Large Sets of Disjoint t-Designs

Yeow Meng Chee, Charles J. Colbourn
Steven C. Furino and Donald L. Kreher

ABSTRACT

In this paper, we show how the basis reduction algorithm of Kreher and Radziszowski [4] can be used to construct large sets of disjoint designs with specified automorphisms. In particular, we construct a (3,4,23;4)-large set which gives rise to an infinite family of large sets of 4-designs via a result of Teirlinck [6].

1 Introduction

Let $\mathcal{X}$ be a finite set of v elements called *points*. We denote by $\binom{\mathcal{X}}{k}$ the set of all k-element subsets of $\mathcal{X}$. A *t-design*, or more specifically, a *t-(v,k,λ) design*, is a pair $(\mathcal{X},\mathcal{B})$ such that $\mathcal{B} \subseteq \binom{\mathcal{X}}{k}$, and every member of $\binom{\mathcal{X}}{t}$ is contained in precisely λ members of $\mathcal{B}$. The members of $\mathcal{B}$ are called *blocks*.

The *divisibility conditions* $\lambda\binom{v-i}{t-i} \equiv 0 \pmod{\binom{k-i}{t-i}}$ for $0 \leq i < t$, provide necessary conditions for the existence of a t-(v,k,λ) design. For any given t, k, and v, we denote by $\lambda^*(t,k,v)$ the minimum positive λ that satisfies the divisibility conditions. When there is no confusion, we simply write λ^* for $\lambda^*(t,k,v)$.

A *$(t,k,v;\Lambda)$-partition* is a partition of $\binom{\mathcal{X}}{k}$ into t-(v,k,λ_i) designs $(\mathcal{X},\mathcal{B}_i)$ where $\lambda_i \in \Lambda$ and $i = 0,\ldots,N-1$. If $\Lambda = \{\lambda\}$, we say that the partition is a *uniform $(t,k,v;\lambda)$-partition*. If $\lambda = \{\lambda^*(t,k,v)\}$ the partition is said to be a *$(t,k,v;\lambda^*)$-large set*. The number of designs in a $(t,k,v;\lambda^*)$-large set is $N = \binom{v-t}{k-t}/\lambda^*$.

The motivation behind this work is the example of a (2,3,9;1)-large set with the property that each of the seven pairwise disjoint designs in the large set admits the permutation $\alpha = (0,8)(6,2,4,3,7,5)$ as an automorphism, and that the permutation $\sigma = (1,2,3,4,5,6,7)$ cyclically permutes these seven designs. Thus this large set is given by the 2-(9,3,1) design { 024, 136, 857, 018, 235, 467, 037, 268, 415, 056, 127, 348 } and its 7 images under σ.

2 Using Basis Reduction

Through out this paper let $\mathcal{X} = \{0,1,\ldots,v-1\}$ and let G be a subgroup of the symmetric group $Sym(\mathcal{X})$. We wish to construct a large set with G as an automorphism of each of its members. The subgroup G acts on the subsets of $\mathcal{X}$ in a natural way. If $S \subseteq \mathcal{X}$ and $g \in G$, then $S^g = \{x^g : x \in S\}$. The orbit of S is $S^G = \{S^g : g \in G\}$. Let $\Delta_1(G)$, $\Delta_2(G)$, $\Delta_3(G)$, $\ldots \Delta_{N_t}(G)$ and $\Gamma_1(G)$, $\Gamma_2(G)$, $\Gamma_3(G)$, $\ldots \Gamma_{N_t}(G)$ be complete lists of all orbits of t-element and k-element subsets of $\mathcal{X}$ under G respectively. For any fixed orbit representative T of $\Delta_i(G)$, the number of members $K \in \Gamma_j(G)$ such that $T \subseteq K$ is denoted by $A_{tk}(G)[i,j]$. This number, $A_{tk}(G)[i,j]$, is independent of the choice of T. In [3] the following observation is made.

A t-(v,k,λ) design $(\mathcal{X},\mathcal{B})$ exists with G as an automorphism group if and only if there is a $(0,1)$-vector U satisfying the matrix equation

$$A_{tk}(G)U = \lambda J, \tag{1}$$

where $J = [1,1,1,\ldots,1]^T$.

