JOURNAL OF COMBINATORIAL THEORY, Series A 25, 117–127 (1978)

# Conjugate Orthogonal Quasigroups

K. T. PHELPS*

*Mathematics Department, Auburn University, Auburn, Alabama 36830*

*Communicated by the Editors*

Received April 20, 1976

## 1. INTRODUCTION

The construction of orthogonal quasigroups, or equivalently orthogonal latin squares, has long been an area of intense mathematical research, culminating in the celebrated disproof of the Euler conjecture by Bose *et al.* [1]. A particularly interesting problem related to this, which has recently been solved by Brayton *et al.* [2], is that of constructing quasigroups orthogonal to their transpose. This, however, is a special case of the more general problem of constructing quasigroups orthogonal to their conjugate for each of the several possible conjugates. The problem was originally posed by Stein [15] in the hope that its solution would lead to a disproof of the Euler conjecture. As we shall see, it is the techniques developed in the disproof of the Euler conjecture which are in fact instrumental in determining the spectrum of conjugate orthogonal quasigroups. Before we proceed let us establish some terminology. In what follows everything is assumed to be finite.

A quasigroup is an ordered pair $(S, \cdot)$, where $S$ is a set and $\cdot$ is a binary operation defined on the set $S$ with unique solvability of the equations $x \cdot a = b$ and $a \cdot y = b$ for $x$ and $y$, respectively. A latin square can be considered as the multiplication table for a quasigroup with the headline and sideline removed. One other well-known concept which we will need is that of an orthogonal array. By an orthogonal array, $OA(n, k)$ we will mean an $n^2 \times k$ array with entries from a set $S$ of $n$ symbols such that if any two columns are juxtaposed, the rows will contain $n^2$ distinct ordered pairs. A quasigroup $(S, \cdot)$ of order $n$ is equivalent to an $OA(n, 3)$ with $(i, j, k)$ as a row if and only if $i \cdot j = k$. There are other characterizations of quasigroups, latin squares, and orthogonal arrays. The interested reader is referred to the excellent study by Denes and Keedwell [4] for further information.

* Present address: Mathematics Department, Georgia Institute of Technology, Atlanta, Georgia 30332.



0097-3165/78/0252-0117$02.00/0

Consider a quasigroup as an $OA(n, 3)$. It is clear that any permutation of the columns is again a quasigroup. The $\alpha$-conjugate of a quasigroup is the quasigroup that results from the application of the permutation $\alpha \in S_3$ (symmetric group on three symbols) to its columns, when considered as an $OA(n, 3)$. Applying the permutation (2, 1, 3) to an $OA(n, 3)$ is evidently the same as taking the transpose. Furthermore, given a quasigroup and its $\alpha$-conjugate we can construct an $n^2 \times 4$ array with $(i, j, k, l)$ as a row if and only if $(i, j, k)$ and $(i, j, l)$ are rows in the quasigroup and its $\alpha$-conjecture, respectively. If the resulting array is in fact an $OA(n, 4)$ then the quasigroup is said to be $\alpha$-conjugate orthogonal, or more specifically, $\alpha$-self-orthogonal. For a more general definition of conjugacy of polyadic algebras see Stein [15]. In what follows the permutation $\alpha = \binom{1\ 2\ 3}{i\ j\ k}$ will be notated by the triple $(i, j, k)$.

## 2. Preliminaries

In determining the spectrum for $\alpha$-self-orthogonal quasigroups we will restrict our attention to the four permutations (2, 3, 1), (3, 1, 2), (1, 3, 2), and (3, 2, 1). With this in mind we have the following definition:

DEFINITION. $B_\alpha = \{n \in Z^+ \mid \exists$ an $\alpha$-self-orthogonal quasigroup of order $n\}$.

