AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **51** (2011), Pages 235–241

Simple 3-designs with block size $d+1$ from PSL(2, 2^n) where $d|(2^n-1)$*

Weixia Li

School of Mathematical Sciences
Qingdao University
Qingdao, Shandong, 266071
China
wxli_math@hotmail.com

Hao Shen

Department of Mathematics
Shanghai Jiao Tong University
Shanghai 200240
China
haoshen@sjtu.edu.cn

Abstract

Let $\mathcal{G}$ be the projective special linear group $\mathrm{PSL}(2,2^n)$, let X be the projective line and B be any subgroup of $GF^*(2^n)$. We give a new infinite family of simple 3-designs by determining the parameter set of $(X,\ \mathcal{G}(B_0))$, where $B_0 = B \cup \{0\}$.

1 Introduction

A 3-(v,k,λ) design is a pair $(X,\mathcal{B})$ in which X is a $v-$set of *points* and $\mathcal{B}$ is a collection of $k-$subsets of X called *blocks*, such that every 3-subset of X is contained in precisely λ blocks. A 3-(v,k,λ) design is *simple* if it contains no repeated blocks. All of the 3-designs in this paper will be simple. Let G denote a subgroup of $\mathrm{Sym}(X)$, the *full symmetric group* on X. Now G acts on the subsets of X in a natural way: If $g \in G$ and $S \subseteq X$, then $g(S) = \{g(x) : x \in S\}$. The group G is called an *automorphism group* of the 3-design $(X,\mathcal{B})$ if $g(S) \in \mathcal{B}$ for all $g \in G$ and $S \in \mathcal{B}$. For $S \subseteq X$, let

$$G(S) = \{g(S) : g \in G\};$$

* Research supported by National Natural Science Foundation of China (No. 11071163) and Doctor Fund of Shandong Province (No. BS2009SF017).

$$G_S = \{g \in G : g(S) = S\}.$$

Here $G(S)$ is called the orbit of S, and G_S is called the stabilizer of S. It is well-known that $|G| = |G_S||G(S)|$ (see [2]). It follows that G is an automorphism group of the 3-design $(X, \mathcal{B})$ if and only if $\mathcal{B}$ is a union of orbits of k-subsets of X under G (see [1]).

Let q be a prime power and let $X = GF(q) \bigcup \{\infty\}$. We define

$$a/0 = \infty, \quad a/\infty = 0, \quad \infty + a = a + \infty = \infty, \quad a\infty = \infty a = \infty$$

and

$$\frac{a\infty + b}{c\infty + d} = \frac{a}{c},$$

where $a,\ b,\ c,\ d \in GF(q)$ and $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$. Here X is called the *projective line*. For any $a, b, c, d \in GF(q)$, if $ad - bc \neq 0$, we define a function $f : X \longrightarrow X$ where

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

The function f is called a *linear fraction*. The determinant of f is

$$det\ f = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

The set of all linear fractions whose determinants are non-zero squares forms a group, called the *linear fractional group* $\mathrm{LF}(2, q)$, which is isomorphic to the *projective special linear group* $\mathrm{PSL}(2, q)$ (see [2]).

The group $\mathrm{PSL}(2, q)$ plays a very important role in the construction of simple 3-designs. When $q \equiv 3 \pmod 4$ or $q = 2^n$, $\mathrm{PSL}(2, q)$ acts 3-homogeneously, i.e., it acts transitively on 3-subsets of the projective line. So unions of orbits for the action of $\mathrm{PSL}(2, q)$ on the set of k-subsets of the projective line yield simple 3-designs. For the case of $q \equiv 3 \pmod 4$, simple 3-designs with $\mathrm{PSL}(2, q)$ as an automorphism group have been investigated in [3, 4, 10]. In [3], all simple 3-designs admitting $\mathrm{PSL}(2, q)$ with block size not congruent to 0 or 1 modulo p, where $q = p^n$, are determined. For the case $q = 2^n$, no similar result has been found.

