_2(\mathbb{Z}_p^n) = \left(\sum_{i=0}^{n} \begin{bmatrix} n \\ i \end{bmatrix}_p\right)^2 - \sum_{i=0}^{n-1} \begin{bmatrix} n \\ i \end{bmatrix}_p F_2(\mathbb{Z}_p^i),$$

where

$$\begin{bmatrix} n \\ i \end{bmatrix}_p = \frac{(p^n - 1)\cdots(p-1)}{(p^i - 1)\cdots(p-1)(p^{n-i} - 1)\cdots(p-1)}$$

is the number of subgroups of $\mathbb{Z}_p^n$ of order p^i. The number $\begin{bmatrix} n \\ i \end{bmatrix}_p$ is called a Gaussian binomial integer. Here, we will use a better formula obtained by the second author.

THEOREM 2.2 [**3**]. *If $G = \mathbb{Z}_p^n$ is an elementary abelian p-group, then*

$$F_2(G) = \sum_{0 \le i+j \le n} p^{ij} \begin{bmatrix} n \\ i, j \end{bmatrix}_p,$$

where

$$\begin{bmatrix} n \\ i, j \end{bmatrix}_p = \frac{(p^n - 1)\cdots(p-1)}{(p^i - 1)\cdots(p-1)(p^j - 1)\cdots(p-1)(p^{n-i-j} - 1)\cdots(p-1)}$$

is a Gaussian trinomial integer.

THEOREM 2.3 [**9**]. *Let $G = D_{2n}$ be a dihedral group. Then,*

$$F_2(G) = \begin{cases} \phi_n + 2\delta_n, & n \text{ odd}, \\ \phi_n + 2\phi_{\frac{n}{2}} + 2\delta_n, & n \text{ even}, \end{cases}$$

where

$$\phi_n = \prod_{i=1}^{m}\left(2\frac{p_i^{\alpha_i+1} - 1}{p_i - 1} - 1\right)$$

and

$$\delta_n = \prod_{i=1}^{m}\left(\alpha_i + \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}\right)$$

for $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$.

https://doi.org/10.1017/S0017089512000766 Published online by Cambridge University Press

THEOREM 2.4 [**9**]. *Let $G = PSL(2, p^n)$ be a projective special linear group. Then,*

$$F_2(G) = \begin{cases} 2|L(G)| + 2p^n(p^{2n} - 1) - 1, & p = 2, n > 1, \\ 2|L(G)| + p^n(p^{2n} - 1) - 1, & p > 2 \text{ and } (p^n - 1)/2 \text{ is odd}, \\ & p^n \neq 3, 7, 11, 19, 23, 59, \\ 2|L(G)| - 1, & p > 2 \text{ and } (p^n - 1)/2 \text{ is even}, \\ & p^n \neq 5, 9, 29 \end{cases}$$

and

$$F_2(G) = 17, 27, 237, 1141, 2033, 4935, 17223, 48261, 68799, 780695$$

if

$$p^n = 2, 3, 5, 7, 9, 11, 19, 23, 29, 59,$$

respectively.

THEOREM 2.5 [**9**]. *Let $G = PGL(2, p^n)$ $(p > 2)$ be a projective general linear group and M be the unique subgroup of G isomorphic to $PSL(2, p^n)$. Then,*

$$F_2(G) = \begin{cases} 3p^n(p^{2n} - 1) + 4|L(G)| - 2|L(M)| - 3, & n \text{ even or } p \equiv 1 \pmod 4, \\ 4p^n(p^{2n} - 1) + 4|L(G)| - 2|L(M)| - 3, & n \text{ odd and } p \equiv 3 \pmod 4 \end{cases}$$

if $p^n > 29$ and

$$F_2(G) = 177, 1103, 3083, 4919, 15549, 14529, 31093, 58429, 111567, 99527, 144297, 192349$$

if

$$p^n = 3, 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29,$$

respectively.

