3-Designs from PGL$(2, q)$

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

[a]Institute for Studies in Theoretical Physics and Mathematics (IPM),
P.O. Box 19395-5746, Tehran, Iran
[b]School of Mathematics, Statistics and Computer Science,
University of Tehran, Tehran, Iran
[c]School of Mathematical Sciences, Queen Mary, University of London, U.K.
E-mails: P.J.Cameron@qmul.ac.uk, tayfeh-r@ipm.ir, omidi@ipm.ir

Submitted: Sep 28, 2005; Accepted: May 9, 2006; Published: May 19, 2006
Mathematics Subject Classifications: 05B05, 20B20

Abstract

The group PGL$(2, q)$, $q = p^n$, p an odd prime, is 3-transitive on the projective line and therefore it can be used to construct 3-designs. In this paper, we determine the sizes of orbits from the action of PGL$(2, q)$ on the k-subsets of the projective line when k is not congruent to 0 and 1 modulo p. Consequently, we find all values of λ for which there exist 3-$(q + 1, k, \lambda)$ designs admitting PGL$(2, q)$ as automorphism group. In the case $p \equiv 3 \pmod 4$, the results and some previously known facts are used to classify 3-designs from PSL$(2, p)$ up to isomorphism.

Keywords: t-designs, automorphism groups, projective linear groups, Möbius functions

1 Introduction

Let $q = p^n$, where p is an odd prime and n is a positive integer. The group PGL$(2, q)$ is 3-transitive on the projective line and therefore, a set of k-subsets of the projective line is the block set of a 3-$(q + 1, k, \lambda)$ design admitting PGL$(2, q)$ as an automorphism group for some λ if and only if it is a union of orbits of PGL$(2, q)$. There are some known results on 3-designs from PGL$(2, q)$ in the literature, see for example [1, 4, 6]. In this paper, we first determine the sizes of orbits from the actions of subgroups of PGL$(2, q)$ on the projective line. Then we use the Möbius inversion to find the sizes of orbits from the action of PGL$(2, q)$ on the k-subsets of the projective line when k is not congruent to 0 and 1 modulo p. Consequently, all values of λ for which there exist 3-$(q + 1, k, \lambda)$ designs admitting PGL$(2, q)$ as automorphism group are identified. We also use the results and some previously known facts to classify 3-designs from PSL$(2, p)$ up to isomorphism when $p \equiv 3 \pmod 4$. We note that similar methods have been used in [7].

2 Notation and Preliminaries

Let t, k, v and λ be integers such that $0 \le t \le k \le v$ 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. If $D = P_k(X)$, then $\mathcal{D}$ is said to be the *trivial* design. 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 $G(x) = \{gx | \ g \in G\}$ and the *stabilizer* of x is $G_x = \{g \in G | \ gx = x\}$. It is well known that $|G| = |G(x)||G_x|$. The orbits of size $|G|$ are called *regular* and the others *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 said to be 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 nonzero 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 the *projective general linear group* and is denoted by $\mathrm{PGL}(2, q)$. If we consider the mappings g with $ad-bc$ a nonzero square, then we find another group called the *projective special linear group* which is denoted by $\mathrm{PSL}(2, q)$. It is well known that $\mathrm{PGL}(2, q)$ is 3-homogeneous (in fact it is 3-transitive) and $|\,\mathrm{PGL}(2, q)| = (q^3 - q)$. **Hereafter, we let p be a prime, $q = p^n$ and $q \equiv \epsilon \pmod 4$, where $\epsilon = \pm 1$.** Since $\mathrm{PGL}(2, q)$ is 3-homogeneous, a set of k-subsets of X is a 3-$(q + 1, k, \lambda)$ design admitting $\mathrm{PGL}(2, q)$ as an automorphism group if and only if it is a union of orbits of $\mathrm{PGL}(2, q)$ on $P_k(X)$. Thus, for constructing designs with block size k admitting $\mathrm{PGL}(2, q)$, we need to determine the sizes of orbits from the action of $\mathrm{PGL}(2, q)$ on $P_k(X)$.

