3-Designs with Block Size 6 from $PSL(2,q)$ and Their Large Sets*

G. R. Omidi, **M. R. Pournaki**, **B. Tayfeh-Rezaie**

Abstract

We investigate the existence of 3-designs and uniform large sets of 3-designs with block size 6 admitting $PSL(2,q)$ as an automorphism group. We show the existence of simple 3-$(28,6,10m)$ designs for $1 \leq m \leq 230$. Most of these designs were previously unknown.

Keywords: 3-Design, Large set of 3-designs, Uniform large set, Projective special linear group.
2000 Mathematics Subject Classification: Primary 05B05, 05B30; Secondary 20D06.

1 Introduction

Let t, k, v, and λ be integers such that $0 \leq t \leq k \leq v$ and $\lambda > 0$. Let X be a v-set and $P_k(X)$ denote the set of all k-subsets of X. A t-(v,k,λ) *design* is a pair $\mathcal{D} = (X, D)$ in which D is a collection of elements of $P_k(X)$ (called *blocks*) such that every t-subset of X appears in exactly λ blocks. If D has no repeated blocks, then it is called *simple*. Here we are concerned only with simple designs. It is well-known that a set of necessary conditions for the existence of a t-(v,k,λ) design is

$$\lambda \binom{v-i}{t-i} \equiv 0 \pmod{\binom{k-i}{t-i}}, \qquad (1)$$

for $0 \leq i \leq t$. An *automorphism* of $\mathcal{D}$ is a permutation σ on X such that $\sigma(B) \in D$ for each $B \in D$. An *automorphism group* of $\mathcal{D}$ is a group whose elements are automorphisms of $\mathcal{D}$. A *large set* of t-(v,k,λ) designs, denoted by LS$[N](t,k,v)$, is a set of N disjoint t-(v,k,λ) designs (X, D_i) such that D_i partition $P_k(X)$ and $N = \binom{v-t}{k-t}/\lambda$. A large set is said to be G-*uniform* if each of its designs admits G as an automorphism group.

Let G be a finite group acting on X. For $x \in X$, the *orbit* of x is $G(x) = \{gx|\ g \in G\}$ and the *stabilizer* of x is $G_x = \{g \in G|\ gx = x\}$. It is well-known that $|G| = |G(x)||G_x|$.

*This research was in part supported by a grant from IPM.

If there is an $x \in X$ such that $G(x) = X$, then G is called *transitive*. The action of G on X induces a natural action on $P_k(X)$. If this latter action is transitive, then G is called *k-homogeneous*.

Let q be a prime power and let $X = GF(q) \cup \{\infty\}$. Then the set of all mappings

$$g:\ x \mapsto \frac{ax+b}{cx+d}$$

on X such that $a, b, c, d \in GF(q)$, $ad-bc$ is a nonzero square and $g(\infty) = a/c$, $g(-d/c) = \infty$ if $c \neq 0$, and $g(\infty) = \infty$ if $c = 0$, is a group under composition of mappings called *projective special linear group* and is denoted by $PSL(2,q)$. It is well-known that $PSL(2,q)$ is 3-homogeneous if and only if $q \equiv 3 \pmod 4$. Note that $|PSL(2,q)| = (q^3-q)/2$. The structure of the elements of $PSL(2,q)$ is well-known (see for example [5,6]) and is given in Table 1 for $q \equiv 3 \pmod 4$ where φ denotes Euler's function.

Throughout this paper, we let q be a prime power congruent to 3 (mod 4), $X = GF(q) \cup \{\infty\}$, and $G = PSL(2,q)$ acting on X. We also denote $G_{\{0,1,\infty\}}$ by H. It is easy to see that

$$H = \left\{x \mapsto x,\ x \mapsto \frac{x-1}{x},\ x \mapsto \frac{1}{1-x}\right\}.$$

Table 1

The structure of the elements of $PSL(2,q)$, $q = p^n$, $q \equiv 3 \pmod 4$

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

The group $PSL(2,q)$ has been used for constructing t-designs by different authors, see for example [1,3,4,7–10]. In [3], all 3-designs and uniform large sets of 3-designs with block sizes 4 and 5 admitting $PSL(2,q)$ as an automorphism group were completely determined. In this paper, we investigate the existence of 3-designs and uniform large sets of 3-designs with block size 6 from $PSL(2,q)$. Since $PSL(2,q)$ is 3-homogeneous, 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 $P_k(X)$. We determine the number of orbits for all possible orbit sizes from the action of $PSL(2,q)$ on $P_6(X)$ and then use the results to construct 3-$(q+1,6,\lambda)$ designs and large sets of these designs. Finally, as a result, we establish the existence of 3-$(28,6,10m)$ designs for $1 \leq m \leq 230$. These designs were mostly unknown prior to this research [9]. Note that the method used in this paper is similar to the one in [10].

