Simple 3-designs of $PSL(2,q)$ with block size 7 *

Luozhong Gong and Weijun Liu †

[a]School of Mathematics, Central South University, Changsha, Hunan, 410075, P. R. China

Abstract

This paper devotes to the investigation of 3-designs admitting the special projective linear group $PSL(2,q)$ as an automorphism group. When $q \equiv 3 \pmod 4$, we determine all the possible values of λ in the simple 3-$(q+1,7,\lambda)$ designs admitting $PSL(2,q)$ as an automorphism group.

1 Introduction

For positive integers k, v and λ with $3 \leq k \leq v$ and $\lambda > 0$, we define a t-(v,k,λ) design to be a finite incidence structure $\mathcal{D} = (X, \mathcal{B}, I)$, where X denotes a set of v points, and $\mathcal{B}$ a set of k-subsets of X called blocks, such that any t-subset of X is incident with exactly λ blocks. We use b to denote the number of the elements of $\mathcal{B}$. Such a design $\mathcal{D}$ is said to be simple if $\mathcal{B}$ has no repeated blocks. In this paper, we only consider simple 3-designs. We consider automorphisms of $\mathcal{D}$ as pairs of permutations on X and $\mathcal{B}$ which preserve incidence. An automorphism group of $\mathcal{D}$ is a group whose elements are automorphisms of $\mathcal{D}$ and call it t-homogeneous if it acts t-homogeneously on the points of $\mathcal{D}$.

Among classical simple groups, the structure of the subgroups and the permutation character of the elements of the projective special linear group $PSL(2,q)$ are best well-known (see [2]). And it is well known that $PSL(2,q)$ is 3-homogeneous if and only if $q \equiv 3 \pmod 4$. Therefore, a 3-$(q+1,k,\lambda)$ design admits $PSL(2,q)$ as an automorphism group if and only if its block set is the union of orbits of $PSL(2,q)$ on the set of k-subsets. Thus it is easy to see that if $k > 3$ each orbit of k-subsets of X is the block set of a simple 3-$(q+1,k,\lambda)$ design for some λ. This simple observation has led different authors to use this group for constructing 3-designs (see [1, 3-9]). In [1], all 3-designs with block size 4 or 5 and admitting $PSL(2,q), q \equiv 3 \pmod 4$ as an automorphism group are completely determined. When $q \equiv 1 \pmod 4$, quadruple systems from $PSL(2,q)$ are determined in [8]. For all 3-designs with block size 6 admitting $PSL(2,q)$, where $q \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$, are reported in [9] and [7] respectively. In this paper, using a similar method as in [9], we investigate the existence of 3-designs with block size 7 from $PSL(2,q)$ and determine all the possible values of λ in the simple 3-$(q+1,7,\lambda)$ designs admitting $PSL(2,q)$ as an automorphism group. Throughout this paper, we let $q \equiv 3 \pmod 4$, and $G = PSL(2,q)$.

*Supported by the National Natural Science Foundation of China (Grant No. 10871205 and 10971252) and Scientific Research Fund of Hunan Provincial Education Department (09C444).

†Corresponding author: wjliu6210@126.com

Main Theorem: There exists a 3-$(q+1,7,\lambda)$ design with automorphism group G and $1 < \lambda \leq \binom{q-2}{4}$ if and only if one of the following cases holds:

(i) If $q \equiv 71, 251 \pmod{420}$, then $\lambda \equiv 0, 1, 15, 21 \pmod{35}$.

(ii) If $q \equiv 211, 391 \pmod{420}$, then $\lambda \equiv 0, 15, 21, 36 \pmod{105}$.

(iii) If $q \equiv 3, 19, 67, 87, 103, 123, 139, 163, 187, 199, 207, 243, 247, 283, 303, 319, 367, 387, 403 \pmod{420}$, then $35|\lambda$.

(iv) If $q \equiv 31, 151, 271, 331 \pmod{420}$, then $\lambda \equiv 0, 21 \pmod{35}$.

(v) If $q \equiv 11, 131, 191, 311 \pmod{420}$, then $\lambda \equiv 0, 21 \pmod{105}$.

(vi) If $q \equiv 27, 43, 127, 139, 183, 223, 267, 307, 363, 379 \pmod{420}$, then $\lambda \equiv 0, 15 \pmod{35}$.

(vii) If $q \equiv 83, 239, 323, 379, 419 \pmod{420}$, then $\lambda \equiv 0, 15 \pmod{105}$.

(viii) If $q \equiv 23, 47, 59, 79, 143, 179, 203, 227, 299, 347, 359, 383 \pmod{420}$, then $105|\lambda$.

