3-Designs and Large Sets of PSL$(2, 2^n)$ with Block Sizes 6

G. R. Omidi [1]
Department of Mathematical Sciences, Isfahan University of Technology,
Isfahan, 84156-83111, Iran
E-mail: romidi@cc.iut.ac.ir

Abstract

We investigate the existence of 3-designs and uniform large sets of 3-designs with block size 6 admitting PSL$(2, 2^n)$ as an automorphism group.

Keywords: 3-Design; Large set of 3-designs; Projective special linear group.
AMS subject classification: 05B05.

1 Introduction

Let t, k, v, and λ be integers such that $0 \le t \le k \le v$ 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

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

[1] Part of the results of this paper is recently obtained by Li and Shen, using a different method ([10]).

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 $\mathrm{LS}[N](t,k,v)$, 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 $G(x) = \{gx \mid g \in G\}$ and the *stabilizer* of x is $G_x = \{g \in G \mid gx = x\}$. It is well known that $|G| = |G(x)||G_x|$. 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 $X = \mathrm{GF}(q) \cup \{\infty\}$. Then the set of all mappings $g: x \mapsto \frac{ax+b}{cx+d}$, on X such that $a,b,c,d \in \mathrm{GF}(q)$, $ad - bc$ is a nonzero 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 general linear group* and is denoted by $\mathrm{PGL}(2,q)$. The set of all elements of $\mathrm{PGL}(2,q)$ for which $ad - bc$ is a square is a group called *projective special linear group* and is denoted by $\mathrm{PSL}(2,q)$. Note that for $q = 2^n$ every element of $\mathrm{GF}(q)$ is a square and so $\mathrm{PSL}(2,q)$ is isomorphic to the $\mathrm{PGL}(2,q)$. Thus $\mathrm{PSL}(2,q)$ is sharply 3-transitive on X and $|\mathrm{PSL}(2,q)| = (q^3 - q)$. The structure of the elements of $\mathrm{PSL}(2,q)$ is well known (see for example [4, 5]) and is given in Table 1, for $q = 2^n$ where φ denotes Euler's function. In this Table the third column show the number of conjugacy classes.

Table 1

The structure of the elements of $\mathrm{PSL}(2,q)$, $q = 2^n$

order	order of centralizer	no. of classes	type
1	$q^3 - q$	1	1^{q+1}
2	q	1	$1^1 2^{\frac{q}{2}}$
$d \mid q-1$	$q-1$	$\frac{\varphi(d)}{2}$	$1^2 d^{\frac{q-1}{d}}$
$d \mid q+1$	$q+1$	$\frac{\varphi(d)}{2}$	$d^{\frac{q+1}{d}}$

The group $\mathrm{PSL}(2,q)$ has been used for constructing t-designs by different authors, see for example [1, 2, 3, 4, 6, 7, 9, 11]. In [3, 11], for $q \equiv 3 \pmod 4$ all 3-designs and uniform large sets of 3-designs with block sizes 4,5 and 6 admitting $\mathrm{PSL}(2,q)$ as an automorphism group were completely determined. In [2], for $q \equiv 3 \pmod 4$ all parameters for which there exist 3-designs with block size not congruent to 0 and 1 modulo p ($q = p^n$) with automorphism group $\mathrm{PSL}(2,q)$ were determined. In [8], for $q = 2^n$ all 3-designs with block sizes 4, 5 admitting $\mathrm{PSL}(2,q)$ 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 $\mathrm{PSL}(2,2^n)$. Recently all 3-designs with block size 6 from $\mathrm{PSL}(2,2^n)$ were determined by Li and Shen, using a different method, ([10]). Since $\mathrm{PSL}(2,q)$ is 3-transitive, a 3-$(q+1,k,\lambda)$ design admits $\mathrm{PSL}(2,q)$ as an automorphism group if and only if its block set is the union of orbits of $\mathrm{PSL}(2,q)$ on $P_k(X)$. We determine the number of orbits for all possible orbit sizes from the action of $\mathrm{PSL}(2,q)$ on $P_6(X)$ and then use the results to construct 3-$(q+1,6,\lambda)$ designs and large sets of these designs.

