Hokkaido Mathematical Journal Vol. 26 (1997) p. 203–209

A remark on the action of $PGL(2, q)$ and $PSL(2, q)$ on the projective line

(Dedicated to Professor Takeshi Kondo on his sixtieth birthday)

Shiro IWASAKI and Thomas MEIXNER

(Received December 25, 1995)

Abstract. Let q be a prime power, $K=GF(q)$ the finite field with q elements, $\Omega=K\cup\{\infty\}$ the project line over K. Let 大 $=PGL(2,q)$ and 小 $=PSL(2,q)$ be the linear fractional group on Ω and the special linear fractional group on Ω, respectively. Let U be any non-trivial subgroup of the (cyclic) multiplicative group $K\backslash\{0\}$ and set $E=U\cup\{\infty\}$. The main purpose of this note is to determine the structures of $大_E$ and $小_E$, the setwise stabilizer of E in 大 and 小, respectively. Then, as an application, by taking various q and U, we obtain various 3-designs $(\Omega, E^{大})$ and 3 (resp. 2)-designs $(\Omega, E^{小})$ in case $q\equiv -1$, (resp. $q\equiv 1$) (mod 4), which contain new designs.

Key words: $PGL(2,q)$, $PSL(2,q)$, stabilizer, Frobenius group, design.

1. Introduction and notation

Throughout this note, we fix the following notation.

p :	any prime number
q :	a power of p
$K := GF(q)$	finite field with q elements
$\Omega := K\cup\{\infty\}$	projective line over K
$F := K\backslash\{0\}$	multiplicative group of K
大[1] $:= PGL(2,q) =$	$\{x\mapsto (ax+b)/(cx+d) \mid a,b,c,d\in K, ad-bc\in F\}$
小[2] $:= PSL(2,q) =$	$\{x\mapsto (ax+b)/(cx+d) \mid a,b,c,d\in K, ad-bc\in F^2\}$
m :	a divisor of $q-1$ with $m>1$
U :	a subgroup of order m of the (cyclic) group F
$E := U\cup\{\infty\}$	

1991 Mathematics Subject Classification : 20E07, 05B05.

1) '大' (dai) means 'large'.

2) '小' (shou) means 'small'.

大$_E$:	setwise stabilizer of E in 大
小$_E$:	setwise stabilizer of E in 小
$\widetilde{\boldsymbol{D}}(q,E) := (\Omega, E^{大})$	block design on the point set Ω, whose blocks are the images of E under the group 大
$\boldsymbol{D}(q,E) := (\Omega, E^{小})$	block design on the point set Ω, whose blocks are the images of E under the group 小

The main purpose of this short note is to determine the structures of 大$_E$ and 小$_E$. This is a generalization of [3, Proposition 3.1] and [4, Theorem]. As an application, by taking various q and U, we obtain various 3-designs $\widetilde{\boldsymbol{D}}(q,E)$ and 3 (resp. 2)-designs $\boldsymbol{D}(q,E)$ in case $q \equiv -1$ (resp. $q \equiv 1$) (mod 4). Some of these designs fill in several blanks in the table of Chee, Colbourn, Kreher [1].

2. Theorems and their proofs

Theorem A *Set $H :=$ 大$_E$. Then the following holds:*

(i) *If $m = 2$, whence $U = \{1, -1\}$, then $H \cong \Sigma_3$, the symmetric group of degree 3, and H is generated by the transformations $x \mapsto -x$ and $x \mapsto (x-3)/(x+1)$.*

(ii) *If $m = 3$, whence $U = \{1, \beta, \beta^2\}$ for some nontrivial cubic root of unity β, then $H \cong A_4$, the alternating group of degree 4, and H is generated by the transformations $x \mapsto \beta x$, and $x \mapsto (x+2)/(x-1)$.*

(iii) *If U is the multiplicative group of some subfield M of K, then H is conjugate in 大 to the group of all affine transformations $x \mapsto ax + b$, $a \in U$, $b \in M$, and H is a Frobenius group of order $m(m+1)$.*

(iv) *In all other cases, $H = \{x \mapsto ux \mid u \in U\}$ is cyclic of order m.*