In the remainder of this section, we shall compute the factorization number of subgroups of type (7) in Theorem 1.1. To prove Theorem 2.6, we need to fix some notations. Let F be a field and $E \subseteq F$. Then, the subfield generated by E is denoted by (E), and we use E^+ and $E^\times$ for an additive and multiplicative subgroup of E, respectively. Also, the notations $E \leq F$, $E^+ \leq F^+$ and $E^\times \leq F^\times$ indicate that E is a subfield of F, E is an additive subgroup of F and E is a multiplicative subgroup of F, respectively. For a subgroup H of $\mathcal{H}$ and a subgroup K of $\mathcal{K}$, the associated additive and multiplicative subgroups E_H^+ and $E_H^\times$ of H and K of $F = GF(p^n)$ are defined as follows, respectively,

$$E_H^+ = \left\{ x \in F : \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \mathcal{Z} \in H \right\}$$

and

$$E_K^\times = \left\{ y \in F : \begin{bmatrix} y & 0 \\ 0 & y^{-1} \end{bmatrix} \mathcal{Z} \in K \right\}.$$

https://doi.org/10.1017/S0017089512000766 Published online by Cambridge University Press

A vector space V over a field E is denoted by V/E. Moreover, if $U \subseteq V$ and $E \leq F$ is a subfield of F, then $U/E \leq V/E$ indicates that U is a subspace of V as vector spaces over E.

The following numbers will be used in the next theorem.

$$\Xi_n(V, F; E_1, E_2) = \sum_{\substack{V=U_1+U_2 \\ U_1/E_1 \leq V/E_1 \\ U_2/E_2 \leq V/E_2}} \left(\frac{|V|}{|U_1|} \cdot \frac{|V|}{|U_2|} \right)^n = \sum_{\substack{V=U_1+U_2 \\ U_1/E_1 \leq V/E_1 \\ U_2/E_2 \leq V/E_2}} \frac{|V|^n}{|U_1 \cap U_2|^n},$$

where V is a vector space over the field F and E_1, E_2 are subfields of F.

THEOREM 2.6. *Let $S = H \rtimes K$ be a subgroup of $PSL(2, p^n)$, where H is an elementary abelian p-group of order p^m and K is a cyclic group whose order divides $p^m - 1$ and $p^n - 1$. Then,*

$$F_2(S) = \sum_{K=XY} \Xi_1\big(H, \big(E_K^{\times 2}\big); \big(E_X^{\times 2}\big), \big(E_Y^{\times 2}\big)\big).$$

Proof. Since S is a subgroup of $PSL(2, p^n)$, its subgroups can be determined via Theorem 1.1. Clearly, S has no subgroups of the form A_5 and a nontrivial special or general linear group as it is solvable. Suppose that S has a non-abelian dihedral subgroup X. Then, $X = \langle x \rangle \rtimes \langle y \rangle$ and $x \notin H$ for x is not a p-element. Hence, $x \in K^h$ for some $h \in H$. Since S/H is abelian we have $[x, y] \in H$. On the other hand, $[x, y] \in K^h$, which implies that $[x, y] = 1$ is a contradiction. If S has an alternating subgroup X of degree four, then $X' \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \leq H$. In particular, $p = 2$ and X is a group of type (7) of Theorem 1.1. Also, if S has a symmetric subgroup X of degree four, then it has the dihedral group of order eight as its subgroup, which contradicts our previous result. Hence, a subgroup of S is an elementary abelian p-group, a cyclic group or a group of type (7) in Theorem 1.1.

Let A and B be subgroups of S. Then, $A = U \rtimes X^{h_1}$ and $B = V \rtimes Y^{h_2}$, where $U \leq H$ is elementary abelian of order p^u $(u \geq 0)$, $V \leq H$ is elementary abelian of order p^v $(v \geq 0)$, $X \leq K$ is cyclic with order dividing $\gcd(p^u - 1, p^n - 1)$, $Y \leq K$ is cyclic with order dividing $\gcd(p^v - 1, p^n - 1)$ and $h_1, h_2 \in H$.