LEMMA 2.1. (a) *$B_\alpha = B_\beta$ where $\alpha = (2, 3, 1)$, $\beta = (3, 1, 2)$.*

(b) *$B_\alpha = B_\beta$ where $\alpha = (3, 2, 1)$, $\beta = (1, 3, 2)$.*

*Proof.* (a) If $n \in B_\alpha$ consider an $OA(n, 4)$ as described at the end of Section 1 with rows $(i, j, k, l)$. The $\alpha$-permutations of $(i, j, k)$ give the rows $(i, j, l)$. But since $\alpha$ and $\beta$ are inverse permutations, the $\beta$-permutations of the rows $(i, j, l)$ give the rows $(i, j, k)$. Thus, if we interchange the last two columns we obtain an $OA(n, 4)$ with rows $(i, j, l, k)$ which represents a $\beta$-self-orthogonal quasigroup of order $n$. Thus $B_\beta \subseteq B_\alpha$, and, by symmetry, $B_\alpha \subseteq B_\beta$.

(b) If $\alpha$ is applied to $(a, b, c)$ then $(c, b, a)$ is obtained. If the transpose permutation (2, 1, 3) is applied to each of these then $(b, a, c)$ and $(b, c, a)$ are obtained, respectively. But if $\beta$ is applied to $(b, a, c)$ then $(b, c, a)$ is also obtained. Since the transpose clearly preserves orthogonality, $B_\alpha = B_\beta$. Thus we need only consider two conjugates (1, 3, 2) and (3, 1, 2).

We now present a series of well-known constructions originally developed by various authors, notably, Bose *et al.* [1], Wilson [16], and Sade [13]. The reader is referred to Denes and Keedwell [4], Hall [6], and Stein [15] for further information. The construction of quasigroups from finite fields and

Abelian groups are two such well-known constructions. Using these constructions Stein was able to show the following.

LEMMA 2.2 (Stein [15]). *If* $n \equiv 0, 1,$ *or* $3 \bmod 4$ *then there exists an* $(1, 3, 2)$*-self-orthogonal quasigroup of order* $n$.

Similarly, we have the following:

LEMMA 2.3. *If* $n$ *is a prime or power of a prime, and* $n > 2$, *then* $n \in B_\alpha$ *where* $\alpha = (3, 1, 2)$.

*Proof.* Choose $a, b \in GF(p^k)$, $p^k > 2$, such that $a, b, a^2 + b \neq 0$, then define the quasigroup operation by $x \circ y = a \cdot x + b \cdot y$, $x, y \in GF(p^k)$ with field operations $\cdot$, $+$. Clearly if $p^k > 2$ we cab choose appropriate $a$ and $b$, for instance, let $a = 1$, $b \neq -1$.

We remark that for $\alpha = (1, 3, 2)$ we can define a quasigroup in a similar except that for $a, b \in GF(p^k)$ we require $a, b, b + 1 \neq 0$. Since it will be needed later we note that in either of the above finite field constructions if we are able to find elements $a, b \in GF(p^k)$ that satisfy the additional constraint $a + b = 1$, then in each case, the quasigroup will be idempotent, that is, $x \circ x = x$ for all $x$.

Next we have the direct product and singular direct product constructions originally due to MacNeish [11] and Sade [13], respectively.

LEMMA 2.4. *If* $n, m \in B_\alpha$ *then* $n \cdot m \in B_\alpha$.

*Proof.* Direct product of quasigroups preserves orthogonality and it is easy to see that the $\alpha$-conjugate of the direct product will just be the direct product of the $\alpha$-conjugates.

The singular direct product (SDP) originally developed by Sade was later generalized and extensively used by Lindner. The definition that follows comes from the later author. Let $(Q, \cdot)$ be a quasigroup with a subquasigroup $(P, \cdot)$, and let $(V, *)$ be an idempotent quasigroup. Let $\bar{P} = Q \backslash P$ and $(\bar{P}, \otimes)$ be any other quasigroup then we can define a quasigroup $(S, \circ)$, where $S = P \cup \bar{P} \times V$, as follows:

