ISRAEL JOURNAL OF MATHEMATICS, Vol. 40, No. 2, 1981

EDGE PARTITIONS OF THE COMPLETE SYMMETRIC DIRECTED GRAPH AND RELATED DESIGNS†

BY

BRIAN ALSPACH,‡ KATHERINE HEINRICH AND MOSHE ROSENFELD

ABSTRACT

We show that the edges of the complete symmetric directed graph on n vertices can be partitioned into directed cycles (or anti-directed cycles) of length $n-1$ so that any two distinct cycles have exactly one oppositely directed edge in common when $n = p^e > 3$, where p is a prime and e is a positive integer. When the cycles are anti-directed p must be odd. We then consider the designs which arise from these partitions and investigate their construction.

§1. Introduction

The problem of partitioning the edges of the complete symmetric directed graph DK_n on n vertices into isomorphic copies of a certain specified subgraph has been considered by many authors. We shall first consider the problem of partitioning the edges of DK_n into directed cycles of length $n-1$ with the property P that any two distinct cycles have exactly one oppositely directed edge in common. We then consider the problem of partitioning the edges of DK_n into anti-directed cycles of length $n-1$ with property P. This second partition gives rise to a new design which we call an A-design. Not all A-designs arise in this way and their existence will be further investigated in Section 3.

§2. Directed graphs

We shall denote by DK_n the complete symmetric directed graph on n vertices; by DC_n the directed cycle of length n; and by AC_n the anti-directed cycle of

†We would like to thank the Mathematics Department of the University of Arizona for their hospitality during January 1979 when this work was begun.

‡Partial support was provided for this research by the Natural Sciences and Engineering Research Council of Canada under Grant A-4792.

Received February 20, 1980 and in revised form February 18, 1981

length n. When we refer to the edge uv we mean the directed edge from u to v. Hence we shall write $D:(d_1, d_2, \cdots, d_k)$ for the directed cycle of length k consisting of the edges $d_1d_2, d_2d_3, \cdots, d_{k-1}d_k, d_kd_1$ and $A:(a_1, a_2, \cdots, a_{2k})$ for the anti-directed cycle of length $2k$ (clearly an anti-directed cycle must have even length) consisting of the edges a_1a_2, a_3a_2, a_3a_4, $a_5a_4, \cdots, a_{2k-1}a_{2k}$, a_1a_{2k}. For other graph theoretic terms the reader is referred to Bondy and Murty [3].

The problem of partitioning the edges of DK_n into copies of DC_{n-1} has been solved by Bermond and Faber [1] who showed that such a partition exists for all $n \geqq 4$. Hering and Rosenfeld [9] have since asked if it is possible to partition the edges of DK_n into copies of DC_{n-1} with the property that if D_1 and D_2 are any two distinct cycles in the partition, then there is exactly one edge uv of DK_n so that uv is an edge of D_1 and vu is an edge of D_2. This property will be referred to as property P and we shall write $DK_n \to DC_{n-1}$ if such an edge partition with property P exists. The partitions given by Bermond and Faber do not have property P. It will be shown that $DK_n \to DC_{n-1}$ when $n = p^e > 3$, where p is a prime and e is a positive integer.

Rosenfeld then went on to ask if the edges of DK_n, n odd, could be partitioned into copies of AC_{n-1} with property P. Writing $DK_n \to AC_{n-1}$ if such a partition exists, we shall show that $DK_n \to AC_{n-1}$ when $n = p^e > 3$, where p is an odd prime and e is a positive integer.

Labelling the vertices of DK_5 by 1, 2, 3, 4, 5 we see that $DK_5 \to DC_4$ as given by the cycles $D_1:(2,4,5,3)$, $D_2:(1,4,3,5)$, $D_3:(1,2,5,4)$, $D_4:(1,5,2,3)$ and $D_5:(1,3,4,2)$ and that $DK_5 \to AC_4$ as given by the cycles $A_1:(2,3,5,4)$, $A_2:(1,3,4,5)$, $A_3:(4,1,5,2)$, $A_4:(2,1,3,5)$, and $A_5:(1,2,3,4)$.

THEOREM 2.1. *When $n = p^e > 3$, where p is a prime and e is a positive integer, then $DK_n \to DC_{n-1}$.*

PROOF. Label the vertices of DK_n with the elements of GF(n) where GF(n) denotes the Galois field with $n = p^e$ elements. Let b be a generator of the multiplicative cyclic group of GF(n).

