AUT Journal of Mathematics and Computing

AUT J. Math. Comput., 4(1) (2023) 47-55
https://doi.org/10.22060/AJMC.2022.21877.1117

Original Article

Designs from maximal subgroups and conjugacy classes of $\mathrm{PSL}(2, q)$, q odd

Xavier Mbaale[a], Bernardo G. Rodrigues[b], Seiran Zandi*[c]

[a] *Department of Mathematics and Statistics, University of Zambia, Lusaka, Zambia*
[b] *Department of Mathematics and Applied Mathematics, University of Pretoria, Hatfield 0028, South Africa*
[c] *Farzanegan 1 High School, Sanandaj, Kurdistan, Iran*

ABSTRACT: In this paper, using a method of construction of 1-designs which are not necessarily symmetric, introduced by Key and Moori, we determine a number of 1-designs with interesting parameters from the maximal subgroups and the conjugacy classes of elements of the group $PSL(2, q)$ for q a power of an odd prime.

Review History:

Received:23 October 2022
Revised:30 December 2022
Accepted:31 December 2022
Available Online:01 February 2023

Keywords:

Linear group
Design
Conjugacy class
Maximal subgroup
Primitive permutation representation

AMS Subject Classification (2010):

20D05; 05E15; 05E20

(*Dedicated to Professor Jamshid Moori*)

1. Introduction

The study of symmetric designs invariant under primitive representations of finite simple groups has by now a vast literature. However, for some time now the investigation of properties of self-dual symmetric 1-design invariant under primitive groups has gained much interest given its connection with the study of linear codes, regular graphs and other combinatorial configurations. The results presented by J. D. Key and J. Moori in [8] paved the way for new explorations: for examples of applications of these results to individual simple groups, see ([8, 10, 13, 15, 16, 17, 18]), and for illustrations of applications to some classes of finite simple groups, see ([19, 20, 22, 21]). These results allowed among other things for the examination of questions such as: given the primitive permutation representations of

*Corresponding author.
E-mail addresses: xavier@aims.ac.za, bernardo.rodrigues@up.ac.za, seiran.zandi@gmail.com

the simple group $\mathrm{PSL}(2,q)$ what are the parameters of the 1-designs that admit $\mathrm{PSL}(2,q)$ as an automorphism group, acting primitively on points and on blocks?

Using the methods presented in [8], Darafsheh [3] constructed designs invariant under $\mathrm{PSL}(2,q)$, for q even and a pair of its maximal subgroups of dihedral type.

In [12], the first and second authors considered all conjugacy classes of maximal subgroups of $\mathrm{PSL}(2,q)$ for $q=p^n$, where p is an odd prime and, using results of [8] constructed all primitive, self-dual and symmetric 1-designs that admit $\mathrm{PSL}(2,q)$ as a permutation group of automorphisms. The said article completed the construction of $\mathrm{PSL}(2,q)$-invariant designs obtained using the conjugacy classes of maximal subgroups of $\mathrm{PSL}(2,q)$.

However, in [9] J D Key and J Moori outlined a construction of 1-designs using a maximal subgroup say M of a finite simple group G and a conjugacy class in G of some element $x \in M$. This construction allowed for the determination of parameters of 1-designs (not necessarily symmetric) invariant under finite simple groups. In particular, in [21] Moori and Saeidi, using results of [8] and [9] constructed $\mathrm{PSL}(2,q)$-invariant designs for $q>2$ a power of 2 for the remaining maximal subgroups not considered in [3]. In [13] and [14], Moori applied results of [9] to construct designs and codes from some maximal subgroups of $\mathrm{PSL}(2,q)$, for some prime powers of q.

For $q=p^n \geq 5$ where p is an odd prime, the present article addresses the question of the determination of $\mathrm{PSL}(2,q)$-invariant 1-designs (not necessarily symmetric) using the construction method presented in [9] and thus completing the study begun in [13] and [14].

Our notation for designs is as in [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 set $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$. If the ordered pair $(p,B) \in \mathcal{I}$, then we say that p is incident with B. It is often convenient to assume that the blocks in $\mathcal{B}$ are subsets of $\mathcal{P}$ so $(p,B) \in \mathcal{I}$ 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 $v=|\mathcal{P}|$. We say that $\mathcal{D}$ is symmetric if it has the same number of points and blocks.

2. Preliminaries

The aim of this section is to collect some facts and results about $\mathrm{PSL}(2,q)$, q odd and its maximal subgroups that will be applied in the sequel. For more details we refer the reader to [4, 6, 11]. Throughout this paper, let $G=\mathrm{PSL}(2,q)$ where $q=p^n \geq 5$ and p is an odd prime.