2 Orbit Counting

In this section we consider the action of G on $P_6(X)$ and determine the possible sizes of orbits and the number of orbits for any fixed size. For a 6-subset B of X, let

$$\Lambda_B = \big\{\{x,y,z\}|\ \{0,1,\infty,x,y,z\} \in G(B)\big\}.$$

The cardinality of Λ_B (denoted by λ_B) is called the *index of* $G(B)$ which is clearly well-defined. Note that $\lambda_B > 0$. We denote the number of orbits of index i by N_i.

Lemma 2.1 *Let $B \in P_6(X)$. Then $\lambda_B|G_B| = 60$ and*
(i) *if $q \equiv 11 \pmod{20}$, then $\lambda_B = 10, 12, 20, 30, 60$,*
(ii) *if $q \not\equiv 11 \pmod{20}$, then $\lambda_B = 10, 20, 30, 60$.*

Proof. Since $G(B)$ is a 3-$(q+1,6,\lambda_B)$ design, we have $|G(B)| = \lambda_B\binom{q+1}{3}/\binom{6}{3}$. Therefore, by $|G| = |G_B||G(B)|$, we find $\lambda_B|G_B| = 60$. By (1), $4|\lambda_B(q-1)$ and so λ_B is even. Moreover, $5|\lambda_B q(q-1)$ and therefore if $q \not\equiv 11 \pmod{20}$, then $5|\lambda_B$. It follows that $\lambda_B = 2,4,6,10,12,20,30,60$, if $q \equiv 11 \pmod{20}$ and $\lambda_B = 10,20,30,60$, otherwise. We now show that $\lambda_B \neq 2,4,6$ or equivalently $|G_B| \neq 10,15,30$ when $q \equiv 11 \pmod{20}$.

First suppose that $|G_B| = 10$. Let K be a normal subgroup of G_B of order 5 and $g \in G_B$ be an element of order 2. Then there are $k_1, k_2 \in K$ such that $gk_1 = k_2 g$. Note that k_1 and k_2 fix exactly one element x of B. Since $g(x) = k_2(g(x))$, we have $g(x) = x$ which is a contradiction with the fact that g has no fixed point.

Now let $|G_B| = 15$. As 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 and therefore $|G_B| \neq 15$.

Finally, let $|G_B| = 30$. Let P_1 and P_2 be 3-Sylow and 5-Sylow subgroups of G_B, respectively. Since P_2 is always normal in G_B, P_1P_2 is a subgroup of order 15 of G_B which is impossible as described above. $\square$

Lemma 2.2 *Let H act on $P_3\big(GF(q)\setminus\{0,1\}\big)$. Then the number of orbits of sizes 1 and 3 are equal to L and $\big(\binom{q-2}{3} - L\big)/3$, respectively, where*

$$L = \begin{cases} \frac{q-3}{3} & \text{if } q \equiv 3 \pmod{12}, \\ \frac{q-4}{3} & \text{if } q \equiv 7 \pmod{12}, \\ \frac{q-2}{3} & \text{if } q \equiv 11 \pmod{12}. \end{cases} \tag{2}$$

Furthermore, the set of orbits of size 1 is

$$\left\{ \left\{ \alpha, \frac{\alpha-1}{\alpha}, \frac{1}{1-\alpha} \right\} \middle|\ \alpha \in GF(q)\setminus\{0,1\},\ \alpha^2-\alpha+1 \neq 0 \right\}.$$

Proof. Let s_1 and s_2 be the number of orbits of sizes 1 and 3, respectively. It is easy to see that

$$s_1 + 3s_2 = \binom{q-2}{3}.$$

The total number of orbits can be found by the Cauchy–Frobenius lemma. We have

$$\begin{aligned} s_1 + s_2 &= \tfrac{1}{|H|} \sum_{g\in H} \mathrm{Fix}(g) \\ &= \tfrac{1}{3}\Big(\tbinom{q-2}{3} + 2L\Big), \end{aligned}$$

where L is the number of 3-subsets of $GF(q)\setminus\{0,1\}$ fixed by $x \mapsto (x-1)/x$ (note that $x \mapsto (x-1)/x$ and $x \mapsto 1/(1-x)$ have the same order and so, by Table 1, fixed the same number of 3-subsets). Therefore, $s_1 = L$ and $s_2 = \big(\binom{q-2}{3} - L\big)/3$. By Table 1, L is easily determined as shown in (2). Now suppose that B lies in an orbit of size 1 and let $\alpha \in B$. Then, $(\alpha-1)/\alpha, 1/(1-\alpha) \in B$. If $\alpha^2-\alpha+1 \neq 0$, then $B = \{\alpha, (\alpha-1)/\alpha, 1/(1-\alpha)\}$.

