JOURNAL OF COMBINATORIAL THEORY, Series A 43, 237–243 (1986)

The Existence of Simple 6-(14, 7, 4) Designs

DONALD L. KREHER AND STANISLAW P. RADZISZOWSKI

School of Computer Science and Technology, Rochester Institute of Technology, Rochester, New York 14623

Communicated by the Managing Editors

Received March 20, 1986

A cyclic 5-(13, 6, 4) design is constructed and is extended to a simple 6-(14, 7, 4) design via a theorem of Alltop. This design is the smallest possible nontrivial simple 6-design that can exist. Both have full automorphism group cyclic of order 13.

1. INTRODUCTION

A *t-design*, or t-(v, k, λ) *design* is a pair (X, B) with a v-set X of *points* and a family B of k-subsets of X called *blocks* such that any t points are contained in exactly λ blocks. A t-(v, k, λ) design (X, B) is said to be *cyclic* if $X = \{0, 1, 2, \ldots, v-1\}$ and whenever K is a block $K+1 = \{x+1 : x \in K\}$ is also a block, addition preformed modulo v.

In this paper we give a brief exposition of our construction of two non-isomorphic pairwise disjoint 6-(14, 7, 4) designs partitioning all of the $\binom{14}{7}$ 7-subsets. We first construct a 5-(13, 6, 4) design by using a cyclic group of order 13 and then extend it to a 6-design with the extension theorem of Alltop [1]. With the exception of the two 5-designs discovered by Kramer [2, 4] and the two 5-designs discovered by Magliveras and Leavitt [9] this is the only other small parameter situation in which a 5-design on an odd number of points is known to exist. Finally, we show that these designs have full automorphism group cyclic of order 13 and are unique up to isomorphism.

0097-3165/86 $3.00

2. Preliminaries

In 1973, Kramer and Mesner [4] made the following observation: A t-(v, k, λ) design exists with $G \leqslant \mathrm{Sym}(X)$ as an automorphism group if and only if there is a (0, 1)-solution vector U to the matrix equation

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

where

(a) the rows of A_{tk} are indexed by the G-orbits of t-subsets of X;

(b) the columns of A_{tk} are indexed by the G-orbits of k-subsets of X;

(c) $A_{tk}[\Delta, \Gamma] = |\{K \in \Gamma : K \supset T_0\}|$, where $T_0 \in \Delta$ is any representative;

(d) $J = [1, 1, 1, \ldots, 1]^T$.

If we choose the group G to be $\mathbb{Z}_{13}$, the integers modulo 13, and $X = \mathbb{Z}_{13}$ then each $g \in G$ can be thought of as the permutation $x \to x + g$. In this action G has exactly $\frac{1}{13}\binom{13}{5} = 99$ orbits of 5-subsets and exactly $\frac{1}{13}\binom{13}{6} = 132$ orbits of 6-subsets. Hence the $A_{5,6}$ matrix belonging to G has 99 rows and 132 columns. Thus to find a cyclic 5-(13, 6, 4) design one need only solve 99 linear Diophantine equations in 132 unknowns for a (0, 1)-solution vector U. This seemingly impossible task was accomplished by our basis reduction algorithm presented at the 17th Southeastern International Conference on Combinatorics Graph Theory and Computing [6]. We should remark that this algorithm is based in part on the L^3 algorithm of Lenstra, Lenstra, and Lovász [8], and was inspired by the work of Lagarias and Odlyzko [7]. The algorithm we have constructed is apparently a powerful tool for searching for short vectors in integer lattices with other applications such as the subset-sum/knapsack problem [10].

The 6-(14, 7, 4) design is constructed via Theorem C of Alltop [1]. That is, if $(X, \mathscr{B})$ is a 5-(13, 6, 4) design and ∞ is a new point not in X then $(X \cup \{\infty\}, \mathscr{B}' \cup \mathscr{B}'')$ is a 6-(14, 7, 4) design where

$$\mathscr{B}' = \{K \cup \{\infty\} : K \in \mathscr{B}\}$$

$$\mathscr{B}'' = \{X - K : K \in \mathscr{B}\}.$$

3. Data

Tables I–IV display the data which exhibit the construction of the new 5-designs.