Theorem 2.1. *The maximal subgroups of G, up to conjugacy, are*

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

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

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

(4) $\mathrm{PSL}(2,q_0)$, *for* $q=q_0^r$ *where r is an odd prime power;*

(5) $PGL(2,q_0)$, *for* $q=q_0^2$ *(two conjugacy classes);*

(6) 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);*

(7) A_4, *for* $q=p \equiv \pm 3 \pmod 8$, $q>3$;

(8) S_4, *for* $q=p \equiv \pm 1 \pmod 8$ *or* $q=p^2$ *and* $3<p \equiv \pm 3 \pmod 8$ *(two conjugacy classes).*

Proof. See [11, Corollary 2.2]. □

Notation. We use the following notation throughout the rest of the paper. Let $t_1=(q-1)/2$, $t_2=(q+1)/2$ and $t_3=p^n$. We denote by $\mathcal{B}_1$ the set of all elementary abelian subgroups of G of order t_1 and $\mathcal{B}_i$ the set of all cyclic subgroups of G of order t_i for $i=2,3$.

Proposition 2.2. *Let $\mathcal{B}_i$ be as above, and suppose that $B_i \in \mathcal{B}_i$ are chosen arbitrarily for $1 \leq i \leq 3$. Then*

(i) *every element of $\mathcal{B}_i$ is a Hall subgroup of G; in particular every two elements of $\mathcal{B}_j$ for a fixed j are conjugate in G;*
(ii) $N_G(B_1)=B_1{:}2 \cong D_{q-1}$;
(iii) $N_G(B_2)=B_2{:}2 \cong D_{q+1}$;
(iv) $N_G(B_3)=B_3{:}(\frac{q-1}{2})$.

Proof. All parts follow from [11, Theorem 2.1]. □

For the rest of the paper, let x be a non-trivial element.

Lemma 2.3. *Assume that $B_i \in \mathcal{B}_i$ for $1 \leq i \leq 3$ and $x \in G$ is non-trivial. Then the following statements hold.*

(i) if $x \in B_1$ and $o(x) \neq 2$ then $|x^G| = q(q+1)$;
(ii) if $x \in B_2$ and $o(x) \neq 2$ then $|x^G| = q(q-1)$;
(iii) if $x \in B_3$ then $|x^G| = \dfrac{(q-1)(q+1)}{2}$;
(iv) for $o(x) = 2$ we have
  (a) if 2 divides $\dfrac{q-1}{2}$ then $|x^G| = \frac{q(q+1)}{2}$;
  (b) if 2 divides $\dfrac{q+1}{2}$ then $|x^G| = \frac{q(q-1)}{2}$.

Proof. We use the orders of centralizers of elements in $\mathrm{PSL}(2, q)$. □

Remark 2.4. *Let G be an arbitrary group and H be a subgroup of G. The subgroup H is called a trivial intersection subgroup, for short TI-subgroup if for every $g \in G$, $H \cap H^g = 1$ or $H \cap H^g = H$.*

Lemma 2.5. *All subgroups in $\mathcal{B}_i$, $i \in \{1, 2, 3\}$, are TI-subgroups in G.*

Proof. It follows from [5, Theorem 1.3]. □

Lemma 2.6. *Let $G = \mathrm{PSL}(2, q)$, $q = p^n$ and p an odd prime. Then there are two conjugacy classes of elements of order p and one conjugacy class of involutions.*

Proof. See [4] and [6]. □

Lemma 2.7. *Let G be a $PGL(2, q)$, $q = p^n$ and p an odd prime.*

(i) There are two conjugacy classes of elements of order 2. One class consists of $\frac{q(q-1)}{2}$, and the other class consists of $\frac{q(q+1)}{2}$.
(ii) All elements of order p are conjugate.

Proof. We refer the reader to [4] and [6]. □

Lemma 2.8. *Let G be an arbitrary group and H be a subgroup of G. Then for each $x \in G$, $x^G \cap H$ is a union of conjugacy classes of H.*

Proof. The proof is straightforward. □

Lemma 2.9. *Let G be a dihedral group of order $2n$.*

(i) if $2 \mid n$ then the number of involutions in G is equal to $n + 1$.
(ii) if $2 \nmid n$ then the number of involutions in G is equal to n.
(iii) if $o(x) = t$ and $2 \neq t \mid n$ then $x^G = \{x, x^{-1}\}$.

