Large sets of 3-designs from PSL(2,q), with block sizes 4 and 5.

C.A. Cusack, S.W. Graham* **and D.L. Kreher†**

Department of Mathematical Sciences, Michigan Technological University, Houghton, Michigan, U.S.A. 49931–1295

ABSTRACT

We determine the distribution of 3–$(q+1, k, \lambda)$ designs, with $k \in \{4, 5\}$, among the orbits of k–element subsets under the action of PSL(2,q), for $q \equiv 3 \pmod 4$, on the projective line. As a consequence, we give necessary and sufficient conditions for the existence of a uniformly–PSL(2,q) large set of 3–$(q+1, k, \lambda)$ designs, with $k \in \{4, 5\}$ and $q \equiv 3 \pmod 4$.

1. INTRODUCTION

A 3–(v, k, λ) design is a pair $(X, \mathcal{B})$ in which X is a v–element set of *points* and $\mathcal{B}$ is a collection of k–element subsets of X called *blocks*, such that every 3–element subset of X is contained in precisely λ blocks. It is *simple* if no two blocks are identical. All of the 3-designs in this paper will be simple. A 3–$(v, 4, \lambda)$ design is also said to be a *quadruple system* of *index* λ and *order* v. If every k–element subset of X is chosen to be in $\mathcal{B}$, then $(X, \mathcal{B})$ is a 3–$(v, k, \binom{v-3}{k-3})$ design; and, in this, case it is said to be the *complete design*. A *large set* of 3–(v, k, λ) designs denoted by LS$[N](3, k, v)$, is a partition, $[(X, \mathcal{B}_i)]_{i=1}^{N}$, of the complete design system into N disjoint 3–$(v, k, \binom{v-3}{k-3}/N)$ designs. A subgroup G of Sym(X) (the *full symmetric group* on X) 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 subgroup G is an *automorphism group* of the 3–design $(X, \mathcal{B})$ if for all $g \in G$ and $S \in \mathcal{B}$, $g(S) \in \mathcal{B}$. If $S \subseteq X$, the orbit of S is $G(S) = \{g(S) : g \in G\}$, and the stabilizer of S is $G_S = \{g \in G : g(S) = S\}$. It is well known that $|G(S)| \cdot |G_S| = |G|$. 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–element subsets of X under G. If every 3–(v, k, λ) design in the large set $[(X, \mathcal{B}_i)]_{i=1}^{N}$ has the group G as an automorphism

*Research supported by National Security Agency grant MDA904–90–H–1026.

†Research supported by National Security Agency grant MDA904–92–H–3036.

group, we say that it is a *uniformly–G* $LS[N](3,k,v)$ or a G–uniform LS$[N](3,k,v)$. For example a uniformly–cyclic $LS[5](3,4,13)$ can be found in [4].

For the entirety of this paper, p is a prime and $q = p^e$ is a prime power congruent to 3 (mod 4). Also we set $X = \mathrm{GF}(q) \cup \{\infty\}$. Then a function of the form

$$x \mapsto \frac{ax+b}{cx+d}, \text{ where } a,b,c,d \in \mathrm{GF}(q)$$

and in which we define $1/0 = \infty$, $1/\infty = 0$, $1-\infty = \infty - 1 = \infty$, and $\infty/\infty = 1$, is called a *linear fractional transformation.* The determinant of f is $\det f = ad - bc$. The set of all linear fractional transformations whose determinant is a nonzero square is a group G of order $(q^3-q)/2$ which is 3-homogeneous on X. It is called the *linear fractional* group and is isomorphic to PSL(2,q). The fact that G is 3-homogeneous implies:

(i) $G(\{0,1,\infty\}) = \binom{X}{3}$. Hence $|G_{\{0,1,\infty\}}| = |G|/\ |\binom{X}{3}| = 3$ and thus

$$G_{\{0,1,\infty\}} = \{x \mapsto x, x \mapsto (x-1)/x, x \mapsto -1/(x-1)\}.$$

(ii) Every orbit of k–element subsets of X is a 3–$(q+1,k,\lambda)$ design for some λ.

The subgroup structure of PSL(2,q) is known [3] and in particular the permutation character χ for this action of G on X is given in Table I, where $\phi(x)$ denotes Euler's totient.

Table I. The permutation character χ of PSL$(2,q)$ on GF$(q) \cup \{\infty\}$, where $q \equiv 3$ (mod 4).

order of g	1	p	2	$d\mid\frac{q-1}{2}$	$d\mid\frac{q+1}{2}$, $d \neq 2$
order of the centralizer of g	$(q^3-q)/2$	q	$q+1$	$(q-1)/2$	$(q+1)/2$
number of conjugacy classes	1	2	1	$\phi(d)/2$	$\phi(d)/2$
number of fixed points $\chi(g)$	$q+1$	1	0	2	0

2. BLOCK SIZE 4

In this section we study 3-designs from PSL$(2,q)$ with block size 4. If $\mathcal{O}$ is an orbit of 4–element subsets of X under G, then $\mathcal{O} = G(\{0,1,\infty,\alpha\})$ for some $\alpha \in X - \{0,1,\infty\}$. Furthermore, $\mathcal{O}$ is a 3–$(q+1,4,\lambda)$ design where $\lambda = |\Lambda(\alpha)|$ and $\Lambda(\alpha) = \{\beta : \{0,1,\infty,\beta\} \in \mathcal{O}\}$.

Proposition 1. *Let $\mathcal{O}$ be an orbit of 4–element subsets of X under G, and set $\Lambda(\alpha) = \{\beta : \{0,1,\infty,\beta\} \in \mathcal{O}\}$. Then,*

$$\Lambda(\alpha) = \begin{cases} G_{\{0,1,\infty\}}(\alpha) & \text{if } -\alpha \text{ and } -(1-\alpha) \text{ are both squares;} \\ G_{\{0,1,\infty\}}(\alpha) \cup G_{\{0,1,\infty\}}(\frac{1}{\alpha}) & \text{otherwise.} \end{cases}$$