In this paper, we will only consider the case $q = 2^n$. Since every element of $GF(2^n)$ is a square, $\mathrm{LF}(2, 2^n)$ is isomorphic to the *projective general linear group* $\mathrm{PGL}(2, 2^n)$. Let $\mathcal{G}$ denote $\mathrm{LF}(2, 2^n)$. Since $\mathcal{G}$ is sharply 3-transitive on X (see [2]), for any orbit Γ of k-subsets of X, (X, Γ) is a simple 3-$(2^n + 1, k, \lambda)$ design for some λ, where $k > 3$. It is well-known (see [2]) that

$$|\mathcal{G}| = (2^n + 1)2^n(2^n - 1).$$

The subgroup structure of $\mathcal{G}$ is known in [5, 6]. The existence of simple 3-designs admitting $\mathrm{PSL}(2, 2^n)$ with block size 4, 5, 6 and 7 is investigated in [7, 8, 9] and a complete solution is given. In this paper, we give a new infinite family of simple 3-designs by determining the parameter set of $\mathcal{G}(B \cup \{0\})$, where B is a subgroup of $GF^*(2^n)$.

2 Preliminaries concerning PSL$(2,\ 2^n)$

In this section, we will make some preparations for the proof of the main theorem. Lemmas 2.1 and 2.2 show some of the fundamental properties of the elements contained in $\mathcal{G}$. Let $\chi(g)$ denote the number of elements of X fixed by $g \in \mathcal{G}$ in both lemmas.

Lemma 2.1 [5] *Suppose $g \in \mathcal{G}$ and $|g| = m > 1$. Then $\chi(g) = 1$ if $m = 2$, $\chi(g) = 2$ if $m|(2^n - 1)$, $\chi(g) = 0$ if $m|(2^n + 1)$.*

Lemma 2.2 [7] *If $g \in \mathcal{G}$ is of order $m > 1$, then g has $a = \chi(g) \leq 2$ fixed points and $b = (2^n + 1 - a)/m$ m-cycles.*

Corollary 2.3 *A k-subset S can be fixed by an element $g \in \mathcal{G}$ with order m if and only if S consists of q m-cycles and r fixed points of g, where $k = mq + r$, $0 \leq r < m$.*

Lemma 2.4 [5, 6] *The subgroups of $\mathcal{G}$ are as follows:*

(i) Elementary abelian groups of order 2^m where $m \leq n$;

(ii) Cyclic subgroups of order d where $d|(2^n \mp 1)$;

(iii) Dihedral subgroups D_{2d} for $d|(2^n \pm 1)$;

(iv) Subgroups of order $2^m d$ each of which is the semidirect product of an elementary abelian group ε of order 2^m and a cyclic group of order d, where $d|(2^n - 1)$. The non-identity elements of ε are involutions and have the same fixed point in X.

(v) Subgroups isomorphic with PSL$(2, 2^k)$, where k is a divisor of n.

(vi) Tetrahedrals A_4.

Lemmas 2.5 and 2.6 are fundamental theorems on the structure of PSL$(2, 2^n)$.

Lemma 2.5 [5] *The linear fractions*

$$S_\mu(x) = x + \mu, \quad \mu \in GF(2^n),$$

form an elementary abelian subgroup $G_s^{(\infty)}$ of order $s = 2^n$. Here $G_s^{(\infty)}$ consists of all the involutions of $\mathcal{G}$ leaving the single element ∞ fixed.

Throughout the remainder of this article, we will assume that d is a positive integer dividing $2^n - 1$ and that α is a primitive element of $GF^*(2^n)$. Let $f(x) = 1/x$, $h(x) = \alpha^{\frac{2^n-1}{d}} x$, and set $H = \langle h(x) \rangle$ and $G = \langle H, f(x) \rangle$.

Lemma 2.6 [5] *All the dihedral subgroups D_{2d} are conjugate.*

Lemma 2.7 *G is a dihedral subgroup D_{2d}.*

Proof. It is easy to prove that h and f satisfy the generational relations

$$h^d = I,\ f^2 = I \ \text{ and } hf = fh^{-1}.$$

So G is a dihedral group D_{2d}. □

Using these preparations, we will prove the main results in the next section.

3 Simple 3-designs with block size $d+1$

Since an orbit $\Gamma = \mathcal{G}(S)$ of a k-subset S is a simple 3-$(2^n+1, k, \lambda)$ design with total number of blocks $b = |\mathcal{G}(S)| = \frac{|\mathcal{G}|}{|\mathcal{G}_S|}$, the following lemma is obvious.

