4-(21,5,λ) Designs from a Group of Order 171

Yeow Meng Chee
Information Technology Institute
National Computer Board
71 Science Park Drive, S0511
Republic of Singapore

*Donald L. Kreher**
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931-1295
U.S.A.

Abstract

Using basis reduction, we settle the existence problem for 4-$(21, 5, \lambda)$ designs with $\lambda \in \{3, 5, 6, 8\}$. These designs each have as an automorphism group the Frobenius group G of order 171 fixing two points. We also show that a 4-$(21, 5, 1)$ design cannot have the subgroup of order 57 of G as an automorphism group.

1 Introduction

In this paper, we assume all sets that are not obviously infinite, to be finite. If X is a set, then $\mathcal{P}(X)$ denotes the set of all subsets of X and $\mathcal{P}_k(X)$ denotes the set of all k-element subsets of X. A t-(v, k, λ) design, where t, v, k and λ are non-negative integers with $t \leq k$, is a pair $(X, \mathcal{B})$, $|X| = v$, such that $\mathcal{B} \subseteq \mathcal{P}_k(X)$ and for every $T \in \mathcal{P}_t(X)$, T is contained in exactly λ elements of $\mathcal{B}$. We call the elements of X *points* and the elements of $\mathcal{B}$ *blocks*. A t-$(v, k, 1)$ design is also commonly known as a *Steiner system*.

An *isomorphism* between two t-(v, k, λ) designs $(X_1, \mathcal{B}_1)$ and $(X_2, \mathcal{B}_2)$ is a bijection $\sigma : X_1 \rightarrow X_2$ such that $\mathcal{B}_1^\sigma = \mathcal{B}_2$ (we identify σ with its canonical

*Research supported by National Science Foundation Grant No. CCR-8920692.

extension to $\mathcal{P}(X_1)$). An *automorphism* of a t-(v,k,λ) design $(X,\mathcal{B})$ is an isomorphism from $(X,\mathcal{B})$ onto $(X,\mathcal{B})$. The set of all automorphisms forms, under functional composition, the *full automorphism group* of $(X,\mathcal{B})$, which is denoted $\mathrm{Aut}(\mathcal{B})$. Any subgroup $H \leq \mathrm{Aut}(\mathcal{B})$ is referred to as *an automorphism group* of $(X,\mathcal{B})$.

Prior to this paper, the existence problem for 4-$(21,5,\lambda)$ designs was completely open for all λ's [1]. Here, we settle the existence problem for 4-$(21,5,\lambda)$ designs with $\lambda \in \{3,5,6,8\}$ in the affirmative by employing a construction technique of Kreher and Radziszowski [7] called basis reduction. Each design will have the Frobenius group G of order 171 fixing two points as an automorphism group. We also prove the impossibility of having a Steiner system 4-$(21,5,1)$ with the subgroup of order 57 of G as an automorphism group. As the Kreher-Radziszowski construction is fundamental in obtaining these results, we briefly review this technique in the next section.

2 Constructing Designs with Given Group

Let $G \leq \mathrm{Sym}(X)$. Then G also acts on the subsets of X by defining $S^g = \{x^g : x \in S\}$ for $S \subseteq X$ and $g \in G$. The *orbit* of $S \subseteq X$ is $S^G = \{S^g : g \in G\}$. Let $\Delta_1(G),\ldots,\Delta_{N_t}(G)$ and $\Gamma_1(G),\ldots,\Gamma_{N_k}(G)$ be complete lists of all orbits of t-element and k-element subsets of X under G respectively. For any fixed orbit representative T of $\Delta_i(G)$, the number of elements $K \in \Gamma_j(G)$ such that $T \subseteq K$ is denoted by $A_{tk}(G)[i,j]$, and is independent of the choice of T. It was observed by Kramer and Mesner [3] that a t-(v,k,λ) design $(X,\mathcal{B})$ exists with G as an automorphism group if and only if there exists a $(0,1)$-vector U satisfying the matrix equation

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

where J is the N_t-dimensional vector of all 1's.

