Simple 3-(q + 1, 5, 3) designs admitting an automorphism group PSL(2, q) with \( q \equiv 1 \pmod{4} \)

Weixia Li  
*School of Mathematical Sciences, Qingdao University*  
Qingdao 266071, China  

Dameng Deng  
*Department of Mathematics, Shanghai JiaoTong University*  
Shanghai 200240, China  

Guangjun Zhang  
*School of Mathematics and Physics, Qingdao University of Science and Technology*  
Qingdao 266061, China  

May 23, 2017

Abstract

In this paper, we give the necessary and sufficient conditions for the existence of simple 3-(q + 1, 5, 3) designs admitting PSL(2, q) as an automorphism group, where \( q \equiv 1 \pmod{4} \). In the conditions, the classification of the simple 3-(q + 1, 5, 3) designs admitting PSL(2, q) as an automorphism group is given and, for any positive integer \( n \), a simple 3-(5\( n \) + 1, 5, 3) design is given and it is minimal in \( \lambda \) when \( n \) is odd. Moreover, by the conditions, a method is given to find a simple 3-(q + 1, 5, 3) design and using the method we find a simple 3-(10, 5, 3) design in which the value of the index \( \lambda \) is also minimal.

AMS Classifications: 05B05

Key words: 3-Designs; Projective special linear group; Automorphism group

*Research supported by National Natural Science Foundation of China under Grant 11501315 and 11601208*
1 Background

When $q \equiv 1 \pmod{4}$, the action of $\text{PSL}(2, q)$ on $X$ is not 3-homogeneous, then unions of orbits do not necessarily yield 3-designs. As a result, the problem for this case becomes more difficult.

1. In [10], all quadruple systems admitting $\text{PSL}(2, q)$ with $q \equiv 1 \pmod{4}$ are completely determined by M. S. Keranen, D. L. Kreher, and P. J. S. Shiue.

2. Other authors[1, 9, 11] have also obtained partial results for a variety of values of block size, however, none of which are as complete as that of Keranen, D. L. etc.

3. Recently, much attention is attracted on the existence and classification of simple 3-designs with small index $\lambda$ admitting $\text{PSL}(2, q)$. In [7, 12], Steiner 3-designs admitting $\text{PSL}(2, q)$ as an automorphism group were investigated. In [7], M. Huber classified all Steiner quadruple systems, and in [12], J. Tang et al. classified all $3-(v, k, 1)$ designs.

In this paper, we discuss the existence and classification of simple 3-$(q + 1, 5, 3)$ designs admitting $\text{PSL}(2, q)$ for the case of $q \equiv 1 \pmod{4}$.

2 Preliminaries

1. Projective special linear group $\text{PSL}(2, q)$.

It is a group acting on the Projective line $X = F_q \cup \{\infty\}$ and consists of all the maps

$$ f : X \rightarrow X, $$

where

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

and $ad - bc$ is a non-zero square.

Classification of the subgroups

1.) Cyclic subgroups of order $d$ where $d|q^\pm 1$;

2.) Elementary Abelian subgroups of order $p^m$, where $m \leq n$;

3.) Dihedral subgroups of order $2d$ where $d|\frac{q^\pm 1}{2}$;

4.) $A_4$(size 12);

5.) $S_4$(size 24) when $q^2 - 1 \equiv 0 \pmod{16}$;

6.) $A_5$(size 60) when $q \equiv \pm 1 \pmod{10}$;

7.) The semidirect product of the elementary Abelian subgroup of order $p^m$ and the cyclic group of order $d$, where $m \leq n$, $d|\frac{q^\pm 1}{2}$ and $d|(p^m - 1)$;

8.) Subgroups $\text{PSL}(2, p^m)$ with $m|n$;

9.) Subgroups $\text{PGL}(2, p^m)$ with $2m|n$. 


2. \( t-(q^n + 1, k, \lambda) \) design

Suppose \( t, v, k \) and \( \lambda \) are given positive integers. A \( t-(v, k, \lambda) \) design, a \( t \)-design in short, is a pair \((X, B)\), where \( X \) is a \( v \)-set of points and \( B \) is a collection of \( k \)-subsets of \( X \) called blocks, such that every \( t \)-subset of \( X \) is contained in precisely \( \lambda \) blocks. The parameter \( \lambda \) is the index of the design. A \( t-(v, k, \lambda) \) design is simple if \( B \) contains no repeated blocks.

