New t-Designs Found by Basis Reduction

Donald L. Kreher[*] *and Stanisław P. Radziszowski*[*]

Rochester Institute of Technology

School of Computer Science and Technology

ABSTRACT

At the Seventeenth Southeastern International Conference on Combinatorics, Graph Theory and Computing we presented a new algorithm for finding t-(v,k,λ) designs without repeated blocks. The central idea of the algorithm was basis reduction. This year we report on the success we have had using it. Namely, the construction of several new simple t-designs including a 4-(12,6,10) design, a 6-(14,7,4) design and 5-(28,6,λ) designs for each admissible λ, $\lambda \neq 1$ (or 22).

1. Introduction

This paper is an expository account of the new t-designs we found using the method we introduced at the Seventeenth Southeastern International Conference on Combinatorics, Graph Theory and Computing, [8]. This method is the first use of basis reduction for finding t-designs. The two works that inspired our development of basis reduction are the 1985 paper of Lagarias and Odlyzko [13] in which they use a similar method to attack the subset sum problem and the 1973 paper of Kramer and Mesner [7] in which they give an algebraic formulation that expresses when a t-design can have an automorphism group.

Recall that a t-(v,k,λ) *design* (X,B) is a family of k-subsets B called *blocks* from a v-set X of *points* such that every t-subset $T \subseteq X$ is contained in exactly λ of the blocks in B. It is said to be *simple* or to have *no repeated blocks* if all of the members of B are distinct. A

[*] Both authors research was supported by the National Science Foundation.

group $G \leq Sym(X)$ is an *automorphism group* of a t-(v,k,λ) design (X,B) if every $g \in G$ preserves B. That is for all $g \in G$ and $K \in B$ the k-set $K^g = (x^g : x \in K)$ is also a block in B. Here x^g denotes the image of x under the permutation g, and K^g is said to be the image of the k-set B. The collection $\Gamma = K^G = (K^g : g \in G)$ is said to be a G-orbit. Clearly, G is an automorphism group of a t-(v,k,λ) design (X,B) if and only if B is a union of G-orbits. The *full automorphism group* of a t-(v,λ) design (X,B) is the set of all automorphism in $Sym(X)$ preserving B. A t-$(v,k\lambda)$ design whose full automorphism group is the trivial group is said to be *rigid*.

Given a group $G \leq Sym(X)$ and integers $0 < t < k < v = |X|$, let $\Delta_1, \cdots, \Delta_i, \cdots, \Delta_{N_t}$ and $\Gamma_1, \cdots, \Gamma_j, \cdots, \Gamma_{N_k}$ be the G-orbits of t and k-subsets, and define the N_t by N_k matrix $A_{tk} = A_{tk}(G|X)$ to have $(i,j)^{th}$-entry equal to $|(K \in \Gamma_j : K \supseteq T)|$ where $T \in \Delta_i$ is any fixed representative. See figure 1.

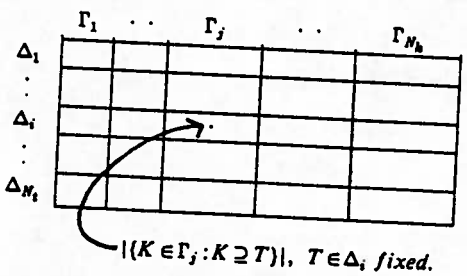

Figure 1: The A_{tk} matrix belonging to G acting on X.

Then the following 1973 observation of Kramer and Mesner is clear.

A t-(v,k,λ) design exists with $G \leq Sym(X)$ as an automorphism group if and only if there is a (0,1)-solution U to the matrix equation

$$A_{tk} U = \lambda J_{N_t}, \tag{1}$$

where $J_{N_t} = [1,1,1,\ldots,1]^T$.

In [8] we gave the following method for finding a solution to equation (1). We let L be the $N_k + 1$ dimensional integer lattice spanned by the columns of the matrix below

$$\begin{bmatrix} I_{N_k} & 0 \\ A_{tk} & -\lambda J_{N_t} \end{bmatrix} \tag{2}$$

Let 0_{N_t} be the N_t-dimensional zero vector. Then as pointed out in [8] the following proposition and discussion is clear.