Table I exhibits the orbit representatives of 5-subsets, listed top to bottom, left to right. To aide in our exhibition of the data after Eq. (1) was

TABLE I

01234	02356	01457	03567	03458	01278	03678	01469	01579
01235	01456	02457	04567	01268	01378	04678	02469	02579
01245	02456	03457	01238	01368	02378	01259	03469	03579
01345	03456	01267	01248	02368	01478	01359	01569	03679
02345	01237	01367	01348	01468	02478	02359	02569	03489
01236	01247	02367	02348	[02468]	03478	01459	03569	02589
01246	01347	01467	01258	03468	01578	02459	01379	03589
01346	02347	02467	01358	01568	02578	03459	02379	03689
02346	01257	03467	02358	02568	03578	01269	01479	01471 0
01256	01357	01567	01458	03568	04578	01369	02479	02471 0
01356	02357	02567	02458	04568	02678	02369	03479	02571 0

solved, the columns of $A_{5,6}$ were permuted so that the first 66 columns give the desired design.

Table II exhibits the orbit representatives, listed top to bottom, left to right, labeling the *first* 66 columns of $A_{5,6}$. Furthermore, if these 66 6-subsets are developed into 858 6-subsets by adding modulo 13 each of 0, 1, 2,..., 12, they will be the blocks of a 5-(13, 6, 4) design.

Table III exhibits the orbit representatives, listed top to bottom, left to right, labeling the *last* 66 columns of $A_{5,6}$. Furthermore, if these 66 6-subsets are developed into 858 6-subsets by adding modulo 13 each of 0, 1, 2,..., 12, they will be the blocks of a 5-(13, 6, 4) design.

Table IV exhibits the $A_{5,6}$ matrix. Each entry in this table represents one of the 99 rows by giving the positions in which there is a nonzero entry. A subscript of 2 indicates the entry is 2, otherwise it is 1. For example, row 50 is given by

$$50 \quad 39\ 51\ 66_2\ 81\ 82\ 84\ 91$$

and represents the row of 132 entries:

000000000000000000000000000000000000100000
000000100000000000000200000000000011010000
001000000000000000000000000000000000000000.

TABLE II

012345	023458	013578	014569	035679	036789
012346	012368	023578	024569	023489	012471 0
012456	013468	024578	012479	013589	023471 0
012357	012568	012678	013479	023589	012571 0
013467	013568	025678	012579	014589	014571 0
023467	014568	045678	[01357 9]	012689	024571 0
013567	034568	013459	034579	[02468 9]	014671 0
023567	012378	023459	023679	034689	013581 0
014567	012478	012369	014679	025689	024581 0
024567	013478	023469	034679	035689	023681 0
012458	023478	012569	025679	014789	[02468 10]

TABLE III

0 1 2 3 5 6	0 1 2 3 4 8	0 2 3 6 7 8	0 2 3 5 6 9	0 1 3 4 8 9	0 1 3 4 7 10
0 1 3 4 5 6	0 1 2 3 5 8	0 1 4 6 7 8	0 3 4 5 6 9	0 1 2 5 8 9	0 1 3 5 7 10
0 2 3 4 5 6	0 1 3 4 5 8	**[0 2 4 6 7 8]**	0 1 2 3 7 9	0 2 4 5 8 9	0 2 3 5 7 10
0 1 2 3 4 7	**[0 1 2 4 6 8]**	0 3 4 6 7 8	0 2 3 4 7 9	0 3 4 5 8 9	0 1 3 6 7 10
0 1 2 4 5 7	**[0 2 3 4 6 8]**	0 1 5 6 7 8	0 2 3 5 7 9	0 1 3 6 8 9	0 2 3 6 7 10
0 1 3 4 5 7	0 2 3 5 6 8	0 3 5 6 7 8	0 1 4 5 7 9	0 2 3 6 8 9	0 2 4 6 7 10
0 2 3 4 5 7	**[0 2 4 5 6 8]**	0 1 2 3 5 9	0 2 4 5 7 9	0 1 4 6 8 9	0 2 5 6 7 10
0 1 2 3 6 7	0 1 2 5 7 8	0 1 2 4 5 9	0 1 2 6 7 9	0 2 4 7 8 9	0 2 3 5 8 10
0 1 2 4 6 7	0 1 4 5 7 8	0 1 2 4 6 9	0 1 3 6 7 9	0 3 4 7 8 9	0 1 4 5 8 10
0 1 2 5 6 7	0 3 4 5 7 8	0 1 3 4 6 9	0 2 4 6 7 9	0 2 5 7 8 9	0 1 3 6 8 10
0 3 4 5 6 7	0 1 3 6 7 8	0 1 3 5 6 9	0 1 5 6 7 9	0 3 5 7 8 9	0 1 4 6 8 10

Observe that in each entry of Table IV there are 4 positions, counting those with subscript 2 twice, that have value less than or equal to 66. These correspond to the orbits used by the design given in Table II to cover each of the 5-subsets in some orbit exactly 4 time. For example, the row 50 entry says to use orbits 39, 51, and 66 to cover orbit number 50 of 5-subsets exactly 4 times. Similarly there are 4 values greater than 66. The orbit representatives in the above example appear in brackets with bold face in Tables I, II, and III.