Proof. Let $\beta \in \Lambda(\alpha)$, then $\{0,1,\infty,\beta\} \in G(\{0,1,\infty,\alpha\})$ and thus there is a $g \in G$ such that $g(\{0,1,\infty,\alpha\}) = \{0,1,\infty,\beta\}$. Let $A,B,C \in \{0,1,\infty,\alpha\}$, be such that $g(\{A,B,C\}) = \{0,1,\infty\}$. Define

$$h(x) = h_{A,B,C}(x) = \frac{(x-A)(B-C)}{(x-C)(B-A)}.$$

Then $h(\{A,B,C\}) = \frac{1}{h}(\{A,B,C\}) = \{0,1,\infty\}$ and $\det h = -\det\frac{1}{h} = (A-C)(B-C)(B-A)$, since -1 is not a square in GF(q). Thus either $h \in G$ or $\frac{1}{h} \in G$. Consequently $g \in G_{\{0,1,\infty\}}h$ if $\det h$ is a square and $g \in G_{\{0,1,\infty\}}\frac{1}{h}$ otherwise. Observe that:

$$G_{\{0,1,\infty\}}h_{A,B,C} = \{h_1,h_2,h_3\} \qquad \text{and} \qquad G_{\{0,1,\infty\}}\frac{1}{h}{}_{A,B,C} = \{\frac{1}{h_1},\frac{1}{h_2},\frac{1}{h_3}\};$$

where

$$\begin{aligned} h_1(x) &= \frac{(x-A)(B-C)}{(x-C)(B-A)}, \\ h_2(x) &= \frac{(x-B)(C-A)}{(x-A)(C-B)}, \text{ and} \\ h_3(x) &= \frac{(x-C)(A-B)}{(x-B)(A-C)}. \end{aligned}$$

Thus for each arrangement A,B,C,D of $0,1,\infty,\alpha$, either $h_i(D) \in \Lambda(\alpha)$ for $i = 1,2,3$ if $\det h$ is a square, or $\frac{1}{h_i}(D) \in \Lambda(\alpha)$ for $i = 1,2,3$ if $\det h$ is a non–square. We also observe that cyclically permuting A, B, and C, in effect permutes cyclically h_1, h_2, and h_3. Hence only eight of the twenty-four possible arrangements need be examined. They are given in Table II. Moreover,

$$\begin{aligned} G_{\{0,1,\infty\}}(\alpha) &= \{\alpha, \frac{\alpha-1}{\alpha}, \frac{1}{1-\alpha}\} \text{ and} \\ G_{\{0,1,\infty\}}(\frac{1}{\alpha}) &= \{\frac{1}{\alpha}, 1-\alpha, \frac{\alpha}{\alpha-1}\}. \end{aligned}$$

We conclude that $\Lambda(\alpha) = G_{\{0,1,\infty\}}(\alpha)$ if $-\alpha$ and $-(1-\alpha)$ are both squares, and that

$\Lambda(\alpha) = G_{\{0,1,\infty\}}(\alpha) \cup G_{\{0,1,\infty\}}(\frac{1}{\alpha})$ otherwise. □

Table II.

A	B	C	D	$h_1(D)$	$h_2(D)$	$h_3(D)$	$\det h = (A-C)(B-C)(B-A)$
0	1	∞	α	α	$\frac{\alpha-1}{\alpha}$	$\frac{1}{1-\alpha}$	1
1	∞	α	0	$\frac{1}{\alpha}$	$1-\alpha$	$\frac{\alpha}{\alpha-1}$	$1-\alpha$
∞	α	0	1	α	$\frac{\alpha-1}{\alpha}$	$\frac{1}{1-\alpha}$	$-\alpha$
α	0	1	∞	$\frac{1}{\alpha}$	$1-\alpha$	$\frac{\alpha}{\alpha-1}$	$-\alpha(1-\alpha)$
1	0	∞	α	$1-\alpha$	$\frac{\alpha}{\alpha-1}$	$\frac{1}{\alpha}$	-1
∞	1	α	0	$\frac{\alpha-1}{\alpha}$	$\frac{1}{1-\alpha}$	α	$-(1-\alpha)$
α	∞	0	1	$1-\alpha$	$\frac{\alpha}{\alpha-1}$	$\frac{1}{\alpha}$	α
0	α	1	∞	$\frac{\alpha-1}{\alpha}$	$\frac{1}{1-\alpha}$	α	$\alpha(1-\alpha)$

Proposition 2. *Let $\alpha \in X - \{0,1,\infty\}$. Then*

$$G_{\{0,1,\infty\}}(\alpha) = G_{\{0,1,\infty\}}(\frac{1}{\alpha}) \Leftrightarrow G_{\{0,1,\infty\}}(\alpha) = \{2, 2^{-1}, -1\}.$$

Proof. If $G_{\{0,1,\infty\}}(\alpha) = G_{\{0,1,\infty\}}(\frac{1}{\alpha})$, then $\alpha = \frac{1}{\alpha}$, $\frac{\alpha}{\alpha-1}$ or $1-\alpha$ and so $\alpha = 2$, 2^{-1} or -1 respectively. On the other hand $G_{\{0,1,\infty\}}(2) = G_{\{0,1,\infty\}}(2^{-1}) = G_{\{0,1,\infty\}}(-1) = \{2, 2^{-1}, -1\}$. □

Proposition 3. *Let $\alpha \in X - \{0,1,\infty\}$. Then*

(i) $|G_{\{0,1,\infty\}}(\alpha)| = |G_{\{0,1,\infty\}}(\frac{1}{\alpha})| = 1$ *or* 3.

(ii) $|G_{\{0,1,\infty\}}(\alpha)| = 1$ *if and only if*
$$\begin{cases} q \equiv 3 \ (mod\ 12) \text{ and } \alpha = -1 \\ \text{or} \\ q \equiv 7 \ (mod\ 12) \text{ and } \alpha = \dfrac{1 \pm \sqrt{-3}}{2}. \end{cases}$$