PROPOSITION 1: *$A_{st}U = d \cdot \lambda J_{N_t}$ for some integer d if and only if $[U,0_{N_t}]^T \in L$.*

Thus to find a (0,1)-solution U to $A_{st}U = \lambda J_{N_t}$ we need only look for a linear combination $U = [U,0_{N_t}]^T$ of the columns of matrix (2) such that U is a (0,1)-vector. If $U \neq J_{N_t}$ then we will have found a t-$(v,k,d \cdot \lambda)$ design for some positive integer d. Note that since the complement of a design is a design then the search can be restricted to $\|U\|^2 \leq n/2$. That is, U is a particular short vector in L.

The algorithm presented in [8] tries to find in L a new basis all of whose vectors are as short as we can make them. We refer to this method as *basis reduction* and the new basis as a *reduced basis*. Apparently, if a solution to (1) exists, it is likely that it will appear in a reduced basis. In fact several new simple t-designs all with $t \geq 4$ were found using this method [9,10,11]. In the sections that follow we give a summary of the new designs and some open problems connected with them.

2. 5-(28,6,λ) designs from $PSL_2(27)$.

In figure 2 appears the $A_{s,6}$ matrix belonging to $PSL_2(27)$. Solutions giving a t-(v,k,λ) design are also shown for each λ, $2 \leq \lambda \leq 11$. A detailed description of these designs appears in [10]. The only open parameter situation with $t = 5$, $k = 6$ and $v = 28$ is thus $\lambda = 1$, since the complement of a t-(v,k,λ) design is a t-$(v,k,23-\lambda)$ design. As was pointed out by Dennis-ton in [6], $PSL_2(27)$ cannot be the automorphism group of a 5-(28,6,1) design hence we state the following problem.

PROBLEM 1: Does there exist a 5-(28,6,1) design?

3. Cyclic 5-(13,6,4) designs and their extensions to 6-(14,7,4) designs

Here we give a summary of what is known about the cyclic 5-designs found in [9] and announce some new 5-(13,6,4) designs that have trivial automorphism group.

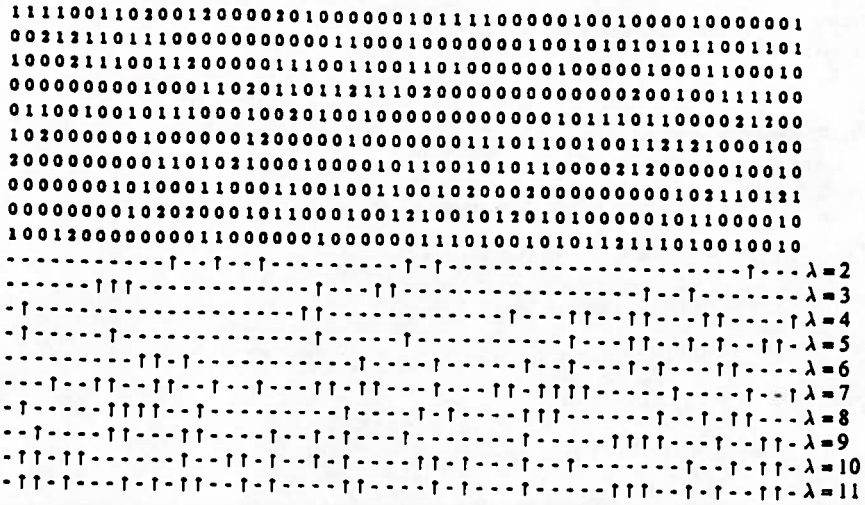

Figure 2: The $A_{5,6}$ matrix belonging to $PSL_2(27)$ acting on the projective line and solutions.

If $X = \mathbb{Z}_{13}$ and $G = \langle x \to x + 1 \rangle$ then G is cylic and the A_{56} matrix belonging to G is 99 by 132 With some modifications our basis reduction algorithm found that there are exactly two non-isomorphic solutions. A complete description of these designs can be found in [9]. Also in the same paper it was established that these two designs are nonisomorphic and each have full automorphism group cyclic of order 13. Furthermore they partition all of the 6-subsets. Using Alltop's Theorem [1] any 5-(13,6,4) design (X,B) can be extended to a 6-(14,7,4) design $(X \cup \{\infty\}, B' \cup B'')$ where

$$B' = \{K \cup \{\infty\} : K \in B\}$$
$$B'' = \{X - K : K \notin B\}$$

These two 6-designs each have full automorphism group cylic of order 13 and they partition all of the 7-subsets.

