A linear algebraic approach to orthogonal arrays and Latin squares

A. A. Khanban*, M. Mahdian†, and E. S. Mahmoodian‡

Abstract

To study orthogonal arrays and signed orthogonal arrays, Ray-Chaudhuri and Singhi (1988 and 1994) considered some module spaces. Here, using a linear algebraic approach we define an inclusion matrix and find its rank. In the special case of Latin squares we show that there is a straightforward algorithm for generating a basis for this matrix using the so-called intercalates. We also extend this last idea.

Keywords: Orthogonal arrays, Latin squares, basis for inclusion matrix, Latin trades

1 Introduction and preliminaries

To show the existence of signed orthogonal arrays, Ray-Chaudhuri and Singhi considered a space of linear forms in variables and calculated its rank, see [13]. Later they pointed out an error in their calculation and provided a correction, see [14]. Here we define a natural inclusion matrix corresponding to orthogonal arrays and signed orthogonal arrays. We compute the rank of this matrix and study bases of its null space. This provides helpful insight for studying these objects. In the special case of Latin squares we show that there is a straightforward algorithm for generating a basis for this matrix using the so-called intercalates. We also extend this idea for more general cases.

We follow the notations of [13] as much as possible. Let $V := \{0, 1, \ldots, v-1\}$ and V^k be the set of all ordered k-tuples of the elements of V, i.e., $V^k := \{(x_1, \ldots, x_k) \mid x_i \in V, i = 1, \ldots, k\}$. Also, let $V_I^t := \{(u_1, \ldots, u_t)_I \mid u_i \in$

*Department of Computing, Imperial College London, London SW7 2BZ, United Kingdom. (khanban@doc.ic.ac.uk)

†Yahoo! Research, Santa Clara, CA, USA. (mahdian@alum.mit.edu)

‡Department of Mathematics, Sharif University of Technology, and Institute for Studies in Theoretical Physics and Mathematics (IPM), Tehran, Iran. (emahmood@sharif.edu)

$V, i = 1, \ldots, t\}$, where I is a subset of size t of the set $\{1, \ldots, k\}$. For a pair of elements of V^k and V_I^t, where $I = \{i_1, \ldots, i_t\}$ and $i_1 < \cdots < i_t$, we define: $(u_1, \ldots, u_t)_I \in (x_1, \ldots, x_k) \iff u_j = x_{i_j}, \quad j = 1, \ldots, t.$

An orthogonal array $\mathrm{OA}_t(v, k, \lambda)$ on a set V is a collection of k-tuples of elements of V such that for each $I \subseteq \{1, \ldots, k\}$, $|I| = t$, every element of V_I^t belongs to exactly λ elements of the collection. Orthogonal arrays were first defined by Rao [12] and have been used in studying designs and codes.

Next we define the t-inclusion matrix $\mathrm{M}(t\text{-}(v, k))$. Columns of this matrix correspond to the elements of V^k (in lexicographic order) and its rows correspond to the elements of $\cup_I V_I^t$, where the union is over all t-subsets of $\{1, \ldots, k\}$. The entries of the matrix are 0 or 1, and are defined as follows. $M_{(u_1,\ldots,u_t)_I,(x_1,\ldots,x_k)} = 1 \iff (u_1, \ldots, u_t)_I \in (x_1, \ldots, x_k)$.

Example 1 *In Figure 1, the matrix* $\mathrm{M}(2\text{-}(3, 3))$ *is shown. To make it more readable, 0 entries of the matrix are represented by "·" signs. The "⋆" signs may be ignored for time being, they will be explained in Section 2.*