Let $H \le \mathrm{PGL}(2, q)$ and define

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

Then we have

$$f_k(H) = \sum_{H \le U \le \mathrm{PGL}(2,q)} g_k(U). \qquad (1)$$

The values of g_k can be used to find the sizes of orbits from the action of $\mathrm{PGL}(2, q)$ on $P_k(X)$. So we are interested in finding g_k. But it is easier to find f_k and then to use it to compute g_k. By the Möbius inversion applied to (1), we have

$$g_k(H) = \sum_{H \le U \le \mathrm{PGL}(2,q)} f_k(U)\mu(H, U), \qquad (2)$$

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

For any subgroup H of $\mathrm{PGL}(2,q)$, 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 (2).

Note that if H and H' are conjugate, then $f_k(H) = f_k(H')$ and $g_k(H) = g_k(H')$. Therefore, we need to apply the above steps only to the representatives of conjugacy classes of subgroups of $\mathrm{PGL}(2,q)$.

In the next section, we will review the structure of subgroups of $\mathrm{PGL}(2,q)$ and their overgroups. Then, Step (i) of the above procedure will be carried out in Section 4 for any subgroup of $\mathrm{PGL}(2,q)$. For Step (ii), we will make use the values of Möbius function of the subgroup lattice of $\mathrm{PSL}(2,q)$ given in [2]. The results will be used to find new 3-designs with automorphism group $\mathrm{PGL}(2,q)$ in Section 7.

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

The subgroups of $\mathrm{PSL}(2,q)$ are well known and are given in [3, 5]. These may also be found in [2] together with some results on the overgroups of subgroups. Since $\mathrm{PGL}(2,q)$ is a subgroup of $\mathrm{PSL}(2,q^2)$ and it has a unique subgroup $\mathrm{PSL}(2,q)$, we can easily extract all necessary information concerning the subgroups of $\mathrm{PGL}(2,q)$ and their overgroups from the results of [2].

Theorem 1 *Let g be a nontrivial element in $\mathrm{PGL}(2,q)$ of order d and with f fixed points. Then $d = p$, $f = 1$ or $d|q \pm \epsilon$, $f = 1 \mp \epsilon$.*

Theorem 2 *The subgroups of $\mathrm{PGL}(2,q)$ are as follows.*

(i) *Two conjugacy classes of cyclic subgroups C_2. One (class 1) consisting of $q(q+\epsilon)/2$ of them which lie in the subgroup $\mathrm{PSL}(2,q)$, the other one (class 2) consisting of $q(q-\epsilon)/2$ subgroups C_2.*

(ii) *One conjugacy class of $q(q \mp \epsilon)/2$ cyclic subgroups C_d, where $d|q \pm \epsilon$ and $d > 2$.*

(iii) *Two conjugacy classes of dihedral subgroups D_4. One (class 1) consisting of $q(q^2 - 1)/24$ of them which lie in the subgroup $\mathrm{PSL}(2,q)$, the other one (class 2) consisting of $q(q^2-1)/8$ subgroups D_4.*

(iv) *Two conjugacy classes of dihedral subgroups D_{2d}, where $d|\frac{q\pm\epsilon}{2}$ and $d > 2$. One (class 1) consisting of $q(q^2-1)/(4d)$ of them which lie in the subgroup $\mathrm{PSL}(2,q)$, the other one (class 2) consisting of $q(q^2-1)/(4d)$ subgroups D_{2d}.*

(v) *One conjugacy class of $q(q^2-1)/(2d)$ dihedral subgroups D_{2d}, where $(q \pm \epsilon)/d$ is an odd integer and $d > 2$.*

(vi) $q(q^2-1)/24$ *subgroups* A_4, $q(q^2-1)/24$ *subgroups* S_4 *and* $q(q^2-1)/60$ *subgroups* A_5 *when* $q \equiv \pm 1 \pmod{10}$. *There is only one conjugacy class of any of these types of subgroups and all lie in the subgroup* $\mathrm{PSL}(2,q)$ *except for* S_4 *when* $q \equiv \pm 3 \pmod 8$.

(vii) *One conjugacy class of* $p^n(p^{2n}-1)/(p^m(p^{2m}-1))$ *subgroups* $\mathrm{PSL}(2,p^m)$, *where* $m|n$.

(viii) *The subgroups* $\mathrm{PGL}(2,p^m)$, *where* $m|n$.

(ix) *The elementary Abelian group of order* p^m *for* $m \leq n$.