Proof. The map $x \mapsto \frac{1}{x}$ shows that $|G_{\{0,1,\infty\}}(\alpha)| = |G_{\{0,1,\infty\}}(\frac{1}{\alpha})|$. Also $|G_{\{0,1,\infty\}}| = 3$ so $|G_{\{0,1,\infty\}}(\alpha)| = 1$ or 3. If $|G_{\{0,1,\infty\}}(\alpha)| = 1$, then $\alpha = (\alpha-1)/\alpha = 1/(1-\alpha)$. Hence $\alpha^2 - \alpha + 1 = 0$ and so $\alpha = 2^{-1}(1 \pm \sqrt{-3})$. Consequently, either -3 is a non–zero square in GF(q) or $q = 3^n$. The latter case gives $\alpha = -1$ and so $G_{\{0,1,\infty\}}(\alpha) = G_{\{0,1,\infty\}}(\frac{1}{\alpha}) = \{-1\}$. Furthermore, $q \equiv 0 \pmod 3$ and $q \equiv 3 \pmod 4$ yield $q \equiv 3 \pmod{12}$. If -3 is a non–zero

square in GF(q), where $q = p^e$ for some odd prime p, then we claim that $p \equiv 1 \pmod 3$. If $p \equiv 2 \pmod 3$, then the Legendre symbol $\left(\frac{-3}{p}\right) = \left(\frac{p}{-3}\right)(-1)^{\frac{p-1}{2}\cdot\frac{-3-1}{2}} = -1$. Therefore, -3 is a not a square modulo p and so x^2+3 is irreducible over $\mathbb{Z}_p$. Thus GF(q), where $q = p^e$ has a subfield F isomorphic to $\mathbb{Z}_p[x]/(x^2+3)$. Therefore e must be even and thus $q \equiv 1 \pmod 4$, contrary to the assumption that $q \equiv 3 \pmod 4$. If $p \equiv 1 \pmod 3$, then $q \equiv 1 \pmod 3$. Hence $q \equiv 7 \pmod{12}$, since $q \equiv 3 \pmod 4$. □

Proposition 4. *Let $\alpha \in X - \{0, 1, \infty\}$. Then $|\Lambda(\alpha)| = 1, 3,$ or 6.*

Proof. Propositions 1, 2, and 3 imply that $|\Lambda(\alpha)| = 1$, 2, 3 or 6. Hence, we need only eliminate the possibility that $|\Lambda(\alpha)| = 2$.

Suppose $|\Lambda(\alpha)| = 2$. Then $-\alpha$ or $-(1-\alpha)$ is a non–square, $q \equiv 7 \pmod{12}$ and $\alpha = (1 \pm \sqrt{-3})/2$. Without loss, $\alpha = (1+\sqrt{-3})/2$ and $1-\alpha = (1-\sqrt{-3})/2$. Observe that $-\alpha = (-1-\sqrt{-3})/2$ is a cube root of 1, so $\alpha^3 = -1$. Thus if $-\alpha$ is a non–square so $\alpha = u^2$ for some u. Consequently the multiplicative order of u is 12. Thus $12|(q-1)$, hence $q \equiv 1 \pmod{12}$ — a contradiction. A contradiction is similarly obtained if $-(1-\alpha)$ is a non–zero square. □

Theorem 1. *The number of orbits of 4–element subset of X under the action of G when $q \equiv 3 \pmod 4$ is*

$$\begin{array}{ll}
\dfrac{5q-7}{24} + \dfrac{2}{3} & \text{if} \quad q \equiv 3 \pmod{24}; \\
\dfrac{5q-7}{24} + \dfrac{11}{6} & \text{if} \quad q \equiv 7 \pmod{24}; \\
\dfrac{5q-7}{24} & \text{if} \quad q \equiv 11 \pmod{24}; \\
\dfrac{5q-7}{24} + \dfrac{4}{3} & \text{if} \quad q \equiv 19 \pmod{24}; \ \text{and} \\
\dfrac{5q-7}{24} + \dfrac{1}{2} & \text{if} \quad q \equiv 23 \pmod{24};
\end{array}$$

Proof. The group G as noted earlier is isomorphic to PSL(2,q), $q \equiv 3 \pmod 4$. Each element $g \in G$ consists of $\chi(g)$ fixed points and $(q+1-\chi(g))/d$ cycles of length $d = |g|$. Let Fix(g) be the number of 4–element subsets of X fixed by $g \in G$. Then by the Cauchy–Frobenius Theorem, the number of orbits of 4–element subsets of X under the action of G is:

$$N = \frac{1}{|G|} \sum_{g \in G} \text{Fix}(g).$$

But only elements of orders 1, 2, 3, or 4 in G can fix a 4–element subset, since $\chi(g) \leq 2$ for all $g \in G$. Thus,

$$N = \frac{1}{|G|}\left[\binom{q+1}{4} + \binom{(q+1)/2}{2}\frac{|G|}{q+1}\right] + m,$$

where

$$m = \frac{1}{|G|} \sum \{\text{Fix}(g) : g \in G \text{ and } |g| = 3 \text{ or } 4\}.$$

Simplifying, we get:

$$N = \frac{5q-7}{24} + m.$$

From Table I we see that G has elements of order 3 if and only if 3 divides q, $\frac{q-1}{2}$ or $\frac{q+1}{2}$, that is $q \equiv 0, 1, 3, 5 \pmod 6$. Also, since $q \equiv 3 \pmod 4$, 4 does not divide $(q-1)/2$ so that G has elements of order 4 if and only if 4 divides $(q+1)/2$, that is $q \equiv -1 \pmod 8$.

The value of m is now easily calculated.

(i) If $q \equiv 0 \pmod 3$, elements of order three fix one point, and thus they fix $q/3$ four–element subsets. They therefore contribute

$$\frac{1}{|G|}\left(\frac{2|G|}{q}\frac{q}{3}\right) = \frac{2}{3} \text{ to } m.$$

(ii) If $q \equiv 1 \pmod 6$, G has $2|G|/(q-1)$ elements of order 3. Each fixes 2 points and has $(q-1)/3$ 3–cycles. Thus, they contribute

$$\frac{1}{|G|}\left(\frac{2|G|}{(q-1)}\frac{2(q-1)}{3}\right) = \frac{4}{3} \text{ to } m.$$

(iii) If $q \equiv -1 \pmod 6$, elements of order 3 have no fixed points and thus fix no 4–element subsets.

(iv) If $q \equiv -1 \pmod 8$, G has $2|G|/(q+1)$ elements of order 4. Each has $(q+1)/4$ 4–cycles and no fixed points. They contribute

$$\frac{1}{|G|}\left(\frac{2|G|}{(q+1)}\frac{(q+1)}{4}\right) = \frac{1}{2} \text{ to } m.$$

$$\text{Hence, } m = \begin{cases} \frac{2}{3} & \text{if} \quad q \equiv 3 \pmod{24}; \\ \frac{11}{6} & \text{if} \quad q \equiv 7 \pmod{24}; \\ 0 & \text{if} \quad q \equiv 11 \pmod{24}; \\ \frac{4}{3} & \text{if} \quad q \equiv 19 \pmod{24}; \text{ and} \\ \frac{1}{2} & \text{if} \quad q \equiv 23 \pmod{24}. \end{cases}$$

