Simple 3-designs and PSL$(2, q)$ with $q \equiv 1 \pmod 4$

Niranjan Balachandran*and Dijen Ray-Chaudhuri†
Department of Mathematics
The Ohio State University
Columbus, Ohio, USA
email: niranj@math.ohio-state.edu, dijen@math.ohio-state.edu

Abstract

In this paper, we consider the action of $(2, q)$ on the finite projective line $\mathbb{F}_q \cup \{\infty\}$ for $q \equiv 1 \pmod 4$ and construct several infinite families of simple 3-designs which admit PSL$(2, q)$ as an automorphism group. Some of the designs are also minimal. We also indicate a general outline to obtain some other algebraic constructions of simple 3-designs.

Key words: 3-designs, automorphism groups, projective special linear groups, homogeneous action.

1 Introduction

Construction of designs using multiply transitive group actions is a very important technique in the construction of t-designs for $t \geq 3$. The cases $t \geq 4$ do not yield infinite families of examples since there is no infinite family of sharply t-transitive groups for $t \geq 4$. The case $t = 3$ has been investigated to some further extent since sharply 3-transitive groups are known in these cases. Groups of 'linear fractional transformations' (the groups PGL$(2, q)$) are examples of triply transitive groups and these groups have been used by Dan Hughes (see for instance,[5]) and several others to construct 3-designs .
The group PSL$(2, q)$ acts 3-homogeneously, i.e., acts transitively on subsets of size 3 of the finite projective line, if $q \equiv 3 \pmod 4$. Thus unions of orbits for the action of PSL$(2, q)$ on the set of subsets of the projective line of size k yield simple 3-designs. Designs of this kind

*Corresponding author
†partially supported by NSF Grant DMS 0302221

have been investigated in detail in [1]. However in the case of $q \equiv 1 \pmod 4$, the action is never 3-homogeneous and hence orbits for this action do not necessarily give us designs. Nonetheless, we construct simple 3-designs admitting $\mathrm{PSL}(2,q)$ as an automorphism group by taking a union of orbits. A similar result occurs in [9], where the author discusses a similar construction and demonstrates two simple 3-designs. One of the results in this paper constructs infinite families of minimal simple designs, which we obtained independently. We also indicate a more general outline on obtaining other simple 3-designs while providing a few examples. Finally, we show an application in constructing an infinite family of Large sets of Group Divisible designs (or simply Divisible designs).

2 Preliminaries

Let t, v, k, λ be given positive integers. Let X be a finite set of size v and $\mathcal{B}$, a collection of k-subsets of X. We say that $(X, \mathcal{B})$ is a $t-(v,k,\lambda)$ design if each subset $\mathcal{T}$ of X of size t is contained in precisely λ members of $\mathcal{B}$.

In the rest of this paper, we let $X := \mathbb{F}_q \cup \{\infty\}$. The set of all mappings of the form:

$$x \to \frac{ax+b}{cx+d}$$

with , $a, b, c, d \in \mathbb{F}_q, ad-bc$ being a square in $\mathbb{F}_q^*$ constitutes the special linear group, $\mathrm{PSL}(2,q)$ on X. The action of $\mathrm{PSL}(2,q)$ induces a natural action on all k-subsets of X. It is well known that this action is transitive on all subsets of size 3 of X, *if and only if* $q \equiv 3 \pmod 4$.

Thus in the case of $q \equiv 1 \pmod 4$, not all 3-subsets are $\mathrm{PSL}(2,q)$ equivalent. In this case, we start with a simple observation which is quite straightforward to verify: any subset $\mathcal{T}$ of X of size 3 satisfies

$$\mathcal{T} \sim \{0, \infty, 1\} \text{ or } \mathcal{T} \sim \{0, \infty, \theta\}$$

where $< \theta >= \mathbb{F}_q^*$, i.e., θ is a primitive root of unity in $\mathbb{F}_q$ and for two subsets $\mathcal{T}_1, \mathcal{T}_2$ of order 3, we say $\mathcal{T}_1 \sim \mathcal{T}_2$ if and only if there is an element $g \in \mathrm{PSL}(2,q)$ such that $g \cdot \mathcal{T}_1 = \mathcal{T}_2$.
We note here that $\{0, \infty, 1\} \not\sim \{0, \infty, \theta\}$ if $q \equiv 1 \pmod 4$ and that accounts for the non-homogeneous action for the case $q \equiv 1 \pmod 4$.

The following proposition is the first step towards understanding the structure of orbits of k-subsets of X induced by the action of $\mathrm{PSL}(2,q)$.

Proposition 1 *: Let $k \in \mathbb{N}$ and consider the action of $\mathcal{G} := PSL(2,q)$ on the set of k-subsets of X. If Γ is an orbit for this action then so is $\theta\Gamma$, where θ is a primitive root of unity in $\mathbb{F}_q$. Moreover, $\theta^2\Gamma = \Gamma$.*

Proof: Suppose $\Gamma := \mathcal{G}B_0 = \{gB_0 : g \in \mathcal{G}\}$, where $gB_0 := \{gb : b \in B_0\}$ for a subset $B_0 \subset X$ of order k. We have

$$\Gamma = \mathcal{G}(B_0) = \Big\{\{\frac{ay+b}{cy+d} : y \in B_0\} : ad - bc \in (\mathbb{F}_q^*)^2\Big\}$$

so that we have

$$\begin{aligned}
\theta\Gamma &:= \{\theta B : B \in \Gamma\} \\
&= \Big\{\theta\{\frac{ay+b}{cy+d} : y \in B_0\} : ad - bc \in (\mathbb{F}_q^*)^2\Big\} \\
&= \Big\{\{\frac{a\theta y+b\theta}{cy+d} : y \in B_0\} : ad - bc \in (\mathbb{F}_q^*)^2\Big\} \\
&= \Big\{\{\frac{a(y\theta)+b\theta}{\frac{c}{\theta}(y\theta)+d} : y \in B_0\} : ad - bc \in (\mathbb{F}_q^*)^2\Big\} \\
&= \Big\{\{\frac{ay+b}{cy+d} : y \in \theta B_0\} : ad - bc \in (\mathbb{F}_q^*)^2\Big\} = \mathcal{G}(\theta B_0)
\end{aligned}$$

since the map $f_\theta := x \to \frac{ax+b\theta}{\frac{c}{\theta}x+d} \in \mathcal{G}$ if and only if the map $f := x \to \frac{ax+b}{cx+d} \in \mathcal{G}$. □

An alternate quick proof[1] of the proposition goes thus: Let $g_\theta := x \to \theta x \in \mathrm{PGL}(2,q)$. Then, $\theta\Gamma = g_\theta\Gamma = g_\theta\mathcal{G}B_0 = g_\theta\mathcal{G}g_\theta^{-1}B_0 = \mathcal{G}g_\theta B_0 = \mathcal{G}\theta B_0$, since $\mathcal{G}$ is a subgroup of $\mathrm{PGL}(2,q)$ of index 2, and is therefore normal.
As a consequence we have the following corollary, which also appears in [9]. But, first, we make a definition. For a set Y, by the term *Set system* of Y, we mean a multiset of subsets of Y. Hence in a set system, one could have several copies of a set.