Kreher and Radziszowski proposed in [5, 6, 7] an efficient and effective algorithm for computing $(0,1)$-vectors U that satisfy $A_{tk}(G)U = \lambda J$. Let M be an integer valued matrix with columns $a_1, a_2, \ldots, a_m$. The **Z**-*module* or *lattice* generated by $a_1, a_2, \ldots, a_m$ is:

$$\mathcal{L}(M) = \left\{ \sum_{i=1}^{m} \zeta_i a_i : \zeta_i \in \mathbf{Z}, 1 \leq i \leq m \right\}.$$

Kreher and Radziszowski observed that if U is any integer vector satisfying $A_{tk}(G)U = \lambda J$, then $\begin{pmatrix} U \\ 0 \end{pmatrix}$ is a vector in the lattice $\mathcal{L}(M)$ generated by the columns of the matrix

$$M = \begin{pmatrix} I & 0 \\ A_{tk}(G) & -\lambda J \end{pmatrix}.$$

They also made the observation that a $(0,1)$-vector U satisfying $A_{tk}(G)U = \lambda J$ is often a short vector in $\mathcal{L}(M)$. Lovász' basis reduction algorithm [8] with added enhancement is then used to obtain a reduced basis M' for a new lattice $\mathcal{L}(M')$. This new lattice $\mathcal{L}(M')$ contains all the integer vectors U satisfying $A_{tk}(G)U = d \cdot \lambda J$ for some integer $d > 0$. In addition, the reduced basis M' contains relatively short vectors of $\mathcal{L}(M')$ and often a $(0,1)$-vector U appears among them. This vector U gives a t-$(v,k,d\cdot\lambda)$ design.

3 Proving Non-Existence with Basis Reduction

The basis reduction algorithm described in Section 2 has been used with much success in finding t-(v,k,λ) designs [4]. However, since the basis reduction algorithm is not an exhaustive search mechanism, its failure to find a solution to $A_{tk}(G)U = \lambda J$ does not prove the non-existence of a t-(v,k,λ) design with G as an automorphism group. In this section, we examine circumstances under which basis reduction can be employed to prove non-existence results concerning t-(v,k,λ) designs.

Let $L = \{|\Gamma_i(G)| : 1 \le i \le N_k\}$ be the set of lengths of orbits of k-element subsets of X under the action of G. For each $\ell \in L$, let n_ℓ denote the number of orbits of k-element subsets of X of length ℓ that appear in a t-(v,k,λ) design $(X,\mathcal{B})$ with G as an automorphism group. Then by considering the number of blocks in $\mathcal{B}$, we obtain the following equation:

$$\sum_{\ell\in L} n_\ell \ell = \lambda\binom{v}{t}/\binom{k}{t}.$$

Now consider M', the reduced basis computed by the algorithm of Kreher and Radziszowski. It follows from the discussion in Section 2 that if $m_1,\ldots,m_{N_k}$ are the columns of M', then every $(0,1)$-vector U satisfying $A_{tk}(G)U = \lambda J$ can be written in the form

$$U = \sum_{i=1}^{N_k} \eta_i m_i,$$

where η_i, $1 \le i \le N_k$, are integers. Thus $||U||^2 \equiv 0 \pmod 2$ if $||m_i||^2 \equiv 0 \pmod 2$ for all $1 \le i \le N_k$. By noting that $||U||^2 = \sum_{\ell\in L} n_\ell$, we have the following theorem.

Orbit Representatives				
0 1 4 7 8	0 1 2 9 11	0 1 4 5 10	0 1 4 6 11	0 1 9 11 15
0 1 9 11 12	0 1 3 9 13	0 1 4 5 14	0 1 4 6 15	0 1 3 6 16
0 1 2 4 17	0 1 3 6 ∞_0	0 1 3 9 ∞_0	0 1 4 7 17	0 1 2 9 ∞_1
0 1 4 12 ∞_0	0 1 9 14 ∞_0	0 1 4 6 ∞_1	0 1 4 9 ∞_1	0 1 9 18 ∞_1
0 1 4 ∞_0 ∞_1				

Table 1: A 4-(21,5,5) Design

Theorem 1 *Let $G \leq \mathrm{Sym}(X)$ and let L be the set of lengths of orbits of k-element subsets of X under the action of G. Further, let n_ℓ, $\ell \in L$, be non-negative integers such that $\sum_{\ell \in L} n_\ell \ell = \lambda\binom{v}{t}/\binom{k}{t}$. Then a t-(v,k,λ) design $(X,\mathcal{B})$ with G as an automorphism group does not exist if $\sum_{\ell \in L} n_\ell \equiv 1 \pmod 2$ and $\|m_i\|^2 \equiv 0 \pmod 2$ for all $1 \leq i \leq N_k$, where $m_1, \ldots, m_{N_k}$ are the columns of the reduced basis M' computed by the Kreher-Radziszowski algorithm.* □

4 The New Designs

Let $X = \mathbf{Z}_{19} \cup \{\infty_0, \infty_1\}$ and let $G \leq \mathrm{Sym}(X)$ be the Frobenius group of order 171 that is generated by the permutations

$$\alpha : x \mapsto x + 1 \pmod{19},$$

$$\beta : x \mapsto 4x \pmod{19},$$

with the convention that $\infty_i + 1 \pmod{19} = \infty_i$ and $4 \cdot \infty_i \pmod{19} = \infty_i$, for $i \in \{0,1\}$. The approach described in Section 2 was taken to find 4-$(21,5,\lambda)$ designs with $\lambda \in \{3,5,6,8\}$ having G as an automorphism group. We list in Tables 1, 2, 3, and 4 the orbit representatives for the blocks of the designs that we have found. All the blocks in each design can be obtained by developing the orbit representatives with permutations in G.