Of the several methods for solving equation (1), the approach taken by Kreher and Radziszowski [4] has been particularly successful. It is described below.

Let $A = \{a_1,\ldots,a_m\}$ be a set of integer valued n-dimensional vectors. The *lattice* generated by A is the set of all integer linear combinations of $a_1,\ldots,a_m$, and is denoted by $\mathcal{L}(A)$. We say that $a_1,\ldots,a_m$ is a basis for $\mathcal{L}(A)$. The following observation is crucial in the approach of Kreher and Radziszowski.

$A_{tk}(G)U = d\cdot\lambda J$ for some integer d if and only if $[U^T,0,\ldots,0]^T$ is in the lattice $\mathcal{L}(M)$ generated by the columns M of the matrix $\begin{bmatrix} I & 0 \\ A_{tk}(G) & -\lambda J \end{bmatrix}$.

Since the complement of a t-design is a t-design, we may assume, without loss of generality, that $\|U\|^2 \le N_k(G)/2$. It follows that the length of $[U^T 0,0,\ldots,0]^T$ is considerably shorter than the lengths of other vectors in $\mathcal{L}(M)$. Kreher and Radziszowski developed a basis reduction algorithm that finds vectors in the lattice $\mathcal{L}$ whose lengths are as short as they can make them. In fact, their algorithm very often finds a (0,1)-solution to $A_{tk}(G)U = \lambda J$. Several thousand new t-designs have been found with this algorithm [2].

We now return to the construction of large sets. Let $G \le H \le Sym(\mathcal{X})$. The *fusion matrix*, denoted $F_k(G,H)$, is the $N_k(H)$ by $N_k(G)$ matrix defined by:

$$F_k(G,H)[i,j] = \begin{cases} 1 & \Gamma_i(G) \subseteq \Gamma_j(H); \\ 0 & \text{otherwise.} \end{cases}$$

Now suppose we want to find a $(t,k,v;\lambda^*)$-large set of disjoint designs $\mathcal{D} = \{(\mathcal{X},\mathcal{B}_i) | i = 0,\ldots,N-1\}$ such that each of the designs $(\mathcal{X},\mathcal{B}_i)$, $0 \le i \le N-1$, has $G \le Sym(\mathcal{X})$ as an automorphism group. Suppose further that we want a permutation $\sigma \in Sym(\mathcal{X})$ to cyclically permute the designs in $\mathcal{D}$. In particular σ^i, $1 \le i < |\sigma|$, does not fix any blocks. Let $H = \langle G,\sigma\rangle$ and consider an orbit $\Gamma_l(H)$. It is the union of some collection $\Gamma_{j_1}(G),\ldots,\Gamma_{j_q}(G)$ of orbits of k-element subsets under G. We observe that

for any $1 \le n \le q$, and for all $1 \le i < |\sigma|$ we have

1. $(\Gamma^{(k)}_{j_n}(G))^{\sigma^i} \subseteq \Gamma^{(k)}_l(H)$ *and*

2. $(\Gamma_{j_n}^{(k)}(G))^{\sigma^i} \cap \Gamma_{j_n}^{(k)}(G) = \emptyset$.

It follows that if we find a design $(\mathcal{X}, \mathcal{B})$ that contains exactly one orbit of k-element subsets from each fusion class, then $\mathcal{B}^{\sigma}$ is disjoint from $\mathcal{B}$. Hence, $\mathcal{D} = \{(\mathcal{X}, \mathcal{B}^{\sigma^j}) | j = 0, \ldots, \binom{v-t}{k-t}/\lambda^* - 1\}$ is a large set of disjoint designs. We call such large set a *cyclic large set with shifter* σ. The above discussion is summarize in the following theorem.

Theorem 1 *There exists a cyclic $(t, k, v; \lambda^*)$-large set $\mathcal{D}$ with G as an automorphism group and shifter σ if there is a $(0,1)$-vector U satisfying the matrix equation*

$$\begin{bmatrix} A_{tk}(G) \\ F_k(G, H) \end{bmatrix} U = \begin{bmatrix} \lambda^* J \\ J \end{bmatrix} \tag{2}$$

where $H = \langle G, \sigma \rangle$.