Proof. The result follows from the structure of dihedral groups. □

Lemma 2.10. *Let $q = p^n$ and p be an odd prime.*

(1) if $2 \mid \frac{q-1}{2}$ then $2 \nmid \frac{q+1}{2}$.
(2) if $2 \mid \frac{q+1}{2}$ then $2 \nmid \frac{q-1}{2}$.

Proof. The proof is straightforward. □

Lemma 2.11. *If $q = q_0^2$, q odd, then $\frac{q_0 \pm 1}{2} \mid \frac{q-1}{2}$.*

Proof. The proof is straightforward. □

3. Constructing designs using Method 2

In this section, we determine the parameters of all possible designs obtained by Method 2 from $\mathrm{PSL}(2,q)$, q odd. The following result is the method that we use to construct our non-symmetric 1-designs.

Lemma 3.1. ***(Method** 2) Let S be a finite simple group, M a maximal subgroup of S and x^S a conjugacy class of elements of order n in S such that $M \cap x^S \neq \emptyset$. Let $B = \{(M \cap x^S)^y | y \in S\}$. Then we have a $1-(|x^S|, |M \cap x^S|, \chi_M(x))$ design $\mathcal{D}$. The group S acts as an automorphism group on $\mathcal{D}$, primitive on blocks and transitive (not necessarily primitive) on points of $\mathcal{D}$.*

Proof. See [13, Theorem 12]. □

In Lemma 3.1 we consider $S = \mathrm{PSL}(2,q)$, for q odd. Let us denote a design obtained using Lemma 3.1, $\mathcal{D}(x, M)$. The following lemma shows that if we obtain two of the three parameters of the design, then the remaining parameter is directly computed.

Lemma 3.2. *[22, Lemma 4.2] Let $\mathcal{D} = (v, k, \lambda)$ be a design obtained by Lemma 3.1. Then $|G{:}M| = \lambda v/k$.*

Definition 3.3. *Let H be a subgroup of G. We say that H controls G-fusion in itself if each pair of elements in H which are conjugate in G are also conjugate in H. Equivalently, if for $x \in H$ we have $x^G \cap H = x^H$.*

Lemma 3.4. *Let G be a finite simple group with a maximal subgroup M and assume that M controls G-fusion in itself. Then the designs constructed by Lemma 3.1 have parameters $1-(|x^G|, |x^M|, |\mathcal{C}_G(x) : \mathcal{C}_M(x)|)$, where x is a non-trivial element of M.*

Proof. See [22, Proposition 3.4]. □

By Lemma 3.4, if M is a maximal subgroup of G that controls G-fusion in itself then the parameters of designs given by Lemma 3.1 can be easily computed.

Definition 3.5. *Let $H \leq G$ and k be a positive integer. We define*

$$\mathrm{cn}_H^G(k) := |\{x^G | x \in H, o(x) = k\}|.$$

Also we write $\mathrm{cn}_H(k) := \mathrm{cn}_H^H(k)$. It is easy to see that if $\mathrm{cn}_H^G(k) = \mathrm{cn}_H(k)$ then for every $x \in H$ with $o(x) = k$ we have $x^G \cap H = x^H$.

3.1. Maximal subgroups of type $C_p^n{:}C_{\frac{q-1}{2}}$

Lemma 3.6. *Let M be a maximal subgroup of G of type (1) in Theorem 2.1. Suppose that $x \in M$ and the order of x is p. Then $x^G \cap M = x^M$.*

Proof. Since a p-Sylow subgroup of M is normal and elementary abelian, the number of elements of order p in M equals $q-1$. On the other hand, $|\mathcal{C}_M(x)| = q$. Then there are two conjugacy classes of elements of order p in M. Also by Lemma 2.6, the number of conjugacy classes of elements of order p in G is 2. Hence $\mathrm{cn}_M^G(p) = \mathrm{cn}_M(p) = 2$ and the result follows. □

Lemma 3.7. *Let M be a maximal subgroup of G of type (1) in Theorem 2.1. Suppose that $x \in M$ where $2 \neq o(x) \mid \frac{q-1}{2}$. Then $|x^G \cap M| = 2|x^M|$.*