Lemma 3.1 *If S is a k-subset of X, then the orbit $\Gamma = \mathcal{G}(S)$ is a 3-$(2^n+1, k, \lambda)$ design with*

$$\lambda = \frac{k(k-1)(k-2)}{|\mathcal{G}_S|}.$$

Lemma 3.2 *Suppose S is a $d{+}1$-subset. There is no dihedral subgroup D_{2d} contained in $\mathcal{G}_S$.*

Proof. Suppose there is a dihedral subgroup $D_{2d} \subseteq \mathcal{G}_S$. By Lemmas 2.6 and 2.7, there exists $g \in \mathcal{G}$ such that

$$gD_{2d}g^{-1} \ = \ G \subseteq g\mathcal{G}_S g^{-1} \ = \ \mathcal{G}_{S'},$$

where $S' = g(S)$. Since $h(x) \in G \subseteq \mathcal{G}_{S'}$, it follows that S' is composed of one d-cycle and exactly one fixed point of $h(x)$ by Corollary 2.3. Thus S' is either

$$\{0,\ a,\ a\alpha^{\frac{2^n-1}{d}},\ a\alpha^{\frac{2(2^n-1)}{d}},\ \ldots,\ a\alpha^{\frac{(d-1)(2^n-1)}{d}}\}$$

or

$$\{\infty,\ b,\ b\alpha^{\frac{2^n-1}{d}},\ b\alpha^{\frac{2(2^n-1)}{d}},\ \ldots,\ b\alpha^{\frac{(d-1)(2^n-1)}{d}}\},$$

where $a,\ b \in GF^*(2^n)$. However, $f(x) = 1/x$ interchanges 0 and ∞ and thus cannot fix S'. This is a contradiction because $f(x) \in G \subseteq \mathcal{G}_{S'}$. Now the proof is complete. □

Let $B = \langle \alpha^{(2^n-1)/d} \rangle$, the unique subgroup of $GF^*(2^n)$ with order d, and set $B_0 = B \cup \{0\}$ and $B_\infty = B \cup \{\infty\}$. Observe that if $d = 2^m - 1$ and $m|n$, then B_0 is a subfield of $GF(2^n)$ and thus

$$A = \{x \to ax + b : a, b \in B_0, a \neq 0\}$$

is a subgroup of $\mathcal{G}$ of order $(d+1)d = 2^m(2^m-1)$, which we call the 1-dimensional affine group over B_0.

Lemma 3.3 *If $d = 2^m - 1 \geq 3$ with $m|n$, then $\mathcal{G}_{B_0} = A$.*

Proof. Since B_0 forms a subfield of $GF(2^n)$, A is a subgroup of $\mathcal{G}_{B_0}$ and $|A| = 2^m(2^m-1)||\mathcal{G}_{B_0}|$. Now $\mathcal{G}_{B_0}$ cannot be in (i), (ii) or (iii) of Lemma 2.4. If $\mathcal{G}_{B_0}$ is in (v), there exists an element of order no less than 2^m+1 contained in $\mathcal{G}_{B_0}$. However, this is a contradiction by Corollary 2.3 and the fact that $|B_0| = 2^m < 2^m+1$. Thus it must be in (iv) or (vi). If $m > 2$, then $|\mathcal{G}_{B_0}| \geq |A| > 3 \times 4 = 12 = |A_4|$ and thus (vi) is not possible. If $m = 2$, then A_4 is isomorphic to A which is a subgroup in (iv). So in both cases $\mathcal{G}_{B_0}$ is in (iv). Then $\mathcal{G}_{B_0}$ is the semidirect product of an elementary abelian group A' and a cyclic subgroup H', where $|A'| = 2^{m'}$, $|H'| = d'$ and $|\mathcal{G}_{B_0}| = 2^{m'}d'$. So $d' = d$, for both of them are the largest order of the elements contained in $\mathcal{G}_{B_0}$. By Lemma 2.4, all the involutions of $\mathcal{G}_{B_0}$ have the same fixed point. Since involutions $S_{\mu_i} = x + \alpha^{\frac{i(2^n-1)}{2^m-1}} \in \mathcal{G}_{B_0}$ ($\mu_i = \alpha^{\frac{i(2^n-1)}{2^m-1}}$, $1 \leq i \leq 2^m-2$) and ∞ is the fixed point of S_{μ_i}, it follows that ∞ is the common fixed point of all the involutions contained in $\mathcal{G}_{B_0}$. So $A' \subseteq G_s^{(\infty)}$ by Lemma 2.5. Thus if $g(x) \in A'$, then $g(x) = x + a$ and $a \in B_0$, for $A' \subseteq \mathcal{G}_{B_0}$ and $0 \in B_0$. So $|A'| \leq |B_0| = 2^m$ and $m' \leq m$. On the other hand $|\mathcal{G}_{B_0}| = 2^{m'}d \geq |A| = 2^m d$, so then $m' \geq m$. So $m' = m$ and $|\mathcal{G}_{B_0}| = 2^m(2^m-1) = |A|$. So $\mathcal{G}_{B_0} = A$. □