5 Results on Steiner System 4-(21,5,1)

The designs we presented in the previous section are actually byproducts of an attempted search for the elusive 4-$(21,5,1)$ design that we have conducted. Although we have not been successful in finding a 4-$(21,5,1)$ design, we manage to obtain the following result.

Orbit Representatives				
0 1 2 6 9	0 1 4 5 7	0 1 2 3 6	0 1 4 6 8	0 1 4 7 8
0 1 4 5 10	0 1 4 6 9	0 1 2 4 10	0 1 2 9 10	0 1 4 6 11
0 1 5 9 11	0 1 4 9 11	0 1 8 9 11	0 1 2 9 12	0 1 5 9 13
0 1 9 11 14	0 1 4 5 14	0 1 3 9 16	0 1 2 4 18	0 1 2 9 18
0 1 2 9 ∞_0	0 1 4 5 ∞_0	0 1 3 8 ∞_0	0 1 5 9 ∞_0	0 1 3 11 ∞_0
0 1 9 13 ∞_0	0 1 4 12 ∞_0	0 1 9 14 ∞_0	0 1 2 4 ∞_1	0 1 3 8 ∞_1
0 1 4 7 ∞_1	0 1 9 15 ∞_1	0 1 5 9 ∞_1	0 1 9 11 ∞_1	0 1 9 13 ∞_1
0 1 2 16 ∞_1	0 1 3 ∞_0 ∞_1	0 1 8 ∞_0 ∞_1	0 1 12 ∞_0 ∞_1	

Table 2: A 4-(21, 5, 5) Design

Orbit Representatives				
0 1 2 6 9	0 1 4 5 6	0 1 2 4 7	0 1 4 5 8	0 1 2 4 9
0 1 4 6 9	0 1 7 8 9	0 1 2 9 10	0 1 4 8 10	0 1 4 7 10
0 1 5 9 11	0 1 6 9 11	0 1 9 11 13	0 1 5 9 13	0 1 9 11 14
0 1 4 5 14	0 1 2 4 14	0 1 4 6 15	0 1 2 9 15	0 1 9 11 16
0 1 3 9 16	0 1 2 4 17	0 1 2 4 18	0 1 2 9 18	0 1 4 5 ∞_0
0 1 3 6 ∞_0	0 1 7 9 ∞_0	0 1 4 9 ∞_0	0 1 5 9 ∞_0	0 1 8 9 ∞_0
0 1 2 9 ∞_1	0 1 9 18 ∞_0	0 1 2 16 ∞_0	0 1 4 6 ∞_1	0 1 2 4 ∞_1
0 1 9 15 ∞_1	0 1 3 9 ∞_1	0 1 9 11 ∞_1	0 1 4 12 ∞_1	0 1 9 14 ∞_1
0 1 3 ∞_0 ∞_1	0 1 2 ∞_0 ∞_1			

Table 3: A 4-(21, 5, 6) Design

Orbit Representatives				
0 1 2 4 6	0 1 2 3 6	0 1 2 4 8	0 1 3 6 8	0 1 4 7 8
0 1 2 4 9	0 1 2 9 11	0 1 4 5 10	0 1 2 8 9	0 1 2 9 10
0 1 4 7 10	0 1 4 6 11	0 1 3 9 11	0 1 6 9 11	0 1 9 11 15
0 1 9 11 12	0 1 2 4 12	0 1 2 9 12	0 1 5 9 12	0 1 4 6 13
0 1 4 5 13	0 1 3 9 13	0 1 5 9 13	0 1 4 6 14	0 1 4 9 14
0 1 2 9 15	0 1 9 11 18	0 1 9 11 16	0 1 4 5 17	0 1 2 4 17
0 1 4 7 17	0 1 4 6 18	0 1 4 6 ∞_0	0 1 2 4 ∞_0	0 1 3 6 ∞_0
0 1 3 8 ∞_0	0 1 4 8 ∞_0	0 1 7 9 ∞_0	0 1 3 9 ∞_0	0 1 5 9 ∞_0
0 1 2 9 ∞_1	0 1 9 18 ∞_0	0 1 9 13 ∞_0	0 1 9 16 ∞_0	0 1 2 16 ∞_0
0 1 3 8 ∞_1	0 1 4 7 ∞_1	0 1 4 8 ∞_1	0 1 3 9 ∞_1	0 1 4 9 ∞_1
0 1 9 11 ∞_1	0 1 4 12 ∞_1	0 1 9 13 ∞_1	0 1 9 14 ∞_1	0 1 9 18 ∞_1
0 1 2 16 ∞_1	0 1 3 ∞_0 ∞_1	0 1 4 ∞_0 ∞_1	0 1 8 ∞_0 ∞_1	0 1 12 ∞_0 ∞_1