If $S = AB$, then an arbitrary element hk of S can be written in the form $ux^{h_1}vy^{h_2}$, where $h \in H, k \in K, u \in U, v \in V, x \in X$ and $y \in Y$. From the equality $hk = ux^{h_1}vy^{h_2}$, it follows that

$$ky^{-1}x^{-1} = h^{-1}uv\tilde{h}[\tilde{h}, x^{-h_1}][h_1, x^{-1}] \in H \cap K = 1,$$

where $\tilde{h} = [h_2, y^{-1}]$. Hence, $H = UV$ and $K = XY$. A simple verification shows that these latter conditions are also sufficient to assure that $S = AB$. Hence, the number of factorizations of S equals the number of simultaneous factorizations $H = UV$ and $K = XY$, where U, V, X and Y satisfy the aforementioned properties. We shall count such factorizations.

By Theorem 1.2, we may assume without loss of generality that $H \subseteq \mathcal{H}$ and $K \subseteq \mathcal{K}$. If $H_0 \leq H$ and $K_0 \leq K$, then

$$H_0 = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \mathcal{Z} : x \in E_{H_0}^+ \right\} \text{ and } K_0 = \left\{ \begin{bmatrix} y & 0 \\ 0 & y^{-1} \end{bmatrix} \mathcal{Z} : x \in E_{K_0}^\times \right\},$$

https://doi.org/10.1017/S0017089512000766 Published online by Cambridge University Press

where $E^+_{H_0} \leq F^+$ is an additive subgroup of F and $E^\times_{K_0} \leq F^\times$ is a multiplicative subgroup of F. Moreover, a simple verification shows that $K_0 \leq N_G(H_0)$ if and only if $E^+_{H_0} = E^+_{H_0}E^{\times 2}_{K_0}$ if and only if $E^+_{H_0} = E^+_{H_0}(E^{\times 2}_{K_0})$ or equivalently $E^+_{H_0}$ is a vector space over the field $(E^{\times 2}_{K_0})$, where $E^{\times 2}_{K_0}$ denotes the group of all squares of $E^\times_{K_0}$.

Now, we construct all the factorization of the group S. Let $K = XY$ be an arbitrary factorization of K into subgroups X and Y. Then, $H = UV$ is a factorization of H into subgroups U and V such that $X \subseteq N_G(U)$ and $Y \subseteq N_G(V)$ if and only if $E^+_H = E^+_U + E^+_V$ and

$$E^+_U \Big/ (E^{\times 2}_X) \leq E^+_H \Big/ (E^{\times 2}_X) \quad \text{and} \quad E^+_V \Big/ (E^{\times 2}_Y) \leq E^+_H \Big/ (E^{\times 2}_Y).$$

On the other hand, the subgroups U and V together with conjugates of X and Y contribute $[H : U]$ and $[H : V]$ distinct subgroups of the form $U \rtimes X^{h_1}$ and $V \rtimes Y^{h_2}$ $(h_1, h_2 \in H)$ giving rise to a factorization of S, respectively. Therefore, the number of factorizations of S is

$$F_2(S) = \sum_{K=XY} \Xi_1\big(H, (E^{\times 2}_K); (E^{\times 2}_X), (E^{\times 2}_Y)\big).$$

The proof is complete. □

3. The size of isomorphism classes of subgroups of $PSL(2, p^n)$. In this section, we shall compute the size of isomorphism classes of subgroups of $G = PSL(2, p^n)$, which enables us to calculate the subgroup permutability degree of G. If S is a subgroup of G, then the size of isomorphism class of subgroups of G with representative S is denoted by $\mathcal{N}_S$. As in the previous section, the size of isomorphism classes of all subgroups of G except those of type (7) in Theorem 1.1 is known. Hence, we compute the size of isomorphism class of subgroups of type (7) in Theorem 1.1.