	⋆ 000	⋆ 001	⋆ 002	⋆ 010	⋆ 011	⋆ 012	⋆ 020	⋆ 021	⋆ 022	⋆ 100	⋆ 101	⋆ 102	⋆ 110	111	112	⋆ 120	121	122	⋆ 200	⋆ 201	⋆ 202	⋆ 210	211	212	⋆ 220	221	222
$(0,0)_{\{1,2\}}$	1	1	1	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
$(0,1)_{\{1,2\}}$	·	·	·	1	1	1	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
$(0,2)_{\{1,2\}}$	·	·	·	·	·	·	1	1	1	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
$(1,0)_{\{1,2\}}$	·	·	·	·	·	·	·	·	·	1	1	1	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
⋆ $(1,1)_{\{1,2\}}$	·	·	·	·	·	·	·	·	·	·	·	·	**1**	1	1	·	·	·	·	·	·	·	·	·	·	·	·
⋆ $(1,2)_{\{1,2\}}$	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	**1**	1	1	·	·	·	·	·	·	·	·	·
$(2,0)_{\{1,2\}}$	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	1	1	1	·	·	·	·	·	·
⋆ $(2,1)_{\{1,2\}}$	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	**1**	1	1	·	·	·
⋆ $(2,2)_{\{1,2\}}$	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	**1**	1	1
$(0,0)_{\{1,3\}}$	1	·	·	1	·	·	1	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
$(0,1)_{\{1,3\}}$	·	1	·	·	1	·	·	1	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
$(0,2)_{\{1,3\}}$	·	·	1	·	·	1	·	·	1	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
⋆ $(1,0)_{\{1,3\}}$	·	·	·	·	·	·	·	·	·	**1**	·	·	1	·	·	1	·	·	·	·	·	·	·	·	·	·	·
⋆ $(1,1)_{\{1,3\}}$	·	·	·	·	·	·	·	·	·	·	**1**	·	·	1	·	·	1	·	·	·	·	·	·	·	·	·	·
⋆ $(1,2)_{\{1,3\}}$	·	·	·	·	·	·	·	·	·	·	·	**1**	·	·	1	·	·	1	·	·	·	·	·	·	·	·	·
⋆ $(2,0)_{\{1,3\}}$	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	**1**	·	·	1	·	·	1	·	·
⋆ $(2,1)_{\{1,3\}}$	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	**1**	·	·	1	·	·	1	·
⋆ $(2,2)_{\{1,3\}}$	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	**1**	·	·	1	·	·	1
⋆ $(0,0)_{\{2,3\}}$	**1**	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·	·
⋆ $(0,1)_{\{2,3\}}$	·	**1**	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·
⋆ $(0,2)_{\{2,3\}}$	·	·	**1**	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·
⋆ $(1,0)_{\{2,3\}}$	·	·	·	**1**	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·	·	1	·	·	·	·	·
⋆ $(1,1)_{\{2,3\}}$	·	·	·	·	**1**	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·	·	1	·	·	·	·
⋆ $(1,2)_{\{2,3\}}$	·	·	·	·	·	**1**	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·	·	1	·	·	·
⋆ $(2,0)_{\{2,3\}}$	·	·	·	·	·	·	**1**	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·	·	1	·	·
⋆ $(2,1)_{\{2,3\}}$	·	·	·	·	·	·	·	**1**	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·	·	1	·
⋆ $(2,2)_{\{2,3\}}$	·	·	·	·	·	·	·	·	**1**	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·	·	1

Figure 1: $\mathrm{M}(2\text{-}(3, 3))$

A Latin square L of order v is a $v \times v$ array with entries chosen from a set, say $V = \{0, 1, \ldots, v-1\}$ in such a way that each element of V occurs precisely once in each row and in each column of the array. For ease of exposition, a Latin square L will be represented by a set of ordered triples $\{(i, j; L_{ij}) \mid \text{element } L_{ij} \text{ occurs in cell } (i, j) \text{ of the array}\}$.

It is folkloric that any Latin square of order v is equivalent to an $\mathrm{OA}_2(v, 3, 1)$. It is easy to see that any $\mathrm{OA}_t(v, k, \lambda)$ can be thought of a solution to the equation

$$\mathrm{M}\mathbf{F} = \lambda\overline{\mathbf{1}}, \tag{1}$$

where $\mathrm{M} = \mathrm{M}(t\text{-}(v, k))$, $\overline{\mathbf{1}}$ is a vector of appropriate size with all components equal to 1, and $\mathbf{F}$ is a non-negative integer-valued frequency vector, i.e., $\mathbf{F}(\mathbf{x})$ represents the number of times that OA contains the ordered k-tuple $\mathbf{x}$. Our discussion will be based on the field of real numbers.

