Row-column Factorial Designs and Mutually Orthogonal Frequency Rectangles

A thesis submitted in partial fulfilment of the

requirements for the degree of

Doctor of Philosophy in Mathematics

by

Fahim Rahim

Department of Mathematics

THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato

February 2023

Abstract

A (full) q^k *factorial design* with replication λ is the multi-set containing all possible q-ary sequences of length k, each occurring exactly λ times. An $m \times n$ *row-column factorial design* is any arrangement of λ replicates of the q^k factorial design in an $m \times n$ array. We say that the design has *strength* t if each row and column is an orthogonal array of strength t. We denote such a design by $I_k(m, n, q, t)$.

A *frequency rectangle* of type $\mathrm{FR}(m, n; q)$ is an $m \times n$ array based on a symbol set S of size q, such that each element of S appears exactly n/q times in each row and m/q times in each column. Two frequency rectangles of the same type are said to be *orthogonal* if each possible pair of symbols appears the same number of times when the two arrays are superimposed. By k–$\mathrm{MOFR}(m, n; q)$ we mean a set of k frequency rectangles of type $\mathrm{FR}(m, n; q)$ in which every pair is orthogonal.

In Chapter 4, we give the necessary and sufficient conditions when a row-column factorial design of strength 1 exists. We show that an array of type $I_k(m, n, q, 1)$ exists if and only if (a) $q|m$, $q|n$ and $q^k|mn$; (b) $(k, q, m, n) \neq (2, 6, 6, 6)$ and (c) if $(k, q, m) = (2, 2, 2)$ then 4 divides n. In Chapter 5, we discuss designs of strength 2 and above. We solve the case completely when $t = 2$ and q is a prime power: we show that there exists an array of type $I_k(q^M, q^N, q, 2)$ if and only if $k \leq M + N$, $k \leq (q^M - 1)/(q - 1)$ and $(k, M, q) \neq (3, 2, 2)$. We also show that $I_{k+\alpha}(2^\alpha b, 2^k, 2, 2)$ exists whenever $\alpha \geq 2$ and $2^\alpha + \alpha + 1 \leq k < 2^\alpha b - \alpha$, assuming there exists a Hadamard matrix of order $4b$. For strength 3 we restrict ourselves to the binary case, solving it completely when q is a power of 2.

In Chapter 6, our focus is on mutually orthogonal frequency rectangles (MOFR). We use orthogonal arrays and Hadamard matrices to construct sets of MOFR. We also describe a new form of orthogonality for a set of frequency rectangles. We say that a k–$\mathrm{MOFR}(m, n; q)$ is t–*orthogonal* if each subset of size t, when superimposed, forms a q^t factorial design with replication mn/q^t. A set of vectors over a finite field is said to be t-*independent* if each subset of size t is linearly independent. We describe a relationship between a set of t–orthogonal MOFR and a set of t-independent vectors. We use known results

from coding theory and related literature to formulate a table for the size of a set of t-independent vectors of length $N \leq 16$, over $\mathbb{F}_2$. We also describe a method to construct a set of $(p-1)$–MOFR$(2p, 2p; 2)$ where p is an odd prime, improving known lower bounds for all $p \geq 19$.

Note on Publications

This thesis is for PhD with publications and the details of the publications are as follows:

Chapter 4: Published Online

F. Rahim and N. J. Cavenagh. Row-column factorial designs with multiple levels. *Journal of Combinatorial Designs*, 29:750-764, 2021. https://doi.org/10.1002/jcd.21799

Chapter 5: Published Online

F. Rahim and N. J. Cavenagh. Row-column factorial designs with strength at least 2. *Linear Algebra and its Applications*, 667:44–70, 2023. https://doi.org/10.1016/j.laa.2023.02.018

Chapter 6: Submitted

F. Rahim and N. J. Cavenagh. Mutually orthogonal frequency rectangles. *arXiv*, 2022. https://doi.org/10.48550/arXiv.2212.10706

Acknowledgements

First and foremost, I would like to extend my deepest gratitude to Allah, the Almighty, for guiding me and providing me with the strength and determination to achieve my goals. I would also like to pay homage to Prophet Muhammad (peace be upon him), who serves as a source of inspiration and guidance in all aspects of my life.

I am profoundly grateful to my advisor, Associate Professor Nicholas Cavenagh, for his unwavering support, guidance, and encouragement throughout my PhD journey. His expertise and passion for the field have been an inspiration to me. He was always patient and kind to me and his ability to bring out the best in me has been instrumental in helping me to reach this point.

I would also like to thank my co-supervisor, Associate Professor Daniel Delbourgo and the rest of the faculty and staff members, at the Department of Mathematics, University of Waikato for providing me with a friendly, supportive and constructive environment for the research.

I am grateful to HEC Pakistan and The Women University of AJK for providing me with the financial support necessary to undertake this PhD journey. The scholarship has been a crucial factor in allowing me to focus fully on my research and has greatly contributed to the completion of my thesis.

With the deepest gratitude and appreciation, I would like to acknowledge my parents, for their unconditional love, support, and encouragement throughout my life. Their unwavering faith in me has been the foundation of my success, and I am forever grateful for the sacrifices they have made to help me reach this point. This achievement is as much theirs as it is mine, and I am proud to dedicate it to them.

I would like to express my sincere gratitude to my friends who made my stay in New Zealand an unforgettable experience. Their kindness, support, and laughter have been a source of constant joy and happiness for me, and I am so grateful to have had them by my side during this amazing adventure. I would like to extend a special thank you to Zubair, Ejaz, Shaheer, Ali, Ataullah, Irfan, Amir, Waqas, Adnan, Atif and many more (it is impossible to write the names of all) for their constant care and support, and for making my time in New Zealand truly special.

I would like to express my deepest love and gratitude to my wife for her unwavering support and encouragement throughout my PhD journey. Her love, patience, and understanding have been a constant source of strength and motivation for me, and I could not have completed this journey without her by my side.

Finally, I would like to dedicate this work to my father, mother, my wife and my beautiful daughter Maahrosh. May ALLAH Almighty bless them with good health and happiness in every step of life.

List of Tables

Contents

Chapter 1

Introduction

Consider an experiment [4, Sec 9.8] in a manufacturing plant. The process of manufacturing is as follows. A piece of material is first chosen from eight available batches and then is prepared by receiving a combination of five treatments (say A, B, C, D and E). The prepared material is then fed into one of four machines for processing.

The experiment aims to analyse the effect of the treatments on the final product. Moreover, we are also interested in the effect of the batch chosen and the machine used for processing. This could be done by carrying out a factorial experiment using the design given in Table 1.1.

		Batches							
		1	2	3	4	5	6	7	8
Machines	1	00000	11000	10101	01101	11011	00011	01110	10110
	2	11001	00001	01100	10100	00010	11010	10111	01111
	3	00111	11111	10010	01010	11100	00100	01001	10001
	4	11110	00110	01011	10011	00101	11101	10000	01000

Table 1.1: A 2^5 Row-column factorial design

Here the binary sequences represent the combination of treatments received, and rows and columns denote the processing machine and the batch of

the material, respectively. For example, the sequence 11010 in column 6 and row 2, represents that the piece of material is chosen from batch 6, treated with treatments A, B and D, and processed by Machine 2.

In the field of experimental design, such designs are referred to as *row-column factorial designs*. Let $[q] = \{0, 1, \ldots, q-1\}$. Formally, the q^k (full) factorial design with replication α is the multi-set consisting of α occurrences of each element of $[q]^k$; we denote this by $\alpha \times [q]^k$. An $m \times n$ row-column factorial design q^k is any arrangement of the elements of $\alpha \times q^k$ into an $m \times n$ array. We say that the rows and columns are *blocking factors* in the above design. A blocking factor is a partition (usually equipartition) of the treatment combinations of the factorial design.

In the above design, the 2^5 factorial is arranged so that if we fix a position (corresponding to a treatment), the entries 0 and 1 appear equally often in each row (or column). This type of regularity is desirable in applications; using experimental design terminology, the main effects are not "confounded" with the blocks (see Chapter 3 for more details). In combinatorics, this property pertains to structures known as *frequency rectangles*. Formally:

A frequency rectangle (also called *F-rectangle*) of type $\mathrm{FR}(m, n; q)$ is an $m \times n$ array based on a symbol set S of size q, such that each element of S appears exactly n/q times in each row and m/q times in each column. A frequency rectangle of type $\mathrm{FR}(n, n; q)$ is known as a *frequency square*.

Frequency rectangles can be thought of as a generalisation of *Latin squares*. A Latin square is a frequency rectangle of type $\mathrm{FR}(n, n; n)$, that is, a square array based on n symbols such that each symbol appears exactly once in each row and in each column.

Two frequency rectangles, F_1 and F_2, of the same type, are said to be *orthogonal* if each possible ordered pair of symbols appear the same number of times when F_1 and F_2 are superimposed. A set of frequency rectangles in which every pair is orthogonal is called a set of *mutually orthogonal frequency rectangles* (MOFR). In the case of frequency squares and Latin squares,

we use the terms MOFS and MOLS respectively. We use the notation k–MOFR$(m, n; q)$ to represent a set of k MOFR of type FR$(m, n; q)$ and the notation k–MOFS$(n; q)$ when $m = n$.

