Orthogonal trades in complete sets of MOLS

Nicholas J. Cavenagh
Department of Mathematics and Statistics
University of Waikato
New Zealand
nickc@waikato.ac.nz

Diane M. Donovan
Centre for Discrete Mathematics and Computing
School of Mathematics and Physics
University of Queensland
Australia
dmd@maths.uq.edu.au

Fatih Demirkale
Department of Mathematics
Yıldız Technical University
Esenler, 34220, İstanbul
Turkey
fatihd@yildiz.edu.tr

Submitted: Jul 27, 2016; Accepted: Jul 17, 2017; Published: Jul 28, 2017
Mathematics Subject Classifications: 05B15

Abstract

Let B_p be the Latin square given by the addition table for the integers modulo an odd prime p (i.e. the Cayley table for $(\mathbb{Z}_p, +)$). Here we consider the properties of Latin trades in B_p which preserve orthogonality with one of the $p-1$ MOLS given by the finite field construction. We show that for certain choices of the orthogonal mate, there is a lower bound logarithmic in p for the number of times each symbol occurs in such a trade, with an overall lower bound of $(\log p)^2/\log\log p$ for the size of such a trade. Such trades imply the existence of orthomorphisms of the cyclic group which differ from a linear orthomorphism by a small amount. We also show that any transversal in B_p hits the main diagonal either p or at most $p - \log_2 p - 1$ times. Finally, if $p \equiv 1 \pmod 6$ we show the existence of a Latin square which is orthogonal to B_p and which contains a 2×2 subsquare.

Keywords: Orthogonal array, MOLS, trade, orthomorphism, transversal.

1 Introduction and Definitions

Let p be an odd prime. Consider the "complete" set of $p-1$ MOLS of order p, constructed via the finite field of order p. (It is conjectured, but not yet proven, that a complete set of MOLS of order p is unique up to isomorphism.) The problem considered in this paper is

0_3	1_4	2	3_0	4_1	5	6
1	2	3	4	5	6	0
2	3_6	4_5	5_3	6_4	0	1
3_5	4_3	5_4	6	0	1	2
4	5	6_0	0_1	1_6	2	3
5_0	6_1	0_6	1_5	2	3	4
6	0	1	2	3	4	5

0	1	2	3	4	5	6
3	4	5	6	0	1	2
6	0	1	2	3	4	5
2	3	4	5	6	0	1
5	6	0	1	2	3	4
1	2	3	4	5	6	0
4	5	6	0	1	2	3

Figure 1: An orthogonal trade in B_7

how to change a "small" number of entries in one of these Latin squares so that it maintains orthogonality with at least one other Latin square in the complete set of MOLS.

To this end, for each k, $1 \leqslant k \leqslant p-1$, define $B_p(k)$ to be the Latin square where the entry in cell (i,j) of $B_p(k)$ is given by $ki+j$, for each $i,j \in \mathbb{Z}_p$. (In the above and throughout this paper, arithmetic is performed modulo p with residues in $\mathbb{Z}_p$ whenever the context makes this clear.) Then it is well-known that

$$\mathcal{B}_p := \{B_p(1), B_p(2), \ldots, B_p(p-1)\}$$

is a set of $p-1$ MOLS of order p. For convenience we often write B_p instead of $B_p(1)$.

The Latin squares B_7 and $B_7(3)$ are given in Figure 1. Observe that after each symbol is replaced by its subscript in B_7, the Latin squares remain orthogonal. We will refer to this change as an *orthogonal trade*. We are interested in determining general properties of orthogonal trades; in particular lower bounds for the size of an orthogonal trade.

Considering a Latin square of order n to be a set of ordered (row, column, entry) triples (in this paper a subset of $\mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n$), a *Latin trade* is a subset T of a Latin square L such that there exists a partially filled-in Latin square T' (called a *disjoint mate* of T) such that for each $(i,j,k) \in T$ (respectively, T'), there exists unique $i' \neq i$, $j' \neq j$ and $k' \neq k$ such that $(i',j,k), (i,j',k)$ and $(i,j,k') \in T'$ (respectively, T). It follows that $(L \setminus T) \cup T'$ is a Latin square not equal to L. In fact, Latin trades describe differences between Latin squares of the same order; see [2] for more details.

We define an *orthogonal trade* (in $\mathcal{B}_p$) of index (ℓ, k) to be a Latin trade $T \subset B_p(\ell)$ such that there exists a disjoint mate T' such that $(B_p(\ell) \setminus T) \cup T'$ is orthogonal to $B_p(k)$. Thus Figure 1 gives an example of an orthogonal trade in $\mathcal{B}_p$ of index $(1,3)$.

Using symmetries of $\mathcal{B}_p$, we may assume certain properties of an orthogonal trade therein. In this paper, k^{-1} is always taken to be the least non-negative integer representing the congruence class of $k^{-1} \pmod p$.

Lemma 1. *Let T be an orthogonal trade in $\mathcal{B}_p$ of index (ℓ, k). Then we may assume, without loss of generality, that $\ell = 1$, $k \leqslant k^{-1}$ and $(0,0,0) \in T$.*

Proof. Let $1 \leqslant x \leqslant p-1$. The mapping $\phi : (a,b,ax+b) \to (a, b/\ell, (ax+b)/\ell)$ maps $B_p(x)$ onto $B_p(x/\ell)$ and thus acts as a bijection on the set $\mathcal{B}_p$. We may thus assume that $\ell = 1$. Next, the mapping $\phi' : (a,b,ax+b) \to (b, -a/x, (b-a)/x)$ maps $B_p(x)$ to

$B_p(x^{-1})$ (again as part of a bijection on the set $\mathcal{B}_p$), fixing $B_p(1)$ and mapping $B_p(k)$ to $B_p(k^{-1})$. We may thus assume $k \leqslant k^{-1}$. Finally, if $0 \leqslant i \leqslant p-1$, the map $\phi'' : (a, b, ax+b) \to (a, b+i, ax+b+i)$ maps each element of $\mathcal{B}_p$ to itself, allowing us to assume that $(0,0,0) \in T$. □

It is possible, of course, to consider Latin trades which preserve orthogonality within pairs of MOLS that do not necessarily belong to $\mathcal{B}_p$. The spectrum of possible sizes of such Latin trades is explored in [7]. However for the rest of the paper we assume that any orthogonal trade is always in B_p with the assumptions of the previous lemma.