(i) $p \circ q = p \cdot q, \qquad p, q \in P;$

(ii) $p \circ (q, v) = (p \cdot q, v), \qquad p \in P, q \in \bar{P}, v \in V,$
$(q, v) \circ p = (q \cdot p, v);$

(iii) $(p, v) \circ (q, v) = p \cdot q \qquad \text{if } p \cdot q \in P,$
$= (p \cdot q, v) \qquad \text{if } p \cdot q \in \bar{P};$

(iv) $(p, v) \circ (q, w) = (p \otimes q, v * w) \qquad \text{if } v \neq w.$

Using the above singular product construction we have:

LEMMA 2.5. *If there exists an idempotent $\alpha$-self-orthogonal quasigroup of order $n$, an $\alpha$-self-orthogonal quasigroup of order $m$ which has a subquasigroup of order $p$, and an $\alpha$-self-orthogonal quasigroup of order $m - p$ then* $n(m - p) + p \in B_\alpha$.

For the sake of brevity we omit the proof and instead refer the reader to Lindner [7, 8] and Steedly [14]. That the singular direct product will preserve orthogonality and conjugacy is contained in the above references.

The final general construction which we will introduce is the well-known construction of quasigroups from pairwise balanced designs. By a pairwise balanced design (PBD) we mean an ordered pair $(P, X)$ where $P$ is a set and $X$ a collection of subsets of $P$, called blocks, such that every two-element subset of $P$ occurs in exactly one block. If $b_1, b_2, ..., b_n$ are the blocks of PBD $(P, X)$ then on each block, $b_j$, we define an idempotent quasigroup $(b_j, \otimes_j)$. We can then define a quasigroup $(P, *)$ by:

(1) $p * p = p$,

(2) $p * q = p \otimes_j q$ where $p, q \in b_j$, $p \neq q$.

Clearly this is a quasigroup and its $\alpha$-conjugate is merely the quasigroup constructed from the same PBD using instead the $\alpha$-conjugates of the quasigroups $(b_j, \otimes_j)$, $j = 1,..., n$. We note that the conditions on the quasigroups $(b_j, \otimes_j)$ can be weakened if there exists a clear set of blocks, that is, a set of $k$ mutually disjoint blocks. In this case if we assume $(P, X)$ is as before and the blocks $b_1, b_2, ..., b_k$ are mutually disjoint then on the blocks $b_j$, $j \leqslant k$ we define any quasigroup $(b_j, \otimes_j)$ and then $(P, *)$ can be defined as follows:

(i) $p * \;= p \otimes_j p$ if $p \in b_j$, $j \leqslant k$

$\quad = p$ otherwise;

(ii) $p * q = p \otimes_j q$, $p \neq q$, $p, q \in b_j$.

Again this is clearly a quasigroup and its $\alpha$-conjugate is the composition of the $\alpha$-conjugates of the quasigroups defined on the blocks of the PBD. Thus we have the next Lemma.

LEMMA 2.6. *If there exists a* PBD $(P, X)$, *with a clear set of blocks, such that for each* $b_j \in X \mid b_j \mid \in B_\alpha$ *and furthermore for each block* $b_j$ *not in the clear set there exists an idempotent $\alpha$-self-orthogonal quasigroup of order* $\mid b_j \mid$, *then* $\mid P \mid \in B_\alpha$.

This establishes the connection between block designs and conjugate orthogonal quasigroups. We now state the following construction of block designs from orthogonal arrays, $OA(n, k)$.

LEMMA 2.7. *If there exists an* $OA(n, k+1)$ *then, for* $0 \leqslant m \leqslant n$, *there exists a* PBD *of order* $kn + m$, *with block sizes* $k$, $k+1$, $n$, $m$. *Furthermore the blocks of cardinalities n and m form a clear set.*

*Proof.* See Hall [6], Wilson [16], or Brayton *et al.* [2, 3] for details of the construction.

With these preliminary lemmas at hand we can now proceed to the first of the two cases under consideration, i.e., $\alpha = (3, 1, 2)$.