In this paper we would like to point out that the extension from 5-(13,6,4) designs to 6-(14,7,4) designs is unique. Furthermore, if $(X \cup \{\infty\}, B' \cup B'')$ is the extension of a cyclic 5-(13,6,4) design (X,B), then the derived designs with respect to any point $x \in X$ have trivial automorphism group. So we state and prove the following theorems.

THEOREM 1: *If (X,B) is a 5-(13,6,4) design it has a unique extension to a 6-(14,7,4) design.*

Proof: Let 1 denote the trivial group and suppose that (X,B) is a 5-(13,6,4) design. Then there is a (0,1) solution U to $A_{56}(1|X)U = 4J_{N_5}$, where $N_5 = \binom{13}{5}$. Furthermore if $X' = X \cup (\infty)$, then arranging the rows and columns so that those sets containing ∞ appear first it is easy to see that

$$A_{67}(1|X') = \begin{bmatrix} A_{56}(1|X) & 0 \\ I_{N_6} & A_{67}(1|X) \end{bmatrix}$$

where I_{N_6} is the N_6 by N_6 identity matrix, $N_6 = \binom{13}{6}$, and 0 denotes the matrix of all zeros. Thus a 5-(13,6,4) design has an extension to a 6-(14,7,4) design if and only if there is a (0,1) vector V such that

$$A_{67}(1|X')\begin{bmatrix} U \\ V \end{bmatrix} = \begin{bmatrix} 4J_{N_5} \\ 4J_{N_6} \end{bmatrix}$$

In particular V must solve

$$U + VA_{67}(1|X) = 4J_{N_6} \tag{3}$$

Observe that $6 + 7 = 13 = |X|$. Hence, by lemma 10 of [12] $A_{67}(1|X)$ has an inverse. Thus V is completely determined by U. Whence, since Alltop's construction [1] provides a (0,1) solution V to (3), any 5-(13,6,4) design has an extension which is unique. □

Recall that if (X,B) is a t-(v,k,λ) design then for each $x \in X$ the *derived design with respect to* x is the $(t-1)$-$(v-1,k-1,\lambda)$ design (Δ,B_x), where $\Delta = X-\{x\}$ and $B_x = \{K-\{x\} : K \in B\}$. If $G \leq Sym(X)$ fixes a subset $\Delta \subseteq X$, then each permutation $g \in G$ induces a permutation g^Δ on Δ and we denote the totality of g^Δ's formed by G^Δ. Note that the stabilizer in G of x is G_x and fixes the set $\Delta = X-\{x\}$.

THEOREM 2: *Let (X,B) be a 6-(14,7,4) design with full automorphism group G. Then for each $x \in X$, the derived design with respect to x has full automorphism group G_x^Δ where $\Delta = X-\{x\}$.*

Proof: Let (X,B) be a 6-(14,7,4) design. Fix $x \in X$, set $\Delta = X-\{x\}$ and let H be the full automorphism group of the the derived design (Δ,B_x) of (X,B) with respect to x. It is easy to see

that

$G_x^{\Delta} \supseteq H$. However, we note by theorem 1 that (X,B) is the unique extension of (Δ,B_x) so it must be obtained by Alltop's construction [1]. That is

$$B = \{K \cup \{x\} : K \in B_x\} \cup \{\Delta - K : K \notin B_x\}.$$

Whence, if $\alpha \in H$ then $(\Delta - K)^{\alpha} = \Delta - (K^{\alpha})$ and then the extension of α to $\hat{\alpha}: X \to X$ given by $y^{\hat{\alpha}} = y^{\alpha}$ if $y \neq x$ and $x^{\hat{\alpha}} = x$ must preserve B. Thus the mapping $\alpha \to \hat{\alpha}$ is an isomorphism: $H \cong G_x$ and $H = G_x^{\Delta}$ as claimed. □

If (X,B) is a t-(v,k,λ) design then $(X,\bar{B})$ where $\bar{B} = \binom{X}{k}$ is a t-$(v,k,\binom{v-t}{k-t}-\lambda)$ design and is called the *complementary design of (X,B)*. We note that the complementary design of a 6-(14,7,4) design is also a 6-(14,7,4) design.