4. Full Automorphism Group

Using computer search techniques the full automorphism groups of these designs were established.

For notation definitions and theorems on permutation groups the reader is directed to Wielandt [12]. Here we introduce some notation and concepts relevant to the present paper. If X is a set then $\mathrm{Sym}(X)$ denotes the symmetric group on X. A group G is said to act on a set X if there is a function $X \times G \to X$ (usually denoted by $(\alpha, g) \to \alpha^g$) such that for all $g, h \in G$ and $\alpha \in X$:

$$\alpha^1 = \alpha \qquad \text{and} \qquad \alpha^{(gh)} = (\alpha^g)^h.$$

Such a function is said to be a group action of G on X and is denoted by $G \mid X$. Thus, if $G \mid X$ is a group action, then G may be thought of as being mapped homomorphically onto a subgroup of $\mathrm{Sym}(X)$, and α^g is the image of $\alpha \in X$ under $g \in G$. If $\alpha \in X$, the *stabilizer* in G of α is the subgroup $G_\alpha = \{g \in G: \alpha^g = \alpha\}$ nd the *orbit* of α under G is $\alpha^G = \{\alpha^g: g \in G\}$. We note that $|G| = |\alpha^G| \cdot |G_\alpha|$. A group action $G \mid X$ induces a natural action on the collection of all k-subsets of X, for any k, $0 \leqslant k \leqslant |X|$. For if $K \subseteq X$, $|K| = k$, and $g \in G$ then we define K^g by $K^g = \{s^g: s \in K\}$.

A group action $G \mid X$ is said to be *transitive* if $\alpha^G = X$, for some $\alpha \in X$, it is *doubly transitive* if both $G \mid X$ and $G_\alpha \mid (X - \{\alpha\})$ are transitive. A subset ψ of X, $1 < |\psi| < |X|$ is said to be a nontrivial *set of imprimitivity* of the group

TABLE IV

Row no.	Non-zero Positions				
1	1_2 2 28 69 70 77 78	34	7 8 45 58 77 90 94 120	67	55 56 57 59 88 89 92 94
2	1 2 4 18 67 73 79 95	35	9 10 28 31 77 93 95 102	68	28 30 32 46 90 91 92 103
3	1 3 6 11 67 71 87 96	36	13 19 27 28 78 79 93 94	69	33 34 35 38 95 96 101 112
4	1 3 8 29 68 72 80 92	37	11 20 44 45 78 81 95 110	70	29 39 40 47 95 99 105 106
5	1 10 12 30 68 69 73 94	38	14 21 53 54 78 80 96 111	71	30 42 43 48 95 100 104 109
6	2 12 13 31 67 70 74 101	39	12 22 29 46 78 82 120 121	72	29 34 49_2 96 105 113 114
7	2 3 4 40 75 81 82 97	40	11 15 31 58 79 85 112 128	73	30 35 51 52 96 106 113 117
8	2 5 14 43 68 71 83 98	41	16 23 47 63 79 80 97 124	74	29 30 40 55 101 114 118 119
9	2 6 32 45 69 72 82 84	42	12 24 48 61 79 83 98 129	75	31 33 50 56 97 107 119 121
10	3 15 22 33 67 74 76 114	43	11 17 33 49 80 86 126 130	76	31 57 60 61 98 99 108 115
11	7 16 24 52 67 68 75 99	44	11 12 25 64 84 99 113 127	77	31 32 41 62 100 116 122 127
12	5 8 25 54 67 69 83 100	45	12 18 34 59 80 87 114 128	78	34 42 59 64 97 98 117 130
13	3 9 17 34 68 76 89 119	46	13 15 26 50 81 102 118 120	79	32 35 51 66 97 109 123 132
14	3 7 10 35 69 84 91 121	47	13 14 16 36 88 115 129 131	80	32 43 52 60 98 101 125 131
15	9 18 27 56 68 69 77 101	48	13 37 64 65 82 83 89 116	81	33 34 49 55 99 110 111 117
16	4 19 30 56 70 74 78 102	49	14 17 38 65 81 90 117 132	82	33 35 44 53 100 125 130 132
17	20 32 36 57 70 71 75 79	50	39 51 66_2 81 82 84 91	83	45 54 62 65 99 100 101 126
18	5 11 21 37 70 72 100 122	51	14 18 52 63 82 92 105 123	84	37 39 41 44 102 107 108 109
19	6 22 35 58 70 73 80 103	52	15 16 17 47 93 107 111 115	85	41 50 51 53 102 103 104 116
20	4 13 38 59 71 76 85 103	53	15 27 53 63 83 84 108 131	86	36 37 42 55 105 126 127 128
21	4 7 23 39 72 81 104 123	54	16 18 42 54 83 94 124 129	87	36 63 65 66 103 106 109 118
22	4 8 14 24 73 104 106 124	55	17 18 28 36 84 96 97 110	88	37 40 43 62 103 119 130 132
23	9 15 41 60 71 72 86 105	56	19 20 26_2 85 88 90 93	89	38 39 46 51 105 110 113 118
24	10 16 25 61 71 73 106 109	57	19 21 23 42 88 107 108 110	90	38 44 64 66 104 106 120 131
25	17 40 44 57 72 73 77 87	58	19 22 24 50 89 111 115 117	91	39 40 45 66 104 121 127 132
26	19 26 46 55 74 75 76 107	59	20 21 55 62 86 90 112 125	92	41 43 45 56 108 122 123 125
27	5 7 20 48 74 88 108 125	60	20 22 25 47 91 118 131 132	93	46 47 49 52 111 112 114 119
28	6 8 21 41 74 89 113 126	61	21 22 49 60 87 92 119 130	94	48 53 59 60 112 113 120 123
29	5 9 42 62 75 85 90 116	62	23 46 48 50 85 86 93 116	95	47 48 54 63 114 121 128 130
30	6 10 23 51 75 91 109 127	63	24 25 27 65 85 115 120 129	96	52 54 56 58 115 116 124 126
31	5 6 43 53 77 86 92 122	64	23 24 61 64 87 94 117 121	97	57 58 60 62 122_2 125 126
32	7 9 26 50 76 93 110 112	65	25 28 29 37 86 87 98 111	98	57 58 61 65 123 124 127 131
33	8 10 27 44 76 88 118 128	66	26 27 36 38 89 91 102 107	99	59 61 63 64 124 128 129_2

