Simple 3–designs of $PSL(2,2^n)$ with block size 7 *

Luozhong Gong[1]† Guobing Fan[2]

[1]Institute of Computational Mathematics, Hunan University of Science and Engineering Yongzhou, Hunan, 425100, P. R. China,

[2]Hunan College of Finance and Economics, Changsha, Hunan, 410205, P. R. China

Abstract

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

MSC: 05B05; 20B25

Keywords: 3–designs; block transitive; projective linear groups

1 Introduction

For positive integers $3 \le k \le v$ and $\lambda > 0$, we define a 3-(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 3-subset of X is incident with exactly λ blocks. 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 [1]). And it is well known that $PSL(2,q)$ is 3-homogeneous if and only if $q \equiv 3 \pmod 4$. Therefore, a 3-$(q+1,k,\lambda)$

*Supported by Scientific Research Fund of Hunan Provincial Education Department(Grant No. 12B050), the Construct Program of the Key Discipline in Hunan University of Science and Engineering and the NNSFC (11271028, 11301377,11326057).

†Corresponding author: gonglztop@126.com

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 a simple 3-$(q+1,k,\lambda)$ design for some λ. When $q = 2^n$, $PSL(2,2^n)$ is isomorphic to projective general linear group $PGL(2,2^n)$, so it is sharp 3-transitive, and certainly is 3-homogeneous. This simple observation has led different authors to use this group for constructing 3-designs(see[2, 3, 4, 5, 6, 7]). In [3], all 3-designs with block size 4 and 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 [7]. For all 3-designs with block size 6 admitting $PSL(2,q)$, when $q \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$, are reported in [4] and [5] respectively. In [8], we investigate the existence of simple 3-designs with block size 7 from $PSL(2,q)$ with $q \equiv 3 \pmod 4$ 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. In the paper, we continue this work, and consider the existence of simple 3-designs with block size 7 from $PSL(2,2^n)$ and determine all the possible values of λ in the simple 3-$(2^n+1,7,\lambda)$ designs admitting $G = PSL(2,2^n)$ as an automorphism group.

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*

$$\lambda = 15x_1 + 21x_2 + 70x_3 + 105x_4 + 210x_5,$$

and

$$0 \leq x_1, x_2 \leq 1, 0 \leq x_3 \leq N_{70}, 0 \leq x_4 \leq N_{105}, 0 \leq x_5 \leq N_{210},$$

where N_λ denotes the number of orbits which form a $3-(2^n+1,7,\lambda)$ design.

2 Notation and Preliminaries

In this section, we give some notations 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 the 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 [9]).

Let q be a prime power and let $X = GF(q) \cup \infty$, called projective line. 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 is denoted by $PSL(2, q)$. When $q = 2^n$, $PSL(2, 2^n)$ is isomorphic to projective general linear group $PGL(2, 2^n)$.

From [1] we can gather some important results on $PSL(2, q)$ which are used below.

Lemma 2.1 *$G = PSL(2, q)$ 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 *$G = PSL(2, q)$ 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 $g's$ of $PSL(2, q), q = 2^n$ is given in the following table, where $\varphi(d)$ denotes the Euler function.*

Order of the g	Order of centralizer	Number of conjugate classes	$\chi(g)$
1	$6\binom{2^n+1}{3}$	1	$2^n + 1$
2	2^n	1	1
$d \mid 2^n - 1$	$2^n - 1$	$\frac{\varphi(d)}{2}$	2
$d \mid 2^n + 1$	$2^n + 1$	$\frac{\varphi(d)}{2}$	0

Where $\chi(g)$ denots the number of fixed points by element g.