THEOREM 3: *Let (X,B) be a 6-(14,7,4) design and let $(X,\bar{B})$ be its complementary design. Then for each $x \in X$ any isomorphism $\alpha:(X-\{x\},B_x) \to (X-\{x\},\bar{B}_x)$ lifts to an isomorphism $\hat{\alpha}:(X,B) \to (X,\bar{B})$.*

Fix $x \in X$, set $\Delta = X - \{x\}$ and suppose $\alpha:(\Delta,B_x) \to (\Delta,\bar{B}_x)$ is an isomorphism. Define $\hat{\alpha}: X \to X$ by $y^{\hat{\alpha}} = y^{\alpha}$ if $y \neq x$ and $x^{\hat{\alpha}} = x$. Then $\hat{\alpha}$ is a isomorphism from (X,B) to $(X,\bar{B})$ since by Alltop's construction and theorem 1 we have

$$B = \{K \cup \{x\} : K \in B_x\} \cup \{\Delta - K : K \notin B_x\}.$$
$$\bar{B} = \{K \cup \{x\} : K \notin \bar{B}_x\} \cup \{\Delta - K : K \in \bar{B}_x\}.$$

□

COROLLARY: *The 6-subsets of a 13-set can be partitioned into two nonisomorphic rigid 5-(13,6,4) designs.*

Proof: Let $\Delta = \mathbb{Z}_{13}$, $X = \Delta \cup \{\infty\}$ and consider the two complementary 6-(14,7,4) designs (X,B) and $(X,\bar{B})$ found in [9]. These two designs are nonisomorphic with full automorphism group cyclic of order 13 generated by the permutation α which is $x \to x + 1$ on Δ and fixes ∞. Now fix $x \in \Delta$ and apply Theorems 2 and 3. The result now follows. □

This section suggests the following problems.

PROBLEM 2: Does there exist a way to partition the 6-subsets of a 13-set into two *isomorphic* designs?

PROBLEM 3: Does there exist a shorter description of the 6-(14,7,4) designs found in [9]?

4. A 1-rotational 4-(12,6,10) design.

Using basis reduction we were also able to establish the existence of 1-rotational simple 4-(12,6,10) designs. A t-(v,k,λ) is said to be *d-rotational* if it has an automorphism that fixes exactly 1 point and has d $\left\lfloor \frac{v-1}{d} \right\rfloor$-cycles on the remaining points. The orbit representatives for a 1-rotational 4-(12,6,10) design appear in figure 3.

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

Figure 3: These 30 orbit representatives when developed into 11·30 = 330 6-sets using the permutation $x \to x + 1$ modulo 11 give a 4-(12,6,10) design.

5. Table of all small t-designs: $v < 15$ and $t > 3$

In table 1 is a list of all t-(v,k,λ) designs with $v < 15$ and $t > 3$ including the designs discussed above. The entry for $\underline{b}$ is the number of blocks in the design with minimum λ if it were to exist. All other number of blocks can easily be calculated from this.

Table I

t	k	v	b	λ	remarks
4	5	11	66	1	Derived design of 5-(12,6,1)
				2	Derived design of 5-(12,6,2)
				3	Derived design of 5-(12,6,3)
4	5	12	396	4	Denniston [5]
4	6	12	66	2	Does not exist Dehon and Oberschelp [14]
				4	5-(12,6,1) as 4-design
				6	Unknown
				8	5-(12,6,2) as 4-design
				10	Kreher and Radziszowski [11]
				12	5-(12,6,3) as 4-design
				14	extension of 3-(11,5,14)
5	6	12	132	1	Witt [15]
				2	Witt two disjoint copies of $\lambda=1$ [15]
				3	Brouwer [2]
4	5	13	429	3	Derived design of 5-(14,6,3)
4	6	13	286	6	Unknown
				12	Kramer & Mesner [7]
				18	5-(13,6,4) as 4-design
5	6	13	858	4	Kreher and Radziszowski [9]
4	6	14	1001	15	Brouwer [2]
4	7	14	572	20	Unknown
				40	5-(14,7,12) as 4-design
				60	Brouwer [2]
5	6	14	1001	3	Brouwer [2]
5	7	14	572	6	Unknown
				12	Kramer & Mesner [7]
				18	6-(14,7,4) as 4-design
6	7	14	1716	4	Extension of 5-(13,6,4)

Brouwer knows it MR 89

We note that if a 5-(14,7,6) design were to exist, then it is a 4-(14,7,20) design and its derived design is a 4-(13,6,6) design. Consequently to complete this table one need only establish the existence of a 5-(14,7,6) design and a 4-(12,6,6) design. Thus we have our next two problems.