Proof. Assume that $y \in x^G \cap M$ and $o(x) = t$ where $t \mid \dfrac{q-1}{2}$. Clearly, the elements x and y are conjugate in G. So there exist $g \in G$ such that $y = x^g$. Let H and H' be two cyclic subgroups of M of order $\frac{q-1}{2}$ such that $x \in H$ and $y \in H'$. Since M is a solvable group, all Hall subgroups of the same order are conjugate in M. Thus, there is an element $m \in M$ such that $H' = H^m$. So we have that $y \in H^m \cap H^g$. Therefore, $mg^{-1} \in N_G(H) = H : \langle j \rangle \cong D_{q-1}$ where $j \notin M$ of order 2. Hence, there are $m, m' \in M$ and $h, h' \in H$ such that $g = hm$ or $g = h'jm'$. Thus, $y = x^g = x^{hm} = x^m$ or $y = x^g = x^{h'jm'} = (x^j)^m$. Now, using Lemma 2.8 we obtain $x^G \cap M = x^M \cup (x^j)^M$. □

Theorem 3.8. *Let M be a maximal subgroup of type (1) in Theorem 2.1,*

(i) If $o(x) = p$ then $|x^M| = |x^G \cap M| = \frac{q-1}{2}$;

(ii) If $2 \neq o(x) = t$ and $t | \frac{q-1}{2}$ then $|x^G \cap M| = 2|x^M| = 2q$.

(iii) If $o(x) = 2$ and $2 \mid \frac{q-1}{2}$ then $|x^G \cap M| = |x^M| = q$ by Lemma 2.6.

Proof. The first and second statements follow immediately from Lemma 3.7. Now, assume that $o(x) = 2$. Since $\mathrm{cn}_M^G(2) = \mathrm{cn}_M(2) = 1$, then $x^G \cap M = x^M$. □

3.2. Maximal subgroups of types D_{q-1} and D_{q+1}

For M a maximal subgroup of the type $D_{q\mp1}$, the next two results allow for the determination of the parameters of the designs obtained by direct application of Lemma 3.1.

Lemma 3.9. *Let M be a maximal subgroup of G of type $D_{q\mp1}$where $2 \nmid \frac{q\mp1}{2}$. Then M controls G-fusion in itself.*

Proof. Assume that $x, y \in M$ are non-trivial elements of order $t \neq 2$. Suppose $t \mid \frac{q\mp1}{2}$ and $x = y^g$ where $g \in G$. We claim that x and y are conjugate in M. Since a subgroup of order $\frac{q\mp1}{2}$ is normal in M, then there is a unique subgroup H of order t in G with $x, y \in H$. On the other hand $x = y^g$ so $x \in H^g$. Therefore $x \in H \cap H^g$. Now by Lemma 2.5, we have $H = H^g$ which implies that $g \in N_G(H) = M$ and the result follows. Finally, assume that $t = 2$. Since G and M have one conjugacy class of elements of order 2 the result follows. □

Theorem 3.10. *Let M be a maximal subgroup of G of type $D_{q\mp1}$. Then for $x \in M$ we have the following*

(i) *if $2 \neq o(x)$, then $x^G \cap M = x^M$,*

(ii) *if $o(x) = 2$ and $2 \nmid \dfrac{q\mp1}{2}$ then $|x^G \cap M| = \dfrac{q\mp1}{2}$.*

(iii) *if $o(x) = 2$ and $2 \mid \dfrac{q-1}{2}$ then $|x^G \cap M| = \dfrac{q+1}{2}$.*

(iv) *if $o(x) = 2$ and $2 \mid \dfrac{q+1}{2}$ then $|x^G \cap M| = \dfrac{q+3}{2}$.*

Proof. By a Lemma 3.9, we have $x^G \cap M = x^M$ for $x \in M$ and $o(x) \neq 2$. Now assume that $o(x) = 2$. Since all elements of order 2 in G are conjugate, the number of elements in $x^G \cap M$ equals the number of elements of order 2 in M. The result follows now by Lemma 2.9. □

3.3. Maximal subgroups of G of type $\mathrm{PSL}(2, q_0)$

In this section, we deal with the maximal subgroups of type $\mathrm{PSL}(2, q_0)$ where $q = q_0^r$, r is an odd prime.

Lemma 3.11. *Let $M \cong \mathrm{PSL}(2, q_0)$, where $q = q_0^r$, be a maximal subgroup of G. Then M controls G-fusion in itself.*