Thus the above design (Table 1.1) can also be seen as a set of five mutually orthogonal frequency rectangles $F_1, \ldots, F_5$ of type FR$(4, 8; 2)$ (given in Table 1.2) with the property that they form a 2^5 factorial design upon superimposition.

$$F_1 = \begin{array}{cccccccc} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array} \qquad F_2 = \begin{array}{cccccccc} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{array}$$

$$F_3 = \begin{array}{cccccccc} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{array} \qquad F_4 = \begin{array}{cccccccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{array}$$

$$F_5 = \begin{array}{cccccccc} 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{array}$$

Table 1.2: Five frequency rectangles of type FR$(4, 8; 2)$ which yield the design in Table 1.1.

It is important to note here that a set of 3 or more MOFR does not always constitute a row-column factorial design when superimposed. For example, in Table 1.3 we have three MOFR of type FR$(6, 12; 2)$ that do not form a row-column factorial design, as the sequences of odd weights (001, 010, 100, 111) appear 6 times while the sequences of even weights (000, 110, 101, 011) appear 12 times in the superimposed array.

000	111	000	101	011	110	000	111	000	101	011	110
111	000	000	011	110	101	111	000	000	011	110	101
000	000	111	110	101	011	000	000	111	110	101	011
101	011	110	010	100	001	101	011	110	010	100	001
011	110	101	100	001	010	011	110	101	100	001	010
110	101	011	001	010	100	110	101	011	001	010	100

Table 1.3: Three mutually orthogonal frequency rectangles of type FR$(6, 12; 2)$

An upper bound on the size of k–MOFR$(m, n; q)$ is given by (see Theorem 6.1):

$$k \leq \frac{(m-1)(n-1)}{(q-1)}.$$

The upper bounds $k \leq (n-1)^2/(q-1)$ ([3]) and $k \leq n-1$ (see Lemma 2.1) for a set of MOFS and a set of MOLS, respectively, can be derived from the above expression.

A set of MOFR that reaches the upper bound (described above) is known as *complete*. Finding complete, or largest possible sets of MOFR is a well-known problem that has been investigated by many mathematicians as these structures have applications in the field of experimental design, coding theory, and cryptology (a survey of applications is given in [5]).

We return now to the experimental application. As we have seen, the fact that the design in Table 1.1 is composed of frequency rectangles is advantageous in estimating the effects of individual treatment factors. However, if we are also interested in analysing the interaction between two treatments, it is desirable to have some additional properties. For example, in order to estimate the effect of the interaction of treatments B and C, ideally, if we fix the corresponding positions (2nd and 3rd) each possible ordered pair of symbols (0 and 1) should appear equally often in each column and in each row. By close inspection, we can see that in the above design (Table 1.1) this property holds for all two-factor interactions except for AB and CD, in the columns (as shown in Table 1.4).

Machines	Batches							
	1	2	3	4	5	6	7	8
1	00000	11000	10101	01101	11011	00011	01110	10110
2	11001	00001	01100	10100	00010	11010	10111	01111
3	00111	11111	10010	01010	11100	00100	01001	10001
4	11110	00110	01011	10011	00101	11101	10000	01000

Table 1.4: The interaction factor AB is confounded with the columns.

In the language of experimental design, the interaction effects AB and CD are confounded with the batches (again, for more details see Chapter 3). Similarly, we want analogous properties if we are interested in estimating three or higher-factor interactions without confounding. We next introduce orthogonal arrays that will be useful to define such designs.

An *orthogonal array* of size N, degree k, strength t based on a symbol set S of size q, denoted by $\mathrm{OA}(N, k, q, t)$, is an $N \times k$ array of elements of S such that if we fix any t columns then each possible t-tuple of symbols appear the same number of times as a row.

Observe that each column of the design in Table 1.1 is an $\mathrm{OA}(4, 5, 2, 1)$ of strength 1 and each row is an $\mathrm{OA}(8, 5, 2, 2)$. For example, the orthogonal arrays based on column 1 and row 1 of Table 1.1 are given below.

$$\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{array}$$

$\mathrm{OA}(4,5,2,1)$

$$\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{array}$$

$\mathrm{OA}(8,5,2,2)$

Table 1.5: Orthogonal arrays based on column 1 and row 1 of the design given in Table 1.1.

Thus if each block (row and column) of a factorial design forms an orthogonal array of strength t, then all t factor interactions are estimable. Now we give a formal definition of such a design.

We say that a row-column factorial design q^k is of *strength* t if each of its columns is an orthogonal array of type $OA(m,k,q,t)$ and each of its rows is the transpose of an $OA(n,k,q,t)$. We denote such a design by $I_k(m,n,q,t)$. In the case of $t=1$ we sometimes drop t and simply write $I_k(m,n;q)$. Note that in Chapter 4, we refer to the designs of strength 1 as *regular* designs. Without loss of generality, we always assume $m \leq n$.

In Chapter 2, we give a brief survey and introduction to the mathematical structures that are closely related to the work done in this thesis, including frequency rectangles, orthogonal arrays, Hadamard matrices, and linear codes. Although the focus of this thesis is not applied experimental design, given the fact that row-column factorial designs are used in practice, we survey these applications in Chapter 3.

One of the key research questions in this thesis is: For which parameters k,m,n,q, and t does a row-column factorial design $I_k(m,n,q,t)$ exist?

In Chapter 4 [7], we answer this question for row-column factorial designs of strength 1. We give three different construction methods to construct the

designs of strength 1. First, we give a recursive method in which we take the Kronecker product of smaller designs in order to construct bigger ones. Our main result related to the recursive construction is as follows:

Theorem 1.1. *If there exist r arrays of types $I_k(m_i, n_i, q_i, 1)$, where $i \in [r]$, then there exist an array of type $I_k(\prod_{i=0}^{r-1} m_i, \prod_{i=0}^{r-1} n_i, \prod_{i=0}^{r-1} q_i, 1)$.*

The above is generalized to strength t in Chapter 5 [9].

When q is a prime power we use polynomials over the finite field $\mathbb{F}_q$ to construct row-column factorial designs:

Theorem 1.2. *Let $q \geq 2$ be a prime power. Let $M, N \geq 1$ and $(M, N, q) \neq (1, 1, 2)$. There exists an array of type $I_{M+N}(q^M, q^N, q, 1)$.*

This generalizes a result in [2].

Another important construction is the one that extends the design of the form $I_{M+N}(q^M, q^N, q, 1)$ to $I_k(q^M b_1, q^N b_2, q, 1)$ where q divides the product $b_1 b_2$:

Theorem 1.3. *Let q be a divisor of $b_1 b_2$. If there exists an array of type $I_{M+N}(q^M, q^N, q, 1)$, then there exists an array of type $I_{M+N+1}(q^M b_1, q^N b_2, q, 1)$.*

Consequently, we give the necessary and sufficient conditions when a row-column factorial design $I_k(m, n, q, 1)$ exists. Our main result in Chapter 4, is the following:

Theorem 1.4. *Let $m \leq n$. There exists an array of type $I_k(m, n, q, 1)$ if and only if q divides m, q divides n, q^k divides mn and neither of the following hold:*

(i) *$k = q = m = 2$ and $n \equiv 2 \pmod 4$.*

(ii) *$k = 2$ and $q = m = n = 6$.*

In Chapter 5 [9], we examine the existence of row-column factorial designs of strength 2 and above. We first give some general recursive constructions

which are applicable to row-column factorial designs of any strength. We categorize arrays into abelian and non-abelian designs. We say that a design $M = I_k(m, n, q, t)$ is *abelian* if there exist two orthogonal arrays R and C of type $\mathrm{OA}(n, k, q, t)$ and $\mathrm{OA}(m, k, q, t)$, respectively, such that the cell in the intersection of row i and column j of M is a vector sum over $\mathbb{F}_q$ of row i of C and column j of R (i.e., that is R is the first row of M and C is the first column of M and each column of M is a coset of C with row i of R). We denote such an array by $C \boxplus R$.

Let A be a matrix over the field $\mathbb{F}_q$. By $\langle A \rangle$, we represent a matrix whose row vectors are the row space of A. We provide a sufficient condition on the product $CA^{\perp}$ ($A^{\perp}$ is defined in the theorem below) such that $C \boxplus \langle A \rangle$ is an abelian row-column factorial design.

Theorem 1.5. *Let G be an $OA(m, k, q, t)$ and let $\langle A \rangle$ be an $OA(q^N, k, q, t)$ where A is an $N \times k$ matrix of full rank and $N \leq k$. Let $A^{\perp}$ be a $k \times (k - N)$ matrix whose columns generate the nullspace of A. Suppose that $GA^{\perp}$ is an $OA(m, k - N, q, k - N)$. Then $G \boxplus \langle A \rangle$ is an array of type $I_k(m, q^N, q, t)$.*

In the case of strength $t = 2$, q a prime power and the number of rows and columns are also powers of q, we solve the existence problem completely as shown in the following result.

Theorem 1.6. *Let $2 \leq M \leq N$, let q be a prime power and let $k \geq 2$. Then there exists an array of type $I_k(q^M, q^N, q, 2)$ if and only if $k \leq M + N$, $k \leq (q^M - 1)/(q - 1)$ and $(k, M, q) \neq (3, 2, 2)$.*

Next, we explore binary designs of the form $I_k(m, n, 2, t)$. We provide some non-existence results in Lemma 5.22 and Corollary 5.43 that are combined in the following lemma.