Consider the cycle $D_0:(1, b, b^2, \cdots, b^{n-2})$ where $b^{n-1} = 1$. Define further $n-1$ cycles by $D_k:(1+b^k, b+b^k, b^2+b^k, \cdots, b^{n-2}+b^k)$ for $k = 1, 2, \cdots, n-1$. It is clear that each of the cycles D_k, $k = 0, 1, \cdots, n-1$, has length $n-1$. If an edge occurred in more than one cycle, we would have either

$$b^i = b^j + b^k \quad \text{and} \quad b^{i+1} = b^{j+1} + b^k, \qquad 1 \leqq k \leqq n-1,$$

or

$$b^i + b^k = b^j + b^{k'} \quad \text{and} \quad b^{i+1} + b^k = b^{j+1} + b^{k'}, \qquad 1 \leqq k < k' \leqq n-1,$$

for some i and j. Both are impossible given that b is not 0 or 1 and $i \neq j$. Thus every edge occurs in at most one cycle and since the n cycles account for $n(n-1)$ edges, then every edge of DK_n occurs in exactly one of the cycles so that $D_0, D_1, \cdots, D_{n-1}$ partition the edges of DK_n.

We must now show that this partition of the edges of DK_n has property P. Consider the system S of equations

$$bx - y = a, \qquad x - by = a$$

in GF(n) where b is as before and a an element of GF(n). Since $1 - b^2 \neq 0$, then S has a unique solution (x, y) with x and y in GF(n).

Let us now suppose that the cycles D_0 and D_k, $1 \leqq k \leqq n-1$, have two oppositely directed edges in common. That is, there are two edges $b^i b^{i+1}$ and $b^j b^{j+1}$ in D_0, $i \neq j$, and two edges $(b^{i'} + b^k)(b^{i'+1} + b^k)$ and $(b^{j'} + b^k)(b^{j'+1} + b^k)$ in D_k, $i' \neq j'$, so that

$$b^i = b^{i'+1} + b^k, \quad b^{i+1} = b^{i'} + b^k, \quad b^j = b^{j'+1} + b^k \quad \text{and} \quad b^{j+1} = b^{j'} + b^k.$$

From these we have two systems of equations

$$bb^i - b^{i'} = b^k, \qquad bb^j - b^{j'} = b^k,$$

and

$$b^i - bb^{i'} = b^k, \qquad b^j - bb^{j'} = b^k,$$

denoted S_1 and S_2, respectively. Clearly S_1 has unique solution $(b^i, b^{i'})$ where $i - i' = (n-1)/2$ and S_2 has unique solution $(b^j, b^{j'})$ where $j - j' = (n-1)/2$. But S_1 and S_2 both represent S and hence $b^i = b^j$ and $b^{i'} = b^{j'}$, whence $i = j$ and $i' = j'$, a contradiction.

By the same argument we can show that the cycles D_k and $D_{k'}$, $1 \leqq k < k' \leqq n-1$, have at most one oppositely directed edge in common. Consequently, any two cycles have at most one oppositely directed edge in common and since every cycle has $n-1$ edges it must have exactly one oppositely directed edge in common with each other cycle. Thus the edge partition has property P. □

It is also known that $DK_{12} \rightarrow DC_{11}$ and $DK_{15} \rightarrow DC_{14}$. These will be dealt with in Section 2.

If we let $2K_n$ denote the complete multigraph on n vertices in which each edge has multiplicity two, let C_n denote the undirected cycle of length n and write $U:(u_1, u_2, \cdots, u_n)$ for the cycle consisting of the undirected edges $u_1u_2, u_2u_3, \cdots, u_{n-1}u_n, u_nu_1$ and let $2K_n \rightarrow C_{n-1}$ mean that we can partition the edges of $2K_n$ into cycles of length $n-1$ in which every pair of distinct cycles have exactly one edge in common, then from Theorem 2.1 we obtain the following corollary.