action $G \mid X$ if for each $g \in G$ the set ψ^g either coincides with ψ or is disjoint from ψ. A transitive group action $G \mid X$ is said to be *imprimitive* if it has at least one nontrivial set of imprimitivity otherwise it is *primitive*. A complete list of primitive group actions on sets of size 20 or less was given by Sims [11]. We note in passing that if $G \mid X$ is doubly transitive or $G \mid X$ is transitive and $|X|$ is prime then necessarily $G \mid X$ is primitive.

THEOREM 1. *The full automorphism group of a cyclic* 5-(13, 6, 4) *design is* C_{13}, *the cyclic group of order* 13.

Proof. Let $(X, \mathscr{B})$ be a cyclic 5-(13, 6, 4) design and suppose that G is its full automorphism group. Then $G \mid X$ is transitive and since $|X| = 13$ is prime G acts primitively. Therefore G is one of 9 groups [11]:

— The symmetric and alternating groups on 13 points, $\mathrm{Sym}(X)$, $\mathrm{Alt}(X)$;

— The projective special linear group $\mathrm{PSL}_3(3)$;

— One of the 6 transitive subgroups of AF(13), the affine group on 13 points, $\mathrm{AF}(13) = \{x \to \alpha x + \beta : \alpha, \beta \in \mathbb{Z}_{13}, \alpha \neq 0\}$.

Both $\mathrm{Sym}(X)$ and $\mathrm{Alt}(X)$ have exactly one orbit of 6-subsets and therefore cannot be the automorphism group of any nontrivial 5-design on 13 points.

If G is $\mathrm{PSL}_3(3)$ then G has 4 orbits Γ_1, Γ_2, Γ_3, and Γ_4 of orders 936, 468, 234, and 78, respectively. It is easy to see that $|\mathscr{B}| = 858$ is not the sum of any of these numbers. Consequently, $\mathrm{PSL}_3(3)$ cannot be an automorphism group of a 5-(13, 6, 4) design.

If G is a transitive subgroup of AF(13) then G is generated by the two permutations given by

$$x \to x + 1 \qquad \text{and} \qquad x \to \omega^i x,$$

where ω is a primitive root modulo 13 and $i \in \{1, 2, 3, 4, 6, 12\}$. It is sufficient to show that i cannot be 6 or 4 since these correspond to the minimal subgroups of AF(13) containing C_{13}. In either of these two cases the matrices are relatively small (57 by 76 and 34 by 48, respectively) and can be computer searched after size reduction given by the algorithm found in [6]. Such a search shows that in both these situations there is no design.