□

Let N_i be the number of orbits $G(\{0, 1, \infty, \alpha\})$ with $\lambda(\alpha) = i$. Then by Proposition 3, $N_i = 0$ unless $i = 1$, 3, or 6. Then, counting the number of 4–element subsets of X that contain $\{0, 1, \infty\}$ (or any given 4–element set), we see that

$$N_1 + 3N_3 + 6N_6 = q - 2.$$

Furthermore, by Theorem 1 we have:

$$N_1 + N_3 + N_6 = \begin{cases} \frac{5q-7}{24} + \frac{2}{3} & \text{if} \quad q \equiv 3 \pmod{24}; \\ \frac{5q-7}{24} + \frac{11}{6} & \text{if} \quad q \equiv 7 \pmod{24}; \\ \frac{5q-7}{24} & \text{if} \quad q \equiv 11 \pmod{24}; \\ \frac{5q-7}{24} + \frac{4}{3} & \text{if} \quad q \equiv 19 \pmod{24}; \text{ and} \\ \frac{5q-7}{24} + \frac{1}{2} & \text{if} \quad q \equiv 23 \pmod{24}. \end{cases}$$

Lastly, by Proposition 3 we know that

$$N_1 = \begin{cases} 2 & \text{if} \quad q \equiv 7, 19 \pmod{24}; \\ 1 & \text{if} \quad q \equiv 3 \pmod{24}; \text{ and} \\ 0 & \text{if} \quad q \equiv 11, 23 \pmod{24}. \end{cases}$$

It is elementary to solve these equations and the following result is obtained:

Theorem 2. *Let N_λ be the number of orbits of 4–element subsets of X under the action of G that are 3–$(q+1, 4, \lambda)$ designs. Then $\lambda = 1$, 3 or 6 and*

$$(N_1, N_3, N_6) = \begin{cases} (1, \frac{q-3}{12}, \frac{q-3}{8}) & \textit{if} \quad q \equiv 3 \ (\textit{mod } 24); \\ (2, \frac{q+5}{12}, \frac{q-7}{8}) & \textit{if} \quad q \equiv 7 \ (\textit{mod } 24); \\ (0, \frac{q+1}{12}, \frac{q-3}{8}) & \textit{if} \quad q \equiv 11 \ (\textit{mod } 24); \\ (2, \frac{q-7}{12}, \frac{q-3}{8}) & \textit{if} \quad q \equiv 19 \ (\textit{mod } 24); \ \textit{and} \\ (0, \frac{q+13}{12}, \frac{q-7}{8}) & \textit{if} \quad q \equiv 23 \ (\textit{mod } 24). \end{cases}$$

This theorem has the following very interesting consequence.

Theorem 3. *Let q be a prime power congruent to 3 modulo 4 and let $N > 1$ be an integer. There is a uniformly-PSL$(2, q)$ LS$[N](3, 4, q+1)$ if and only if $q \equiv 2 \ (\textit{mod } 3N)$, $q \equiv 11$ or $23 \ (\textit{mod } 24)$ and $N \leq \frac{q-2}{15}$ or $N = 5$ and $q = 47$.*

Proof. Let $[(X, \mathcal{B}_i)]_{i=1}^N$ be a uniformly-PSL$(2, q)$ LS$[N](3, 4, q+1)$. Then each $\mathcal{B}_i$ is a 3–$(q+1, 4, \lambda)$, where $\lambda = (q-2)/N$. Furthermore each $\mathcal{B}_i$ is a union of A_i orbits that are 3–$(q+1, 4, 3)$'s, B_i orbits that are 3–$(q+1, 4, 6)$'s, and C_i orbits that are 3–$(q+1, 4, 1)$'s. Thus, $\lambda = 3A_i + 6B_i + C_i$ for all i. If for some i, $C_i \neq 0$, then from Theorem 2 and $N > 1$ we see that $\lambda \equiv 1 \pmod 3$ and $N = 2$. This is impossible since N divides $q - 2$, which is odd. Thus $C_i = 0$ and $\lambda = 3m$ for some m. Consequently, $N = \frac{q-2}{3m}$ for some m. This proves our assertion that $q \equiv 2 \pmod{3N}$. In particular, $q \equiv 2 \pmod 3$, so we must have $q \equiv 11$ or $23 \pmod{24}$. Suppose $N > \frac{q-2}{15}$, then $m = 1$ or 3. If $m = 1$, then $\lambda = 3$, and so $B_i = 0$ for all i. Theorem 2 shows that this is impossible. If $m = 3$, then $\lambda = 9$, and so for all i, we must have either $(A_i, B_i) = (3, 0)$ or $(A_i, B_i) = (1, 1)$. Thus in particular we have $N_6 \leq N_3$. In the case $q \equiv 11 \pmod{24}$, this says, by Theorem 2, that $\frac{q-3}{8} \leq \frac{q+1}{12}$, which implies $q = 11$. But when $q = 11$, we have $N_3 = N_6 = 1$, and consequently the desired large set does not exist. In the case $q \equiv 23 \pmod{24}$, this says,

by Theorem 2, that $\frac{q-7}{8} \leq \frac{q+13}{12}$, which implies $q = 23$ or $q = 47$. When $q = 23$, we have $N_3 = 3$, $N_6 = 2$, and consequently the desired large set does not exist. If $q = 47$, then $N_3 = N_6 = 5$, and an LS[5](3, 4, 48) is obtained.

Conversely, suppose $q \equiv 2 \pmod{3N}$, $q \equiv 11$ or $23 \pmod{24}$, and $N \leq \frac{q-2}{15}$. First note that from Theorem 2 every orbit of 3-element subsets of PSL$(2, q)$ is either a 3–$(q+1, 4, 3)$ or a 3–$(q+1, 4, 6)$. Thus the designs in a uniformly-PSL$(2, q)$ LS$[N](3, 4, q+1)$ are 3–$(q+1, 4, 3m)$ designs, where $m = \frac{q-2}{3N}$. We will construct an LS$[N](3, 4, q+1)$ in which the i-th design $(X, \mathcal{B}_i)$ uses exactly A_i orbits of PSL(2,q) that are 3–$(q+1, 4, 3)$'s and exactly B_i orbits that are 3–$(q+1, 4, 6)$'s. Write $N_6 = N\ell + r$, where $0 \leq r < N$. Set

$$\begin{aligned} B_1 = B_2 = \cdots = B_r &= \ell + 1; \\ B_{r+1} = B_{r+2} = \cdots = B_N &= \ell; \\ \text{and define } A_i &= \frac{q-2}{3N} - 2B_i \text{ for all } i. \end{aligned}$$

