www.combinatorics.ir

Transactions on Combinatorics
ISSN (print): 2251-8657, ISSN (on-line): 2251-8665
Vol. x No. x (20xx), pp. xx-xx.

www.ui.ac.ir

SYMMETRIC 1-DESIGNS FROM $\mathrm{PSL}_2(q)$, FOR q A POWER OF AN ODD PRIME

XAVIER MBAALE AND BERNARDO G. RODRIGUES*

Abstract. Let $G = \mathrm{PSL}_2(q)$, where q is a power of an odd prime. Let M be a maximal subgroup of G. Define $\left\{\frac{|M|}{|M\cap M^g|} : g \in G\right\}$ to be the set of orbit lengths of the primitive action of G on the conjugates of a maximal subgroup M of G. By using a method described by Key and Moori in the literature, we construct all primitive symmetric 1-designs that admit G as a permutation group of automorphisms.

1. Introduction

A program to determine symmetric 1-designs invariant under finite primitive permutation groups has been considered by Key and Moori in [9]. In [11] (see also [13]), Key and Moori described another method of construction of designs which considers the action of the groups on the conjugacy classes of elements and maximal subgroups. In this case the designs are not necessarily symmetric. These methods have been called Method 1 and Method 2, respectively in the literature [15].

Darafsheh [4] using Method 1 constructed designs from $\mathrm{PSL}_2(q)$, for q even and a pair of its maximal subgroups of dihedral type. In [16] Moori and Saeidi using Method 1 and Method 2 constructed $\mathrm{PSL}_2(q)$-invariant designs for $q > 2$ a power of 2 for the remaining maximal subgroups not considered in [4]. In [13] and [14], Moori applied Method 2 to construct designs and codes from some maximal subgroups of $\mathrm{PSL}_2(q)$, for some prime powers of q.

Communicated by Mohammad Reza Darafsheh
MSC(2020): Primary: 05B05; Secondary: 05E30, 20D60.
Keywords: 1-design, symmetric designs, primitive design, projective special linear group.
Received: 26 June 2020, Accepted: 14 August 2020.
*Corresponding author.

http://dx.doi.org/10.22108/toc.2020.123692.1740

.

In a forthcoming paper, using Method 2 we deal with the remaining classes of maximal subgroups not considered in [13] and [14] and thus complete the classification of $\mathrm{PSL}_2(q)$ invariant designs using both Method 1 and Method 2.

Given that primitive groups of the same class need not have uniform structural properties, the various classes of groups appear to need to be examined separately, although similar techniques can be used over various classes. In particular, [12] gives a complete account on the designs constructed from the primitive action of the projective general linear group $\mathrm{PGL}_2(q)$ for $q = p^n$ a power of an odd prime p.

In this paper we consider all conjugacy classes of maximal subgroups of $\mathrm{PSL}_2(q)$ for $q = p^n$, where p is an odd prime and using Method 1 we construct all primitive, self-dual and symmetric 1-designs that admit $\mathrm{PSL}_2(q)$ as a permutation group of automorphisms. When combined with the results in the literature, our results complete the construction of $\mathrm{PSL}_2(q)$-invariant designs using Method 1.

In the theorem given below, we summarize our results; the specific results relating to the designs are given as lemmas and propositions in the following sections.

Theorem 1.1. *Let G be the projective special linear group $\mathrm{PSL}_2(q)$ for $q = p^n$, p an odd prime and $n \in \mathbb{N}, n \geq 1$. Let $M \ncong C_p^n \rtimes C_{\frac{q-1}{2}}$ be a maximal subgroup of G. Let $\mathcal{D}$ be a self-dual, symmetric and primitive 1-$([G:M], |\Delta|, |\Delta|)$-design invariant under G constructed using Result 3.1. Then $\mathcal{D}$ has parameters v, k and λ as given in Table 1.*

Table 1: Non-trivial 1-designs from $\mathrm{PSL}_2(q)$, q a power of an odd prime using Method 1

Maximal Subgroup	$l = \lvert M \cap M^g \rvert$	$v = [G:M]$	$k = \lambda = \frac{\lvert M \rvert}{l}$
$\mathrm{D}_{q\pm1}$	1	$\frac{q(q\mp1)}{2}$	$q \pm 1$
	2	$\frac{q(q\mp1)}{2}$	$\frac{q\pm1}{2}$
	4 *if* $\lvert M \rvert \equiv 0 \pmod 4$	$\frac{q(q\mp1)}{2}$	$\frac{q\pm1}{4}$
$\mathrm{PGL}_2(p)$	p	$\frac{p(p^2+1)}{2}$	p^2-1
	$p-1$	$\frac{p(p^2+1)}{2}$	$p(p+1)$
	$p+1$ *if* $p \neq 5$	$\frac{p(p^2+1)}{2}$	$p(p-1)$
	$2(p-1)$ *if* $p \equiv 3 \pmod 4$	$\frac{p(p^2+1)}{2}$	$\frac{p(p+1)}{2}$
	$2(p+1)$ *if* $p \equiv 1 \pmod 4$	$\frac{p(p^2+1)}{2}$	$\frac{p(p-1)}{2}$

http://dx.doi.org/10.22108/toc.2020.123692.1740

$\mathrm{PSL}_2(p)$	1	$\frac{p^r(p^r+1)(p^r-1)}{p(p^2-1)}$	$\frac{p(p^2-1)}{2}$
	p	$\frac{p^r(p^r+1)(p^r-1)}{p(p^2-1)}$	$\frac{p^2-1}{2}$
	$\frac{p\pm1}{2}$	$\frac{p^r(p^r+1)(p^r-1)}{p(p^2-1)}$	$p(p\mp1)$
A_5	1, *if* $q=p\neq 11,19$	$\frac{q(q^2-1)}{120}$	60
	2, *if* $q=p\neq 11$	$\frac{q(q^2-1)}{120}$	30
	3, *if* $q=p\neq 11$	$\frac{q(q^2-1)}{120}$	20
	5, *if* $q=p\neq 11,19$	$\frac{q(q^2-1)}{120}$	12
	6, *if* $q=p\equiv\pm1 \pmod{10}$ *and* $p\equiv\pm1 \pmod{12}$ *or* $q=p^2$, $p\equiv\pm3 \pmod{10}$	$\frac{q(q^2-1)}{120}$	10
	10, *if* $q=p\equiv\pm1 \pmod{10}$ *and* $p\equiv\pm1 \pmod{20}$	$\frac{q(q^2-1)}{120}$	6
	12, *if* $q=p\equiv\pm1 \pmod{10}$ *and* $p\equiv\pm1 \pmod{8}$ *or* $q=p^2$, $p\equiv\pm3 \pmod{10}$	$\frac{q(q^2-1)}{120}$	5
A_4	1	$\frac{q^3-q}{24}$	12
	2	$\frac{q^3-q}{24}$	6
	3	$\frac{q^3-q}{24}$	4
S_4	1, *if* $q=p\neq 7$	$\frac{q^3-q}{48}$	24
	2, *if* $q=p\neq 7$	$\frac{q^3-q}{48}$	12
	3, *if* $q=p\neq 7$	$\frac{q^3-q}{48}$	8
	4	$\frac{q^3-q}{48}$	6
	6, *if* $q=p\equiv\pm1 \pmod{8}$ *and* $p\equiv\pm1 \pmod{12}$	$\frac{q^3-q}{48}$	4
	8, *if* $q=p\equiv\pm1 \pmod{8}$ *and* $p\equiv\pm1 \pmod{16}$	$\frac{q^3-q}{48}$	3

http://dx.doi.org/10.22108/toc.2020.123692.1740

Remark 1.2. (1) The first column of Table 1 describes the structure of the maximal subgroup M of G, column 2 indicates the value $l = |M \cap M^g|$, the cardinality of the intersection of a maximal subgroup M and its conjugate $M^g \neq M$, column 3 indicates the number v of points of $\mathcal{D}$ and the last column gives the block size k of a block Δ and λ the number of blocks which contain a given point.

(2) Note that Table 1 should be read in conjunction with Theorem 2.4(ii) - (vii). If a prime p is chosen so that the conditions of Theorem 2.4(ii) - (vii) are satisfied, then using the columns of Table 1 one can determine the corresponding 1-design.

As an example, suppose $M \cong \mathrm{A}_5$ and $p = 11$. Then the only possibility for l is $l = 6$ and we obtain the trivial 1-$(11, 10, 10)$ design. However, for $p = 19$, we have $l = 2, 3, 10$ and so we obtain the designs with parameters 1-$(57, 30, 30)$, 1-$(57, 20, 20)$ and 1-$(57, 6, 6)$, respectively.

The paper is organized as follows: in Section 2 we outline some background results and notation and give a brief but complete overview on the group $\mathrm{PSL}_2(q)$. In Section 3 we describe the construction method used and give our results on all $\mathrm{PSL}_2(q)$-invariant self-dual, symmetric and primitive 1-designs.