(x) *A semidirect product of the elementary Abelian group of order* p^m, *where* $m \leq n$ *and the cyclic group of order* d, *where* $d|q-1$ *and* $d|p^m-1$.

Here, we are specially interested in the subgroups (i)-(vi) in Theorem 2. For any subgroup of types (i)-(vi), we may find the number of overgroups which are of these types using Theorem 2 and the next two lemmas.

Lemma 1 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 2 *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 3 *The numbers of proper cyclic and dihedral overgroups of* C_2 *and* D_4 *are given in the following table, where c1 and c2 refer to classes 1 and 2, respectively.*

overgroups	C_2 (*c1*)	C_2 (*c2*)	D_4 (*c1*)	D_4 (*c2*)
C_{2f} $(f\|\frac{q+\epsilon}{2}, f>1)$	0	1	–	–
C_{2f} $(f\|\frac{q-\epsilon}{2}, f>1)$	1	0	–	–
D_4 (*c1*)	$\frac{q-\epsilon}{4}$	0	–	–
D_4 (*c2*)	$\frac{q-\epsilon}{4}$	$\frac{q+\epsilon}{2}$	–	–
D_{2f} $(f\|\frac{q\pm\epsilon}{2}, f \text{ even}, f>2)$ (*c1*)	$\frac{(q-\epsilon)(f+1)}{2f}$	0	3	0
D_{2f} $(f\|\frac{q\pm\epsilon}{2}, f \text{ even}, f>2)$ (*c2*)	$\frac{q-\epsilon}{2f}$	$\frac{q+\epsilon}{2}$	0	1
D_{2f} $(f\|\frac{q\pm\epsilon}{2}, f \text{ odd}, f>2)$ (*c1*)	$\frac{q-\epsilon}{2}$	0	0	0
D_{2f} $(f\|\frac{q\pm\epsilon}{2}, f \text{ odd}, f>2)$ (*c2*)	0	$\frac{q+\epsilon}{2}$	0	0
D_{2f} $(f \nmid \frac{q\pm\epsilon}{2}, f\|q\pm\epsilon, 4\|f)$	$\frac{(q-\epsilon)(f+2)}{2f}$	$\frac{q+\epsilon}{2}$	3	1
D_{2f} $(f \nmid \frac{q\pm\epsilon}{2}, f\|q\pm\epsilon, 4 \nmid f, f>2)$	$\frac{q-\epsilon}{2}$	$\frac{(q+\epsilon)(f+2)}{2f}$	0	2

Lemma 4 *Let* $ld|q \pm \epsilon$ *and* $d > 2$.

(i) *Any* C_d *is contained in a unique subgroup* C_{ld}.

(ii) *Any* C_d *is contained in* $(q \pm \epsilon)/(ld)$ *subgroups* D_{2ld} *(if this latter group has more than one conjugacy classes, then* C_d *is contained in the same number of groups for each of classes).*

(iii) *Any* D_{2d} *is contained in a unique subgroup* D_{2ld} *(if this latter group has more than one conjugacy classes, then its class number must be same as* D_{2d}*).*

Lemma 5

(i) *Any* C_2 *of class 1 is contained in* $(q - \epsilon)/2$ *subgroups* S_4 *as a subgroup with* 6 *conjugates (see Lemma 2) when* $q \equiv \pm 1 \pmod 8$.

(ii) *Any* C_2 *of class 2 is contained in* $(q + \epsilon)/2$ *subgroups* S_4 *as a subgroup with* 6 *conjugates (see Lemma 2) when* $q \equiv \pm 3 \pmod 8$.

(iii) *Any* C_2 *of class 1 is contained in* $(q - \epsilon)/2$ *subgroups* A_5 *when* $q \equiv \pm 1 \pmod{10}$.

(iv) *Let* $3|q \pm \epsilon$. *Then any* C_3 *is contained in* $(q \pm \epsilon)/3$ *subgroups* A_4, $(q \pm \epsilon)/3$ *subgroups* S_4 *and* $(q \pm \epsilon)/3$ *subgroups* A_5 *when* $q \equiv \pm 1 \pmod{10}$.

(v) *Any* A_4 *is contained in a unique* S_4 *and* 2 *subgroups* A_5 *when* $q \equiv \pm 1 \pmod{10}$.