2 Notation and Preliminaries

In this section, we give some notation and preliminaries which will be used throughout this paper.

For $B \subseteq X$, let $G(B) = \{g(B) : g \in G\}$ denote the orbit of B under G and $G_B = \{g \in G : g(B) = B\}$ denote the stabilizer of B under G. It is well known that $|G| = |G(B)||G_B|$. It follows that G is an automorphism group of a 3-design $(X, \mathcal{B}, I)$ if and only if $\mathcal{B}$ is a union of orbits of k-subsets of X under G (see [3]). If $G(B)$ is the set of blocks of a $3-(v,k,\lambda)$ design, then we call $G(B)$ forms a $3-(v,k,\lambda)$ design or $G(B)$ is a 3-$(q+1,7,\lambda)$ design.

Let $q = p^f$, where p is a prime and f a positive integer, and let $X = GF(q) \cup \infty$. We define $b/0 = \infty, b/\infty = 0, b - \infty = \infty - b = \infty, \infty/\infty = 1$. For any $a, b, c, d \in GF(q)$, if $ad - bc$ is a non zero square , then the set of all mappings

$$f(x) = \frac{ax+b}{cx+d}$$

on X is a group under composition of mappings, called projective special linear group and denoted as $PSL(2,q)$. From [2] we gather some important results on $PSL(2,q)$ which are used below.

Lemma 2.1 *The group $G = PSL(2,q)$ acts 2-transitively on the point set of X, and each non-identity element of G has at most two fixed points on X.*

Lemma 2.2 *Let P be a p-Sylow subgroup of $PSL(2,q)$, then P is isomorphic to the additive group of $GF(q)$, and the elements of P have a common fixed point and each non-identity element of P only has this fixed point.*

Lemma 2.3 *The subgroup U of $G = PSL(2,q)$ which fixes the number 0 and ∞ is a cycle-group of order $u = \frac{p^f-1}{d}$, where $d = (p^f-1, 2)$.*

Lemma 2.4 *The group $G = PSL(2,q)$ has a cycle-group S of order $u = \frac{p^f+1}{d}$, where $d = (p^f-1, 2)$. And if $e \neq s \in S$, then s has no fixed points on $GF(q) \cup \infty$.*

Lemma 2.5 *The structure of the elements of $PSL(2,q), q = p^f, q \equiv 3 \pmod 4$ is given in the following table, where $\varphi(d)$ denotes the Euler function.*

Order	Order of the centralizer	Number of conjugacy classes	Type
1	$\frac{q^3-q}{2}$	1	1^{q+1}
2	$q+1$	1	$2^{(q+1)/2}$
p	q	2	$1^1\, p^{q/d}$
$d\|\frac{q-1}{2}$	$\frac{q-1}{2}$	$\frac{\varphi(d)}{2}$	$1^2\, d^{(q-1)/d}$
$d\|\frac{q+1}{2},\ d\neq 2$	$\frac{q+1}{2}$	$\frac{\varphi(d)}{2}$	$d^{(q-1)/d}$

where a^b denotes the cycle decomposition of b a-cycles.

Lemma 2.6 *(see[3]) Let $\mathcal{D}=(X,\mathcal{B},I)$ be a t-(v,k,λ) design. Then the following equations hold:*

(a) $bk=vr$.

(b) $\binom{v}{t}\lambda=b\binom{k}{t}$.

3 Orbits of 7-subsets

In this section we will determine the possible sizes of orbits of 7-subsets of X under G and its number. Let B be a 7-subset of X. Now we discuss the order of G_B.

Lemma 3.1 *Let B be a 7-subset of X. Then $|G_B|\neq 21,35,105,15$.*

Proof. First suppose $|G_B|=15$. By Sylow theorem, $n_3=n_5=1$, where n_3 and n_5 denote the number of Sylow 3-subgroups and Sylow 5-subgroups, respectively. Therefore there is a unique group of order 15 which is cyclic, G_B has an element of order 15, but such an element cannot fix B, a contradiction.

When $|G_B|=21$, then $3|q(q-1)(q+1)$. Note that $q\equiv 3 \pmod 4$, and so $3|q$ or $3|(q-1)$. First suppose that $3|(q-1)$. Since there is a normal subgroup H of order 7 and 7 subgroups $K_i (i=1,2,\cdots,7)$ of order 3 in G_B, for any $h\in H$ and $k_1\in K_i$(for some i) there exists some $k_2\in K_j$(for some j) such that $hk_1=k_2$. By Lemma 2.3, k_1 and k_2 fix exactly two elements x_1,x_2 of B. Since $hk_1(x_i)=k_2(x_i)=x_i (i=1,2)$, we have $h(x_i)=x_i$ which conflicts with the fact that h has no fixed points in B or $|h|=7$. For $3|q$, similar arguments hold. So $|G_B|\neq 21$.