In Section 2 we find the nullity and the rank of $\mathrm{M}(t\text{-}(v, k))$. In Section 3 we show that a very simple basis exists in the case of $\mathrm{M}(2\text{-}(v, 3))$, i.e., when the OA corresponds to a Latin square, which consist of so-called intercalates. In Section 4 we generalize the result of Section 3 for any $\mathrm{M}(t\text{-}(v, t+1))$.

2 Orthogonal arrays

The main result of this section is the following theorem,

Theorem 1 *The rank of the matrix* $\mathrm{M}(t\text{-}(v, k))$ *is equal to*

$$\mathrm{rank}(M) = \sum_{i=0}^{t} \binom{k}{i} (v-1)^i.$$

This theorem results from the following lemmas. But first we need the following notations. For every ordered k-tuple $\mathbf{x} = (x_1, \ldots, x_k)$, the set $F_{\mathbf{x}}$ is defined as

$$F_{\mathbf{x}} = \{(z_1, \ldots, z_k) \mid z_i \in \{0, x_i\}, i = 1, \ldots, k\}.$$

Also, we define $A_{\mathbf{x}} = \{i \mid x_i \neq 0\}$, $L_{\mathbf{x}} = |A_{\mathbf{x}}|$, and let $C_{\mathbf{x}}$ denote the column of the matrix M corresponding to the k-tuple $\mathbf{x}$.

Lemma 1 *For every* $\mathbf{x} \in F_{\mathbf{y}}$*,* $\mathbf{x} \neq \mathbf{y}$*, we have* $L_{\mathbf{x}} < L_{\mathbf{y}}$ *and* $\mathbf{x} \prec \mathbf{y}$*, where* $\prec$ *denotes the lexicographic order.*

Proof. Clearly, for every i, if $x_i \neq 0$, then $y_i = x_i \neq 0$. Therefore, $L_{\mathbf{x}} \leq L_{\mathbf{y}}$. Now if the equality $L_{\mathbf{x}} = L_{\mathbf{y}}$ holds, then for every non-zero y_i, the corresponding x_i is non-zero and hence equal to y_i. This implies $\mathbf{x} = \mathbf{y}$, contradicting the hypothesis. For the second part, notice that for every i, either $x_i = y_i$, or $0 = x_i \leq y_i$. Hence $\mathbf{x} \preceq \mathbf{y}$ and since $\mathbf{x} \neq \mathbf{y}$, we have $\mathbf{x} \prec \mathbf{y}$. ■

Lemma 2 *The number of linearly independent rows of* $\mathrm{M}(t\text{-}(v,k))$ *is at least the number of columns* $C_{\mathbf{x}}$ *with* $L_{\mathbf{x}} \le t$.

Proof. We show that for every column $C_{\mathbf{x}}$ with $L_{\mathbf{x}} \le t$, there exists a corresponding row such that its pivot 1 (that is the first 1 in that row) is in column $C_{\mathbf{x}}$. These rows are clearly linearly independent. Corresponding to the column $C_{\mathbf{x}}$, we construct an element $\mathbf{u}_I = (u_1, \ldots, u_t)_I$ of V_I^t as follows. Since $L_{\mathbf{x}} \le t$, we can pick a set $I = \{i_1, \ldots, i_t\}$ with $A_{\mathbf{x}} \subseteq I$. Note that there may be more than one choice for I, but choosing any of them will serve our purpose. For every $j = 1, \ldots, t$, we let $u_j = x_{i_j}$. This defines an element $\mathbf{u}_I$ such that $\mathbf{u}_I \in \mathbf{x}$. Therefore, there is a 1 in the intersection of the column $C_{\mathbf{x}}$, and the row corresponding to $\mathbf{u}_I$ in $\mathrm{M}(t\text{-}(v,k))$.

Next, we prove that every $\mathbf{y}$ such that $\mathbf{u}_I \in \mathbf{y}$ satisfies $\mathbf{x} \preceq \mathbf{y}$. This would imply that the first 1 in the row corresponding to $\mathbf{u}_I$ lies in the column $C_{\mathbf{x}}$, which completes the proof. Since for every $j = 1, \ldots, t$, $u_j = x_{i_j}$ and $u_j = y_{i_j}$, we have $x_i = y_i$ for every $i \in I$. Also, since $x_i = 0$ for every $i \notin I$, we have $x_i \in \{0, y_i\}$ for every i, or in other words, $\mathbf{x} \in F_{\mathbf{y}}$. Therefore, by Lemma 1, $\mathbf{x} \preceq \mathbf{y}$. ■

Lemma 3 $\mathrm{rank}(\mathrm{M}(t\text{-}(v,k))) \ge \sum_{i=0}^{t} \binom{k}{i} (v-1)^i$.