Proof. By Lemma 2.6, $\mathrm{cn}_M^G(2) = \mathrm{cn}_M(2) = 1$ and $\mathrm{cn}_M^G(p) = \mathrm{cn}_M(p) = 2$. Then for all elements of order 2 and p respectively, the statement holds. Now suppose that $2 \neq o(x) = t \mid \frac{q_0\mp1}{2}$ and $y \in x^G \cap M$. Then there is $g \in G$ such that $y = x^g$. Since $o(x) = o(y) = t$ and t divides $\frac{q_0\mp1}{2}$, there are two cyclic subgroups, say H_1 and K_1 of order $\frac{q_0\mp1}{2}$ such that $x \in H_1$ and $y \in K_1$. By Lemma 2.2, there is an element $m \in M$ such that $K_1 = H_1^m$, and thus $y \in H_1^m$. It is clear that $\frac{q_0\mp1}{2} \mid \frac{q\mp1}{2}$. So there is a cyclic subgroup H such that $H_1 \leq H$. Clearly, $y \in H^m \cap H^g$. Therefore $H^g = H^m$ from Lemma 2.5. Hence $mg^{-1} \in N_G(H) = H : \langle j \rangle$ for some $j \in M$. Then we have $mg^{-1} = j^i h$ for some $h \in H$ and $i \in \{0, 1\}$. Since $j \in M$ and H is cyclic, we obtain $y = x^g = x^{h^{-1}j^i m} = x^{j^i m} = x^{m'}$. We conclude that x and y are conjugate in M. □

Theorem 3.12. *Let $M \cong \mathrm{PSL}(2, q_0)$, where $q = q_0^r$, be a maximal subgroup of G. We have*

(i) *for $o(x) = 2$*

  (*) *if $2 \mid \frac{q_0-1}{2}$ then $|x^G \cap M| = |x^M| = \frac{q_0(q_0+1)}{2}$;*

  (**) *if $2 \mid \frac{q_0+1}{2}$ then $|x^G \cap M| = |x^M| = \frac{q_0(q_0-1)}{2}$;*

(ii) *if $o(x) = p$ then $|x^G \cap M| = |x^M| = \frac{(q_0+1)(q_0-1)}{2}$;*

(iii) *if $2 \neq o(x) \mid \frac{q_0-1}{2}$ then $|x^G \cap M| = |x^M| = q_0(q_0 + 1)$;*

(iv) *if $2 \neq o(x) \mid \frac{q_0+1}{2}$ then $|x^G \cap M| = |x^M| = q_0(q_0 - 1)$.*

Proof. The proof is straightforward using Lemma 3.11 and Lemma 2.3. □

3.4. Maximal subgroups of G of type $PGL(2, q_0)$

In this section, we consider the maximal subgroups of type $PGL(2, q_0)$ where $q = q_0^2$.

Lemma 3.13. *Let $M \cong PGL(2, q_0)$, where $q = q_0^2$, be a maximal subgroup of G. Then we have the following statements:*

(i) if $o(x) = 2$ then $|x^G \cap M| = q_0^2$;
(ii) if $o(x) \neq 2$ then $x^G \cap M = x^M$.

Proof. (i) Since all involutions are conjugate in G, then $|x^G \cap M|$ equals the number of involutions in M. By Lemma 2.7, M has two conjugacy classes of involutions of orders $\frac{q_0(q_0-1)}{2}$ and $\frac{q_0(q_0+1)}{2}$, respectively. Then $|x^G \cap M| = \frac{q_0(q_0-1)}{2} + \frac{q_0(q_0+1)}{2} = q_0^2$.

(ii) Since all elements of order p are conjugate in M, we conclude that $x^G \cap M = x^M$ where $o(x) = p$. The arguments used for the proof of Lemma 3.11 work for the remaining cases.

□

Theorem 3.14. *Let $M \cong PGL(2, q_0)$, where $q = q_0^2$, be a maximal subgroup of G. We have*

(i) if $o(x) = 2$ then $|x^G \cap M| = q_0^2$;
(ii) if $o(x) = p$ then $|x^G \cap M| = |x^M| = (q_0 + 1)(q_0 - 1)$;
(iii) if $2 \neq o(x) \mid q_0 - 1$ then $|x^G \cap M| = |x^M| = q_0(q_0 + 1)$;
(iv) if $2 \neq o(x) \mid q_0 + 1$ then $|x^G \cap M| = |x^M| = q_0(q_0 - 1)$.

Proof. The proof follows straightforwardly using Lemma 3.13 and Lemma 2.3. □

3.5. Maximal subgroups of types A_5, A_4 and S_4

In this section, we deal with the remaining types of maximal subgroups of G.

Lemma 3.15. *Let M be a maximal subgroup of G of type A_5. Then*

(i) if $o(x) = 2$, then $|x^G \cap M| = |x^M| = 15$;
(ii) if $o(x) = 3$, then $|x^G \cap M| = |x^M| = 20$;
(iii) if $o(x) = 5$, then $|x^G \cap M| = |x^M| = 12$.