When $|G_B|=35$, by Sylow theorem, $n_7=n_5=1$, where n_7 and n_5 denote the number of Sylow 7-subgroups and Sylow 5-subgroups , respectively. Therefore there is a unique group of order 35 which is cyclic, G_B has an element of order 35. but such an element cannot fix B.

Finally suppose $|G_B|=105$, and we let n_3,n_5 and n_7 denote the number of Sylow 3-subgroups, Sylow 5-subgroups and Sylow 7-subgroups, respectively. Then at least one of n_3,n_5 and n_7 equals one. If $n_3=1$ or $n_5=1$, then there is a normal subgroup of order 5 or 3 in G_B, and so there is a cyclic subgroup of order 15 in G_B, which is impossible. If $n_7=1$, then there is a normal subgroup of order 7 in G_B. Thus there is a subgroup of order 35 in G_B, which is impossible.

It is well known that the necessary conditions for the existence of a t-(v,k,λ) design is

$$\lambda\binom{v-i}{t-i}\equiv 0\left(mod\binom{k-i}{t-i}\right) \qquad (1)$$

for $0 \leq i \leq t$. This fact together with Lemma 2.6 can deduce the following Lemma.

Lemma 3.2 *Every orbit of 7-subsets under G is the set of blocks of a 3-$(q+1, 7, \lambda)$ design with $\lambda \in \{15, 21, 35, 105\}$.*

Proof. Since $G(B)$ is a 3-$(q+1, 7, \lambda)$ design, we have by Lemma 2.6

$$G(B) = \lambda \binom{q+1}{3} / \binom{7}{3}.$$

Therefore, by $|G| = |G(B)||G_B|$, we see $\lambda|G_B| = 105$. By condition (1), $5|\lambda(q-1)$ and so if $q \not\equiv 11 \pmod{20}$, then $5|\lambda$. It follows that $\lambda = 5, 15, 35, 105$. If $q \equiv 11 \pmod{20}$, then $\lambda = 1, 3, 5, 7, 15, 21, 35, 105$. By Lemma 3.1, $\lambda \neq 1, 3, 5, 7$, so $\lambda \in \{15, 21, 35, 105\}$.

From now on, we let N_λ denote the number of the orbits each of which forms a 3-$(q+1, 7, \lambda)$ design. Let B be a 7-subset of X, and $G(B)$ is the set of blocks of a $3-(q+1, 7, \lambda)$ design. Then G acts block-transitively on this design.

Remark 1. If both $G(B)$ and $G(B')$ are all the $3-(q+1, 7, \lambda)$ designs, then either $G(B) \cap G(B') = \emptyset$ or $G(B) = G(B')$. Therefore, for fixed λ, the number of B satisfying $G(B)$ is a $3-(q+1, 7, \lambda)$ design is equal to

$$\lambda \binom{q+1}{3} N_\lambda / \binom{7}{3}.$$

In the following, we will determine the N_λ for $\lambda \in \{15, 21, 35, 105\}$.

Lemma 3.3 *If $q \equiv 11 \pmod{20}$, then $N_{21} = 1$. Otherwise, $q \equiv 3, 7, 19 \pmod{20}$ and $N_{21} = 0$.*

Proof. Let $G(B)$ form a 3-$(q+1, 7, 21)$ design. Since $\lambda|G_B| = 105$ and $\lambda = 21$, we have $|G_B| = 5$. Thus every element of order 5 of G_B fixes at least two points of B. By Lemmas 2.2-2.4, we have 5 divides $(q-1)$. Since $q \equiv 3 \pmod 4$, we have $q \equiv 11 \pmod{20}$. By **Remark 1**, the number of such $B's$ is $21 \binom{q+1}{3} N_{21} / \binom{7}{3}$. On the other hand, by Lemma 2.5 each element of order 5 of G fixes exactly $(q-1)/5$ 7-subsets of X each of which is fixed exactly by 4 elements of order 5, and there are exactly $2q(q+1)$ elements of order 5 in G. Therefore, the elements of order 5 of G fix exactly $q(q+1)(q-1)/10$ distinct 7-subsets of X. So we have $21 \binom{q+1}{3} N_{21} / \binom{7}{3} = q(q+1)(q-1)/10$, and hence $N_{21} = 1$.