LEMMA 3.1. *If $S = H \rtimes K$ is a subgroup of $PSL(2, p^n)$, where H is an elementary abelian p-group of order p^m and K is a cyclic group whose order divides $p^m - 1$ and $p^n - 1$, then*

$$\mathcal{N}_S = p^n(p^n + 1)\frac{1}{p^{m_K}l}\binom{\frac{n}{m_K}}{l}_{p^{m_K}},$$

where $p^{m_K} = |(E^\times_K)|$ and $m = m_K l$.

Proof. Without loss of generality, we assume that $H \leq \mathcal{H}$ and $K \leq \mathcal{K}$. Let $\mathcal{H}_K$ be a minimal K-invariant subgroup of $\mathcal{H}$ and let $|\mathcal{H}_K| = p^{m_K}$. We show that $Y = \{\mathcal{H}^g_K : g \in \mathcal{K}\}$ forms a partition for $\mathcal{H}$. Clearly, the elements of Y are pairwise disjoint by minimality of $\mathcal{H}_K$. On the other hand, the number of conjugates of $\mathcal{H}_K$ under conjugation by $\mathcal{K}$ equals $|\mathcal{K}|/|C| = (p^n - 1)/d|C|$, in which $C \leq \mathcal{K}$ and $N_G(\mathcal{H}_K) = \mathcal{H}C$. Then, $C \supseteq K$ and $|C|$ divide $p^{m_K} - 1$. Hence,

$$p^n = |\mathcal{H}| \geq \left|\bigcup_{g\in\mathcal{K}} \mathcal{H}^g_K\right| = 1 + \frac{p^n - 1}{d|C|} \cdot (p^{m_K} - 1),$$

https://doi.org/10.1017/S0017089512000766 Published online by Cambridge University Press

which holds only if $|C| = (p^{m_K} - 1)/d$ and Y forms a partition for $\mathcal{H}$. In particular, $E_C = (E_K^{\times})^{\times d}$ and H is a disjoint union of some subgroups in Y. It is easy to see that $|H| = p^{m_K l}$ for some $l \geq 1$.

A subset $\{\mathcal{H}_K^{g_1}, \ldots, \mathcal{H}_K^{g_i}\}$ of X is said to be independent if $|\mathcal{H}_K^{g_1} \ldots \mathcal{H}_K^{g_i}| = p^{m_K i}$. Let I_X and I_Y be the set of all l-element independent subsets of X and Y, where X is the set of all subgroups in Y contained in H. It is easy to see that

$$|I_X| = \prod_{i=0}^{l-1} \left(\frac{p^{m_K l} - 1}{p^{m_K} - 1} - \frac{p^{m_K i} - 1}{p^{m_K} - 1} \right)$$

and

$$|I_Y| = \prod_{i=0}^{l-1} \left(\frac{p^{n} - 1}{p^{m_K} - 1} - \frac{p^{m_K i} - 1}{p^{m_K} - 1} \right).$$

Hence, the number of K-invariant subgroups of $\mathcal{H}$ of order $p^{m_K l}$ equals

$$\begin{aligned}
\frac{|I_Y|}{|I_X|} &= \frac{(p^n - 1)(p^n - p^{m_K}) \cdots (p^n - p^{m_K(l-1)})}{(p^{m_K l} - 1)(p^{m_K l} - p^{m_K}) \cdots (p^{m_K l} - p^{m_K(l-1)})} \\
&= \frac{(p^n - 1)(p^{n-m_K} - 1) \cdots (p^{n-m_K(l-1)} - 1)}{(p^{m_K l} - 1)(p^{m_K(l-1)} - 1) \cdots (p^{m_K} - 1)} \\
&= \frac{((p^{m_K})^{\frac{n}{m_K}} - 1)((p^{m_K})^{\frac{n}{m_K}-1} - 1) \cdots ((p^{m_K})^{\frac{n}{m_K}-l+1} - 1)}{((p^{m_K})^{l} - 1)((p^{m_K})^{l-1} - 1) \cdots (p^{m_K} - 1)} \\
&= \frac{((p^{m_K})^{\frac{n}{m_K}} - 1) \cdots ((p^{m_K}) - 1)}{((p^{m_K})^{l} - 1) \cdots ((p^{m_K}) - 1)((p^{m_K})^{\frac{n}{m_K}-l} - 1) \cdots (p^{m_K} - 1)}.
\end{aligned}$$

