On the Existence of Simple 3-(30, 7, 15) and 3-(26, 12, 55) Designs *

Weixia Li †‡

† *Department of Mathematics, Shanghai Jiao Tong University*
Shanghai 200240, China

‡ *School of Mathematical Sciences, Qingdao University*
Qingdao 266071, China

E-mail: lwxlnk@sjtu.edu.cn

Abstract

For each of the parameter sets (30, 7, 15) and (26, 12, 55), a simple 3-design is given. They have PSL(2, 29) and PSL(2, 25) as their automorphism group, respectively. Each of the two simple 3-designs is the first one ever known with the parameter set given and λ in each of the the two parameter sets is minimal for the given v and k.

Keywords: 3-design; linear fraction; projective special linear group

1 Introduction

A 3-(v, k, λ) *design* is a pair $(X, \mathcal{B})$ where X is a v-element set of *points* and $\mathcal{B}$ is a collection of k-element subsets of X (*blocks*) with the property that every 3-element subset of X is contained in exactly λ blocks. A 3-(v, k, λ) design is *simple* if no two blocks are identical.

Let G denote a subgroup of Sym(X), the *full symmetric group* on X. G acts on the subsets of X in a natural way: If $g \in G$ and $S \subseteq$

*Research supported by National Natural Science Foundation of China under Grant 10471093

X, then $g(S) = \{g(x) : x \in S\}$. 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

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

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

$G(S)$ 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 $X = GF(q) \bigcup \{\infty\}$. We define

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

and

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

where a, b, c, $d \in GF(q)$ and $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$. 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

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

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]). Let $\mathcal{G}$ denote $\mathrm{PSL}(2, q)$ with $q = p^n \equiv 1 (\mathrm{mod}\ 4)$ in this paper. It is well known that

$$|\mathcal{G}| = (q + 1)q(q - 1)/2.$$

In the next section of this paper, two simple 3-designs with $\mathrm{PSL}(2, 29)$ and $\mathrm{PSL}(2, 25)$ as their automorphism group, respectively, will be given. Each of these 3-designs is the first one ever known with that parameter set according to [3] and [5].

2 Two simple 3-designs

In this section, we give two simple 3-designs mentioned above. The following two lemmas 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. [4] Suppose $g \in \mathcal{G}$ and $|g| = m > 1$. Then $\chi(g) = 1$ if $m = p$, $\chi(g) = 2$ if $m|\frac{q-1}{2}$, $\chi(g) = 0$ if $m|\frac{q+1}{2}$.

Lemma 2.2. [6] If $g \in \mathcal{G}$ of order $m > 1$, then g has $a = \chi(g) \leq 2$ fixed points and $b = (q+1-a)/m$ m-cycles.

Remark of Lemma 2.2: We can see from Lemma 2.2, that 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 2.3. [7] There are exactly two orbits of triples,

$$\Delta_1 = \mathcal{G}(\{0, 1, \infty\}) \text{ and } \Delta_2 = \mathcal{G}(\{0, \gamma, \infty\}),$$

each of which contains half of the triples, where γ is a primitive root in $GF(q)$.

We denote the number of k-subsets of an orbit Γ that contains a special triple of Δ_i by $\lambda_\Gamma^i (i = 1, 2)$.

Lemma 2.4 [7] Let γ be a primitive root in $GF(q)$. If Γ is any orbit of subsets of X, then $\gamma\Gamma$ is also an orbit.

Lemma 2.5 Let $\Gamma = \mathcal{G}(B)$ be an orbit of k-subsets. Then $\lambda_\Gamma^1 = \lambda_{\gamma\Gamma}^2, \lambda_{\gamma\Gamma}^1 = \lambda_\Gamma^2$ and $(X, \gamma\Gamma \cup \Gamma)$ is a 3-$(q+1, k, \lambda)$ design with

$$\lambda = \lambda_\Gamma^1 + \lambda_{\gamma\Gamma}^1 = \lambda_\Gamma^2 + \lambda_{\gamma\Gamma}^2 = \frac{k(k-1)(k-2)}{|\mathcal{G}_B|},$$

where γ is a primitive root of $GF(q)$.