Corollary 2 *: Let $\lambda_\Delta(\mathcal{T})$ denote the number of subsets of the set system Δ containing the set $\mathcal{T}$. If Γ is an orbit for the action of $\mathcal{G}$ on k-subsets of X, we have*

$$\lambda_\Gamma(\{0,\infty,1\}) = \lambda_{\theta\Gamma}(\{0,\infty,\theta\}), \quad (1)$$
$$\lambda_{\theta\Gamma}(\{0,\infty,1\}) = \lambda_\Gamma(\{0,\infty,\theta\}). \quad (2)$$

Consequently, if $\mathcal{B} := \Gamma \cup \theta\Gamma$, then $\lambda_\mathcal{B}(\{0,\infty,1\}) = \lambda_\mathcal{B}(\{0,\infty,\theta\})$.

Proof: For the set system Δ, let $\mathcal{A}_\Delta := \{A \in \Delta : 0,\infty,1 \in A\}$ and let $\mathcal{B}_\Delta := \{B \in \Delta : 0,\infty,\theta \in B\}$. From the previous proposition, it is clear that $A \in \mathcal{A}_\Gamma$ if and only if $\theta A \in \mathcal{B}_{\theta\Gamma}$, so the first statement is clear. For the second part, note that $B \in \Gamma$ holds if and only if $\theta B \in \theta\Gamma$. But $\theta B \in \theta\Gamma$ if and only if $\theta^{-2}(\theta B) = \theta^{-1}B \in \theta\Gamma$ since the map $x \to \theta^{-2}x$ is an element of $\mathrm{PSL}(2,q)$. This implies that $B \in \mathcal{B}_\Gamma$ if and only if $\theta^{-1}B \in \mathcal{A}_{\theta\Gamma}$ and that completes the proof.
The last statement follows by adding equations (1) and (2). □

[1]We thank the referees for indicating this simpler line of argument.

In the course of the proof of the results in the later sections, we shall need two particular theorems that can be found in [2], (pf 285-286). The first of the theorems lists the subgroups of $\mathrm{PSL}(2,q)$. The second proposition is a lemma regarding number of fixed points of X by various elements of $\mathrm{PSL}(2,q)$.

Theorem 3 *(see [2],[6]): The subgroups of $PSL(2,q)(q=p^n)$ are as follows:*

1. *Cyclic subgroups $C_d, d|\frac{q\pm1}{2}$,*
2. *Dihedral subgroups of order $2d, d|\frac{q\pm1}{2}$,*
3. *A_4 (size 12)*
4. *S_4 when $q^2 \equiv 1 \pmod{16}$ (size 24),*
5. *A_5 when $q^2 \equiv 1 \pmod{5}$. (size 60),*
6. *Subgroups $PSL(2,p^m)$ with $m|n$,*
7. *Subgroups $PGL(2,p^m)$ with $2m|n$,*
8. *The elementary abelian groups of order $p^m, m \leq n$,*
9. *A semidirect product of the elementary abelian group of order p^m and the cyclic group of order d where $d|\frac{q-1}{2}$ and $d|(p^m-1)$.*

Since we are dealing with the case $q \equiv 1 \pmod 4$, we have $q^2 \equiv 1 \pmod{16}$ if and only if $q \equiv 1 \pmod 8$, and $q^2 \equiv 1 \pmod 5$ if and only if $q \equiv 1, 9 \pmod{20}$.

Proposition 4 *: Let g be an element of $\mathcal{G}(= PSL(2,q))$ of order m. Then the number of fixed elements $\chi(g)$ by g, in $X(= \mathbb{F}_q \cup \{\infty\})$, is given by*

1. *$\chi(g) = 1$ if $m = p, q = p^n$ for some n.*
2. *$\chi(g) = 2$ if $m|\frac{q-1}{2}$.*
3. *$\chi(g) = 0$ if $m|\frac{q+1}{2}$.*

3 The Theorems

We are now ready to state our first theorem.

Theorem 5 *: Let $q \equiv 13 \pmod{16}$ or $q \equiv 1 \pmod{16}$ be a prime with $q > 121$. Let $k = \frac{q-1}{4}$. Then there exists a non-trivial simple $3-(q+1, k, \frac{(k-1)(k-2)}{2})$ design. Further, if $q \equiv 13 \pmod{16}$ then this value of λ is minimal, i.e., for any simple $3-(q+1, k, \lambda)$ design, $\frac{(k-1)(k-2)}{2}$ divides λ.*

Proof : Note that $q \equiv 1 \pmod{4}$ holds, by the hypothesis. Consider the projective line $X := \mathbb{F}_q \cup \{\infty\}$ and the group $\mathcal{G} := \mathrm{PSL}(2, q)$ acting on X. Let $\theta \in \mathbb{F}_q^*$ be a primitive root of unity and let $B := \{1, \theta^4, \theta^8, \theta^{12}, \ldots, \theta^{(q-5)}\}$. Let Γ denote the orbit, $\Gamma := \mathcal{G}B$ of the induced action of $\mathcal{G}$ on $\binom{X}{k}$, the set of k-subsets of X. Consider the set system $\mathcal{B} := \Gamma \cup \theta\Gamma$. From corollary 2 it follows that $(X, \mathcal{B})$ is a 3-design with parameters $3-(q+1, k, \lambda_0)$ for some λ_0. To calculate λ_0, note that,

$$
\begin{aligned}
|\mathcal{B}| &= 2|\Gamma| && (3)\\
&= 2\frac{|\mathrm{PSL}(2,q)|}{|\mathcal{G}_B|} && (4)\\
&= 2\frac{(q^2-1)q}{2|\mathcal{G}_B|} = \frac{(q^2-1)q}{|\mathcal{G}_B|}. && (5)
\end{aligned}
$$

On the other hand, $|\mathcal{B}| = \lambda_0 \left(\frac{(q+1)q(q-1)}{k(k-1)(k-2)}\right)$ since $(X, \mathcal{B})$ is a 3-design (simple or not). Comparing the two expressions, we get $\lambda_0 = \frac{k(k-1)(k-2)}{|\mathcal{G}_B|}$.