If $\alpha^2 - \alpha + 1 = 0$, then it is easily seen that every element of B satisfies the equation $x^2 - x + 1 = 0$. But this is an impossibility since this equation has at most two solutions in $GF(q)$. Finally, every subset of the form $\{\alpha, (\alpha-1)/\alpha, 1/(1-\alpha)\}$ clearly belongs to an orbit of size 1. $\square$

Lemma 2.3 *Let $A_\alpha := \{0, 1, \infty, \alpha, (\alpha-1)/\alpha, 1/(1-\alpha)\}$, where $\alpha \in GF(q) \setminus \{0, 1\}$ and let $B \in P_6(X)$. Then*
(i) $|G_B| = 3, 6$ *if and only if* $G(B) = G(A_\alpha)$ *for some* α*,*
(ii) *if* $|G_B| = 6$*, then* $G(B)$ *contains exactly one element of the form* A_α*,*
(iii) *if* $|G_B| = 3$*, then* $G(B)$ *contains exactly two elements of the form* A_α*,*
(iv) $|G_B| = 6$ *if and only if* $G(B) = G(A_\alpha)$ *for some* α *such that* $-\alpha^2 + \alpha - 1$ *is a nonzero square or,* $\alpha = 2$ *and* $q \not\equiv 0 \pmod 3$*.*

Proof. (i) If $G(B) = G(A_\alpha)$ for some α, then $H \le G_{A_\alpha}$. Therefore, $3 \mid |G_B|$. Conversely, let $3 \mid |G_B|$. Then $\lambda_B = 10, 20$. Since Λ_B is the union of orbits of H on $P_3(GF(q) \setminus \{0, 1\})$, it must contain some orbits of size 1 which are of the form $\{\alpha, (\alpha-1)/\alpha, 1/(1-\alpha)\}$. Therefore, $A_\alpha \in G(B)$ for some α.

(ii), (iii) Suppose that $A_\alpha, A_\beta \in G(B)$ where $A_\alpha \neq A_\beta$. Hence, there is a $g \in G$ such that $g(A_\alpha) = A_\beta$. Note that G_{A_α} and G_{A_β} contain H as a normal subgroup. So there are $h_1, h_2 \in H$ such that $h_1 g = g h_2$. Hence,

$$g(\{0, 1, \infty\}) = \Big\{\beta, \frac{\beta - 1}{\beta}, \frac{1}{1-\beta}\Big\}. \tag{3}$$

Now let $A_\gamma \in G(B)$ be distinct from A_α and A_β and $k \in G$ such that $k(A_\beta) = A_\gamma$. With a similar argument as for g we have $k(\{0, 1, \infty\}) = \{\gamma, (\gamma-1)/\gamma, 1/(1-\gamma)\}$. So by (3), $kg(\{0, 1, \infty\}) = \{0, 1, \infty\}$ and therefore $kg \in H$. Now $kg(A_\alpha) = A_\alpha$ and on the other hand $k\big(g(A_\alpha)\big) = A_\gamma$ which is a contradiction. Therefore, $G(B)$ contains at most two distinct blocks of the form A_α. Since $\lambda_B = 10$ or 20, the assertion follows.

(iv) Let $|G_B| = 6$. Then by (ii), $A_\alpha \in G(B)$ for some α. Assume that $g \in G_{A_\alpha}$ is of order 2. Then, similar to (3), $g(\{0, 1, \infty\}) = \{\alpha, (\alpha-1)/\alpha, 1/(1-\alpha)\}$. With no loss of generality, suppose $g(0) = \alpha$. If $g(\infty) = 1/(1-\alpha)$, then clearly $g(x) = (x-\alpha)/\big((1-\alpha)x - 1\big)$ and therefore $-\alpha^2 + \alpha - 1$ is a nonzero square. If $g(\infty) = (\alpha-1)/\alpha$, then $g(x) = \big((\alpha-1)x - \alpha^2 + \alpha\big)/(\alpha x - \alpha + 1)$. Since $g(1) = 1/(1-\alpha)$, we obtain $(1-\alpha)^3 = -1$ and therefore $\alpha = 2$ and necessarily $q \not\equiv 0 \pmod 3$. Conversely, if $-\alpha^2 + \alpha - 1$ is a nonzero square, then $g(x) = (x-\alpha)/\big((1-\alpha)x - 1\big)$ is of order 2, and $g(A_\alpha) = A_\alpha$, and therefore $|G_{A_\alpha}| = |G_B| = 6$. If $\alpha = 2$ and $q \not\equiv 0 \pmod 3$, then $g(x) = (x-2)/(2x-1)$ or $g(x) = (2x-1)/(x-2)$ belongs to G and since both of them are of order 2 and fix A_α, we have $|G_{A_\alpha}| = |G_B| = 6$. $\square$

