3-designs from $\mathrm{PSL}(2, q)$

P. J. Cameron [a,1] H. R. Maimani [b,d] G. R. Omidi [b,c]
B. Tayfeh-Rezaie [b]

[a] *School of Mathematical Sciences, Queen Mary, University of London, U.K.*

[b] *Institute for Studies in Theoretical Physics and Mathematics (IPM), Iran*

[c] *Department of Mathematics, University of Tehran, Iran*

[d] *Department of Mathematics, Shahid Rajaee Teacher Training University, Iran*

Abstract

The group $\mathrm{PSL}(2, q)$ is 3-homogeneous on the projective line when q is a prime power congruent to 3 modulo 4 and therefore it can be used to construct 3-designs. In this paper, we determine all 3-designs admitting $\mathrm{PSL}(2, q)$ with block size not congruent to 0 and 1 modulo p where $q = p^n$.

Key words: t-designs, automorphism groups, projective special linear groups, subgroup lattices, Möbius function

1 Introduction

The group $\mathrm{PSL}(2, q)$ is 3-homogeneous on the projective line when q is a prime power congruent to 3 modulo 4. Therefore, a set of k-subsets of the projective line is the block set of a 3-$(q + 1, k, \lambda)$ design admitting $\mathrm{PSL}(2, q)$ for some λ if and only if it is a union of orbits of $\mathrm{PSL}(2, q)$. This simple observation has led different authors to use this group for constructing 3-designs, see for example [1–3,6,8–10]. All 3-designs with block sizes 4, 5, and 6 admitting $\mathrm{PSL}(2, q)$ as an automorphism group were completely determined [2,10]. Other authors have also obtained partial results for a variety of values of block size. In this paper, we investigate the existence of 3-designs with block size not congruent to 0 and 1 modulo p ($q = p^n$) with automorphism group $\mathrm{PSL}(2, q)$. In particular, when q is prime, we give a complete solution. We hope to settle the general problem in a forthcoming paper.

[1] Corresponding author, email: `p.j.cameron@qmul.ac.uk`.

2 Notation and Preliminaries

Let t, k, v, and λ be integers such that $0 \leq t \leq k \leq v$ and $\lambda > 0$. Let X be a v-set and $P_k(X)$ denote the set of all k-subsets of X. A t-(v, k, λ) *design* is a pair $\mathcal{D} = (X, D)$ in which D is a collection of elements of $P_k(X)$ (called *blocks*) such that every t-subset of X appears in exactly λ blocks. If D has no repeated blocks, then it is called *simple*. Here we are concerned only with simple designs. It is well known that a set of necessary conditions for the existence of a t-(v, k, λ) design is

$$\lambda\binom{v-i}{t-i} \equiv 0 \pmod{\binom{k-i}{t-i}}, \tag{1}$$

for $0 \leq i \leq t$. An *automorphism* of $\mathcal{D}$ is a permutation σ on X such that $\sigma(B) \in D$ for each $B \in D$. An *automorphism group* of $\mathcal{D}$ is a group whose elements are automorphisms of $\mathcal{D}$.

Let G be a finite group acting on X. For $x \in X$, the *orbit* of x is $G(x) = \{gx \mid g \in G\}$ and the *stabilizer* of x is $G_x = \{g \in G \mid gx = x\}$. It is well known that $|G| = |G(x)||G_x|$. Orbits of size $|G|$ are called *regular* and the others are called *non-regular*. If there is an $x \in X$ such that $G(x) = X$, then G is called *transitive*. The action of G on X induces a natural action on $P_k(X)$. If this latter action is transitive, then G is called *k-homogeneous*.

Let q be a prime power and let $X = GF(q) \cup \{\infty\}$. Then the set of all mappings

$$g: \ x \mapsto \frac{ax+b}{cx+d},$$

on X such that $a, b, c, d \in GF(q)$, $ad - bc$ is a nonzero square and $g(\infty) = a/c$, $g(-d/c) = \infty$ if $c \neq 0$, and $g(\infty) = \infty$ if $c = 0$, is a group under composition of mappings called *projective special linear group* and is denoted by $\mathrm{PSL}(2, q)$. It is well known that $\mathrm{PSL}(2, q)$ is 3-homogeneous if and only if $q \equiv 3 \pmod 4$. Note that $|\mathrm{PSL}(2, q)| = (q^3 - q)/2$. **Throughout this paper, we let q be a power of a prime p and congruent to $3 \pmod 4$.** Since $\mathrm{PSL}(2, q)$ is 3-homogeneous, a set of k-subsets is a 3-$(q + 1, k, \lambda)$ design admitting $\mathrm{PSL}(2, q)$ as an automorphism group if and only if it is a union of orbits of $\mathrm{PSL}(2, q)$ on $P_k(X)$. Thus, for constructing designs with block size k admitting $\mathrm{PSL}(2, q)$, we need to determine the sizes of orbits in the action of $\mathrm{PSL}(2, q)$ on $P_k(X)$.

Let $H \leq \mathrm{PSL}(2, q)$ and let define

$f_k(H) :=$ the number of k-subsets fixed by H,
$g_k(H) :=$ the number of k-subsets with the stabilizer group H.

Then we have

$$f_k(H) = \sum_{H \leq U \leq \mathrm{PSL}(2,q)} g_k(U). \tag{2}$$

We are mostly interested in finding g_k which help us directly to obtain the sizes of orbits. It is a fairly simple task to find f_k and then to use it to compute g_k. By Möbius inversion applied to (2), we have

$$g_k(H) = \sum_{H \leq U \leq \mathrm{PSL}(2,q)} f_k(U)\mu(H,U), \tag{3}$$

where μ is the Möbius function of the subgroup lattice of $\mathrm{PSL}(2,q)$.