Lemma 6

(i) *Any* D_4 *of class 1 is contained in a unique* A_4 *and it is in a unique* S_4 *in which it is normal.*

(ii) *Any* D_6 *of class 1 is contained in* 2 *subgroups* S_4 *when* $q \equiv \pm 1 \pmod 8$ *and* 2 *subgroups* A_5 *when* $q \equiv \pm 1 \pmod{10}$.

(iii) *Any* D_6 *of class 2 is contained in* 2 *subgroups* S_4 *when* $q \equiv \pm 3 \pmod 8$.

(iv) *Any* D_8 *of class 1 is contained in* 2 *subgroups* S_4 *when* $q \equiv \pm 1 \pmod 8$.

(v) *Any* D_8 *is contained in one subgroup* S_4 *when* $q \equiv \pm 3 \pmod 8$.

(vi) *Any* D_{10} *of class 1 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 $\mathrm{PGL}(2,q)$ on the projective line. Here, the main tool is the following observation: If $H \leq K \leq \mathrm{PGL}(2,q)$, then any orbit of K is a union of orbits of H. In the following lemmas we suppose that H is a subgroup of $\mathrm{PGL}(2,q)$ and N_l denotes the number of orbits of size l. We only give non-regular orbits.

Lemma 7 *Let H be the cyclic group of order d, where $d|q \pm \epsilon$.*

(i) *Let $d = 2$. Then for H in class 1, we have $N_1 = 1 + \epsilon$ and for H in class 2, $N_1 = 1 - \epsilon$.*

(ii) *Let $d > 2$. Then $N_1 = 1 \mp \epsilon$.*

Proof. This is trivial by Theorem 1. □

Lemma 8 *Let H be the dihedral group of order $2d$, where $d|q \pm \epsilon$.*

(i) *Let $d = 2$. Then for H in class 1, we have $N_2 = 3(1 + \epsilon)/2$ and for H in class 2, $N_2 = (3 - \epsilon)/2$.*

(ii) *Let $d > 2$. Then $N_2 = (1 \mp \epsilon)/2$ and*

	$d\|\frac{q+\epsilon}{2}$, (c1)	$d\|\frac{q+\epsilon}{2}$, (c2)	$d\|\frac{q-\epsilon}{2}$, (c1)	$d\|\frac{q-\epsilon}{2}$, (c2)	$d \not\|\frac{q+\epsilon}{2}$	$d \not\|\frac{q-\epsilon}{2}$
N_d	$1+\epsilon$	$1-\epsilon$	$1+\epsilon$	$1-\epsilon$	1	1

where c1 and c2 denote classes 1 and 2, respectively.

Proof. (i) We know that H does not stabilize any point. So the orbits are of sizes 2 or 4. Now the assertion follows from solving the equations $N_2 + N_4 = \frac{1}{4}\sum_{g \in H} \mathrm{fix}(g)$ and $2N_2 + 4N_4 = q + 1$.

(ii) By Lemma 7, the orbits are of sizes 2, d or $2d$. The orbits of size 2 have the unique subgroup C_d of D_{2d} as their stabilizers. So by Lemma 7, we have $N_2 = (1 \mp \epsilon)/2$. Now N_d and N_{2d} are easily found in the same way to (i). □

Lemma 9 *Let H be the group A_4. Then $N_6 = (1 + \epsilon)/2$ and*

(i) *if $3|q \pm \epsilon$, then $N_4 = 1 \mp \epsilon$,*

(ii) *if $3|q$, then $N_4 = 1$.*

Proof. H has D_4 as a subgroup and therefore by Lemma 8, the orbit sizes are even. Since A_4 has no subgroup of order 6, there is no orbit of size 2. Hence, the possible orbit sizes are 4, 6 or 12. A_4 has 3 subgroups C_2 each fixing $1 + \epsilon$ points and therefore, we have $N_6 = (1 + \epsilon)/2$.

(i) H has a subgroup of order 3 fixing $1 \mp \epsilon$ points and therefore, $N_4 = 1 \mp \epsilon$.