2 The theory of Latin trades in B_p

In this section we give relevant known results and theory of Latin trades in B_p - that is, the operation table for the integers modulo p, also known as the *back circulant Latin square*. Since an orthogonal trade necessarily is also a Latin trade in B_p, this theory will be useful in later sections.

A *trade matrix* $A = [a_{ij}]$ is an $m \times m$ matrix with integer entries such that for all $1 \leqslant i, j \leqslant m$: (1) $a_{ii} > 0$; (2) $a_{ij} \leqslant 0$ whenever $i \neq j$ and (3) $\sum_{j=1}^{m} a_{ij} \geqslant 0$.

Lemma 2. (Lemma 7 of [3])*: If $A = [a_{ij}]$ is an $m \times m$ trade matrix,* $\det(A) \leqslant \Pi_{i=1}^{m} a_{ii}$.

The following lemmas are implied by the theory in [3]. The results therein are expressed in terms of symbols rather than rows; however statements about rows, columns and symbols are equivalent due to equivalences of B_p.

Lemma 3. *Let $x_1, x_2, \ldots, x_m, x_{m+1}$ be the non-empty rows of a Latin trade T in B_p. Then there exists an $(m+1) \times (m+1)$ trade matrix A such that $AX = B$, where $X = (x_1, x_2, \ldots, x_m, x_{m+1})^T$, a_{ii} gives the number of entries in row x_i of T and B is an $(m+1) \times 1$ vector of integers, each a multiple of p. Moreover, the row and column sums of A are each equal to* 0.

Lemma 4. *Let A be an $m \times m$ trade matrix such that* $\det(A) \neq 0$ *and there exist $m \times 1$ vectors X and B such that $AX = B$, where each entry of B is divisble by p but each entry of X is not divisible by p. Then* $\det(A)$ *is divisible by p.*

Lemma 5. *If T is a Latin trade in B_p, then $|T| \geqslant mp^{1/m} + 2$.*

We will also need the following corollary from the theory in [3].

Lemma 6. *There does not exist a row i of a trade matrix A such that $a_{ii} = 2$ and $a_{ij} = -2$ where $j \neq i$.*

Proof. If such a row exists, Equation (1) of [3] becomes $2x_i \equiv 2x_j \pmod{p}$, which implies $x_i = x_j$ since p is odd, a contradiction to the rows being distinct. □

Those readers who refer back to the detail in paper [3] may notice that the step of proving that a trade matrix has a non-zero determinant is omitted. However Theorem 8 in the next section addresses the original oversight from that paper.

3 Smallest orthogonal trade

In this section we give a lower bound on the number of times each symbol occurs in an orthogonal trade (Theorem 10) and an overall lower bound for the size of an orthogonal trade (Theorem 11).

Suppose that $k \neq 1$ and symbol s occurs in the rows in the set $R = \{r_1, r_2, \ldots, r_m\}$ of an orthogonal trade T of index $(1, k)$. Then clearly the set of columns of T which include s is equal to $\{s - r_1, s - r_2, \ldots, s - r_m\}$. Let ϕ be the devolution on R such that s occurs in the set of cells

$$\{(r_i, s - \phi(r_i)) \mid r_i \in R\}$$

in T'. Note that if $\phi(r_i) = r_i$ for some i, T and T' are not disjoint, contradicting the definition of a Latin trade; therefore ϕ is indeed a devolution. Observe that $(k-1)r_i + s$ occurs in cell $(r_i, s - r_i)$ of $B_p(k)$. Thus, considering orthogonality, the set of orthogonal ordered pairs $\{(s, (k-1)r_i + s) \mid r_i \in R\}$ must be covered after T is replaced by T'; it follows that

$$\{(k-1)r_i + s \mid r_i \in R\} \quad = \quad \{kr_i + s - \phi(r_i) \mid r_i \in R\}. \tag{1}$$

Thus we may define another permutation ϕ' on R such that $\phi'(r_i) = (kr_i - \phi(r_i))/(k-1)$ for each $r_i \in R$. If $\phi'(r_i) = r_i$ for some $r_i \in R$, ϕ is not a devolution, a contradiction. Similarly, $\phi'(r_i) \neq \phi(r_i)$ for each $r_i \in R$. This gives a linear system of the form $A\mathbf{u} = \mathbf{0} \pmod p$, where $\mathbf{u} = (r_1, r_2, \ldots, r_m)^T$ and A is a square matrix of dimensions $m \times m$ with the following properties:

(P1) Each entry of the main diagonal of A is k.

(P2) Each off-diagonal entry of A is either 0, -1 or $1 - k$.

(P3) The sum of each row and column of A is 0.

In the example in Figure 1 with $s = 0$, we have $R = \{0, 4, 5\}$, $\phi = (045)$, $\phi' = (054)$, $\mathbf{u} = (0, 4, 5)^T$ and

$$A = \begin{bmatrix} 3 & -1 & -2 \\ -2 & 3 & -1 \\ -1 & -2 & 3 \end{bmatrix}.$$

The following lemma is immediate.

Lemma 7. *Any symbol in an orthogonal trade occurs at least* 3 *times.*

Next, property (P3) above implies that $\det(A) = 0$. From Lemma 1, we may assume without loss of generality that $r_1 = 0$. Let A' be the $(m-1) \times (m-1)$ matrix obtained by deleting the first row and column of A and let $\mathbf{u}' = (r_2, \ldots, r_m)^T$. Then $A'\mathbf{u}' = \mathbf{0}$, where A' satisfies (P1), (P2) and the following properties:

(P4) The sum of each row of A is 0 except for at least two rows which have a positive sum.

(P5) The sum of each column of A is 0 except for at least two columns which have a positive sum.