COROLLARY 2.2. *When $n = p^e > 3$, where p is a prime and e is a positive integer, then $2K_n \to C_{n-1}$.*

PROOF. The proof follows immediately from Theorem 2.1. Simply take the construction there and replace each of the $n(n-1)$ directed edges by an undirected edge. □

It can also be shown that $2K_6 \to C_5$, $2K_{10} \to C_9$, $2K_{14} \to C_{13}$, $2K_{12} \to C_{11}$ and $2K_{15} \to C_{14}$. The latter two follow from the comment after Theorem 2.1 and Corollary 2.2 while the first three are given below. None of the three can be oriented to give $DK_n \to DC_{n-1}$. The fact that $2K_6 \to C_5$ is of particular interest since $DK_6 \to DC_5$ is impossible as we shall see in Section 3.

Labelling the vertices of $2K_n$ by $1, 2, \cdots, n$ we see that $2K_6 \to C_5$ as given by the cycles $U_1:(2,3,6,4,5)$, $U_2:(1,3,4,5,6)$, $U_3:(1,2,4,6,5)$, $U_4:(1,5,3,2,6)$, $U_5:(1,2,6,3,4)$ and $U_6:(1,3,5,2,4)$. We see that $2K_{10} \to C_9$ as given by the cycles $U_1:(2,7,4,3,8,6,5,9,10)$, $U_6:(2,8,7,10,3,1,4,5,9)$, $U_{\sigma^i(1)}$ and $U_{\sigma^i(6)}$, $1 \leqq i \leqq 4$, where σ is the permutation $(1\,2\,3\,4\,5)(6\,7\,8\,9\,10)$ and $U_{\sigma^i(k)}$ is obtained by applying the permutation σ^i to the vertices in U_k, $k = 1$ or 6. Finally we see that $2K_{14} \to C_{13}$ as given by the cycles $U_1:(4,11,9,12,5,7,6,14,13,3,8,2,10)$, $U_8:(3,12,2,7,6,11,10,13,4,1,5,9,14)$, $U_{\sigma^i(1)}$ and $U_{\sigma^i(8)}$, $1 \leqq i \leqq 6$, where σ is the permutation $(1\,2\,3\,4\,5\,6\,7)(8\,9\,10\,11\,12\,13\,14)$ and $U_{\sigma^i(k)}$ is obtained by applying σ^i to the vertices of U_k, $k = 1$ or 8.

The next two theorems deal with the problem of partitioning the edges of DK_n into anti-directed cycles with property P.

THEOREM 2.3. *When $n = p^e$, where p is a prime, e is a positive integer and $n \equiv 1$ (modulo 4), then $DK_n \to AC_{n-1}$.*

PROOF. As before label the elements of DK_n with the elements of $\mathrm{GF}(n)$. Let b be a generator of the multiplicative cyclic group of $\mathrm{GF}(n)$ and consider the anti-directed cycle $A_0:(1, b, b^2, \cdots, b^{n-2})$ where $b^{n-1} = 1$. We now define another $n-1$ anti-directed cycles by $A_k:(1+b^k, b+b^k, \cdots, b^{n-2}+b^k)$ for $k = 1, 2, \cdots, n-1$.

If we now show that no edge occurs in two cycles, then by a simple counting argument it follows that we have a partition of the edges of DK_n into anti-directed cycles of length $n-1$. Suppose some edge occurs in two cycles. First, let one of the cycles be A_0 and the other A_k, $1 \leqq k \leqq n-1$. The edge then is either represented as $b^{2i}b^{2i-1}$ and $(b^{2j}+b^k)(b^{2j-1}+b^k)$, or as $b^{2i}b^{2i-1}$ and

$(b^{2i}+b^k)(b^{2j+1}+b^k)$ where i and j are distinct and $1 \leqq i, j \leqq (n-1)/2$. In the first case we have $b^{2i-1}(b-1) = b^{2j-1}(b-1)$, and since b is not 0 or 1 and $1 \leqq i$, $j \leqq (n-1)/2$, then we must have $i = j$ which is a contradiction. In the second case we have $b^{2i-1}(b-1) = b^{2j}(1-b)$ and since b is not 0 or 1 and $b^{(n-1)/2} \neq -1$, then $2i - 1 \equiv 2j + (n-1)/2$ (modulo $n-1$). But since $n \equiv 1$ (modulo 4), then $(n-1)/2 \equiv 0$ (modulo 2) and so $2i - 1 \not\equiv 2j + (n-1)/2$ (modulo $n-1$) and the desired equality can never hold. The case when the two cycles are A_k and $A_{k'}$, $1 \leqq k < k' \leqq (n-1)/2$, is dealt with in the same way.

