Product Constructions for Cyclic Block Designs
II. Steiner 2-Designs

M. J. GRANNELL AND T. S. GRIGGS

Division of Mathematics and Statistics, Preston Polytechnic, Corporation Street, Preston PR1 2TQ, Lancashire, England

Communicated by the Managing Editors

Received June 30, 1983

Let CS(2, k, v) denote a cyclic Steiner 2-design of order v with block size k. Our main result is a product construction for obtaining a CS(2, q, uv) from a CS(2, q, u) and a CS(2, q, v) when q is a prime power and at least one of the latter two systems is composed entirely of full orbits.

1. INTRODUCTION, NOTATION, AND TERMINOLOGY

In [4] we introduced a product construction for cyclic Steiner quadruple systems. The purpose of this paper is to modify the construction so that it is applicable to cyclic Steiner 2-designs. A cyclic Steiner 2-design is a Steiner system S(t, k, v), 2 ≤ t < k < v, in which t = 2 and which has an automorphism of order v. We denote such a system by CS(2, k, v). Under suitable conditions we show how a CS(2, k, uv) may be obtained from a CS(2, k, u) and a CS(2, k, v).

CS(2, 3, v) exist for all admissible v (i.e., v ≡ 1 or 3 (mod 6)) apart from v = 9 [6]. However, for k > 3, the values of v for which a CS(2, k, v) exists have not been precisely determined. A survey of known results in this field is given by Colbourn and Mathon in [3]. In [2] Colbourn and Colbourn give product constructions for cyclic balanced incomplete block designs (which are quite different from the constructions presented here). Their constructions, together with ours, considerably extend the spectrum of v for which cyclic systems are known to exist. We believe that the smallest new system generated by our constructions is when k = 5, this system being a CS(2, 5, 441) obtained as the product of two CS(2, 5, 21)'s.

Given a positive integer v we denote by [v] the set \{0, 1, 2, ..., v − 1\} and we represent all CS(2, k, v) as unions of k-block orbits formed from elements of [v] under the action of the cyclic group \langle z → z + 1 (mod v)\rangle. The orbits will be referred to as full or \((1/n)\)th orbits according as their
length is \( v \) or \( v/n \), respectively. An orbit starter is any one \( k \)-block of the orbit and a set of starters for a system is simply a set of such \( k \)-blocks, precisely one from each orbit of the system.

When \( m \mid v \) we define a beheaded design, denoted by \( \text{CS}(2, k, v, -m) \), as a system composed of cyclic \( k \)-block orbits with block entries in \([v]\) which has the property that every pair \( \{a, b\} \) of distinct elements of \([v]\) whose difference is divisible by \( v/m \) does not occur in any \( k \)-block of the system, while every other pair of distinct elements occurs precisely once. The concept of a beheaded system was first introduced by Colbourn and Colbourn in [1] in connection with Steiner quadruple systems. The existence of a \( \text{CS}(2, k, v, -m) \) and a \( \text{CS}(2, k, m) \) implies that of a \( \text{CS}(2, k, v) \); the latter system is obtained by taking a set of starters for \( \text{CS}(2, k, m) \), multiplying the entries in each by \( v/m \) and taking the resulting sets together with starters for \( \text{CS}(2, k, v, -m) \) as a set of starters for \( \text{CS}(2, k, v) \).

2. Constructions

**Theorem 1.** Suppose \( p \) is prime and that there exists a \( \text{CS}(2, p, u) \) and a \( \text{CS}(2, p, v) \) the latter system being composed entirely of full orbits. Then there exists a \( \text{CS}(2, p, uv) \).

**Proof.** Let \( F_o \) and \( P_o \) denote sets of starters for (resp.) full and \((1/p)\)th orbits collectively forming a \( \text{CS}(2, p, u) \) and let \( F_v \) denote a set of starters for full orbits collectively forming a \( \text{CS}(2, p, v) \). Put \( A_o = A_v = \{\{0, 0, \ldots, 0\}\} \) (\( p \) zeros).

We next define the product \( XY \) for \( X = F_o, P_o, A_o \) and \( Y = F_v \) and \( A_v \), with the exception of \( A_oA_v \). Each such product consists of a set of starters and the orbits generated by these collectively form a \( \text{CS}(2, p, uv) \). The definition of each of these five products is similar, one to another, the differences relating to just one point; namely the elimination of "obvious" duplicate starters. The basic construction is as follows.