An $m \times m$ matrix $A = (a_{ij})$ is said to be *diagonally dominant* if

$$2|a_{ii}| \geqslant \sum_{j=1}^{m} |a_{ij}|$$

for each $i \in [m]$. Clearly A' above is diagonally dominant.

Theorem 8. ([10, 12]) *If A is diagonally dominant and irreducible and there is an integer $k \in [m]$ such that*

$$2|a_{kk}| \quad > \quad \sum_{j=1}^{m} |a_{kj}|, \tag{2}$$

then A is non-singular.

If A' is irreducible, we have from the previous theorem, $\det(A') \neq 0$. However the case when A' is reducible can be dealt with in the following lemma, which is easy to prove.

Lemma 9. *Let A' be a diagonally dominant matrix satisfying* (P1), (P2), (P4) *and* (P5) *above. Then there exists an irreducible, diagonally dominant $m' \times m'$ matrix A'' with $m' \leqslant m$ satisfying* (P1), (P2) *and Equation* (2).

Thus there exists an $m' \times m'$ matrix A'', satisfying (P1), (P2) and Equation (2) above, with non-zero determinant, where $m' \leqslant m$. Moreover, A'' is a type of *trade matrix* as defined in the previous section. From Lemma 2, the determinant of A'' is bounded above by k^{m-1} and from Lemma 4, $p < k^{m-1}$, so we have shown the following.

Theorem 10. *Let $K = \min\{k, k^{-1}\}$. The number of times each symbol occurs in an orthogonal trade is greater than $\log_K p + 1$.*

We next find a lower bound on the size of T.

Theorem 11. *If T is an orthogonal trade of index $(1, k)$, then*

$$|T| > \frac{\log p \log_K p}{\log \log_K p}.$$

where $K = \min\{k, k^{-1}\}$.

Proof. Let T contain m distinct symbols and let s_i be the the number of times symbol i occurs in T, where $1 \leqslant i \leqslant m$. From Lemma 5, for any Latin trade in B_p, $\sum_{i=1}^{m} s_i = |T| > mp^{1/m}$. Let $x = |T|/m = (\sum_{i=1}^{m} s_i)/m$. From Lemma 7, $x \geqslant 3$. Also, from above, $x > p^{1/m}$ which implies that $m > (\log p)/(\log x)$. Thus $|T| > (x/\log x)\log p$. But the function $x/\log x$ is strictly increasing for $x > e$; thus the result follows from the previous theorem. □

0_4	1_5	2_6	3_0	4_1	5_2	6_3
1	2	3	4	5	6	0
2	3	4	5	6	0	1
3	4	5	6	0	1	2
4_5	5_6	6_0	0_1	1_2	2_3	3_4
5_0	6_1	0_2	1_3	2_4	3_5	4_6
6	0	1	2	3	4	5

0	1	2	3	4	5	6
3	4	5	6	0	1	2
6	0	1	2	3	4	5
2	3	4	5	6	0	1
5	6	0	1	2	3	4
1	2	3	4	5	6	0
4	5	6	0	1	2	3

Figure 2: An orthogonal trade derived from Figure 1 as in Theorem 12.

4 Orthogonal trades permuting entire rows

In this section we consider the case when T and T' are constructed taking complete rows of B_p and permuting them. It turns out that such orthogonal trades arise from considering a symbol from an arbitrary orthogonal trade.

Theorem 12. *Let T be an orthogonal trade in B_p. Let R be the set of rows that contain a particular symbol s in T. Then there exists an orthogonal trade of size $p|R|$ constructed by permuting the rows of R.*

Proof. Fix $s \in \mathbb{Z}_p$. Equation 1 implies that

$$\{(k-1)r_i + s + j \mid r_i \in R, j \in \mathbb{Z}_p\} = \{kr_i + s - \phi(r_i) + j \mid r_i \in R, j \in \mathbb{Z}_p\}.$$

Thus if we replace row r_i with row $\phi(r_i)$ for each $r_i \in R$ we obtain an orthogonal trade. □

In fact, the existence of an orthogonal trade permuting entire rows is equivalent to the existence of any matrix A satisfying properties from Section 2.

Corollary 13. *Let A be an $m \times m$ matrix satisfying properties* (P1), (P2) *and* (P3) *from Section* 2. *Suppose furthermore there is a solution to $A\mathbf{u} = \mathbf{0}$ where $\mathbf{u} = (r_1, r_2, \ldots, r_m)^T$ and $r_1, r_2, \ldots, r_m$ are distinct residues in $\mathbb{Z}_p$. Then there exists an orthogonal trade T of index $(1, k)$ whose disjoint mate T' is formed by permuting the rows $r_1, r_2, \ldots, r_m$ of T.*

Proof. Define $\phi(r_i) = r_j$ if and only if $A_{ij} = -1$ and define $\phi'(r_i) = r_j$ if and only if $A_{ij} = -(k-1)$. Then ϕ and ϕ' are disjoint devolutions on the set $\{r_1, r_2, \ldots, r_m\}$ and $\phi'(r_i)(k-1) = kr_i - \phi(r_i)$ for each i, $1 \leqslant i \leqslant m$. In turn, Equation 1 is satisfied. The proof then follows by Theorem 12. □

From the previous theorem and Theorem 10, we have the following.

Corollary 14. *Let T be an orthogonal trade of index $(1, k)$ consisting of m entire rows of B_p which are permuted to create the disjoint mate T'. Then $m \geqslant \log_K p + 1$, where $K = \min\{k, k^{-1}\}$.*

Theorem 15. *There exists an orthogonal trade T consisting of 3 entire rows of B_p which are permuted to create the disjoint mate T' if and only if $p \equiv 1 \pmod 6$.*

Proof. From the theory in the previous section, the determinant of A' must be equal to $k^2 - k + 1$. However $k^2 - k + 1 = 0$ has a solution mod p if and only if -3 is a square mod p. Elementary number theory can be used to show that -3 is a square mod p if and only if $p \equiv 1 \pmod 6$. Finally, if $p \equiv 1 \pmod 6$, replacing row 0 with row 1, row 1 with row k and row k with row 0 in B_p creates a Latin square which remains orthogonal to $B_p(k)$. □

It is an open problem to determine whether there exists an orthogonal trade permuting a bounded number of rows for any odd prime p.