It remains now to show that the partition has property P. To do this it suffices to show that any two distinct cycles have at least one oppositely directed edge in common.

First we write A_k^* to denote the cycle A_k in which the orientation on each edge is reversed. Again, consider the system S of equations

$$bx - y = a, \qquad x - by = a$$

in GF(n) where b is as defined earlier and a is an element of GF(n). Since $b^2 - 1 \neq 0$, then S has a unique solution (x, y) where x and y are in GF(n). Putting $x = b^r$ and $y = b^s$, and substituting in S yields

$$b^{r+1} - b^s = a, \qquad b^r - b^{s+1} = a$$

implying $b^r = -b^s$ and hence $r \equiv s + (n-1)/2$ (modulo $n-1$). Since $n \equiv 1$ (modulo 4) then r and s have the same parity.

In the case when both r and s are odd, let $b^r = b^{2i-1}$ and $b^s = b^{2j-1}$ and let $a = b^k$. Then we have

$$b^{2i} - b^{2j-1} = b^k, \qquad b^{2i-1} - b^{2j} = b^k$$

implying that

$$b^{2i} = b^{2j-1} + b^k, \qquad b^{2i-1} = b^{2j} + b^k.$$

So identifying vertices in the cycles A_0 and A_k^* means that the edge $b^{2i}b^{2i-1}$ in A_0 is the same as the edge $(b^{2j-1}+b^k)(b^{2j}+b^k)$ in A_k^*. Letting $a = b^k - b^{k'}$ and using the above argument shows that A_k^* and $A_{k'}$ have an edge in common.

Now, in the case when both r and s are even, let $b^r = b^{2i}$ and $b^s = b^{2j}$. The desired result follows in the same way as when both r and s are odd. □

Theorem 2.4. *When $n = p^e > 3$, where p is a prime, e is a positive integer and $n \equiv 3$ (modulo 4), then $DK_n \to AC_{n-1}$.*

Proof. Label the vertices of DK_n with the elements of GF(n). Let b be a generator of the multiplicative cyclic group of non-zero elements of GF(n). Then b^2 generates the quadratic residues, denoted $Q(n)$. For each $m = 1, 2, \cdots, (n-1)/2$ we claim that the sequence of vertices $1, b^{2m+3}, b^2, b^{2m+5}, b^4, b^{2m+7}, \cdots, b^{n-3}, b^{2m+n}$ are all distinct. This follows since the entries in the odd indexed coordinates are just the elements from $Q(n)$ while the remaining entries are $b^{2m+3} \cdot Q(n)$ and since b^{2m+3} is a quadratic non-residue these are all the non-zero quadratic non-residues of GF(n).

For some $m \in \{1, 2, \cdots, (n-1)/2\}$ we claim that $(b^{2m+3}-1)/(b^{2m+1}-1)$ is not a quadratic residue. If

$$\frac{b^{2m+3}-1}{b^{2m+1}-1} = \frac{b^{2j+3}-1}{b^{2j+1}-1},$$

then $b^{2j+1}(b^2-1) = b^{2m+1}(b^2-1)$ which implies $b^{2j+3} = b^{2m+3}$. Thus the elements $(b^{2m+3}-1)/(b^{2m+1}-1)$ are all distinct for $m = 1, 2, \cdots, (n-1)/2$. Since none of them equals 1, since they are all distinct and since the number of quadratic residues equals $(n-1)/2$, the claim is seen to be true.

Let $m \in \{1, 2, \cdots, (m-1)/2\}$ be such that $(b^{2m+3}-1)/(b^{2m+1}-1)$ is not a quadratic residue in GF(n). Consider the anti-directed cycle $A_0 : (1, b^{2m+3}, b^2, b^{2m+5}, b^4, \cdots, b^{n-1}, b^{2m+n})$ and, as in Theorem 2.3, define another $n-1$ anti-directed cycles $A_k : (1 + b^k, b^{2m+3} + b^k, b^2 + b^k, b^{2m+5} + b^k, \cdots, b^{n-1} + b^k, b^{2m+n} + b^k)$ for $1 \leqq k \leqq n-1$. We shall now prove that the anti-directed cycles $A_0, A_1, \cdots, A_{n-1}$ partition the edges of DK_n and have property P. If the same edge of DK_n is in two distinct cycles, say A_k and $A_{k'}$, then we have one of the following:

(i) $b^k + b^{2r} = b^{k'} + b^{2s}$ and $b^k + b^{2m+2r+1} = b^{k'} + b^{2m+2s+1}$,

(ii) $b^k + b^{2r} = b^{k'} + b^{2s}$ and $b^k + b^{2m+2r+1} = b^{k'} + b^{2m+2s+3}$,

(iii) $b^k + b^{2r} = b^{k'} + b^{2s}$ and $b^k + b^{2m+2r+3} = b^{k'} + b^{2m+2s+3}$.

Subtracting the two equations in each of (i) and (iii) leads to $b^{2r} = b^{2s}$ which is impossible because $k \neq k'$. Subtracting the equations in (ii) leads to $b^{2r}(b^{2m+1}-1) = b^{2s}(b^{2m+3}-1)$ or $b^{2r}/b^{2s} = (b^{2m+3}-1)/(b^{2m+1}-1)$. The left hand side of this equation is a quadratic residue but m was chosen so that the right hand side is not a quadratic residue. Hence, (ii) cannot happen and we see that the anti-directed cycles partition DK_n.

It now suffices to prove that any two of the cycles intersect in two oppositely directed edges. First we remark that

$$\frac{b^{2(n-3)/2+3}-1}{b^{2(n-3)/2+1}-1} = \frac{b-1}{b^{n-2}-1} = \frac{b(b-1)}{1-b} = -b$$

is a quadratic residue because $b \not\in Q(n)$. Thus, $2m+3 \neq 1$ so that $2m+3 \in \{3, 5, \cdots, n-2\}$ which means that $b^{2m+3}b^{2m+1} \neq 1$. Thus, the system S of linear equations

$$x - b^{2m+1}y = a, \qquad b^{2m+3}x - y = a$$

has a unique solution (x, y) where x and y are in $\mathrm{GF}(n)$. If $a \neq 0$, both x and y are non-zero. In this case let $x = b^r$ and $y = b^s$. Substitution in S yields $b^r(1 - b^{2m+3}) = b^s(b^{2m+1} - 1)$ which implies that $r \equiv s$ (modulo 2).

We now consider the cycles A_k and $A_{k'}$, $k \neq k'$ and both non-zero, and consider the case that r and s are both even. Substitute $b^{2i} = x$ and $b^{2j} = y$ in S with $a = b^k - b^{k'}$ to obtain

$$b^{2i} - b^{2m+2j+1} = b^k - b^{k'}, \qquad b^{2m+3+2i} - b^{2j} = b^k - b^{k'}.$$

This yields $b^{k'} + b^{2i} = b^k + b^{2m+2j+1}$ and $b^{k'} + b^{2m+2i+3} = b^k + b^{2j}$ or $(b^{k'} + b^{2i})(b^{k'} + b^{2m+2i+3}) = (b^k + b^{2m+2j+1})(b^k + b^{2j})$. The first is an edge of $A_{k'}$ and the second is an edge of A_k^*. In the case that both r and s are odd, a similar result is obtained by noticing that if (x, y) is a solution of S with $a = b^k - b^{k'}$, then $(-x, -y)$ is a solution of S with $a = b^{k'} - b^k$. Now $-x = b^{2i}$ and $-y = b^{2j}$ so that we again obtain that A_k and $A_{k'}^*$ intersect in an edge.

Finally, if either $k = 0$ or $k' = 0$, then a similar intersection result is easy to obtain. □

In a preliminary draft of this paper, the proof of Theorem 2.4 used a construction which needed a generator b of the multiplicative group of nonzero elements of $\mathrm{GF}(n)$ such that $-(b^2 + b + 1)$ is a quadratic residue of $\mathrm{GF}(n)$. W. Veléz was asked about the existence of such an element in $\mathrm{GF}(n)$ and this eventually led to more general work with D. Madden [13]. Unfortunately, their results do not work for fields of characteristic 3 and so the above alternate construction was found.