2. Preliminaries

Our notation for designs is standard and follows that of [1]. Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be an incidence structure, i.e, a triple with point set $\mathcal{P}$, block set $\mathcal{B}$ disjoint to $\mathcal{P}$ and incidence relation $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$. If the ordered pair $(p, B) \in \mathcal{I}$ we say that p is incident with $B \in \mathcal{B}$. It is often convenient to assume that the blocks in $\mathcal{B}$ are subsets of $\mathcal{P}$ so $(p, B) \in \mathcal{D}$ if and only if $p \in B$. For a positive integer t, we say that $\mathcal{D}$ is a *t-design* if every block $B \in \mathcal{B}$ is incident with exactly k points and every t distinct points are together incident with λ blocks. In this case, we write $\mathcal{D} = t$-(v, k, λ) where $v = |\mathcal{P}|, k = |B|$. The *complement* of $\mathcal{D}$ is the structure $\tilde{\mathcal{D}} = (\mathcal{P}, \mathcal{B}, \tilde{\mathcal{I}})$, where $\tilde{\mathcal{I}} = \mathcal{P} \times \mathcal{B} - \mathcal{I}$. The *dual* structure of $\mathcal{D}$ is $\mathcal{D}^t = (\mathcal{B}, \mathcal{P}, \mathcal{I}^t)$, where $(B, p) \in \mathcal{I}^t$ if and only if $(p, B) \in \mathcal{I}$. Thus the transpose of an incidence matrix for $\mathcal{D}$ is an incidence matrix for $\mathcal{D}^t$. We say that $\mathcal{D}$ is *symmetric* if it has the same number of points and blocks, and *self dual* if it is isomorphic to its dual. An isomorphism of t-designs $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ and $\mathcal{D}' = (\mathcal{P}', \mathcal{B}')$ is a permutation of X which sends blocks of $\mathcal{D}$ to blocks of $\mathcal{D}'$. An isomorphism from $\mathcal{D}$ to itself is called *automorphism*. The group of all automorphisms of $\mathcal{D}$ is denoted by $\mathrm{Aut}\mathcal{D}$.

We call a t-design $\mathcal{D}$ primitive if there exists an automorphism group $G \leq \mathrm{Aut}\mathcal{D}$ which acts primitively on the point and block of the designs.

Let $GF(q)$ denote the Galois field with q elements and $X := GF(q) \cup \{\infty\}$, where ∞ is a symbol not in $GF(q)$. Then we can define a fractional linear transformation $T : X \to X$ by

$$T : x \mapsto \frac{\alpha x + \beta}{\gamma x + \delta}, \alpha, \beta, \gamma, \delta \in GF(q),$$

such that $\alpha\delta - \beta\gamma$ is a non-zero square in $GF(q)$ and $T(\infty) = \frac{\alpha}{\gamma}$, $T(\frac{-\delta}{\gamma}) = \infty$, if $\gamma \neq 0$, $T(\infty) = \infty$ if $\gamma = 0$ and $T(x) \in GF(q)$ for all $x \in GF(q)$ such that $\gamma x + \delta \neq 0$. Let $T_1 : x \mapsto \frac{\alpha x+\beta}{\gamma x+\delta}$ and $T_2 : x \mapsto \frac{ax+b}{cx+d}$

http://dx.doi.org/10.22108/toc.2020.123692.1740

and define the composition of T_2 with T_1 by

$$T_2T_1 = \frac{\alpha\left(\frac{ax+b}{cx+d}\right)+\beta}{\gamma\left(\frac{ax+b}{cx+d}\right)+\delta} = \frac{(\alpha a+\beta c)x+\alpha b+\beta d}{(\gamma a+\delta c)x+\gamma b+\delta d,}$$

then the set of all such fractional linear transformations forms a group under composition known as the *Projective General Linear Group* of degree 2 over $GF(q)$ and denoted $\mathrm{PGL}_2(q)$. In the special case where $\alpha\delta-\beta\gamma=1$, we obtain the *Projective Special Linear Group* denoted $\mathrm{PSL}_2(q)$. Each fractional linear transformation $\frac{\alpha x+\beta}{\gamma x+\delta}$ has an inverse $\frac{\delta x-\beta}{-\gamma x+\alpha}$. The group $\mathrm{PSL}_2(q)$ has order $\frac{q(q^2-1)}{2}$.

The following result distinguishes the elements of $\mathrm{PSL}_2(q)$ as follows:

Lemma 2.1. [3, Theorem 2] *Let g be a non-trivial element in $\mathrm{PSL}_2(q)$ of order d and with f fix points. Then $d \mid \frac{p^n+1}{2}$ and $f=0$, $d=p$ and $f=1$, or $d \mid \frac{p^n-1}{2}$ and $f=2$.*

A subgroup A of any finite group G satisfying $A\cap A^g=\{1_G\}$ or $A\cap A^g=A$, for every $g\in G$ is called a TI-subgroup, (trivial intersection).

The subgroup structure of $\mathrm{PSL}_2(q)$ is well known and is given in detail in ([5], [17]). According to Dickson [5], every element of $\mathrm{PSL}_2(q)$ belongs to one of the following types of subgroups.

Theorem 2.2. [5, Chapter XII]*)*

(i) *Let P be a Sylow p-subgroup of $\mathrm{PSL}_2(q)$ of order p^n. Then every non-trivial element of P has a single fix point and P is a* TI*-subgroup.*

(ii) *Let H be a cyclic subgroup of $\mathrm{PSL}_2(q)$ of order $\frac{p^n-1}{2}$. Then every non-trivial element of H fixes two points. Further, there is no element of $\mathrm{PSL}_2(q)\backslash H$ that fixes these points and so H is a* TI*-subgroup.*

(iii) *Let K be a cyclic subgroup of $\mathrm{PSL}_2(q)$ of order $\frac{p^n+1}{2}$. Then K contains all elements that have no fix point in $\mathrm{PSL}_2(q)$ and K is a* TI*-subgroup.*

Remark 2.3. [5, Chapter XII]. The group $G=\mathrm{PSL}_2(p^n)$, for p an odd prime, has p^n+1 subgroups of type P with $p^{2n}-1$ distinct fractional linear transformations that fix a point, $\frac{p^n(p^n+1)}{2}$ subgroups of type H with $\frac{p^n(p^n+1)(p^n-3)}{4}$ distinct fractional linear transformations that fix two points and $\frac{p^n(p^n-1)}{2}$ subgroups of type K with $\frac{p^n(p^n-1)^2}{4}$ distinct fractional linear transformations that do not fix any point.

The following theorem from [8] gives the list of all maximal subgroups $G=\mathrm{PSL}_2(q), q=p^n$ for p an odd prime, up to conjugacy.

Theorem 2.4. [8, Theorem 2.2]. *Let $q=p^n\geq 5$ where p is an odd prime. Then the maximal subgroups of $G=\mathrm{PSL}_2(q)$ are:*

(i) $C_p^n \rtimes C_{\frac{q-1}{2}}$, *that is the stabilizer of a point of a projective line,*

(ii) D_{q-1}, *for* $q\geq 13$,

(iii) D_{q+1}, *for* $q\neq 7,9$,

http://dx.doi.org/10.22108/toc.2020.123692.1740

(iv) $\mathrm{PGL}_2(p)$, *for* $q = p^2$ *(two conjugacy classes),*

(v) $\mathrm{PSL}_2(p)$, *for* $q = p^r$ *where* r *is an odd prime,*

(vi) A_5, *for* $q \equiv \pm 1 \pmod{10}$, *where either* $q = p$ *or* $q = p^2$ *and* $p \equiv \pm 3 \pmod{10}$ *(two conjugacy classes),*

(vii) A_4, *for* $q = p \equiv \pm 3 \pmod{8}$ *and* $q \not\equiv \pm 1 \pmod{10}$,

(viii) S_4, *for* $q = p \equiv \pm 1 \pmod{8}$ *(two conjugacy classes).*

3. The construction of the designs

The designs in this paper come from the following construction, described in [9, Proposition 1], corrected in [10] and later used in [13].

Result 3.1. Let G be a finite primitive permutation group acting on the set Ω of size n. Let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer G_α of α. If $\mathcal{B} = \{\Delta^g \mid g \in G\}$ and, given $\delta \in \Delta$, $\mathcal{E} = \{\{\alpha, \delta\}^g \mid g \in G\}$, then $\mathcal{D} = (\Omega, \mathcal{B})$ forms a symmetric 1-$(n, |\Delta|, |\Delta|)$ design. Further, if Δ is a self-paired orbit of G_α then $\Gamma = (\Omega, \mathcal{E})$ is a regular connected graph of valency $|\Delta|$, $\mathcal{D}$ is self-dual, and G acts as an automorphism group on each of these structures, primitive on vertices of the graph, and on points and blocks of the design.

Adopting the designation given in [16], we also call the method of construction described in Result 3.1 by Method 1.

Let M be a maximal subgroup of G, then G acts by conjugation on the set $\mathcal{M}$ of all conjugates of M in G. We use this action of G on $\mathcal{M}$ to construct primitive, self-dual and symmetric 1-designs invariant under G. This is based on the following result.