For any subgroup H of $\mathrm{PSL}(2,q)$ we need to carry out the following:

(i) Find the sizes of orbits from the action of H on the projective line and then compute $f_k(H)$.
(ii) Calculate $\mu(H,U)$ for any overgroup U of H and then compute $g_k(H)$ using (3).

Note that if H and H' are conjugate, then $f_k(H) = f_k(H')$ and $g_k(H) = g_k(H')$.

In Section 4, we determine the action of subgroups of $\mathrm{PSL}(2,q)$ on the projective line. Section 5 is devoted to the Möbius function on the subgroup lattices of subgroups of $\mathrm{PSL}(2,q)$. We will compute f_k and g_k in Sections 6 and 7, respectively and then will use the results to find new 3-designs with automorphism group $\mathrm{PSL}(2,q)$ in Section 8.

The following useful lemma is trivial by (1).

Lemma 1 *Let B be a k-subset of the projective line, and let G be its stabilizer group under the action of* $\mathrm{PSL}(2,q)$. *Then $|G|$ divides $3\binom{k}{3}$.*

3 The subgroups of $\mathrm{PSL}(2,q)$

The subgroups of $\mathrm{PSL}(2,q)$ are well known and given in [4,7]. In the following theorems and lemmas we present a brief account on the structure of elements and subgroups of $\mathrm{PSL}(2,q)$. These information will be used in the subsequent sections.

Theorem 2 [4,7] *Let g be a nontrivial element in* $\mathrm{PSL}(2,q)$ *of order d and with f fixed points. Then $d = p$ and $f = 1$, $d|\frac{q+1}{2}$ and $f = 0$, or $d|\frac{q-1}{2}$ and $f = 2$.*

Theorem 3 **[4,7]** *The subgroups of* $\mathrm{PSL}(2,q)$ *are as follows.*

(i) $q(q\mp 1)/2$ *cyclic subgroups of order* d *where* $d|\frac{q\pm1}{2}$.
(ii) $q(q^2-1)/(4d)$ *dihedral subgroups of order* $2d$ *where* $d|\frac{q\pm1}{2}$ *and* $d>2$ *and* $q(q^2-1)/24$ *subgroups* D_4.
(iii) $q(q^2-1)/24$ *subgroups* A_4.
(iv) $q(q^2-1)/24$ *subgroups* S_4 *when* $q\equiv 7 \pmod 8$.
(v) $q(q^2-1)/60$ *subgroups* A_5 *when* $q\equiv \pm1 \pmod{10}$.
(vi) $p^n(p^{2n}-1)/(p^m(p^{2m}-1))$ *subgroups* $\mathrm{PSL}(2,p^m)$ *where* $m|n$.
(vii) *The elementary Abelian group of order* p^m *for* $m\leq n$.
(viii) *A semidirect product of the elementary Abelian group of order* p^m *and the cyclic group of order* d *where* $d|\frac{q-1}{2}$ *and* $d|p^m-1$.

In this paper we are specially interested in the subgroups (i)-(v) in Theorem 3. Note that isomorphic subgroups of $\mathrm{PSL}(2,q)$ of types (i)–(v) in Theorem 3 are conjugate in $\mathrm{PGL}(2,q)$. Now since $\mathrm{PSL}(2,q)$ is normal in $\mathrm{PGL}(2,q)$, for any subgroup of $\mathrm{PSL}(2,q)$ of types (i)-(v) one can easily find the number of overgroups which are of these types using Theorem 3. We have the following lemmas.

Lemma 4 C_d *has a unique subgroup* C_l *for any* $l>1$ *and* $l|d$. *The nontrivial subgroups of the dihedral group* D_{2d} *are as follows:* d/l *subgroups* D_{2l} *for any* $l|d$ *and* $l>1$, *a unique subgroup* C_l *for any* $l|d$ *and* $l>2$, d *subgroups* C_2 *if* d *is odd and* $d+1$ *subgroups* C_2 *otherwise. Moreover* D_{2d} *has a normal subgroup* C_2 *if and only if* d *is even.*

Lemma 5 *The conjugacy classes of nontrivial subgroups of* A_4, S_4, *and* A_5 *are as follows.*

group	C_2	C_2	C_3	C_4	C_5	D_4	D_4	D_6	D_8	D_{10}	A_4
A_4	3		4			1					
S_4	3	6	4	3		1	3	4	3		1
A_5	15		10		6	5		10		6	5

Lemma 6 *Let* $l|\frac{q\pm1}{2d}$ *and* $f|\frac{q\pm1}{2}$.

(i) *Any* C_d *is contained in a unique* C_{ld}.
(ii) *If* $d>2$, *then any* C_d *is contained in* $(q\pm1)/(2ld)$ *subgroups* D_{2ld}.
(iii) *Any* C_2 *is contained in* $(q+1)/4$ *subgroups* D_4, $(q+1)/2$ *subgroups* D_{2f} *if* $f>1$ *is odd, and* $(q+1)(f+1)/(2f)$ *subgroups* D_{2f} *if* f *is even.*
(iv) *If* $d>2$, *then any* D_{2d} *is contained in a unique* D_{2ld}.
(v) *Any* D_4 *is contained in* 3 *subgroups* D_{2f} *for* $f>2$ *even.*