5 Orthogonal trades via Latin trades in B_p

Our aim in this section is to construct an orthogonal trade T with index $(1, 2)$ with disjoint mate T' such that T' permutes $O(\log p)$ entire rows of T. We do this by showing the existence of orthogonal Latin trades in B_p with size $O(\log p)$.

Theorem 16. *For each prime p there exists a Latin trade T of size $O(\log p)$ within B_p such that each symbol occurs either twice in T or not at all.*

Theorem 17. *For each prime p there exists an orthogonal trade of index $(1, 2)$ permuting $O(\log p)$ rows.*

Proof. From Section 2, the trade matrix A corresponding to the trade T given by the previous theorem has the following properties. Firstly, the number of rows (and the number of columns of A) is $O(\log p)$. Secondly, each entry of the main diagonal is 2, every other entry is either -2, -1 or 0 and the row and column sums are at least 0. From Lemma 6, there are no entries -2. Moreover, from Lemma 5, $A\mathbf{u} = \mathbf{0}$ has a solution in $\mathbb{Z}_p$ where the entries of $\mathbf{u}$ are distinct. The result follows by Corollary 13. □

In order to prove Theorem 16 we modify a construction given by Szabados [11] which proved the following.

Theorem 18. (Szabados, [11]) *For each prime p there exists a Latin trade of size at most $5 \log_2 p$ within B_p.*

Since our proof is a modification of that given in [11] (which was in turn inspired by classic results on dissections of squares by Brooks, Smith, Stone and Tutte [1, 14] and Trustum [13]) we borrow from the notation given in [11].

A *dissection* of order k of a rectangle R with integer sides is a set of k squares of integral side which partition the area of the rectangle (i.e. they cover the rectangle and overlap at most on their boundaries). A dissection is said to be $\oplus$-free if no four of them share a common point.

For the following definition we position our rectangle R with a corner at the origin, its longest side along the positive x-axis and another side along the negative y-axis.

We say that a dissection is *good* if it is:

(G1) $\oplus$-free;

(G2) the square with the origin as a corner point has side at least 3;

(G3) there is no line of gradient -1 intersecting corner points of more than one square; and

(G4) the lines $y = 1 - x$ and $y = 2 - x$ do not intersect corner points of any square.

We wish to construct a good dissection of a rectangle of dimensions $n \times (n+3)$ for any $n \geqslant 3$. We first deal with small values of n.

Lemma 19. *There exists a good dissection of the rectangle $n \times (n+3)$ for $3 \leqslant n \leqslant 14$ with at most 8 squares.*

Proof. In every case, make one of the squares an $n \times n$ square with the origin as a corner point and another 3×3 subsquare with $(n+3, -n)$ as a corner point. Then (G2) and (G4) are satisifed. It is then easy to find a dissection of the remaining $(n-3) \times 3$ rectangle satisfying (G1) and (G3), using at most 6 squares for each case (one can simply use a greedy algorithm, cutting off a largest possible square at each step). □

Figure 3 displays a good dissection of the 5×8 rectangle into 5 squares.

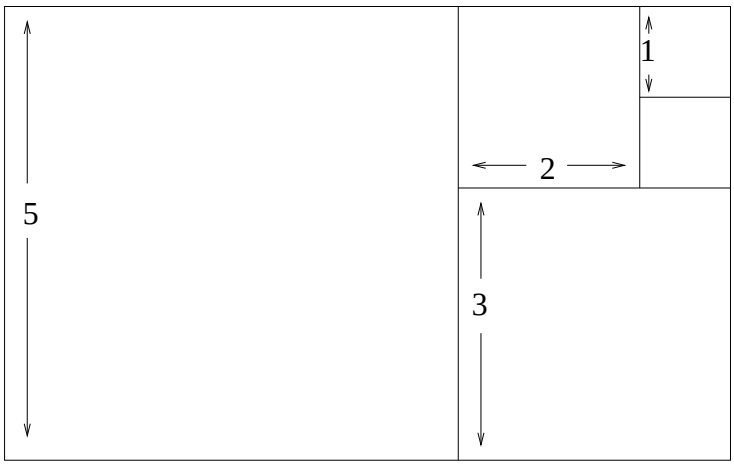

Figure 3: An example of a good dissection into squares

For n of the form $4k + z$ with $k \geqslant 3$, $z \in \{3, 4, 5, 6\}$ we may dissect an $n \times (n+3)$ rectangle into at most 5 squares and a rectangle of size $2k \times 2(k+3)$, as shown in Figure 4.

Lemma 20. *For each $n \geqslant 3$, there exists a good dissection of an $n \times (n+3)$ rectangle using at most $3 + 5\log_4(n+1)$ squares.*