Theorem 3.2. [18, Proposition 2.1]. *Let* G *be a finite group with a maximal subgroup* M*. Then the action of* G *by conjugation on the set* $\mathcal{M}$ *of left (right) cosets of* M *in* G *is primitive.*

For a maximal subgroup M of a group G we adopt the definition of $\mathcal{A}_M$ given in [15], i.e.,

$$\mathcal{A}_M = \{|M \cap M^g| | g \in G\}.$$

Note that $\mathcal{A}_M$ is non-empty since $|M| \in \mathcal{A}_M$ for all $g \in M$. The following lemma gives the lengths of the orbits when a finite simple group G acts on $\mathcal{M}$.

Lemma 3.3. [15, Lemma 3.3] *Let* G *be a finite simple group acting on the set of conjugates of a maximal subgroup* M *by conjugation. Then the lengths of the orbits of a point stabilizer in* G *are given as elements of the set*

$$\left\{ \frac{|M|}{l} : l \in \mathcal{A}_M \right\}$$

so that every design constructed using Result 3.1 is a 1-$([G : M], \frac{|M|}{l}, \frac{|M|}{l})$ *design for some* $l \in \mathcal{A}_M$.

http://dx.doi.org/10.22108/toc.2020.123692.1740

Remark 3.4. It follows from Lemma 3.3 that in order to find the orbit lengths of the action given in Result 3.1, one only needs to determine the set $\mathcal{A}_M$.

In what follows, we examine each of the classes of maximal subgroups of $\mathrm{PSL}_2(q)$, $q = p^n$, where p is an odd prime and n a positive integer; and for a representative M of each class of maximal subgroups we determine $\mathcal{A}_M$ with a view to constructing all $\mathrm{PSL}_2(q)$-invariant, self-dual, primitive and symmetric 1-designs.

It should be noted that when $M \cong C_p^n \rtimes C_{\frac{q-1}{2}}$, the set $\mathcal{M}$ has $q+1$ points on which G acts 2-transitively. In this case, the designs constructed from M using Method 1 (i.e., using Result 3.1) are trivial and of no interest for classification purposes.

Thus, in order to prove Theorem 1.1 we start by considering $M \cong D_{q\pm1}$, a maximal subgroup of dihedral type in G. In what follows we assume that $M = \langle a, b : a^{\frac{q\pm1}{2}} = b^2 = 1, bab = a^{-1}\rangle$, $A = \langle a\rangle$ and $B = \langle b\rangle$ and prove a number of results related with these maximal subgroups of G.

Lemma 3.5. *Let $M \cong D_{q\pm1}$ be a maximal subgroup of G of dihedral type and $g \in G$. If $M \cap M^g \neq M$ and $1_G \neq x \in M \cap M^g$, then the order of x equals 2.*

Proof. Suppose for a contradiction that $x \in M \cap M^g$ is a non-trivial element and that $o(x) \neq 2$. Then $x, x^{g^{-1}} \in M$. Since A is a normal subgroup and also a trivial intersection subgroup of M we have $x, x^{g^{-1}} \in A$, and so $1_G \neq x \in A \cap A^g = A$. From this we obtain $g \in N_G(A) = M$. This shows that $M \cap M^g = M$, which contradicts the hypothesis. Hence, for all $g \in G \setminus M$ and $1_G \neq x \in M \cap M^g$ it follows that x is of order 2. □

Lemma 3.6. *Let $M \cong D_{q\pm1}$ be a maximal subgroup of G of dihedral type and $g \in C_G(b) \setminus M$. Then $M \cap M^g = \{1_G, b\}$.*

Proof. Suppose $A \cap A^g = A$, then $M^g = M$, since $N_G(A) = D_{q\pm1} = M$ (recall that $A \trianglelefteq M$) and so $M^g \cap M = M$. Thus, assume $A \cap A^g = \{1_G\}$ and let $1_G \neq x \in M \cap M^g$. Then $x \in M$ and $x \in M^g$ so that $x = a^i b = (a^j b)^g = (a^j)^g b^g = (a^j)^g b$ (since $g \in C_G(b)$). So $a^i = (a^j)^g \in A \cap A^g = \{1_G\}$. From this we obtain $x = b$ and $M \cap M^g = \{1_G, b\}$. □

Lemma 3.7. *Let $g \in G \setminus M$ such that $M \cap A^g = \{1_G, x\}$ and $A \cap A^g = \{1_G\}$. Then $M \cap M^g = \{a^{\frac{q\pm1}{4}}, x, xa^{\frac{q\pm1}{4}}, 1_M\}$, where $x = a^i b$, $1 \leq i \leq \frac{q\pm1}{2}$.*

Proof. First we note that involutions in G are in a single conjugacy class. Since $a^{\frac{q\pm1}{4}} \in A$, there must exist $g \in G \setminus M$ such that $\left(a^{\frac{q\pm1}{4}}\right)^g = a^i b \in M \cap M^g, 1 \leq i \leq \frac{q\pm1}{4}$. Note also that $a^{\frac{q\pm1}{4}} b$ is in M and $\left(a^{\frac{q\pm1}{4}} b\right)^g = \left(a^{\frac{q\pm1}{4}}\right)^g b^g = (a^i b)(a^j b) = ba^i ba^j = a^{-i}a^j, 1 \leq i, j \leq \frac{q\pm1}{4}$ which forces $j - i = \frac{q\pm1}{4}$, so that $a^{-i}a^j$ is an involution. Thus $\left(a^{\frac{q\pm1}{4}} b\right)^g = a^{\frac{q\pm1}{4}} \in M \cap M^g$. It now follows that for $g \in G \setminus M$, such that $M \cap A^g = \{1_G, a^i b\}$, $M \cap M^g = \{a^{\frac{q\pm1}{4}}, a^i b, a^{\frac{2i+q\pm1}{4}} b, 1_M\}$, where $1 \leq i \leq \frac{q\pm1}{4}$ and $\frac{2i+q\pm1}{4}$ is taken modulo $\frac{q\pm1}{2}$. □

http://dx.doi.org/10.22108/toc.2020.123692.1740

Before we prove the next theorem, we need the following result and remark.

Lemma 3.8. *Let $k \neq 1$ such that k divides $\frac{q\pm1}{2}$. Then the number of elements in G of order k equals $\frac{\Phi(k)q(q\mp1)}{2}$ where Φ is Euler's Phi-function.*

Proof. Let H be a cyclic subgroup of G of order $\frac{q\pm1}{2}$. By [6, pp. 242 – 243], $N_G(H) = D_{q\pm1}$. Further, if S is a subgroup of H, then $N_G(S) = D_{q\pm1}$. Let $k \neq 1$ such that k divides $\frac{q\pm1}{2}$. Then the number of elements in G of order k equals $[G : N_G(S)]\Phi(k) = \frac{q(q-1)(q+1)\Phi(k)}{2(q\pm1)} = \frac{\Phi(k)q(q\mp1)}{2}$. □

We make the following remark on involutions in a dihedral group D_{2n}.

Remark 3.9. Recall that for a dihedral group D_{2n}, the elements of the form $a^ib, 1 \leq i \leq n$ are involutions. If n is even, the element $a^{\frac{n}{2}}$ is also an involution. Thus D_{2n} has $n+1$ involutions for n is even, and n involutions for n odd.

Theorem 3.10. *Let $M \cong D_{q\pm1}$ be a maximal subgroup of G of dihedral type. Then for all $g \in G$, $|M \cap M^g| \in \{1, 2, 4, |M|\}$ if $|M| \equiv 0 \pmod 4$ and $|M \cap M^g| \in \{1, 2, |M|\}$, if $|M| \equiv 2 \pmod 4$.*

Proof. From Lemma 3.6 and Lemma 3.7, we see that $M \cap M^g$ is a subgroup of M of order 2 or 4 and for all $1_G \neq x \in M \cap M^g$, $o(x) = 2$. Hence $M \cap M^g \cong V_4$ or C_2, where $V_4 \cong C_2 \times C_2$. Therefore, it only remains to show that there exists some $g \in G$ such that $M \cap M^g = \{1_G\}$. We do this by examining the possible intersections of conjugates of M and use the fact that these intersections consist only of involutions. Hence we consider the following two cases:

Case 1: If $q \equiv 1 \pmod 4$, then it follows by Lemma 3.8 that G has $\frac{q(q+1)}{2}$ involutions. Let $M \cong D_{q+1}$ where $q+1 \equiv 2 \pmod 4$. Then, using Remark 3.9 we deduce that M has $\frac{q+1}{2}$ involutions. Furthermore, the number of distinct conjugates of M in G is $\frac{q(q-1)(q+1)}{2(q+1)} = \frac{q(q-1)}{2}$, and each involution of G is in $\frac{\left(\frac{q(q-1)}{2}\right)\left(\frac{q+1}{2}\right)}{\frac{q(q+1)}{2}} = \frac{q-1}{2}$ of these conjugates. For a fixed M, the number of intersections $M \cap M^g$ of M with its conjugate M^g $(\neq M)$ equals $\frac{q(q-1)}{2} - 1 = \frac{q(q-1)-2}{2}$. Of these intersections, those for which $M \cap M^g$ is of size two equals $\left(\frac{q-1}{2} - 1\right)\left(\frac{q+1}{2}\right)$. Direct calculations show that the number of those intersections for $|M \cap M^g| = 1$ is $\frac{q(q-1)-2}{2} - \left(\frac{q-1}{2} - 1\right)\left(\frac{q+1}{2}\right) = \frac{q^2-1}{4}$, and this is different from zero for all q.