Proof. Since $\mathrm{cn}_M^G(2) = \mathrm{cn}_M(2) = 1$ and $\mathrm{cn}_M(3) = 1$, then $x^G \cap M = x^M$. It is known that A_5 has two conjugacy classes of elements of order 5. Also it is easy to check that $\mathrm{PSL}(2, q)$ has two conjugacy classes of elements of order 5 where G has elements of order 5. We conclude that $\mathrm{cn}_M^G(5) = \mathrm{cn}_M(5) = 2$ for $M \cong A_5$. Now it is a simple matter to compute the number of x^M for $x \in M$. □

Lemma 3.16. *Assume that $M \cong A_4$ is a maximal subgroups of G and $x \in M$. Then*

(i) if $o(x) = 3$, then $|x^G \cap M| = 2|x^M| = 8$;
(ii) if $o(x) = 2$, then $|x^G \cap M| = 3$.

Proof. If G has a maximal subgroup of type A_4 then $3 < q = p \equiv \pm 3 \pmod 8$.

(i) By the structure of A_4 and G, we have $\mathrm{cn}_M^G(3) = 1$ and $\mathrm{cn}_M(3) = 2$. We conclude that the number of elements of order 3 in $x^G \cap M$ equals the number of all elements of order 3 in M. Since M has two conjugacy classes of elements of order 3, so $|x^G \cap M| = 2|x^M|$.

(ii) Assume that $o(x) = 2$. Since all elements of order 2 are conjugate in G. Then the number of involutions in $x^G \cap M$ equals the number of elements of order 2 in M. But there are 3 elements of order 2 in M, and so $|x^G \cap M| = 3$.

□

Lemma 3.17. *Suppose that $M \cong S_4$ is a maximal subgroups of G and $x \in M$. Then*

(i) if $o(x) = 3$, then $|x^G \cap M| = |x^M| = 8$;
(ii) if $o(x) = 4$, then $|x^G \cap M| = |x^M| = 6$;
(ii) if $o(x) = 2$, then $|x^G \cap M| = 9$.

Proof. Since $\mathrm{cn}_M(3) = 1$ and $\mathrm{cn}_M(4) = 1$, then $x^G \cap M = x^M$. By the structure of M, the statements (i) and (ii) hold. Now assume that $o(x) = 2$. Since all involutions are conjugate in G, then $|x^G \cap M|$ equals the number of elements of order 2 in M. By the structure of M, we easily obtain that the number of all elements of order 2 in M is 9. So $|x^G \cap M| = 9$. □

3.6. Main Theorem

By using results in Section 2 and Subsections 3.1, 3.2, 3.3, 3.4 and 3.5, we are able to state and prove our main result in Theorem 3.18. This subsection ends with Table 1, which gives the parameters of the constructed designs.

Theorem 3.18. *Let $M_i, (1 \leq i \leq 8)$ be a maximal subgroup of G of type (i) as in Theorem 2.1 and let $x \in M_i$ be a non-trivial element. Then the parameters of all non-trivial 1-designs $\mathcal{D}(x, M_i) = (v, k, \lambda)$ are as given in Table 1.*

Proof. By Lemma 3.1, $\mathcal{D}(x, M_i) = (|x^G|, |M_i \cap x^G|, \chi_{M_i}(x))$. The first parameter $|x^G|$ is given by Lemma 2.3. By the results of this section, either $|M_i \cap x^G|$ or $\chi_{M_i}(x)$ are known, and the other can be directly computed using Lemma 3.2. The proof of the theorem is now complete. ☐

Table 1: Non-trivial designs from $G = \mathrm{PSL}(2, q)$, q odd, using construction Method 2