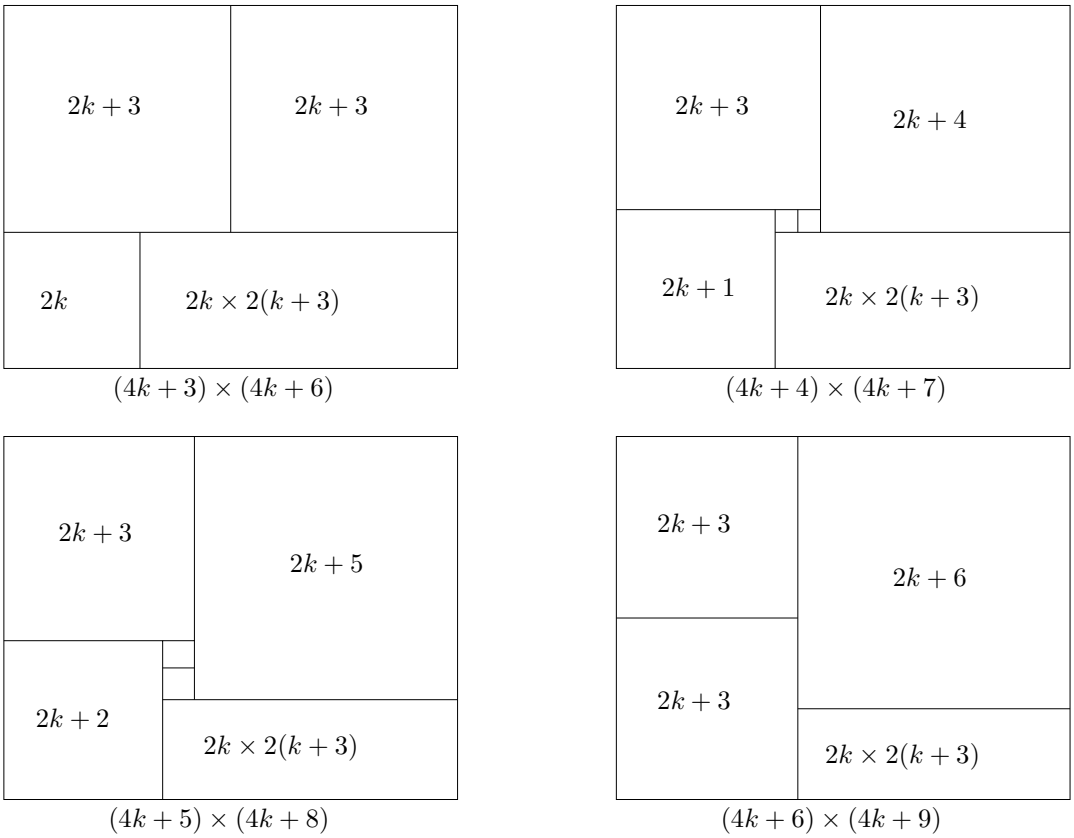

Figure 4: Dissecting a rectangle of size $n \times (n+3)$ (Figure 1. from [11])

Proof. From the previous lemma, the result holds for $3 \leqslant n \leqslant 14$. If $n \geqslant 15$, write $n = 4k+z$ where $k \geqslant 3$ and $z \in \{3,4,5,6\}$ and use a dissection as in Figure 4, recursively using a good dissection of the $k \times (k+3)$ rectangle with the length of each square doubled. Property (G2) of the smaller rectangle ensures that (G1) holds for the larger rectangle. Property (G2) clearly holds for the larger rectangle as $k \geqslant 3 > 0$. Next, property (G4) (avoiding the line $y = 1-x$) for the smaller rectangle ensures that (G3) holds for the larger rectangle. Finally, property (G4)(avoiding the line $y = 2-x$) for the smaller rectangle ensures than (G4) holds for the larger rectangle. Note in the previous that $y = 2-x$ with respect to the larger rectangle cannot hit any corner of squares in the smaller rectangle because each square has even length side.

Suppose such a recursion occurs α times to an intial rectangle of order $m \times (m+3)$ where $3 \leqslant m \leqslant 14$. Then $n \geqslant g^\alpha(m)$, where $g(m) = 4m+3$ and g^α is the function g composed with itself α times. Observe that $g^\alpha(m) = 4^\alpha m + 4^\alpha - 1$. Thus $(n - 4^\alpha + 1)/4^\alpha \geqslant 3$ and $\alpha \leqslant \log_4(n+1) - 1$. Each recursive step gives at most 5 extra squares; with at most 8 squares in the initial step, the result follows by Lemma 20. □

The proof of Theorem 16 now follows from the following theorem, which is outlined in [11] and first established in [8].

Theorem 21. *Suppose there exists a good dissection of order k of an $n \times m$ rectangle. Then there exists a Latin trade T in the addition table for the integers modulo $m+n$ (i.e. B_{m+n} if $m+n$ is prime) such that each entry of T appears exactly twice and T has size $2k+2$.*

Proof. The proof follows from the construction, first given in [8], showing that a dissection of a right-angled isoceles triangle (with two sides of length p) into smaller, integer-sided right-angled isoceles triangles gives rise to a Latin trade T in B_p, provided that no point is the vertex of 6 of the smaller triangles. In such a construction, the number of smaller triangles gives the size of the Latin trade. Reposition the triangle on the Euclidean plane so that its vertices have positions $(0,0)$, $(0,p)$ and $(p,0)$. Then the coordinates of the vertices of the smaller triangles give precisely the cells of B_p which T occupies.

Next, reposition the $n \times m$ rectangle so that its vertices have coordinates $(0,0)$, $(0,m)$, $(n,0)$ and (m,n). Embed this rectangle into an isocoles right-angled triangle as above (with two equal sides of length $n+m$). Dissect each square in the good dissection into two triangles so that the sides of each triangle are parallel to the larger triangle. This gives a dissection of the right-angled triangle into $2k+2$ smaller right-angled isoceles triangles. Reposition the triangle as above.

Then in our construction, the line segements of gradient -1 contain the same symbol in B_p. Each such line segment intersects only two corners of squares and thus only two vertices of triangles. Together with condition (G3), this ensures that each symbol occurs exactly twice in the Latin trade. □

Apply the process in the above theorem to the example in Figure 3. This results in the following Latin trade T in B_{13} (with a unique disjoint mate T'):

$$T := \{(0,0,0),(0,5,5),(5,0,5),(5,3,8),(8,0,8),(5,5,10),(7,3,10),\\ (7,4,11),(8,3,11),(7,5,12),(8,4,12),(8,5,0)\}.\\ T' := \{(0,0,5),(0,5,0),(5,0,8),(5,3,10),(8,0,0),(5,5,5),(7,3,11),\\ (7,4,12),(8,3,8),(7,5,10),(8,4,11),(8,5,12)\}.$$

Note that each symbol occurs twice. For a general proof of why this construction gives a Latin trade, see [8].