Now, consider $M \cong D_{q-1}$ where $q - 1 \equiv 0 \pmod 4$. Then M has $\frac{q-1}{2} + 1 = \frac{q+1}{2}$ involutions. The number of distinct conjugates of M in G is $\frac{q(q-1)(q+1)}{2(q-1)} = \frac{q(q+1)}{2}$, and each involution of G is in $\frac{\left(\frac{q(q+1)}{2}\right)\left(\frac{q+1}{2}\right)}{\frac{q(q+1)}{2}} = \frac{q+1}{2}$ such conjugates. In this case, we obtain that the number of distinct intersections of a fixed M with its conjugates M^g $(\neq M)$ is $\frac{q(q+1)}{2} - 1 = \frac{q(q+1)-2}{2}$. In addition, the number of such intersections for which $M \cap M^g$ has size four equals $\frac{q+1}{2} - 1 = \frac{q-1}{2}$. This follows from the proof of Lemma 3.7, since there is only one fixed involution, i.e., $a^{\frac{q-1}{4}}$, in all intersections consisting of four elements. Furthermore, since there are $\frac{q-1}{2}$ intersections $M \cap M^g$ consisting of four elements, we have accounted for $2 \times \frac{q-1}{2}$ involutions of M(excluding the involution $a^{\frac{q-1}{4}}$ which occurs in all intersections

http://dx.doi.org/10.22108/toc.2020.123692.1740

$M \cap M^g$ of size four). Thus, each involution in M occurs in exactly two intersections $M \cap M^g$ of size 4. We have thus shown that the number of intersections of M with its conjugates M^g ($\neq M$) of size two equals $\left(\frac{q-1}{2} - 2\right)\left(\frac{q-1}{2}\right)$. Similarly, the number of intersections $M \cap M^g$ with size 1 equals $\frac{q(q+1)-2}{2} - \left(\frac{q-1}{2}\right) - \left(\frac{q-5}{2}\right)\left(\frac{q-1}{2}\right) = \frac{q^2+6q-7}{4}$. Since this is distinct from zero for all q, the result follows.

Case 2: Consider $q \equiv 3 \pmod 4$. Then G has $\frac{q(q-1)}{2}$ involutions. Let $M \cong D_{q+1}$ where $q+1 \equiv 0 \pmod 4$. Then M has $\frac{q+1}{2} + 1 = \frac{q+3}{2}$ involutions. The number of distinct conjugates of M in G is $\frac{q(q-1)(q+1)}{2(q+1)} = \frac{q(q-1)}{2}$, and each involution of G is in $\frac{\left(\frac{q(q-1)}{2}\right)\left(\frac{q+3}{2}\right)}{\frac{q(q-1)}{2}} = \frac{q+3}{2}$ of the conjugates M^g. For a fixed M, the number of distinct intersections of M with its conjugates ($\neq M$) is $\frac{q(q-1)}{2} - 1 = \frac{q(q-1)-2}{2}$ and the number of these intersections with size four equals $\frac{q+3}{2} - 1 = \frac{q+1}{2}$. This follows from Lemma 3.7, since there is only one fixed involution in all intersections consisting of four elements. Since there are $\frac{q+1}{2}$ intersections $M \cap M^g$ of size 4, these account for $2 \times \frac{q+1}{2}$ involutions of M (excluding the involution $a^{\frac{q+1}{4}}$ that occurs in all intersections $M \cap M^g$ of size 4). Thus each involution in M occurs in two intersections $M \cap M^g$ of size 4. With this we have shown that the number of intersections $M \cap M^g$ of size two equals $\left(\frac{q+1}{2} - 2\right)\left(\frac{q+1}{2}\right)$ and similarly the number of intersections $M \cap M^g$ with size one equals $\frac{q(q-1)-2}{2} - \left(\frac{q+1}{2}\right) - \left(\frac{q-3}{2}\right)\left(\frac{q+1}{2}\right) = \frac{q^2-2q-3}{4}$, and moreover that this is distinct from zero for all q.

Finally, let $M \cong D_{q-1}$ where $q-1 \equiv 2 \pmod 4$. Then M has $\frac{q-1}{2}$ involutions. Calculating the number of distinct conjugates of M in G we obtain that there are $\frac{q(q-1)(q+1)}{2(q-1)} = \frac{q(q+1)}{2}$, and each involution of G is in $\frac{\left(\frac{q(q+1)}{2}\right)\left(\frac{q-1}{2}\right)}{\frac{q(q-1)}{2}} = \frac{q+1}{2}$ of these conjugates. Similar to the previous cases, for a fixed M, the number of distinct intersections of M with its conjugates ($\neq M$) is $\frac{q(q-1)}{2} - 1 = \frac{q(q-1)-2}{2}$. The number of intersections $M \cap M^g$ with $|M \cap M^g| = 2$ equals $\left(\frac{q+1}{2} - 1\right)\left(\frac{q-1}{2}\right)$. Hence, the number of intersections $M \cap M^g$ such that $|M \cap M^g| = 1$ is $\frac{q(q+1)-2}{2} - \left(\frac{q+1}{2} - 1\right)\left(\frac{q-1}{2}\right) = \frac{q^2+4q-5}{4}$ and this is never zero for all q. □

From Theorem 3.10 we infer the following result on the sizes of the non-trivial orbits of the conjugation action of G on the set of conjugates of $M \cong D_{q\pm1}$.

Corollary 3.11. *Let $M = D_{q\pm1}$ be a maximal subgroup of G and $\mathcal{M}$ be the set of conjugates of M in G on which G acts by conjugation.*

(i) *If $q \equiv 1 \pmod 4$ and $|M| = q+1 \equiv 2 \pmod 4$ then the primitive action of G on $\mathcal{M}$ has the following non-trivial orbit lengths:*
(a) $\frac{q-3}{2}$ orbits of length $\frac{q+1}{2}$, b) $\frac{q-1}{4}$ orbits of length $q+1$.

(ii) *If $q \equiv 1 \pmod 4$ and $|M| = q-1 \equiv 0 \pmod 4$ then the primitive action of G on $\mathcal{M}$ has the following non-trivial orbit lengths:*
(a) 2 orbits of length $\frac{q-1}{4}$, b) $\frac{q-5}{2}$ orbits of length $\frac{q-1}{2}$, c) $\frac{q+7}{4}$ orbits of length $q-1$.

http://dx.doi.org/10.22108/toc.2020.123692.1740

(iii) *If* $q \equiv 3 \pmod 4$ *and* $|M| = q+1 \equiv 0 \pmod 4$ *then the primitive action of* G *on* $\mathcal{M}$ *has the following non-trivial orbit lengths:*
(a) 2 *orbits of length* $\frac{q+1}{4}$, *b)* $\frac{q-3}{2}$ *orbits of length* $\frac{q+1}{2}$, *c)* $\frac{q-3}{4}$ *orbits of length* $q+1$.

(iv) *If* $q \equiv 3 \pmod 4$ *and* $|M| = q-1 \equiv 2 \pmod 4$ *then the primitive action of* G *on* $\mathcal{M}$ *has the following non-trivial orbit lengths:*
(a) $\frac{q-1}{2}$ *orbits of length* $\frac{q-1}{2}$, *b)* $\frac{q+5}{4}$ *orbits of length* $q-1$.

Proof. The orbit lengths are calculated using Theorem 3.10 and Lemma 3.3. Observe that the number of orbits of a given length is obtained by taking the quotient between the number of intersections $M \cap M^g$ that give that orbit length and the corresponding orbit length. □

We now consider the case when M is a maximal subgroup of $\mathrm{PSL}_2(p^2)$ isomorphic to $\mathrm{PGL}_2(p)$.

Lemma 3.12. *Let* H *be a subgroup of* $\mathrm{PSL}_2(p^2)$ *of order* p^2 *generated by elements of the form* $h_\mu = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}, \mu \in GF(p^2)$. *Then* H *is an elementary abelian* p*-group. Moreover, if for some* $g \in G$, $g^{-1}h_\mu g = h_\mu$ *then* g *is of the form* $g_\beta = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}, \beta \in GF(p^2)$.