Thus,

$$\frac{|I_Y|}{|I_X|} = \binom{\frac{n}{m_K}}{l}_{p^{m_K}}.$$

Finally, since $[G : N_G(\mathcal{H})] = p^n + 1$, $[\mathcal{HK} : N_{\mathcal{HK}}(\mathcal{K})] = p^n$ and $[G : N_{\mathcal{HK}}(\mathcal{K})] = p^n(p^n + 1)/2$, the subgroup K lies in the normalizer of two different conjugates of $\mathcal{H}$. Therefore,

$$\begin{aligned}
\mathcal{N}_S &= \frac{|\{(A, B) : A \cong H, B \cong K, B \leq N_G(A)\}|}{[S : N_S(K)]} \\
&= \frac{[G : N_G(K)] \cdot 2 \cdot \binom{\frac{n}{m_K}}{l}_{p^{m_K}}}{|H|} \\
&= \frac{\frac{p^n(p^n+1)}{2} \cdot 2 \cdot \binom{\frac{n}{m_K}}{l}_{p^{m_K}}}{p^{m_K l}} \\
&= p^n(p^n + 1)\frac{1}{p^{m_K l}} \binom{\frac{n}{m_K}}{l}_{p^{m_K}}.
\end{aligned}$$

The proof is complete. □

https://doi.org/10.1017/S0017089512000766 Published online by Cambridge University Press

Let $\mathcal{N}_i$ denote the number of subgroups of type (i) in Theorem 1.1. Invoking Dickson's results in [**2**] in conjunction with the previous lemma, we obtain the following result.

LEMMA 3.2. *The number of subgroups of G of a given type is*

(1) $\mathcal{N}_1 = (p^n+1)\sum_{m=1}^{n} \binom{n}{m}_p$,

(2) $\mathcal{N}_2 = \frac{p^n(p^n+1)}{2}\left(\tau\left(\frac{p^n-1}{d}\right)-1\right) + \frac{p^n(p^n-1)}{2}\left(\tau\left(\frac{p^n+1}{d}\right)-1\right)$,

(3) $\mathcal{N}_3 = \frac{1}{2}|G|\left(\frac{d}{p^n-1}\sigma\left(\frac{p^n-1}{d}\right) + \frac{d}{p^n+1}\sigma\left(\frac{p^n+1}{d}\right)-2\right)$,

(4) $\mathcal{N}_4 = \frac{1}{12}|G|$ *if* $p>2$ *and zero otherwise,*

(5) $\mathcal{N}_5 = \frac{1}{12}|G|$ *if* $p^n \equiv -1 \pmod 8$ *and zero otherwise,*

(6) $\mathcal{N}_6 = \frac{1}{30}|G|$ *if* $p^n \equiv \pm 1 \pmod{10}$ *and zero otherwise,*

(7) $\mathcal{N}_7 = p^n(p^n+1)\left(\sum_{m|n}\alpha_{p,m}\beta_{p^m,\frac{n}{m}} - \beta_{p,n}\right)$,

(8) $\mathcal{N}_8 = |G|\left(\sum_{m|n}\frac{1}{|PSL(2,p^m)|} + \sum_{2m|n}\frac{1}{|PGL(2,p^m)|}\right)$,

where

$$\alpha_{p,m} = |\{h : dh|p^m-1, dh\nmid p^k-1, k<m, k|m\}|$$

is the number of generators of the field $GF(p^m)$ in $GF(p^m)^d$ and

$$\beta_{p^m,\frac{n}{m}} = \frac{1}{p^n}\sum_{l=1}^{\frac{n}{m}}\binom{\frac{n}{m}}{l}_{p^m} p^{ml} = \frac{1}{|V|}\sum_{0\neq U\leq V}|U|,$$

in which $V = GF(p^n)/GF(p^m)$ is a vector space of dimension n/m over the field of order p^m.