Lemma 7(i) *Any C_2 is contained in $(q+1)/2$ subgroups S_4 as a subgroup C_2 of S_4 with 6 conjugates (see Lemma 5) when $q \equiv 7 \pmod 8$.*
(ii) *Any C_2 is contained in $(q+1)/2$ subgroups A_5 when $q \equiv \pm 1 \pmod{10}$.*
(iii) *Let $3 | \frac{q\pm 1}{2}$. Then any C_3 is contained in $(q \pm 1)/3$ subgroups A_4, $(q \pm 1)/3$ subgroups S_4 when $q \equiv 7 \pmod 8$, and $(q \pm 1)/3$ subgroups A_5 when $q \equiv \pm 1 \pmod{10}$.*
(iv) *Any A_4 is contained in a unique S_4 when $q \equiv 7 \pmod 8$ and 2 subgroups A_5 when $q \equiv \pm 1 \pmod{10}$.*

Lemma 8(i) *Any D_4 is contained in a unique A_4 and if $q \equiv 7 \pmod 8$, then it is in a unique S_4 in which it is normal.*
(ii) *Any D_6 is contained in 2 subgroups S_4 when $q \equiv 7 \pmod 8$ and 2 subgroups A_5 when $q \equiv \pm 1 \pmod{10}$.*
(iii) *Any D_8 is contained in 2 subgroups S_4 when $q \equiv 7 \pmod 8$.*
(iv) *Any D_{10} is contained in 2 subgroups A_5 when $q \equiv \pm 1 \pmod{10}$.*

4 The action of subgroups on the projective line

In this section we determine the sizes of orbits from the action of subgroups of $\mathrm{PSL}(2, q)$ on the projective line. Here, the main tool is the following observation: If $H \leq K \leq \mathrm{PSL}(2, q)$, then any orbit of K is a union of orbits of H. In the following lemmas we suppose that H is a subgroup of $\mathrm{PSL}(2, q)$ and N_l denotes the number of orbits of size l.

Lemma 9 *Let H be the cyclic group of order d. Then*

(i) *if $d | \frac{q+1}{2}$, then $N_d = (q+1)/d$,*
(ii) *if $d | \frac{q-1}{2}$, then $N_1 = 2$ and $N_d = (q-1)/d$.*

PROOF. This is trivial by Theorem 2.

Lemma 10 *Let H be the dihedral group of order $2d$. Then*

(i) *if $d | \frac{q+1}{2}$, then $N_{2d} = (q+1)/(2d)$,*
(ii) *if $d | \frac{q-1}{2}$, then $N_2 = 1$ and $N_{2d} = (q-1)/(2d)$.*

PROOF. (i) H has a cycle subgroup of order d and therefore by Lemma 9, its orbit sizes are multiples of d. Since H has at least d elements of order 2 which are fixed point free, it does not have orbits of size d. Therefore all orbits are of size $2d$.

(ii) Since H has a cycle subgroup of order 2, all orbits are of even size. On the other hand, H has a cycle subgroup of order d and therefore by Lemma 9, we have one orbit of size 2 and all other orbits are regular.

Lemma 11 *Let H be the group A_4. Then*

(i) *if* $3|\frac{q+1}{2}$, *then* $N_{12} = (q+1)/12$,
(ii) *if* $3|\frac{q-1}{2}$, *then* $N_4 = 2$ *and* $N_{12} = (q-7)/12$,
(iii) *if* $3|q$, *then* $N_4 = 1$ *and* $N_{12} = (q-3)/12$.

PROOF. If B is a 6-subset of the projective line, then $|G_B| \leq 6$ (see [10, Lemma 2.1]). Hence $N_6 = 0$. There is an element of order 2 in H. So by Lemma 9, all orbits are of even order.

(i) H has a fixed point free element of order 3 and therefore by Lemma 9, its orbit sizes are multiples of 6. Since $N_6 = 0$, all orbits are regular.

(ii) H has an element of order 3 with two fixed points. Hence by Lemma 9, orbit sizes are 2,4,12. If $N_2 = 1$, then $N_4 = 0$ and $N_{12} = (q-1)/12$ which is not integer. So $N_2 = 0, N_4 = 2$, and $N_{12} = (q-7)/12$.

(ii) H has an element of order 3 with one fixed point. Hence by Lemma 9, orbit sizes are 4 and 12. We have $N_4 = 1$ and $N_{12} = (q-3)/12$.

Lemma 12 *Let H be the group S_4. Then*

(i) *if* $3|\frac{q+1}{2}$, *then* $N_{24} = (q+1)/24$,
(ii) *if* $3|\frac{q-1}{2}$, *then* $N_8 = 1$ *and* $N_{24} = (q-7)/24$.

PROOF. We have $q \equiv 7 \pmod 8$. Hence $3 \not| q$. Note that H has a subgroup A_4. Therefore, by Lemma 11, orbits are of sizes 4,8,12,24. If B is a 4-subset of the projective line, then by Lemma 1, $|G_B| \mid 12$ and so $N_4 = 0$. By a similar argument, $N_{12} = 0$.

(i) It is obvious by Lemma 11(i).

(ii) By Lemma 11(ii), we necessarily have $N_8 = 1$ and all other orbits of size 24.

Lemma 13 *the Let H be group A_5. Then*

(i) *if* $15|\frac{q+1}{2}$, *then* $N_{60} = (q+1)/60$,
(ii) *if* $3|\frac{q+1}{2}$ *and* $5|\frac{q-1}{2}$, *then* $N_{12} = 1$ *and* $N_{60} = (q-11)/60$,
(iii) *if* $3|\frac{q-1}{2}$ *and* $5|\frac{q+1}{2}$, *then* $N_{20} = 1$ *and* $N_{60} = (q-11)/60$,

(iv) *if* $15|\frac{q-1}{2}$, *then* $N_{12}=1, N_{20}=1$, *and* $N_{60}=(q-31)/60$.