Proof. Let $\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} \in H, \beta, \mu \in GF(p^2)$. Then,

$$\overbrace{\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}\cdots\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}}^{p} = \begin{pmatrix} 1 & \overbrace{\mu+\mu+\cdots+\mu}^{p} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

since for every $\mu \in GF(p^2)$, $\overbrace{\mu+\mu+\cdots+\mu}^{p} = p\mu = 0$ in $GF(p^2)$. Hence every element of H has order p. The subgroup H is abelian since,

$$\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \mu+\beta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}.$$

http://dx.doi.org/10.22108/toc.2020.123692.1740

To prove the other part of the lemma, let $v = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G$, then

$$v^{-1}h_\mu v = \begin{pmatrix} \alpha & -\beta \\ -\gamma & \delta \end{pmatrix} \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha & -\beta \\ -\gamma & \delta \end{pmatrix} \begin{pmatrix} \alpha & \alpha\mu+\beta \\ \gamma & \gamma\mu+\delta \end{pmatrix}$$
$$= \begin{pmatrix} \delta\alpha - \gamma\beta - \gamma\alpha\mu & -\beta\alpha + \alpha^2\mu + \alpha\beta \\ \delta\gamma - \gamma^2\mu - \gamma\delta & -\gamma\beta + \gamma\alpha\mu + \alpha\delta \end{pmatrix}$$
$$= \begin{pmatrix} 1 - \alpha\gamma\mu & \alpha^2\mu \\ -\gamma^2\mu & 1 + \alpha\gamma\mu \end{pmatrix}$$

and $v^{-1}h_\mu v$ is in H if and only if $\gamma = 0$, when it becomes $h_{\alpha^2\mu} = \begin{pmatrix} 1 & \alpha^2\mu \\ 0 & 1 \end{pmatrix}$. Hence H is normalized by elements in G of the form $h_\lambda = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ where $\lambda \in GF(p^2)$. □

Corollary 3.13. *Let M be a maximal subgroup of $\mathrm{PSL}_2(p^2)$ isomorphic to $\mathrm{PGL}_2(p)$. Then there exists $g \in G \setminus M$, where g is of the form $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$, $\lambda \in GF(p^2)$ such that $|M \cap M^g| = p$.*

Proof. The proof follows from the fact that M has a subgroup of order p which is also a subgroup of H as given in Lemma 3.12. □

Proposition 3.14. [5, page 267] *Let $d > 2$ such that $d|\frac{p^2-1}{2}$ with quotient s. If s is even, then $\mathrm{PSL}_2(p^2)$ contains dihedral groups D_{2d} which are normalized under the dihedral group $D_{2(2d)}$.*

Lemma 3.15. *Let $d = p \pm 1$, p an odd prime. Then $d|\frac{p^2-1}{2}$. Moreover, the quotient $\frac{p+1}{2}$ is even if $p \equiv -1 \pmod 4$, and the quotient $\frac{p-1}{2}$ is even if $p \equiv 1 \pmod 4$.*

Proof. The proof follows using arguments from elementary number theory. So we omit it. □

Corollary 3.16. *Let M be a maximal subgroup of $G = \mathrm{PSL}_2(p^2)$ isomorphic to $\mathrm{PGL}_2(p)$. If $g \in D_{2(2(p\pm1))} \setminus D_{2(p\pm1)}$ but $g \notin M$, then $|M \cap M^g| = 2(p+1)$ if $p \equiv 1 \pmod 4$, and $|M \cap M^g| = 2(p-1)$ if $p \equiv -1 \pmod 4$.*

http://dx.doi.org/10.22108/toc.2020.123692.1740

Proof. We show that $D_{2(2(p\pm1))}$ is a subgroup of $\mathrm{PSL}_2(p^2)$ whenever the conditions on p given in the hypothesis are satisfied. We first note that for $D_{2(2(p\pm1))}$ to be a subgroup of $\mathrm{PSL}_2(p^2)$, its order $4(p\pm1)$ must divide $\frac{p^2(p^2-1)(p^2+1)}{2}$ i.e., $4(p\pm1)|\frac{p^2(p\pm1)(p^2+1)}{2}$. Since p is an odd prime, then $p^2+1\equiv 2 \pmod 4$. Thus $\frac{p^2(p-1)(p^2+1)}{8}\equiv 0 \pmod 4$ if $p\equiv 1 \pmod 4$ and $\frac{p^2(p+1)(p^2+1)}{8}\equiv 0 \pmod 4$ if $p\equiv -1 \pmod 4$. Since a subgroup $D_{2(p\pm1)}$ of M is also a subgroup of $D_{2(2(p\pm1))}$, the result follows immediately by Proposition 3.14. □

Lemma 3.17. [5, pages 263 - 264] *Let A be a cyclic subgroup of $\mathrm{PSL}_2(p^2)$ of order $\frac{p^2-1}{2}$. Then the dihedral group D_{p^2-1} is the largest subgroup of $\mathrm{PSL}_2(p^2)$ in which A is normalized.*

Corollary 3.18. *Let $C_{p\pm1}$ be a cyclic subgroup of A as given in Lemma 3.17 and M be a maximal subgroup of $\mathrm{PSL}_2(p^2)$ isomorphic to $\mathrm{PGL}_2(p)$. Then there exists some $g\in D_{p^2-1}\setminus C_{p\pm1}$, $g\notin M$, such that $|M\cap M^g|=p\pm1$ for all $p\geq 5$, where p is an odd prime except if $p=5$ when $|M\cap M^g|\neq p+1$.*

Proof. The proof that $|M\cap M^g|=p\pm1$ follows by Lemma 3.17 since $C_{p\pm1}$ is normal in D_{p^2-1}. However, when $p=5$, $D_{5^2-1}\cong D_{2(2(5+1))}$ and by Proposition 3.14, D_{24} is the normalizer of D_{12}. Since C_6 is a subgroup of D_{12}, it follows that for $g\in D_{24}\setminus C_6$, $g\notin M$, $|M\cap M^g|=12$ and not 6. □

Theorem 3.19. *Let M be a maximal subgroup of $\mathrm{PSL}_2(p^2)$ isomorphic to $\mathrm{PGL}_2(p)$, where $p\geq 7$. Then $|M\cap M^g|\in\{p,p\pm1,2(p+1),|M|\}$ if $p\equiv 1 \pmod 4$, and $|M\cap M^g|\in\{p,p\pm1,2(p-1),|M|\}$ if $p\equiv 3 \pmod 4$. Moreover, these are the only possibilities for $|M\cap M^g|$.*

Further, for $p=5$, $\mathrm{PSL}_2(p^2)$ is rank 4 on its primitive action on 65 points with non-trivial orbits of lengths 30, 24 and 10.

Proof. For $g\in M$ we have $|M\cap M^g|=|M|$. For the other possibilities, see Corollary 3.13, Corollary 3.18 and Corollary 3.16, respectively. The number of distinct conjugates of M in $\mathrm{PSL}_2(p^2)$ is $\frac{p^2(p^2-1)(p^2+1)}{2p(p+1)(p-1)}=\frac{p(p^2+1)}{2}$. The number of distinct intersections $M\cap M^g\neq M$ equals $\frac{p(p^2+1)}{2}-1$. For $p\equiv 3 \pmod 4$ and $p\equiv 1 \pmod 4$, respectively it can be shown that $\frac{p(p+1)}{2}$ of these intersections are of size $2(p-1)$, (p^2-1) of size p, $\frac{(p-3)(p^2+p)}{4}$ of size $p-1$ and $\frac{(p-3)(p^2-p)}{4}$ of size $p+1$, respectively when $p\equiv 3 \pmod 4$. Furthermore, if $p\equiv 1 \pmod 4$ then $\frac{p(p-1)}{2}$ of these intersections are of size $2(p+1)$, (p^2-1) are of size p, $\frac{(p-1)(p^2+p)}{4}$ of size $p-1$ and $\frac{(p-5)(p^2-p)}{4}$ of size $p+1$, respectively. Direct calculations show that if $p\equiv 3 \pmod 4$, then

$$\frac{p(p^2+1)}{2}=\frac{p(p+1)}{2}+p^2-1+\frac{(p-3)(p^2+p)}{4}+\frac{(p-3)(p^2-p)}{4}+1,$$

while if $p\equiv 1 \pmod 4$

$$\frac{p(p^2+1)}{2}=\frac{p(p-1)}{2}+p^2-1+\frac{(p-1)(p^2+p)}{4}+\frac{(p-5)(p^2-p)}{4}+1.$$

By these calculations we have accounted for all conjugates of M for each of the two congruences given above.

http://dx.doi.org/10.22108/toc.2020.123692.1740

It follows from [6, Appendix B, Table B.2] that when $p = 5$, $\mathrm{PSL}_2(p^2)$ is rank 4 on its primitive action on 65 points with non-trivial orbits of lengths 30, 24 and 10. □

The next results gives the lengths of the non-trivial orbits of the action of G on $\mathcal{M}$, for $\mathcal{M}$ the set of conjugates of $M \cong \mathrm{PGL}_2(q)$.

Corollary 3.20. *Suppose $M \cong \mathrm{PGL}_2(p)$ is a maximal subgroup of $\mathrm{PSL}_2(p^2)$. Let $\mathcal{M}$ be the set of conjugates of M in G on which G acts by conjugation.*

(i) *If $q \equiv 3 \pmod 4$ then the primitive action of G on $\mathcal{M}$ has the following non-trivial orbit lengths:*
   (a) one orbit of length $\frac{p(p+1)}{2}$, b) one orbit of length p^2-1, c) $\frac{p-3}{4}$ orbits of length $p(p+1)$, d) $\frac{p-3}{4}$ orbits of length $p(p-1)$.

(ii) *If $q \equiv 1 \pmod 4$ then the primitive action of G on $\mathcal{M}$ has the following non-trivial orbit lengths:*
   (a) one orbit of length $\frac{p(p-1)}{2}$, b) one orbit of length p^2-1, c)$\frac{p-1}{4}$ orbits of length $p(p+1)$, d) $\frac{p-5}{4}$ orbits of length $p(p-1)$.

Proof. The proof follows from Theorem 3.19 and Lemma 3.3. □

Next we consider the case where M the maximal subgroup of G is isomorphic to $\mathrm{PSL}_2(p)$.