Lemma 2.4 *The value of N_{10} is given by*

$$N_{10} = \begin{cases} 0 & \textit{if } q \equiv 3 \pmod{12}, \\ \frac{q-1}{6} & \textit{if } q \equiv 7 \pmod{12}, \\ \frac{q+7}{6} & \textit{if } q \equiv 11 \pmod{12}. \end{cases}$$

Proof. Let $S = \big\{t \in GF(q) \setminus \{0,1\} |\ -t^2 + t - 1 \text{ is a nonzero square}\big\}$. By Lemma 2.3, it suffices to find $|S|$. Let $T = \big\{t \in GF(q) \setminus \{0,1\} |\ t^2 - t + 1 \text{ is a square}\big\}$. Note that $|S| + |T| = q - 2$ and $S \cap T = \emptyset$. We have

$$\begin{aligned} |T| &= |\big\{t \in GF(q) \setminus \{0,1\} |\ \exists x \in GF(q),\ x^2 - 3 = (2t-1)^2\big\}| \\ &= |\big\{y \in GF(q) \setminus \{-1,1\} |\ \exists x \in GF(q),\ -3 = (y-x)(y+x)\big\}| \\ &= |\big\{y \in GF(q) \setminus \{-1,1\} |\ \exists a,b \in GF(q),\ ab = -3,\ y = (a+b)/2\big\}| \\ &= |\big\{\{a,b\} |\ a,b \in GF(q),\ ab = -3,\ a+b \neq \pm 2\big\}| \\ &= |\big\{\{a,b\} |\ a,b \in GF(q),\ ab = -3,\ \{a,b\} \neq \{-1,3\}, \{-3,1\}\big\}|. \end{aligned}$$

Therefore,

$$|T| = \begin{cases} q-2 & \text{if } q \equiv 3 \pmod{12}, \\ \frac{q-3}{2} & \text{if } q \equiv 7 \pmod{12}, \\ \frac{q-5}{2} & \text{if } q \equiv 11 \pmod{12}. \end{cases}$$

Using the fact that -3 is nonsquare if and only if $q \equiv 11 \pmod{12}$ (see [2] or deduce it from Lemma 2.2), we have

$$|S| = \begin{cases} 0 & \text{if } q \equiv 3 \pmod{12}, \\ \frac{q-1}{2} & \text{if } q \equiv 7 \pmod{12}, \\ \frac{q+1}{2} & \text{if } q \equiv 11 \pmod{12}. \end{cases}$$

Now Lemma 2.3 implies that

$$N_{10} = \begin{cases} 0 & \text{if } q \equiv 3 \pmod{12}, \\ \frac{q-1}{6} & \text{if } q \equiv 7 \pmod{12}, \\ \frac{q+7}{6} & \text{if } q \equiv 11 \pmod{12}. \quad \square \end{cases}$$

Lemma 2.5 *If $q \equiv 11 \pmod{20}$, then $N_{12} = 2$.*

Proof. The number of $B \in P_6(X)$ such that $|G_B| = 5$ is $12\binom{q+1}{3}N_{12}/\binom{6}{3}$. On the other hand, by Table 1, each element of order 5 of G fixes exactly $2(q-1)/5$ elements of $P_6(X)$ and there are exactly $2q(q+1)$ elements of order 5 in G. Therefore, $(q+1)q(q-1)/5$ distinct 6-subsets are fixed by the elements of order 5 of G. We now have $12\binom{q+1}{3}N_{12}/\binom{6}{3} = (q-1)q(q+1)/5$ and hence $N_{12} = 2$. $\square$

Theorem 2.6 *The number of orbits of $PSL(2,q)$ on $P_6(X)$ for all possible orbit indices are given below.*

$q \pmod{60}$	N_{10}	N_{12}	N_{20}	N_{30}	N_{60}
$3, 27$	0	0	$\frac{q-3}{6}$	$\frac{q^2-4q+3}{24}$	$\frac{2q^3-33q^2+72q+27}{720}$
$7, 19, 43$	$\frac{q-1}{6}$	0	$\frac{q-7}{12}$	$\frac{q^2-8q+7}{24}$	$\frac{2q^3-33q^2+132q+7}{720}$
$23, 47, 59$	$\frac{q+7}{6}$	0	$\frac{q-11}{12}$	$\frac{q^2-8q-9}{24}$	$\frac{2q^3-33q^2+132q+167}{720}$
11	$\frac{q+7}{6}$	2	$\frac{q-11}{12}$	$\frac{q^2-8q-9}{24}$	$\frac{2q^3-33q^2+132q-121}{720}$
31	$\frac{q-1}{6}$	2	$\frac{q-7}{12}$	$\frac{q^2-8q+7}{24}$	$\frac{2q^3-33q^2+132q-281}{720}$