Since $q \equiv 13 \pmod{16}$ or $1 \pmod{16}$, it follows that $k \equiv 0, -1 \pmod{4}$. Now note that for the block B as before, the following maps $f(x) := \theta^4 x, g(x) := \frac{1}{x}$ are both members of $\mathcal{G}_B$. Since $gf = f^{-1}g$ it follows that $\mathcal{D}_{2k}$, the dihedral group of size $2k$, is contained in $\mathcal{G}_B$. Hence $|\mathcal{G}_B|$ is divisible by $2k$ and $\lambda_0|\frac{(k-1)(k-2)}{2}$. By the hypothesis, $\frac{(k-1)(k-2)}{2}$ is odd and that implies that $\Gamma \neq \theta\Gamma$. Therefore, the design is simple. To complete our calculation of λ_0, we make use of the list of subgroups of $\mathcal{G}$.
Since q is prime, there are no nontrivial subgroups of types 6 and 7 from the list in the theorem. Since $D_{2k} \subset \mathcal{G}_B$, the group $\mathcal{G}_B$ cannot be of types 1 or 8. By size considerations (from the hypothesis on q), types 3, 4 and 5 are also ruled out. Finally, for type 9, note that such a subgroup of $\mathcal{G}$ has size, a multiple of q. But we have $|\mathcal{G}_B||\frac{k(k-1)(k-2)}{2}$, so that we have $q|\frac{k(k-1)(k-2)}{2}$ and that is a contradiction since q is prime and $q > k$.
Hence it follows that $\mathcal{G}_B$ is a dihedral group containing $\mathcal{D}_{2k}$. But again, from the list of subgroups of $\mathrm{PSL}(2, q)$, the dihedral subgroups of $\mathcal{G}$ are the groups $\mathcal{D}_{2d}$ where $d|2k+1$ or $d|2k$, since $q = 4k+1$. Since $\mathcal{D}_{2k} \subset \mathcal{G}_B$, we must have $\mathcal{G}_B = \mathcal{D}_{2k}$ or $\mathcal{G}_B = \mathcal{D}_{4k}$. The later is ruled out since $\frac{(k-1)(k-2)}{2}$ is odd. Therefore, we have $\mathcal{G}_B = \mathcal{D}_{2k}$ and $\lambda_0 = \frac{(k-1)(k-2)}{2}$.

Now, for any $3-(q+1, k, \lambda)$ design, we have the arithmetic conditions

- $k(k-1)(k-2) \mid \lambda(q+1)q(q-1)$,
- $(k-1)(k-2) \mid \lambda q(q-1)$,

- $(k-2) \mid \lambda(q-1)$.

The hypothesis implies that k is odd so that $(k, k-2) = 1$. Also, from the assumptions on q, we have $(k-1, q-1) = (k-1, 4k) = 2$. It is now a simple check to see that $\frac{(k-1)(k-2)}{2} | \lambda$. Since the designs constructed achieve this value of λ, the designs are minimal, as claimed. And last but not the least, it is quite simple to see that this is not the trivial design either. $\square$

Remark: It is possible to improve upon the result stated in the theorem above by ruling out possibilities other than D_{2k} for $\mathcal{G}_B$ with some more detailed calculation, for smaller values of q. It is also possible to, in a similar fashion, extend the same to the case when q is a prime power and not simply a prime. We shall however, not get into those details now.

Remark: The union $\Gamma \cup \theta\Gamma$ in fact turns out to be simply an orbit for the action of the action of $\mathrm{PGL}(2, q)$. The reason we are more interested in dealing with the action of $\mathrm{PSL}(2, q)$ is due to the fact that for q prime, the lattice of subgroups of $\mathrm{PSL}(2, q)$ is well known and hence one could, as in [1], calculate the Möbius function for $\mathrm{PSL}(2, q)$ in less messy a fashion than for[2] $\mathrm{PGL}(2, q)$. Moreover, as we shall see subsequently, we are specifically interested in the nature of the action of $\mathrm{PSL}(2, q)$ on the orbits of $\mathrm{PGL}(2, q)$, i.e., whether the action of $\mathrm{PSL}(2, q)$ splits the corresponding orbit of $\mathrm{PGL}(2, q)$ or not. We shall,shortly, state this more precisely .

Note that if for some B, we have $\Gamma = \theta\Gamma$, where Γ is the orbit of B, then, from the preceding discussions, (X, Γ) would be a simple 3-design. Hence we can always obtain a simple design by either simply taking an orbit Γ or taking the union $\Gamma \cup \theta\Gamma$.

It is possible that $\Gamma = \theta\Gamma$ for a non-trivial block B ($B = \mathbb{F}_q^*$ is the trivial case). We indicate two such instances here.

- $k = 4$: If 2 is a primitive root of unity in $\mathbb{F}_q^*$, we could take $\theta = 2$. Consider the block $B = \{0, 1, 2, \infty\}$. The map $f(x) := 4\left(\frac{x-1}{x}\right)$ satisfies $f(0) = \infty, f(\infty) = 4, f(1) = 0$ and $f(2) = 2$, so that $f(B) = \theta B$ and it is clear that $f \in \mathrm{PSL}(2, q)$.
- $k = 5$: If $q \equiv 5 \pmod 8$, consider the block $B_0 = \{0, \theta, \infty, \theta\alpha, \theta\beta\}$, where $\alpha = \frac{i}{i-1}$ with $i^2 = -1$ in $\mathbb{F}_q^*$, and $\beta = \frac{\alpha-1}{\alpha}$. Then the map $f(x) := \beta\left(\frac{x}{x-\theta}\right)$ satisfies, $f(0) = 0, f(\theta) = \infty, f(\infty) = \beta, f(\theta\alpha) = 1$ and $f(\theta\beta) = \alpha$ so that $f(B) = \theta^{-1}B$ (note that θ^{-1} also is a primitive root of unity in $\mathbb{F}_q^*$). Again, it is easy to see that $f \in \mathcal{G}$.The fact that $f \in \mathcal{G}$ follows from the assumption that i (as above) does not have a square root in $\mathbb{F}_q^*$.