Theorem 3.21. *Let $M \cong \mathrm{PSL}_2(p)$ be a maximal subgroup of $\mathrm{PSL}_2(p^r)$ where r is an odd prime. Then for all $g \in G$, $|M \cap M^g| \in \left\{1, p, \frac{p\pm1}{2}, |M|\right\}$.*
If $p = 3$ then $\mathcal{A}_{\mathcal{M}} = \{1, p, \frac{p+1}{2}, |M|\}$.

Proof. If $g \in M$, then $M \cap M^g = M$. Let $g \in G \setminus M$, then by Theorem 2.2, every $x \in M$ and consequently $x \in G$ is in one of the subgroups of types P, H or K of G. Since these are all TI-subgroups in G, there exists some $g \in G$ such that $|M \cap M^g| \in \{p, \frac{p\pm1}{2}\}$.

Using Remark 2.3 we obtain that M has p^2-1 elements of order p and by [3, Theorem 3] it follows that G has $p^{2r}-1$ elements of order p. Thus each element of order p in G occurs in $\frac{\frac{p^r(p^r+1)(p^r-1)}{p(p-1)(p+1)}(p^2-1)}{p^{2r}-1}$ $= p^{r-1}$ of the conjugates of M. Moreover, the number of intersections $M \cap M^g$ such that $|M \cap M^g| = p$ equals $\frac{(p^{r-1}-1)(p^2-1)}{p-1} = (p^{r-1}-1)(p+1)$. Once again, using Remark 2.3 we find that M has $\frac{p(p+1)}{2}$ cyclic subgroups of order $\frac{p-1}{2}$, so that M also has $\frac{p(p+1)}{2}$ elements of the form $x = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$, where ω is a primitive root in $GF(p)$, and x generates a cyclic group of order $\frac{p-1}{2}$. Further, from [3, Theorem 3(i)] G has $\frac{p^r(p^r+1)}{2}$ elements that generate cyclic subgroups of order $\frac{p-1}{2}$. Thus each x in G is in $\frac{\frac{p^r(p^r+1)(p^r-1)}{p(p-1)(p+1)}\left(\frac{p(p+1)}{2}\right)}{\frac{p^r(p^r+1)}{2}} = \frac{p^r-1}{p-1}$ conjugates of M. From Remark 2.3, we have that M has $\frac{p(p+1)(p-3)}{4}$

elements of order $\frac{p-1}{2}$. Hence $\frac{\left(\frac{p^r-1}{p-1}-1\right)\left(\frac{p(p+1)(p-3)}{4}\right)}{\frac{p-3}{2}} = \frac{p^2(p+1)(p^{r-1}-1)}{2(p-1)}$ of the intersections $M \cap M^g$ are of size $\frac{p-1}{2}$.

Using Remark 2.3 and [3, Theorem 3] it can be shown that M has $\frac{p(p-1)}{2}$ elements that generate cyclic subgroups of order $\frac{p+1}{2}$ while G has $\frac{p^r(p^r-1)}{2}$ elements that generate cyclic subgroups of order $\frac{p+1}{2}$. Each of the elements of G that generate cyclic subgroups of order $\frac{p+1}{2}$ occur in $\frac{\frac{p^r(p^r+1)(p^r-1)}{p(p-1)(p+1)}\left(\frac{p(p-1)}{2}\right)}{\frac{p^r(p^r-1)}{2}} = \frac{p^r+1}{p+1}$ distinct conjugates of M. Now, it can be shown using Remark 2.3 that M has $\frac{p(p-1)^2}{4}$ elements of order $\frac{p+1}{2}$. From this we deduce that $\frac{\left(\frac{p^r+1}{p+1}-1\right)\left(\frac{p(p-1)^2}{4}\right)}{\frac{p-1}{2}} = \frac{p^2(p-1)(p^{r-1}-1)}{2(p+1)}$ of the intersections $M \cap M^g$ are such that $|M \cap M^g| = \frac{p+1}{2}$. Since for a fixed M the number of intersections $M \cap M^g$ is $\frac{p^r(p^r+1)(p^r-1)}{p(p-1)(p+1)} - 1$ and since

$$\begin{aligned} &1 + (p^{r-1}-1)(p+1) + \frac{p^2(p+1)(p^{r-1}-1)}{2(p-1)} + \frac{p^2(p-1)(p^{r-1}-1)}{2(p+1)} \\ &= 1 + \frac{(p^{r-1}-1)(p^4+p^3+2p^2-p-1)}{p^2-1} < \frac{p^r(p^r+1)(p^r-1)}{p(p-1)(p+1)}, \end{aligned}$$

there must exists $g \in G$ such that $M \cap M^g = \{1_G\}$.
Since for $p = 3$ we have $\frac{p-1}{2} = 1$, then it follows that $\mathcal{A}_{\mathcal{M}} = \{1, p, \frac{p+1}{2}, |M|\}$. □

Corollary 3.22. *Let $M \cong \mathrm{PSL}_2(p)$ be a maximal subgroup of $\mathrm{PSL}_2(p^r)$, r an odd prime and let $\mathcal{M}$ be the set of conjugates of M in G on which G acts by conjugation. Then the primitive action of G on $\mathcal{M}$ has the following non-trivial orbit lengths.*

a) $\frac{p(p^{r-1}-1)}{2(p-1)}$ *orbits of length* $p(p+1)$, *b)* $\frac{2(p^{r-1}-1)}{p-1}$ *orbits of length* $\frac{p^2-1}{2}$, *c)* $\frac{p(p^{r-1}-1)}{2(p+1)}$ *orbits of length* $p(p-1)$, *d)* $\frac{2\left[p^{3r-2}-p^{r+2}-p^{r+1}-2p^r+p^{r-1}+p^3+p^2+p-1\right]}{(p^2-1)^2}$ *orbits of length* $\frac{p(p^2-1)}{2}$.

Proof. The proof follows az a direct application of Theorem 3.21. □

Now, consider the maximal subgroup of type A_5 of $G = \mathrm{PSL}_2(q)$.

Proposition 3.23. *Let M be a maximal subgroup of $G = \mathrm{PSL}_2(q)$ isomorphic to A_5, then for every $g \in G$, $\mathcal{A}_M$ is one of the following:*

a) $\{1, 2, 3, 5, 12, 60\}$, *if* $q = p \equiv \pm 1 \pmod{10}$ *and* $q = p \equiv \pm 1 \pmod{8}$ *but* $q = p \not\equiv \pm 1 \pmod{20}$ *and* $q = p \not\equiv \pm 1 \pmod{12}$ *;*

b) $\{1, 2, 3, 5, 6, 12, 60\}$, *if* $q = p \equiv \pm 1 \pmod{10}$, $q = p \equiv \pm 1 \pmod{8}$ *and* $q = p \equiv \pm 1 \pmod{12}$ *but* $q = p \not\equiv \pm 1 \pmod{20}$ *or* $q = p^2$ *where* $p \equiv \pm 3 \pmod{10}$*;*

c) $\{1, 2, 3, 5, 10, 12, 60\}$, *if* $q = p \equiv \pm 1 \pmod{10}$, $q = p \equiv \pm 1 \pmod{8}$ *and* $q = p \equiv \pm 1 \pmod{20}$ *but* $q = p \not\equiv \pm 1 \pmod{12}$*;*

d) $\{1, 2, 3, 5, 6, 10, 60\}$, *if* $q = p \equiv \pm 1 \pmod{10}$, $q = p \equiv \pm 1 \pmod{12}$ *and* $q = p \equiv \pm 1 \pmod{20}$ *but* $q = p \not\equiv \pm 1 \pmod{8}$.

http://dx.doi.org/10.22108/toc.2020.123692.1740

Proof. Since $A_5 \cong \mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5)$, the fact that the subgroups of orders $1, 2, 3, 5, 60$ are in $\mathcal{A}_M$ is dealt with in [16, Proposition 2.6] and Theorem 3.21 above. Thus it only remains to prove that 6, 10 and 12 are in $\mathcal{A}_M$. Now $N_G(A_4) = S_4$ whenever $q = p^2 \equiv 1 \pmod{16}$ and thus $12 \in \mathcal{A}_M$ if and only if $q = p \equiv \pm 1 \pmod 8$. Also $N_G(S_3) = D_{12}$, so that $6 \in \mathcal{A}_M$ if and only if $q = p \equiv \pm 1 \pmod{12}$. Further, $N_G(D_{10}) = D_{20}$ whenever $q = p \equiv \pm 1 \pmod{20}$, thus $10 \in \mathcal{A}_M$ if and only $q = p \equiv \pm 1 \pmod{20}$. For $q = p^2$ where $p \equiv \pm 3 \pmod{10}$, $p^2 \equiv 1 \pmod{12}$ and $p^2 \equiv 1 \pmod 8$ and hence for such q, both subgroups of order 6 and 12 occur together in $\mathcal{A}_M$.