(ii) H has a subgroup of order 3 with one fixed point. Hence, $N_4 = 1$. □

Lemma 10 *Let H be the group S_4. Then $N_6 = (1+\epsilon)/2$ and*

(i) *if $3|q+\epsilon$ and $8|q-\epsilon$, then $N_8 = \frac{1-\epsilon}{2}$ and $N_{12} = \frac{1+\epsilon}{2}$,*

(ii) *if $3|q+\epsilon$ and $8|q+3\epsilon$, then $N_8 = \frac{1-\epsilon}{2}$ and $N_{12} = \frac{1-\epsilon}{2}$,*

(iii) *if $3|q-\epsilon$ and $8|q-\epsilon$, then $N_8 = \frac{1+\epsilon}{2}$ and $N_{12} = \frac{1+\epsilon}{2}$,*

(iv) *if $3|q-\epsilon$ and $8|q+3\epsilon$, then $N_8 = \frac{1+\epsilon}{2}$ and $N_{12} = \frac{1-\epsilon}{2}$,*

(v) *if $3|q$, then $N_4 = 1$.*

Proof. By Lemma 9, the orbits are of sizes 4, 6, 8, 12 or 24. The orbits of size 6 have C_4 as their stabilizer and S_4 has three subgroups C_4. So by Lemma 7 and noting that $4|q-\epsilon$ and $4 \not| q+\epsilon$, we obtain that $N_6 = (1+\epsilon)/2$.

(i)–(iv) Let $3|q \pm \epsilon$. Since D_6 does not stabilize any point, there is no orbit of size 4. Now Lemma 9(i) implies $N_8 = \frac{1 \mp \epsilon}{2}$. If $8|q-\epsilon$, then H has a subgroup D_8 which by Lemma 8, apart from the regular orbits it has $(1+\epsilon)/2$ orbits of size 2 and $1+\epsilon$ orbits of size 4. So in this case, $N_{12} = (1+\epsilon)/2$. If $8|q+3\epsilon$, then H has a subgroup D_8 which by Lemma 8 has $(1+\epsilon)/2$ orbits of size 2 and one orbit of size 4. Hence, $N_{12} = (1-\epsilon)/2$.

(v) By Lemma 9(ii), $N_4 = 1$. We show that $N_{12} = 0$. If $8|q-\epsilon$, then $\epsilon = 1$ and H has a subgroup D_8 which by Lemma 8, apart from the regular orbits it has two orbits of size 4. So in this case $N_{12} = 0$. If $8|q+3\epsilon$, then $\epsilon = -1$ and H has a subgroup D_8 which apart from the regular orbits it has one orbit of size 4 by Lemma 8. Hence, we have $N_{12} = 0$. □

Lemma 11 *Let $5|q \pm \epsilon$ and H be the group A_5. Then $N_{12} = (1 \mp \epsilon)/2$ and*

(i) *if $3|q \pm \epsilon$, then $N_{20} = (1 \mp \epsilon)/2$ and $N_{30} = (1+\epsilon)/2$,*

(ii) *if $3|q$, then $N_{10} = 1$.*

Proof. H has 6 subgroups C_5 which are the stabilizer groups of their own fixed points. Therefore, by Lemma 7, $N_{12} = (1 \mp \epsilon)/2$.

(i) By Lemma 9, a subgroup A_4 of H has $(1 \mp \epsilon)/2$ orbits of size 4, $(1+\epsilon)/2$ orbits of size 6 and all other orbits are regular. So clearly the assertion holds.

(ii) We have $\epsilon = 1$. By Lemma 9, a subgroup A_4 of H has one orbit of size 4, one orbit of size 6 and all other orbits are regular. Therefore, the assertion is obvious. □

Lemma 12 *Let H be the elementary Abelian group of order p^m, where $m \leq n$. Then $N_1 = 1$.*

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 13 *Let H be a semidirect product of the elementary Abelian group of order p^m, where $m \leq n$ and the cyclic group of order d, where $d|q-1$ and $d|p^m-1$. Then $N_1 = 1$ and $N_{p^m} = 1$.*

Proof. H has an elementary Abelian subgroup of order p^m. So by Lemma 12, 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 7, the orbit sizes are congruent 0 or 1 modulo d. If congruent 0 modulo 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 14 *Let H be* $\mathrm{PSL}(2,p^m)$ *or* $\mathrm{PGL}(2,p^m)$, *where $m|n$. Then*

(i) *if $p^m+1|p^n-1$, then $\epsilon=1$ and we have $N_{p^m+1}=1$ and $N_{p^m(p^m-1)}=1$,*

(ii) *if $p^m+1|p^n+1$, then $N_{p^m+1}=1$.*

Proof. First let H be $\mathrm{PSL}(2,p^m)$. All subgroups $\mathrm{PSL}(2,p^m)$ of $\mathrm{PGL}(2,q)$ are conjugate by Theorem 2. So we may suppose that H is the group with the 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 $GF(p^m)\cup\{\infty\}$, we have one 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 13, all other orbits of H are of multiples of $p^m(p^m-1)/2$.