Lemma 1.7. *The following designs do not exist:*

(i) *An array of type $I_3(4, 4b, 2, 2)$, where b is odd.*

(ii) *An array of type $I_4(8, 8, 2, 3)$ and $I_8(16, 16, 2, 3)$.*

The main results related to these designs are as follows:

Theorem 1.8. *If there exists a Hadamard matrix $H(4b)$, then there exists $I_{k+\alpha}(2^\alpha b, 2^k, 2, 2)$ for any $2 \leq \alpha$; $2^\alpha + \alpha + 1 \leq k < 2^\alpha b - \alpha$.*

The following result relies on the existence of a Hadamard matrix of order $4m$, where m is odd, containing two sets of non-trivial columns such that their sums are orthogonal.

Theorem 1.9. *Let m and b be odd. If there exists a Hadamard matrix of order $4m$, where m is odd, containing two sets of nontrivial columns such that their sums are orthogonal, then $I_k(4m, 2^a b, 2, 2)$ exists if and only if $(k, 4m, 2^a b, 2, 2)$ is admissible and*

$$(k, 4m, 2^a b, 2, 2) \notin \{(3, 4m, 4, 2, 2), (3, 4, 4m, 2, 2) \mid m \text{ is odd}\}.$$

ar

Theorem 1.10. *Let $m \leq 5$ and b odd. Then $I_k(4m, 2^a b, 2, 2)$ exists for all admissible*

$$(k, 4m, 2^a b, 2, 2) \notin \{(3, 4m, 4, 2, 2), (3, 4, 4m, 2, 2) \mid m \text{ is odd}\}.$$

We also completely classify binary row-column factorial designs of strength 3 when the dimensions of the array are powers of 2.

Theorem 1.11. *Let $M \leq N$. Then an array of type $I_k(2^M, 2^N, 2, 3)$ exists if and only if $3 \leq k \leq M + N$, $3 \leq M$, $k \leq 2^{M-1}$ and $(k, M, N) \notin \{(4, 3, 3), (8, 4, 4)\}$.*

Chapter 6 [8] is dedicated to frequency rectangles. Our main focus is on binary frequency rectangles, however, where possible we give results that are applicable to frequency rectangles with more than two symbols. We also utilize orthogonal arrays and Hadamard matrices to construct sets of MOFR as indicated in the following results.

Theorem 1.12. *Suppose there exists an* $\mathrm{OA}(mn, k, 2, 2)$. *Then there exist* k–$\mathrm{MOFR}(2m, 2n; 2)$.

Theorem 1.13. *Suppose there exists a Hadamard matrix $H(4a)$. Then there exists $(4a-2)$–MOFR$(4, 2a; 2)$.*

We also show that an OA$(2n, k, 2, 2)$ and a set of k frequency rectangle of type FR$(2, 2n; 2)$ are equivalent.

Lemma 1.14. *There exist k–MOFR$(2, 2n; 2)$ if and only if there exists an OA$(2n, k, 2, 2)$.*

We describe a new form of orthogonality for a set of frequency rectangles. We say that a set M of frequency rectangles of type FR$(m, n; q)$ is *t–orthogonal*, $t \geq 2$, if upon superimposition of any t elements in M, each of the possible q^t ordered t–tuples occurs the same number of times (mn/q^t) in the resulting array.

This type of orthogonality is stronger than the one described earlier, as a set of t–orthogonal frequency rectangles is also a mutually orthogonal set. The existence of an $I_k(m, n, q, t)$, $t \geq 1$ implies the existence of a set of k, k–orthogonal MOFR of type FR$(m, n; q)$.

A set of vectors is said to be *t–independent* if each subset of size t is independent. We also depict a relationship between a set of t–independent vectors and a set of t–orthogonal MOFR as shown in the following theorem.

Theorem 1.15. *Let S be a set of k t-independent vectors in $(\mathbb{F}_q)^{M+N}$ such that for each $\mathbf{v} = (v_1, \ldots, v_{M+N}) \in S$*

(i) $(v_1, \ldots, v_M) \neq (0, \ldots, 0)$,

(ii) $(v_{M+1}, \ldots, v_{M+N}) \neq (0, \ldots, 0)$,

*then there exists a t–orthogonal k–*MOFR$(q^M, q^N; q)$.

We include results from the literature which describe bounds on the size of a set of t–independent vectors over a finite field. By using these results and known bounds on linear codes, we formulate a table (Table 6.3) which includes the values for the size of the largest possible set of t–independent vectors in $(\mathbb{F}_2)^N$ for all $N \leq 16$ and $4 \leq t \leq N$.

At the end of Chapter 6, we describe a method to construct a set of $p-1$ binary MOFS of order $2p$, where p is an odd prime.

Theorem 1.16. *Let $p \geq 3$ be a prime. Then there exists a set of $p-1$ binary MOFS of order $2p$.*

This improves the previously known lower bounds for a set of binary MOFS of order $2p$ provided in [1] and [6] for all $p \geq 19$. It is also the first known lower bound linear in p.

Finally, in Chapter 7, we explore open problems and future work.

References

[1] T. Britz, N. J. Cavenagh, A. Mammoliti, and I. M. Wanless. Mutually orthogonal binary frequency squares. *The electronic journal of combinatorics*, 27(3), 2020.

[2] J. Godolphin. Construction of row–column factorial designs. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 81(2):335–360, 2019.

[3] A. Hedayat, D. Raghavarao, and E. Seiden. Further contributions to the theory of f-squares design. *The Annals of Statistics*, 3:712–716, 1975.

[4] K. Hinkelmann and O. Kempthorne. *Design and Analysis of Experiments, Volume 2: Advanced Experimental Design*. Wiley Series in Probability and Statistics. Wiley, 2005.

[5] C. Laywine and G. Mullen. *Discrete Mathematics Using Latin Squares*. 1484 Series. Wiley, 1998.

[6] M. Li, Y. Zhang, and B. Du. Some new results on mutually orthogonal frequency squares. *Discrete Mathematics*, 331:175–187, 2014.

[7] F. Rahim and N. J. Cavenagh. Row-column factorial designs with multiple levels. *Journal of Combinatorial Designs*, 29:750–764, 2021.

[8] F. Rahim and N. J. Cavenagh. Mutually orthogonal frequency rectangles. *arXiv preprint arXiv:2212.10706*, 2022.

[9] F. Rahim and N. J. Cavenagh. Row-column factorial designs with strength at least 2. *Linear Algebra and its Applications*, 667:44–70, 2023.

Chapter 2

Preliminaries and Literature Review

In this chapter, we give an introduction to the combinatorial structures that are closely related to the work done in this thesis. We also include a brief survey of relevant results in each case.

2.1 Latin Squares

The concept of a Latin square is not new in the field of combinatorics; its origins in the form of a magic square can be found in the Arab world as early as the ninth century A.D. (see, for example, [8]).

Definition 2.1. A *Latin square* L is an $n \times n$ array of n distinct symbols such that each symbol appears exactly once in each row and in each column. Let $[n] = \{0, 1, 2, 3, \ldots, n-1\}$. We take the symbol set to be $[n]$.

The study of Latin squares caught more attention of mathematicians in the late 18^{th} century when Euler posed the famous 36 officers problem [24]. The problem was to arrange 36 officers of 6 different ranks drawn from 6 different regiments in a square array such that each line (both vertical and horizontal) contains an officer from all six regiments and ranks.

Definition 2.2. Two Latin squares L_1 and L_2 of the same size are said to be

orthogonal if each ordered pair of symbols appears exactly once when L_1 is superimposed with L_2.

The 36 officers problem is then equivalent to the existence of two orthogonal Latin squares of order 6. Euler remained unsuccessful in obtaining such a pair for every $n \equiv 2 \pmod{n}$ and he conjectured that there does not exist a pair of orthogonal Latin squares for these n. In 1900, Tarry [24] verified that the conjecture is true when $n = 6$. Finally, in the late 1950s, by the combined efforts of Bose, Shrikhande and Parker, it was proved that Euler's conjecture is false for all other values of n. They exhibited a pair of orthogonal Latin squares of order 22 [4] and described a method to construct a pair for every $n \equiv 2 \pmod{n}$ and $n > 6$ [5]. However, it is still not known whether there exists a set of three Latin squares of order 10 which are orthogonal to each other (mutually orthogonal).

Definition 2.3. A set M of two or more Latin squares of order n is said to be a *mutually orthogonal set* if each pair of Latin squares in M is orthogonal. We usually call it a set of MOLS (mutually orthogonal Latin squares).

The following lemma shows the upper bound on the size of a set of MOLS.

Lemma 2.1. *Let k be the size of a set of MOLS of order n. Then $k \leq n - 1$.*

Proof. Let L_1, L_2 be two Latin squares of order n. Without loss of generality, we may assume that the entries in the first row of L_1, L_2 are in sequential order $(0, 1, 2, \ldots, n-1)$. Now consider the first two rows of L_1 and L_2:

$$L_1 = \boxed{\begin{array}{ccccc} 0 & 1 & 2 & \ldots & n-1 \\ \alpha & - & - & \ldots & - \end{array}} \qquad L_2 = \boxed{\begin{array}{ccccc} 0 & 1 & 2 & \ldots & n-1 \\ x & - & - & \ldots & - \end{array}}$$

Observe that if L_2 is orthogonal to L_1, then $x \notin \{0, \alpha\}$. Thus there are $n-2$ choices for x and hence there are only $n-2$ possible Latin squares that can be orthogonal to L_1. This completes the proof. □

A set of $n-1$ MOLS of order n is said to be *complete*. A complete set of MOLS can be constructed using finite fields whenever n is a prime power.