Proof. The number $\mathcal{N}_1$ is simply obtained using Theorem 1.2 and the fact that the number of subspaces of dimension m in a vector space of dimension n over a field of order q equals $\binom{n}{m}_q$. The numbers $\mathcal{N}_2,\ldots,\mathcal{N}_6$ and $\mathcal{N}_8$ are given by Dickson in [**2**, 260. pp. 285–286]. Hence, it is enough to compute the number of subgroups of type (7).

By Lemma 3.1, the number of subgroups of type (7) equals

$$\begin{aligned}
\mathcal{N}_7 &= p^n(p^n+1)\sum_{1\neq K\leq\mathcal{K}}\sum_{l=1}^{\frac{n}{m_K}}\frac{1}{p^{m_K l}}\binom{\frac{n}{m_K}}{l}_{p^{m_K}}\\
&= p^n(p^n+1)\sum_{K\leq\mathcal{K}}\sum_{l=1}^{\frac{n}{m_K}}\frac{1}{p^{m_K l}}\binom{\frac{n}{m_K}}{l}_{p^{m_K}} - t\\
&= p^n(p^n+1)\sum_{\substack{x\in F^\times\\ d||x|}}\frac{1}{\varphi(|x|)}\sum_{l=1}^{\frac{n}{m_{(x)}}}\frac{1}{p^{m_{(x)}l}}\binom{\frac{n}{m_{(x)}}}{l}_{p^{m_{(x)}}} - t
\end{aligned}$$

https://doi.org/10.1017/S0017089512000766 Published online by Cambridge University Press

$$= p^n(p^n+1)\sum_{E\le F}\sum_{\substack{E=(x)\\ d||x|}}\frac{1}{\varphi(|x|)}\sum_{l=1}^{\frac{n}{m_{(x)}}}\frac{1}{p^{m_{(x)}l}}\binom{\frac{n}{m_{(x)}}}{l}_{p^{m_{(x)}}} - t$$

$$= p^n(p^n+1)\sum_{E\le F}\left(\sum_{\substack{E=(x)\\ d||x|}}\frac{1}{\varphi(|x|)}\right)\left(\sum_{l=1}^{\frac{n}{E_p}}\frac{1}{|E|^l}\binom{\frac{n}{E_p}}{l}_{|E|}\right) - t,$$

where $E_p = \log_p |E|$ and $t = p^n(p^n+1)\sum_{l=1}^{n}\frac{1}{p^l}\binom{n}{l}_p$. Now if $E \le F$ and $|E| = p^m$ (m divides n), then it is easy to see that

$$\sum_{\substack{E=(x)\\ d||x|}}\frac{1}{\varphi(|x|)} = \alpha_{p,m}$$

and

$$\begin{aligned}\sum_{l=1}^{\frac{n}{E_p}}\frac{1}{|E|^l}\binom{\frac{n}{E_p}}{l}_{|E|} &= \sum_{l=1}^{\frac{n}{m}}\frac{1}{(p^m)^{\frac{n}{m}-l}}\binom{\frac{n}{m}}{\frac{n}{m}-l}_{p^m}\\ &= \frac{1}{p^n}\sum_{l=1}^{\frac{n}{m}}\binom{\frac{n}{m}}{l}_{p^m}(p^m)^l\\ &= \beta_{p^m,\frac{n}{m}}.\end{aligned}$$

Moreover $t = p^n(p^n+1)\beta_{p,n}$ and we have

$$\mathcal{N}_7 = p^n(p^n+1)\left(\sum_{m|n}\alpha_{p,m}\beta_{p^m,\frac{n}{m}} - \beta_{p,n}\right).$$

□

A direct consequence of the above lemma is given in the following corollary.