COROLLARY 1. *The full automorphism group of a* 6-(14, 7, 4) *design with a cyclic derived design is cyclic of order* 13.

Proof. Let $(X, \mathscr{B})$ be a 6-(14, 7, 4) design and let $G = \mathrm{Aut}(\mathscr{B})$ be its full automorphism group. If $\alpha \in X$ is such that the 5-(13, 6, 4) design $(X - \{\alpha\}, \mathscr{B}_\alpha)$, where $\mathscr{B}_\alpha = \{K - \{\alpha\} : \alpha \in K \text{ and } K \in \mathscr{B}\}$ is cyclic then by Theorem 1, $G_\alpha = \{g \in G : \alpha = \alpha\}$ is cyclic of order 13. Whence, if $G \neq G_\alpha$ then G would be doubly transitive and hence primitive of order $|\alpha^G| \cdot |G_\alpha| = 14 \cdot 13$. There is, however, no such group [11 or 12]. Thus, G is cyclic of order 13 as claimed.

To check if the designs in Tables II and III are not isomorphic one need only consider those permutations that normalize C_{13}. That is, we need only check inside AF(13). This easy procedure shows that the two designs are

indeed nonisomorphic. Finally, a computer search was successfully completed enumerating all the possible cyclic 5-designs on 13 points. This search resulted in exactly two nonisomorphic designs. That is, the designs given in tables II and III are unique up to isomorphism. Consequently, we state

THEOREM 2. *There are exactly two nonisomorphic cyclic* 5-(13, 6, 4) *designs. Furthermore, these designs are pairwise disjoint and partition all of the* $\binom{13}{6}$ 6*-subsets.*

An argument similar to the proof of Corollary 1 gives the following result:

COROLLARY 2. *There are exactly two nonisomorphic* 6-(14, 7, 4) *designs with cyclic derived designs. Furthermore, these designs are pairwise disjoint and partition all of the* $\binom{14}{7}$ 7*-subsets.*

REFERENCES

1. W. O. ALLTOP, Extending t-designs, *J. Combin. Theory Ser. A* **18** (1975), 177–186.
2. E. S. KRAMER, Some t-designs for $t \geqslant 4$ and $t = 17$, 18, *in* "Proceedings, Sixth Southeast. Conf. Combin. Graph Theory, Comput.," pp. 443–460, Congress. Numer. Vol. 14, Utilitas Math., Winnipeg, Manitoba, Canada, 1975.
3. E. S. KRAMER, D. W. LEAVITT, AND S. S. MAGLIVERAS, "Construction Procedures for t-Designs and the Existence of New Simple 6-Designs," Ann. Discrete Math. Vol. 26, pp. 247–274, North-Holland, Amsterdam, 1985.
4. E. S. KRAMER AND D. M. MESNER, t-Designs on hypergraphs, *Discrete Math.* **15** (1976), 263–296.
5. E. S. KRAMER, S. S. MAGLIVERAS, AND D. M. MESNER, t-Designs from the large Mathieu groups, *Discrete Math.* **36** (1981), 171–189.
6. D. L. KREHER AND S. P. RADZISZOWSKI, Finding simple t-designs by basis reduction, *in* "Proceedings, 17th Southeast. Conf. Combin. Graph Theory, Comput.," Congress. Numer. Utilitas Math., Winnipeg, Manitoba, Canada, 1986.
7. J. C. LAGARIAS AND A. M. ODLYZKO, Solving low-density subset sum problem, *J. Assoc. Comput. Mach.* **32**, No. 1 (1985), 229–246.
8. A. K. LENSTRA, H. W. LENSTRA, AND L. LOVÁSZ, Factoring polynomials with rational coefficients, *Math. Ann.* **261** (1982), 515–534.
9. S. S. MAGLIVERAS AND D. W. LEAVITT, Simple 6-(33, 8, 36) designs from $P\Gamma L_2(32)$, *in* "Comput. Group Theory, Proceedings, London Math. Soc. Sympos. Comput. Group Theory," pp. 337–352, Academic Press, New York, 1984.
10. S. P. RADZISZOWSKI AND D. L. KREHER, Solving subset-sum problem with the L^3 algorithm, 1986, to appear.
11. C. C. SIMS, Computational methods in the study of permutation groups, *in* "Computational Problems in Abstract Algebra" (John Leech, Ed.), Pergamon, Elmsford, N.Y., 1970.
12. H. WIELANDT, "Finite Permutation Groups," Academic Press, New York/London, 1964.