Lemma 3.4 *If $q \equiv 15, 27 \pmod{28}$, then $N_{15} = 1$. Otherwise, $q \equiv 3, 7, 11, 19, 23 \pmod{28}$ and $N_{15} = 0$.*

Proof. Let $G(B)$ form a 3-$(q+1, 7, 15)$ design. Then $|G_B| = 7$. Thus 7 divides $q(q-1)(q+1)$. If $7|(q+1)$, then $q \equiv 27 \pmod{28}$. By Lemma 2.5 each element of order 5 of G fixes exactly $(q+1)/7$ 7-subsets of X each of which is fixed exactly by 6 elements of order 7 and there are exactly $3q(q-1)$ elements of order 7 in G. Therefore, the elements of order 7 of G fix exactly $q(q+1)(q-1)/14$ distinct 7-subsets of X. By **Remark 1**, we have $15\binom{q+1}{3}N_{15}/\binom{7}{3} = q(q+1)(q-1)/14$. and hence $N_{15} = 1$. If $7|(q-1)$, then $q \equiv 15 \pmod{28}$. Similarly, we can get $N_{15} = 1$. If $7|q$, then $q = 7^f$ with f odd (note that here $q \equiv 3 \pmod 4$). By Lemma 2.5 each element of order 7 of G fixes exactly $q/7$ 7-subsets of X each of which is fixed exactly by 6 elements of order 7 and there are exactly $(q-1)(q+1)$ elements of order 7 in G. Therefore, the elements of order 7 of G fix exactly $q(q+1)(q-1)/42$ distinct 7-subsets of X. By **Remark 1**, we have $15\binom{q+1}{3}N_{15}/\binom{7}{3} = q(q+1)(q-1)/42$, and hence $N_{15} = 1/3$, which is impossible.

Lemma 3.5 *The value of N_{35} is given by*

$$N_{35} = \begin{cases} \frac{q-3}{6} & \text{if } q \equiv 3 \pmod{12} \\ \frac{q-4}{3} & \text{if } q \equiv 7 \pmod{12} \\ 0 & \text{if } q \equiv 11 \pmod{12} \end{cases}.$$

Proof. Let $G(B)$ form a 3-$(q+1,7,35)$ design. Then $|G_B| = 3$. Thus the elements of order 3 fix at least one point of B. By Lemmas 2.2-2.4, we have $3|q$ or $3|(q-1)$. If $3|(q+1)$, then $N_{35} = 0$ and $q \equiv 11 \pmod{12}$. If $3|q$, then, by Lemma 2.5, each element of order 3 of G fixes exactly $\binom{\frac{q}{3}}{2} = \frac{q(q-3)}{18}$ 7-subsets of X each of which is fixed exactly by 2 elements of order 3 and there are exactly $(q-1)(q+1)$ elements of order 3 in G. Therefore, the elements of order 3 of G fix exactly $q(q+1)(q-1)(q-3)/36$ distinct 7-subsets of X. By **Remark 1**, we have $35\binom{q+1}{3}N_{35}/\binom{7}{3} = q(q+1)(q-1)(q-3/36$, and hence $N_{15} = \frac{q-3}{6}$.

If $3|(q-1)$, by Lemma 2.5 each element of order 3 of G fixes exactly $2\binom{\frac{q-1}{3}}{2} = \frac{(q-1)(q-4)}{9}$ 7-subsets of X each of which is fixed exactly by 2 elements of order 3 and there are exactly $q(q+1)$ elements of order 3 in G. Therefore, the elements of order 3 of G fix exactly $q(q+1)(q-1)(q-4)/18$ distinct 7-subsets of X. By **Remark 1** again, we have $35\binom{q+1}{3}N_{35}/\binom{7}{3} = q(q+1)(q-1)(q-4)/18$, and hence $N_{35} = \frac{q-4}{3}$.

Lemma 3.6 *The value of N_{105} is in the following:*
(1) If $q \equiv 27, 267, 183, 363 \pmod{420}$, then

$$N_{105} = \frac{q^4 - 14q^3 + 71q^2 - 294q + 180}{2520};$$

(2)If $q \equiv 3, 123, 243, 303, 87, 207, 387 \pmod{420}$, then

$$N_{105} = \frac{q^4 - 14q^3 + 71q^2 - 294q + 540}{2520};$$

(3) If $q \equiv 211, 391 \pmod{420}$, then

$$N_{105} = \frac{q^4 - 14q^3 + 71q^2 - 434q + 376}{2520};$$

(4) If $q \equiv 31, 151, 271, 331 \pmod{420}$*, then*

$$N_{105} = \frac{q^4 - 14q^3 + 71q^2 - 434q + 736}{2520};$$

(5) If $q \equiv 139, 379, 223, 43, 307, 127 \pmod{420}$*, then*

$$N_{105} = \frac{q^4 - 14q^3 + 71q^2 - 434q + 880}{2520};$$

(6) If $q \equiv 7, 343 \pmod{420}$*, then*

$$N_{105} = \frac{q^4 - 14q^3 + 71q^2 - 434q + 1000}{2520};$$

(7) If $q \equiv 283, 403, 103, 163, 67, 187, 247, 367, 19, 139, 199, 319 \pmod{420}$*, then*