Table 4: A 4-(21, 5, 8) Design

Theorem 2 *Let $H \leq G$, where $H = \langle \gamma, \delta \rangle$,*

$$\gamma : x \mapsto x + 1 \pmod{19},$$

$$\delta : x \mapsto 7x \pmod{19}.$$

Then H is not an automorphism group of any 4-(21, 5, 1) *design* $(X, \mathcal{B})$.

Proof. A careful examination of the 117×369 matrix $A_{45}(H)$ reveals that 132 of the 369 columns contain some entry $A_{45}(H)[i,j] > 1$. Hence, none of these 132 corresponding orbits of 5-element subsets of X under the action of H can be part of a 4-(21, 5, 1) design with $H \leq \mathrm{Aut}(\mathcal{B})$. It is then clear that if $\tilde{A}_{45}(H)$ is the matrix $A_{45}(H)$ with these 132 columns deleted, then a 4-(21, 5, 1) design exists with $H \leq \mathrm{Aut}(\mathcal{B})$ if and only if there exists a (0, 1)-vector U satisfying $\tilde{A}_{45}(H)U = J$. The orbits corresponding to the columns of $\tilde{A}_{45}(H)$ are of two types: those with length 19 and those with length 57. By considering the number of blocks in $\mathcal{B}$, there must exist non-negative integers x and y such that $19x + 57y = 1197$. This implies that $x + y \equiv 1 \pmod{2}$. The algorithm of Kreher and Radziszowski was used on the initial basis

$$M = \begin{pmatrix} I & 0 \\ \tilde{A}_{45}(H) & -J \end{pmatrix}.$$

All columns m of the final reduced basis were found to satisfy $||m||^2 \equiv 0 \pmod{2}$. Hence, the theorem is proved by invoking Theorem 1. □

6 Conclusion

In this paper, the basis reduction algorithm of Kreher and Radziszowski is used to construct new 4-(21, 5, λ) designs with $\lambda \in \{3, 5, 6, 8\}$. This leaves the existence problem for 4-(21, 5, λ) designs unsettled for only four values of λ, namely $\lambda \in \{1, 2, 4, 7\}$. The non-existence of a 4-(21, 5, 1) design with the Frobenius group of order 57 fixing two points as an automorphism group is also proven using the basis reduction algorithm. This is not the first instance where non-existence results are established using basis reduction. Chee and Royle [2] have earlier used it to prove that 2-(25, 3, 1) designs of certain configurations do not exist. We are hopeful that basis reduction will be useful in ruling out possible automorphism groups for other designs.

References

[1] Y. M. Chee, C. J. Colbourn, and D. L. Kreher. *Simple t-designs with $v \leq 30$*, Ars Combinatoria **29** (1990) 193–258.

[2] Y. M. Chee and G. F. Royle. *The 2-rotational Steiner triple systems of order 25*, Discrete Mathematics **97** (1991) 93–100.

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

[4] D. L. Kreher, Y. M. Chee, D. de Caen, C. J. Colbourn, and E. S. Kramer. *Some new simple t-designs*, Journal of Combinatorial Mathematics and Combinatorial Computing **7** (1990) 53–90.

[5] D. L. Kreher and S. P. Radziszowski. *The existence of simple 6-*(14, 7, 4) *designs*, Journal of Combinatorial Theory (A) **43** (1986) 237–243.

[6] D. L. Kreher and S. P. Radziszowski. *Finding simple t-designs by basis reduction*, Congressus Numerantium **55** (1986) 235–244.

[7] D. L. Kreher and S. P. Radziszowski. *Constructing 6-(14,7,4) designs*, Contemporary Mathematics **111** (1990) 137–151.

[8] A. K. Lenstra, Jr. H. W. Lenstra, and L. Lovász. *Factoring polynomials with rational coefficients*, Mathematische Annalen **261** (1982) 515–534.