## 3. (3, 1, 2)—SELF-ORTHOGONAL QUASIGROUPS

Our method in this as well as the other case parallels that of Brayton *et al.* [2]. We first establish a recursive construction: Using finite fields one can construct an idempotent (3, 1, 2)-self-orthogonal quasigroup of orders 7, 8, and 9 (Lemma 2.3). This fact along with Lemma 2.7 gives us the following:

LEMMA 3.1. *If there exists an* $OA(n, 8)$ *and* $n, m \in B_{(3,1,2)}$ *then* $7n + m \in B_{(3,1,2)}$. *If there exists an* $OA(n, 9)$ *then* $8n + m \in B_{(3,1,2)}$ *as well.*

Next we remark that these exists an $OA(n, 8)$ for all $n \geqslant 91$ and for many lesser values (Wilson [17], Van Lint [10]). Obviously 2 and 6 are not in the spectrum; however, $7n + 2 = 7(n-1) + 9$ and $7n + 6 = 7(n-1) + 13$. Clearly then for $n \geqslant 92$ we can invoke Lemma 3.1 but we must first establish the existence of (3, 1, 2)-self-orthogonal quasigroups for smaller orders, i.e., $n \leqslant 644$. To this end, we consider some specific constructions.

First note that the existence of an $OA(n, 4)$ which is invariant under cyclic permutation of its columns implies that there exists an (3, 1, 2)-self-orthogonal $_3$quasigroup of order $n$. If $(i, j, k, l)$ is a row of such an orthogonal array then $(j, k, l, i)$, $(k, l, i, j)$, and $(l, i, j, k)$ are also rows in this array. Thus if $(P, \circ)$ is a quasigroup defined by the first three columns we have $i \circ j = k$ and $l \circ i = j$; thus the (3, 1, 2) conjugate of $(P, \circ)$, denoted by $(P, \circ(3, 1, 2))$, will have $i \circ (3, 1, 2) j = l$. In other words $(P, \circ(3, 1, 2))$ is the quasigroup defined by the first, second, and fourth columns. The spectrum of $OA(n, 4)$ which are invariant under cyclic permutation is unknown, however, it does suggest the use of a construction, known as a method of differences, ad described in Hall [6], Denes and Keedwell [4], or Brayton *et al.* [2, 3].

Let us illustrate this construction for $n = 10$. Let $A_0$ be the array 3.10 below and let $A_0, A_1, A_2, A_3$ be the arrays that result from the cyclic permutation of the rows of $A_0$. Now let $P_0 = (A_0, A_1, A_3, V)$ where $V$ is a column vector of zeros and let $P_i$ be the array of residues modulo 7 that results from adding $i$ to each integer in the array $P_0$. Finally if $X$ is an $OA(3, 4)$ on the symbols $x_1, x_2, x_3$ which corresponds to a (3, 1, 2)-self-orthogonal quasigroup and its (3, 1, 2) conjugate then the transpose of the array $(P_0, P_1, P_2, \ldots, P_6, X)$ is an $OA(10, 4)$ which defines a (3, 1, 2)-self-orthogonal quasigroup and its (3, 1, 2) conjugate.

Example 3.18 was constructed by the author, the other examples can be found in the references previously cited as well as elsewhere.

(3.10)
$$\begin{pmatrix} x_1 & x_2 & x_3 \\ 0 & 0 & 0 \\ 1 & 2 & 4 \\ 4 & 1 & 2 \end{pmatrix};$$

(3.14)
$$\begin{pmatrix} 0 & x & x_2 & x_3 \\ 1 & 0 & 0 & 0 \\ 4 & 4 & 6 & 9 \\ 6 & 1 & 2 & 8 \end{pmatrix};$$

(3.18)
$$\begin{pmatrix} 0 & 0 & x_1 & x_2 & x_3 \\ 1 & 7 & 0 & 0 & 0 \\ 4 & 6 & 2 & 4 & 8 \\ 9 & 2 & 14 & 13 & 3 \end{pmatrix};$$

(3.26)
$$\begin{pmatrix} 0 & 0 & 0 & 0 & x_1 & x_2 & x_3 \\ 3 & 6 & 2 & 1 & 0 & 0 & 0 \\ 8 & 20 & 12 & 16 & 20 & 17 & 8 \\ 12 & 16 & 7 & 2 & 19 & 6 & 21 \end{pmatrix}.$$

With this construction, we are ready for the following lemma.