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

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

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 $\Lambda_B = \{\{x,y,z\} |\ \{0,1,\infty,x,y,z\} \in G(B)\}$. 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 $\lambda_B|G_B| = 120$ and*
i) *if $n \equiv 0 \pmod 4$, then $\lambda_B = 20, 24, 40, 60, 120$,*
ii) *if $n \not\equiv 0 \pmod 4$, then $\lambda_B = 20, 40, 60, 120$,*

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 $\lambda_B|G_B| = 120$. By (1), $4|\lambda_B(q-1)$ and so $4|\lambda_B$. Moreover, $5|\lambda_B q(q-1)$ and therefore if $n \not\equiv 0 \pmod 4$, then $5|\lambda_B$. It follows that $\lambda_B = 20, 40, 60, 120$, if $n \not\equiv 0 \pmod 4$ and $\lambda_B = 4, 8, 12, 20, 24, 40, 60, 120$, otherwise. We now show that $\lambda_B \neq 4, 8, 12$ or equivalently $|G_B| \neq 30, 15, 10$.

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. Then at least one of the P_1 or P_2 is normal in G_B. Therefore, P_1P_2 is a subgroup of order 15 of G_B which is impossible as described above. □

Lemma 2.2 *Let H act on $P_3(\mathrm{GF}(q) \setminus \{0,1\})$. Then all nonregular orbits are of size 2 and the number of these orbits are $(q-i)/6$, where $i = 4$ for even n and $i = 2$ otherwise.*

Proof Since each element of order 2 in H cannot fix any element of $P_3(\mathrm{GF}(q)\setminus\{0,1\})$, all nonregular orbits are of size 2. Let $i=4$ for even n and $i=2$ otherwise. Let s_1 and s_2 be the number of orbits of sizes 2 and 6, respectively. It is easy to see that $2s_1+6s_2=\binom{q-2}{3}$. The total number of orbits can be found by the Cauchy-Frobenius lemma. We have

$$s_1+s_2 = \frac{1}{|H|}\sum_{g\in H}\mathrm{Fix}(g) = \frac{1}{6}\left(\binom{q-2}{3}+L\right),$$

where L is the number of 3-subsets of $\mathrm{GF}(q)\setminus\{0,1\}$ fixed by $x\mapsto(x-1)/x$ or $x\mapsto 1/(x-1)$. Therefore, $s_1=L/4$ and $s_2=\left(2\binom{q-2}{3}-L\right)/12$. By Table 1, we can see that $L=2(q-i)/3$. □

Lemma 2.3 *If* $n\equiv 0 \pmod 4$, *then* $N_{24}=1$.

Proof The number of $B\in P_6(X)$ such that $|G_B|=5$ is $(q^3-q)N_{24}/5$. 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 $(q^3-q)N_{24}/5=(q-1)q(q+1)/5$ and hence $N_{24}=1$. □

Lemma 2.4 *We have* $N_{20}+N_{60}=(q-2)(q-4)/24$ *and*

$$N_{20}+2N_{40}=\begin{cases}\frac{(q-4)}{6} & \text{if } n\equiv 0,2 \pmod 4,\\ \frac{(q-2)}{6} & \text{if } n\equiv 1,3 \pmod 4.\end{cases}$$

Proof Let $S=\{(g,B)|g(B)=B, o(g)=2\}$. By double counting and using Table 1, we have $|S|=3|G|\frac{N_{20}}{6}+|G|\frac{N_{60}}{2}=\frac{|G|\binom{q/2}{3}}{q}$. So $N_{20}+N_{60}=(q-2)(q-4)/24$. Now let $S=\{(g,B)|g(B)=B, o(g)=3\}$. By double counting and using Table 1 we have

$$|S|=2|G|\frac{N_{20}}{6}+2|G|\frac{N_{40}}{3}=\begin{cases}\frac{|G|\binom{(q-1)/3}{2}}{q-1} & \text{if } n\equiv 0,2 \pmod 4,\\ \frac{|G|\binom{(q+1)/3}{2}}{q+1} & \text{if } n\equiv 1,3 \pmod 4.\end{cases}$$