Then it is easy to see that $\sum_{i=1}^{N} B_i = N_6$, $\sum_{i=1}^{N} A_i = N_3$; and $3A_i + 6B_i = \frac{q-2}{N} = 3m$ for all i. Thus, if $A_i \geq 0$ for all $i = 1, 2, \ldots N$, we can arrange the orbits of 4-element subsets under the action of PSL$(2, q)$ into the desired large set. Observe that:

$$A_i = \frac{q-2}{3N} - 2B_i \geq \frac{q-2}{3N} - 2\ell - 2 = m - 2\ell - 2. \qquad (*)$$

Furthermore, using Theorem 2 we see that:

$$\ell = \left\lfloor \frac{N_6}{N} \right\rfloor \leq \left\lfloor \frac{q-3}{8} \frac{3m}{q-2} \right\rfloor \leq \left\lfloor \frac{3m}{8} \right\rfloor \leq \frac{3m}{8}.$$

If $m \geq 9$, then $\ell \leq \frac{3m}{8}$, and the right hand side of $(*)$ shows that $A_i \geq 1$. Now suppose $m < 9$. Then either $m = 5$ or 7, since $N \leq (q-2)/5$, and $q - 2$ is odd. If $m = 5$, then $\ell \leq \lfloor \frac{15}{8} \rfloor = 1$, and $(*)$ shows that $A_i \geq 1$. If $m = 7$, then $\ell \leq \lfloor \frac{21}{8} \rfloor = 2$, and $(*)$ shows that $A_i \geq 1$. □

The reader should observe that Theorem 3 does not settle any new parameter situations for LS$[N](3, 4, v)$s since in [5] Teirlinck established Theorem 4 below. It does say however when an LS$[N](3, 4, v)$ can exist with PSL$(2, q)$ as an automorphism group on each of its designs. We will use Teirlinck theorem in the next section.

Theorem 4. (Teirlinck [5]) *An LS$[N](3, 4, v)$ exists when v and N satisfy:*

$v \equiv 0 \pmod{6}$ *and* $v \equiv 3 \pmod{3N}$; *or*

$v \equiv 3 \pmod{12}$ *and* $v \equiv 3 \pmod{12N}$; *or*

$v \equiv 9 \pmod{12}$ *and* $v \equiv 3 \pmod{6N}$.

3. BLOCK SIZE 5

In this section we will study 3-designs from PSL$(2,q)$ with block size 5. If $\mathcal{O}$ is an orbit of 5–element subsets of X under G, then $\mathcal{O} = G(\{0,1,\infty,\alpha,\beta\})$ for some $\alpha,\beta \in X-\{0,1,\infty\}$. Furthermore $\mathcal{O}$ is a 3–$(q+1,5,\lambda)$ design where $\lambda = |\Lambda(\alpha,\beta)|$ and $\Lambda(\alpha,\beta) = \{\{\gamma,\delta\} : \{0,1,\infty,\gamma,\delta\} \in \mathcal{O}\}$.

Let (A,B,C) be a fixed order of any of the ten 3-element subsets of $\{0,1,\infty,\alpha,\beta\}$, and let $\{D,E\}$ be the remaining two elements. Define

$$h_{A,B,C}(x) = \frac{(x-A)(B-C)}{(x-C)(B-A)}.$$

Then $h_{A,B,C}(\{A,B,C\}) = h_{C,B,A}(\{A,B,C\}) = \{0,1,\infty\}$, and $\det h_{A,B,C} = -\det h_{C,B,A}$. Thus either $h_{A,B,C} \in G$ or $h_{C,B,A} \in G$, since -1 is not a square in $GF(q)$. So, either $G_{\{0,1,\infty\}}h_{A,B,C} \subseteq G$ and $G_{\{0,1,\infty\}}h_{A,B,C}(\{D,E\}) \subseteq \Lambda(\alpha,\beta)$ or $G_{\{0,1,\infty\}}h_{C,B,A} \subseteq G$ and $G_{\{0,1,\infty\}}h_{C,B,A}(\{D,E\}) \subseteq \Lambda(\alpha,\beta)$. Notice that $G_{\{0,1,\infty\}}h_{A,B,C} = \{h_{A,B,C}, h_{B,C,A}, h_{C,A,B}\}$ and $G_{\{0,1,\infty\}}h_{C,B,A} = \{h_{C,B,A}, h_{A,C,B}, h_{B,A,C}\}$.

Now, $\{\gamma,\delta\} \in \Lambda(\alpha,\beta)$ implies that there is a $g \in G$ such that $g\{0,1,\infty,\alpha,\beta\} = \{0,1,\infty,\gamma,\delta\}$. In particular,

$$g\{A,B,C\} = \{0,1,\infty\} \text{ for some } \{A,B,C\} \in \{0,1,\infty,\alpha,\beta\}.$$

So either $g \in G_{\{0,1,\infty\}}h_{A,B,C}$ if $h_{A,B,C} \in G$ since $gh^{-1}_{A,B,C} \in G_{\{0,1,\infty\}}$, or $g \in G_{\{0,1,\infty\}}h_{C,B,A}$ if $h_{C,B,A} \in G$ since $gh^{-1}_{C,B,A} \in G_{\{0,1,\infty\}}$. These observations yield the following:

Proposition 5. *$\Lambda(\alpha,\beta)$ is the union of $G_{\{0,1,\infty\}}h_{A,B,C}\{D,E\}$ for some order (A,B,C) of each of the ten 3-element subsets of $\{0,1,\infty,\alpha,\beta\}$, with $\{D,E\}$ the remaining two elements.*

Proposition 6. *Elements of order $2n$ in G cannot fix a 5-element set.*

Proof. Let $g \in G$ be an element of order $2n$. If g fixes a 5-element set, then so must g^n, which has order 2, and thus $\chi(g^n) = 0$. But it is impossible for an element of order 2 to fix a 5-element set without fixing a point. □

Proposition 7. *Let $B \subseteq X$, $|B| = 5$, and let $\mathcal{B}$ be the $3-(q+1,5,\lambda)$ design $G(B)$, then $\lambda = \frac{30}{|G_B|}$.*

Proof. First observe that $|G(B)| = [G : G_B] = |G|/|G_B| = (q+1)q(q-1)/2|G_B|$. We also know that $\mathcal{B} = G(B)$ is a $3-(q+1,5,\lambda)$ design, so $|G(B)| = \frac{(q+1)q(q-1)}{5\cdot 4\cdot 3}\lambda$. Solving these two equations for λ, we get the desired result. □

Proposition 8. *Let $B \subseteq X$, $|B| = 5$, and let $\mathcal{B}$ be the $3-(q+1,5,\lambda)$ design $G(B)$,*

then 2 divides λ.