Lemma 3.4 *If $d = 2^m - 1 \geq 3$ with $m|n$, then $\Gamma = \mathcal{G}(B_0)$ is a simple 3-$(2^n+1, 2^m, 2^m-2)$ design.*

Proof. The conclusion follows from Lemmas 3.1 and 3.3. □

Lemma 3.5 *If $\mathcal{G}_{B_0}$ is in (iv) with order $2^m d$, where $d \geq 3$, then B_0 forms a subfield of $GF(2^n)$. So $m|n$, $d = 2^m-1$ and*

$$|\mathcal{G}_{B_0}| = |A| = 2^m(2^m-1).$$

Proof. Since B is a subgroup of $GF^*(2^n)$, we need only show that B_0 forms an additive group with the addition operation.

Obviously, $H \subseteq \mathcal{G}_{B_0}$, so $\mathcal{G}_{B_0}$ is a semidirect product of an elementary abelian group N and H. Then the fixed point of involutions contained in $\mathcal{G}_{B_0}$ must be one of $\{0, \infty\}$ which is the set of fixed points by $h(x)$. Since $|B_0| = d+1$ is even, B_0 contains no fixed point of an involution in $\mathcal{G}_{B_0}$ by Corollary 2.3, and so ∞ is the fixed point of the involutions contained in $\mathcal{G}_{B_0}$. Then $N \subseteq G_s^{(\infty)}$, and hence there exists an element $a \in GF^*(2^n)$ such that $g(x) = x + a \in N$. Since $0 \in B_0$ and $g(x) \in \mathcal{G}_{B_0}$, it follows that $a \in B_0$, and then $a = \alpha^{\frac{k(2^n-1)}{d}}$ for some integer k such that $0 \leq k \leq d-1$. So

$$\alpha^{\frac{k(2^n-1)}{d}} + \alpha^{\frac{i(2^n-1)}{d}} \in B_0. \quad (0 \leq i \leq d-1)$$

Then we have

$$\alpha^{\frac{i(2^n-1)}{d}} + \alpha^{\frac{j(2^n-1)}{d}} = \alpha^{\frac{(i-k)(2^n-1)}{d}}(\alpha^{\frac{k(2^n-1)}{d}} + \alpha^{\frac{[j-(i-k)](2^n-1)}{d}}) \in B_0 \quad (0 \leq i,\ j \leq d-1),$$

because $\alpha^{\frac{(i-k)(2^n-1)}{d}} \in B,\ \alpha^{\frac{k(2^n-1)}{d}} + \alpha^{\frac{[j-(i-k)](2^n-1)}{d}} \in B_0$ and B is a multiplicative subgroup of $GF^*(2^n)$. So B_0 forms a subfield of $GF(2^n)$. Thus $\mathcal{G}_{B_0} = A$ by Lemma 3.3. Hence $m|n$, $d = 2^m - 1$ and

$$|\mathcal{G}_{B_0}| = |A| = 2^m(2^m - 1).$$

□

Lemma 3.6 $\Gamma = \mathcal{G}(B_0)$ *is a simple* 3-$(2^n + 1, d + 1, d^2 - 1)$ *design if* $d \geq 3$ *and* $d \neq 2^m - 1$ *for any* $m|n$.