PROBLEM 4: Does there exist a 5-(14,7,6) design?

PROBLEM 5: Does there exist a 4-(12,6,6) design?

6. Summary

The results and problems presented in this paper are summarized below.

New Designs

- 5-(28,6,λ) designs for each $\lambda = 2, 3, 4, \ldots, 21$.
- Two non-isomorphic cyclic 5-(13,6,4) designs.
- Two non-isomorphic rigid 5-(13,6,4) designs.
- Two non-isomorphic 1-rotational 6-(14,7,4) designs.
- A 1-rotational 4-(12,6,10) design.

Problems

PROBLEM 1: Does there exist a 5-(28,6,1) design?

PROBLEM 2: Does there exist a way to partition the 7-subsets of a 14-set into two *isomorphic* designs?

PROBLEM 3: Does there exist a shorter description of the 6-(14,7,4) designs found in [9]?

PROBLEM 4: Does there exist a 5-(14,7,6) design?

PROBLEM 5: Does there exist a 4-(12,6,6) design?

We add one aditional general problem.

PROBLEM 6: Under what conditions will basis reduction always be able to find a (0,1)-solution to the Diophantine system $AU = B$?

We are now in the progress of trying to answer these problems and invite the reader to do the same. We wish you the best of luck.

Acknowledgements

We are indebted to Alexander Rosa for his help in verifying the acuracy of Table I.

References

1. W. O. Alltop, Extending t-designs *J. Combinatorial Theory Series A*, Vol. 18 (1975), 177-186.
2. A.E. Brouwer, The t-designs with $v < 18$, *Stichting Mathematisch Centrum* zn 76/77.
3. A.E. Brouwer, A new 5-design, *Math. Centre report* ZW 97, Amsterdam, May 1977.
4. M. Dehon, Non-existence d'un 3-design de parameters $\lambda = 2, k = 5$ et $v = 11$, *Discr. Math.*, 15 (1975) 23-25.
5. R.H.F. Denniston, A small 4-design, *Annals of Discrete Mathematics*, 18 (1983) 291-294.
6. R.H.F. Denniston, The Problem of the Higher Values of t, *Annals of Discrete Mathematics*, 7 (1980) 65-70.
7. E.S. Kramer and D. Mesner, t-designs on Hypergraphs, *Discr. Math.* 15 (1976) 263-296.
8. D.L. Kreher and S.P. Radziszowski, Finding Simple t-Designs by Using Basis Reduction, *Congressus Numerantium, Proceedings of the 17-th Southeastern Conference on Combinatorics, Graph Theory and Computing*, 55 (1986) 235-244.
9. D.L. Kreher and S.P. Radziszowski, The Existence of Simple 6-(14,7,4) designs *Journal of Combinatorial Theory Series A*, 43, No. 2 (1986) 237-243.
10. D.L. Kreher and S.P. Radziszowski, Simple 5–(28,6,λ) designs from $PSL_2(27)$ *Annals of Discrete Mathematics*, to appear.
11. D.L. Kreher and S.P. Radziszowski, A 1-Rotational simple 4-(12,6,10) design, *in preperation.*
12. D.L. Kreher, An Incidence Algebra for t-Designs with Automorphisms, *Journal of Combinatorial Theory A* 42, No. 2 (1986) 239-251.
13. J.C. Lagarias and A.M. Odlyzko, Solving Low-Density Subset Sum Problems, *Journal of the ASCM*, 32, No. 1 (1985) 229-246.
14. W. Oberschelp, Lotto-Garantiesysteme und Block-pläne, *Mathematisch-Phys. Semesterberichte*, XIX (1972) 55-67.
15. E. Witt, Über Steinersche System, *Abh. Math. Sem. Hamburg*, 12 (1938) 265-275.