(i) It is easy to see that $\epsilon=1$. H has a subgroup D_{p^m+1}. By Lemma 8, we have one orbit of size $l(p^m+1)/2+2$ which is divisible by $p^m(p^m-1)/2$. Now we immediately find out that this orbit is of size $p^m(p^m-1)$. The remaining orbits are of sizes $p^m(p^m-1)/4$ or $p^m(p^m-1)/2$. Since C_2 is not the stabilizer of any point, we conclude that there is no orbit of size $p^m(p^m-1)/4$.

(ii) H has a 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 are of sizes $p^m(p^m-1)/4$ or $p^m(p^m-1)/2$. Since C_2 is not the stabilizer of any point, there is no orbit of size $p^m(p^m-1)/4$.

Now let H be $\mathrm{PGL}(2,p^m)$. Since H has a subgroup $\mathrm{PSL}(2,p^m)$ and C_2 is not the stabilizer of any point, the assertion follows immediately from the paragraphs above. □

5 The Möbius functions

In [2], we have made some calculations on the Möbius functions of the subgroup lattices of subgroups of $\mathrm{PSL}(2,q)$. We make use of the results of [2] and it turns out those are enough for our purposes and we will need no more calculations. For later use, we summarize the results in the following theorem.

Theorem 3 [2]

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

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

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

(iv) $\mu(A_4, S_4) = -1$, $\mu(D_8, S_4) = -1$, $\mu(D_6, S_4) = -1$, $\mu(C_4, S_4) = 0$, $\mu(D_4, S_4) = 3$ *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 2) and* $\mu(C_2, S_4) = 2$ *otherwise, and* $\mu(1, S_4) = -12$.

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

6 Determinations of f_k and g_k

In Section 4, we determined the sizes of orbits from the action of subgroups of $\mathrm{PGL}(2, q)$ on the projective line. The results are 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

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

The results of Section 4 show that any nontrivial subgroup H of $\mathrm{PGL}(2, q)$ has at most three non-regular orbits and so it is an easy task to compute f_k. Here, we do not give the values of f_k for the sake of briefness. As an example, the reader is referred to [2], where a table of values of f_k for the subgroups of $\mathrm{PSL}(2, q)$ is given.

The values of f_k are used to compute g_k. Let $1 \leq k \leq q+1$ and $k \not\equiv 0, 1 \pmod{p}$. The latter condition imposes $f_k(H)$ and $g_k(H)$ to be zero for any subgroup H belonging to one of the classes (vii)-(x) in Theorem 2. Let H be a subgroup lying in one of the classes (i)-(vi). By

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

we only need to care about those overgroups U of H for which $f_k(U)$ and $\mu(H, U)$ are nonzero. All we need on overgroups are provided by Theorem 2 and Lemmas 4–6. We also know the values of the Möbius functions and f_k. So we are now able to compute g_k. We will not give the explicit formulas for g_k, since we think it is only the simple problem of substituting the appropriate values in the above formula.

7 Orbit sizes and 3-designs from $\mathrm{PGL}(2, q)$

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

Lemma 15 *Let* H *be a subgroup of* $\mathrm{PGL}(2, q)$ *and let* $u(H)$ *denote the number of subgroups of* $\mathrm{PGL}(2, q)$ *conjugate to* H. *Then the number of orbits of* $\mathrm{PGL}(2, q)$ *on the* k*-subsets whose elements have stabilizers conjugate to* H *is equal to* $u(H)g_k(H)|H|/|\mathrm{PGL}(2, q)|$.