Max	$t = o(x)$	$v = \|x^G\|$	$k = \|M \cap x^G\|$	$\lambda = \chi_{M_i}(x)$
$M_1 \cong C_p^n : C_{\frac{q-1}{2}}$	$t = 2 \mid \frac{q-1}{2}$	$\frac{q(q+1)}{2}$	q	2
$M_1 \cong C_p^n : C_{\frac{q-1}{2}}$	$t = p$	$\frac{(q-1)(q+1)}{2}$	$\frac{q-1}{2}$	1
$M_1 \cong C_p^n : C_{\frac{q-1}{2}}$	$2 \neq t \mid \frac{q-1}{2}$	$q(q+1)$	$2q$	2
$M_2 \cong D_{q-1}$	$t = 2 \mid \frac{q-1}{2}$	$\frac{q(q+1)}{2}$	$\frac{q+1}{2}$	$\frac{q+1}{2}$
$M_2 \cong D_{q-1}$	$t = 2 \nmid \frac{q-1}{2}$	$\frac{q(q-1)}{2}$	$\frac{q-1}{2}$	$\frac{q+1}{2}$
$M_2 \cong D_{q-1}$	$2 \neq t \mid \frac{q-1}{2}$	$q(q+1)$	2	1
$M_3 \cong D_{q+1}$	$t = 2 \mid \frac{q+1}{2}$	$\frac{q(q-1)}{2}$	$\frac{q+3}{2}$	$\frac{q+3}{2}$
$M_3 \cong D_{q+1}$	$t = 2 \nmid \frac{q+1}{2}$	$\frac{q(q+1)}{2}$	$\frac{q+1}{2}$	$\frac{q-1}{2}$
$M_3 \cong D_{q+1}$	$2 \neq t \mid \frac{q+1}{2}$	$q(q-1)$	2	1
$M_4 \cong \mathrm{PSL}(2, q_0)$	$t = 2 \mid \frac{q-1}{2}$	$\frac{q(q+1)}{2}$	$\frac{q_0(q_0+1)}{2}$	$\frac{q-1}{q_0-1}$
$M_4 \cong \mathrm{PSL}(2, q_0)$	$t = 2 \mid \frac{q+1}{2}$	$\frac{q(q-1)}{2}$	$\frac{q_0(q_0-1)}{2}$	$\frac{q+1}{q_0+1}$
$M_4 \cong \mathrm{PSL}(2, q_0)$	$t = p$	$\frac{(q-1)(q+1)}{2}$	$\frac{(q_0-1)(q_0+1)}{2}$	$\frac{q}{q_0}$
$M_4 \cong \mathrm{PSL}(2, q_0)$	$t \mid \frac{q-1}{2}$	$q(q+1)$	$q_0(q_0+1)$	$\frac{q-1}{q_0-1}$
$M_4 \cong \mathrm{PSL}(2, q_0)$	$t \mid \frac{q+1}{2}$	$q(q-1)$	$q_0(q_0-1)$	$\frac{q+1}{q_0+1}$
$M_5 \cong PGL(2, q_0)$	$t = 2 \mid \frac{q-1}{2}$	$\frac{q(q+1)}{2}$	q_0^2	q_0
$M_5 \cong PGL(2, q_0)$	$t = p$	$\frac{(q-1)(q+1)}{2}$	$(q_0-1)(q_0+1)$	q_0
$M_5 \cong PGL(2, q_0)$	$2 \neq t \mid q_0 - 1$	$q(q+1)$	$q_0(q_0+1)$	$\frac{q_0+1}{2}$
$M_5 \cong PGL(2, q_0)$	$2 \neq t \mid q_0 + 1$	$q(q+1)$	$q_0(q_0-1)$	$\frac{q_0-1}{2}$
$M_6 \cong A_5$	$t = 2 \mid \frac{q-1}{2}$	$\frac{q(q+1)}{2}$	15	$\frac{q-1}{4}$
$M_6 \cong A_5$	$t = 2 \mid \frac{q+1}{2}$	$\frac{q(q-1)}{2}$	15	$\frac{q+1}{4}$
$M_6 \cong A_5$	$t = 3 \mid \frac{q-1}{2}$	$q(q+1)$	20	$\frac{q-1}{6}$
$M_6 \cong A_5$	$t = 3 \mid \frac{q+1}{2}$	$q(q-1)$	20	$\frac{q+1}{6}$
$M_6 \cong A_5$	$t = 3 \mid q$	$\frac{(q-1)(q+1)}{2}$	20	$\frac{q}{3}$
$M_6 \cong A_5$	$t = 5 \mid \frac{q-1}{2}$	$q(q+1)$	12	$\frac{q-1}{10}$
$M_6 \cong A_5$	$t = 5 \mid \frac{q+1}{2}$	$q(q-1)$	12	$\frac{q+1}{10}$
$M_7 \cong A_4$	$t = 2 \mid \frac{q-1}{2}$	$\frac{q(q+1)}{2}$	3	$\frac{q-1}{4}$
$M_7 \cong A_4$	$t = 2 \mid \frac{q+1}{2}$	$\frac{q(q-1)}{2}$	3	$\frac{q+1}{4}$
$M_7 \cong A_4$	$t = 3 \mid \frac{q-1}{2}$	$q(q+1)$	8	$\frac{q-1}{3}$
$M_7 \cong A_4$	$t = 3 \mid \frac{q+1}{2}$	$q(q-1)$	8	$\frac{q+1}{3}$
$M_8 \cong S_4$	$t = 2 \mid \frac{q-1}{2}$	$\frac{q(q+1)}{2}$	9	$\frac{3(q-1)}{8}$
$M_8 \cong S_4$	$t = 2 \mid \frac{q+1}{2}$	$\frac{q(q-1)}{2}$	9	$\frac{3(q+1)}{8}$
$M_8 \cong S_4$	$t = 3 \mid \frac{q-1}{2}$	$q(q+1)$	8	$\frac{q-1}{6}$
$M_8 \cong S_4$	$t = 3 \mid \frac{q+1}{2}$	$q(q-1)$	8	$\frac{q+1}{6}$
$M_8 \cong S_4$	$t = 4 \mid \frac{q-1}{2}$	$\frac{q(q+1)}{2}$	6	$\frac{q-1}{4}$
$M_8 \cong S_4$	$t = 4 \mid \frac{q+1}{2}$	$\frac{q(q-1)}{2}$	6	$\frac{q+1}{4}$