The approach we take to solve equation (2) is to apply the basis reduction algorithm of Kreher and Radziszowski as described earlier to the lattice generated by the columns of the matrix

$$M = \begin{bmatrix} I & 0 \\ A_{tk}(G) & -\lambda^* J \\ F_k(H, G) & -J \end{bmatrix}.$$

Using this method, we were able to construct a cyclic (3,5,13;15)-large set. This large set consists of designs having $G = \langle \alpha, \beta \rangle$ where $\alpha = (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12)$, and $\beta = (1, 8, 12, 5)(2, 3, 11, 10)(4, 6, 9, 7)$ as an automorphism group. The orbit representatives for the blocks in one of the three designs in the large set are listed below.

0 2 3 4 5	0 1 2 4 5	0 2 4 5 6	0 2 4 7 8	0 1 2 4 8
0 1 4 5 9	0 1 2 6 9	0 2 3 7 9	0 1 2 6 10	0 2 4 7 10

Applying the permutation

$$\sigma = (1, 3, 9)(2, 6, 5)(4, 12, 10)(7, 8, 11)$$

twice generates the other two designs.

The requirement that the desired large set is cyclic is often too strong a condition for us to be able to find a solution. In particular, this restriction yields a large set of *isomorphic* designs. In this section, we propose two approaches for for finding large sets when no additional requirements such as cyclic are made.

It is easy to see that constructing a $(t, k, v; \lambda^*)$-large set of disjoint designs, each with G as an automorphism group, is equivalent to partitioning the columns of the matrix, $A_{tk}(G)$, into $\binom{v-t}{k-t}/\lambda^*$ classes, so that the row sums across the columns in each class is equal λ^*. Our first approach works as follows. We find a (0,1)-vector U solving equation (1) using the basis reduction algorithm of Kreher and Radziszowski. The columns corresponding to the (0,1)-vector U are then removed from $A_{tk}(G)$. This procedure is repeated until one of two things happens :

1. We get a partition of the columns of $A_{tk}(G)$ into classes corresponding to a $(t, k, v; \lambda^*)$-large set.

2. We get a partition of the columns of $A_{tk}(G)$ into classes corresponding to a $(t, k, v; \{\lambda^*, \lambda\})$-partition, $\lambda > \lambda^*$.

Our second approach is again to use the basis reduction algorithm of Kreher and Radziszowski to repeatedly generate a set $\mathcal{S}$ of many distinct (0,1)-vectors U solving equation (1). This is achieved by randomly ordering the basis vectors at each iteration so that each time after reducing the basis, different short vectors appear in the basis. An *independent set* in $\mathcal{S}$ is a set of pairwise orthogonal vectors in $\mathcal{S}$. It is not hard to see that $\mathcal{S}$ contains a $(t, k, v; \lambda^*)$-large set if and only if there is an independent set of size $\binom{v-t}{k-t}/\lambda^*$ in $\mathcal{S}$. We can choose $\mathcal{S}$ to be not too large so that we can check $\mathcal{S}$ for a maximum independent set in reasonable time.

Using these two approaches, sometimes in combination, we were able to construct the (3,4,23;4)-large set and a (4,6,14;15)-large set appearing in Table I and Table II.

The (3,4,23;4)-large set is of particular interest because of a recent result of Teirlinck [6]. Teirlinck proved that $(4, 5, 20u + 4; \lambda^*)$-large sets exist for all positive integers u that are relatively prime to 30 if there exists a (3,4,23;4)-large set. Hence we now have the following theorem.

Theorem 2 *There exist* $(4, 5, 20u + 4; \lambda^*)$*-large sets for all positive integers* u *that are relatively prime to 30.*

This family of $(4, 5, 20u + 4; \lambda^*)$-large sets is one of the only two non-trivial infinite families of $(t, k, v; \lambda^*)$-large sets known for $t \geq 4$.