Proof. By Lemma 2, the rank of M is at least the number of columns $C_{\mathbf{x}}$ with $L_{\mathbf{x}} \le t$. It is easy to note that the number of vectors $\mathbf{x}$ for which $L_{\mathbf{x}} = i$ is equal to $\binom{k}{i}(v-1)^i$. This completes the proof of the lemma. ■

As it can be noted in Figure 1, in each column $C_{\mathbf{x}}$ where at least one of the components of $\mathbf{x}$ is 0, i.e. $L_{\mathbf{x}} \le 2$, there exists at least one row having a pivot 1 in that column. For example for the column C_{010} both $(0,1)_{\{1,2\}}$ and $(1,0)_{\{2,3\}}$ rows have such property. All such columns and one of the rows corresponding to that column are indicated with a "$\star$" sign and such 1's are shown in bold face and underlined.

To show the other direction in Theorem 1, we prove the following lemma.

Lemma 4 *For every vector* $\mathbf{x} \in V^k$ *with* $L_{\mathbf{x}} > t$*, we have*

$$\sum_{\mathbf{y} \in F_{\mathbf{x}}} (-1)^{L_{\mathbf{y}}} C_{\mathbf{y}} = \overline{\mathbf{0}}. \tag{2}$$

Where $\overline{\mathbf{0}}$ *is a vector of appropriate size with all components equal to* 0.

Proof. It is enough to focus on a fixed row, say $\mathbf{u}_I$, and count the number of ones in the intersection of this row and columns $C_{\mathbf{y}}$ for $\mathbf{y} \in F_{\mathbf{x}}$, by taking the signs in the above expression into account, and show that the corresponding entry in the left-hand side of the above equation is 0.

Consider a row $\mathbf{u}_I$ with $I = \{i_1, \ldots, i_t\}$ where $i_1 < \cdots < i_t$.

If there is an element $i_j \in I \setminus A_{\mathbf{x}}$ such that $u_j \neq 0$, then all the entries in the intersection of this row and columns $C_{\mathbf{y}}$ with $\mathbf{y} \in F_{\mathbf{x}}$ are 0, since for all such $\mathbf{y}$, y_{i_j} is 0 and therefore is not equal to u_j. Thus, the entry in the left-hand side of Equation (2) in the row corresponding to $\mathbf{u}_I$ is 0.

Now, suppose $u_j = 0$, for every j where $i_j \in I \setminus A_{\mathbf{x}}$. Consider the set Y of vectors, $\mathbf{y} \in F_{\mathbf{x}}$, such that the entry in the intersection of the row corresponding to $\mathbf{u}_I$ and the column $C_{\mathbf{y}}$ is 1. For every $\mathbf{y} \in Y$, $\alpha = |A_{\mathbf{x}} \cap I|$ of its entries have a value equal to the corresponding entry in $\mathbf{u}_I$. Therefore, there are $L_{\mathbf{x}} - \alpha$ entries in $\mathbf{y}$ that can take either a value of 0, or the value of the corresponding entry in $\mathbf{x}$. We call these $L_{\mathbf{x}} - \alpha$ entries the *free* entries of $\mathbf{y}$. Consider the set of all $\mathbf{y} \in Y$ that have j non-zero free entries (i.e., are equal to the corresponding value in $\mathbf{x}$). The number of such $\mathbf{y}$'s is $\binom{L_{\mathbf{x}}-\alpha}{j}$ and for each such $\mathbf{y}$, $L_{\mathbf{y}} = j + \alpha - \zeta$, where ζ is the number of zeros in the intersection of I and A_x. Therefore, the entry in the row corresponding to $\mathbf{u}_I$ in the left-hand side of Equation (2) is equal to

$$\sum_{j=0}^{L_{\mathbf{x}}-\alpha} (-1)^{j+\alpha-\zeta} \binom{L_{\mathbf{x}} - \alpha}{j} = (-1)^{\alpha-\zeta} \sum_{j=0}^{L_{\mathbf{x}}-\alpha} (-1)^j \binom{L_{\mathbf{x}} - \alpha}{j} = 0.$$

Thus, all entries of the vector in the left-hand side of Equation (2) are 0. ■

Lemma 5 $\quad \mathrm{rank}(\mathrm{M}(t\text{-}(v,k))) \leq \sum_{i=0}^{t} \binom{k}{i}(v-1)^i$.