PROOF. We have $q \equiv \pm 1 \pmod{10}$. Hence $3 \not| q$ and $5|\frac{q\pm 1}{2}$. Note that H has a subgroup A_4.

(i) By Lemma 11(i), all orbit sizes are multiples of 12. On the other hand, H has a fixed point free element of order 5 which means that all orbit sizes are multiples of 5. Therefore, all orbits are regular.

(ii) By Lemma 11(i), all orbit sizes are multiples of 12. On the other hand, H has an element of order 5 with two fixed points which implies the existence of one orbit of sizes 12. Hence, $N_{12}=1$ and all other orbits of size 60.

(iii) If B is a 4-subset of the projective line, then by Lemma 1, $|G_B| \mid 12$ and so $N_4=0$. Now by Lemma 11(ii), we have one orbit of size 20 and all other orbits are of orders 12 or 60. On the other hand, H has a fixed point free element of order 5 which means that all orbit sizes are multiples of 5. Therefore, $N_{12}=0$ and all remaining orbits are regular.

(iv) Similar to (iii), we have one orbit of size 20 and all other orbits are of orders 12 or 60. On the other hand, H has an element of order 5 with two fixed points which forces $N_{12}=1$ and all other orbits to be regular.

Lemma 14 *Let H be the elementary Abelian group of order p^m. Then $N_1=1$ and $N_{p^m}=p^{n-m}$.*

PROOF. By the Cauchy-Frobenius lemma, the number of orbits is $p^{n-m}+1$. Note that all orbit sizes are powers of p. Therefore, we just have one orbit of size one and all other orbits are regular.

Lemma 15 *Let H be a semidirect product of the elementary Abelian group of order p^m and the cyclic group of order d where $d|\frac{q-1}{2}$ and $d|p^m-1$. Then $N_1=1, N_{p^m}=1$, and $N_{dp^m}=(p^n-p^m)/(dp^m)$.*

PROOF. H has an elementary Abelian subgroup of order p^m. So by Lemma 14, we have one orbit of size 1 and all other orbit sizes are multiples of p^m. On the other hand, H has a cyclic subgroup of order d and therefore by Lemma 9, orbit sizes are congruent 0 or 1 module d. If congruent 0 module d, then orbit size is necessarily dp^m. Otherwise, orbit size must be 1 or p^m. Now the assertion follows from the fact that an element of order d has two fixed points.

Lemma 16 *Let H be* $\mathrm{PSL}(2,p^m)$ *where $m|n$. Then $N_{p^m+1}=1$ and all other orbits are regular.*

PROOF. All subgroups of the form $\mathrm{PSL}(2,p^m)$ of $\mathrm{PSL}(2,q)$ are conjugate [4]. So we can suppose that H is the group with elements $x \mapsto \frac{ax+b}{cx+d}$, $a,b,c,d \in GF(p^m)$, where $GF(p^m)$ is the unique subfield of order p^m of $GF(p^n)$. Since H is transitive on $GF(p^m)$ we have an orbit of size p^m+1. H has a subgroup of order $p^m(p^m-1)/2$ which is a semidirect product of the elementary Abelian group of order p^m and the cyclic group of order $(p^m-1)/2$. So by Lemma 15, all other orbits of H are multiples of $p^m(p^m-1)/2$. On the other hand H has an fixed point free element of order $(p^m+1)/2$ which forces orbits to be of sizes of multiples of $(p^m+1)/2$. Hence all orbits except one are regular.

We summarize the results of the previous lemmas in the following theorem.

Theorem 17 *The sizes of non-regular orbits for any subgroup H of* $\mathrm{PSL}(2,q)$ *are as given in Table 1. (Subgroups with no non-regular orbits do not appear in the table).*

H	*Condition*	*The sizes of non-regular orbits*
C_d	$d \mid \frac{q-1}{2}$	$1,1$
D_{2d}	$d \mid \frac{q-1}{2}$	2
A_4	$3 \mid \frac{q-1}{2}$	$4,4$
A_4	$3 \mid q$	4
S_4	$3 \mid \frac{q-1}{2}$	8
A_5	$3 \mid \frac{q+1}{2},\ 5 \mid \frac{q-1}{2}$	12
A_5	$3 \mid \frac{q-1}{2},\ 5 \mid \frac{q+1}{2}$	20
A_5	$15 \mid \frac{q-1}{2}$	$12, 20$
Z_p^m	$m \leq n$	1
$Z_p^m \rtimes C_d$	$m \leq n, d \mid (p^n-1, p^m-1)$	$1, p^m$
$\mathrm{PSL}(2,p^m)$	$m \mid n$	p^m+1

Table 1
Sizes of non-regular orbits of subgroups

5 The Möbius function of the subgroup lattice of subgroups of $\mathrm{PSL}(2, q)$

In this section we do some calculations on the Möbius function of the lattice of subgroups of $\mathrm{PSL}(2, q)$ which will be useful in Section 7. We start with the cyclic subgroups C_d.

Lemma 18 *$\mu(1, C_d) = \mu(d)$ and $\mu(C_l, C_d) = \mu(d/l)$ if $l|d$.*

PROOF. Since C_l is normal in C_d, we have $\mu(C_l, C_d) = \mu(1, C_{d/l})$. So it suffices to find $\mu(1, C_d)$. By Lemma 4, C_d has a unique subgroup of order m for any divisor m of d. Therefore, $\sum_{m|d} \mu(1, C_m) = 0$. On the other hand $\sum_{m|d} \mu(m) = 0$ and $\mu(1) = 1$. So by the initial condition $\mu(1, 1) = 1$, we obtain that $\mu(1, C_d) = \mu(d)$.