3 Using t-Homogeneous Groups

For notation, definitions and theorems on permutation groups the reader is directed to the book by Wielandt [7] and also to the book by Biggs and White [1]. Here we introduce some of the notation and concepts that are relevant to this paper. A subgroup $G \leq Sym(\mathcal{X})$ is said to be *t-homogeneous* if the orbit of any t-element subset is all of the t-element subsets. In this case, it is easy to see that the orbit B^G of any k-element subset, $B \subseteq \mathcal{X}$, is a t-(v, k, λ) design, where $\lambda = |G|\binom{k}{t} / |G_B|\binom{v}{t}$ and $G_B = \{g \in G : B^g = B\}$. Thus, the the complete list $\mathcal{D}$ of all the orbits of k-element subsets partition $\binom{\mathcal{X}}{k}$ into t-designs. In particular, if $|G_B| = 1$ for every $B \subseteq \mathcal{X}$, $|B| = k$, then $\mathcal{D}$ is a uniform $(t, k, v; \lambda)$-partition with $\lambda = |G|\binom{k}{t}/\binom{v}{t}$.

Given a subgroup action $G \leq Sym(\mathcal{X})$, a permutation $g \in G$ having e_i cycles of length c_i is said to have *type*

$$type(g) = \prod_{i=1}^{v} c_i^{e_i}.$$

We make the following observation.

Table I: A (3,4,23;4)-large set.

Group generators				
$\alpha = x \mapsto x + 1 \pmod{23}$				
$\beta = x \mapsto 5x \pmod{23}$				
Orbit representatives				
design 1	design 2	design 3	design 4	design 5
0 1 3 12	0 1 3 6	0 1 3 4	0 1 2 3	0 1 4 5
0 1 3 8	0 1 3 13	0 1 2 5	0 1 3 5	0 1 3 7
0 1 2 10	0 1 3 15	0 1 2 7	0 1 3 18	0 1 3 14
0 1 3 21	0 1 4 20	0 1 3 10	0 1 3 19	0 1 3 22

Table II: A (4,6,14;15)-large set.

Group generators					
$\alpha = (1,2,3,4,5,6,7,8,9,10,11,12,13)$					
$\beta = (2,4,10)(3,7,6)(5,13,11)(8,9,12)$					
Orbit representatives					
design 1		design 2		design 3	
1 2 3 5 8 10	0 1 2 3 4 5	1 2 3 5 7 8	1 2 3 4 5 6	1 2 3 4 5 7	0 1 2 3 5 6
0 1 2 3 5 7	1 2 3 5 6 7	0 1 2 4 5 6	0 1 2 3 4 7	0 1 2 4 5 7	0 1 2 3 5 8
1 2 4 5 6 7	0 1 2 4 6 8	0 1 2 4 6 7	1 2 3 5 6 8	0 1 2 3 4 8	0 1 2 3 6 8
0 1 2 3 5 9	0 1 2 6 7 8	1 2 3 4 5 8	0 1 2 3 7 8	0 1 2 4 7 8	0 1 2 4 6 9
1 2 3 4 5 9	0 1 2 4 5 9	1 2 3 4 7 8	0 1 2 3 8 9	0 1 2 3 7 9	0 1 2 3 4 10
1 2 3 4 7 9	1 2 4 6 7 9	1 2 3 5 6 9	1 2 4 6 7 8	1 2 3 7 8 9	1 2 4 6 8 9
1 2 3 5 8 9	1 2 3 4 8 9	0 1 2 3 4 9	1 2 3 5 7 9	1 2 4 7 8 9	1 2 3 5 8 11
0 1 2 3 8 10	1 2 3 4 7 10	1 2 4 5 7 9	1 2 3 4 8 10	1 2 3 4 5 11	1 2 4 5 9 10
0 1 2 4 8 10	0 1 2 3 4 11	1 2 4 7 8 10	0 1 2 3 5 11	1 2 3 4 7 11	1 2 4 6 7 11
1 2 3 4 9 10	1 2 3 5 6 11	1 2 4 5 6 11	1 2 3 5 7 11	0 1 2 3 7 12	0 1 2 3 4 12
0 1 2 4 6 11	1 2 3 4 5 12	1 2 3 4 9 11	0 1 2 3 9 11	1 2 3 5 9 11	1 2 3 5 6 12
0 1 2 4 5 12	1 2 4 5 6 12	0 1 2 3 5 12	0 1 2 4 6 12	1 2 3 5 7 12	1 2 4 5 7 12
1 2 3 5 8 12	1 2 3 7 9 12	1 2 3 4 7 12	0 1 2 3 5 13	1 2 4 6 7 12	1 2 3 5 6 13
1 2 3 5 7 13		1 2 3 4 9 12		1 2 3 5 8 13	