3. The acting of \( PSL(2,q) \) on a \( t-(v,k,\lambda) \) design \((X,B)\)

\[ B^{PSL(2,q)} = \{ Bg | g \in PSL(2,q) \} \]

where \( Bg = \{ xg | x \in B \} \). We know \( B \) is a union of some orbits of \( k \)-subsets contained in \( X \) under \( PSL(2,q) \).

3 Main results

1.) Simple \( 3-(q+1, 5, 3) \) designs on which the action of \( \mathcal{G} \) is block-transitive

In this section, we will give the necessary and sufficient conditions for the existence of a simple \( 3-(q+1, 5, 3) \) design on which \( \mathcal{G} \) acts block-transitively. By the conditions given, we give a method to find a simple \( 3-(q+1, 5, 3) \) design and using the method we find a simple \( 3-(10,5,3) \) design which is minimal in \( \lambda \). The simple \( 3 \)-design of the same parameter has already been known and it is also known that \( \lambda = 3 \) is minimal[4].

**Lemma 3.1** Let \( q = 5^n \). If \( n \) is odd, then \( F_5^q = (\gamma F_5^q)^\mathcal{G} \) and \((X, F_5^q \cup (X, (\gamma F_5^q)^\mathcal{G}))\) is a simple \( 3-(5^n + 1, 5, 3) \) design in which the value of the index \( \lambda \) is minimal. If \( n \) is even, then \( F_5^q \cap (\gamma F_5^q)^\mathcal{G} = \emptyset \) and \((X, F_5^q \cup (\gamma F_5^q)^\mathcal{G})\) is a simple \( 3-(5^n + 1, 5, 3) \) design.

**Lemma 3.2** Suppose \( 5 |(q+1) \), \( \theta \) is a nonsquare of \( F_q \) and \( \theta^2 - 4\theta - 1 = 0 \), then \((X, \{0, 1, -1, \theta, -\theta \})^\mathcal{G}\) is a simple \( 3-(q+1, 5, 3) \) design.

**Theorem 3.3** \((X, B)\) is a simple \( 3-(q+1, 5, 3) \) design on which \( \mathcal{G} \) acts block-transitively if and only if one of the following cases occurs:

1. \( 5 |(q+1) \) and \( B = \{0, 1, -1, \theta, -\theta \}^\mathcal{G} \), where \( \theta \) is a nonsquare and \( \theta^2 - 4\theta - 1 = 0 \).
2. \( q = 5^n \), \( n \) is odd, and \( B = F_5^q \).

**Proof.** The sufficiency follows from Lemmas 3.1 and 3.2. Let us prove the necessity. Because the action of \( \mathcal{G} \) on \((X, B)\) is block-transitive, we may suppose \( B = B^\mathcal{G} \), where \( B \) is a 5-subset of \( X \). By Lemma 3.1, we know that \( |G_B| = 10 \). Then \( G_B \) must contain a linear fraction of order 5, so does \( \mathcal{G} \). Thus \( 5 ||\mathcal{G}| = \frac{(q+1)(q-1)}{2} \). Because \( \frac{q+1}{2}, q - 1 \) and \( q \) are pairwise coprime,
then $5| \frac{q+1}{2}$, $5| \frac{q-1}{2}$ or $5|q$, and in the last case $q = 5^n$ for some positive integer $n$.

**Case 1.** $5| \frac{q+1}{2}$

By Lemma ??, $G_B$ is not a cyclic group, then the elements contained in $G_B$ are of order 1, 2 or 5 each of which is not equal to $p(q = p^n)$. By Lemma ??, $G_B$ is $D_{10}$, a Dihedral group of order 10 (Other subgroups are of order larger than 10 or contain an element of order $p$). Then $G_B$ contains an element of order 2 which is conjugate with the linear fraction $g$ such that $x^g = -x$ for any $x \in X$. Then

$$B = B^g = \{0, \alpha, -\alpha, \beta, -\beta\}^g \text{ or } \{\infty, \alpha, -\alpha, \beta, -\beta\}^g$$

for some $\alpha, \beta \in F_q^*$. Let $h$ be the linear fraction such that $x^h = \frac{1}{2}$, then $h \in G$ and

$$\{0, \alpha, -\alpha, \beta, -\beta\}^h = \{\infty, \alpha^{-1}, -\alpha^{-1}, \beta^{-1}, -\beta^{-1}\}.$$