Proof. The number of k-subsets whose stabilizers are conjugate to H is $u(H)g_k(H)$ and such k-subsets lie in the orbits of size $|\operatorname{PGL}(2,q)|/|H|$. □

The lemma above and Theorem 2 help us to compute the sizes of orbits from the action of $\operatorname{PGL}(2,q)$ on the k-subsets of the projective line. Once the sizes of orbits are known, one may utilize them to find all values of λ for which there exist 3-$(q+1,k,\lambda)$ designs admitting $\operatorname{PGL}(2,q)$ as automorphism group.

Theorem 4 *Let $1 \leq k \leq q+1$ and $k \not\equiv 0,1 \pmod p$. Then the numbers of orbits of $G = \operatorname{PGL}(2,q)$ on the k-subsets of the projective line are as follows (where $d \mid q \pm \epsilon$ and $d > 2$) (c1 and c2 refer to classes 1 and 2, respectively).*

stabilizer	*id*	A_4	S_4	A_5	C_2 $(c1)$	C_2 $(c2)$	C_d
number of orbits	$\frac{g_k(1)}{q^3-q}$	$\frac{g_k(A_4)}{2}$	$g_k(S_4)$	$g_k(A_5)$	$\frac{g_k(C_2)}{q-\epsilon}$	$\frac{g_k(C_2)}{q+\epsilon}$	$\frac{dg_k(C_d)}{2(q\pm\epsilon)}$

stabilizer	D_4 $(c1)$	D_4 $(c2)$	$D_{2d}(c1, c2, d \mid \frac{q\pm\epsilon}{2})$	$D_{2d}(d \nmid \frac{q\pm\epsilon}{2})$
number of orbits	$\frac{g_k(D_4)}{6}$	$\frac{g_k(D_4)}{2}$	$\frac{g_k(D_{2d})}{2}$	$g_k(D_{2d})$

8 Non-isomorphic designs from $\operatorname{PSL}(2,p)$ and $\operatorname{PGL}(2,p)$

It is known that $\operatorname{PGL}(2,p)$ is maximal in S_{p+1} for $p > 23$ [8]. Let $p \equiv 3 \pmod 4$ and $p > 23$. Let X be the projective line and let H and K be some fixed subgroups $\operatorname{PSL}(2,p)$ and $\operatorname{PGL}(2,p)$ of the symmetric group on X, respectively such that $H < K$. For a given λ, let $\mathcal{S}$ and $\mathcal{G}$ be the sets of all nontrivial 3-$(p+1,k,\lambda)$ designs on X admitting H and K as automorphism group, respectively. Clearly, $\mathcal{G} \subseteq \mathcal{S}$. Since $\operatorname{PGL}(2,p)$ is not normal in S_{p+1}, all designs in $\mathcal{G}$ are mutually non-isomorphic. Moreover, these designs admit $\operatorname{PGL}(2,p)$ as their full automorphism group. Since $\operatorname{PSL}(2,p)$ is maximal in $\operatorname{PGL}(2,p)$, all designs in $\mathcal{F} = \mathcal{S} \setminus \mathcal{G}$ admit $\operatorname{PSL}(2,p)$ as their full automorphism group. It is easy to show that any design in $\mathcal{F}$ has exactly one isomorphic copy in $\mathcal{F}$. In fact, the normalizer of $\operatorname{PSL}(2,p)$ in S_{p+1} is $\operatorname{PGL}(2,p)$. So $g(\mathcal{D}) = \mathcal{D}'$ for distinct designs $\mathcal{D}$ and $\mathcal{D}'$ in $\mathcal{F}$ if and only if $g \in \operatorname{PGL}(2,p) \setminus \operatorname{PSL}(2,p)$.

References

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

[2] P. J. Cameron, H. R. Maimani, G. R. Omidi and B. Tayfeh-Rezaie, 3-Designs from $\mathrm{PSL}(2, q)$, *Discrete Math.*, to appear.

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

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

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

[6] S. Iwasaki and T. Meixner, A remark on the action of $\mathrm{PGL}(2, q)$ and $\mathrm{PSL}(2, q)$ on the projective line, *Hokkaido Math. J.* **26** (1997), 203–209.

[7] R. Laue, S. S. Magliveras and A. Wassermann, New large sets of t-designs, *J. Combin. Des.* **9** (2001), 40–59.

[8] M. W. Liebeck, Cheryl E. Praeger and J. Saxl, A classification of the maximal subgroups of the finite alternating and symmetric groups, *J. Algebra* **111** (1987), 365–383.