Acknowledgements

The authors wish to thank the both referees for their comments and suggestions, The second author acknowledges support by the National Research Foundation of South Africa (Grant Number 120846).

References

[1] E. F. Assmus, Jr. and J. D. Key, *Designs and their codes*, vol. 103 of Cambridge Tracts in Mathematics, Cambridge University Press, Cambridge, 1992.

[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, $\mathbb{ATLAS}$ *of finite groups*, Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

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

[4] L. E. Dickson, *Linear groups: With an exposition of the Galois field theory*, Dover Publications, Inc., New York, 1958. With an introduction by W. Magnus.

[5] T. Fritzsche, *The depth of subgroups of* $\mathrm{PSL}(2,q)$, J. Algebra, 349 (2012), pp. 217–233.

[6] B. Huppert, *Endliche Gruppen. I*, Die Grundlehren der mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin-New York, 1967.

[7] I. M. Isaacs, *Character theory of finite groups*, Dover Publications, Inc., New York, 1994. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423 (57 #417)].

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

[9] ——, *Designs from maximal subgroups and conjugacy classes of finite simple groups*, J. Combin. Math. Combin. Comput., 99 (2016), pp. 41–60.

[10] J. D. Key, J. Moori, and B. G. Rodrigues, *On some designs and codes from primitive representations of some finite simple groups*, J. Combin. Math. Combin. Comput., 45 (2003), pp. 3–19.

[11] O. H. King, *The subgroup structure of finite classical groups in terms of geometric configurations*, in Surveys in combinatorics 2005, vol. 327 of London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, 2005, pp. 29–56.

[12] X. Mbaale and B. G. Rodrigues, *Symmetric 1-designs from* $\mathrm{PSL}_2(q)$*, for q a power of an odd prime*, Trans. Comb., 10 (2021), pp. 43–61.

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

[14] ——, *Designs and codes from* $PSL_2(q)$, in Group theory, combinatorics, and computing, vol. 611 of Contemp. Math., Amer. Math. Soc., Providence, RI, 2014, pp. 137–149.

[15] J. Moori and B. G. Rodrigues, *A self-orthogonal doubly even code invariant under* $M^cL:2$, J. Combin. Theory Ser. A, 110 (2005), pp. 53–69.

[16] ——, *Some designs and codes invariant under the simple group* Co_2, J. Algebra, 316 (2007), pp. 649–661.

[17] ——, *A self-orthogonal doubly-even code invariant under* M^cL, Ars Combin., 91 (2009), pp. 321–332.

[18] ——, *On some designs and codes invariant under the Higman-Sims group*, Util. Math., 86 (2011), pp. 225–239.

[19] J. Moori, B. G. Rodrigues, A. Saeidi, and S. Zandi, *Some symmetric designs invariant under the small Ree groups*, Comm. Algebra, 47 (2019), pp. 2131–2148.

[20] ——, *Designs from maximal subgroups and conjugacy classes of Ree groups*, Adv. Math. Commun., 14 (2020), pp. 603–611.

[21] J. Moori and A. Saeidi, *Constructing some designs invariant under* $PSL(2,q)$*, q even*, Commun. Algebra, 46 (2018), pp. 160–166.

[22] ———, *Some designs invariant under the Suzuki groups*, Util. Math., 109 (2018), pp. 105–114.

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

Please cite this article using:

Xavier Mbaale, Bernardo G. Rodrigues, Seiran Zandi, Designs from maximal subgroups and conjugacy classes of PSL$(2, q)$, q odd, AUT J. Math. Comput., 4(1) (2023) 47-55
DOI: https://doi.org/10.22060/AJMC.2022.21877.1117