Thus we may suppose $B = \{0, \alpha, -\alpha, \beta, -\beta\}^g$ for some $\alpha, \beta \in F_q^*$. Since $(X, B^g)$ is a 3-design and there are 10 3-subsets in $B$ altogether, then $N_1(B) = N_2(B) = 5$. If both $\alpha$ and $\beta$ are squares or nonsquares, then $\alpha^{-1}\beta$ is a square. Let $u$ be the linear fraction such that $x^u = \alpha^{-1}\beta x$ for any $x \in X$. Since $g, u \in G$,

$$\{\alpha, \beta, -\beta\}^g = \{-\alpha, \beta, -\beta\}, \quad \{0, \alpha, -\beta\}^g = \{0, -\alpha, \beta\},$$

$$\{0, \alpha, \beta\}^g = \{0, -\alpha, -\beta\}, \quad \{\alpha, -\alpha, \beta\}^g = \{\alpha, -\alpha, -\beta\}$$

and

$$\{0, \alpha, -\alpha\}^u = \{0, \beta, -\beta\},$$

then both $N_1(B)$ and $N_2(B)$ are even which is a contradiction to the fact that $N_1(B) = N_2(B) = 5$. Hence, exactly one of the two elements $\alpha$ and $\beta$ is a square, and we may suppose $\alpha$ is a square and $\beta$ is a nonsquare. Let $v$ be the linear fraction such that $x^v = \alpha^{-1}x$ for any $x \in X$, then $v \in G$. Let

$$C = \{0, \alpha, -\alpha, \beta, -\beta\}^v = \{0, 1, -1, \alpha^{-1}\beta, -\alpha^{-1}\beta\},$$

then

$$B = C^g = \{0, 1, -1, \theta_1, -\theta_1\}^g,$$

where $\theta_1 = \alpha^{-1}\beta$ which is a nonsquare.

We know that there exists a linear fraction $f$ which is of order 5 such that $G_C = \langle f, g \rangle$ and $(0, 0^f, 0^f, 0^f, 0^f)$ is a 5-cycle of $f$. Then there exists a positive integer $k(1 \leq k \leq 4)$ such that $0^{f^k} = 1$, and then $1^{f^{-k}} = 0$, i.e., $1^{g^{f^{-k}}} = 0$. So $(-1)^{f^k} = (-1)^{g^{f^{-k}}} = 0$. From $0^{f^k} = 1$ and $(-1)^{f^k} = 0$, we have $x^{f^k} = \frac{x + 1}{a x + 1}$ for some $a \in F_q$. Then $1^{f^k} = \theta_1$ and $\theta_1^{f^k} = -\theta_1$ or $1^{f^k} = \theta_1^{f^k} = -\theta_1$ or $1^{f^k} = \theta_1^{f^k} = \theta_1$.
Let $\theta = \theta_1$ if $\theta_1^2 - 4\theta_1 - 1 = 0$ and $\theta = -\theta_1$ if $(-\theta_1)^2 - 4(-\theta_1) - 1 = 0$, then
\[ B = C^\theta = \{0, 1, -1, \theta, -\theta\}^G, \]
where $\theta$ is a nonsquare and $\theta^2 - 4\theta - 1 = 0$.

**Case 2.** $q = 5^n$

In this case, $5|\frac{q^2 - 1}{2}$, so $G_B$ is not a Dihedral subgroup of order 10. $G_B$ is not an elementary subgroup or a cyclic subgroup because $|G_B|$ is not a power of 5 and $G_B$ can not contain an element of order larger than 5. By Lemma 3.3, $G_B$ must be the semidirect product of an elementary Abelian group $P = \langle f \rangle$ of order 5 and a cyclic group $H$ of order 2, for each of the rest is a subgroup of order larger than $|G_B|$. Then $B$ consists of a 5-cycle of $f$. Let $x_0 \in X$ be the unique fixed point of $f$ and $g$ be the linear fraction such that $x^g = \frac{1}{x_{20}}$ for any $x \in X$, then $g \in G$ and $x_0^g = \infty$. So $g^{-1}fg$ has a unique fixed point $\infty$. Then there exists an element $\mu \in F_5^*$, such that $x^g = x + \mu$ for any $x \in X$. Because $g^{-1}fg \in G_B$, then $B^g$ consists of a 5-cycle of $g^{-1}fg$ by Lemma 3.3, and then we may suppose
\[ B^g = \{\alpha, \alpha + \mu, \alpha + 2\mu, \alpha + 3\mu, \alpha + 4\mu\} \]
for some $\alpha \in F_5$. Let $g_1$ be the linear fraction such that $x^{g_1} = x - \alpha$ for any $x \in X$, then $g_1 \in G$ and
\[ B^{g_1} = \{0, \mu, 2\mu, 3\mu, 4\mu\}. \]
Let $g_2$ be the linear fraction such that $x^{g_2} = \mu^{-1}x$ if $\mu$ is a square and $x^{g_2} = \gamma \mu^{-1}x$ if $\mu$ is a nonsquare. Then $g_2 \in G$ and
\[ B^{g_1g_2} = \{0, 1, 2, 3, 4\} = F_5 \text{ or } \gamma F_5. \]
Then $B = F_5^\theta$ or $(\gamma F_5)^\theta$. Because $G$ acts block transitively, $n$ is odd and $B = F_5^\theta$ or $(\gamma F_5)^\theta$ by Lemma 3.1. \[ \blacksquare \]