For each starter in \( X \) and for each starter in \( Y \) we select an arbitrary but fixed order for the elements forming that starter. Then for each \( \{x_0, x_1, \ldots, x_{p-1}\} \in X \) and each \( \{\alpha_0, \alpha_1, \ldots, \alpha_{p-1}\} \in Y \) we list all starters of the form \( \{x_0v + \alpha_b, x_1v + \alpha_{a+b}, \ldots, x_{p-1}v + \alpha_{(p-1)a+b}\} \), where \( a, b \in [p], \ a \neq 0, \) the subscript arithmetic is carried out modulo \( p \) and the resulting \( x_iu + \alpha_j \) terms lie in \([uv]\). \( XY \) consists of all starters so formed, except that if a number of starters lie in a single orbit then we discard all but one of these. If \( |\cdot| \) denotes cardinality then in all cases \( |XY| \leq p(p-1) |X| |Y| \). We denote by \#XY the number of distinct \( p \)-blocks formed by the starters in \( XY \) under the action of the cyclic group \( \langle z \rightarrow z + 1 \ (\text{mod} \ uv) \rangle \). We give details below of the five individual products which we require.
(1) $F_u F_v$. This follows the general construction. Note $\# F_u F_v \leq p(p - 1) u|F_u| \cdot |F_v|$.

(2) $P_u F_v$. For a given a, different values of b will produce starters lying in a common orbit. Hence $\# P_u F_v \leq (p - 1) u|P_u| \cdot |F_v|$.

(3) $A_u F_v$. All the $p(p - 1)$ starters formed from each $\{\alpha_0, \alpha_1, \ldots, \alpha_{p - 1}\} \in F_v$ will be identical. Hence $\# A_u F_v \leq u|F_v|$.

(4) $F_u A_v$. Similarly to 3 above, $\# F_u A_v \leq u|F_u|$.

(5) $P_u A_v$. As in 4 above, $\# P_u A_v \leq u|P_u|$.

We define $P$ to be the union of the sets of starters defined in (1)–(5) above (some of which may be empty). Let $\# P$ denote the number of distinct p-blocks generated by $P$ and $|\text{CS}(2, p, u)|$ denote the number of p-blocks forming a CS(2, p, u). We prove that

(a) $\# P \leq |\text{CS}(2, p, u)|$

(b) the collection of p-blocks generated by $P$ contains every 2-block of distinct elements.

It follows from (a) and (b) that $P$ generates a CS(2, p, u).

(a) From (1)–(5) above

$$\# P \leq u\left[p(p - 1)|F_u| \cdot |F_v| + (p - 1)|P_u| \cdot |F_v| + |F_v| + |F_u| + \frac{1}{p} |P_u|\right].$$

But $|F_u| + (1/p)|P_u| = |\text{CS}(2, p, u)| / u = (u - 1)/p(p - 1)$. Hence

$$\# P \leq u\left[(u - 1)|F_v| + |F_v| + (u - 1)/p(p - 1)\right]$$

$$= u\left[u|F_v| + (u - 1)/p(p - 1)\right]$$

$$= u\left[u(v - 1)/p(p - 1) + (u - 1)/p(p - 1)\right]$$

$$= uv(v - 1)/p(p - 1)$$

$$= |\text{CS}(2, p, u)|.$$

(b) Take any 2-block $\{X_0, X_1\}$ where $X_0, X_1 \in \{u\}$ and $X_0 \neq X_1$. Take

$$\alpha_0, \alpha_1 \in \{v\} \quad \text{such that} \quad \alpha_0 \equiv X_0 \pmod{v} \quad \text{and} \quad \alpha_1 \equiv X_1 \pmod{v}.$$

Consider the 2-block $\{\alpha_0, \alpha_1\}$. One of the starters in $F_v \cup A_v$ will generate a p-block containing $\{\alpha_0, \alpha_1\}$. Hence there exists a $k \in \{v\}$ with the property that if $k_0, k_1$ are given by $k_0 \equiv \alpha_0 + k \pmod{v}$ and $k_1 \equiv \alpha_1 + k \pmod{v}$ then there exists $k_2, k_3, \ldots, k_{p - 1} \in \{v\}$ such that $\{k_0, k_1, \ldots, k_{p - 1}\} \in F_v \cup A_v$.  

Now take \( x_0, x_1 \in [u] \) such that \( X_0 + k \equiv x_0v + k_0(\text{mod } uv) \) and \( X_1 + k \equiv x_1v + k_1(\text{mod } uv) \) and consider \( \{x_0, x_1\} \). By a similar argument to that given in the previous paragraph we deduce that there exists an \( l \in [u] \) such that if \( l_0, l_1 \in [u] \) are given by \( l_0 \equiv x_0 + l(\text{mod } u) \) and \( l_1 \equiv x_1 + l(\text{mod } u) \) then there exists \( l_2, l_3, ..., l_{p-1} \in [u] \) such that \( \{l_0, l_1, ..., l_{p-1}\} \in F_u \cup P_u \cup A_u \).