We shall say a little more on this in the last section.

[2]One could list the subgroups of $\mathrm{PGL}(2, q)$ using the fact that there is an embedding $\mathrm{PSL}(2, q) < \mathrm{PGL}(2, q) < \mathrm{PSL}(2, q^2)$and use the Möbius function from $\mathrm{PSL}(2, q)$ to calculate the Möbius function on the lattice of subgroups of $\mathrm{PGL}(2, q)$ as well.

We now show another application of the same idea to obtain another infinite family of simple 3-designs. In all the examples that follow, $\Gamma \neq \theta\Gamma$.

Theorem 6 *: Let $q \equiv 1 \pmod{20}$ be a prime. Then there exists a non-trivial simple 3-design $3-(q+1,7,21)$.*

Proof: Suppose $q = 20r+1$. As before, let θ be a primitive root of unity in $\mathbb{F}_q^*$. Let $B_0 = \{0,\infty\} \cup \{1, \theta^{4r}, \theta^{8r}, \theta^{12r}, \theta^{16r}\}$. As in theorem 3, consider the set system $\mathcal{B} := \Gamma \cup \theta\Gamma$ where $\Gamma := \mathcal{G}B_0$ is the orbit of B_0 under the action of $\mathcal{G} := \mathrm{PSL}(2,q)$. Again $(X,\mathcal{B})$ is a 3-design $3-(q+1,7,\lambda)$ with $\lambda = \frac{7\cdot 6\cdot 5}{|\mathcal{G}_{B_0}|}$.
Now note that the map $f := x \to \frac{1}{x}$ is an element of $\mathrm{PSL}(2,q)$ when $q \equiv 1 \pmod 4$ and that $f(B_0) = B_0$, so that $2||\mathcal{G}_{B_0}|$(since $f \circ f = I$, where I is the identity map on X). Then clearly, λ is odd which implies that $\Gamma \neq \theta\Gamma$. So, the design is simple as before[3]. It remains to check that $\lambda = 21$. Note also that $h := x \to \theta^{4r}x$ also stabilizes B_0 and hence $H :=< f, h > \subset \mathcal{G}_{B_0}$. Since $f^2 = 1, h^5 = 1$, and as before, $fh(x) = h^{-1}f(x)$, so that $H \simeq D_{10}$. It follows that $\lambda|21$.
We make note of the proposition stated in the Preliminaries section; this can be found in [2], for instance.
Now if the subgroup $\mathcal{G}_{B_0}$ contains an element of order 3, then it has to fix exactly one element of B_0. But since q is a prime and $q > 3$, the proposition above gives us a contradiction.
Next, suppose that $\mathcal{G}_{B_0}$ contains an element g of order 7. Since the set B_0 is partitioned as a union of cycles for the action of the cyclic subgroup generated by g with each cycle size being a multiple of 7, no proper subset of B_0 is invariant under the action of g.
In this case, $2,5,7||\mathcal{G}_{B_0}|$, so that $\mathcal{G}_{B_0}$ is a non-abelian group (since it contains H) whose size is at least 70. From the list of subgroups of $\mathcal{G}$ (see the theorem stated in the preliminary section), it follows that $\mathcal{G}_{B_0}$ is a dihedral group and hence g centralizes h, i.e., $gh = hg$.
Consequently, $g(0) = g(h(0)) = h(g(0))$,so, $g(0)$ is fixed by h. Since g has no fixed points, we have $g(0) = \infty$. By the same token, we get $g(\infty) = 0$. Hence g fixes the subset $\{0,\infty\}$ of B_0 which is a contradiction.
Consequently, we have $\mathcal{G}_{B_0} = H \simeq D_{10}$ and that completes the proof. $\square$.

The arguments in the preceding theorems can be viewed from a more general perspective as follows. Fix $k \geq 4$ and consider the induced action of $\mathrm{PSL}(2,q)$ on the set of k-subsets of X, namely, $\binom{X}{k}$. The set $\binom{X}{k}$ is partitioned into orbits $\Gamma_i, i = 1,\ldots,r$ for some r, so that we have

$$\binom{X}{k} = \bigcup_i \Gamma_i.$$

Let $\mathfrak{O} = \{\Gamma_1, \Gamma_2, \ldots, \Gamma_r\}$. Then the content of proposition 1 simply implies that the group $\mathbb{F}_q^*$ acts on $\mathfrak{O}$ as

$$g \cdot \Gamma = g\Gamma, \text{ for } g \in \mathbb{F}_q^*, \Gamma \in \mathfrak{O}.$$

[3]In fact taking a block B_0 satisfying $B_0 = -B_0$, and $k \equiv 3 \pmod 4$ always gives us a simple design by this technique, with the only restriction on q being it is prime. However, calculation of λ depends on the choice of B_0.

Thus we can write

$$\mathfrak{O} = \bigcup_{i \in I} \mathfrak{O}_i$$

where each $\mathfrak{O}_i$ is an orbit of $\mathfrak{O}$ under the action of $\mathbb{F}_q^*$. Furthermore, since the map $x \to \theta^2 x$ is an element of $\mathrm{PSL}(2,q)$, it follows that $|\mathfrak{O}_i| = 1$ or 2.
Hence each orbit for the action described above gives us a simple 3-design with $\mathrm{PSL}(2,q)$ acting as a group of automorphisms.

We now work to understand this viewpoint, a little more concretely. The next proposition is a starting step of sorts; it can also be viewed as an independent result.

Proposition 7 *: Let $q \equiv 1 \pmod 8$ be an odd prime. Let $B_0 := \{0, \infty, 1, -1\}$ and $\Gamma = \mathcal{G}B_0$. Then $\mathfrak{O} := \mathfrak{O}(\Gamma)$, the orbit of Γ under the action of $\mathbb{F}_q^*$ as described above has size 2. Consequently, there exist simple 3-designs $3-(q+1,4,3)$ for $q \equiv 1 \pmod 8$ admitting $PSL(2,q)$ as an automorphism group.*