§3. Designs

Many authors have studied the relationship between combinatorial designs and certain edge partitions of graphs. The reader is referred to Bermond and Sotteau [2], Dénes and Keedwell [5, chapter 9], Harary and Wallis [6], Hell and Rosa [8], Kotzig [11] and in particular Keedwell [10], although there are many more papers on the subject. We shall further study this relationship.

A latin square of order n is an $n \times n$ array with the property that each of the elements $1, 2, \cdots, n$ occurs exactly once in each row and column of the array. We write the latin square A as $A = (a_{ij})$ where a_{ij} denotes the element in the ith row and jth column. Two latin squares $A = (a_{ij})$ and $B = (b_{ij})$ of order n are orthogonal if when superimposed, the ordered pairs (a_{ij}, b_{ij}) constitute all n^2 ordered pairs from the set $\{1, 2, \cdots, n\}$. A latin square A is self-orthogonal if it is orthogonal to its transpose A^T. For further definitions the reader is referred to [5].

THEOREM 3.1. *If $DK_n \to DC_{n-1}$, then there exists a self-orthogonal latin square of order n.*

PROOF. Label the vertices of DK_n with the elements $1, 2, \cdots, n$. Since each vertex of DK_n is contained in exactly $n-1$ of the n directed cycles in the partition, there is exactly one cycle which does not contain that vertex. Label all edges in this cycle with the same label as this vertex.

Construct an order n array $A = (a_{ij})$ as follows. Put $a_{ii} = i$ for all i and $a_{ij} = k$, $i \neq j$, if and only if k is the label on the edge ij. We claim that A is a self-orthogonal latin square.

Consider the ith row of A. Since the vertex labelled i occurs exactly once in each cycle except the one with edges labelled i, then the edges ij, $j = 1, 2, \cdots, i-1, i+1, \cdots, n$, are labelled $1, 2, \cdots, i-1, i+1, \cdots, n$ in some order. Consequently, each row of A contains the elements $1, 2, \cdots, n$. The same argument can be applied to the columns and hence A is a latin square.

Let $k \neq k'$ with $1 \leqq k, k' \leqq n$. We know there exists an edge ij of DK_n such that the cycle whose edges are labelled with k contains ij and the cycle whose edges are labelled with k' contains ji. Hence, the ordered pair (k, k') occurs when A^T and A are superimposed. The ordered pair (k, k) occurs in the kth row and kth column when A^T and A are superimposed. Hence A is a self-orthogonal latin square. □

Since it is now a well known fact that there exists a self-orthogonal latin square of every order n, $n \neq 2, 3, 6$ (Brayton, Coppersmith and Hoffman [4]), the result of Theorem 3.1 serves only to illustrate the relationship between edge partitions of graphs and designs. It is not difficult to see that the converse of Theorem 3.1 is not true although the latin squares of orders 12 and 15 given by Brayton, Coppersmith and Hoffman do in fact give rise to edge partitions showing that $DK_{12} \to DC_{11}$ and $DK_{15} \to DC_{14}$.

A more interesting design arises when we look at $DK_n \to AC_{n-1}$. In this case an order n array $A = (a_{ij})$ is constructed by first labelling the vertices and cycles of DK_n as was done in Theorem 3.1 and then putting $a_{ii} = i$ for all i and $a_{ij} = k$, $i \neq j$, if and only if the edge ij is labelled k. This array A, which we shall call an A-design of order n where n is odd, has the following properties.

(1) The array contains only the elements $1, 2, \cdots, n$.

(2) The main diagonal of A consists of the elements $1, 2, \cdots, n$.

(3) If the element k occurs in the ith row (or column), $k \neq i$, then it occurs twice in that row (or column).

(4) The element i occurs exactly once in the ith row and ith column ($a_{ii} = i$).

(5) Between them the ith row and ith column contain each of the elements $1, 2, \cdots, n$ exactly twice. (We count i twice; once in the row and once in the column.)

(6) When A is superimposed on its transpose every ordered pair (i, j), $i, j \in \{1, 2, \cdots, n\}$, occurs exactly once.

An A-design of order 21 is shown in Fig. 3.1.

As seen from the A-design of order 21 the existence of an A-design does not imply that $DK_n \to AC_{n-1}$. However, the A-design of order n gives a "covering" of DK_n in the sense that it defines a partition of the edges so that each set of edges in the partition forms anti-directed cycles which cover all but one vertex of DK_n.