LEMMA 3.2. *For all* $n$, $1 \leqslant n \leqslant 62$, $n \neq 2$ *or* 6, $n \in B_{(3,1,2)}$.

*Proof.* First we have a table of special cases.

| $n$ | Comment | Lemma | $n$ | Comment | Lemma |
|---|---|---|---|---|---|
| 10 | Example (3.10) mod 7 | | 34 | $11(4 - 1) + 1$ | 2.5 |
| 14 | Example (3.14) mod 11 | | 38 | $5(10 - 3) + 3$ | 2.5 |
| 18 | Example (3.18) mod 15 | | 46 | $5(10 - 1) + 1$ | 2.5 |
| 22 | $7(4 - 1) + 1$ | 2.5 | 58 | $19(4 - 1) + 1$ | 2.5 |
| 26 | Example (3.26) mod 23 | | 62 | $8 \cdot 8 + 1 - 3$ | 2.6 |

*Note.* For $n = 62$ we take the affine plane of order 8 and add a new point to each line in *one* pencil of lines giving $8 \cdot 8 + 1$ points. We then delete any three collinear points from a line with eight points (i.e., any line not in the original pencil) and the result is a PBD with block sizes 5, 7, 8, and 9.

All other cases are swept out by Lemmas 2.3 and 2.4 (direct product and finite fields).

LEMMA 3.3. *For all n*, $63 \leqslant n \leqslant 704$, $n \in B_{(3,1,2)}$.

*Proof.* For these cases we apply Lemma 3.1, that is $7t + m$ and $8t + m$, with certain exceptions, since $m \neq 2$ or 6. We then have the following table:

| $n$ | Lemma 3.1 | $n$ | Lemma 3.1 |
|---|---|---|---|
| 63–72 | $7 \cdot 9 + m$ | 189–216 | $7 \cdot 27 + m$ |
| 72–81 | $8 \cdot 9 + m$ | 203 232 | $7 \cdot 29 + m$ |
| 77–88 | $7 \cdot 11 + m$ | 217–261 | $7 \cdot 31 + m, 8 \cdot 29 + m$ |
| 88–104 | $8 \cdot 11 + m, 7 \cdot 13 + m$ | 259–296 | $7 \cdot 37 + n, 8 \cdot 31 + m$ |
| 104–117 | $8 \cdot 13 + m$ | 296–344 | $8 \cdot 37 + n, 7 \cdot 43 + m$ |
| 112–128 | $7 \cdot 16 + m$ | 343–392 | $8 \cdot 43 + n, 7 \cdot 49 + m$ |
| 128–144 | $8 \cdot 16 + m$ | 371–424 | $7 \cdot 53 + m$ |
| 136–153 | $8 \cdot 17 + m$ | 413–477 | $7 \cdot 59 + m, 8 \cdot 53 + m$ |
| 152–171 | $8 \cdot 19 + m$ | 469–536 | $7 \cdot 67 + m$ |
| 161–184 | $7 \cdot 23 + m$ | 511–584 | $7 \cdot 73 + m$ |
| 175–299 | $7 \cdot 25 + m$ | 560–640 | $7 \cdot 80 + m$ |
| | | 616–704 | $7 \cdot 88 + m$ |