6 Orthomorphisms of cyclic groups and transversals in B_p

As in previous sections we assume that p is prime. An *orthomorphism* of the cyclic group $\mathbb{Z}_p$ is a permutation ϕ of the elements of $\mathbb{Z}_p$ such that $x \mapsto \phi(x) - x$ is also a permutation. Orthomorphisms may be defined for arbitrary groups; however in this section we assume that orthomorphisms are of the cyclic group only. Trivial examples of orthomorphisms are given by $\phi(x) = kx$ for any k, $2 \leqslant k \leqslant p-1$. Given any orthomorphism ϕ, construct a Latin square L_ϕ by placing $\phi(r) + c$ in cell (r,c). Then by definition L_ϕ is orthogonal to B_p.

Given two orthomorphisms ϕ and ϕ', the *distance* between ϕ and ϕ' is defined to be the number of values x for which $\phi(x) \neq \phi'(x)$. Corollary 14 implies the following result about orthomorphisms.

Theorem 22. *Let ϕ' be an orthomorphism not equal to $\phi(x) = kx$. Then the distance between ϕ and ϕ' is at least $\log_K p + 1$ where $K = \min\{k, k^{-1}\}$.*

A *transversal* of a Latin square of order n is a set of ordered triples that include each row, column and symbol exactly once. Given any orthomorphism ϕ, the set of triples $(x, \phi(x) - x, \phi(x))$ is a transversal of B_p. For example, if $\phi(x) = 2x$ we obtain a transversal on the main diagonal of B_p. So we have the following corollary.

Corollary 23. *Any transversal of B_p not equal to the main diagonal has at least $\log_2 p + 1$ elements off the main diagonal.*

In contrast, for odd $n > 5$, there exist two transversals in B_n which intersect in k elements, for each $0 \leqslant k \leqslant n - 3$ (Theorem 5 of [5]). From Theorem 17, we also have the following.

Theorem 24. *There exists a transversal of B_p not equal to the main diagonal which has $O(\log p)$ elements not on the main diagonal.*

7 A construction for an orthogonal trade with size not divisible by p

In this section we construct an orthogonal trade of size not divisible by p whenever $p \equiv 1 \pmod 6$. Figure 1 gives the construction for $p = 7$. Figure 5 is an example of the construction for $p = 13$, where the trademate is shown via subscripts.

Let $k \geqslant 2$; since $p \equiv 1 \pmod 6$ there exists k such that $k^2 - k + 1$ is divisible by p (since -3 is a square modulo p if and only if $p - 1$ is divisible by 6). Note that if k is a solution then $1 - k$ is also a solution modulo p; thus we assume in this section that k is an integer such that $2 \leqslant k \leqslant (p + 1)/2$. We remind the reader that all values are evaluated modulo p with a residue between 0 and $p - 1$. We define the following subsets $T_0, T_1, \ldots, T_{k-1}$ of B_p:

$$T_0 := \{(0, j, j), (0, k + j, k + j) \mid 0 \leqslant j \leqslant k - 2\}$$

and if $1 \leqslant i \leqslant k - 1$,

$$T_i := \{(i(k-1), j, i(k-1) + j) \mid i \leqslant j \leqslant 2(k-1)\} \cup$$

$$\{(i(k-1) + 1, j, i(k-1) + j + 1) \mid 0 \leqslant j \leqslant k + i - 2\}.$$

We then define T to be the union of all these sets; i.e.

$$T := \bigcup_{i=0}^{k-1} T_i.$$

0_4	1_5	2_6	3	4_0	5_1	6_2	7	8	9	10	11	12
1	2	3	4	5	6	7	8	9	10	11	12	0
2	3	4	5	6	7	8	9	10	11	12	0	1
3	4_8	5_9	6_7	7_4	8_5	9_6	10	11	12	0	1	2
4_7	5_4	6_5	7_6	8	9	10	11	12	0	1	2	3
5	6	7	8	9	10	11	12	0	1	2	3	4
6	7	8_{12}	9_{10}	10_{11}	11_8	12_9	0	1	2	3	4	5
7_{10}	8_{11}	9_8	10_9	11_7	12	0	1	2	3	4	5	6
8	9	10	11	12	0	1	2	3	4	5	6	7
9	10	11	12_0	0_1	1_2	2_{12}	3	4	5	6	7	8
10_0	11_1	12_2	0_{12}	1_{10}	2_{11}	3	4	5	6	7	8	9
11	12	0	1	2	3	4	5	6	7	8	9	10
12	0	1	2	3	4	5	6	7	8	9	10	11

Figure 5: An orthogonal trade of index $(1, 4)$ and size 36 in B_{13}

The condition $p > 2k - 2$ ensures that the above sets are disjoint. Observe that $|T_0| = 2(k-1)$ and for each $1 \leqslant i \leqslant k-1$, $|T_i| = 3k-2$. Thus $|T| = 3k(k-1)$ which is not divisible by p. In the case where $p = k^2 - k + 1$ (where p and k are integers), the size of T is $3(p-1)$, but in general may be larger relative to p.

We will show that T is a Latin trade which preserves orthogonality between the Latin squares B_p and $B_p(k)$.

With this aim in view, we define a partial Latin square T' which we will show is a disjoint mate of T. Let

$$T'_0 := \{(0, j, k+j), (0, k+j, j) \mid 0 \leqslant j \leqslant k-2\}$$

and if $1 \leqslant i \leqslant k-1$,

$$\begin{aligned} T'_i := \quad & \{(i(k-1), j, i(k-1)+j+k) \mid i \leqslant j \leqslant k-2\} \cup \\ & \{(i(k-1), j, i(k-1)+j+1) \mid k-1 \leqslant j \leqslant k+i-2\} \cup \\ & \{(i(k-1), j, (i-1)(k-1)+j) \mid k+i-1 \leqslant j \leqslant 2(k-1)\} \cup \\ & \{(i(k-1)+1, j, i(k-1)+j+k) \mid 0 \leqslant j \leqslant i-1\} \cup \\ & \{(i(k-1)+1, j, i(k-1)+j) \mid i \leqslant j \leqslant k-1\} \cup \\ & \{(i(k-1)+1, j, i(k-1)+j-k+1) \mid k \leqslant j \leqslant k+i-2\}. \end{aligned}$$

Note that for $i = k-1$ the first set in T'_i is empty and for $i = 0$ the last set is empty. We define T' to be the union of the above sets; i.e.

$$T' := \bigcup_{i=0}^{k-1} T'_i.$$

By observation, T and T' occupy the same set of cells and are disjoint. We next check that corresponding rows contain the same set of symbols. This is easy to check for row 0.