Lemma 19 *Let $d > 1$.*

(i) $\mu(1, D_{2d}) = -d\mu(d)$,
(ii) $\mu(D_{2l}, D_{2d}) = \mu(d/l)$,
(iii) $\mu(C_l, D_{2d}) = -(d/l)\mu(d/l)$ *if* $l|d$ *and* $l > 2$,
(iv) $\mu(C_2, D_{2d}) = -(d/2)\mu(d/2)$ *if* C_2 *is normal in* D_{2d} *and* $\mu(C_2, D_{2d}) = \mu(d)$ *otherwise.*

PROOF. (i) We have

$$\begin{aligned}\mu(1, D_{2d}) &= -\sum_{1 \leq H < D_{2d}} \mu(1, H) \\ &= -\sum_{m|d} \mu(1, C_m) - \sum_{m|d, m \neq d} \frac{d}{m} \mu(1, D_{2m}) \\ &= -\sum_{m|d, m \neq d} \frac{d}{m} \mu(1, D_{2m}).\end{aligned}$$

On the other hand, $-d\mu(d) = \sum_{m|d, m \neq d} \frac{d}{m} m\mu(m)$ and $-2\mu(2) = 2$. So by the initial condition $\mu(1, D_4) = 2$, we obtain that $\mu(1, D_{2d}) = -d\mu(d)$.

(ii) Let $D_{2l} \leq H \leq D_{2d}$ and $|H| = 2ml$. Then H is unique and it is a dihedral group. Now we have $\mu(D_{2l}, D_{2d}) = -\sum_{m|\frac{d}{l}, m \neq \frac{d}{l}} \mu(D_{2l}, D_{2ml})$. On the other hand, $\mu(\frac{d}{l}) = -\sum_{m|\frac{d}{l}, m \neq \frac{d}{l}} \mu(m)$ and $\mu(1) = 1$. So by the initial condition $\mu(D_{2l}, D_{2l}) = 1$, we obtain that $\mu(D_{2l}, D_{2d}) = \mu(d/l)$.

(iii) since C_l is normal in D_{2d} it is obvious by (i).

(iv) If C_2 is normal in D_{2d}, then the assertion follows by (i). Otherwise, a similar argument to (ii) is applied.

Lemma 20 *$\mu(1, A_4) = 4$, $\mu(C_2, A_4) = 0$, $\mu(C_3, A_4) = -1$, and $\mu(D_4, A_4) = -1$.*

PROOF. The subgroup lattice of A_4 is shown in Figure 1. So the assertion can easily be verified.

Lemma 21 *$\mu(A_4, S_4) = -1$, $\mu(D_8, S_4) = -1$, $\mu(D_6, S_4) = -1$, $\mu(C_4, S_4) = 0$, $\mu(D_4, S_4) = 3$ for normal subgroup D_4 of S_4 and $\mu(D_4, S_4) = 0$ otherwise, $\mu(C_3, S_4) = -1$, $\mu(C_2, S_4) = 0$ if C_2 is a subgroup with 3 conjugates (see Lemma 5) and $\mu(C_2, S_4) = 2$ otherwise, and $\mu(1, S_4) = -12$.*

PROOF. The subgroup lattice of S_4 is obtained by GAP [5]. The maximal subgroups of S_4 are A_4, D_8, and D_6. Therefore, $\mu(A_4, S_4) = \mu(D_8, S_4) = \mu(D_6, S_4) = -1$. Any subgroup C_4 is contained in a unique maximal subgroup D_8 of S_4. Hence, $\mu(C_4, S_4) = 0$. This is true also for subgroup D_4 which is not normal. Using the sublattices of subgroups of S_4 containing D_4, C_3, or C_2 shown in Figure 2, the calculation of the remaining cases is straightforward. Note that $\mu(1, S_4)$ is already known [11] and it is also obtained by the relation $\sum_{1 \le H \le S_4} \mu(H, S_4) = 0$ and the previous results.

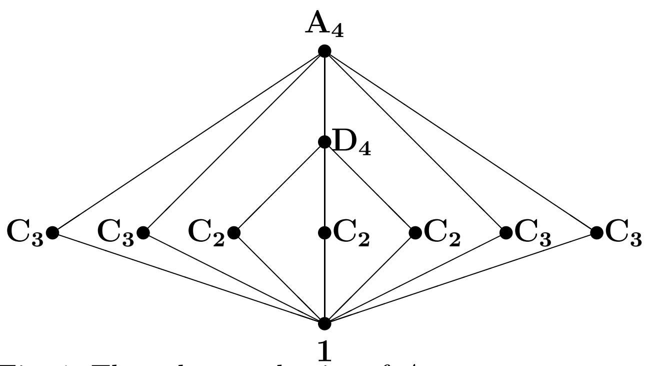

Fig. 1. The subgroup lattice of A_4

Lemma 22 *$\mu(A_4, A_5) = -1$, $\mu(D_{10}, A_5) = -1$, $\mu(D_6, A_5) = -1$, $\mu(C_5, A_5) = 0$, $\mu(D_4, A_5) = 0$, $\mu(C_3, A_5) = 2$, $\mu(C_2, A_5) = 4$, and $\mu(1, A_5) = -60$,*