Exceptions are of the form $7t + 2$, $7t + 6$, $8t + 2$, $8t + 6$. Most of these are covered in the above table. For example, $78 = 8 \cdot 9 + 6$ but also $78 = 7 \cdot 11 + 1$. We have these exceptions remaining:

| $n$ | Lemma |
|---|---|
| $74 = 9 \cdot 9 - 7$ (PBD) | 2.6 |
| $106 = 7(16 - 1) + 1$ (SDP) | 2.5 |
| $118 = 13(10 - 1) + 1$ (SDP) | 2.5 |
| $134 = 7 \cdot 17 + 15$ | 3.1 |
| $158 = 9 \cdot 19 - 13$ (PBD) | 2.6 |
| $298 = 11 \cdot (28 - 1) + 1$ (SDP) | 2.5 |

*Note.* For $n = 74$ we take an affine plane of order 9 and delete six collinear points and one point from a different line giving a PBD with block sizes 3, 7, 8, and 9. For $n = 158$ we take 9 parallel lines of an affine plane of order 19 delete 12 points from one line and one from another line. This gives us $9 \cdot 19 - 13 = 158$ points, the blocks being the original lines restricted to these points. Thus the block sizes will be 7, 8, 9, 18, 19 with the one block of size 18 forming a clear set. All other exceptions are covered by Lemmas 2.3 and 2.4.

THEOREM 3.4. *For all positive integers $n$, $n \neq 2$ or 6, there exists a* (3, 1, 2)-*self-orthogonal quasigroup of order $n$.*

*Proof.* $1 \leqslant n \leqslant 704$, $n \neq 2$ or 6 by Lemmas 3.2 and 3.3. For $n > 704$, $n$ can be represented in the form $n = 7t + k$, where $k < 7$ and $t > 92$. But there exists an $OA(t, 8)$ and an $OA(t-1, 8)$. Thus $n = 7t + k = 7(t-1) + (k+1)$ and by Lemma 3.1 $n \in B_{(3,1,2)}$.

COROLLARY 3.5. *If $n \neq 2$ or 6 then there exists a* (2, 3, 1)-*self-orthogonal quasigroup of order $n$.*

*Proof.* Lemma 2.1(a) and Theorem 3.4. This completes this section; we now consider the other case.

## 4. (1, 3, 2)—SELF-ORTHOGONAL QUASIGROUPS

Our method is essentially the same as before. In this case we use the following lemma:

LEMMA 4.1. *If $n, m \in B_{(1,3,2)}$ $0 \leqslant m \leqslant n$ and there exists a $OA(n, 5)$ then $4n + m \in B_{(1,3,2)}$.*

*Proof.* There exists an idempotent (1, 3, 2)-self-orthogonal quasigroup of orders 4 and 5 via the finite field construction. This along with Lemmas 2.6 and 2.7 gives us the result.

We immediately note that for $n \geqslant 46$ there exists an $OA(n, 5)$ (see Wilson [17, 18] or Van Lint [10]). Because of Lemma 2.2 we need only consider $n \equiv 2 \bmod 4$ to establish our construction.

THEOREM 4.2. *For all $n \neq 2$ or 6 there exists an* (1, 3, 2)-*self-orthogonal quasigroup of order $n$, except possibly $n = 14$ and 26.*

*Proof.*

*Case* I. $1 \leqslant n \leqslant 50$, $n \neq 2$ or 6.

| $n$ | Comment | Lemma | $n$ | Comment | Lemma |
|---|---|---|---|---|---|
| 10 | Example (4.10) | | 34 | $11(4-1)+1$ | 2.5 |
| 14 | (?) | | 38 | $5(10-3)+3$ | 2.5 |
| 18 | $4^2+4+1-3$ | 2.6 | 42 | $5 \cdot 9 - 3$ | 2.6 |
| 22 | $7(4-1)+1$ | 2.5 | 46 | $5(10-1)+1$ | 2.5 |
| 26 | (?) | | | | |