Proof. Assume 2 does not divide λ, then by Proposition 7, 2 divides $|G_B|$. But this implies that there is an element of order 2 that fixes a 5-element set, contradicting Proposition 6. □

Proposition 9. *Let $B \subseteq X$, $|B| = 5$, and let $\mathcal{B}$ be the $3-(q+1,5,\lambda)$ design $G(B)$, then $\lambda = 6, 10,$ or 30.*

Proof. Proposition 7 implies that $\lambda = 1$, 2, 3, 5, 6, 10, 15 or 30, but Proposition 8 reduces this list to $\lambda = 2$, 6, 10, or 30. So we need only rule out $\lambda = 2$. If $\lambda = 2$, then Proposition 7 implies that $|G_B| = 15$. The only group of order 15 is cyclic, which implies that a permutation of order 15 fixes the 5-element set B. Permutations of this type have either zero or two fixed points, so they can't fix a 5-element set. Thus $\lambda \neq 2$. □

Proposition 10. *Let $\alpha, \beta \in X - \{0, 1, \infty\}$, $\alpha \neq \beta$. Then*

$$\left|G_{\{0,1,\infty\}}(\alpha,\beta)\right| = \begin{cases} 1 & \text{iff } q \equiv 7 \bmod 12, \alpha = \frac{1\pm\sqrt{-3}}{2}, \text{ and } \beta = \frac{1\mp\sqrt{-3}}{2} \\ 3 & \text{otherwise} \end{cases}$$

Proof. Since $|G_{\{0,1,\infty\}}| = 3$, either $|G_{\{0,1,\infty\}}(\alpha,\beta)| = 1$ or 3.
If $|G_{\{0,1,\infty\}}(\alpha,\beta)| = 1$, then

$$\{\alpha,\beta\} = \{\frac{\alpha-1}{\alpha}, \frac{\beta-1}{\beta}\} = \{\frac{1}{1-\alpha}, \frac{1}{1-\beta}\}$$

This implies that $\alpha^2 - \alpha + 1 = 0$ and $\beta^2 - \beta + 1 = 0$, so that $\alpha = \frac{1\pm\sqrt{-3}}{2}, \beta = \frac{1\mp\sqrt{-3}}{2}$, and either -3 is a non–zero square in GF(q) or $q = 3^n$. The latter case gives $\alpha = \beta = -1$, But $\alpha \neq \beta$, so $q \neq 3^n$. If -3 is a non–zero square in GF(q), where $q = p^e$ for some odd prime p, then we claim that $p \equiv 1 \pmod 3$. If $p \equiv 2 \pmod 3$, then, by Gauss' reciprocity, the Legendre symbol

$$(\frac{-3}{p}) = (\frac{p}{-3})(-1)^{\frac{p-1}{2}\cdot\frac{-3-1}{2}} = -1.$$

Therefore, -3 is not a square modulo p, and so $x^2 + 3$ is irreducible over $\mathbb{Z}_p$. Thus GF(q) has a subfield F isomorphic to $\mathbb{Z}_p[x]/(x^2+3)$, e must be even, and $q \equiv 1 \pmod 4$, contradicting our assumption that $q \equiv 3 \pmod 4$. If $p \equiv 1 \pmod 3$, then $q \equiv 1 \pmod 3$. Thus $q \equiv 3 \pmod 4$ implies that $q \equiv 7 \pmod{12}$. □

Corollary 1. *Let $\{A, B, C, D, E\} = \{0, 1, \infty, \alpha, \beta\}$, $\alpha, \beta \in X - \{0, 1, \infty\}$, $\alpha \neq \beta$. Then*

$$\left|G_{\{0,1,\infty\}} h_{A,B,C}\{D,E\}\right| = \begin{cases} 1 & \text{iff } q \equiv 7 \bmod 12, D = h^{-1}_{A,B,C}(\frac{1\pm\sqrt{-3}}{2}), \\ & \text{and } E = h^{-1}_{A,B,C}(\frac{1\mp\sqrt{-3}}{2}) \\ 3 & \text{otherwise} \end{cases}$$

Proof. By Proposition 10,

$$\left|G_{\{0,1,\infty\}}h_{A,B,C}\{D,E\}\right| = \left|G_{\{0,1,\infty\}}\left\{(h_{A,B,C}(D), h_{A,B,C}(E)\right\}\right| = 1$$

if and only if $q \equiv 7 \pmod{12}$, $h_{A,B,C}(D) = \frac{1\pm\sqrt{-3}}{2}$, and $h_{A,B,C}(E) = \frac{1\mp\sqrt{-3}}{2}$. But the last two conditions happen if and only if $D = h^{-1}_{A,B,C}(\frac{1\pm\sqrt{-3}}{2})$ and $E = h^{-1}_{A,B,C}(\frac{1\mp\sqrt{-3}}{2})$ □

Let N_i be the number of orbits $G(\{0,1,\infty,\alpha,\beta\})$ with $|\Lambda(\alpha,\beta)| = i$. Then by Proposition 9, $N_i = 0$ unless $i = 6$, 10 or 30.

Proposition 11. *The number of orbits of 5–element subsets of X under G that are 3–$(q+1,5,10)$ designs is*

$$N_{10} = \begin{cases} 1 & \text{if } q \equiv 7 \ (mod\ 12) \\ 0 & \text{otherwise} \end{cases}$$

Proof. By Corollary 1, $\left|G_{\{0,1,\infty\}}h_{A,B,C}\{D,E\}\right| = 1$ if and only if $q \equiv 7 \pmod{12}$, $D = h^{-1}_{A,B,C}(\frac{1\pm\sqrt{-3}}{2})$ and $E = h^{-1}_{A,B,C}(\frac{1\mp\sqrt{-3}}{2})$ In this case, we see by Proposition 5 that $\lambda = |\Lambda(\alpha,\beta)| = 1 + 3n$, for some $0 < n < 10$. Then by Proposition 9, $\lambda = 10$. If $q \not\equiv 7 \pmod{12}$, then $\lambda = 3n$ for some $0 < n \leq 10$, so, in particular, $\lambda \neq 10$. □