$|G_B| \neq 1$ *for some k-element subset* $B \subseteq \mathcal{X}$ *if and only if there is a* $g \in G$ *with* $type(g) = \prod_{i=1}^{v} c_i^{e_i}$ *such that k can be written as* $k = \sum_{i=1}^{v} f_i c_i$ *with each* $f_i \leq e_i$, $i = 1, \ldots, v$.

Thus, knowing the types of all the elements of G is sufficient to decide when the orbits of k-element subsets under G is a uniform $(t, k, v; \lambda)$-partition with $\lambda = |G|\binom{k}{t}/\binom{v}{t}$. Using this observation, we present two examples.

3.1 $t = 2$

For this example, we consider the class of groups known as the *affine special linear groups*. Let $\mathcal{X} = GF(p^n)$ be the finite field of order $v = p^n$, p a prime. Then the affine special linear group of order v is

$$ASL(v) = \{x \mapsto ax + b : a, b \in \mathcal{X} \text{ and } a \text{ is a nonzero square}\}.$$

It is an easy exercise to show that $ASL(v)$ acting on $\mathcal{X}$ is 2-homogeneous, for v a prime congruent to 3 modulo 4. Using elementary group theory, the distribution of the types of elements in $ASL(v)$ can easily be obtained. These are displayed in Table III and the relevant theorem follows.

Table III

$type(g)$	Number
1^v	1
p^n	$v-1$
$1 \cdot d^{(v-1)/d}$	$v\phi(d)$

Theorem 3 *Let v be a prime congruent to 3 modulo 4,* $2 < k < v$, *let* $\mathcal{X} = GF(v)$ *and let* $\mathcal{D}$ *be a complete list of orbits of k-element subsets under* $ASL(v)$.

1. *If* $gcd(k, v) = gcd(k(k-1), (v-1)/2) = 1$, *then* $\mathcal{D}$ *is a uniform* $(2, k, v; \binom{k}{2})$-*partition.*

2. *If* $gcd(k(k-1), v(v-1)) = 2$, *then* $\mathcal{D}$ *is a* $(2, k, v; \binom{k}{2})$-*large set.*

Proof. Part (1) follows from the observation and part (2) adds only the condition that $gcd(k-1, v) = 1$. The divisibility conditions then give $\lambda^* = \binom{k}{2}$ and thus the result holds. ∎

3.2 $t = 3$

We now focus our attention on the *projective special linear group* $PSL_2(v)$, where $v = p^n$ is a prime power. Recall that $PSL_2(v)$ is the set of all 2 by 2 matrices over $GF(v)$ whose determinant is a nonzero square. It is also isomorphic to the *linear fractional group* $G = LF(v)$ which is the set of all mappings

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

such that $a, b, c, d \in GF(v)$ and $ad - bc$ is a nonzero square. If we define $a/\infty = 0$ and $a/0 = \infty$ for all $a \in GF(v)$, $a \neq 0$, then it is easy to see that G acts transitively on $\mathcal{X} = GF(v) \cup \{\infty\}$, the so-called *projective line*. ¿From this representation of $PSL_2(v)$, it is not difficult to establish the distribution of types of elements in G. This distribution is given in Table IV for the case $v \equiv 3 \pmod 4$.