Proof. Firstly, we prove that $\lambda_\Gamma^1 = \lambda_{\gamma\Gamma}^2$. If there exists a k-subset $A \in \Gamma$ such that $\{0, 1, \infty\} \subseteq A$, then

$$\{0, \gamma, \infty\} = \gamma\{0, 1, \infty\} \subseteq \gamma A \in \gamma\Gamma.$$

Conversely, suppose there exists $\gamma A \in \gamma\Gamma$ containing $\{0, \gamma, \infty\}$, where $A \in \Gamma$, then

$$\{0,1,\infty\} = \gamma^{-1}\{0,\gamma,\infty\} \subseteq \gamma^{-1}(\gamma A) = A \in \Gamma.$$

So $\lambda^1_\Gamma = \lambda^2_{\gamma\Gamma}$.

Secondly, we prove that $\lambda^1_{\gamma\Gamma} = \lambda^2_\Gamma$. If there exists $A \in \gamma\Gamma$ containing $\{0,1,\infty\}$, then

$$\{0,\gamma,\infty\} = \gamma\{0,1,\infty\} \subseteq \gamma A \in \gamma^2\Gamma = \Gamma,$$

since γ^2 is a square. Conversely, suppose there exists $A \in \Gamma$ containing $\{0,\gamma,\infty\}$, then

$$\{0,1,\infty\} = \gamma^{-1}\{0,\gamma,\infty\} \subseteq \gamma^{-1}A \in \gamma^{-1}\Gamma = \gamma^{q-2}\Gamma = \gamma^2 \cdot \gamma^{q-2}\Gamma = \gamma\Gamma.$$

So $\lambda^1_{\gamma\Gamma} = \lambda^2_\Gamma$.

By the above arguments, we have $\lambda^1_\Gamma + \lambda^1_{\gamma\Gamma} = \lambda^2_\Gamma + \lambda^2_{\gamma\Gamma}$. So $(X, \gamma\Gamma \cup \Gamma)$ is a 3-$(q+1,k,\lambda)$ design with

$$\lambda = \lambda^1_\Gamma + \lambda^1_{\gamma\Gamma} = \lambda^2_\Gamma + \lambda^2_{\gamma\Gamma}.$$

Since the total number of blocks is

$$b = 2|\Gamma| = 2|\mathcal{G}(B)| = 2\frac{|\mathcal{G}|}{|\mathcal{G}_B|},$$

so

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

Theorem 2.1. Let $B_1 = \{1,\ \gamma_1^4,\ \gamma_1^8, \cdots, \gamma_1^{24}\}$ be the subgroup of $GF^*(29)$ with order 7, where γ_1 is a primitive root of $GF(29)$. Let $X_1 = GF(29) \cup \{\infty\}$, $\mathcal{G}_1$ =PSL(2, 29) and $\Gamma_1 = \mathcal{G}_1(B_1)$. Then $(X_1, \gamma_1\Gamma_1 \cup \Gamma_1)$ is a simple 3-(30, 7, 15) design.

Proof. By Lemma 2.5, $(X_1, \gamma_1\Gamma_1 \cup \Gamma_1)$ is a 3-$(30,7,\lambda_1)$ design with

$$\lambda_1 = \frac{7 \times 6 \times 5}{|\mathcal{G}_{1B_1}|}. \tag{1}$$

Since $3|\frac{29+1}{2}$ and $5|\frac{29+1}{2}$, by Lemma 2.1, an element contained in $\mathcal{G}_1$ with order 3 or 5 has no fixed points. So an element of order 3 or 5 can not be contained in the stabilizer of a 7-subset by Remark of Lemma 2.2. So $3 \not| \ |\mathcal{G}_{1B_1}|$ and $5 \not| \ |\mathcal{G}_{1B_1}|$. Then $|\mathcal{G}_{1B_1}|\ |14$ by (1). Obviously,