Lemma 2.6 *(see[9]) 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 Order of stabilisers of 7-subsets

In this section we will determine the possible sizes of orbits of 7-subset 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 $|G_B| \neq 6, 30, 70, 210$.*

Proof. (1) If $|G_B| = 6$, by Sylow theorem, there is a normal subgroup H of order 3 and 3 subgroups of order 2, K_1, K_2, K_3 in G_B. Let $k \in G_B$ be one element of order 2, then there are $h_1, h_2 \in H$. such that $kh_1 = h_2k$. Note that h_1, h_2 fix exactly one element x of B. we have $k(x) = k(h_1(x_i)) = h_2(k(x))$, then $k(x) = x$, which implies that k and h fix a same point in B. By lemma 2.5, h fix exactly two pionts in X, write as $\{x, x'\}$. Since $H^k = H$, so H fix $k(x')$, which implies $k(x') = x'$ since $k(x) = x$, a contridiction.

(2) If $|G_B| = 30$, then there is $H \leq G_B$ with $|H| = 15$ by Sylwo theorem. Also 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 of H, 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.

(3) If $|G_B| = 70, 210$,then there $H \leq G_B = 35$ with $|H| = 35$ by Sylow theorem. Then $n_7 = n_5 = 1$, where n_7 and n_5 denote the number of Sylow 7-subgroups and Sylow 5-subgroups of H 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.

Lemma 3.2 *Let B be a 7-subset of X. If $5 \mid |G_B|$ or $7 \mid |G_B|$ then $2 \mid |G_B|$, and the $G(B)$ is the only orbit content with the condition.*

Proof. If $5|G_B$, let $g \in G_B$ be an element of order 5, then g fix two element of B, write $\{x_1, x_2\}$. Write $B = \{x_1, x_2, a_1, a_2, \cdots, a_5\}$. Since G is 3-transitive, there is $h \in G$ such that $h(x_1) = 0, h(x_2) = \infty, h(a_1) = 1$. Let $B' = h(B) = \{0, \infty, 1, h(a_2), \cdots, h(a_5)\}$, then $\mathrm{fix}(hgh^{-1}) = \{0, \infty\}$ and $\{1, h(a_2), \cdots, h(a_5)\}$ is it's 5-cycle. Therefore there is $a \in GF^*(2^n)$ such that $hgh^{-1} = ax$ and $|a| = 5$. So $B' = \{0, \infty 1, a, \cdots, a^4)\}$. Clealy, $\{1, a, \cdots, a^4)\}$ is subgroup of order 5, and it is uniqueness in $GF^*(2^n)$. So $G(B) = G(B')$ is uniqueness. Clealy element of order 2 $f(x) = \frac{1}{x} \in G_{B'}$. Similiar hold for $7 \mid |G_B|$.

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

$$\lambda \begin{pmatrix} v-i \\ t-i \end{pmatrix} \equiv 0 \left(mod \begin{pmatrix} k-i \\ t-i \end{pmatrix} \right), \qquad (1)$$

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

Remark 1. If both $G(B)$ and $G(B')$ are all the 3-$(2^n + 1, 7, \lambda)$ designs, then either $G(B) \cap G(B') = \emptyset$ or $G(B) = G(B')$. Therefore, for fixed λ, what the number of B statisfying $G(B)$ is a 3-$(2^n + 1, 7, \lambda)$ design is equal to $\lambda\left(\begin{array}{c}2^n+1\\3\end{array}\right)N_\lambda/\left(\begin{array}{c}7\\3\end{array}\right)$.

Lemma 3.3 *Every orbit of 7-subset is a 3-$(2^n+1,7,\lambda)$ design with $\lambda\in\{5,15,21,70,105,210\}$.*

Proof. Since $G(B)$ is a 3-$(2^n+1,7,\lambda)$ design,

$$|G(B)|=\lambda\left(\begin{array}{c}2^n+1\\3\end{array}\right)/\left(\begin{array}{c}7\\3\end{array}\right)$$

by Lemma 2.6. Therefore, by $|G|=|G(B)||G_B|$, we see $\lambda|G_B|=210$. By Lemma 3.1 and 3.2 we can get the results.