PROOF. The subgroup lattice of A_5 is obtained by GAP [5]. The maximal subgroups of A_5 are A_4, D_{10}, and D_6. Therefore, $\mu(A_4, A_5) = \mu(D_{10}, A_5) = \mu(D_6, A_5) = -1$. Any subgroup C_5 is contained in a unique maximal subgroup of A_5. Hence, $\mu(C_5, A_5) = 0$. This is true also for any subgroup D_4. Using the

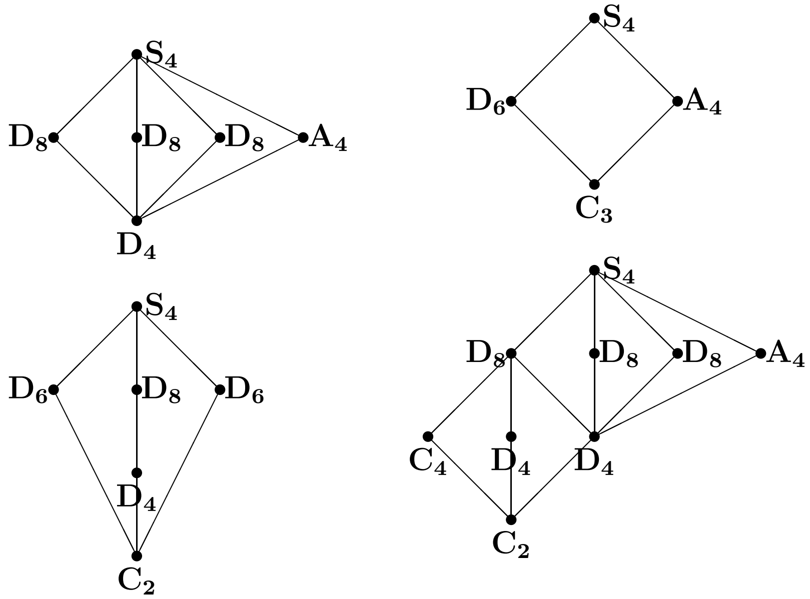

Fig. 2. The sublattices of subgroups of S_4 containing D_4, C_3, or C_2

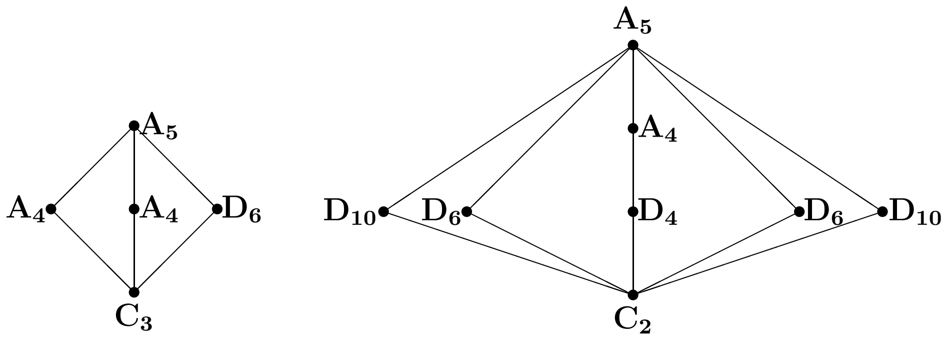

Fig. 3. The sublattices of subgroups of A_5 containing C_3, or C_2

sublattices of subgroups of A_5 containing C_3 or C_2 shown in Figure 3, the calculation of the remaining cases is straightforward. Note that $\mu(1, A_5)$ is found using the relation $\sum_{1\leq H\leq A_5} \mu(H, A_5) = 0$ and the preceding results.

6 Determination of f_k

In Section 4, we determined the sizes of orbits from the action of subgroups of $\mathrm{PSL}(2, q)$ on the projective line. The results can be used to calculate $f_k(H)$ for any subgroup H and $1 \leq k \leq q+1$. Suppose that H has r_i orbits of size

l_i $(1 \leq i \leq s)$. Then by the definition we have

$$f_k(H) = \sum_{\sum_{i=1}^{s} m_i l_i = k} \left(\prod_{i=1}^{s} \binom{r_i}{m_i} \right).$$

Any subgroup of $\mathrm{PSL}(2, q)$ has at most two non-regular orbits and so it is an easy task to compute f_k.

Theorem 23 *Let $z(H)$ denote the sum of sizes of the non-regular orbits of subgroup H of $\mathrm{PSL}(2, q)$ and let $k \equiv l \pmod{|H|}$ where $l < |H|$. Then $f_k(H) = c\binom{(q+1-z(H))/|H|}{(k-l)/|H|}$ in which*

(i) *$c = 1$ if l is a sum of some non-regular orbit sizes (possibly none) and H has no two non-regular orbits of size l,*
(ii) *$c = 2$ if H has two non-regular orbits of size l,*
(iii) *$c = 0$ otherwise.*

In Table 2, we present the values of $f_k(H)$ for subgroups H of $\mathrm{PSL}(2, q)$ and k for which $f_k(H)$ is nonzero.

7 Determination of g_k

In this section, we suppose that $1 \leq k \leq q + 1$ and $k \not\equiv 0, 1 \pmod{p}$ and try to calculate $g_k(H)$ for subgroups H of $\mathrm{PSL}(2, q)$. Note that the condition $k \not\equiv 0, 1 \pmod{p}$ imposes $f_k(H)$ and $g_k(H)$ to be zero for any subgroup H belonging to one of the classes (vi)-(viii) in Theorem 3. By

$$g_k(H) = \sum_{H \leq U \leq \mathrm{PSL}(2,q)} f_k(U)\mu(H, U),$$

we only need to focus on those overgroups U of H for which $f_k(U)$ and $\mu(H, U)$ are nonzero. All what we need on overgroups are provided by Theorem 3 and Lemmas 6–8. The values of the Möbius function and f_k have been determined in Sections 5 and 6, respectively. Now we are ready to compute g_k.