Example 2.2. A complete set of mutually orthogonal Latin squares of order 5.

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

Table 2.1: 4 MOLS of order 5.

The method of constructing complete sets of MOLS when n is a prime power is described in the next section for more general structures called frequency squares. Whether there exists a complete set of MOLS for non-prime powers is one of the most well-known open questions in the area.

2.2 Frequency Squares

A frequency square is a generalization of a Latin square in which symbols are allowed to appear more than once in each row and in each column. Formally,

Definition 2.4. A *frequency square* of type $\mathrm{F}(n;q)$ is an $n \times n$ array of q symbols such that each symbol appears exactly n/q times in each row and in each column.

The orthogonality between a pair of frequency squares is defined as follows.

Definition 2.5. Two frequency squares F_1 and F_2 of the same type $\mathrm{F}(n;q)$ are said to be *orthogonal* if each ordered pair of symbols appear the same number of times when F_1 and F_2 are superimposed.

Example 2.3. Two orthogonal frequency squares of type $\mathrm{F}(6;3)$:

0	0	1	1	2	2
0	1	2	0	1	2
1	2	0	2	0	1
1	0	2	0	2	1
2	1	0	2	1	0
2	2	1	1	0	0

F_1

1	1	0	0	2	2
0	1	2	1	2	0
2	0	2	1	0	1
0	2	1	2	1	0
2	2	0	0	1	1
1	0	1	2	0	2

F_2

Table 2.2: Two MOFS of type F$(6;3)$

Observe that when F_1 and F_2 are superimposed, each of the 3^2 possible ordered pair of symbols appears exactly 4 times in the resultant array:

01	01	10	10	22	22
00	11	22	01	12	20
12	20	02	21	00	11
10	02	21	02	21	10
22	12	00	20	11	01
21	20	11	12	00	02

Table 2.3: F_1 and F_2 superimposed.

We would like to mention here that in the literature a frequency square of type F$(n;q)$ is often represented by F$(n;\lambda)$ where $\lambda = n/q$ is the frequency of each symbol in each row and in each column. However, we stick to the notation F$(n;q)$ where q is the size of the symbol set to remain consistent with the notations used in this thesis. Also, a frequency square in its most generalized form can have a different frequency for distinct symbols (see [19] and [10]).

In [18] Hedayat et. al. give an upper bound for the number of MOFS of type F$(n;q)$ in the form of the following theorem:

Theorem 2.4. *The maximal number, k, of orthogonal frequency squares of*

type $\mathrm{F}(n;q)$*, where* $n = \lambda q$*, satisfies the inequality*

$$k \leq (n-1)^2/(q-1). \tag{2.1}$$

Proof. The following proof is based on [18]. Let $F_1, F_2, \ldots, F_k$ be a set of k mutually orthogonal frequency squares of type $\mathrm{F}(n;q)$. Corresponding to each F_α we define an $n^2 \times q$ matrix $H_\alpha = (h_{(ij),\theta})$, where $i = 1, 2, \ldots, n; j = 1, 2, \ldots, n$, θ runs over the symbols set, and

$$h_{(ij),\theta} = \begin{cases} 1 & \textit{if the symbol } \theta \textit{ occurs in the } (i,j)^{th} \textit{ cell of } F_\alpha. \\ 0 & \textit{otherwise.} \end{cases}$$

Let

$$M = (H_1 \mid H_2 \mid \cdots \mid H_k).$$

Since each position in the frequency square corresponds to a row of M and each row of F_α contains each symbol exactly λ times, the n rows of M that correspond to a fixed row (or a fixed column) of the frequency square contain the entry 1 exactly at λ places in each column.

Thus, if we add a set of rows that correspond to the i^{th} row of frequency squares we obtain a row with each entry equal to λ. And since we can make n such distinct sets, there are $n-1$ dependent rows in M. Similarly, by taking the set of rows corresponding to the columns of frequency squares, we get another $n-1$ dependent rows in M.

Consequently, there are at least $2(n-1)$ dependent rows in M, or, the number of independent rows in M is at most $n^2 - 2(n-1) = (n-1)^2 + 1$.

This implies

$$\mathrm{Rank}(M) \leq \min\{(n-1)^2 + 1, kq\},$$

where $\mathrm{Rank}(M)$ denotes the rank of M.

Now consider the product $H_r^T H_s$. First suppose that $r = s$ and consider a diagonal entry at position (i,i) of $H_r^T H_r$. The i^{th} row of H_r^T (and so the

i^{th} column of H_r) has an entry 1 exactly at $n\lambda$ places corresponding to the appearances of i^{th} symbol in F_r. Thus all the diagonal entries in $H_r^T H_s$ are $n\lambda$. Since the two distinct symbols cannot occupy the same position in F_r, the product of i^{th} row of H_r^T and j^{th} column of H_s for $i \neq j$ is zero. Consequently, we have $H_r^T H_s = n\lambda I_q$, where I_q is an identity matrix of order q.

In the case when $r \neq s$, the orthogonality of F_r and F_s implies that each pair of symbols coincides at exactly λ^2 places. Hence $H_r^T H_s = \lambda^2 J_q$, where J_q is a square matrix of order q having entry 1 at all places. Therefore, we obtain:

$$M^T M = \begin{pmatrix} n\lambda I_q & \lambda^2 J_q & \dots & \lambda^2 J_q \\ \lambda^2 J_q & n\lambda I_q & \dots & \lambda^2 J_q \\ \vdots & \vdots & \ddots & \vdots \\ \lambda^2 J_q & \lambda^2 J_q & \dots & n\lambda I_q \end{pmatrix}.$$

The eigenvalues of the above matrix, $M^T M$, are $n\lambda k, n\lambda$ and 0 with multiplicities $1, k(q-1)$ and $k-1$ respectively (see Theorem 6.1 in Section 6.2 and Appendix 6.7 for detailed elaboration). Since the sum of multiplicities of non-zero eigenvalues gives the rank of $M^T M$,

$$kq - k + 1 = \text{Rank}(M^T M) = \text{Rank}(M) \leq \min\{(n-1)^2 + 1, kq\},$$

which gives the required result. □

Note that if we take $q = n$ in the inequality (2.1) we get the upper bound $k \leq n - 1$ in Lemma 2.1 for a set of mutually orthogonal Latin squares.

Definition 2.6. A set of $(n-1)^2/(q-1)$ frequency squares of type $\text{F}(n; q)$ is said to be *complete*.

It has been shown that the complete set of frequency squares exists for all prime power orders and there are several methods to construct such a set using: factorial designs [18], finite fields [35], affine resolvable designs [28], complete sets of MOLS [26]. Later Mavron [34] showed that almost all of these methods can be derived from a single method.

We include here a method given in Theorem 4.2, in [27, p. 65] which uses finite fields to construct a complete set of MOFS of type $\mathrm{F}(q^r; q)$. We generalize this idea in Theorem 6.12 to construct sets of frequency rectangles. Before stating the theorem we give a lemma that helps in the proof.

Lemma 2.5. *Let q be a prime power and $r \geq 1$. Then there exists a set M of $(q^r-1)^2/(q-1)$ vectors in $(\mathbb{F}_q)^{2r}$ such that:*

(i) *Any two elements in M are linearly independent and*

(ii) *For each $\mathbf{a} = (a_1, \ldots, a_{2r}) \in M$,*

(a) $(a_1, \ldots, a_r) \neq (0, \ldots, 0)$.

(b) $(a_{r+1}, \ldots, a_{2r}) \neq (0, \ldots, 0)$.

Proof. Let $\mathbf{u} = (a_1, \ldots, a_r)$ and $\mathbf{w} = (a_{r+1}, \ldots, a_{2r})$. Observe that there are exactly $2q^r - 1$ vectors $\mathbf{a}$ in $(\mathbb{F}_q)^{2r}$ in which either $\mathbf{u} = \mathbf{0}$ or $\mathbf{w} = \mathbf{0}$. This implies there are $q^{2r} - 2q^r + 1 = (q^r-1)^2$ vectors which have $\mathbf{u} \neq \mathbf{0}$ and $\mathbf{w} \neq \mathbf{0}$. Let H be the set containing these vectors. For each $\mathbf{a} \in H$, there are at most $q-1$ vectors in H that are scalar multiple of $\mathbf{a}$, this shows that there are at least $(q^r-1)^2/(q-1)$ vectors in H such that every pair is linearly independent.