Proof: Proposition 1 yields that $(X, \mathcal{B})$ is a $3-(q+1,4,\lambda)$-design (simple or not) for some λ, where $\mathcal{B} = \Gamma \cup \theta\Gamma$, and θ is a primitive root of unity. From the proof of theorem 3, we have $\lambda = \frac{4 \cdot 3 \cdot 2}{|\mathcal{G}_{B_0}|}$. Consider the maps $f(x) := -x, g(x) := \frac{1}{x}$ and $h(x) := -\frac{1+x}{1-x}$ in $\mathcal{G} = \mathrm{PSL}(2,q)$. The claim that $f, g \in \mathcal{G}$ follows from the fact that -1 is a square in $\mathbb{F}_q$ and that $h \in \mathcal{G}$ follows, if 2 is a square in $\mathbb{F}_q^*$ which is indeed the case, by the hypothesis. It is straightforward to verify that f fixes the subset $\{1,-1\}$ and fixes 0 and ∞, g fixes the set $\{0,\infty\}$ and fixes $1,-1$ and finally, h fixes the sets $\{1,\infty\}$ and $\{0,-1\}$ but fixes no point. Hence $G :=< f, g, h >$ fixes B_0 so that $G \subset \mathcal{G}_{B_0}$. Also, it is simple to see that $|G| = 8$. Note that in particular, the group G acts transitively on B_0.
Now, if $\mathcal{G}_{B_0}$ has an element of order 3, then by conjugation with an element of G, if necessary, we may assume that it has one such element which fixes ∞ since any element of order 3 fixes exactly one element of B_0. Taking its square, if necessary, we may assume that it acts on B_0 as $(1 \;\; 0 \;\; -1)(\infty)$. But $\mathfrak{g} := x \to x-1$ is the unique element of $\mathcal{G}$ satisfying $\mathfrak{g}(1) = 0, \mathfrak{g}(0) = -1, \mathfrak{g}(\infty) = \infty$ and $\mathfrak{g}(-1) = -2 \neq 1$ since q is prime and $q \geq 4$.
This contradicts the assumption of the existence of an element of $\mathcal{G}_{B_0}$ of order 3.

Finally since λ is odd, it follows that $|\mathfrak{O}| = 2$ and hence $\Gamma \neq \theta\Gamma$ and so $(X, \mathcal{B})$ is a simple design. $\square$.

Our next result is an 'existential' result for simple 3-designs inasmuch as the exact value of λ is not specified.

Theorem 8 *: For any k fixed, $k \geq 4$, and q, a prime satisfying $q \equiv 1 \pmod 4$ and q being sufficiently large, i.e., for $q \geq q_0(k)$ for some integer $q_0(k)$, there exists a set $B_0 \subset X$ of size k such that the orbits Γ and $\theta\Gamma$ are distinct, where, $\Gamma := \mathcal{G}(B_0)$, where $\mathcal{G} = PSL(2,q)$ with q prime. Consequently, there exist simple $3-(q+1,k,\lambda)$ designs for all 'sufficiently large' q.*

Remark: The preceding proposition considers the case $k = 4$ and $q \equiv 1 \pmod 8$. In that case, we did exhibit a concrete instance of a set B_0 and were also able to compute λ.

Proof: We show that for each $k \geq 4$, there exists $B_0 \subset X$, such that there is no element $\mathfrak{g} \in \mathcal{G}$ satisfying, $\mathfrak{g}B_0 = \theta B_0$, where as always, $\theta B_0 := \{\theta x : x \in B_0\}$.
Let us first consider the case $k = 4$. Note that by the observation in the Preliminaries section, we know that $\{0, \infty, 1\}$ and $\{0, \infty, \theta\}$ are $\mathcal{G}$-*inequivalent*, i.e., there exists no $\mathfrak{g} \in \mathcal{G}$ such that $\mathfrak{g}\big(\{0, 1, \infty\}\big) = \{0, \theta, \infty\}$.
Consider the sets $B_y := \{0, 1, \infty, y\}$ with $y \in \mathbb{F}_q^* \setminus \{1\}$. We shall prove that for some $\eta \in \mathbb{F}_q^* \setminus \{1\}$, the sets B_η and θB_η are $\mathcal{G}$-inequivalent.
Suppose there exists $\mathfrak{g} \in \mathcal{G}$ such that $\mathfrak{g}B_y = \theta B_y$. For the sake of notation we write

$$\begin{aligned} \mathfrak{g}(0) &= \alpha, && (6)\\ \mathfrak{g}(1) &= \beta, && (7)\\ \mathfrak{g}(\infty) &= \gamma, \text{ and} && (8)\\ \mathfrak{g}(y) &= \delta, && (9) \end{aligned}$$

where $\{\alpha, \beta, \gamma, \delta\} = \theta B_y$. Note that if $\delta = \theta y$, then $\mathfrak{g}$ maps the set $\{0, 1, \infty\}$ into $\{0, \theta, \infty\}$ which, by the observation above is impossible. Hence, $\theta y \neq \delta$.
We introduce some further notation here: $\pm i$ denote the elements in $\mathbb{F}_q^*$ satisfying $i^2 = -1$ (such elements exist in $\mathbb{F}_q^*$ since $q \equiv 1 \pmod 4$). Similarly, $x = \pm\sqrt{3}$ are the elements (such elements exist if and only if $q \equiv 1 \pmod 3$) of $\mathbb{F}_q^*$ satisfying $x^2 = 3$.

The following table presents a list of all the (revised in light of this observation) possibilities as we vary over the ordered quadruple, $(\alpha, \beta, \gamma, \delta)$.