So

$$N_{20} + 2N_{40} = \begin{cases} \frac{(q-4)}{6} & \text{if } n \equiv 0,2 \pmod 4, \\ \frac{(q-2)}{6} & \text{if } n \equiv 1,3 \pmod 4. \end{cases}$$

□

Theorem 2.1 *Let* $n = r \pmod 4$. *Then the number of orbits of* PSL$(2, 2^n)$ *on* $P_6(X)$ *for all possible orbit indices are given below.*

r	N_{20}	N_{24}	N_{60}	N_{120}
0	$\frac{q-4}{6}$	1	$\frac{(q-4)(q-6)}{24}$	$\frac{q^3-24q^2+156q-448}{720}$
2	$\frac{q-4}{6}$	0	$\frac{(q-4)(q-6)}{24}$	$\frac{(q-4)(q^2-20q+76)}{720}$
1, 3	$\frac{q-2}{6}$	0	$\frac{(q-2)(q-8)}{24}$	$\frac{(q-2)(q^2-22q+112)}{720}$

Proof Since all k-subsets are partitioned by the orbits, we have

$$|G|\frac{N_{20}}{6} + |G|\frac{N_{24}}{5} + |G|\frac{N_{40}}{3} + |G|\frac{N_{60}}{2} + |G|N_{120} = \binom{q+1}{6}$$

So by lemmas 2.1, 2.2, 2.3, 2.4, the proof is complete. □

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 $G = \text{PSL}(2, q)$ is a union of distinct orbits of G on $P_6(X)$.

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

Proof Let $\mathcal{D}$ denote a 3-$(q+1,6,\lambda)$ design with automorphism group $\mathrm{PSL}(2,q)$. If $\mathcal{D}$ exists, then by (1), $4|\lambda$ and $1 \le \lambda \le \binom{q-2}{3}$. By Theorem 2.1, the indices of orbits of G on $P_6(X)$ are $20, 24, 60, 120$. Therefore, $\lambda \equiv 0, 4 \pmod{20}$ and $\lambda \ne i, \binom{q-2}{3} - i$ for $i = 4$.

Conversely, note that there are designs for $\lambda = 20, 24, 60, 120$. 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-$(q+1,6,\lambda+20)$ design. Otherwise, there are no more unused orbits and $\mathcal{D}$ is the complete 3-$(q+1,6,\binom{q-2}{3})$ design. □

Theorem 3.2 *Let* $n \not\equiv 0 \pmod 4$. *Then, there are* 3-$(q+1,6,\lambda)$ *designs with automorphism group* $\mathrm{PSL}(2,q)$ *if and only if* $20|\lambda$ *and* $1 \le \lambda \le \binom{q-2}{3}$.

Proof Suppose that a 3-$(q+1,6,\lambda)$ design with automorphism group $\mathrm{PSL}(2,q)$ exists. By Theorem 2.1, the indices of orbits of G on $P_6(X)$ are $20, 60, 120$. Therefore, $20|\lambda$.

Conversely, similar to the proof of Theorem 3.1, one can show that for any λ such that $20|\lambda$ and $1 \le \lambda \le \binom{q-2}{3}$, there exists a 3-$(q+1,6,\lambda)$ design. □

Theorem 3.3 *Let* $n \equiv 0 \pmod 4$. *Then, there are no* $\mathrm{PSL}(2,q)$*-uniform* $\mathrm{LS}[N](3,6,q+1)$.

Proof Consider the action of G on $P_6(X)$. Since $N_{24} = 1$ and the other orbits have indices which are multiple of 20, we have no G-uniform $\mathrm{LS}[N](3,6,q+1)$. □

Theorem 3.4 *Let* $n \not\equiv 0 \pmod 4$. *Then, there are* $\mathrm{PSL}(2,q)$*-uniform* $\mathrm{LS}[N](3,6,q+1)$ *if and only if one of the following holds:*
i) $\binom{q-2}{3}/N \equiv 0 \pmod{120}$,
ii) $\binom{q-2}{3}/N \equiv 20, 80 \pmod{120}$ *and* $N \le N_{20}$,
iii) $\binom{q-2}{3}/N \equiv 40, 100 \pmod{120}$ *and* $N \le [N_{20}/2]$,
iv) $\binom{q-2}{3}/N \equiv 60 \pmod{120}$ *and* $N \le N_{60} + [N_{20}/3]$.