Denote by \( \{k'_0, k'_1, ..., k'_{p-1}\} \) the starter \( \{k_0, k_1, ..., k_{p-1}\} \) with its elements permuted into the arbitrary but fixed order referred to in the third paragraph of this proof. Likewise \( \{l'_0, l'_1, ..., l'_{p-1}\} \) is the appropriate permutation of \( \{l_0, l_1, ..., l_{p-1}\} \). Suppose \( l'_0 = l_0 \) and \( l'_i = l_i, \; i \neq j \). Since the group \( \langle z \rightarrow az + b(\text{mod } p), \; a \neq 0 \rangle \) is doubly transitive, there will be a pair of values \( a \) and \( b \) for which \( k'_a + b = k_0 \) and \( k'_a + b = k_1 \). For these values of \( a \) and \( b \) the starter \( \{l'_0v + k'_b, \; l'_1v + k'_a + b, \; ..., l'_pv + k'_a + b, \; l'_1v + k'_a + b\} \) (or a starter giving rise to the same orbit) will lie in the collection \( P \) provided that we do not have both \( \{l_0, l_1, ..., l_{p-1}\} \in A_u \) and \( \{k_0, k_1, ..., k_{p-1}\} \in A_v \). To see that the starter is not of this form consider its image under the mapping \( z \rightarrow z - (l_0v + k)(\text{mod } uv) \). The image of \( l'_0v + k'_a + b \) is \( l_0v + k_0 - (l_0v + k) \equiv X_0 \) and the image of \( l'_1v + k'_a + b \) is \( l_1v + k_1 - (l_0v + k) \equiv X_1 \).

Moreover, the starter quoted above clearly generates a \( p \)-block which contains the 2-block \( \{X_0, X_1\} \), thus completing the proof.

**Theorem 2.** Suppose \( p \) is prime and that there exists a CS(2, \( p, u \)) and a CS(2, \( p, v, -m \)), the latter system being composed entirely of full orbits. Then there exists a CS(2, \( p, uv, -um \)).

**Proof.** The proof follows that of Theorem 1. The products \( F_vF_u, P_vF_v, \) and \( A_uF_v \) are defined as before except that \( F_v \) now denotes a set of starters for full orbits forming a CS(2, \( p, v, -m \)). The collection \( P \) is the union of these three products alone and we therefore obtain \( \#P \leq uv(\text{mod } uv) \), where \( |F_v| = (v-1)/p(p-1) - (m-1)/p(p-1) = (v-m)/p(p-1) \). Hence \( \#P \leq uv(\text{mod } uv) \).

The argument locating a 2-block \( \{X_0, X_1\} \) holds as before provided that \( X_1 - X_0 \) is not divisible by \( v/m \). (If \( (v/m)(X_1 - X_0) \) then one of the starters in \( F_v \) will generate a \( p \)-block containing \( \{x_0, x_1\} \), where \( x_0 \equiv X_0(\text{mod } v) \) and \( x_1 \equiv X_1(\text{mod } v) \)). It follows that \( P \) necessarily generates a CS(2, \( p, uv, -um \)).

**Corollary.** If, in addition to the conditions of the theorem, there exists a CS(2, \( p, um \)), then there exists a CS(2, \( p, uv \)).

**Theorem 3.** The results of Theorems 1 and 2 remain true if the prime \( p \)
is replaced by a prime power $p^x$ ($x > 1$), provided that there is a system CS(2, $p^x$, $u$) composed entirely of full orbits.

Note. At first sight the construction appears to apply to CS(2, $p^x$, $u$) composed of both full and $(1/p)$th orbits. However, there are no such systems; the admissibility conditions ensure that a CS(2, $p^x$, $u$) containing a $(1/p)$th orbit contains a $(1/p^2)$th orbit.

Proof. The modifications to the two earlier proofs are identical, all subscripts and subscript arithmetic to be in $GF(p^x)$ with $a, b \in GF(p^x)$, $a \neq 0$. The construction of the individual products is as before, omitting $P_u$. In the location of a given 2-block $\{X_0, X_1\}$ we note that the group $\langle z \to az + b, a, b \in GF(p^x), a \neq 0 \rangle$ is doubly transitive on $GF(p^x)$.

3. CONCLUDING REMARKS

We observe that in the case of Theorem 1, a modified construction is possible whenever $u$ and $v$ are coprime. The modifications are that the product starters $\{(x, \alpha)\}$ with elements in $[uv]$ are replaced by $\{(x, \alpha)\}$ with elements in $[u] \times [v]$ and that the orbits are now generated by the action of the group $\langle (x, \alpha) \to (x + 1 (\text{mod } u), \alpha + 1 (\text{mod } v)) \rangle$ which is cyclic of order $uv$. The requirement for $u$ and $v$ to be coprime clearly implies that at most one of the systems CS(2, $p$, $u$) and CS(2, $p$, $v$) contains a $(1/p)$th orbit, and so it appears that this modified construction cannot yield an improvement on our results given above.

ACKNOWLEDGMENTS

We would like to express our thanks to the referee for bringing to our attention the results of Jimbo and Kuriki [5] where both the results of Colbourn and Colbourn [2] and the present results are obtained in the context of orthogonal arrays and row difference schemes.

REFERENCES

6. R. PELTESOHN, Eine Lösung der beiden Heffterschen Differenzenprobleme, Compositio Math. 6 (1939), 251-257.