For $n = 18$, we take the projective plane of order 4 and delete three points which are not collinear; the result is a PBD and the blocks of size 3 form a clear set. For $n = 42$, choose five parallel lines in an affine plane of order 9. Again delete three points which are not collinear. This gives a PBD on $5 \cdot 9 - 3 = 42$ points with block sizes 3, 4, 5, 7, 8, 9 and the blocks of size 3 form a clear set. Again the blocks are the original lines intersecting with this set of points. For $n = 10$ the example below is a modification of a method of differences mentioned previously. The construction is the same except there are only three rows to permute. The result is an $OA(10, 3)$, with a sub-$OA(3, 3)$ on $x_1, x_2, x_3$ which corresponds to a (1, 3, 2)-self-orthogonal quasigroup of order 10:

$$(4.10) \qquad \begin{pmatrix} 0 & x_1 & x_2 & x_3 \\ 1 & 0 & 0 & 0 \\ 3 & 3 & 5 & 6 \end{pmatrix}.$$

For $n = 30$ and $50$ we apply Lemma 2.3 with $30 = 3.10$ and $50 = 5.10$.

*Case* II. $n > 50$: For all $n > 50$ where $n = 4t + k$ and $k \neq 2$, $0 \leqslant k \leqslant 4$ if there exists an $OA(t, 5)$ and $t \in B_{(1,3,2)}$ then we can conclude by Lemma 4.1 that $n \in B_{(1,3,2)}$. Similarly if $n = 4t + 2$ then $n$ can be written as $n = 4(t-2) + 10$. Thus if there exists an $OA(t-2, 5)$ and $t - 2 \in B_{(1,3,2)}$ then we can again use Lemma 4.1 to conclude that $n \in B_{(1,3,2)}$. (Note that $n > 50$ implies $t \geqslant 12$.)

There exists an $OA(t, 5)$ for all orders $t \geqslant 11$ except for those values of $t$ listed below. For $t = 0$ or $1 \bmod 4$ Mills [11] has shown that there exists an $OA(t, 5)$. For other orders we again refer to Wilson [17, 18] and Van Lint [10]. For those values of $t$ for which an $OA(t, 5)$ is not known to exist we have two expectations to deal with; when $n = 4t + k$, $0 \leqslant k \leqslant 4$ and when $n = 4(t+2) + 2 = 4t + 10$. In the table below all of these exceptions are covered by suitable applications of Lemma 4.1 except where noted.

| $t$ | $n = 4t + k$ | Lemma 4.1 | $n = 4t + 10$ | Lemma 4.1 |
|---|---|---|---|---|
| 14 | 56–59 | $4 \cdot 12 + m, 4 \cdot 13 + m$ | 66 | $3 \cdot 22$* |
| 18 | 72–75 | $4 \cdot 16 + m$ | 82 | $9(10 - 1) + 1$** |
| 22 | 88–92 | $4 \cdot 20 + m$ | 98 | $4 \cdot 20 + 18$ |
| 26 | 104–106 | $4 \cdot 24 + m, 4 \cdot 25 + m$ | 114 | $4 \cdot 24 + 18$ |
| 34 | 136–139 | $4 \cdot 31 + m, 4 \cdot 32 + 10$ | 146 | $4 \cdot 32 + 18$ |
| 38 | 152–155 | $4 \cdot 31 + m$ | 166 | $4 \cdot 37 + 18$ |
| 42 | 168–171 | $4 \cdot 37 + m$ | 178 | $4 \cdot 40 + 18$ |

(*) Lemma 2.4, (**) Lemma 2.5

With these exceptions taken care of, we can recursively construct a (1, 3, 2)-self-orthogonal quasigroup of orde $n$ for all $n > 50$ by using Lemma 4.1.

COROLLARY 4.3. *For all* $n \neq 2$ *or* 6, *with the possible exception of* $n = 14$ *and* 26, *there exists a* (3, 2, 1)*-self-orthogonal quasigroup of order* $n$.

*Proof.* Lemma 2.1(b) and Theorem 4.2.

We remark that the existence of an $OA(n, 4)$ which is invariant under a permutation that fixes one column and cyclically permutes the other three implies the existence of a (1, 3, 2)-self-orthogonal quasigroup of order $n$. The spectrum for the existence of such an array is unsettled and furthermore there is no straightforward construction of such an array via a method of differences.