$f_1(x) = \gamma_1^4 x \in \mathcal{G}_{1B_1}$, $h(x) = \frac{1}{x} \in \mathcal{G}_{1B_1}$ and $\langle h(x), f_1(x)\rangle \subseteq \mathcal{G}_{1B_1}$ is a dihedron of order 14. So $|\mathcal{G}_{1B_1}| = 14$, $\lambda = 15$ and $(X_1, \gamma_1\Gamma_1 \cup \Gamma_1)$ is a 3-$(30, 7, 15)$ design. To prove $(X_1, \gamma_1\Gamma_1 \cup \Gamma_1)$ is simple, we need only to show $\Gamma_1 \neq \gamma_1\Gamma_1$. If $\Gamma_1 = \gamma_1\Gamma_1$, then

$$\lambda_1 = \lambda^1_{\Gamma_1} + \lambda^1_{\gamma_1\Gamma_1} = 2\lambda^1_{\Gamma_1}$$

must be an even number, which is a contradiction to $\lambda_1 = 15$. So $(X_1, \gamma_1\Gamma_1 \cup \Gamma_1)$ is a simple 3-$(30, 7, 15)$ design.

Theorem 2.2. Let $B_2 = \{1,\ \gamma_2^2,\ \gamma_2^4, \cdots, \gamma_2^{22}\}$ be the subgroup of $GF^*(25)$ with order 12, where γ_2 is a primitive root of $GF(25)$. Let $X_2 = GF(25) \cup \{\infty\}$, $\mathcal{G}_2$ =PSL(2, 25) and $\Gamma_2 = \mathcal{G}_2(B_2)$. Then $(X_2, \Gamma_2 \cup \gamma_2\Gamma_2)$ is a simple 3-$(26, 12, 55)$ design.

Proof. By Lemma 2.5, $(X_2, \Gamma_2 \cup \gamma_2\Gamma_2)$ is a 3-$(26, 12, \lambda_2)$ design with

$$\lambda_2 = \frac{12 \times 11 \times 10}{|\mathcal{G}_{2B_2}|}. \qquad (2)$$

Since $11 \not| \, |\mathcal{G}_2|$, then $11 \not| \, |\mathcal{G}_{2B_2}| \mid |\mathcal{G}_2|$. By Lemma 2.1, an element of order 5 has exactly one fixed point, so $\mathcal{G}_{2B_2}$ contains no elements of order 5 by Remark of Lemma 2.2. So $5 \not| \, |\mathcal{G}_{2B_2}|$. Then $|\mathcal{G}_{2B_2}| \mid 24$. Obviously $f_2(x) = \gamma_2^2 x \in \mathcal{G}_{2B_2}$, $h(x) = \frac{1}{x} \in \mathcal{G}_{2B_2}$ and $\langle f_2(x), h(x)\rangle$ is a dihedron of order 24. So $|\mathcal{G}_{2B_2}| = 24$ and $(X_2, \Gamma_2 \cup \gamma_2\Gamma_2)$ is a 3-$(26, 12, 55)$ design. It is simple since 55 is odd.

Acknowledgement. The author would like to express her sincere thanks to the referees for valuable comments and suggestions.

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] Charles J.Colbourn, Jeffrey H.Dinitz, The CRC handbook of combinatorial designs, CRC press, Boca Raton, New York, London, Tokyo, 1996, 48-52

[4] L.E.Dickson, Linear groups, with an introduction to the Galois field theory, Dover Publications, New York, 1958, 260-265

[5] Home Page for Jeff Dinitz (http://www.cems.uvm.edu/ dinitz /newresults.html)

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

[7] M.S.Keranen, D.L.Kreher, and P.J.S.Shiue, The quadruple systems of the projective special linear group PSL(2,q), J. Combin. Des. 11(2003), 339-351.