Proof. By applying Lemma 4, repeatedly, to any column $C_{\mathbf{x}}$ with $L_{\mathbf{x}} > t$, we can write $C_{\mathbf{x}}$ in terms of columns $C_{\mathbf{y}}$ with $L_{\mathbf{y}} \leq t$. Thus the latter columns form a spanning set for the column space of $\mathrm{M}(t\text{-}(v,k))$. We noted earlier that there are exactly $\sum_{i=0}^{t} \binom{k}{i}(v-1)^i$ of such columns. ■

Theorem 1 follows from Lemma 5 and Lemma 3.

3 Latin squares and Latin trades

As we noted earlier, a Latin square of order v may be viewed as an $\mathrm{OA}_2(v,3,1)$. So the matrix $\mathrm{M}(2\text{-}(v,3))$ is of special interest. In this section we find a basis for $\mathrm{M}(2\text{-}(v,3))$ which consists of the so-called intercalates.

We start with a few definitions. A partial Latin square P of order v is a $v \times v$ array in which some of the entries are filled with elements from a set $V = \{0, 1, \ldots, v-1\}$ in such a way that each element of V occurs at most once in each row and at most once in each column of the array. In other words, there are cells in the array that may be empty, but the positions that are filled conform with the Latin property of array. Once again a partial Latin square may be represented as a set of ordered triples. However in this case we will include triples of the form $(i, j; \emptyset)$ and read this to mean that cell (i, j) of the partial Latin square is empty. The set of cells $\mathcal{S}_P = \{(i, j) \mid (i, j; P_{ij}) \in P, \text{ for some } P_{ij} \in V\}$ is said to determine the **shape** of P and $|\mathcal{S}_P|$ is said to be the **volume** of the partial Latin square. That is, the volume is the number of nonempty cells. For each row r, $0 \le r \le v - 1$, we let $\mathcal{R}_P^r$ denote the set of entries occurring in row r of P. Formally, $\mathcal{R}_P^r = \{P_{rj} \mid P_{rj} \in V \wedge (r, j; P_{rj}) \in P\}$. Similarly, for each column c, $0 \le c \le v - 1$, we define $\mathcal{C}_P^c = \{P_{ic} \mid P_{ic} \in V \wedge (i, c; P_{ic}) \in P\}$.

A **Latin trade**, $T = (P, Q)$, of **volume** s is an ordered set of two partial Latin squares, of order v, such that

1. $\mathcal{S}_P = \mathcal{S}_Q$,
2. for each $(i, j) \in \mathcal{S}_P$, $P_{ij} \neq Q_{ij}$,
3. for each r, $0 \le r \le v - 1$, $\mathcal{R}_P^r = \mathcal{R}_Q^r$, and
4. for each c, $0 \le c \le v - 1$, $\mathcal{C}_P^c = \mathcal{C}_Q^c$.

Thus a Latin trade is a pair of disjoint partial Latin squares of the same shape and order, which are row-wise and column-wise mutually balanced. We refer to the shape of a Latin trade T as the shape of the individual components P and Q.

Example 2 *Below is an example of two partial Latin squares which together form a Latin trade of order 5 and of volume 19. To conserve space we will display a Latin trade by superimposing one partial Latin square on top of the other, and using subscripts to differentiate the entries of the second from those of the first, as shown below.*

·	·	2	3	1
·	2	·	1	4
1	·	0	4	3
0	4	1	·	2
4	1	3	2	0

·	·	1	2	3
·	1	·	4	2
4	·	3	1	0
1	2	0	·	4
0	4	2	3	1

·	·	2_1	3_2	1_3
·	2_1	·	1_4	4_2
1_4	·	0_3	4_1	3_0
0_1	4_2	1_0	·	2_4
4_0	1_4	3_2	2_3	0_1

Figure 2: A Latin trade

The concept of a Latin trade in a Latin square is similar to the concept of a mutually balanced set or a trade in a block design, see [9]. The same as trades in design theory, the discussion of Latin trades is related to intersection problems.