**Corollary 3.4** If $f(x) = x^2 - 4x - 1 \in F_{p^m}[x]$ is a primitive polynomial over $F_{p^m}$ and $\alpha \in F_{p^m}$ is a root of $f(x)$, where $p^{2m} \equiv 1 \pmod{4}$ and $5|\frac{p^{2m} - 1}{2}$, then $(X, \{0, 1, -1, \alpha, -\alpha\}^{PSL(2,p^{2m})})$ is a simple $3-(p^{2m} + 1, 5, 3)$ design.

**Proof.** The conclusion follows from Lemma 3.2 and the fact that $\alpha$ is a nonsquare. \[ \blacksquare \]
Example 3.5 Let $\alpha_1$ be a root of the irreducible polynomial $f(x) = x^2 - x - 1 = x^2 - 4x - 1$ over $F_3$, then $\alpha_1$ is a primitive element of $F_9$, then $(X, \{0, 1, -\alpha_1, -\alpha_1\})^{PSL(2,9)}$ is a simple $3\cdot(10, 5, 3)$ design which is minimal in $\lambda$.

Example 3.6 Let $\alpha_2$ be a root of the irreducible polynomial $f(x) = x^2 - 4x - 1$ over $F_7$, then $(\{0, 1, -\alpha_2, -\alpha_2\})^{PSL(2,49)}$ is not a simple $3\cdot(50, 5, 3)$ design because $\alpha_2$ is a square of $F_{49}$. 
2.) Simple 3-(\(q+1,5,3\)) designs on which the action of \(G\) is not block-transitive

In this section, we will give the necessary and sufficient conditions for the existence of a simple 3-(\(q + 1, 5, 3\)) design on which the action of \(G\) is not block-transitive.

**Theorem 3.7** \((X, B)\) is a simple 3-(\(q + 1, 5, 3\)) design on which the action of \(G\) is not block-transitive if and only if \(q = 5^n\), \(n\) is even, and \(B = F_5^G \cup (\gamma F_5)^G\).

**Proof.** The sufficiency follows from Lemma 3.1. Let us prove the necessity. Suppose \((X, B)\) is a simple 3-(\(q + 1, 5, 3\)) design on which the action of \(G\) is not block-transitive. Then \(B = k \bigcup_{i=1}^k \Gamma_i\) (\(k \geq 2\)), where \(\Gamma_i = B \gamma_i G (i = 1, 2, \cdots, k)\) is an orbit of \(G\) containing \(B_i\). For any \(i(i = 1, 2, \cdots, k)\), all the possible cases for the orbit incidence matrix \(M_i\) of \(\{\Delta_1, \Delta_2\}\) versus \(\{\Gamma_i\}\) are:

\[
\begin{pmatrix}
0 & 1 \\
1 & 0 \\
\end{pmatrix}, \quad \begin{pmatrix}
0 & 2 \\
2 & 0 \\
\end{pmatrix}, \quad \begin{pmatrix}
0 & 3 \\
3 & 0 \\
\end{pmatrix}, \quad \begin{pmatrix}
1 & 0 \\
0 & 1 \\
\end{pmatrix}, \quad \begin{pmatrix}
1 & 2 \\
2 & 1 \\
\end{pmatrix}, \quad \begin{pmatrix}
1 & 3 \\
3 & 1 \\
\end{pmatrix}, \quad \begin{pmatrix}
2 & 0 \\
0 & 2 \\
\end{pmatrix}, \quad \begin{pmatrix}
2 & 1 \\
1 & 2 \\
\end{pmatrix}, \quad \begin{pmatrix}
2 & 2 \\
2 & 2 \\
\end{pmatrix}, \quad \begin{pmatrix}
2 & 3 \\
3 & 2 \\
\end{pmatrix}, \quad \begin{pmatrix}
3 & 0 \\
0 & 3 \\
\end{pmatrix}.
\]