The question now is, "Does there exist an A-design for every odd order n?". Clearly an A-design exists when $n = p^e > 3$, where p is an odd prime and e is a positive integer, and, as is easily seen, does not exist when $n = 3$.

1	5	2	5	2	9	6	9	6	13	10	13	10	17	14	17	14	21	18	21	18
4	2	1	1	4	21	19	20	18	9	7	8	6	21	19	20	18	9	7	8	6
4	5	3	5	4	20	18	21	19	8	6	9	7	20	18	21	19	8	6	9	7
3	3	2	4	2	18	20	19	21	6	8	7	9	18	20	19	21	6	8	7	9
3	3	1	1	5	19	21	18	20	7	9	6	8	19	21	18	20	7	9	6	8
8	17	15	16	14	6	1	1	8	5	3	4	2	5	3	4	2	17	15	16	14
8	16	14	17	15	9	7	9	8	4	2	5	3	4	2	5	3	16	14	17	15
7	14	16	15	17	7	6	8	6	2	4	3	5	2	4	3	5	14	16	15	17
7	15	17	14	16	7	1	1	9	3	5	2	4	3	5	2	4	15	17	14	16
12	17	15	16	14	21	19	20	18	10	1	1	12	21	19	20	18	17	15	16	14
12	16	14	17	15	20	18	21	19	13	11	13	12	20	18	21	19	16	14	17	15
11	14	16	15	17	18	20	19	21	11	10	12	10	18	20	19	21	14	16	15	17
11	15	17	14	16	19	21	18	20	11	1	1	13	19	21	18	20	15	17	14	16
16	13	11	12	10	13	11	12	10	9	7	8	6	14	1	1	16	9	7	8	6
16	12	10	13	11	12	10	13	11	8	6	9	7	17	15	17	16	8	6	9	7
15	10	12	11	13	10	12	11	13	6	8	7	9	15	14	16	14	6	8	7	9
15	11	13	10	12	11	13	10	12	7	9	6	8	15	1	1	17	7	9	6	8
20	13	11	12	10	13	11	12	10	5	3	4	2	5	3	4	2	18	1	1	20
20	12	10	13	11	12	10	13	11	4	2	5	3	4	2	5	3	21	19	21	20
19	10	12	11	13	10	12	11	13	2	4	3	5	2	4	3	5	19	18	20	18
19	11	13	10	12	11	13	10	12	3	5	2	4	3	5	2	4	19	1	1	21

Fig. 3.1.

THEOREM 3.2. *If there exists an A-design of order n, an A-design of order k and a pair of orthogonal latin squares of order k, then there exists an A-design of order nk.*

PROOF. Let A be an A-design of order n, let B be an A-design of order k and let C and D be a pair of orthogonal latin squares of order k. Begin with $A = (a_{ij})$ and replace each element a_{ii} with a copy of B, adding $k(a_{ii} - 1)$ to each element in B. If $i > j$ replace each element a_{ij} with a copy of C, adding $k(a_{ij} - 1)$ to each element in C; and if $i < j$ replace each element a_{ij} with a copy of D^T, again adding $k(a_{ij} - 1)$ to each element in D^T.

It is not difficult to verify that the resulting array is an A-design of order nk. □

COROLLARY 3.3. *If n is odd and $n \not\equiv 3$ or 6 (modulo 9), then there exists an A-design of order n.*

PROOF. Since there exists an A-design of order $p^e > 3$, where p is an odd prime and e is a positive integer, and since there exists a pair of orthogonal latin squares of every odd order greater than 3, then by Theorem 3.2 there exists an A-design of odd order n except perhaps when $n \equiv 3$ or 6 (modulo 9). □

Although we have not been able to construct A-designs for every odd order n, $n \equiv 3$ or 6 (modulo 9), we have constructed many infinite families of these orders. To do this we use a construction based on the singular direct product for quasigroups which was first introduced by Sade (see Lindner [12]).

THEOREM 3.4. *If there exists an A-design of order n, an A-design of order m with an A-subdesign of order k and a pair of orthogonal latin squares of order $m - k$, then there exists an A-design of order $n(m - k) + k$.*

PROOF. Let $A = (a_{ij})$ be an A-design of order n, let B be an A-design of order m with an A-subdesign C of order k, and let D and E be a pair of orthogonal latin squares of order $m - k$.