Let $1 \leqslant i \leqslant k-1$. Row $i(k-1)$ of T' contains the symbols $\{i(k-1)+j+k \mid i \leqslant j \leqslant k-2\} = \{i(k-1)+j \mid i+k \leqslant j \leqslant 2(k-1)\}$, $\{i(k-1)+j+1 \mid k-1 \leqslant j \leqslant k+i-2\} = \{i(k-1)+j \mid k \leqslant j \leqslant k+i-1\}$ and $\{(i-1)(k-1)+j \mid k+i-1 \leqslant j \leqslant 2(k-1)\} = \{i(k-1)+j \mid i \leqslant j \leqslant k-1\}$. Thus row $i(k-1)$ of T' contains the same set of symbols as the corresponding row of T.

Next, row $i(k-1)+1$ of T' contains the symbols $\{i(k-1)+j+k) \mid 0 \leqslant j \leqslant i-1\} = \{i(k-1)+j+1) \mid k-1 \leqslant j \leqslant i+k-2\}$, $\{i(k-1)+j) \mid i \leqslant j \leqslant k-1\} = \{i(k-1)+j+1) \mid i-1 \leqslant j \leqslant k-2\}$ and $\{i(k-1)+j-k+1) \mid k \leqslant j \leqslant k+i-2\} = \{i(k-1)+j+1) \mid 0 \leqslant j \leqslant i-2\}$. Thus row $i(k-1)+1$ of T' contains the same set of symbols as the corresponding row of T. We have shown that T and T' share the same sets of symbols in correpsonding rows.

We now show this property for the columns. It suffices to show that each symbol in a column of T' occurs within the same column of T. First consider elements of T'_0. Let $0 \leqslant j \leqslant k-2$. Then symbol $j+k$ in cell $(0,j)$ of T'_0 belongs also to cell (k,j) of T_1. Moreover symbol j in cell $(0,k+j)$ of T'_0 belongs also to cell $((k-1)^2, k+j)$ of T_{k-1} since $(k-1)^2+k$ is divisible by p.

In this paragraph we deal with symbols which occur in row $i(k-1)$ of T'_i for some $1 \leqslant i \leqslant k-1$. Consider symbol $i(k-1)+j+k$ in column j of T'_i where $i \leqslant j \leqslant k-2$. This symbol also lies in cell $((i+1)(k-1)+1, j)$ of T_{i+1}. Consider symbol $i(k-1)+j+1$ in column j of T'_i where $k-1 \leqslant j \leqslant k+i-2$. This symbol lies in cell $(i(k-1)+1, j)$ of T_i. Consider symbol $(i-1)(k-1)+j$ in column j of T'_i where $k+i-1 \leqslant j \leqslant 2(k-1)$. This symbol lies in cell $((i-1)(k-1), j)$ of T_{i-1}.

Finally, to verify that T' is indeed a disjoint mate of T, we look at symbols which occur in row $i(k-1)+1$ of T'_i for some $1 \leqslant i \leqslant k-1$. Consider symbol $i(k-1)+j+k$ which occurs in column j of T'_i where $0 \leqslant j \leqslant i-1$. This symbol occurs in cell $((i+1)(k-1)+1, j)$ of T_{i+1} (if $i < k-1$) or T_0 (if $i = k-1$). Next consider symbol $i(k-1)+j$ which occurs in column j of T'_i where $i \leqslant j \leqslant k-1$. This symbol occurs in cell $(i(k-1), j)$ of T_i. Thirdly, consider symbol $i(k-1)+j-k+1$ of T'_i where $k \leqslant j \leqslant k+i-2$. This symbol occurs in cell $((i-1)(k-1), j)$ of T_{i-1}.

We have shown that T is a Latin trade in B_p with disjoint mate T'. Next we show orthogonality. it suffices to show that for each element $(r, c, r+c) \in T$, there is a cell $(r', c') \in T'$ containing $r+c$ such that (r', c') contains $rk+c$ in $B_p(k)$ (equivalently, $r'k+c' = rk+c$).

Firstly, let $(0, j, j) \in T_0$ where $0 \leqslant j \leqslant k-2$. Then $(p-k, j+k-1, j) \in T'_{k-1}$. Next let $1 \leqslant i \leqslant k-1$. Let $(i(k-1), j, i(k-1)+j) \in T_i$ where $i \leqslant j \leqslant k-1$ ($i \leqslant j \leqslant k-2$ when $i = 0$). Then $((i-1)(k-1), j-1, i(k-1)+j) \in T'_{i-1}$. Next let $1 \leqslant i \leqslant k-1$. Let $(i(k-1), j, i(k-1)+j) \in T_i$ where $k \leqslant j \leqslant k+i-1$. Then $(i(k-1)+1, j-k, i(k-1)+j) \in T'_i$. Let $0 \leqslant i \leqslant k-2$. Let $(i(k-1), j, i(k-1)+j) \in T_i$ where $k+i \leqslant j \leqslant 2(k-1)$. Then $((i+1)(k-1)+1, j-k+1, i(k-1)+j) \in T'_{i+1}$.

Next let $1 \leqslant i \leqslant k-1$. Let $(i(k-1)+1, j, i(k-1)+1+j) \in T_i$ where $i-1 \leqslant j \leqslant k-2$. Then $(i(k-1), j+k, i(k-1)+1+j) \in T'_i$. Let $2 \leqslant i \leqslant k-1$. Let $(i(k-1)+1, j, i(k-1)+1+j) \in T_i$ where $0 \leqslant j \leqslant i-2$. Then $((i-1)(k-1), j+k-1, i(k-1)+1+j) \in T'_{i-1}$. Finally let $1 \leqslant i \leqslant k-1$. Let $(i(k-1)+1, j, i(k-1)+1+j) \in T_i$ where $k \leqslant j \leqslant k+i-2$. Then $((i+1)(k-1)+1, j+1, i(k-1)+1+j) \in T'_{i+1}$.