COROLLARY 3.3. *The number of subgroups of the group G is*

$$|L(G)| = 1 + \mathcal{N}_1 + \mathcal{N}_2 + \mathcal{N}_3 + \mathcal{N}_4 + \mathcal{N}_5 + \mathcal{N}_6 + \mathcal{N}_7 + \mathcal{N}_8.$$

Let $L_i^*(G)$ be the set of representatives of isomorphism classes of subgroups of G of type (i) in Theorem 1.1 and

$$\mathcal{N}_i' = \sum_{S\in L_i^*(G)}\mathcal{N}_S F_2(S)$$

for $i = 1, \ldots, 8$. Then

THEOREM 3.4. *The subgroup permutability degree of $G = PSL(2, p^n)$ is*

$$spd(G) = \frac{1 + \mathcal{N}_1' + \mathcal{N}_2' + \mathcal{N}_3' + \mathcal{N}_4' + \mathcal{N}_5' + \mathcal{N}_6' + \mathcal{N}_7' + \mathcal{N}_8'}{(1 + \mathcal{N}_1 + \mathcal{N}_2 + \mathcal{N}_3 + \mathcal{N}_4 + \mathcal{N}_5 + \mathcal{N}_6 + \mathcal{N}_7 + \mathcal{N}_8)^2}.$$

https://doi.org/10.1017/S0017089512000766 Published online by Cambridge University Press

Proof.

$$spd(G) = \frac{1}{|L(G)|^2} \sum_{S \in L^*(G)} \mathcal{N}_S F_2(S) = \frac{1}{(1 + \sum_{i=1}^{8} \mathcal{N}_i)^2} \left(1 + \sum_{i=1}^{8} \mathcal{N}_i'\right),$$

as required. □

Problem 1. Give an explicit formula for the numbers $\alpha_{p,m}$.

Problem 2. Give an explicit formula for the numbers $\Xi_n(V, F; E_1, E_2)$. Is there a closed formula for the special cases $n = 0, 1$?

REFERENCES

1. M. Blaum, Factorizations of the simple groups $PSL_3(q)$ and $PSU_3(q^2)$, *Arch. Math.* **40** (1983), 8–13.

2. L. E. Dickson, *Linear groups with an exposition of the galois field theory* (Dover Publications, New York, 1958).

3. M. Farrokhi D. G., Factorization numbers of finite abelian groups, *Internat. J. Group Theory* **2**(2) (2013), 1–8.

4. T. R. Gentchev, Factorizations of the sporadic simple groups, *Arch. Math.* **47** (1986), 97–102.

5. T. R. Gentchev, Factorizations of the groups of Lie type of Lie rank 1 or 2, *Arch. Math.* **47** (1986), 493–499.

6. W. H. Gustafson, What is the probability that two group elements commute? *Amer. Math. Monthly* **80** (1973), 1031–1304.

7. B. Huppert, *Endliche Gruppen I* (Springer-Verlag, Berlin, Heidelberg, 1967).

8. N. Ito, On the factorizations of the linear fractional group $LF(2, p^n)$, *Acta Sci. Math. (Szeged, Hungary)* **15** (1953), 79–84.

9. F. Saeedi and M. Farrokhi D. G., Factorization numbers of some finite groups, *Glasgow Math. J.* **54** (2012), 345–354.

10. M. Tărnăuceanu, Subgroup commutativity degrees of finite groups, *J. Algebra* **321**(9) (2009), 2508–2520.

11. M. Tărnăuceanu, Addendum to "Subgroup commutativity degrees of finite groups" [*J. Algebra* **321** (9) (2009), 2508–2520], *J. Algebra*, **337**(9) (2011), 363–368.

12. K. B. Tchakerian and T. R. Gentchev, Factorizations of the groups $G_2(q)$, *Arch. Math.* **44** (1985), 230–232.