## 5. CONCLUDING REMARKS

Quasigroup identities which imply conjugate orthogonality have not received much attention in the literature for conjugates other than the transpose. Much can be done in this area. For a general characterization of these identities see Evans [5]. The connection between orthogonal arrays $OA(n, 4)$ which are invariant under conjugation (i.e., permutation of columns) and quasigroup identities has recently been studied by Lindner and Mendelsohn [9]. The spectrum of such arrays also is investigated in their paper, however, much remains to be done in this area too. It appears that the techniques and results of this paper will help solve some of these questions but that is a subject for another paper.

## REFERENCES

1. R. C. BOSE, E. T. PARKER, AND S. SHRIKHANDE, Further results on the construction of mutually orthogonal latin squares and the falsity of Euler's conjecture, *Canad. J. Math.* **12** (1960), 189–203.

2. R. K. BRAYTON, D. Coppersmith, AND A. J. HOFFMAN, Self-orthogonal latin squares of all orders $n \neq 2$, 3 or 6, *Bull. Amer. Math. Soc.* **80** (1974), 116–118.
3. R. K. BRAYTON, D. Coppersmith, AND A. J. HOFFMAN, Self-orthogonal latin squares, "Colloquio Internationale sulle Teorie Combinatorie" (Roma, 1973) TOMOI, *Atti dei Convegni Lincei*, No. 17, Accad. Naz. Lincei, Rome, 1976.
4. J. DENES AND A. D. KEEDWELL, "Latin Squares and Their Applications," Academic Press, New York/London, 1974.
5. T. EVANS, Algebraic structures associated with latin squares and orthogonal arrays, *in* "Proceedings of the Conference on Algebraic Aspects of Combinatorics, (University of Toronto, 1974) Utilitas Mathematica, Jan. 1975."
6. M. HALL, "Combinatorial Theory," Blaisdell, Waltham, Mass., 1967.
7. C. C. LINDNER, The generalized singular direct product for quasigroups, *Canad. Math. Bull.* **14** (1971), 61–63.
8. C. C. LINDNER, Latin Squares and the Singular Direct Product, *in* "Proceedings of a Conference on Combinatorics, Memphis State University."
9. C. C. LINDNER AND E. MENDELSOHN, On the conjugates of an $n^2 \times 4$ orthogonal array, *Discrete Math.* **20** (1977/78), No. 2, 123–132.
10. J. H. VAN LINT, "Combinatorial Theory Seminar Eindhoven," Lecture Notes in Mathematics, Vol. 382, Springer-Verlag, Berlin/Heidelberg/New York, 1974.
11. H. F. MACNEISH, Euler squares, *Ann. of Math.* **23** (1922), 221–227.
12. W. H. MILLS, Three mutually orthogonal latin squares, *J. Combinatorial Theory* **13** (1972), 79–82.
13. A. SADE, Produit direct-singulier de quasigroups orthogonaux et anti-abelians, *Ann. Soc. Sci. Bruxelles, Sér. I* **74** (1960), 91–99.
14. D. STEEDLY, "Separable Quasigroups," Ph. D. Thesis, Auburn University, 1973.
15. S. K. STEIN, On the foundations of quasigroups, *Trans. Amer. Math. Soc.* **85** (1957), 228–256.
16. R. M. WILSON, An existence theory for pairwise balanced designs, Parts I and II, *J. Combinatorial Theory Ser. A.* **13** (1972), 220–273.
17. R. M. WILSON, Concerning the number of mutually orthogonal latin squares. *Discrete Math.* **9** (1974), 181–198.
18. R. M. WILSON, A few more squares, *in* "Proceedings of the Fifth Southeastern Conference on Combinatorics, Graph Theory and Computing" (Florida Atlantic University, Boca Raton, Florida 1974), pp. 661–673. Congressus Numeratum, No. X, Utilitas, Math. 1974.