□

Theorem 2.6. [27] *There exists a complete set of MOFS of type $\mathrm{F}(q^r; q)$, where q is a prime power and $r \geq 1$.*

Proof. Let M be the set of vectors described in Lemma 2.5. Corresponding to each $\mathbf{a} = (a_1, \ldots, a_{2r}) \in M$ we define a polynomial $f_{\mathbf{a}}$:

$$f_{\mathbf{a}}(x_1, \ldots, x_{2r}) = a_1 x_1 + \cdots + a_{2r} x_{2r}.$$

By using the polynomial $f_{\mathbf{a}}$ we construct a $q^r \times q^r$ array as follows. Label the rows and columns of the array by using the set of all r-tuples over the field $\mathbb{F}_q$. We place the element $f_{\mathbf{a}}(b_1, \ldots, b_r, c_1, \ldots, c_r)$ in the intersection of row $(b_1, \ldots, b_r)$ and column $(c_1, \ldots, c_r)$ of the $q^r \times q^r$ array.

Now we show that the array obtained in this way is a frequency square of type $\mathrm{F}(q^r; q)$, that is every element of $\mathbb{F}_q$ appears exactly q^{r-1} times in each row and in each column. Consider a row which is labelled by $(b_1, \ldots, b_r)$ and take an element $\alpha \in \mathbb{F}_q$. For this row the equation

$$f_{\mathbf{a}}(b_1, \ldots, b_r, x_{r+1}, \ldots, x_{2r}) = \alpha$$

reduces to the equation

$$K + a_{r+1}x_{r+1} + \cdots + a_{2r}x_{2r} = \alpha \tag{2.2}$$

where K is a constant. Now by of Lemma 2.5(ii)(b), there is at least one $a_i \neq 0$, for some $r+1 \leq i \leq 2r$. We solve the equation (2.2) for that x_i,

$$x_i = \frac{1}{a_i}(\alpha - K - a_{r+1}x_{r+1} - \cdots - a_{i-1}x_{i-1} - a_{i+1}x_{i+1} - \cdots - a_{2r}x_{2r}). \tag{2.3}$$

Since there are q elements in $\mathbb{F}_q$ and the $r-1$ variables on the right side of equation (2.3) can take any value from $\mathbb{F}_q$, the equation (2.3) has exactly q^{r-1} solutions in $\mathbb{F}_q$. This implies that the symbol α appears exactly at q^{r-1} places in the row $(b_1, \ldots, b_r)$. By a similar argument, we can prove that each symbol appears exactly q^{r-1} times in each column. Thus the resulting array is a frequency square of type $\mathrm{F}(q^r; q)$.

Now we show that the two frequency squares defined by two polynomials $f_{\mathbf{a}}$ and $f_{\mathbf{a}'}$, where $\mathbf{a}, \mathbf{a}' \in M$ are orthogonal. Let α, β be any two arbitrary elements of $\mathbb{F}_q$. By condition (i) in Lemma 2.5, the system of equations

$$\begin{aligned} f_{\mathbf{a}} &= a_1x_1 + \cdots + a_{2r}x_{2r} = \alpha \\ f_{\mathbf{a}'} &= a'_1x_1 + \cdots + a'_{2r}x_{2r} = \beta \end{aligned} \tag{2.4}$$

has rank two and, hence, has exactly $q^{2r-2} = q^{r-1}q^{r-1}$ solutions in $\mathbb{F}_q$. Thus, the pair of symbols $\alpha\beta$ appears exactly $(q^{r-1})^2$ times when the two frequency squares are superimposed. □

Next, we give an example to elaborate a little further on the method given in Theorem 2.6.

Example 2.7. Suppose we want to construct a complete set of MOFS of type $\mathrm{F}(4;2)$. In this case $q = 2$ and $r = 2$, so we take the field $\mathbb{F}_2$. Now consider a polynomial

$$f(x_1, \ldots, x_4) = x_1 + x_2 + x_4 \tag{2.5}$$

over the field $\mathbb{F}_2$, where we have chosen $a_1 = 1, a_2 = 1, a_3 = 0$ and $a_4 = 1$. It is easy to see that this polynomial satisfies the conditions in Lemma 2.5. Label the rows and columns of 4×4 array using all the ordered pairs over $\mathbb{F}_2$:

	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$				
$(0,1)$			1	
$(1,0)$				
$(1,1)$				

Entry 1 in the highlighted cell is obtained by substituting its row and column labels in polynomial f, that is $f(0,1,1,0) = 0 + 1 + 0 = 1$. Similarly, we can obtain all the other entries of the 4×4 array.

A complete set of MOFS of type $\mathrm{F}(4;2)$ together with their representative polynomials is given below:

$x_1 + x_3$			
0	0	1	1
0	0	1	1
1	1	0	0
1	1	0	0

$x_1 + x_4$			
0	1	0	1
0	1	0	1
1	0	1	0
1	0	1	0

$x_2 + x_3$			
0	0	1	1
1	1	0	0
0	0	1	1
1	1	0	0

$x_2 + x_4$			
0	1	0	1
1	0	1	0
0	1	0	1
1	0	1	0

$x_1 + x_2 + x_3$			
0	0	1	1
1	1	0	0
1	1	0	0
0	0	1	1

$x_1 + x_2 + x_4$			
0	1	0	1
1	0	1	0
1	0	1	0
0	1	0	1

$x_1 + x_3 + x_4$			
0	1	1	0
0	1	1	0
1	0	0	1
1	0	0	1

$x_2 + x_3 + x_4$			
0	1	1	0
1	0	0	1
0	1	1	0
1	0	0	1

$x_1 + x_2 + x_3 + x_4$			
0	1	1	0
1	0	0	1
1	0	0	1
0	1	1	0

Table 2.4: A complete set of MOFS of type $\mathrm{F}(4;2)$.

A complete set of MOFS can exist for non-prime powers, for example, in [20] a method is given to construct complete sets of MOFS of type $\mathrm{F}(4t;2t)$ using a Hadamard matrix. A table was formulated by Laywine and Mullen [29], which gives the lower bounds (number of constructed MOFS) for different values of n and λ. The table was improved by Li et. al in 2014 [30]. Recently, in [6], the authors have shown that there exist at least 17 binary MOFS of type $\mathrm{F}(n;2)$, where $n \equiv 2 \pmod 4$. They have also proved that a complete set does not exist for these parameters. In Section 6.5, we show that a set of $p-1$ binary MOFS of order $2p$ exists whenever p is an odd prime. Thus improving the lower bound for all cases when $p \geq 19$.

2.3 Frequency Rectangles

A frequency rectangle is a further generalization of a frequency square in which the number of columns and the number of rows are allowed to have different values. Formally:

Definition 2.7. A *frequency rectangle* (also called *F-rectangle*) of type FR$(m, n; q)$ is an $m \times n$ array based on a symbol set S of size q, such that each element of S appears exactly n/q times in each row and m/q times in each column.

The orthogonality between a pair of frequency rectangles is defined as follows.

Definition 2.8. Two frequency rectangles, F_1 and F_2, of the same type, are said to be *orthogonal* if each possible ordered pair of symbols appear the same number of times when F_1 and F_2 are superimposed. A set of k frequency rectangles in which every pair is orthogonal is called a set of *mutually orthogonal frequency rectangles*, denoted by k–MOFR$(m, n; q)$.

An upper bound,

$$k \leq \frac{(m-1)(n-1)}{(q-1)}. \tag{2.6}$$

for k–MOFR$(m, n; q)$ can be derived from a more general result proved in [33]. However, we have given an independent proof similar to Theorem 2.4 (see Theorem 6.1).

Definition 2.9. A k–MOFR$(m, n; q)$ or k–MOFS$(n; q)$ is said to be *complete* if k reaches the upper bound given in (2.6).

Complete sets of MOFR of type FR$(q^M, q^N; q)$ are known to exist when q is a prime power [14]. For q a prime power, Mandeli [32] describes a method to construct a complete set of MOFR$(q^M, 2q^N, q)$. For $m = 4a$ and $n = 4b$, Cheng [9] showed the existence of a complete set of MOFR$(m, n; 2)$ provided that Hadamard matrices of order $4a$ and $4b$ exist. Also, assuming the existence

of a Hadamard matrix of order $4b$, Federer, Hedayat, and Mandeli [14] describe a method to construct a complete set of MOFR$(2, 4b; 2)$.

We introduce a stronger form of orthogonality called t–orthogonality for a set of frequency rectangles.

Definition 2.10. A set M of frequency rectangles of type FR$(m, n; q)$ is said to be *t–orthogonal*, $t \geq 2$, if upon superimposition of any t elements in M, each of the possible q^t ordered t–tuples occurs the same number of times in the resulting array.

In Section 6.2, a set of 3–orthogonal 6–MOFR$(4, 4; 2)$ is provided in Example 6.2 as an illustration.

Observe that by definition a t–orthogonal ($t \geq 2$) set of frequency rectangles is also a mutually orthogonal set. Further results and the connection of t–orthogonal frequency rectangles with the set of independent vectors over finite fields are discussed in Section 6.4.