4 Orbits of 7-subsets

From now on, we let N_λ denote the number of the orbits each of which forms a 3-$(2^n+1,7,\lambda)$ design. Let B be a 7-subset of X, and $G(B)$ be the set of blocks of a 3-$(2^n+1,7,\lambda)$ design. Then the group G is block-transitive on this design.

In the following, we will determine the N_λ for $\lambda\in\{5,15,21,105,210\}$.

Lemma 4.1 *Let B be a 7-subset of X. If the orbit $G(B)$ is a $3-(2^n+1,7,\lambda)$ design, then $N_5=0$,*

$$N_{15}=\begin{cases}1 & \textit{when } n\equiv 0 \pmod 3\\ 0 & \textit{otherwise}\end{cases},$$

$$N_{21}=\begin{cases}1 & \textit{when } n\equiv 0 \pmod 4\\ 0 & \textit{otherwise}\end{cases}.$$

Proof. Let $G(B)$ form a 3-$(2^n+1,7,21)$ design. Since $\lambda|G_B|=210$, and $G_B=10$. Thus $5|2^n-1$, that is $n\equiv 0 \pmod 4$ by lemma 2.5, and every element of order 5 of G_B fixes exactly two points of B, and $N_{15}=1$ by Lemma 3.2. Otherwise when $5\nmid 2^n-1$, or $n\equiv 1,2,3 \pmod 4$, $N_{21}=0$. Similiarly, when $n\equiv 0 \pmod 3$, $N_{21}=1$. When $n\equiv 1,2, \pmod 3$, $N_{21}=0$. By Lamme 3.2, $N_{15}+N_5\leq 1$. By calculating the numbers of 7-subset including points $\{0,1,\infty\}$, we have

$$210N_{210}+105N_{105}+70N_{70}+21N_{21}+15N_{15}+5N_5=\left(\begin{array}{c}2^n-2\\4\end{array}\right).$$

So,

$$21N_{21}+15N_{15}+5N_5\equiv\left(\begin{array}{c}2^n-2\\4\end{array}\right) \pmod{35}. \qquad (2)$$

If $N_5 \neq 0$, then $3|n$ and $N_{15} = 0$. If $4|n$, then $n = 12k$ and $N_{21} = 1$, then

$$21N_{21} + 15N_{15} + 5N_5 \equiv 26 \pmod{35}.$$

But this time,

$$\begin{pmatrix} 2^n - 2 \\ 4 \end{pmatrix} = \frac{(2^n-2)(2^n-3)(2^n-4)(2^n-5)}{24} \equiv \frac{(36-2)(36-3)(36-4)(36-5)}{24} \equiv 1 \pmod{35}.$$

Since $2^{12k} \equiv 1 \pmod{35}$. This is cotradiction with equation (2). If $4 \nmid n$, then $n \equiv 3, 6, 9 \pmod{35}$ and $21N_{21} + 15N_{15} + 5N_5 \equiv 5 \pmod{35}$. But this time

$$\begin{pmatrix} 2^n - 2 \\ 4 \end{pmatrix} = \frac{(2^n-2)(2^n-3)(2^n-4)(2^n-5)}{24} \equiv 12, 15, 3 \pmod{35}.$$

Since $2^{12k} \equiv 1 \pmod{35}$. This is cotradiction with equation (2). Therefore $N_5 = 0$, the results hold.

Lemma 4.2 *When* $n \equiv 0 \pmod 2$, $N_{70} = \frac{2^n-4}{6}$; *Otherwise,* $N_{70} = 0$.