Proof. Obviously, $H \subseteq \mathcal{G}_{B_0}$. If there are no involutions contained in $\mathcal{G}_{B_0}$, then $|\mathcal{G}_{B_0}| = d$ by Lemma 2.4. So $\lambda = d^2 - 1$ and Γ is a simple 3-$(2^n + 1,\ d + 1,\ d^2 - 1)$ design by Lemma 3.1. Therefore we need only show that there are no involutions contained in $\mathcal{G}_{B_0}$.

Suppose there exists an involution contained in $\mathcal{G}_{B_0}$. When $d = 3$, since A_4 is isomorphic to a subgroup in Lemma 2.4(iv) with order $4d$, it follows that $\mathcal{G}_{B_0}$ cannot be A_4 by Lemma 3.5. If $d \geq 5$, then $\mathcal{G}_{B_0}$ cannot be A_4 either, for A_4 contains no element of order d.

So $\mathcal{G}_{B_0}$ is in (iv) or (v) by Lemmas 2.4 and 3.2. If $\mathcal{G}_{B_0}$ is in (iv), then $|\mathcal{G}_{B_0}| = 2^m d$ for some m, so $m|n$ and $d = 2^m - 1$ by Lemma 3.5. This is impossible, since $d \neq 2^m - 1$ for any $m|n$. So $\mathcal{G}_{B_0}$ must be in (v). Since d is the largest order of the elements contained in $\mathcal{G}_{B_0}$,

$$|\mathcal{G}_{B_0}| = (d - 2)(d - 1)d,$$

and this implies that there exists a dihedral subgroup D_{2d} contained in $\mathcal{G}_{B_0}$, which is impossible by Lemma 3.2. Hence there exist no involutions contained in $\mathcal{G}_{B_0}$. Now the proof is complete. □

By Lemmas 3.4 and 3.6, we have the main theorem.

Theorem 3.1 *Suppose* $d|(2^n - 1)$ *and* $d \geq 3$. *For any subgroup* B *of* $GF^*(2^n)$ *with order* d, *letting* $B_0 = B \cup \{0\}$, *we have* $\mathcal{G}(B_0)$ *is one of the following:*

1. *a simple* 3-$(2^n + 1, 2^m, 2^m - 2)$ *design if* $d = 2^m - 1$ *for some* $m|n$;
2. *a simple* 3-$(2^n + 1, d + 1, d^2 - 1)$ *design if* $d \neq 2^m - 1$ *for any* $m|n$.

References

[1] T. Beth, D. Jungnickel and H. Lenz, *Design theory*, Cambridge University Press, Cambridge, England, 1993.

[2] N. L. Biggs and A. T. White, *Permutation groups and combinatoral structures*, Cambridge University Press 1979.

[3] P.J. Cameron, H.R. Maimani, G.R. Omidi and B. Tayfeh-Rezaie, 3-designs from $\mathrm{PSL}(2,q)$, *Discrete Math.* 306 (2006), 3063–3073.

[4] 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. Combin. Des.* 3 (1995), 147–160.

[5] L.E. Dickson, *Linear groups, with an introduction to the Galois field theory*, Dover Publications, New York, 1958.

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

[7] M.S. Keranen and D.L. Kreher, 3-designs from $\mathrm{PSL}(2,2^n)$, with block sizes 4 and 5, *J. Combin. Des.* 12 (2004), 103–111.

[8] W. Li and H. Shen, Simple 3-designs of $\mathrm{PSL}(2,2^n)$ with block size 6, *Discrete Math.* 308 (2008), 3061–3072

[9] W. Li and H. Shen, Simple 3-designs of $\mathrm{PSL}(2,2^n)$ with block size 7, *J. Combin. Des.* 1 (2008), 1–17

[10] Gh.R. Omidi, M.R. Pournaki and B. Tayfeh-Rezaie, 3-Designs from $\mathrm{PSL}(2,q)$ with block size 6 and their large sets, *Discrete Math.* 307 (2007), 1580–1588.

(Received 3 Mar 2011; revised 29 June 2011)