Theorem 5. *The number of orbits of 5–element subsets of X under the action of G when $q \equiv 3 \ (mod\ 4)$ is:*

$$\begin{aligned}
&\frac{(q-2)(q-3)}{60} && \text{if} \quad q \equiv 3, 23, 27, \ \text{or } 47 \ (mod\ 60); \\
&\frac{(q-2)(q-3)}{60} + \frac{2}{3} && \text{if} \quad q \equiv 7, \ \text{or } 43 \ (mod\ 60); \\
&\frac{(q-2)(q-3)}{60} + \frac{4}{5} && \text{if} \quad q \equiv 11, \ \text{or } 59 \ (mod\ 60); \\
&\frac{(q-2)(q-3)}{60} + \frac{22}{15} && \text{if} \quad q \equiv 19, \ \text{or } 31 \ (mod\ 60);
\end{aligned}$$

Proof. Each element $g \in G$ consists of $\chi(g)$ fixed points and $(q+1-\chi(g))/d$ cycles of length $d = |g|$. Let $\mathrm{Fix}(g)$ be the number of 5–element subsets of X fixed by $g \in G$. Then by the Cauchy–Frobenius Theorem we have that the number of orbits of 5–element subsets of X under the action of G is:

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

Only elements of orders 1, 3, or 5 in G can fix a 5–element subset since by Proposition 6 elements of order $2n$ do not fix 5–element sets. Thus

$$N = \frac{1}{|G|}\left[\binom{q+1}{5}\right] + m = \frac{(q-2)(q-3)}{60} + m,$$

where

$$m = \frac{1}{|G|}\sum\{\mathrm{Fix}(g) : g \in G, |g| = 3 \text{ or } 5\}.$$

From Table I we see that G has elements of order 3 if and only if 3 divides q, $\frac{q-1}{2}$ or $\frac{q+1}{2}$, that is $q \equiv 0, 1, 3, 5 \pmod 6$. Also, since $q \equiv 3 \pmod 4$, 5 does not divide q so that G has elements of order 5 if and only if 5 divides $(q-1)/2$ or $(q+1)/2$, that is $q \equiv 1, 9 \pmod{10}$.

The value of m is now easily calculated:

(i) If $q \equiv 0 \pmod 3$, an element of order 3 has one fixed point and thus fixes no 5–element subsets.

(ii) If $q \equiv 5 \pmod 6$, an element of order 3 has no fixed points and thus fixes no 5–element subsets.

(iii) If $q \equiv 1 \pmod 6$, elements of order 3 fix two points, and thus they fix $(q-1)/3$ 5–element subsets. There are $2|G|/(q-1)$ such elements, so they contribute

$$\frac{1}{|G|}\left(\frac{2|G|}{(q-1)}\frac{(q-1)}{3}\right) = \frac{2}{3} \text{ to } m.$$

(iv) If $q \equiv 1 \pmod{10}$, elements of order 5 fix two points, and thus they fix $(q-1)/5$ 5–element subsets. There are $4|G|/(q-1)$ such elements, so they contribute

$$\frac{1}{|G|}\left(\frac{4|G|}{(q-1)}\frac{(q-1)}{5}\right) = \frac{4}{5} \text{ to } m.$$

(v) If $q \equiv 9 \pmod{10}$, elements of order 5 fix no points, and thus they fix $(q+1)/5$ 5–element subsets. There are $4|G|/(q+1)$ such elements, so they contribute

$$\frac{1}{|G|}\left(\frac{4|G|}{(q+1)}\frac{(q+1)}{5}\right) = \frac{4}{5} \text{ to } m.$$

$$\text{Hence, } m = \begin{cases} 0 & \text{if} \quad q \equiv 3, 23, 27, \text{ or } 47 \pmod{60}; \\ \frac{2}{3} & \text{if} \quad q \equiv 7, \text{ or } 43 \pmod{60}; \\ \frac{4}{5} & \text{if} \quad q \equiv 11, \text{ or } 59 \pmod{60}; \\ \frac{22}{15} & \text{if} \quad q \equiv 19, \text{ or } 31 \pmod{60}; \end{cases}$$

□

Now, counting the number of 5–element subsets of X that contain $\{0, 1, \infty\}$ (or any given 3–element set) we see that

$$6N_6 + 10N_{10} + 30N_{30} = \binom{q-2}{2}.$$

Furthermore by Theorem 5 we have:

$$N_6 + N_{10} + N_{30} = \begin{cases} \frac{(q-2)(q-3)}{60} & \text{if} \quad q \equiv 3, 23, 27, \text{ or } 47 \pmod{60}; \\ \frac{(q-2)(q-3)}{60} + \frac{2}{3} & \text{if} \quad q \equiv 7, \text{ or } 43 \pmod{60}; \\ \frac{(q-2)(q-3)}{60} + \frac{4}{5} & \text{if} \quad q \equiv 11, \text{ or } 59 \pmod{60}; \\ \frac{(q-2)(q-3)}{60} + \frac{22}{15} & \text{if} \quad q \equiv 19, \text{ or } 31 \pmod{60}; \end{cases}$$

Lastly, by Proposition 11 we know that

$$N_{10} = \begin{cases} 1 \text{ if } q \equiv 7 \pmod{12} \\ 0 \text{ otherwise} \end{cases}$$

It is elementary to solve these equations and the following result is obtained:

Theorem 6. *Let N_λ be the number of orbits of 5–element subsets of X under the action of G that are 3–$(q+1, 5, \lambda)$ designs. Then $\lambda = 6$, 10 or 30 and*

$$(N_6, N_{10}, N_{30}) = \begin{cases} (0, 0, \frac{q^2-5q+6}{60}) & \text{if} \quad q \equiv 3, 23, 27, \text{ or } 47 \ (\text{mod } 60); \\ (0, 1, \frac{q^2-5q-14}{60}) & \text{if} \quad q \equiv 7, \text{ or } 43 \ (\text{mod } 60); \\ (1, 0, \frac{q^2-5q-6}{60}) & \text{if} \quad q \equiv 11, \text{ or } 59 \ (\text{mod } 60); \\ (1, 1, \frac{q^2-5q-26}{60}) & \text{if} \quad q \equiv 19, \text{ or } 31 \ (\text{mod } 60). \end{cases}$$

This theorem has the following consequence.