Proof. Let $G(B)$ form a 3-$(2^n+1, 7, 70)$ design. Then $|G_B| = 3$. Thus the elements of order 3 fix at least one point of B. By lemma 2.2-2.4, we have $3|2^n - 1$, and then $n \equiv 0 \pmod 2$. Therefore, by **Remark 1** we see that the number of such $B's$ is $70\begin{pmatrix} 2^n+1 \\ 3 \end{pmatrix} N_{70} / \begin{pmatrix} 7 \\ 3 \end{pmatrix}$. On the other hand, since $3|2^n - 1$, by Lemma 2.3 each element of order 3 of G fixes exactly $2\begin{pmatrix} \frac{2^n-1}{3} \\ 2 \end{pmatrix} = \frac{(2^n-1)(2^n-4)}{9}$ 7-subsets of X each of which is fixed exactly by 2 elements of order 3 and there are exactly $2^n(2^n+1)$ elements of order 3 in G. Therefore, the elements of order 3 of G fix exactly $2^n(2^n+1)(2^n-1)(2^n-4)/18$ distinct 7-subsets of X. So we have $70\begin{pmatrix} 2^n+1 \\ 3 \end{pmatrix} N_{70} / \begin{pmatrix} 7 \\ 3 \end{pmatrix} = 2^n(2^n+1)(2^n-1)(2^n-4)/18$, and hence $N_{70} = \frac{2^n-4}{6}$.

Lemma 4.3 *The number of orbits* $\mathcal{O}_7$ *of 7-subsets is*

$$\mathcal{O}_7 = \begin{cases} \mathcal{T} + \frac{70\cdot 2^n + 242}{630}, & n \equiv 0 \pmod{12}; \\ \mathcal{T} + \frac{70\cdot 2^n - 280}{630}, & n \equiv 2, 10 \pmod{12}; \\ \mathcal{T} + \frac{270}{630}, & n \equiv 3, 9 \pmod{12}; \\ \mathcal{T} + \frac{70\cdot 2^n - 10}{630}, & n \equiv 6 \pmod{12}; \\ \mathcal{T} + \frac{40\cdot 2^n - 16}{630}, & n \equiv 4, 8 \pmod{12}; \\ \mathcal{T}, & n \equiv 1, 5, 7, 11 \pmod{12}. \end{cases}$$

where $\mathcal{T} = (\frac{2^{n-1}-1)(2^{n-2}-1)((2^n-3)(2^n-5)+105}{630}$.

proof. Let $\chi_7(g)$ denote the number of 7-subsets of X fixed by element g. Then by lemma 2.5, $\chi_7(g) \neq 0$, only when $g \in \{1,2,3,5,7\}$. Therefore, by Cauchy-Frobenius-Burnside lemma, we have

$$\mathcal{O}_7 = \frac{1}{|G|}\sum_{g\in G}\chi_7(g) = \frac{1}{|G|}\sum_{g\in G, |g|=1,2,3,5,7}\chi_7(g)$$

Clearly,

$$\sum_{|g|=1}\chi_7(g) = \binom{2^n+1}{7} =$$

$$\frac{2^n(2^{n+1}-1)(2^{n-1}-1)(2^{n-2}-1)(2^n-3)(2^n-5)}{630}$$

and

$$\sum_{|g|=2}\chi_7(g) = \binom{2^{n-1}}{3}\frac{|G|}{2^n} \doteq \frac{2^n(2^{n-1}-1)(2^{n-2}-1)(2^{n+1}-1)}{6}.$$

Also by lemma 2.5, we can get

$$\sum_{|g|=3}\chi_7(g) = \begin{cases} 2\binom{\frac{2^n-1}{3}}{2}\frac{|G|}{2^n-1} = \frac{(2^n-4)|G|}{9}, \\ \text{when } n \equiv 0,2,4,6,8,10 \pmod{12} \\ 0, \quad \text{otherwise} \end{cases}.$$

and

$$\sum_{|g|=5}\chi_7(g) = \begin{cases} \frac{2^n-1}{5}\cdot\frac{2|G|}{2^n-1} = \frac{2|G|}{5} & \text{when } n \equiv 2,6,10 \pmod{12} \\ 0 & \text{otherwise} \end{cases}.$$

and

$$\sum_{|g|=7}\chi_7(g) = \begin{cases} \frac{3|G|}{7} & \text{when } n \equiv 0,3,6,9 \pmod{12} \\ 0 & \text{otherwise} \end{cases}.$$

So the results hold.