Proof. First, we show that the stabilizer H_∞ of ∞ in H also stabilizes the point 0, and equals the group $C := \{x \mapsto ux \mid u \in U\}$. Clearly, C stabilizes 0 and is contained in H_∞. Conversely, let $\sigma : x \mapsto ax + b$ ($a \in F$, $b \in K$) be any element of H_∞ and take an element $u \in U \backslash \{1\}$. Then

$$aU + b = U^\sigma = U = uU = u(aU + b) = aU + ub,$$

and so $aU = aU + c$, where $c = b(u-1)$. Therefore, adding the number c to the elements of aU only permutes these elements. Hence, the set aU is a union of left cosets of the subgroup $\langle c \rangle$ of the additive group $(K,+)$. But the field K has characteristic p, so the subgroup $\langle c \rangle$ has order 1 or p. As the order of aU equals the order of U, and $m = |U|$ is a divisor of $q-1$, the order of aU can not be divisible by p, hence $\langle c \rangle$ has order 1 and $c = 0$. This forces $b = 0$, as u was chosen to be different from 1. Consequently, $a \in U$ and $\sigma \in C$. Thus, we have $H_\infty = C$, which acts regularly on U, is isomorphic to U, and hence cyclic of order m.

Assume H is not transitive on E, then the point ∞ must be fixed by H and $H = H_\infty$, and so $H = C$ by the above. Then we are in case (iv).

Assume that H is transitive on E. Then, as $C = H_\infty$ acts regularly on U, the group H acts sharply 2-transitively on the $m+1$ points of E and so is a Frobenius group of order $m(m+1)$ (see [2] V.8.2). Hence H has a normal subgroup N, which is regular on E, and $C = H_\infty$ acts transitively on the non-identity elements of N. This implies that N is an elementary abelian r-group for some prime r, and $m+1$ is some power of the prime r (see [2] II.2.3). As H is transitive on nonidentity elements of N, there is no proper nontrivial subgroup of N normal in H. This implies that N is contained in 小. Assume r is different from 2 and p. Then N is cyclic by Dickson's list of subgroups of 小 $= PSL(2,q)$ (see [2] II.8.27). Hence $|N| = r = m+1$. Moreover, the normalizer of N in 小 is dihedral (see [2] II.8.3–8.5) and N is a maximal cyclic subgroup of H. As $H \cap$ 小 has order $m(m+1)$ or $m(m+1)/2$ and is contained in the normalizer of N in 小, we see that $m/2 \leq 2$ and $m \leq 4$. Therefore, $r = 3$ or $r = 5$.

Assume $r = 5$. Then there is a Frobenius group of order 20 contained in 大 $= PGL(2,q) \subset PSL(2,q^2)$, which contradicts [2] II.8.27. Hence $r = 3$, and $m = 2$. Clearly, there is only one subgroup U of order 2 in F, hence we are in case (i). Conversely, for p odd, the transformations $x \mapsto -x$ and $x \mapsto (x-3)/(x+1)$ generate a subgroup H of 大 isomorphic to Σ_3 acting 2-transitively on $E = \{\infty\} \cup \{1,-1\}$.

Assume $r = 2$, different from p, whence N is an elementary abelian 2-group and from Dickson's list it follows that N has order 4 and $m = 3$. Now we are in case (ii). Conversely, if 3 divides $q-1$, take some nontrivial cubic root of unity β, then the transformations $x \mapsto \beta x$ and $x \mapsto (x+2)/(x-1)$ generate a subgroup H of 大 isomorphic to A_4 acting 2-transitively on $E = \{\infty\} \cup \{1, \beta, \beta^2\}$.

Assume $r = p$. The sharply 2-transitive group H on E now has a normal Sylow p-subgroup N. It is easily seen that the group N must have a unique fixed point α on Ω, left invariant by the whole of H, in particular by $C = H_\infty$, and so α must be one of the two fixed points of C, which are ∞ and 0. As N acts regularly on $E = U \cup \{\infty\}$, the unique fixed point of N must be 0. Hence H fixes the point 0.

Consider the element $t : x \mapsto 1/x$ of 大. It interchanges the points 0 and ∞ and leaves invariant the set U. It is easily verified that the transformation t normalizes C and maps E onto the set $M := E^t = \{0\} \cup U$. And H^t acts sharply 2-transitively on E^t, fixing the point ∞. Hence H^t acts on Ω through transformations $x \mapsto ax + b$, $a \in F$, $b \in K$. It is easily seen that elements of order p in this group act as transformations $x \mapsto x + b$.