2.4 Hadamard Matrices

In [17] Hadamard showed that for a square matrix $A = (a_{ij})$ of order n with complex entries on the unit disc $|a_{ij}| \leq 1$, the determinant of the matrix satisfies the inequality:

$$|\det A| \leq n^{n/2}. \tag{2.7}$$

However, the name Hadamard matrix is used to refer to real matrices that satisfy the equality in relation (2.7), formally:

Definition 2.11. A *Hadamard matrix* H_n is a square matrix of order n, having entries from the set $\{1, -1\}$ such that any two rows are orthogonal; that is it satisfies the equation:

$$H_n H_n^T = nI_n. \tag{2.8}$$

Example 2.8. Below are Hadamard matrices of orders 1, 2, and 4.

$$H_1 = \begin{bmatrix} 1 \end{bmatrix}, \quad H_2 = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}, \quad H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix}$$

By equation (2.8) it is easy to see that the columns of a Hadamard matrix are also orthogonal. Observe that if H_n is a Hadamard matrix then the matrix obtained by permuting its rows (or columns) and negating any rows (or columns) will also be a Hadamard matrix; we say that this matrix is *equivalent* to H_n. Using such transformations we can always transform H_n to an equivalent matrix with all the entries in the first row and first column equal to "+1". Such a matrix is called a *normalized Hadamard matrix*. In Example 2.8, H_1 and H_4 are normalized Hadamard matrices.

For a normalized Hadamard matrix H_n, where $n > 2$, the following lemma is not difficult to prove.

Lemma 2.9. *Let $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ be two distinct rows, other than the first, of a normalized Hadamard matrix of order n, $n > 2$. Then*

(i) *half of the entries a_i are $+1's$ and half of them are $-1's$.*

(ii) *the multiset $\{(a_i, b_i) : i = 1, 2, \ldots, n\}$ contains each type of ordered pair exactly $n/4$ times.*

(iii) *the conditions (i) and (ii) are also true for the columns of a normalized Hadamard matrix.*

From the above lemma, we have the following result.

Corollary 2.10. *If there exists a Hadamard matrix H_n of order n then $n = 1, 2$ or $n \equiv 0 \pmod 4$.*

Once we have a Hadamard matrix we can use it to construct Hadamard matrices of larger sizes.

Definition 2.12. Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be two matrices of sizes $m \times n$ and $u \times v$, respectively. The *Kronecker product*, $A \otimes B$, of A and B is an $mu \times nv$ matrix defined by:

$$A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{pmatrix} \tag{2.9}$$

Now we state the result in the following theorem.

Theorem 2.11. *If H_m and H_n are two Hadamard matrices of order m and n respectively, then their Kronecker product is a Hadamard matrix H_{mn} of order mn.*

Thus if there exists a Hadamard matrix of order l we can construct Hadamard matrices of order $2l, 4l, 8l, \dots$, so on by using the Hadamard matrix of order 2.

Example 2.12. By taking the Kronecker product of H_2 and H_4 in Example 2.8 we get the following Hadamard matrix of order 8:

$$H_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \end{bmatrix}$$

The following result is due to [2, 12] and is more general than taking the Kronecker product.

Theorem 2.13 ([2, 12])**.** *If there exist Hadamard matrices of order $4l, 4m, 4n$ and $4q$ then there exist Hadamard matrices of order $8mn$ and $16lmnq$.*

There exist several other methods to construct Hadamard matrices that work for specific orders. For example: Payley constructions that use Galois fields can be used to construct H_n where either $n-1$ is a prime power or $n = 2(s+1)$ and $s \equiv 1 \pmod 4$ is a prime power [36]; the John Williamson construction which uses a 4×4 array of circulant matrices [38]; and the Goethals and Seidel method ([15], [31]). Arguably the most famous unsolved conjecture on Hadamard matrices is the following.

Conjecture 2.14. *There exists a Hadamard matrix of order* $4r$*, whenever* r *is a positive integer.*

Before 2005, Hadamard matrices of all orders less than 1000 were found except the orders; 428, 668, 716, 764 and 892 [13]. In 2005, Kharaghani et. al were able to construct some new Hadamard matrices by using T-sequences (see [25]); among these, there was a matrix of order 428. Two years later Djokovic [13] constructed a Hadamard matrix of order 764 by using a technique called symmetric difference sets. Currently the only remaining admissible orders less than 1000 for which it is not known whether a Hadamard matrix exists or not are 668, 716, and 892.

2.5 Generalisations of Hadamard Matrices

There are several ways to generalise Hadamard matrices depending upon the contextual aim; whether this lies in obtaining maximal determinants or in retaining the balancing properties between the rows and columns of the Hadamard matrices. In this section, we are only interested in the latter case and shall introduce two of the most relevant generalisations in this channel. The first one allows the matrices to be rectangular with the balancing properties in rows and are called *partial Hadamard matrices* or *Hadamard rectangles*. We utilize partial Hadamard matrices in Chapter 6 to construct set of MOFR. Formally:

Definition 2.13. An $m \times n$ matrix H having entries from the set $\{1, -1\}$ is called a partial Hadamard matrix if every two rows of H are orthogonal, equivalently if H satisfies the following relation:

$$HH^T = nI_m$$

We shall denote the partial Hadamard matrix of order $m \times n$ by $H(m, n)$. Similar operations (as in the case of Hadamard matrices) can be performed on a partial Hadamard matrix $H(m, n)$ to obtain an equivalent *normalized partial*

Hadamard matrix having all the entries in the first row and the first column to be 1.

It is easy to observe that if an $H(m,n)$ exists then so does $H(h,n)$ for all $h < m$. Some of the natural questions related to the existence of $H(m,n)$ are: "For a particular value of n what is the maximum value of m?" and "For a particular m, what could be the values of n?". For smaller values of m the following lemma answers these questions. Here $\mathbf{e}_t$ denotes a row of t 1's.

Lemma 2.15. [11] *Let H be an $H(m,n)$. Then*

(i) $m \leq n$;

(ii) $H(1,n)$ *is equivalent to* $\boldsymbol{e}_n$;

(iii) *if $m = 2$ then n is even and H is equivalent to* $\begin{bmatrix} \mathbf{e}_{\frac{n}{2}} & \mathbf{e}_{\frac{n}{2}} \\ \mathbf{e}_{\frac{n}{2}} & -\mathbf{e}_{\frac{n}{2}} \end{bmatrix}$;

(iv) *if $m > 2$ then n is a multiple of 4 and any three rows of H are equivalent to*

$$\begin{bmatrix} \mathbf{e}_{\frac{n}{4}} & \mathbf{e}_{\frac{n}{4}} & \mathbf{e}_{\frac{n}{4}} & \mathbf{e}_{\frac{n}{4}} \\ \mathbf{e}_{\frac{n}{4}} & \mathbf{e}_{\frac{n}{4}} & -\mathbf{e}_{\frac{n}{4}} & -\mathbf{e}_{\frac{n}{4}} \\ \mathbf{e}_{\frac{n}{4}} & -\mathbf{e}_{\frac{n}{4}} & -\mathbf{e}_{\frac{n}{4}} & \mathbf{e}_{\frac{n}{4}} \end{bmatrix};$$

(v) *if $m = 4$ then H is equivalent to a $H(4,n)$ of the form*

$$\begin{bmatrix} \mathbf{e}_{\frac{n}{4}} & \mathbf{e}_{\frac{n}{4}} & \mathbf{e}_{\frac{n}{4}} & \mathbf{e}_{\frac{n}{4}} \\ \mathbf{e}_{\frac{n}{4}} & \mathbf{e}_{\frac{n}{4}} & -\mathbf{e}_{\frac{n}{4}} & -\mathbf{e}_{\frac{n}{4}} \\ \mathbf{e}_{\frac{n}{4}} & -\mathbf{e}_{\frac{n}{4}} & -\mathbf{e}_{\frac{n}{4}} & \mathbf{e}_{\frac{n}{4}} \\ \mathbf{a} & -\mathbf{a} & \mathbf{a} & -\mathbf{a} \end{bmatrix}, \tag{2.10}$$

where $\mathbf{a}$ is a row of ± 1's of length $\frac{n}{4}$;

(vi) *if H is normalized, then all row sums of H except the first are 0.*

(vii) *if c_i represents the column sum of the ith column of H, then $\sum_{i=1}^{n} c_i^2 = mn$.*

(viii) *if $m \geq 5$ and H contains* (2.10) *as a submatrix, with $\mathbf{a} = \mathbf{e}_{\frac{n}{4}}$, then $n \equiv 0 \pmod 8$.*

It is clear that if the Hadamard conjecture is true then the existence problem of partial Hadamard matrices is completely solved. However, there is a type of partial Hadamard matrix, called a maximal partial Hadamard matrix, which cannot be extended to a Hadamard matrix. Formally, a partial Hadamard matrix $H(m,n)$ is said to be *maximal* if it is not a submatrix of any $H(m+1,n)$. For example, the matrix $H(5,12)$ given below is a maximal partial Hadamard matrix [11].

$$H(5,12) = \begin{bmatrix} + & + & + & + & + & + & + & + & + & + & + & + \\ + & + & + & + & + & + & - & - & - & - & - & - \\ + & + & + & - & - & - & + & + & + & - & - & - \\ + & + & - & + & - & - & + & + & - & + & - & - \\ + & + & - & + & - & - & - & - & + & - & + & + \end{bmatrix}.$$

Here "+" represents 1 and "−" represents a -1.

Similarly, by Lemma 2.15(viii) any matrix of the form:

$$\begin{bmatrix} \mathbf{e}_s & \mathbf{e}_s & \mathbf{e}_s & \mathbf{e}_s \\ \mathbf{e}_s & \mathbf{e}_s & -\mathbf{e}_s & -\mathbf{e}_s \\ \mathbf{e}_s & -\mathbf{e}_s & -\mathbf{e}_s & \mathbf{e}_s \\ \mathbf{e}_s & -\mathbf{e}_s & \mathbf{e}_s & -\mathbf{e}_s \end{bmatrix},$$

with s odd is also maximal.