Proof. We use the Cauchy–Frobenius lemma to count the total number M of orbits of G on $P_6(X)$. We have

$$M = \frac{1}{|G|}\sum_{g \in G} |\mathrm{Fix}(g)|,$$

where $|\mathrm{Fix}(g)|$ is the number of 6-subsets of X fixed by g. We refer to Table 1 to find $|\mathrm{Fix}(g)|$. If $|\mathrm{Fix}(g)| \neq 0$, then $o(g) = 1, 2, 3, 5, 6$, where $o(g)$ denotes the order of g. Let n_i

be the number of elements of order i in G. If $o(g) = 1$, then $|\mathrm{Fix}(g)| = \binom{q+1}{6}$. If $o(g) = 2$, then $|\mathrm{Fix}(g)| = \binom{(q+1)/2}{3}$ and $n_2 = |G|/(q+1)$. If $o(g) = 3$, then

$$|\mathrm{Fix}(g)| = \begin{cases} \binom{\frac{q}{3}}{2} & \text{if } q \equiv 3 \pmod{12}, \\ \binom{\frac{q-1}{3}}{2} & \text{if } q \equiv 7 \pmod{12}, \\ \binom{\frac{q+1}{3}}{2} & \text{if } q \equiv 11 \pmod{12}, \end{cases}$$

and

$$n_3 = \begin{cases} \frac{2|G|}{q} & \text{if } q \equiv 3 \pmod{12}, \\ \frac{2|G|}{q-1} & \text{if } q \equiv 7 \pmod{12}, \\ \frac{2|G|}{q+1} & \text{if } q \equiv 11 \pmod{12}. \end{cases}$$

If $o(g) = 5$, then $q \equiv 11 \pmod{20}$, $|\mathrm{Fix}(g)| = 2(q-1)/5$, and $n_5 = 4|G|/(q-1)$. If $o(g) = 6$, then $q \equiv 11 \pmod{12}$, $|\mathrm{Fix}(g)| = (q+1)/6$, and $n_6 = 2|G|/(q+1)$. We now obtain

$$M = \begin{cases} \frac{2q^3-3q^2+72q-243}{720} & \text{if } q \equiv 3, 27 \pmod{60}, \\ \frac{2q^3-3q^2+72q-323}{720} & \text{if } q \equiv 7, 19, 43 \pmod{60}, \\ \frac{2q^3-3q^2+72q+77}{720} & \text{if } q \equiv 23, 47, 59 \pmod{60}, \\ \frac{2q^3-3q^2+72q+1229}{720} & \text{if } q \equiv 11 \pmod{60}, \\ \frac{2q^3-3q^2+72q+829}{720} & \text{if } q \equiv 31 \pmod{60}. \end{cases}$$

The total number of orbits gives the equation

$$N_{10} + N_{12} + N_{20} + N_{30} + N_{60} = M. \tag{4}$$

By Lemmas 2.2 and 2.3, we also have

$$N_{10} + 2N_{20} = \begin{cases} \frac{q-3}{3} & \text{if } q \equiv 3 \pmod{12}, \\ \frac{q-4}{3} & \text{if } q \equiv 7 \pmod{12}, \\ \frac{q-2}{3} & \text{if } q \equiv 11 \pmod{12}. \end{cases} \tag{5}$$

On the other hand, by counting the 6-subsets of X containing $0, 1, \infty$, we have

$$10N_{10} + 12N_{12} + 20N_{20} + 30N_{30} + 60N_{60} = \binom{q-2}{3}. \qquad (6)$$

According to Lemmas 2.4 and 2.5, N_{10} and N_{12} are known. Therefore, the system of equations containing (4)–(6) are easily solved and the values of N_{20}, N_{30}, and N_{60} are determined. $\square$

3 3-Designs and Large Sets

In this section we use the results of previous section to find 3-$(q+1, 6, \lambda)$ designs with automorphism group $PSL(2, q)$ and large sets of these designs. Recall that every 3-$(q+1, 6, \lambda)$ design with automorphism group $G = PSL(2, q)$ is a union of distinct orbits of G on $P_6(X)$.