$(\alpha,\beta,\gamma,\delta)$	$\mathfrak{g}$	$\mathfrak{g}\in \mathrm{PGL}(2,q)$ iff $y=$	$\mathfrak{g}\in \mathrm{PSL}(2,q)$ iff
$(\theta y,\theta,\infty,0)$	$-\theta(x-y)$	2	Never in $\mathrm{PSL}(2,q)$
$(\theta y,\theta,0,\infty)$	$\frac{\theta(1-y)}{x-y}$	$\frac{1\pm i\sqrt{3}}{2}$	Never in $\mathrm{PSL}(2,q)$
$(\theta y,0,\theta,\infty)$	$\theta\frac{x-1}{x-y}$	-1	$y-1\notin(\mathbb{F}_q^*)^2$
$(\theta y,\infty,\theta,0)$	$\theta\frac{x-y}{x-1}$	$\mathfrak{g}\in \mathrm{PGL}(2,q)$	$y-1\notin(\mathbb{F}_q^*)^2$
$(\theta y,0,\infty,\theta)$	$\frac{\theta(x-1)}{y-1}$	$\frac{1\pm i\sqrt{3}}{2}$	Never in $\mathrm{PSL}(2,q)$
$(\theta y,\infty,0,\theta)$	$\frac{\theta(y-1)}{x-1}$	$\frac{1}{2}$	$y-1\notin(\mathbb{F}_q^*)^2$
$(0,\theta y,\infty,\theta)$	$(\theta y)x$	±1	Never in $\mathrm{PSL}(2,q)$
$(0,\theta y,\theta,\infty)$	$\theta\frac{x}{x-y}$	$\frac{1\pm i\sqrt{3}}{2}$	$y\notin(\mathbb{F}_q^*)^2$
$(\infty,\theta y,0,\theta)$	$\frac{\theta y}{x}$	$\mathfrak{g}\in \mathrm{PGL}(2,q)$	$y\notin(\mathbb{F}_q^*)^2$
$(\infty,\theta y,\theta,0)$	$\theta\frac{x-y}{x}$	$\frac{1}{2}$	$y\notin(\mathbb{F}_q^*)^2$
$(\theta,\theta y,0,\infty)$	$\frac{-\theta y}{x-y}$	2	$y\notin(\mathbb{F}_q^*)^2$
$(\theta,\theta y,\infty,0)$	$\frac{-\theta(x-y)}{y}$	$\frac{1\pm i\sqrt{3}}{2}$	$y\notin(\mathbb{F}_q^*)^2$
$(0,\infty,\theta y,\theta)$	$\theta y\frac{x}{x-1}$	$\frac{1\pm i\sqrt{3}}{2}$	$y\notin(\mathbb{F}_q^*)^2$
$(0,\theta,\theta y,\infty)$	$\theta y\frac{x}{x-y}$	$\frac{1}{2}$	Never in $\mathrm{PSL}(2,q)$
$(\infty,0,\theta y,\theta)$	$\frac{\theta y(x-1)}{x}$	2	$y\notin(\mathbb{F}_q^*)^2$
$(\infty,\theta,\theta y,0)$	$\frac{\theta y(x-y)}{x}$	$\frac{1\pm i\sqrt{3}}{2}$	Never in $\mathrm{PSL}(2,q)$
$(\theta,0,\theta y,\infty)$	$\theta y\frac{x-1}{x-y}$	$\mathfrak{g}\in \mathrm{PGL}(2,q)$	$y(y-1)\notin(\mathbb{F}_q^*)^2$
$(\theta,\infty,\theta y,0)$	$\theta y\frac{x-y}{x-1}$	-1	$y(y-1)\notin(\mathbb{F}_q^*)^2$

The table above is to be read as follows: for instance, the third row in the table tells us that corresponding to the quadruple $(\alpha,\beta,\gamma,\delta)=(\theta y,0,\theta,\infty)$, there exists $\mathfrak{g}\in\mathrm{PGL}(2,q)$ satisfying $\mathfrak{g}(0)=\theta y,\mathfrak{g}(1)=0,\mathfrak{g}(\infty)=\theta,\mathfrak{g}(y)=\infty$ if and only if $y=-1$ and $\mathfrak{g}(x):=\theta\dfrac{x-1}{x-y}$. Further, this element of $\mathrm{PGL}(2,q)$ is also an element of $\mathcal{G}$ if and only if $y-1=-2\notin(\mathbb{F}_q^*)^2$. Similarly, row 4 of the table corresponds to the case where the map $\mathfrak{g}(x):=\theta\dfrac{x-y}{x-1}$ is always an element of $\mathrm{PGL}(2,q)$ but is an element of $\mathcal{G}$ if and only if $(y-1)\notin(\mathbb{F}_q^*)^2$.

Note that if $q\equiv 1 \pmod 8$, we have $2\in(\mathbb{F}_q^*)^2$, so that the case $B:=\{1,0,\infty,-1\}$ (row 3 of the table) corresponds to the statement of the preceding theorem.
In order that B_η and θB_η are $\mathcal{G}$-inequivalent, we need $\eta\in\mathbb{F}_q^*$ such that all the conditions in the last column of the table are violated. By an inspection of the table, we conclude that if there exists $\eta\in\mathbb{F}_q^*\setminus\{1\}$ such that η and $(\eta-1)$ are both non-zero squares in $\mathbb{F}_q$, then all the conditions of the last column are simultaneously violated, so that the set B_η cannot be mapped by an element of $\mathcal{G}$ to the set θB_η.

To see that, we first prove a very simple lemma.

Lemma 9 *: Suppose $n>1$. Then a set $A\subset\{1,2,\ldots,4n\}$ satisfying*

1. $|A| = 2n$,

2. $x \in A$ *if and only if* $4n + 1 - x \in A$,

3. $1, 4 \in A$,

contains two consecutive elements.

Proof of the lemma: By condition 2, the set A contains precisely n elements among $\{1, 2, \ldots, 2n\}$. If $2n \in A$, then $2n + 1 \in A$ by condition 2 and we are through. Similarly, if $\{2, 3, 5\} \cap A \neq \emptyset$, then we are through since $1, 4 \in A$. Hence, suppose $2, 3, 5, 2n \notin A$. In particular, $n \geq 3$. If $n \geq 4$, then since the set $\{6, \ldots, 2n - 1\}$ can be partitioned into $n - 3$ disjoint pairs $(6, 7), (8, 9) \ldots, (2n - 2, 2n - 1)$, and $|A \cap \{6, \ldots, 2n - 1\}| = n - 2$ by the observation above, the lemma follows by the pigeon-hole principle. For $n = 3$, since $|A \cap \{1, 2 \ldots, 6\}| = 3$ and $2, 3, 5 \notin A, 6 = 2 \cdot 3 \in A$ but then $7 \in A$ by condition 2 and we are through. $\square$

Now, for $q > 5$ prime and $q \equiv 1 \pmod 4$, we can represent $\mathbb{F}_q^*$ by the set of residues congruent modulo q, so that we may write $\mathbb{F}_q^* := \{1, 2, \ldots, q - 1\}$. Since $q \equiv 1 \pmod 4$, $A := (\mathbb{F}_q^*)^2$ satisfies the conditions 1,2 and 3 of the lemma above. Hence there exists $\eta \in (\mathbb{F}_q^*)^2$ such that $\eta - 1 \in (\mathbb{F}_q^*)^2$. By the observation made before the lemma, the proof of theorem 8 for the case $k = 4$ is complete.