Proof Consider the action of G on $P_6(X)$. Let $\binom{q-2}{3} = N(120m + l)$ where $0 \le l \le 120$. Suppose that there is a G-uniform large set of 3-$(q+1,6,120m+l)$ designs. Then by Theorem 2.1, $l \equiv 0 \pmod{20}$. If

$l = 20, 80$, then all designs of the large set contain at least one orbit of index 20. Therefore, $N \leq N_{20}$. If $l = 40, 100$, then all designs in the large set contain at least two orbits of index 20. Hence, $N \leq [N_{20}/2]$. If $l = 60$, then some designs in the large set contain orbits of index 60 and each of the other designs contains at least three orbits of index 20. Therefore, $N \leq N_{60} + [N_{20}/3]$.

Conversely, let one of (i)–(iv) hold. Let D_f $(1 \leq f \leq N)$ be N empty sets. Here is a useful observation. If there are x_1, x_2, and x_3 orbits of indices 20, 60, and 120, respectively, such that $20x_1 + 60x_2 + 120x_3 = 120x$, then it is easy to see that by suitable combinations of these orbits we can find x disjoint 3-$(q+1, 6, 120)$ designs. If (i) holds, then by this observation we are done. Now let (ii) hold. Note that $N_{60} \geq N_{20}$. Choose N orbits of index 20 and add to each of D_i $(1 \leq i \leq N)$ one of them. If $l = 80$, then Choose N orbits of index 60 and add to each of D_i $(1 \leq i \leq N)$ one of them. If $l = 20$ (respectively, $l = 80$), this leaves $\binom{q-2}{3} - 20N = 120mN$ (respectively, $\binom{q-2}{3} - 20N - 60N = 120mN$) 6-subsets unused. Therefore, by the observation above, D_f $(1 \leq f \leq N)$ can be filled with suitable unused orbits to obtain N sets with the same size. Now $\{(X, D_f) | \ 1 \leq f \leq N\}$ is the desired large set. Now suppose that (iii) holds. Choose $2N$ orbits of index 20 and add to each of D_i $(1 \leq i \leq N)$ two of them. If $l = 100$, then also add to each of D_i $(1 \leq i \leq N)$, one orbit of index 60. The number of unused blocks is equal to $120mN$. Therefore, by the observation above, the remaining orbits can be divided between to D_f $(1 \leq f \leq N)$ to obtain N sets of the same size which results in large set $\{(X, D_f) | \ 1 \leq f \leq N\}$. Finally, assume that (iv) holds. Choose x orbits $(0 \leq x \leq \min\{N, N_{60}\})$ of index 60 and add to each of D_i $(1 \leq i \leq x)$ one of them. Choose $y = 3(N - x)$ orbits of index 20 and add to each of D_j $(x < j \leq N)$ three of them. There are totaly $\binom{q-2}{3} - 60x - 20(3(N - x)) = 120mN$ unused 6-subsets and therefore, by the observation above, the remaining orbits can be appended in a suitable way to D_f $(1 \leq f \leq N)$ to obtain N sets of the same size. Now $\{(X, D_f) | \ 1 \leq f \leq N\}$ is the desired large set. □

4. Acknowledgments

This work was partially supported by IUT (CEAMA).

References

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

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

[3] C. A. Cusack, S. W. Graham and D. L. Kreher, Large Sets of 3-Designs from PSL$(2, q)$, with Block Sizes 4 and 5, J. Combin. Des. **3** (1995), 147-160.

[4] C. A. Cusack and S. S. Magliveras, Semiregular Large Sets, Des. Codes Cryptogr. **18** (1999), 81-87.

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

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

[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** (1997), 95-110.

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

[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), 47-66.

[10] W. Li and H. Shen, Simple 3-designs of PSL$(2, 2^n)$ with Block Sizes 6, Discrete Math., In Press, Corrected Proof, Available online 24 September 2007.

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