Table IV

$type(g)$	Number
1^{v+1}	1
$1 \cdot p^{v/p}$	$v^2 - 1$
$1^2 \cdot 2^{(v-1)/2}$	$(v^2 - v)/2$
$1^2 \cdot d^{(v-1)/d}$	$\phi(d)(v^v + v)/2$
$d^{(v+1)/d}$	$\phi(d)(v^v - v)/2$

By applying the Cauchy-Frobenius-Burnside lemma, it is easy to show that when $v \equiv 3 \pmod 4$, $PSL_2(v)$ acts 3-homogeneously on $\mathcal{X}$, the projective line. Thus, by Table IV and careful examination of the divisibility conditions, we have

Theorem 4 *Let $v = p^n + 1$ for some prime power $p^n \equiv 3 \pmod 4$, $3 < k < v$ and let G be the representation of $PSL_2(v)$ acting on the projective line $\mathcal{X}$.*

1. *If $gcd(k(k-1), p) = gcd(k(k-1)(k-2), (v-1)/2) = gcd(k, (v+1)/2) = 1$, then the orbits of k-element subsets of $\mathcal{X}$ under G form a uniform $(3, k, v; 3\binom{k}{3})$-partition.*

2. *If in addition to the hypothesis of (1) we have*

   - *For k even.* $gcd(k-2, v-1) = 2$ *and* $gcd(k-1, v(v-1)/2) = gcd(k, (v+1)v(v-1)/2) = 1$
   - *For k odd.* $gcd((k-1)(k-2), v(v-1)) = 2$ *and* $gcd(k-2, v-1) = gcd(k, (v+1)v(v-1)/2) = 1$

   then the orbits of k-element subsets of $\mathcal{X}$ under G form a $(3, k, v; 3\binom{k}{3})$-large set.

The applicability of theorems 3 and 4 in constructing large sets is indicated in the tables below, showing all large sets of 2-designs with $v \leq 24$ and 3-designs with $v \leq 100$ that are constructed:

Table of 2-designs

2-(11,3,3)	2-(11,4,6)	2-(19,5,10)	2-(19,8,28)
2-(23,3,3)	2-(23,4,6)	2-(23,5,10)	2-(23,6,15)
2-(23,7,21)	2-(23,8,28)	2-(23,9,36)	2-(23,10,45)

Table of 3-designs

3-(44,7,5)	3-(44,19,969)	3-(68,7,35)	3-(68,11,15)
3-(68,31,4495)	3-(80,19,969)	3-(80,23,1771)	

Note: Interested persons can get electronic access to lists of the assorted starter blocks by sending electronic mail to D. L. Kreher or to C. J. Colbourn.

Acknowledgements: This work was done while YMC was holding a National Computer Board (Singapore) Postgraduate Scholarship. CJC was supported from NSERC of Canada grant A0579.

References

[1] N. L. Biggs and A. T. White, *Permutation Groups and Combinatorial Structures* (Cambridge University Press: London Mathematical Society Lecture Note Series **33**, 1979).

[2] D. de Caen, Y. M. Chee, C. J. Colbourn, E. S. Kramer and D. L. Kreher, "New Simple t-Designs", *J. Combin. Math. Combin. Comput.*, to appear.

[3] E. S. Kramer and D. M. Mesner, "t-Designs on Hypergraphs", *Discrete Mathematics* **15** (1976) 263-296.

[4] D. L. Kreher and S. P. Radziszowski, "Finding Simple t-Designs by Basis Reduction", *Congressus Numerantium* **55** (1986) 235-244.

[5] K. T. Phelps, "A Class of Large Sets of Steiner Triple Systems of Order 15", *Discrete Mathematics*, to appear.

[6] L. Teirlinck, "Locally Trivial t-Designs and t-Designs Without Repeated Blocks", *Discrete Mathematics* **77** (1989).

[7] H. Wielandt, *Finite Permutation Groups* (New York and London: Academic Press, 1964).

Author Addresses:

Yeow Meng Chee
Dept. of Computer Science
University of Waterloo
Waterloo, Ontario N2L 3G1
CANADA

Charles J. Colbourn
Dept. of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario N2L 3G1
CANADA

cjcolbourn%hippo.waterloo.edu@watdcs.uwaterloo.ca

Steven C. Furino
St. Jerome's College
University of Waterloo
Waterloo, Ontariao N2L 3G1
CANADA

Donald L. Kreher
Dept. of Mathematics
University of Wyoming
Laramie, Wyoming 82071
U.S.A.

kreher@corral.uwyo.edu