For example, they are relevant to the problem of finding the possible number of intersections for Latin squares (see [7], [6], [2], and [1]). Also Latin trades arise naturally in the discussion of critical sets in Latin squares (see for example [10] and [11]).

Latin trades have been studied by many authors. Fu and Fu [6] used the term “disjoint and mutually balanced” (DMB) partial Latin squares, Keedwell [10] used “critical partial Latin square” (CPLS), while Donovan et al. [4] used the term “Latin interchange”. Adams et al. [1] suggest the terminology ‘2-way Latin trade” for consistency with similar concepts in other combinatorial structures such as block designs, graph colouring, cycle systems, etc. See for instance [9], [15], [8], and [3] for further use of trades.

A Latin trade of volume 4 which is unique (up to isomorphism), is called an intercalate (see Figure 3).

·	·	·	·	·	·
·	1_2	·	2_1	·	·
·	·	·	·	·	·
·	2_1	·	1_2	·	·
·	·	·	·	·	·
·	·	·	·	·	·

Figure 3: An intercalate

Similar to orthogonal arrays which correspond to solutions of the Equation (1), it is clear that any Latin trade may also be treated as a solution $\mathbf{T}$, to the equation:

$$\mathrm{M}\mathbf{T} = \overline{\mathbf{0}}, \tag{3}$$

where $M = \mathrm{M}(2\text{-}(v,3))$ and $\mathbf{T}$ is a (signed) frequency vector derived from the trade $T = (P,Q)$, i.e.,

$$\mathbf{T}_{ijk} = \begin{cases} 1 & \text{if } (i,j;k) \in P \\ -1 & \text{if } (i,j;k) \in Q \\ 0 & \text{otherwise.} \end{cases}$$

Therefore Latin trades are in the null space of $\mathrm{M}(2\text{-}(v,3))$.

Theorem 2 *There exists a basis for the null space of the matrix* $\mathrm{M}(2\text{-}(v,3))$ *consisting only of intercalates.*

Proof. Latin trades are in the null space of $\mathrm{M}(2\text{-}(v,3))$. By Theorem 1 we know that

$$\mathrm{null}(\mathrm{M}(2\text{-}(v,3))) = (v-1)^3.$$

For each i, j, k; $1 \leq i, j, k \leq v - 1$, consider the ijk'th intercalate defined in Figure 4.

$$\begin{array}{c|ccccc} & 0 & \cdots & j & \cdots \\ \hline 0 & 0_k & \cdots & k_0 & \cdots \\ \vdots & \vdots & \ddots & \vdots & \ddots \\ i & k_0 & \cdots & 0_k & \cdots \\ \vdots & \vdots & \cdots & \vdots & \cdots \end{array}$$

Figure 4: Basis intercalates

There are $(v - 1)^3$ of them. The vectors corresponding to these intercalates are independent, as for example, the frequency vector of the ijk'th intercalate has an entry -1 in the (i, j, k) coordinate while all others have 0 in that coordinate. Therefore, they form a basis for the null space of M(2-$(v, 3)$). ■

The above theorem shows, existentially, that every Latin trade can be written as the sum of intercalates. In [5], Donovan and Mahmoodian introduced a simple combinatorial algorithm which enables one to compute such a decomposition. But by linear algebraic approach and knowing a basis which consists only of intercalates, makes it straightforward to do this task. We give an example of this method:

$$\begin{array}{|c|c|c|c|}\hline 0_1 & 1_2 & 2_3 & 3_0 \\ \hline 1_2 & 2_1 & \cdot & \cdot \\ \hline 2_3 & \cdot & 3_2 & \cdot \\ \hline 3_0 & \cdot & \cdot & 0_3 \\ \hline \end{array} = \begin{array}{|c|c|c|c|}\hline 0_1 & 1_0 & \cdot & \cdot \\ \hline 1_0 & 0_1 & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot \\ \hline \end{array} - \begin{array}{|c|c|c|c|}\hline 0_2 & 2_0 & \cdot & \cdot \\ \hline 2_0 & 0_2 & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot \\ \hline \end{array}$$