Suppose now that $k \geq 4$. By the proof of the part for $k = 4$, we know that there exists an element $\eta \in (\mathbb{F}_q^*)^2$ such that B_η and θB_η are $\mathcal{G}$-inequivalent. Fix one such η. In order to prove the theorem for $k \geq 4$, we prove the following stronger statement:
For q, a 'sufficiently large' prime (we shall see a more precise meaning of this in the course of the proof) satisfying $q \equiv 1 \pmod 4$, there exists a set $B_0 \subset X$ of size k, containing the set $B_\eta = \{0, 1, \infty, \eta\}$ such that no $\mathfrak{g} \in \mathrm{PSL}(2, q)$ satisfies $\mathfrak{g}(0) = \theta\alpha, \mathfrak{g}(1) = \theta\beta, \mathfrak{g}(\eta) = \theta\gamma$ and $\mathfrak{g}(\infty) = \theta\delta$ for all 4-tuples of distinct elements $(\alpha, \beta, \gamma, \delta)$ in B_0. Clearly, this stronger statement proves our theorem since for such a B_0, it must necessarily follow that B_0 and θB_0 are $\mathcal{G}$-inequivalent.

We prove this by induction on k. The case $k = 4$ has already been settled. Hence let $k > 4$. Suppose by the induction hypothesis that we have a set B_0' of size $k-1$ that contains B_η and satisfies the conditions of the stronger statement.
Let $(\alpha_0, \beta_0, \gamma_0)$ be an ordered triple of the elements of B_η and (α, β, γ), an ordered triple of the elements of B_0'. Since $\mathrm{PGL}(2, q)$ acts sharply 3-transitively on X, there exists a unique element $\mathfrak{g} \in \mathrm{PGL}(2, q)$ such that $\mathfrak{g}(\alpha_0) = \theta\alpha, \mathfrak{g}(\beta_0) = \theta\beta$ and $\mathfrak{g}(\gamma_0) = \theta\gamma$. Hence there is at most one element $\delta = \delta_{(\alpha_0,\beta_0,\gamma_0)}(\alpha, \beta, \gamma)$ in X such that $\mathfrak{g}(\delta_0) = \theta\delta$, where $\{\delta_0\} = B_\eta \setminus \{\alpha_0, \beta_0, \gamma_0\}$. Let

$$\begin{aligned} Y_{(\alpha_0,\beta_0,\gamma_0)} &:= \{\delta_{(\alpha_0,\beta_0,\gamma_0)}(\alpha, \beta, \gamma) : \alpha, \beta, \gamma \in B_0' \text{ and } \alpha, \beta, \gamma \text{ are distinct}\}, \\ Y &:= B_0' \cup \bigcup_{(\alpha_0,\beta_0,\gamma_0)} Y_{(\alpha_0,\beta_0,\gamma_0)}, \end{aligned}$$

where the union is over all the ordered triples $(\alpha_0, \beta_0, \gamma_0)$ of distinct elements of B_η.
Now, if $Y' := \mathbb{F}_q \setminus Y \neq \emptyset$, there exists an element $\delta^* \in Y'$, which by definition, satisfies the following:
For all 4-tuples $(\alpha_1, \beta_1, \gamma_1, \delta_1)$ with $\{\alpha_1, \beta_1, \gamma_1, \delta_1\} = \{\alpha, \beta, \gamma, \delta^*\}$ where $\alpha, \beta, \gamma \in B'_0$ and distinct, there exists no element $\mathfrak{g} \in \mathrm{PSL}(2, q)$ satisfying $\mathfrak{g}(0) = \theta\alpha_1, \mathfrak{g}(1) = \theta\beta_1, \mathfrak{g}(\eta) = \theta\gamma_1$ and $\mathfrak{g}(\infty) = \theta\delta_1$. Indeed, if not, then for some α, β and γ in B'_0, we have $\delta^* \in Y_{(\alpha_0,\beta_0,\gamma_0)}$ where $(\alpha_0, \beta_0, \gamma_0)$ is a suitable permutation of (α, β, γ) and that is a contradiction.
Set $B_0 := B'_0 \cup \{\delta_0\}$. Since B'_0 satisfies the inductive hypothesis, it now follows that B_0 fulfills the conditions of the stronger statement as a consequence of the preceding statement. Finally, note that since $|Y| = O(k^3)$, we have $Y' \neq \emptyset$ if $q > q_0(k) = ck^3$ for some suitably large constant c (independent of k). That completes the induction and the proof of theorem 8. □

4 Large sets of $3 - DDs$

We consider an application of the ideas discussed in the preceding section and demonstrate an instance whereby one can obtain a large set of Divisible Designs. By a 3 - Divisible Design or $3 - DD$, we mean a triple $(Y, \Gamma, \mathcal{B})$ satisfying:

1. Y is a set of size v,
2. $\Gamma = \{G_1, G_2, \ldots\}$ is a partition of Y into non-empty subsets (called groups or point classes)[4] ,
3. $\mathcal{B}$ is a family of subsets of Y(called blocks), each of cardinality k such that each block intersects any group in fewer than two points,
4. Each 3-subset of points with each point from a different group is contained in a unique block.

By a *Large set of* $3 - DDs$ on a set Y admitting a partition Γ into groups, we mean a partition $(\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_r)$ of the set

$$\mathfrak{B} := \{B \subset Y : |B| = k, |B \cap G_i| \leq 1 \text{ for all } i\}$$

where, for each i, $(Y, \Gamma, \mathcal{B}_i)$ is a $3 - DD$.

We now show a construction for a Large set of DDs with block size k, for any $k \geq 4$ and $q + 1$ groups, where q is a prime power.

[4]The groups need not be equal in size; however in our constructions, that shall be the case.

Theorem 10 *: Let q be a prime power. Then there exists λ such that for all $d \geq \binom{q+1}{3}$, there exists a Large set of $3-DDs$ with $q+1$ groups and fixed group size of λ^d.*

Proof: We first consider the case $q \equiv 3 \pmod 4$. Consider the induced action of $\mathrm{PSL}(2,q)$ on the set of k subsets of $X := \mathbb{F}_q \cup \{\infty\}$. As seen in section 3,

$$\binom{X}{k} = \bigcup_{i=1}^{r} \mathfrak{O}_i,$$

where each $\mathfrak{O}_i$ is an orbit of this induced action and as mentioned in the introduction, $(X, \mathfrak{O}_i)$ is a $3-(q+1,k,\lambda_i)$ for some λ_i. Consider the set of designs $(X, \mathcal{A}_i)$, where $n_i = \frac{\mathrm{lcm}(\lambda_1,\lambda_2,\ldots,\lambda_r)}{\lambda_i}$ and $\mathcal{A}_i := n_i \cdot \mathfrak{O}_i$ denotes the design where each block of $\mathfrak{O}_i$ is repeated n_i times. Writing $n = \mathrm{lcm}(\lambda_1, \lambda_2, \ldots, \lambda_r)$, we have, by the choice of the n_i's, the conclusion that each $(X, \mathcal{A}_i)$ is a design $3-(q+1,k,n)$.