We claim that M is a subfield of K with multiplicative group U, and the group H^t consists of all transformations $x \mapsto ax + b$, $b \in M$, $a \in U$. Clearly, as $0 \in E^t$, and since N^t is an elementary abelian p-group, the Frobenius kernel N^t of H^t consists of the transformations $x \mapsto x + b$, $b \in M$. As N^t is a group, M is an additive subgroup of K. Clearly, $M \backslash \{0\} = U$ is a (multiplicative) subgroup of F, and so M is a subfield of K. Still, $C = C^t$ acts on the projective line by transformations $x \mapsto ax$, $a \in U$, and so the group H^t consists of all the transformations $x \mapsto ax + b$, $a \in U$, $b \in M$, and we are in case (iii).

Conversely, if M is some subfield of K, and $U = M \backslash \{0\}$, then consider the group A of all transformations $x \mapsto ax + b$, $a \in U$, $b \in M$. It acts sharply 2-transitively on the subset M of Ω. The subgroup A^t of 大 for the transformation $t : x \mapsto 1/x$, acts 2-transitively on $E = \{\infty\} \cup U$. □

Remark. If U is a subgroup of F^2, then C is contained in 小, and the statements of the theorem hold for 小 instead of 大. In particular, the stabilizer of E in 大 is contained in 小. If U does not consist of squares only, the stabilizer of E in 大 contains properly the stabilizer of E in 小. Moreover we note that if 3 divides $q - 1$, then -3 is a square in K, whence the involution $x \mapsto (x + 2)/(x - 1)$ in (ii) of Theorem A is contained in 小. In fact, since $x^2 + x + 1 = (x - \beta)(x - \beta^2)$ for a nontrivial cubic root of unity β, by setting $x = 1$, we have $3 = (1 - \beta)(1 - \beta^2) = (1 - \beta) \cdot \beta^2 (\beta - 1) = -\beta^2(\beta - 1)^2$.

From this remark, we easily derive the following theorem.

Theorem B *Set $H :=$ 小$_E$. Then the following holds:*
(i) *If $m = 2$, whence $U = \{1, -1\}$ and q is odd, then $H \cong \Sigma_3$, and*

H is generated by $x \mapsto -x$, $x \mapsto (x-3)/(x+1)$, if -1 is a square in F, whereas $H \cong A_3$, and H is generated by the transformation $x \mapsto (x-3)/(x+1)$, if -1 is not a square in F.

(ii) *If $m = 3$, whence $U = \{1, \beta, \beta^2\}$ for some nontrivial cubic root of unity β, then $H \cong A_4$, and H is generated by the transformations $x \mapsto \beta x$, and $x \mapsto (x+2)/(x-1)$.*

(iii) *If U is the multiplicative group of some subfield M of K, then H is conjugate in 大 to the group of all affine transformations $x \mapsto ax+b$, $a \in U \cap F^2$, $b \in M$, hence H is a Frobenius group of order $m(m+1)$ or $m(m+1)/2$.*

(iv) *Otherwise, $H = \{x \mapsto ux \mid u \in U \cap F^2\}$ is cyclic of order m or $m/2$.*

3. Application of Theorems

We recall a well-known general fact that, for a t-homogeneous group H on a finite set Γ with $|\Gamma| = v$ and a subset A of Γ with $|A| = k \geq t$, the pair (Γ, A^H) is a t-(v,k,λ) design, where A^H is the set of images of A under the group H, $\lambda = |H| \binom{k}{t} / |H_A| \binom{v}{t}$ and H_A is the setwise stabilizer of A in H. Since 大 is 3-homogeneous on Ω of order $(q+1)q(q-1)$ and 小 is 3 (resp. 2)-homogeneous on Ω of order $(q+1)q(q-1)/2$ in case $q \equiv -1$ (resp. $q \equiv 1$) (mod 4), we have at once

Lemma *The following holds.*

(1) *$\widetilde{\boldsymbol{D}}(q,E)$ is a 3-$(q+1, |E|, |E|(|E|-1)(|E|-2)/|\text{大}_E|)$ design.*

(2) (i) *If $q \equiv -1 \pmod 4$, then*
$\boldsymbol{D}(q,E)$ is a 3-$(q+1, |E|, |E|(|E|-1)(|E|-2)/2|\text{小}_E|)$ design.