$$+ \begin{array}{|c|c|c|c|}\hline 0_2 & \cdot & 2_0 & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot \\ \hline 2_0 & \cdot & 0_2 & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot \\ \hline \end{array} - \begin{array}{|c|c|c|c|}\hline 0_3 & \cdot & 3_0 & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot \\ \hline 3_0 & \cdot & 0_3 & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot \\ \hline \end{array} + \begin{array}{|c|c|c|c|}\hline 0_3 & \cdot & \cdot & 3_0 \\ \hline \cdot & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot \\ \hline 3_0 & \cdot & \cdot & 0_3 \\ \hline \end{array}$$

Figure 5: An example of the algorithm

4 A basis for the null space of M(t-$(v, t + 1)$)

In this section we generalize the notion of Latin trades and find a basis for the null space of M(t-$(v, t + 1)$). First we note that each Latin trade $T = (P, Q)$ may be represented by a homogeneous polynomial of order 3 as follows. The polynomial is over a non-commutative ring, hence the terms are ordered multiplicatively (meaning that $x_{i_1}x_{i_2}x_{i_3}$ is different from, say $x_{i_2}x_{i_1}x_{i_3}$):

$$P(x_0, x_1, \ldots, x_{v-1}) = \sum_{(i_1,i_2;i_3)\in P} x_{i_1}x_{i_2}x_{i_3} - \sum_{(j_1,j_2;j_3)\in Q} x_{j_1}x_{j_2}x_{j_3}.$$

Note that the positive terms correspond to the elements of P while the negative terms correspond to the elements of Q. For example the intercalates which form a basis for the null space of M(2-$(v, 3)$) in Theorem 2 are:

$$\begin{aligned} P(x_0, x_1, \ldots, x_{v-1}) &= x_0x_0x_0 + x_0x_jx_k + x_ix_0x_k + x_ix_jx_0 \\ &\quad - x_0x_0x_k - x_0x_jx_0 - x_ix_0x_0 - x_ix_jx_k \\ &= (x_0 - x_i)(x_0 - x_j)(x_0 - x_k), \quad 1 \le i, j, k \le v - 1. \end{aligned}$$

Similarly, each homogeneous polynomial $P(x_0, x_1, \ldots, x_{v-1})$ of order k, whose terms are ordered multiplicatively, corresponds to a frequency vector $\mathbf{T}$. If $\mathbf{T}$ satisfies

$$\mathrm{M}\mathbf{T} = \overline{\mathbf{0}}, \tag{4}$$

where $M = \mathrm{M}(t\text{-}(v, k))$, we call it a t-(v, k) Latin trade. So, a Latin trade defined in Section 3 is also 2-$(v, 3)$ Latin trade. Any t-$(v, t+1)$ Latin trade of the following form will be called a t-$(v, t+1)$ intercalate:

$$P(x_0, x_1, \ldots, x_{v-1}) = (x_{i_1} - x_{j_1})(x_{i_2} - x_{j_2}) \cdots (x_{i_{t+1}} - x_{j_{t+1}}),$$

where i_m and $j_n \in \{0, \ldots, v-1\}$, and for each l, i_l is distinct from j_l. A 2-$(v, 3)$ intercalate is simply an intercalate in a Latin square, defined in the previous section.

Theorem 3 *There exists a basis for the null space of the matrix* M(t-$(v, t+1)$) *consisting only of* t-$(v, t+1)$ *intercalates.*

Proof. It can easily be checked that t-$(v, t+1)$ intercalates are included in the null space of M(t-$(v, t+1)$). By Theorem 1 we know that $\mathrm{null}(\mathrm{M}(t\text{-}(v, t+1))) = (v-1)^{t+1}$.