Another important generalisation of Hadamard matrices is square matrices having entries from a finite group; these are known as generalised Hadamard matrices. Although we don't directly make use of these in this thesis, we have included a brief introduction here as they could be useful in extending the work in future (see Chapter 7).

Definition 2.14. Let $(N,*)$ be a finite group of order w. A square matrix $H = [h_{ij}]$ of order v having entries from N is called a *generalised Hadamard matrix* if, for all $i \neq j$, the multi-set $\{h_{ik} * h_{jk}^{-1} : 1 \leq k \leq v\}$ contains each element of N exactly λ times.

Necessarily, w divides v and $\lambda = v/w$. We denote such a matrix by $GH(w,\lambda)$. A $GH(w,\lambda)$ with the first row and the first column consisting entirely of the identity element of the group N is called a *normalised* $GH(w,\lambda)$.

Example 2.16. [21] The first matrix below is a normalised $GH(4,1)$ with $N = \mathbb{Z}_2 \times \mathbb{Z}_2$ and the second is a normalised $GH(3,2)$ over the group $N = \mathbb{Z}_3$.

$$\begin{bmatrix} 00 & 00 & 00 & 00 \\ 00 & 01 & 10 & 11 \\ 00 & 10 & 11 & 01 \\ 00 & 11 & 01 & 10 \end{bmatrix} \qquad \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 1 & 0 & 2 & 2 & 1 \\ 0 & 2 & 1 & 2 & 1 & 0 \\ 0 & 2 & 2 & 1 & 0 & 1 \end{bmatrix}.$$

Following are some common examples and constructions of generalised Hadamard matrices, the details of which can be found in [21].

1. Let $\mathbb{F}_q$ be a finite field, then the multiplication table of $\mathbb{F}_q$ is a $GH(q,1)$ with $N = (\mathbb{F}_q, +)$.

2. If $H = [h_{ij}]$ is a $GH(w,\lambda)$ then the matrix obtained by replacing each entry h_{ij} with its inverse h_{ij}^{-1} is also a $GH(w,\lambda)$.

3. If H is a $GH(w,\lambda)$ and H' is a $GH(w,\lambda')$ over the same group N then their tensor product $H \otimes H'$is a $GH(w,\lambda\lambda' w)$ over N.

4. If N is abelian then the transpose of a $GH(w,\lambda)$ is also a $GH(w,\lambda)$.

Part (4.) was first given in [23] and was corrected in [7].

2.6 Orthogonal Arrays

This section briefly introduces orthogonal arrays and some elementary results related to their existence. We also discuss their relation with Hadamard matrices. For a detailed overview, we refer the reader to [20].

Definition 2.15. An *orthogonal array* $\mathrm{OA}(n,k,q,t)$ is an array of size $n \times k$, having entries from a set S of size q such that every $n \times t$ subarray contains each $t-$tuple based on S (that is, every element of S^t) exactly λ times as a row.

Trivially t satisfies the condition $0 \leq t \leq k$ and is called the *strength* of the orthogonal array. The parameter λ is known as the *index* of the array and by definition satisfies the following relation:

$$n = \lambda q^t \tag{2.11}$$

As previously we take the symbol set S to be $[q]$.

Example 2.17. Here are examples of orthogonal arrays of strength 2 and 3, based on symbol sets $\{0, 1, 2\}$ and $\{0, 1\}$, respectively.

0	0	0	0
0	1	1	2
1	0	1	1
0	2	2	1
2	0	2	2
1	1	2	0
1	2	0	2
2	1	0	1
2	2	1	0

Table 2.5: OA$(9, 4, 3, 2)$

0	0	0	0
0	0	1	1
0	1	0	1
1	0	0	1
0	1	1	0
1	0	1	0
1	1	0	0
1	1	1	1

Table 2.6: OA$(8, 4, 2, 3)$

Example 2.18. Any $n \times k$ array is an orthogonal array of strength zero. Arrays of strength 1 for any value of k are trivial to construct.

0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1
2	2	2	2	2	2	2	2	2
3	3	3	3	3	3	3	3	3

Table 2.7: OA$(4, 9, 4, 1)$

Remark 1. By the definition of an orthogonal array, the following observations are immediate.

(i) Any orthogonal array of type OA(n, k, q, t) of strength t is an array of type OA(n, k, q, t') for any t' satisfying $0 \leq t' \leq t$.

(ii) Any permutation of rows, columns or symbols will not affect the type of an orthogonal array.

(iii) Let A_i be an orthogonal array of type $\mathrm{OA}(n_i, k, q, t_i)$ for each $i = 1, 2, \ldots, r$, then the array A,

$$A = \begin{pmatrix} A_1 \\ \vdots \\ A_r \end{pmatrix},$$

obtained by the juxtaposition of these arrays, is an orthogonal array of type $\mathrm{OA}(N, k, q, t)$, where $N = n_1 + \cdots + n_r$ for some $t \geq \min\{t_1, \ldots, t_r\}$.

Generally, the larger the value of t the harder it is to construct an orthogonal array. One of the important problems related to orthogonal arrays is to determine the maximal value of k for fixed values of n, q, and t for which an $\mathrm{OA}(n, k, q, t)$ exists. The first-ever bounds on these parameters were obtained by Rao [37] in the form of implicit relations known as *Rao's inequalities*.

Theorem 2.19. *If an* $\mathrm{OA}(n, k, q, t)$ *exists then the following inequalities must be satisfied:*

$$n \quad \geq \quad \sum_{i=0}^{s} \binom{k}{i} (q-1)^i, \quad if \quad t = 2s, \tag{2.12}$$

$$n \quad \geq \quad \sum_{i=0}^{s} \binom{k}{i} (q-1)^i + \binom{k-1}{s} (q-1)^{s+1}, \quad if \quad t = 2s+1, \tag{2.13}$$

for $s \geq 0$.

The above inequalities in the case of strengths 2 and 3 give the following bounds.

Corollary 2.20. *An* $\mathrm{OA}(n, k, q, 2)$ *satisfies the following inequality:*

$$k \leq \frac{n-1}{q-1}. \tag{2.14}$$

Corollary 2.21. *An* $\mathrm{OA}(n, k, q, 3)$ *satisfies the following inequality:*

$$k \leq \frac{n/q - 1}{q-1} + 1. \tag{2.15}$$

These relations imply that the parameters of the orthogonal arrays given in Example 2.17 have maximal values for k. Orthogonal arrays which reach the above bounds for their parameters are called *tight*.

There are various construction methods that are useful to construct orthogonal arrays with some specific set of parameters. The following theorem is due to the Addelman and Kempthorne [1].

Theorem 2.22. *If q is an odd prime power then an* $\mathrm{OA}(2q^N, 2(q^N-1)/(s-1)-1, q, 2)$ *exists for all $N \geq 2$.*

Another important construction that uses Galois fields to construct orthogonal arrays of strength two is sometimes called the Rao-Hamming construction.

Theorem 2.23. [20, p. 49] *For q a prime power there exists an* $\mathrm{OA}(q^N, (q^N-1)/(q-1), q, 2)$ *whenever $N \geq 2$.*

Hadamard matrices are also useful for constructing orthogonal arrays when n is a multiple of four, as shown in the following theorem.

Theorem 2.24. [20] *A Hadamard matrix of order 4λ exists if and only if there exist orthogonal arrays* $\mathrm{OA}(4\lambda, 4\lambda-1, 2, 2)$ *and* $\mathrm{OA}(8\lambda, 4\lambda, 2, 3)$.

The existence of a row-column factorial design $I_k(m, n, q, t)$ implies the existence of orthogonal arrays $\mathrm{OA}(m, k, q, t)$ and $\mathrm{OA}(n, k, q, t)$. Therefore, any bound on an orthogonal array signifies a bound on the existence of factorial designs. In Chapter 5, we use orthogonal arrays of strength 2 to construct abelian row-column factorial designs of strength 2. Also, some of the bounds on the parameter k are ascribed to orthogonal arrays. In Chapter 6, we use orthogonal arrays to construct sets of mutually orthogonal frequency rectangles.

2.7 Linear Codes

In this section, we discuss the connection between coding theory and the results that are useful to construct maximal sets of t-independent vectors. Although our major focus is linear codes we give here some general definitions and terminologies related to the codes. The definitions and notations used here are consistent with the notations used in [20].

Definition 2.16. A code C of length n over a symbol set (or alphabet) S is any subset of the set S^n. The elements or vectors in C are called *codewords*. The *hamming weight* $w(\mathbf{u})$ of a codeword $\mathbf{u} = (u_1, \ldots, u_n)$ is the number of non-zero components u_i. The *hamming distance* $d(\mathbf{u}, \mathbf{v})$ between two codewords $\mathbf{u}$ and $\mathbf{v}$ is the number of components at which they contain different symbols. The *minimum distance* d of a code C is defined to be the smallest hamming distance between two distinct codewords in C, i.e.,

$$d = \min\{d(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}\}.$$

If a code C has no codeword then we say that the minimum distance d is undefined and if the code has only one codeword of length n then d is defined to be $n + 1$.

If a code C has M codewords of length n, over a symbol set of size s, and a minimum distance d, then we refer it to as an $(n, M, d)_s$ code.