Let $F = (f_{ij})$ be an array of order $n + 1$. Replace f_{11} with a copy of C. Replace the four elements f_{11}, f_{1i}, f_{i1} and f_{ii} with a copy of B so that its A-subdesign C is in the upper left corner and agrees with the copy of C already in the f_{11} position. This copy of C is based on the elements $1, 2, \cdots, k$ and we add $(m - k)(a_{ii} - 1)$ to each of the elements $k + 1, k + 2, \cdots, m$ in B. If $i > j$ replace f_{ij} with a copy of D, adding $(m - k)(a_{ij} - 1) + k$ to each element in D; and if $i < j$ replace f_{ij} with a copy of E^T, again adding $(m - k)(a_{ij} - 1) + k$ to each element in E^T.

It is not difficult to check that the resultant array is an A-design of order $n(m - k) + k$. □

Using Theorem 3.4 many A-designs of order n, $n \equiv 3$ or 6 (modulo 9) can be constructed. For example, if $n \equiv 3$ (modulo 9) and $n = 3mk$ where $m \equiv 2$ (modulo 5), then by Theorem 3.4 there exists an A-design of order $3m$ (as $3m = 3(5r+2) = 5((3r+2)-1)+1$) and hence by Theorem 3.2 there exists an A-design of order $n = 3mk$. The A-design of order 21 was obtained in this way. It is not difficult to find many other infinite families in similar ways.

However, many orders remain unknown, the first being as small as order 15. What we hope for is a direct construction of A-designs of order $3p$, where p is a prime, as this and Theorem 3.2 would suffice to show the existence of A-designs of every odd order n, $n \geqq 5$.

To our knowledge these designs (A-designs) have not arisen before although certain "generalizations" of orthogonality for latin squares have been considered (see [5, pp. 461–466] and [7]).

References

1. J.-C. Bermond and V. Faber, *Decomposition of the complete directed graph into k-circuits*, J. Combinatorial Theory Ser. B, **21** (1976), 146–155.

2. J.-C. Bermond and D. Sotteau, *Graph decompositions and G-designs*, Proc. Fifth British Combinatorial Conf., Aberdeen (1975), Congressus Num. XV, Utilitas Math., Winnipeg, pp. 53–72.

3. J. A. Bondy and U. S. R. Murty, *Graph Theory with Applications*, Macmillan, London, 1976.

4. R. K. Brayton, Don Coppersmith and A. J. Hoffman, *Self-orthogonal latin squares*, Teorie Combinatorie, Rome (1973), Vol. II (1976), pp. 509–517.

5. J. Dénes and A. D. Keedwell, *Latin Squares and their Applications*, Akadémiai Kiado, Budapest, 1974.

6. F. Harary and W. D. Wallis, *Isomorphic factorizations II; Combinatorial designs*, Proc. Eighth Southeastern Conf. Combinatorics, Graph Theory and Computing, 1977, pp. 13–28.

7. A. Hedayat and E. Seiden, F-*square and orthogonal* F-*square designs: A generalization of latin squares and orthogonal latin square designs*, Ann. Math. Statist. **41** (1970), 2035–2044.

8. Pavol Hell and Alexander Rosa, *Graph decompositions, handcuffed prisoners and balanced* P-*designs*, Discrete Math. **2** (1972), 229–252.

9. F. Hering and M. Rosenfeld, *Problem number* 38, in *Unsolved problems: Summer Research Workshop in Algebraic Combinatorics* (Katherine Heinrich, ed.), Simon Fraser University, 1979.

10. A. D. Keedwell, *On decompositions of complete graphs defined by quasigroups*, unpublished manuscript.

11. A. Kotzig, *Groupoids and partitions of complete graphs*, in *Combinatorial Structures and their Applications*, Proc. Calgary International Conf., 1969, pp. 215–221.

12. C. C. Lindner, *Applications of the singular direct product to constructing various types of orthogonal latin squares*, Proc. Conf. Combinatorics, Memphis State University, 1972. pp. 122–155.

13. D. Madden and William Yslas Veléz, *Polynomials that represent quadratic residues as primitive roots*, preprint.

Simon Fraser University
Burnaby, B.C., Canada V5A 1A6

Ben Gurion University of the Negev
Beer Sheva, Israel