If \(M_i = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\) or \(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\), then \((X, \Gamma_i \cup \gamma \Gamma_i)\) is a 3-(\(q + 1, 5, 1\)) design by Lemma 3.2, or \((X, \Gamma_i)\) is a 3-(\(q + 1, 5, 1\)) design. This is impossible (see[12]). Then \(M_i\) is not \(\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}\) or \(\begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}\) either, otherwise, there must exist another orbit \(\Gamma_j (1 \leq j \leq k)\) such that \(M_j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\) or \(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\). If \(M_i = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\) or \(\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\), then \(\frac{N_1(B_i)}{N_2(B_i)} = \frac{1}{2}\) or \(\frac{2}{7}\). However, there are altogether 10 3-subsets in \(B_i\), then \(3N_1(B_i) = 10\) or \(3N_2(B_i) = 10\), both of which are impossible. Similarly, it is impossible for \(M_i\) to be \(\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\) or \(\begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}\). So \(M_i\) cannot be \(\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}\) or \(\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\), otherwise, there exists another orbit \(\Gamma_j (1 \leq j \leq k)\) such that \(M_j\) is \(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\), \(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\), \(\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\), \(\begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}\).

Hence \(M_i = \begin{pmatrix} 0 & 3 \\ 3 & 0 \end{pmatrix}\) or \(\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}\), then \(k = 2\) and \(B = \Gamma_1 \cup \Gamma_2\), where
\[ M_1 = \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}. \]

By Lemma ??, we know that \(|G_{B_i}| = 20(i = 1, 2)|. By Lemma ??, \(G_{B_i}\) cannot contain an element of order larger than 5, so \(G_{B_i}\) is not a cyclic group or a Dihedral group. And \(G_{B_i}\) is also not an elementary subgroup, for \(|G_{B_i}|\) is not a power of some prime. By Lemma ??, we know that \(G_{B_i}\) is the semidirect product of an elementary Abelian group \(P\) of order 5 and a cyclic group \(H\) of order 4, for the rest are of order not equal to 20. Therefore \(q = 5^n\) and \(q \equiv 1(\mod 8)\), i.e., \(n\) is even.

Let \(f\) be the linear fraction such that \(xf = \overline{2}x = 2x\) for any \(x \in X\), then \(f\) is of order 4 and \(f \in G\) by Lemma ??, and so
\[
\Gamma_i = B_i^G = \{0, 2\alpha, 4\alpha, 3\alpha\}^G = \{0, \alpha, 2\alpha, 3\alpha, 4\alpha\}\] for some \(\alpha \in F_5^*\) by Lemma ??, because
\[
\{\infty, \alpha, 2\alpha, 3\alpha, 4\alpha\}^g = \{0, \alpha^{-1}, 2\alpha^{-1}, 3\alpha^{-1}, 4\alpha^{-1}\},
\]
where \(x^r = \frac{1}{x}\) for any \(x \in X\), then we may suppose
\[
\Gamma_i = \{0, \beta, 2\beta, 3\beta, 4\beta\}^G,
\]
for some \(\beta \in F_5^*\). If \(\beta\) is a square, \(\Gamma_i = \{0, 1, 2, 3, 4\}^G = F_5^G\), and if \(\beta\) is a nonsquare, \(\Gamma_i = \{0, \gamma, 2\gamma, 3\gamma, 4\gamma\}^G = (\gamma F_5)^G\). So \(\Gamma_1 = (\gamma F_5)^G\) and \(\Gamma_2 = F_5^G\). 

References

[1] N. Balachandran and D. Ray-Chaudhuri, Simple 3-designs and PSL(2, q) with \(q \equiv 1(\mod 4)\), Des. Codes Cryptogr. 44(2007), 263-274.


[9] S. Iwasaki, Infinite families of 2- and 3-designs with parameters $v = p + 1, k = (p - 1)/2^e + 1$, where $p$ odd prime, $2^e | (p - 1), e \geq 2, 1 \leq i \leq e$, J. Combin. Des., 5(1997), 95-110.


[11] W. Li, On the existence of simple 3-(30,7,15) and 3-(26,12,55) designs, Ars. Combin., 95(2010), 531-536