(ii) *If $q \equiv 1 \pmod 4$, then*
$D(q,E)$ is a 2-$(q+1, |E|, |E|(|E|-1)(q-1)/2|\text{小}_E|)$ design.

It is clear, that for any choice of E, the designs $\widetilde{\boldsymbol{D}}(q,E)$ and $\boldsymbol{D}(q,E)$ coincide, if 大 $=$ 小, i.e. if $p = 2$, or if $p > 2$ and $|\text{大}_E| = 2|\text{小}_E|$. In case $p > 2$ and $\text{大}_E = \text{小}_E$, the design $\widetilde{\boldsymbol{D}}(q,E)$ has twice as many blocks as the design $\boldsymbol{D}(q,E)$.

Assume $p > 2$. Then the situation is clearly well understood in case (i), i.e. for $m = 2$, where the blocks of $\widetilde{\boldsymbol{D}}(q,E)$ are just all 3-subsets of Ω. In cases (iii) and (iv), the situation depends on the question, whether $2m$ divides $q-1$ or not. Remarkably, in case (ii), always $\widetilde{\boldsymbol{D}}(q,E)$ and $\boldsymbol{D}(q,E)$ are different.

By combining the lemma with Theorems A and B, and taking various q and U, we obtain various 3-and 2-designs. In a particular, [3, Theorem 3.2] (resp. [4, Theorem]) dealt with the case $q \equiv -1 \pmod 4$ and $U = F^2$ (resp. q is a prime and $q-1 = 2^e m$, m odd, $e \geq 2$, and $U = F^{2^i}$, $1 \leq i \leq e$).

Here, we give only examples which fill in blanks in the table of [1] (the new ones are marked with $*$, whereas desigs given already in [3, 4] are marked with $*'$).

q	$q-1$	U	$\boldsymbol{D}(q,E)$: 2- or 3-$(q+1,k,\lambda)$	$\widetilde{\boldsymbol{D}}(q,E)$: 3-$(q+1,k,\lambda)$
		F^2	2-$(26,13,12\cdot 13)$	3-$(26,13,11\cdot 13)^*$
		F^3	2-$(26,9,72\cdot 3)$	3-$(26,9,21\cdot 3)^*$
5^2	$2^3\cdot 3$	F^4	2-$(26,7,42\cdot 2)^*$	3-$(26,7,35)$
		F^6	2-$(26,5,4\cdot 3)$	3-$(26,5,3)^*$
		F^8	2-$(26,4,6\cdot 2)$	3-$(26,4,2)$
3^3	$2\cdot 13$	F^2	3-$(28,14,6\cdot 14)^{*'}$	3-$(28,14,6\cdot 28)^*$
		F^2	2-$(30,15,14\cdot 15)$	3-$(30,15,13\cdot 15)^{*'}$
29	$2^2\cdot 7$	F^4	2-$(30,8,28\cdot 4)^{*'}$	3-$(30,8,6\cdot 8)^{*'}$
		F^7	2-$(30,5,4\cdot 35)$	3-$(30,5,3\cdot 5)^*$

References

[1] Chee Y.M., Colbourn C.J. and Kreher D.L., *Simple t-designs with $v \leq 30$.* Ars Combin. **29** (1990), 193–258.

[2] Huppert B., *Endliche Gruppen I.* Springer, 1967.

[3] Iwasaki S., *An elementary and unified approach to the Mathieu-Witt systems.* J. Math. Soc. Japan **40** (1988), 393–414.

[4] Iwasaki S., *Infinite families of 2-and 3-designs with parameters $v = p+1$, $k = (p-1)/2^i + 1$, where p odd prime, $2^e \top (p-1)$, $e \geq 2$, $1 \leq i \leq e$.* (to appear in J. Combin. Designs)

Shiro Iwasaki
Department of Mathematics
Hitotsubashi University
Kunitachi, Tokyo 186, Japan
E-mail: iwasaki@math.hit-u.ac.jp

Thomas Meixner
Mathematisches Institut der
Justus-Liebig-Universität Gießen
Arndtstraße 2, 35392 Gießen, Deutschland
E-mail: Thomas.Meixner@math.uni-giessen.de