Theorem 24

$$\begin{aligned} g_k(1) =& f_k(1) + \frac{q(q^2-1)}{12}(2f_k(A_4) - 6f_k(S_4) - 12f_k(A_5) + f_k(D_4)) \\ &+ \sum_{l>1, l | \frac{q \pm 1}{2}} \frac{q(q \mp 1)}{2} \mu(l) f_k(C_l) - \frac{q(q^2-1)}{4} \sum_{l>2, l | \frac{q \pm 1}{2}} \mu(l) f_k(D_{2l}). \end{aligned}$$

H	Condition on q	$l \equiv k \pmod{\lvert H\rvert}$	$f_k(H)$
1		0	$\binom{q+1}{k}$
C_d	$d\lvert\frac{q+1}{2}$	0	$\binom{(q+1)/d}{(k-l)/d}$
C_d	$d\lvert\frac{q-1}{2}$	$0,2$	$\binom{(q-1)/d}{(k-l)/d}$
C_d	$d\lvert\frac{q-1}{2}$	1	$2\binom{(q-1)/d}{(k-l)/d}$
D_{2d}	$d\lvert\frac{q+1}{2}$	0	$\binom{(q+1)/2d}{(k-l)/2d}$
D_{2d}	$d\lvert\frac{q-1}{2}$	$0,2$	$\binom{(q-1)/2d}{(k-l)/2d}$
A_4	$3\lvert\frac{q+1}{2}$	0	$\binom{(q+1)/12}{(k-l)/12}$
A_4	$3\lvert\frac{q-1}{2}$	$0,8$	$\binom{(q-7)/12}{(k-l)/12}$
A_4	$3\lvert\frac{q-1}{2}$	4	$2\binom{(q-7)/12}{(k-l)/12}$
A_4	$3\lvert q$	$0,4$	$\binom{(q-3)/12}{(k-l)/12}$
S_4	$3\lvert\frac{q+1}{2},\ 8\lvert(q+1)$	0	$\binom{(q+1)/24}{(k-l)/24}$
S_4	$3\lvert\frac{q-1}{2},\ 8\lvert(q+1)$	$0,8$	$\binom{(q-7)/24}{(k-l)/24}$
A_5	$15\lvert\frac{q+1}{2}$	0	$\binom{(q+1)/60}{(k-l)/60}$
A_5	$3\lvert\frac{q+1}{2},\ 5\lvert\frac{q-1}{2}$	$0,12$	$\binom{(q-11)/60}{(k-l)/60}$
A_5	$3\lvert\frac{q-1}{2},\ 5\lvert\frac{q+1}{2}$	$0,20$	$\binom{(q-19)/60}{(k-l)/60}$
A_5	$15\lvert\frac{q-1}{2}$	$0,12,20,32$	$\binom{(q-31)/60}{(k-l)/60}$
Z_p^m	$m \leq n$	$0,1$	$\binom{q/p^m}{(k-l)/p^m}$
$Z_p^m \rtimes C_d$	$d\lvert\frac{q-1}{2}, d\lvert p^m-1$	$0,1,p^m,p^m+1$	$\binom{(q-p^m)/dp^m}{(k-l)/dp^m}$
$\mathrm{PSL}(2,p^m)$	$m\lvert n$	$0,p^m+1$	$\binom{2(q-p^m)/p^m(p^{2m}-1)}{2(k-l)/p^m(p^{2m}-1)}$

Table 2
The nonzero values of $f_k(H)$ for subgroups H of $\mathrm{PSL}(2,q)$

Theorem 25

$$g_k(C_2) = \frac{q+1}{4}(4f_k(S_4) + 8f_k(A_5) - f_k(D_4)) + \sum_{l|\frac{q+1}{4}} \mu(l) f_k(C_{2l})$$
$$+ \sum_{l>1,\, 2\nmid l,\, l|\frac{q\pm1}{2}} \frac{q+1}{2}\mu(l) f_k(D_{2l}) + \sum_{l>1,\, l|\frac{q+1}{4}} \frac{q+1}{2}\left(\mu(2l) - \frac{\mu(l)}{2}\right) f_k(D_{4l}).$$

Theorem 26 *Let* $3|\frac{q\pm1}{2}$. *Then*

$$g_k(C_3) = \frac{q\pm1}{3}(2f_k(A_5) - f_k(A_4) - f_k(S_4))$$
$$+ \sum_{l|\frac{q\pm1}{6}} \mu(l)\left(f_k(C_{3l}) - \frac{q\pm1}{6} f_k(D_{6l})\right).$$

Theorem 27 *Let* $d > 3$ *and* $d|\frac{q\pm1}{2}$. *Then*

$$g_k(C_d) = \sum_{l|\frac{q\pm1}{2d}} \mu(l)\left(f_k(C_{ld}) - \frac{q\pm1}{2d} f_k(D_{2ld})\right).$$

Theorem 28 *Let* $h_k(D_{2d}) = \sum_{l|\frac{q\pm1}{2d}} \mu(l) f_k(D_{2ld})$. *Then*
$g_k(D_4) = 3f_k(S_4) - f_k(A_4) - 2f_k(D_4) + 3h_k(D_4)$,
$g_k(D_6) = -2f_k(S_4) - 2f_k(A_5) + h_k(D_6)$,
$g_k(D_8) = -2f_k(S_4) + h_k(D_8)$, $g_k(D_{10}) = -2f_k(A_5) + h_k(D_{10})$, *and*
$g_k(D_{2d}) = h_k(D_{2d})$ *if* $d > 5$ *and* $d|\frac{q\pm1}{2}$.