An *intercalate* in a Latin square is a 2×2 subsquare. The construction in this section shows the potential of using trades to construct MOLS with particular properties. We demonstrate this with the following theorem.

Theorem 25. *Let p be a prime such that $p \equiv 1 \pmod 6$. Then there exists a Latin square L orthogonal to B_p such that L contains an intercalate.*

Proof. Let $L := (B_p \setminus T) \cup T'$, where T and T' are defined as in this section. We have shown above that L is orthogonal to $B_p(k)$. Observe that $(k-1, 1, 2k), (k-1, k, k)$ and $(k, 1, k)$ are each elements of T'_1 and thus L. Finally, cell (k, k) is not included in T so $(k, k, 2k) \in L$. □

8 Computational results

In this section, we give some computational results on the spectrum of the possible sizes of orthogonal trades mentioned in the previous sections. These orthogonal trades can be found as ancillary files in [4].

Let S_p be the set of sizes so that an orthogonal trade in B_p of index $(1, k)$ exists for some k. For $p = 5$, $S_5 = \{0, 10, 15, 20, 25\}$.

The results for $p = 7$ and $p = 11$ are summarised in the following lemma.

Lemma 26. *The spectrum of the sizes of orthogonal trades for $p = 7$ and $p = 11$ are $S_7 = \{0, 14, 18, 21, 24, 25, \ldots, 49\}$ and $S_{11} = \{0, 22, 33, 36, 37, \ldots, 121\}$, respectively.*

Note that an orthogonal trade in B_7 of size 18 is given in Figure 1.

Our theoretical results only considered orthogonal trades when p is prime. A similar question can be studied for odd values of p in general. Here $B_p(1)$ is orthogonal to $B_p(k)$ if and only if $k \not\equiv 1 \pmod p$. Then the spectrum of the sizes of orthogonal trades in B_9 is the set $\{0, 6, 9, 12, 15, 16, 18, 19, \ldots, 81\}$.

In Section 4, we considered orthogonal trades in B_p which are constructed by permuting entire rows. These trades preserve orthogonality with one of the $p-1$ MOLS. The possible number of rows needed to be permuted are the elements of sets $\{4, 5\}$, $\{3, 5, 6, 7\}$, $\{5, 6, 7, 8, 9, 10, 11\}$ and $\{3, 4, 6, 7, 8, 9, 10, 11, 12, 13\}$ for $p = 5, 7, 11$ and 13, respectively.

This idea can be generalised for trades in B_p which preserve orthogonality with more than one of the $p-1$ MOLS. We analyse this question for orders $p = 5, 7, 11$ and 13.

We start by considering the orthogonal trades in B_p which preserve orthogonality with *two* other MOLS from the complete set of size $p-1$ - but only those formed by permuting entire rows. So, these orthogonal trades are formed in three MOLS of order p. The possible number of rows needed to be permuted are the elements of sets $\{4, 5\}$, $\{6, 7\}$, $\{5, 6, 8, 9, 10, 11\}$ and $\{4, 6, 8, 9, 10, 11, 12, 13\}$ for $p = 5, 7, 11$ and 13, respectively.

Here, the non-trivial cases occur when the number of rows are not $p-1$ or p. So, we continue with only those cases.

Next, we consider the orthogonal trades in B_p which preserve orthogonality with *three* other MOLS from the complete set of size $p-1$. The possible number of rows needed to be permuted are the sets $\{5, 9\}$ and $\{6, 11\}$ for $p = 11$ and 13, respectively.

The orthogonal trades which preserve orthogonality with four of the $p-1$ MOLS can be constructed by permuting 6 or 11 rows for $p = 13$. Lastly, an orthogonal trade which preserve orthogonality with five of the $p-1$ MOLS cannot be constructed by permuting entire rows for these orders.

References

[1] R. L. Brooks, C. A. B. Smith, A. H. Stone and W. T. Tutte. The dissection of rectangles into squares. *Duke Math. J.*, 7:312–340, 1940.

[2] N. J. Cavenagh. The theory and application of Latin bitrades: a survey. *Math. Slovaca* 58:691–718, 2008.

[3] N. J. Cavenagh. The size of the smallest latin trade in a back circulant Latin square. *Bull. Instit. Combin. Appl.* 38:11–18, 2003.

[4] N. J. Cavenagh, D. M. Donovan and F. Demirkale. Orthogonal trades in complete sets of MOLS. Preprint, arXiv:1607.04429, 2016.

[5] N. J. Cavenagh and I. Wanless. On the number of transversals in Cayley tables of cyclic groups. *Disc. Appl. Math.* 158:136–146, 2010.

[6] C. J. Colbourn and J. H. Dinitz. The Handbook of Combinatorial Designs. Second Edition. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[7] F. Demirkale, D. M. Donovan, Selda Küçükçifçi and E. Ş. Yazıcı. Orthogonal trades and the intersection problem for orthogonal arrays. *Graphs and Combinatorics*, 32:903–912, 2016.

[8] A. Drápal. On a planar construction for quasigroups. *Czechosolvak Math. J.*, 41:538–548, 1991.

[9] F. O. Farid. Criteria for invertibility of diagonally dominant matrices. *Lin. Algebra Appl.*, 215:63–93, 1995.

[10] R. A. Horn and C. R. Johnson. Matrix Analysis, Cambridge U.P., Cambridge, 1985.

[11] M. Szabados. Distances of group tables and Latin squares via equilateral triangle dissections. *J. Combinatorial Theory Ser. A*, 123:1–7, 2104.

[12] O. Taussky. A recurring theme on determinants. *Amer. Math. Monthly*, 56:672–676, 1949.

[13] G. B. Trustrum. Mrs Perkins's quilt. *Proc. Cambridge Philos. Soc.*, 61:7–11, 1965.

[14] W. B. Tutte. The dissection of equilateral triangles into equilateral triangles. *Proc. Cambridge Philos. Soc.*, 44:463–482, 1948.