Now for any $d \geq \binom{q+1}{3}$, consider the set $Y := X \times I_{n^d}$, where I_n denotes the set $\{1, 2, \ldots, n\}$, and the family of 3-subsets

$$\mathcal{T} := \Big\{ \{(x,i_1),(y,i_2),(z,i_3)\}, x,y,z \in X, x,y,z \text{ distinct and } i_1,i_2,i_3 \in I_{n^d} \Big\}.$$

By the method of 'block spreading' (see [7]), there exists a partial design $(X \times I_{n^d}, \mathcal{B}_i)$ such that every element of $\mathcal{T}$ is contained in exactly one block of $\mathcal{B}_i$.[5] Moreover since each member of $\mathcal{B}_i$ has size k and contains at most one element from each set $I_x := \{x\} \times I_{n^d}$, it follows that $(X \times I_{n^d}, \{I_x : x \in X\}, \mathcal{B}_i)$ is a $3-DD$ with block size k. Moreover, since $(X, \mathfrak{O}_i)$ is a 3-design for each i, it follows that $\bigcup_{i=1}^{r} \mathcal{B}_i = \mathfrak{B}$, as claimed.

The case of $q \equiv 1 \pmod 4$ is entirely similar; of course, here each $(X, \mathfrak{O}_i)$ is not necessarily a 3-design, but, as seen in section 3, the set of orbits $\mathfrak{O} := \{\mathfrak{O}_i : 1 \leq i \leq r\}$ is partitioned into orbits for the action of $\mathbb{F}_q^*$ on $\mathfrak{O}$ and each orbit for the action of $\mathbb{F}_q^*$ gives us a simple design. The same procedure as above gives us the desired result. □

5 Concluding Remarks

Denniston([3]) first used the 3-homogeneous action of $\mathrm{PSL}(2,q)$ to obtain, in fact, Steiner 5-designs on $q+1$ points for some values of q ($q = 27, 47, 83$) which was emulated by others ([4], [8]) to obtain similar results. It is indeed desirous to see if one can suitably also obtain Steiner 5-designs for $q \equiv 1 \pmod 4$.
Coming back to an earlier point, the occurrence of blocks B_0 for which the corresponding orbit Γ satisfies $\Gamma = \theta\Gamma$ is certainly a non-trivial possibility. As seen earlier, the orbits

[5]The condition on d arises as one of the conditions of the statement in [7]. Roughly speaking, the blocks of $\mathcal{B}_i$ project onto the blocks of $\mathcal{A}_i$ and hence the name, 'Block Spreading'.

of these blocks give a 3-design and we have already seen instances with $k = 4, 5$. Ad-hoc methods allow for constructions of such blocks in many of these situations as well. For instance, suppose $q \equiv 1 \pmod{40}$ or $q \equiv 9 \pmod{40}$. Then, $q \equiv \pm 1 \pmod 5$, so that 5 is a square in $\mathbb{F}_q^*$.
Let $\alpha := \frac{3+\sqrt{5}}{2}$ (so that α satisfies the equation $\alpha^2 - 3\alpha + 1 = 0$) and $\beta := \alpha - 1$. Note that $\alpha = \frac{\alpha-1}{\alpha-2} = \frac{\beta}{\beta-1}$. Consider the block $\{0, \infty, \theta, \alpha, \beta\}$ and the map

$$\mathfrak{g} := x \to \alpha \frac{x - \theta}{x} \in \mathrm{PGL}(2, q).$$

It is easy to see that $\mathfrak{g}$ satisfies $\mathfrak{g}(\theta) = 0, \mathfrak{g}(0) = \infty, \mathfrak{g}(\infty) = \alpha, \mathfrak{g}(\theta\alpha) = \beta$ and $\mathfrak{g}(\theta\beta) = 1$. Note that if α is a non-square in $\mathbb{F}_q^*$ then $\mathfrak{g} \in \mathcal{G}(= \mathrm{PSL}(2, q))$. One could also start with $\alpha := \frac{3-\sqrt{5}}{2}$ to obtain the same conclusion.

It seems likely that the same holds for arbitrary values of k, i.e., one can always construct a block B_0 of any fixed size k for which $\Gamma = \theta\Gamma$ holds, where $\Gamma = \mathcal{G}(B_0)$. It is worth characterizing the set,

$$\mathcal{B}_G := \left\{ B \in \binom{X}{k} : \Gamma = \theta\Gamma, \Gamma = \mathcal{G}(B) \text{ and } \mathrm{Stab}(B) = G \right\}$$

for small subgroups $G \subset \mathcal{G}$. We hope to answer these questions in a satisfactory manner in the near future.

Acknowledgment

The authors would like to thank our anonymous referees for making several invaluable comments, pointing out a few errors in the proofs, notably one in the original proof of theorem 8, and suggestions to help us improve the overall presentation of the paper.

References

[1] P. J. Cameron, H. R. Maimani, G. R. Omidi, B. Tayfeh-Rezaie, 3-designs from $\mathrm{PSL}(2, q)$, to appear in *Discrete Math, 2006*.

[2] L.E.Dickson, *Linear Groups with an exposition of the Galois theory*, Dover Publications Inc., New York, 1958.

[3] R. H. F. Denniston, Some new 5-designs, *Bulletin of the London Mathematical Society*, 8(1976), 263-267.

[4] M.J. Grannell, T.S. Griggs, and R.A. Mathon, Some Steiner 5-designs with 108 and 132 points, *Journal of Combinatorial Designs*, 1(1993), 213-238.

[5] D. Hughes, On t-designs and groups, *American Joural of Mathematics*, 87(1965), 761-778.

[6] B.Huppert, *Endliche Gruppen I*, Springer Verlag, Berlin, 1967.

[7] H. Mohacsy, and Dijen Ray-Chaudhuri, A construction for group divisible t-designs with strength $t \geq 2$ and index unity, *J. Statist. Plann. Inference*, 109(2003), 167-177.

[8] W.H.Mills, A new 5-design, *Ars Combinatorica*, 6(1978), 193-195.

[9] Weixia Li, The existence of a simple $3-(30,7,15)$ Design and a simple $3-(26,12,55)$ Design, *preprint*.