$$N_{105} = \frac{q^4 - 14q^3 + 71q^2 - 434q + 1240}{2520};$$

(8) If $q \equiv 71, 251 \pmod{420}$*, then*

$$N_{105} = \frac{q^4 - 14q^3 + 71q^2 - 154q - 744}{2520};$$

(9) If $q \equiv 311, 11, 131, 191 \pmod{420}$*, then*

$$N_{105} = \frac{q^4 - 14q^3 + 71q^2 - 154q - 384}{2520};$$

(10) If $q \equiv 323, 83, 379, 139, 239, 419 \pmod{420}$*, then*

$$N_{105} = \frac{q^4 - 14q^3 + 71q^2 - 154q - 240}{2520}.$$

(11) If $q \equiv 23, 143, 203, 383, 47, 227, 347, 59, 79, 179, 299, 359 \pmod{420}$*, then*

$$N_{105} = \frac{q^4 - 14q^3 + 71q^2 - 154q + 120}{2520}.$$

Proof. By counting the 7-subsets of X containing $0, 1, \infty$, we have the equation

$$15N_{15} + 21N_{21} + 35N_{35} + 105N_{105} = \binom{q-2}{4}. \tag{2}$$

According to Lemmas 3.3-3.5, N_{15}, N_{21} and N_{35} are known. Therefore, we solve easily the value of N_{105} from equation (3.2).

4 The proof of the main theorem

Proof. (i) Let $\mathcal{D}$ be a a simple 3-$(q+1,7,\lambda)$ design admitting G as an automorphism group. It is well known that a simple 3-$(q+1,7,\lambda)$ design admits G as an automorphism group if and only if its block set is the union of orbits of G on the set of 7-subsets. By Lemma 3.2, we know that in each orbit of G on the set of 7-subsets the possible numbers of blocks incident with $\{0,1,\infty\}$ are 15, 21, 35, 105. If $q \equiv 71, 251 \pmod{420}$, then $N_{21} = 1 = N_{15}$ by Lemmas 3.3 and 3.4. Therefore, $\lambda \equiv 0, 1, 15, 21 \pmod{35}, 1 < \lambda \leq \binom{q-2}{4}$, so the necessity follows.

Conversely, for each $\lambda \equiv 0, 1, 15, 21 \pmod{35}, 1 < \lambda \leq \binom{q-2}{4}$, there exist non-negative integers $x \leq N_{35}$, $y \leq N_{105}$, $z \leq 1$ and $u \leq 1$ such that

$$\lambda = 35x + 105y + 15z + 21u.$$

We take x orbits of length $|G|/3$, y orbits of length $|G|$, z orbits of length $|G|/7$ and u orbits of length $|G|/5$, then this gives a simple 3-$(q+1,7,\lambda)$ design admitting G as an automorphism group. This proves the sufficiency.

Similar to the proof of (i), we can show the cases (ii)-(viii).

Acknowledgment

The first author would like to express deep gratitude to his supervisor Prof. Liu Weijun whose guidance and support were crucial for the successful completion of this paper. The authors also would like to thank the referee for pointing out errors in the original version of this paper.

References

[1] C.A. Cusack, S.W. Graham, D.L. Kreher, Large sets of 3-designs from $PSL(2,q)$ with block sizes 4 and 5, J. Combin. Des. 3(2)(1995),147-160.

[2] L.E. Dickson, Linear Groups, with an Introduction to the Galois Field Theory, Dover Publications, NewYork, 1958.

[3] T. Beth, D. Jungnickel, H. Lenz, Design Theory, Cambridge University Press, Cambridge, England, 1993.

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

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

[6] R. Laue, S.S. Magliveras, A.Wassermann, New large sets of t-designs, J. Combin. Des. 9 (1) (2001), 40-59.

[7] W. Li and H. Shen, 3-Designs of $PSL(2,2^n)$ with block size 6, Discrete Math 308(2008),3061-3071.

[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. Combin. Des. 5(2) (1997), 95-110.

[9] G.R. Omidi, M.R. Pournaki and B. Tayfeh-Rezaie, 3-Designs with block size 6 from $PSL(2,q)$ and their large sets, Discrete Math 307(2007)1580-1588.