Theorem 3.1 *Let* $q \equiv 11 \pmod{20}$. *Then, there exist* 3-$(q+1, 6, \lambda)$ *designs with automorphism group* $PSL(2, q)$ *if and only if* $\lambda \equiv 0, 2, 4 \pmod{10}$, $1 \leq \lambda \leq \binom{q-2}{3}$, *and* $\lambda \neq i, \binom{q-2}{3} - i$ *for* $i = 2, 4, 14$.

Proof. Let $\mathcal{D}$ denote a 3-$(q+1, 6, \lambda)$ design with automorphism group $PSL(2, q)$. If $\mathcal{D}$ exists, then by (1), $2|\lambda$ and $1 \leq \lambda \leq \binom{q-2}{3}$. By Theorem 2.6, the indices of orbits of G on $P_6(X)$ are $10, 12, 20, 30, 60$. Therefore, $\lambda \equiv 0, 2, 4 \pmod{10}$ and $\lambda \neq i, \binom{q-2}{3} - i$ for $i = 2, 4, 14$.

Conversely, note that there are designs for $\lambda = 10, 12, 20, 22, 24$. It is easy to see that if there exists $\mathcal{D}$, then by replacing some suitable orbits of $\mathcal{D}$ by some unused orbits, one can obtain a 3-$(q+1, 6, \lambda+10)$ design. Otherwise, there are no more unused orbits and $\mathcal{D}$ is the complete 3-$(q+1, 6, \binom{q-2}{3})$ design. $\square$

Theorem 3.2 *Let* $q \not\equiv 11 \pmod{20}$. *Then, there are* 3-$(q+1, 6, \lambda)$ *designs with automorphism group* $PSL(2, q)$ *if and only if* $10|\lambda$ *and* $1 \leq \lambda \leq \binom{q-2}{3}$ *except for* $\lambda = 10$ *when* $q \equiv 0 \pmod{3}$.

Proof. Suppose that a 3-$(q+1, 6, \lambda)$ design with automorphism group $PSL(2, q)$ exists. By Theorem 2.6, the indices of orbits of G on $P_6(X)$ are $10, 12, 20, 30, 60$. Therefore, $10|\lambda$.

Conversely, similar to the proof of Theorem 3.1, one can show that for any λ such that $10|\lambda$ and $1 \leq \lambda \leq \binom{q-2}{3}$, a 3-$(q+1, 6, \lambda)$ design exists except for $\lambda = 10$ when $q \equiv 0 \pmod{3}$. $\square$

Theorem 3.3 *Let* $q \equiv 11 \pmod{20}$*. Then, there are* $PSL(2,q)$*-uniform* $\mathrm{LS}[N](3,6,q+1)$ *if and only if* $N = 2$ *and* $q \equiv 11, 91 \pmod{120}$*.*

Proof. Consider the action of G on $P_6(X)$. Suppose that there is a G-uniform $\mathrm{LS}[N](3,6,q+1)$. Since $N_{12} = 2$ and the other orbits have indices which are multiple of 10, we have $N = 2$. On the other hand, by the necessary conditions (1), $\binom{q-2}{3}(q-1)/8$ must be integer. Therefore, $q \equiv 11$ or $91 \pmod{120}$.

Conversely, let $N = 2$ and $q \equiv 11, 91 \pmod{120}$. First let $q \equiv 11 \pmod{120}$. In this case, N_{10} and N_{30} are odd and N_{20} is even. Let D be an empty set. Consider $1, (N_{10}-3)/2, N_{20}/2$, and $(N_{30}-1)/2$ orbits of indices $12, 10, 20$, and 30, respectively, and add them to D. If N_{60} is odd, then also add $[N_{60}/2], 3$, and 1 orbits of indices $60, 10$, and 30, respectively, to D. If N_{60} is even, then add $[N_{60}/2]$ and 1 orbits of indices 60 and 30, respectively, to D. Now $\{(X,D),(X,P_6(X)\setminus D)\}$ is a $\mathrm{LS}[2](3,6,q+1)$. Now let $q \equiv 91 \pmod{120}$. Note that N_{10}, N_{20}, and N_{30} are odd. Consider $(N_{10}-1)/2, (N_{20}-1)/2$, and $(N_{30}-1)/2$ orbits of indices $10, 20$ and 30, respectively, and add them to D. If N_{60} is odd, then also add $[N_{60}/2], 1, 1$, and 1 orbits of indices $60, 10, 20$, and 30, respectively, to D. If N_{60} is even, then add $[N_{60}/2]$ orbits of index 60 and one orbit of index 30 to D. Now $\{(X,D),(X,P_6(X)\setminus D)\}$ is a $\mathrm{LS}[2](3,6,q+1)$. $\square$