To illustrate the argument for the proof we deal with part a) of the proposition. The remaining cases can be dealt with using a similar approach. Firstly, we note that A_4 is a maximal subgroup in M so that the number of intersections $M \cap M^g$ of size twelve is 5 (the index of A_4 in M). By Lemma 3.8, G has $\frac{4q(q\pm1)}{2}$ elements of order 5. Thus each element of order 5 in G is in $\frac{\left[\frac{q(q^2-1)}{120}\right]\times 24}{2(q(q\pm1))}$ $= \frac{q\mp1}{10}$ conjugates M^g. This means that there are $\frac{\left(\frac{q\mp1}{10}-1\right)\times 24}{4} = 6\left(\frac{q\mp1}{10}-1\right)$ intersections $M \cap M^g$ of size five. From Lemma 3.8 we have that G has $q(q \pm 1)$ elements of order 3. Thus, each element of order 3 in G is in $\frac{\left[\frac{q(q^2-1)}{120}\right]\times 20}{q(q\pm1)} = \frac{q\mp1}{6}$ conjugates M^g. But we note that elements of order 3 in G also appear in intersections $M \cap M^g$ of size twelve. Easy calculations show that each element of order 3 in G is in $\frac{5\times 8}{20} = 2$ of the intersections $M \cap M^g$ of size twelve. Thus there are $\frac{\left(\frac{q\mp1}{6}-3\right)\times 20}{2}$ $= 10\left(\frac{q\mp1}{6}-3\right)$ intersections $M \cap M^g$ of size three. But by Lemma 3.8, G has $\frac{q(q\pm1)}{2}$ elements of order 2. This shows that each element of order 2 in G is in $\frac{\left[\frac{q(q^2-1)}{120}\right]\times 15}{\frac{q(q\pm1)}{2}} = \frac{q\mp1}{4}$ conjugates M^g. Note in addition that each element of order 2 in G is in $\frac{5\times(3)}{15} = 1$ intersections $M \cap M^g$ of size twelve. Hence, $15\left(\frac{q\mp1}{4}-2\right)$ of the intersections $M \cap M^g$ are of size two. Finally, observe that $1 + 5 + 6\left(\frac{q\mp1}{10}-1\right) + 10\left(\frac{q\mp1}{6}-3\right) + 15\left(\frac{q\pm1}{4}-2\right) < \frac{q(q^2-1)}{120}$ for $q \geq 31$. Hence there exists $g \in G$ such that $M \cap M^g = \{1_M\}$. □

Remark 3.24. Notice that the primes 11 and 19 do not fall in any of the cases of Proposition 3.23. However, it is known that when $p = 11$, $\mathrm{PSL}_2(11)$ has rank 2 on its primitive action on 11 points, while for $p = 19$, $\mathrm{PSL}_2(19)$ has rank 4 in its primitive action on 57 points with non-trivial orbits of lengths $30, 20$ and 6, see [6, Appendix B, Table B.2].

Corollary 3.25. *Let M be a maximal subgroup of $\mathrm{PSL}_2(q)$ isomorphic to A_5 and $\mathcal{M}$ be the set of conjugates of M in G on which G acts by conjugation. Then the primitive action of G on $\mathcal{M}$ has non-trivial orbits of lengths $5, 6, 10, 12, 20, 30$ and 60, respectively. In particular if $q = p \equiv \pm 1 \pmod{10}$ and $q = p \equiv \pm 1 \pmod 8$ but $q = p \not\equiv \pm 1 \pmod{20}$ and $q = p \not\equiv \pm 1 \pmod{12}$, then the primitive action of G on $\mathcal{M}$ has the following non-trivial orbit lengths:*
a) one orbit of length 5; *b) $\frac{1}{2}\left(\frac{q\mp1}{10}-1\right)$ orbits of length 12;* *c) $\frac{1}{2}\left(\frac{q\mp1}{6}-3\right)$ orbits of length 20;*

d) $\frac{1}{2}\left(\frac{q\pm1}{4}-2\right)$ *orbits of length* 30*;*
e) $\frac{\left[\frac{q(q^2-1)}{120}-\left(1+5+6\left(\frac{q\mp1}{10}-1\right)+10\left(\frac{q\mp1}{6}-3\right)+15\left(\frac{q\pm1}{4}-2\right)\right)\right]}{60}$ *orbits of length* 60*.*

Proof. The proof follows direct from Proposition 3.23 □

We now consider the case where M the maximal subgroup of G is isomorphic to A_4. In order to prove the next theorem, we first give a remark followed by a lemma.

Remark 3.26. A_4 is a maximal subgroup of $G = \mathrm{PSL}_2(q)$ when $q = p \equiv \pm 3 \pmod 8$ and $q \not\equiv \pm 1 \pmod{10}$. The number of conjugates of A_4 in G is $\frac{q^3-q}{24}$ and by Lemma 3.8, G has $\frac{q(q\pm1)}{2}$ involutions. Since $A_4 \cong (C_2 \times C_2) \rtimes C_3$, then A_4 has 3 involutions and 8 elements of order 3 (4 subgroups of order 3).

Lemma 3.27. [7, Theorem 1.3] *Let $V_4 \cong C_2 \times C_2$ be a subgroup of $G = \mathrm{PSL}_2(p)$ for p odd. If $p \equiv \pm 1 \pmod 8$ then $N_G(V_4) \cong S_4$ and if $p \equiv \pm 3 \pmod 8$ and $q \not\equiv 1 \pmod{10}$, then $N_G(V_4) \cong A_4$.*

We now prove the following theorem on the determination of cardinality $|M \cap M^g|$ for $M \cong A_4$.

Theorem 3.28. *Let M be a maximal subgroup of G isomorphic to A_4. Then for every $g \in G$, $|M \cap M^g| \in \{1, 2, 3, |M|\}$.*

Proof. First we note that since the normalizer in G of $C_2 \times C_2$ is either A_4 or S_4, then we have that $|A_4 \cap A_4^g| \neq 4$. Therefore, the only non-trivial subgroups of $A_4 \cap A_4^g$ are C_2 and C_3. Each involution of G is in $\frac{3 \times \left(\frac{q^3-q}{24}\right)}{\frac{q(q\pm1)}{2}} = \frac{q\mp1}{4}$ conjugates of M. Hence there are $3\left(\frac{q\mp1}{4}-1\right)$ intersections $M \cap M^g$ of order 2. It follows by Lemma 3.8 that the number of elements of order 3 in $\mathrm{PSL}_2(q)$ is either $q(q+1)$ or $q(q-1)$. Each element of order 3 in $\mathrm{PSL}_2(q)$ is in $\frac{8 \times \left(\frac{q^3-q}{24}\right)}{q(q\pm1)} = \frac{q\mp1}{3}$ conjugates of A_4. The number of distinct intersections of M with its conjugates ($\neq M$) such that $|M \cap M^g| = 3$ equals $\frac{8\times\left(\frac{q\mp1}{3}-1\right)}{2} = 4\left(\frac{q\mp1}{3}-1\right)$. Since $1 + 3\left(\frac{q\mp1}{4}-1\right) + 4\left(\frac{q\mp1}{3}-1\right) < \frac{q^3-q}{24}$, then there exist $g \in G$ such that $A_4 \cap A_4^g = \{1_G\}$. □

Corollary 3.29. *Let $M \cong A_4$ be a maximal subgroup of G and $\mathcal{M}$ be the set of conjugates of M in G on which G acts by conjugation. Then the primitive action of G on $\mathcal{M}$ has the following non-trivial orbit lengths;*
a) $\left(\frac{q\mp1}{3}-1\right)$ *orbits of length* 4*;* *b)* $\frac{1}{2}\left(\frac{q\mp1}{4}-1\right)$ *orbits of length* 6*;*
c) $\frac{\frac{q^3-q}{24}-\left[4\left(\frac{q\mp1}{3}-1\right)+3\left(\frac{q\mp1}{4}-1\right)+1\right]}{12}$ *orbits of length* 12*;*

Proof. The proof follows directly from Theorem 3.28. □

Lastly, we consider the maximal subgroups of type S_4 in $\mathrm{PSL}_2(q)$.

http://dx.doi.org/10.22108/toc.2020.123692.1740

Proposition 3.30. *Let M be a maximal subgroup of $G = \mathrm{PSL}_2(q)$ isomorphic to S_4. Then for every $g \in G$, $\mathcal{A}_M$ is one of the following:*

a) $\{1,2,3,4,8,24\}$ *if* $q = p \equiv \pm 1 \pmod 8$ *and* $q = p \equiv \pm 1 \pmod{16}$ *but* $q = p \not\equiv \pm 1 \pmod{12}$*;*

b) $\{1,2,3,4,6,24\}$ *if* $q = p \equiv \pm 1 \pmod 8$ *and* $q = p \equiv \pm 1 \pmod{12}$ *but* $q = p \not\equiv \pm 1 \pmod{16}$*;*

c) $\{1,2,3,4,24\}$ *if* $q = p \equiv \pm 1 \pmod 8$ *but* $q = p \neq 7$, $q = p \not\equiv \pm 1 \pmod{12}$ *and* $q = p \not\equiv \pm 1 \pmod{16}$*;*

d) $\{1,2,3,4,6,8,24\}$ *if* $q = p \equiv \pm 1 \pmod 8$, $q = p \equiv \pm 1 \pmod{12}$ *and* $q = p \equiv \pm 1 \pmod{16}$.