Theorem 7. *Let $q > 3$ be a prime power congruent to 3 modulo 4 and let $N > 1$ be a integer. There is a uniformly-PSL$(2, q)$ LS$[N](3, 5, q+1)$ if and only if $q \equiv 3, 23, 27,$ or $47 \ (\text{mod } 60)$ and N divides $(q-2)(q-3)/60$.*

Proof. Let $[(X, \mathcal{B}_i)]_{i=1}^N$ be a uniformly-PSL$(2, q)$ LS$[N](3, 5, q+1)$. Then each $\mathcal{B}_i$ is a $3-(q+1, 5, \lambda)$, where $\lambda = (q-2)(q-3)/2N$. Furthermore each $\mathcal{B}_i$ is a union of A_i orbits that are $3-(q+1, 5, 6)$ designs, B_i orbits that are $3-(q+1, 5, 10)$ designs and C_i orbits that are $3-(q+1, 5, 30)$ designs. Thus, $\lambda = 6A_i + 10B_i + 30C_i$, for all i. We see from Theorem 6 that if for some i, $B_i \neq 0$, then $B_i = 1$, and $B_i = 0$ for all other i. But $B_i = 1$ implies that $\lambda \equiv 1 \pmod 3$, and $B_i = 0$ implies that $\lambda \equiv 0 \pmod 3$. So $B_i = 0$. Also, if for some i, $A_i \neq 0$, then $A_i = 1$, and $A_i = 0$ for all other i. But $A_i = 1$ implies that $\lambda \equiv 6 \pmod{10}$, and $A_i = 0$ implies that $\lambda \equiv 0 \pmod{10}$. So $A_i = 0$. Thus $\lambda = 30m$, for

some m, and $q \equiv 3, 23, 27$ or $47 \pmod{60}$ In this case, $30m = (q-2)(q-3)/2N$ implies that N divides $(q-2)(q-3)/60$.

Conversely, let $q \equiv 3, 23, 27$ or $47 \pmod{60}$, and $N|(q-2)(q-3)/60$. By Theorem 5, every orbit of 5–element subsets of PSL$(2,q)$ is a $3-(q+1,5,30)$ design, and there are $N_{30} = (q-2)(q-3)/60$ of them. Let $N = (q-2)(q-3)/60m$. Then $Nm = N_{30}$, and taking m of these orbits at a time, a uniformly-PSL$(2,q)$ LS$[N](3,5,q+1)$ is constructed. □

The existence of a uniformly-PSL$(2,q)$ LS$[(q-1)(q-3)/60](3,5,q+1)$, $q \equiv 3 \pmod{4}$, was established in [1], but stated incorrectly.

For given positive integers $t < K$ and N let LS$[N](t,k)$ denote the set of all v such that there exist an LS$[N](t,k,v)$. In [6] the following result is given .

Theorem 8. (Qiu-rong Wu [6]) *If* $v, w, \in LS[N](t-1,t+1)$ *and* $v-1, w-1, \in LS[N](t-1,t)$, *then* $v+w-t \in LS[N](t-1,t+1)$.

Corollary 2. *If* $v_1, v_2, \ldots, v_x \in LS[N](t-1,t+1)$ *and* $v_1-1, v_2-1, \ldots, v_x-1 \in LS[N](t-1,t)$, *then* $t - tx + \sum_{i=1}^{x} v_i \in LS[N](t-1,t+1)$.

Proof. Recursively apply Theorem 8. □

We use this to establish our next theorem.

Theorem 9. *For all nonnegative integers* $R, S, n_1, n_2, \ldots, n_R$

(i) $4-3R+\sum_{j=1}^{R} 3^{4n_j+1} \in LS[N](3,5)$ *for all* N *dividing* $\gcd\{(3^{4n_j+1}-3)/60 : 1 \le j \le R\}$,

(ii) $4-3R+\sum_{j=1}^{R} 3^{4n_j+3} \in LS[N](3,5)$ *for all* N *dividing* $\gcd\{(3^{4n_j+3}-3)/12 : 1 \le j \le R\}$, *and*

(iii) $4-3R+9S+\sum_{j=1}^{R} 3^{2n_j+1} \in LS[3](3,5)$.

Proof. To prove part (i), we let n be a non–negative integer, and we define $a_n = (3^{4n+1}-2)$, $b_n = (3^{4n+1}-3)/60$. An easy congruence argument shows that b_n is an integer. By Theorem 7, $1+3^{4n+1} \in$ LS$[N](3,5)$ for any N dividing $a_n b_n$. By Theorem 4, $3^{4n+1} \in$ LS$[N](3,4)$ for any N dividing $5b_n$. Therefore, $1+3^{4n+1} \in$ LS$[N](3,5)$ and $3^{4n+1} \in$ LS$[N](3,4)$ for any N dividing $(3^{4n+1}-3)/60$. The result now follows from Corollary 2.

To prove part (ii), we let n be a non–negative integer, and we define $c_n = (3^{4n+3}-2)/5$, $d_n = (3^{4n+3}-3)/12$. Easy congruence arguments show that c_n and d_n are integers. By Theorem 7, $1+3^{4n+3} \in$ LS$[N](3,5)$ for any N dividing $c_n d_n$. By Theorem 4, $3^{4n+3} \in$ LS$[N](3,4)$ for any N dividing d_n. Therefore, $1+3^{4n+3} \in$ LS$[N](3,5)$ and $3^{4n+3} \in$ LS$[N](3,4)$ for any N dividing $(3^{4n+3}-3)/12$. The result now follows from Corollary 2.

□

ACKNOWLEDGMENTS

Some of the results in section 3 are also included in the Master Thesis [2] of the first author, which was written under the supervision of the third author. The third author would like to thank the Nebraska combinatorics group, especially Doug Stinson, for useful discussions following a seminar presentation of this topic.

REFERENCES

[1] Y.M. Chee, C.J. Colbourn, S.C. Furino and D.L. Kreher, *Large sets of disjoint t-designs*, *The Australasian Journal of Combinatorics* **2** (1990) 111-119.

[2] C.A. Cusack, *PSL(2, q) as an automorphism group Of a* $3-(q+1,5,\lambda)$ *Design* Master Thesis, Michigan Technological University, (1994).

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

[4] E.S. Kramer, S.S. Magliveras, E.A. O'Brien, *Some new large sets of t-designs*, Australasian Journal of Combinatorics **7** (1993), 189-193.

[5] L. Teirlinck, *On large sets of disjoint quadruple systems*, Ars Combinatoria **17** (1984), 173-176.

[6] Qiu-rong Wu, *A note on extending t-designs*, Australasian Journal of Combinatorics **4** (1991) 229-235.