Consider the following set of $(v-1)^{t+1}$ intercalates:

$$P(x_0, x_1, \ldots, x_{v-1}) = (x_0 - x_{i_1})(x_0 - x_{i_2}) \cdots (x_0 - x_{i_{t+1}}),$$
$$1 \le i_1, i_2, \ldots, i_k \le v - 1.$$

The intercalates in this set are independent. For example, the frequency vector of the $i_1 i_2 \cdots i_{t+1}$'th intercalate has a non-zero entry, namely $(-1)^{t+1}$, in the $(i_1, i_2, \ldots, i_{t+1})$th coordinate, while all others have 0 in that coordinate. Therefore, they form a basis for the null space of M(t-$(v, t+1)$). ■

Finally, we note that given the above generalization of the concept of Latin trades, many questions similar to the ones in the theory of t-trades in block designs, may be raised. For example, it would be interesting to characterize the possible support sizes of t-(v, k) Latin trades.

Acknowledgement

The authors appreciate comments of John van Rees, specially for the last lines of the proof of Lemma 4. This work was partly done while the third author was spending his sabbatical leave in the Microsoft and also in the Institute for Advanced Studies in Basic Sciences (IASBS), Zanjan and finally in the Institute for Studies in Theoretical Physics and Mathematics (IPM). . He would like to thank all these institutions for their warm and generous hospitality and support.

References

[1] Peter Adams, Elizabeth J. Billington, Darryn E. Bryant, and E. S. Mahmoodian. The three-way intersection problem for Latin squares. *Discrete Math.*, 243(1-3):1–19, 2002.

[2] Elizabeth J. Billington. The intersection problem for combinatorial designs. *Congr. Numer.*, 92:33–54, 1993. Twenty-second Manitoba Conference on Numerical Mathematics and Computing (Winnipeg, MB, 1992).

[3] Elizabeth J. Billington and D. G. Hoffman. Trades and graphs. *Graphs Combin.*, 17(1):39–54, 2001.

[4] Diane Donovan, Adelle Howse, and Peter Adams. A discussion of Latin interchanges. *J. Combin. Math. Combin. Comput.*, 23:161–182, 1997.

[5] Diane Donovan and E. S. Mahmoodian. An algorithm for writing any Latin interchange as a sum of intercalates. *Bull. Inst. Combin. Appl.*, 34:90–98, 2002. Corrigendum: *Bull. Inst. Combin. Appl.* 37:44, 2003.

[6] Chin Mei Fu and Hung-Lin Fu. The intersection problem of Latin squares. *J. Combin. Inform. System Sci.*, 15(1-4):89–95, 1990. Graphs, designs and combinatorial geometries (Catania, 1989).

[7] H-L. Fu. *On the construction of certain type of latin squares with prescribed intersections*. PhD thesis, Auburn University, 1980.

[8] M. T. Hajiaghaee, E. S. Mahmoodian, V. S. Mirrokni, A. Saberi, and R. Tusserkani. On the simultaneous edge-coloring conjecture. *Discrete Math.*, 216(1-3):267–272, 2000.

[9] A. S. Hedayat. The theory of trade-off for t-designs. In *Coding theory and design theory, Part II*, volume 21 of *IMA Vol. Math. Appl.*, pages 101–126. Springer, New York, 1990.

[10] A. D. Keedwell. Critical sets for Latin squares, graphs and block designs: a survey. *Congr. Numer.*, 113:231–245, 1996. Festschrift for C. St. J. A. Nash-Williams.

[11] A. D. Keedwell. Critical sets in latin squares and related matters: an update. *Util. Math.*, 65:97–131, 2004.

[12] C. Radhakrishna Rao. Factorial experiments derivable from combinatorial arrangements of arrays. *Suppl. J. Roy. Statist. Soc.*, 9:128–139, 1947.

[13] D. K. Ray-Chaudhuri and N. M. Singhi. On existence and number of orthogonal arrays. *J. Combin. Theory Ser. A*, 47(1):28–36, 1988.

[14] D. K. Ray-Chaudhuri and N. M. Singhi. Corrigendum: "On existence and number of orthogonal arrays" [J. Combin. Theory Ser. A **47** (1988), no. 1, 28–36; MR0924450 (89a:05039)]. *J. Combin. Theory Ser. A*, 66(2):327–328, 1994.

[15] Anne Penfold Street. Defining sets for block designs: an update. In *Combinatorics advances (Tehran, 1994)*, volume 329 of *Math. Appl.*, pages 307–320. Kluwer Acad. Publ., Dordrecht, 1995.