Theorem 3.4 *Let* $q \not\equiv 11 \pmod{20}$*. Then, there are* $PSL(2,q)$*-uniform* $\mathrm{LS}[N](3,6,q+1)$ *if and only if one of the following holds:*

(i) $\binom{q-2}{3}/N \equiv 0 \pmod{60}$*,*

(ii) $\binom{q-2}{3}/N \equiv 10, 40 \pmod{60}$ *and* $N \le N_{10} + [N_{20}/2]$*,*

(iii) $\binom{q-2}{3}/N \equiv 20, 50 \pmod{60}$ *and* $N \le [N_{10}/2] + N_{20}$*,*

(iv) $\binom{q-2}{3}/N \equiv 30 \pmod{60}$ *and* $N \le N_{20} + N_{30} + [(N_{10}-N_{20})/2]$*.*

Proof. Consider the action of G on $P_6(X)$. Let $\binom{q-2}{3} = N(60m+l)$ where $0 \le l \le 60$. Suppose that there is a G-uniform large set of 3-$(q+1, 6, 60m+l)$ designs. Then by Theorem 2.6, $l \equiv 0 \pmod{10}$. If $l = 10, 40$, then some designs of the large set contain orbits of index 10 and each of the other designs contains necessarily at least two orbits of index 20. Therefore, $N \le N_{10} + [N_{20}/2]$. If $l = 20, 50$, then some designs in the large set contain orbits of index 20 and each of the other designs contains at least two orbits of index 10. Hence, $N \le [N_{10}/2] + N_{20}$. If $l = 30$, then some designs in the large set contain orbits of index 30 and each of the other designs contains one orbit of index 10 and one orbit of index 20 or at least three orbits of index 10. Therefore, $N \le N_{20} + N_{30} + [(N_{10}-N_{20})/2]$.

Conversely, let one of (i)–(iv) hold. Let D_f $(1 \le f \le N)$ be N empty sets. Here is a useful observation. If there are x_1, x_2, x_3, and x_4 orbits of indices $10, 20, 30$, and 60, respectively, such that $10x_1 + 20x_2 + 30x_3 + 60x_4 = 60x$, then it is easy to see that by suitable combinations of these orbits we can find x disjoint 3-$(q+1, 6, 60)$ designs. If (i) holds, then by this observation we are done. Now let (ii) hold. Note that $N_{30} \ge [N_{20}/2]$ and $N_{30} \ge N_{10}$. Choose x $(0 \le x \le \min\{N, N_{10}\})$ orbits of index 10 and add to each of D_i $(1 \le i \le x)$ one of them. Choose $2(N-x)$ orbits of index 20 and add to each of D_j $(x < j \le N)$ two of them. If $l = 10$ (respectively, $l = 40$), then also add to each of D_j (respectively, D_i) one orbit of index 30. If $l = 10$ (respectively, $l = 40$), this leaves $\binom{q-2}{3} - 10x - 70(N-x) = 60xm + 60(N-x)(m-l)$ (respectively, $\binom{q-2}{3} - 40x - 40(N-x) = 60xm + 60(N-x)m$) 6-subsets unused. Therefore, by the observation above, D_f $(1 \le f \le N)$ can be filled with suitable unused orbits to obtain N sets with the same size. Now $\{(X, D_f)|\ 1 \le f \le N\}$ is the desired large set. Now suppose that (iii) holds. Choose x $(0 \le x \le \min\{N, N_{20}\})$ orbits of index 20 and add to each of D_i $(1 \le i \le x)$ one of them. Choose $2(N-x)$ orbits of index 10 and add to each of D_j $(x < j \le N)$ two of them. If $l = 50$, then also add to each of D_i $(1 \le i \le N)$, one orbit of index 30 (note that $N_{30} \ge [N_{10}/2] + N_{20}$). The number of unused blocks is equal to $\binom{q-2}{3} - lx - l(N-x) = 60mN$. Therefore, by the observation above, the remaining orbits can be divided between to D_f $(1 \le f \le N)$ to obtain N sets of the same size which results in large set $\{(X, D_f)|\ 1 \le f \le N\}$. Finally, assume that (iv) holds. Choose x orbits $(0 \le x \le \min\{N, N_{30}\})$ of index 30 and add to each of D_i $(1 \le i \le x)$ one of them. Choose y orbits $(0 \le y \le \min\{N_{20}, N-x\})$ of index 10 and y orbits of index 20 and add to each of D_j $(x < j \le N-x-y)$ one orbit of index 10 and one orbit of index 20. There are totaly $\binom{q-2}{3} - 30x - 30y - 30(N-x-y) = 60mN$ unused 6-subsets and therefore, by the observation above, the remaining orbits can be appended in a suitable way to D_f $(1 \le f \le N)$ to obtain N sets of the same size. Now $\{(X, D_f)|\ 1 \le f \le N\}$ is the desired large set. $\square$