Proof. First we note that $N_G(A_4) = S_4$ and hence $A_4 \notin M \cap M^g$ for all $g \in G$. But $N_G(S_3) = D_{12}$ so that $6 \in \mathcal{A}_M$ if and only if $q = p \equiv \pm 1 \pmod{12}$. Further, $N_G(D_8) = D_{16}$ and thus $8 \in \mathcal{A}_M$ if and only if $q = p \equiv \pm 1 \pmod{16}$.

As an illustration, we prove case c) of the proposition. The other cases can be proven using a similar approach. We begin by observing that the elements of order 3 in G lie in $\frac{8\times\left(\frac{q^3-q}{48}\right)}{q(q\pm1)} = \frac{q\mp1}{6}$ conjugates of M. There are $\frac{8\times\left(\frac{q\mp1}{6}-1\right)}{2} = 4\left(\frac{q\mp1}{6}-1\right)$ conjugates of M not equal to M whose intersection with M is of order 3. Similarly, for elements of order 4, there are $3\left(\frac{q\mp1}{8}-1\right)$ conjugates of M not equal to M whose intersection with M has size 4. Since, by Lemma 3.27, $N_G(V_4) \cong S_4$, then $S_4 \cap S_4^g \neq V_4$, for $g \in G$. Of the nine elements of order 2 in S_4, three are in V_4 and the remaining six form a single conjugacy class in S_4. Since all the involutions in G form a single conjugacy class, each of the six involution of S_4 not in V_4 is conjugate to a non-trivial element of V_4 in G. Let x, y, z be in involutions in S_4 and $x, z \in S_4 \setminus V_4$. Without loss of generality, we can find an involution $g \in C_G(z)$ such that $x^g = y$, where $1_{V_4} \neq y \in V_4$. Observe that $y^g = (x^g)^g = x$, so that for such a $g \in G$, $S_4^g \cap S_4 = \{1_{S_4}, x, y, z\}$ which is isomorphic to a subgroup containing elements such as those in the set $\{1, (a,b), (c,d), (a,b)(c,d)\}$ in S_4. Since there are six elements of type x in S_4 then there are six more intersections $M \cap M^g$ with $g \in G$ such that $|M \cap M^g| = 4$. Now, since each involution in G is in $\frac{\left(\frac{q^3-q}{48}\right)\times 9}{\frac{q(q\pm1}{2}} = \frac{3(q\mp1)}{8}$ of the conjugates M^g it follows that there are $9\left(\frac{3(q\mp1)}{8}-1\right)$ intersections $M \cap M^g$ that contain an involution. But involutions are also in intersections $M \cap M^g$ such that $|M \cap M^g| = 4$. Then we have to subtract those cases from $9\left(\frac{3(q\mp1)}{8}-1\right)$. This accounts for $9\left(\frac{3(q\mp1)}{8}-1\right) - 3\left(\frac{q\mp1}{8}-1\right) - 18$ intersections $M \cap M^g$ for which $|M \cap M^g| = 2$. This in turn shows that for $q \geq 41$, $1 + 4\left(\frac{q\pm1}{6}-1\right) + 3\left(\frac{q\mp1}{8}-1\right) + 6 + 9\left(\frac{3(q\mp1)}{8}-1\right) - 3\left(\frac{q\mp1}{8}-1\right) - 18 < \frac{q^3-q}{48}$. Hence there must exist some $g \in G$ such that $|M \cap M^g| = 1 \in \mathcal{A}_M$. Thus $\mathcal{A}_M = \{1,2,3,4,24\}$, if $q = p \equiv \pm 1 \pmod 8$ but $q = p \not\equiv \pm 1 \pmod{12}$ and $q = p \not\equiv \pm 1 \pmod{16}$. □

Remark 3.31. The only exception to Proposition 3.30 occurs when $p = 7$ where $\mathrm{PSL}_2(p)$ has rank 2 on its primitive action on 7 points.

Corollary 3.32. *Let M be a maximal subgroup of $G = \mathrm{PSL}_2(q)$ isomorphic to S_4 and $\mathcal{M}$ be the set of conjugates of M in G on which G acts by conjugation. Then the primitive action of G on $\mathcal{M}$ has*

non-trivial orbits of lengths $3, 4, 6, 8, 12$ *and* 24*, respectively. In the case where* $q = p \equiv \pm 1 \pmod 8$ *but* $q = p \not\equiv \pm 1 \pmod{12}$ *and* $q = p \not\equiv \pm 1 \pmod{16}$*. Then the primitive action of* G *on* $\mathcal{M}$ *has the following non-trivial orbit lengths:*

a) $\frac{1}{2}\left(\frac{q\mp 1}{8} - 1\right) + 1$ *orbits of length* 6*;* *b)* $\frac{1}{2}\left(\frac{q\pm 1}{6} - 1\right)$ *orbits of length* 8*;*

c) $\frac{3\left(\frac{3(q\mp 1)}{8} - 1\right) - \left(\frac{q\mp 1}{8} - 1\right) - 6}{4}$ *orbits of length* 12*;*

d) $\frac{\frac{q^3-q}{48} - \left[1 + 4\left(\frac{q\pm 1}{6} - 1\right) + 3\left(\frac{q\mp 1}{8} - 1\right) + 6 + 9\left(\frac{3(q\mp 1)}{8} - 1\right) - 3\left(\frac{q\mp 1}{8} - 1\right) - 18\right]}{24}$ *orbits of length* 24*.*

The proof of Theorem 1.1 stated in Section 1 follows from Corollaries 3.11, 3.20, 3.22, 3.25, 3.29 and 3.32.

Acknowledgments

The authors would like to thank Amin Saeidi and Seiran Zandi for their comments and suggestions which improved significantly the quality and presentation of the paper.

This work is based on the research supported by the National Research Foundation of South Africa (Grant Numbers 106071 and 120846).

References

[1] E. F. Assmus, Jr and J. D. Key, *Designs and their Codes*, Cambridge: Cambridge University Press, 1992. Cambridge Tracts in Mathematics, **103**, (Second printing with corrections, 1993).

[2] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Comput.*, **24** (1997) 235–265.

[3] P. J. Cameron, H. R. Maimani, G. R. Omidi and B. Tayfeh-Rezaie, 3-Designs from $\mathrm{PSL}_2(q)$, *Discrete Math.*, **306** (2006) 3063–3073.

[4] M. R. Darafsheh, Designs from the group $\mathrm{PSL}_2(q)$, q even, *Des. Codes Cryptogr.*, **39** (2006) 311–316.

[5] L. E. Dickson, *Linear groups with an exposition of the Galois field theory*, Dover Publications, Inc., New York, 1958.

[6] J. D. Dixon and B. Mortimer, *Permutation Groups*, Springer-Verlag New York Inc., 1996.

[7] T. Fritzsche, The depth of subgroups of $\mathrm{PSL}_2(q)$, *J. Algebra*, **381** (2013) 37–53.

[8] M. Giudici, Maximal subgroups of almost simple groups with socle $\mathrm{PSL}_2(q)$, arXiv:math/0703685 [math.GR](2007), http://adsabs.harvard.edu/abs/2007math......3685G.

[9] J. D. Key and J. Moori, Designs, codes and graphs from the Janko groups J_1 and J_2, *J. Combin. Math and Combin. Comput.*, **40** (2002) 143–159.

[10] J. D. Key and J. Moori, Codes, Codes, designs and graphs from the Janko groups J_1 and J_2, *J. Combin. Math and Combin. Comput.*, **40** (2002) 143-159.

[11] J. D. Key and J. Moori, Designs from maximal subgroups and conjugacy classes of finite simple groups, *J. Combin. Math and Combin. Comput.*, **99** (2016) 41– 60.

[12] X. Mbaale and B. G. Rodrigues, *Symmetric* 1*-designs from* $\mathrm{PGL}_2(q)$*, for* q *an odd prime power*, Glasniki Mathematicki. To appear.

[13] J. Moori, Finite groups, designs and codes. Information security, coding theory and related combinatorics, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., **29**, IOS, Amsterdam, (2011) 202–230.

[14] J. Moori, Designs and Codes from $PSL_2(q)$, Group theory, combinatorics, and computing, Contemp. Math., *Amer. Math. Soc.*, Providence, RI,**611** 137–149 (2014).

[15] J. Moori and A. Saeidi, Some designs invariant under the Suzuki groups, *Util. Math.*, **109** (2018) 105–114.

[16] J. Moori and A. Saeidi, Constructing some designs invariant under $PSL_2(q)$, q even, *Commun. Algebra*, **46** (2018) 160–166.

[17] M. Suzuki, *Group Theory I*, Springer-Verlag, New York, 1982.

[18] R. A. Wilson, *The finite simple groups*, London: Springer-Verlag London Ltd., Graduate Texts in Mathematics, **251** 2009.

Xavier Mbaale

School of Mathematics, Statistics and Computer Science, University of KwaZulu-Natal, Durban 4000, South Africa

Email: xavier@aims.ac.za

Bernardo G. Rodrigues

Department of Mathematics and Applied Mathematics, University of Pretoria, Hatfield 0028, Pretoria, South Africa

Email: bernardo.rodrigues@up.ac.za

http://dx.doi.org/10.22108/toc.2020.123692.1740