Theorem 29 $g_k(A_4) = f_k(A_4) - f_k(S_4) - 2f_k(A_5)$, $g_k(S_4) = f_k(S_4)$, *and* $g_k(A_5) = f_k(A_5)$.

8 3-Designs from $\mathrm{PSL}(2, q)$

We use the results of previous sections to show the existence of large families of new 3-designs. First we state the following simple result.

Lemma 30 *Let* H *be a subgroup of* $\mathrm{PSL}(2, q)$ *and let* $u(H)$ *denote the number of subgroups of* $\mathrm{PSL}(2, q)$ *isomorphic to* H. *Then the number of orbits of* $\mathrm{PSL}(2, q)$ *on* k*-subsets whose elements have stabilizers isomorphic to* H *is equal to* $u(H)g_k(H)|H|/|\,\mathrm{PSL}(2, q)|$.

PROOF. The number of k-subsets whose stabilizers are isomorphic to H is $u(H)g_k(H)$ and such k-subsets lie in orbits of size $|\,\mathrm{PSL}(2, q)|/|H|$.

The lemma above and Theorem 3 help us to compute the sizes of orbits of the action of $\mathrm{PSL}(2,q)$ on k-subsets of the projective line. When the sizes of orbits are known, we can utilize them to determine all 3-designs from $\mathrm{PSL}(2,q)$ as shown in Theorem 32.

Theorem 31 *Let $1 \le k \le q+1$ and $k \not\equiv 0,1 \pmod p$. Then the sizes of orbits of $G = \mathrm{PSL}(2,q)$ on k-subsets are as in Table 3, where $d \mid \frac{q\pm1}{2}$ and $d > 1$.*

orbit size	$\lvert G\rvert$	$\frac{\lvert G\rvert}{4}$	$\frac{\lvert G\rvert}{12}$	$\frac{\lvert G\rvert}{24}$	$\frac{\lvert G\rvert}{60}$	$\frac{\lvert G\rvert}{d}$	$\frac{\lvert G\rvert}{2d}$ $(d>2)$
number of orbits	$\frac{2g_k(1)}{q^3-q}$	$\frac{g_k(D_4)}{3}$	$g_k(A_4)$	$2g_k(S_4)$	$2g_k(A_5)$	$\frac{dg_k(C_d)}{q\pm1}$	$g_k(D_{2d})$

Table 3
Sizes of orbits on k-sets

Theorem 32 *Let $3 \le k \le q-2$ and $k \not\equiv 0,1 \pmod p$. Then there exist 3-$(q+1, k, 3\binom{k}{3}\lambda)$ designs with automorphism group $\mathrm{PSL}(2,q)$ if and only if*

$$\lambda = a_1 + \frac{a_2}{4} + \frac{a_3}{12} + \frac{a_4}{24} + \frac{a_5}{60} + \sum_{d>1, d\mid\frac{q\pm1}{2}} \frac{i_d}{d} + \sum_{d>2, d\mid\frac{q\pm1}{2}} \frac{j_d}{2d},$$

where $a_1, \ldots, a_5, i_d, j_d$ are non-negative integers satisfying $a_1 \le 2g_k(1)/(q(q^2-1))$, $a_2 \le g_k(D_4)/3$, $a_3 \le g_k(A_4)$, $a_4 \le 2g_k(S_4)$, $a_5 \le 2g_k(A_5)$, $i_d \le dg_k(C_d)/(q\pm1)$, $j_d \le g_k(D_{2d})$.

References

[1] T. Beth, D. Jungnickel, and H. Lenz, *Design theory*, Second edition, Cambridge University Press, Cambridge, 1999.

[2] C. A. Cusack, S. W. Graham, and D. L. Kreher, Large sets of 3-designs from $\mathrm{PSL}(2,q)$, with block sizes 4 and 5, *J. Combinatorial Designs* **3** (1995), 147–160.

[3] C. A. Cusack and S. S. Magliveras, Semiregular large sets, *Designs Codes Cryptogr.* **18** (1999), 81–87.

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

[5] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.3; 2002, (`http://www.gap-system.org`).

[6] D. R. Hughes, On t-designs and groups, *Amer. J. Math.* **87** (1965), 761–778.

[7] B. Huppert, *Endliche gruppen I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin–New York, 1967,

[8] S. Iwasaki, Infinite families of 2- and 3-designs with parameters $v = p + 1$, $k = (p-1)/2^i + 1$, where p odd prime, $2^e \top (p-1)$, $e \geq 2$, $1 \leq i \leq e$, *J. Combinatorial Designs* **5** (1997), 95–110.

[9] D. L. Kreher, t-Designs, $t \geq 3$, in: *The CRC Handbook of Combinatorial Designs* (C. J. Colbourn and J. H. Dinitz, eds.), CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton (1996), pp. 47–66.

[10] G. R. Omidi, M. R. Pournaki, and B. Tayfeh-Rezaie, 3-Designs from $\mathrm{PSL}(2, q)$ with block size 6 and their large sets, submitted.

[11] J. Shareshian, On the Möbius number of the subgroup lattice of the symmetric group, *J. Combinatorial Theory* Ser. A **78** (1997), 236–267.