4 3-$(28, 6, 10m)$ Designs

The existence of 3-$(28, 6, 10m)$ designs has been known only for a small number of some large values of m (see [9]). In the previous section we showed that these designs exist for all possible values of m, i.e., $1 \le m \le 230$ except for $m = 1, 229$ (Theorem 3.2). Note that the existence of 3-$(28, 6, 10m)$ designs for $m = 1$ implies the existence of such designs for $m = 229$. By [9], a 3-$(28, 6, 10)$ design with repeated blocks exists, but no simple one is known. We now construct a simple 3-$(28, 6, 10)$ design by prescribing a suitable subgroup of $PSL(2, 27)$ as its automorphism group. Let $PSL(2, 27) = \langle a, b \rangle$ where

$$a = (1\ 2)(3\ 4)(5\ 7)(6\ 8)(9\ 12)(10\ 13)(11\ 15)(14\ 19)(16\ 20)(17\ 21)(18\ 22)(23\ 25)(24\ 26)(27\ 28),$$

$$b = (2\ 3\ 5)(4\ 6\ 9)(7\ 10\ 14)(8\ 11\ 16)(12\ 17\ 20)(13\ 18\ 23)(15\ 19\ 22)(21\ 24\ 27)(25\ 26\ 28).$$

Consider the subgroup $L = \langle b, c \rangle$ of $PSL(2, 27)$ in which

$$c = (2\ 3\ 19\ 21\ 25\ 27\ 20\ 15\ 10\ 23\ 5\ 16\ 17)(4\ 26\ 13\ 22\ 18\ 8\ 28\ 7\ 24\ 9\ 12\ 11\ 6).$$

The order of L is 351. The union of orbits of L with representatives

$$\{1, 2, 3, 4, 7, 19\}, \{2, 3, 4, 5, 6, 9\},$$

$$\{2, 3, 4, 9, 22, 23\}, \{2, 3, 5, 8, 11, 16\},$$

$$\{2, 3, 4, 8, 23, 24\}, \{2, 3, 4, 6, 13, 21\},$$

identify the block set of a 3-$(28, 6, 10)$ design. This design was found via DISCRETA, a program to construct t-designs with prescribed automorphism group written at the Mathematics Department, University of Bayreuth, Germany.

Acknowledgment: This work was done while the second author was a Postdoctoral Research Associate at the School of Mathematics, Institute for Studies in Theoretical Physics and Mathematics (IPM). He would like to thank IPM for the financial support.

References

[1] T. Beth, D. Jungnickel, H. Lenz, "*Design Theory*", Vol. I, Second edition, Cambridge University Press, Cambridge, 1999.

[2] W. Burnside, "*Theory of Groups of Finite Order*", Second edition, Dover Publications, Inc., New York, 1955.

[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** (1995), no. 2, 147-160.

[4] C. A. Cusack, S. S. Magliveras, *Semiregular Large Sets*, Des. Codes Cryptogr. **18** (1999), no. 1-3, 81-87.

[5] L. E. Dickson, "*Linear Groups with an Exposition of the Galois Field Theory*", Dover Publications, Inc., New York, 1958.

[6] D. Gorenstein, "*Finite Groups*", Second edition, Chelsea Publishing Co., New York, 1980.

[7] D. R. Hughes, *On t-Designs and Groups*, Amer. J. Math. **87** (1965), 761-778.

[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** (1997), no. 2, 95-110.

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

[10] R. Laue, S. S. Magliveras, A. Wassermann, *New Large Sets of t-Designs*, J. Combin. Des. **9** (2001), no. 1, 40-59.

The Authors' Addresses

G. R. Omidi, Department of Mathematics and Computer Science, Faculty of Science, University of Tehran, Tehran, Iran, and School of Mathematics, Institute for Studies in Theoretical Physics and Mathematics, P.O. Box 19395-5746, Tehran, Iran.

E-mail address: `omidi@ipm.ir`

M. R. Pournaki, School of Mathematics, Institute for Studies in Theoretical Physics and Mathematics, P.O. Box 19395-5746, Tehran, Iran.

E-mail address: `pournaki@ipm.ir`

B. Tayfeh-Rezaie, School of Mathematics, Institute for Studies in Theoretical Physics and Mathematics, P.O. Box 19395-5746, Tehran, Iran.

E-mail address: `tayfeh-r@ipm.ir`