Lemma 4.4

$$N_{105} = \begin{cases} \frac{(2^{n-1}-1)(2^{n-2}-1)}{3} - 70, & n \equiv 0 \pmod{12} \\ \frac{(2^{n-1}-1)(2^{n-2}-1)}{3}, & n \equiv 1,2,5,7,10,11 \pmod{12} \\ \frac{(2^{n-1}-1)(2^{n-2}-1)}{3} - 1, & n \equiv 3,4,6,8,9 \pmod{12} \end{cases}.$$

$$N_{210} = \begin{cases} \mathcal{M} - \frac{35\cdot 2^n - 592}{630}, & n \equiv 0 \pmod{12}; \\ \mathcal{M} - \frac{70\cdot 2^n + 210}{630}, & n \equiv 2, 10 \pmod{12}; \\ \mathcal{M} + \frac{180}{630}, & n \equiv 3, 9 \pmod{12}; \\ \mathcal{M} - \frac{70\cdot 2^n + 439}{630}, & n \equiv 6 \pmod{12}; \\ \mathcal{M} - \frac{70\cdot 2^n + 246}{630}, & n \equiv 4, 8 \pmod{12}; \\ \mathcal{M} & n \equiv 1, 5, 7, 11 \pmod{12}. \end{cases} .$$

where $\mathcal{M} = \frac{(2^{n-1}-1)(2^{n-2}-1)((2^n-3)(2^n-5)-105}{630}$.

Proof. By Lemma 3.3 and Lemma 4.1, any orbit of 7-subsets of X is a $3-(2^n+1, 7, \lambda)$ design, where $\lambda \in \{15, 21, 70, 105, 210\}$. So we have

$$15N_{15} + 21N_{21} + 70N_{70} + 105N_{105} + 210N_{210} = \binom{2^n - 2}{4}. \quad (3)$$

On the other hand, we also have

$$N_{15} + N_{21} + N_{70} + N_{105} + N_{210} = O_7 \quad (4)$$

So by Lemma 4.1-4.3 and equation (3) and (4), we can get the results easily.

5 The proof of the main theorem

Let $\mathcal{D}$ be a simple 3-$(2^n+1, 7, \lambda)$ design admitting G as an automorphism group. It is well known that a simple 3-$(2^n+1, 7, \lambda)$ 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 Lemma4.1-4.4, we find 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, 70, 105, 210. So $\lambda = 15x_1 + 21x_2 + 70x_3 + 105x_4 + 210x_5$, $0 \le x_1, x_2 \le 1, 0 \le x_3 \le N_{70}, 0 \le x_4 \le N_{105}, 0 \le x_5 \le N_{210}$. This proves the necessity.

Conversely, by Lemmas 4.1-4.4, there exist non-negative integers $0 \le x_1, x_2 \le 1, 0 \le x_3 \le N_{70}, 0 \le x_4 \le N_{105}, 0 \le x_5 \le N_{210}$. such that

$$\lambda = 15x_1 + 21x_2 + 70x_3 + 105x_4 + 210x_5.$$

We take x_1 orbits of length $|G|/14$,x_2 orbits of length $|G|/10$, x_3 orbits of length $|G|/3$, x_4 orbits of length $|G|/2$ and x_5 orbits of length $|G|$, then this gives a simple 3-$(2^n+1, 7, \lambda)$ design admitting G as an automorphism group. This proves the sufficiency.

References

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

[2] C.A. Cusack, S.S. Magliveras, Semiregular large Sets, Design Codes Cryptogr. 18 (1-3) (1999), 81-87.

[3] 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.

[4] 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.

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

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

[7] 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.

[8] L.Z. Gong and W.J. Liu, 3-Designs of $PSL(2,q)$ with block size 7, Ars Comb. 95(2010),289-296.

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