Example 2.25. Consider $C = \{00000, 11111, 10101, 10010\}$. This is a $(5, 4, 2)_2$ code.

Definition 2.17. If the symbol set of a code is the finite field $\mathbb{F}_q$ of order q, and C is a k-dimensional subspace of the vector space $(\mathbb{F}_q)^n$ then C is called a *linear code* of dimension k and length n. We call a linear code with minimum distance d an $[n, k, d]$ q-ary code.

Thus an $[n, k, d]$ q-ary code is also an $(n, q^k, d)_q$ code. We reserve the former notation only for a linear code. In the case of a linear code, the minimum

distance d is the minimum weight among all the nonzero vectors in C, i.e.,

$$d = \min_{\substack{\mathbf{u}\in C \\ \mathbf{u}\neq 0}} w(\mathbf{u})$$

A linear code can be concisely specified with the help of a *generator matrix*.

Definition 2.18. A generator matrix G of an $[n, k, d]$ linear code C over $\mathbb{F}_q$ is any $k \times n$ matrix whose rows form a basis for C.

Note that if G is a generator matrix for C then,

$$C = \{\mathbf{v}G : \mathbf{v} \in \mathbb{F}_q^k\}.$$

We can also describe C with the help of an $(n-k) \times n$ matrix H, called *parity check matrix*, such that C is the null space of H, i.e.,

$$\mathbf{v} \in C \iff H\mathbf{v}^T = 0.$$

If the generator matrix G of a linear code C has the form $G = [I_k|A]$, then we say that G is in *standard form*. The following result shows the relationship between the generator matrix in standard form and the parity check matrix of a linear code C.

Theorem 2.26. *If $G = [I_k \mid A]$ is a generator matrix of a linear code C, then $H = [-A^T \mid I_{n-k}]$ is a parity check matrix for C.*

Example 2.27. [22] The following matrices are respectively generator and parity check matrices for a $[7, 4, 3]$ binary code.

$$G = \left[\begin{array}{cccc:ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right] \qquad H = \left[\begin{array}{cccc:ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right].$$

The next result indicates the relationship between a linear code and a set of independent vectors, which we make use of in Section 6.4 to construct sets of frequency rectangles. First, we give here the definition of t–independent vectors.

Definition 2.19. A set S of vectors in $(\mathbb{F}_q)^n$ is said to be *t–independent* if each of its subset of size t is linearly independent.

Theorem 2.28. [10] *A linear code C with a parity check matrix H has minimum distance d if and only if the matrix H contains a set of d dependent columns but each set of $d-1$ columns is independent.*

In the theory of codes, for fixed parameters n and M, a code with the highest possible d is desirable. Similarly, for fixed n and d, a code of maximum size is preferred. Therefore a significant effort has been put into finding the bounds in terms of these parameters. Here we include some of these results.

Theorem 2.29 (**Singleton bound**). [3] *If C is an (n, M, d) q-ary code, then $M \leq q^{n-d+1}$. In the case of linear $[n, k, d]$ code, $d \leq n - k + 1$.*

Theorem 2.30 (**Sphere-packing bound**). [3] *If C is an (n, M, d) q-ary code of packing radius $\rho = \lfloor (d-1)/2 \rfloor$, then*

$$M\left(1 + (q-1)n + (q-1)^2\binom{n}{2} + \cdots + (q-1)^\rho\binom{n}{\rho}\right) \leq q^n,$$

and in the linear case:

$$\sum_{i=0}^{\rho}(q-1)^i\binom{n}{i} \leq q^{n-k}.$$

The next result gives a lower bound on n for a linear $[n, k, d]$ code, given its minimum weight and dimension.

Theorem 2.31 (**Griesmer Bound**). [22] *Let C be an $[n, k, d]$ q-ary code with $k \geq 1$. Then*

$$n \geq \sum_{i=0}^{k-1}\left\lceil \frac{d}{q^i} \right\rceil.$$

We refer the reader to [22] for a detailed overview of research in this field. A useful online repository for the bounds on codes over finite fields of size less than or equal to 9 is available at [16].

References

[1] S. Addelman and O. Kempthorne. Some main-effect plans and orthogonal arrays of strength two. *Annals of Mathematical Statistics*, 32(4):1167–1176, 1961.

[2] S. S. Agaian. *Hadamard Matrices and Their Application*. Springer, 1985.

[3] E. F. Assmus and J. D. Key. *Designs and their Codes*. Number 103. Cambridge University Press, 1994.

[4] R. C. Bose and S. S. Shrikhande. On the falsity of Euler's conjecture about the non-existence of two orthogonal latin squares of order $4t + 2$. *Proceedings of the National Academy of Sciences of the United States of America*, 45(5):734, 1959.

[5] R. C. Bose, S. S. Shrikhande, and E. T. Parker. Further results on the construction of mutually orthogonal latin squares and the falsity of Euler's conjecture. *Canadian Journal of Mathematics*, 12:189–203, 1960.

[6] T. Britz, N. J. Cavenagh, A. Mammoliti, and I. M. Wanless. Mutually orthogonal binary frequency squares. *The electronic journal of combinatorics*, 27(3), 2020.

[7] B. W. Brock. Hermitian congruence and the existence and completion of generalized hadamard matrices. *Journal of Combinatorial Theory, Series A*, 49(2):233–261, 1988.

[8] S. Cammann. The evolution of magic squares in China. *Journal of the American Oriental Society*, 80(2):116–124, 1960.

[9] C.-S. Cheng. Orthogonal arrays with variable numbers of symbols. *The Annals of Statistics*, 8:447–453, 1980.

[10] C. J. Colbourn and J. H. Dinitz. *Handbook of Combinatorial Designs, Second Edition (Discrete Mathematics and Its Applications)*. Chapman & Hall/CRC, 2006.

[11] R. Craigen, G. Faucher, R. Low, and T. Wares. Circulant partial hadamard matrices. *Linear Algebra and its Applications*, 439(11):3307–3317, 2013.

[12] R. Craigen, J. Seberry, and X.-M. Zhang. Product of four hadamard matrices. *Journal of Combinatorial Theory, Series A*, 59(2):318–320, 1992.

[13] D. Z. Djokovic. Hadamard matrices of order 764 exist. *Combinatorica*, 28:487–489, 2008.

[14] W. Federer, A. Hedayat, and J. Mandeli. Pairwise orthogonal f-rectangle designs. *Journal of statistical planning and inference*, 10(3):365–374, 1984.

[15] J. Goethals and J. J. Seidel. Orthogonal matrices with zero diagonal. *Canadian Journal of Mathematics*, 19:1001–1010, 1967.

[16] M. Grassl. Code tables: Bounds on the parameters of various types of codes. Accessed Nov 2022. http://codetables.markus-grassl.de/.

[17] J. Hadamard. Résolution d'une question relative aux déterminants. *Bull. des Sciences Math*, 17:240–246, 1893.

[18] A. Hedayat, D. Raghavarao, and E. Seiden. Further contributions to the theory of f-squares design. *The Annals of Statistics*, 3:712–716, 1975.

[19] A. Hedayat and E. Seiden. f-square and orthogonal f-squares design: A generalization of latin square and orthogonal latin squares design. *The Annals of Mathematical Statistics*, 41(6):2035–2044, 1970.

[20] S. Hedayat, Sloane. *Orthogonal Arrays*. Springer, New York, NY, 1999.

[21] K. J. Horadam. *Hadamard matrices and their applications*. Princeton university press, 2012.

[22] W. Huffman, J. Kim, and P. Sole. *Concise Encyclopedia of Coding Theory*. CRC Press, 2021.

[23] D. Jungnickel. On difference matrices, resolvable transversal designs and generalized hadamard matrices. *Mathematische Zeitschrift*, 167(1):49–60, 1979.

[24] A. D. Keedwell and J. Dénes. *Latin squares and their applications*. Elsevier, 2015.

[25] H. Kharaghani and B. Tayfeh-Rezaie. A hadamard matrix of order 428. *Journal of Combinatorial Designs*, 13(6):435–440, 2005.

[26] C. Laywine. A geometric construction for sets of mutually orthogonal frequency squares. *Utilitas Mathematica*, 35:95–102, 1989.

[27] C. Laywine and G. Mullen. *Discrete Mathematics Using Latin Squares*. 1484 Series. Wiley, 1998.

[28] C. F. Laywine and G. L. Mullen. Generalizations of Bose's equivalence between complete sets of mutually orthogonal latin squares and affine planes. *Journal of Combinatorial Theory, Series A*, 61(1):13–35, 1992.

[29] C. F. Laywine and G. L. Mullen. A table of lower bounds for the number of mutually orthogonal frequency squares. *Ars Combinatoria*, 59:85–96, 2001.

[30] M. Li, Y. Zhang, and B. Du. Some new results on mutually orthogonal frequency squares. *Discrete Mathematics*, 331:175–187, 2014.

[31] S. London. *Constructing new Turyn type sequences, T-sequences and Hadamard matrices*. PhD thesis, University of Illinois at Chicago, 2013.

[32] J. Mandeli. Complete-sets of mutually orthogonal frequency rectangle designs having twice a prime power number of columns. *Utilitas Mathematica*, 41:151–160, 1992.

[33] J. Mandeli and W. Federer. On the construction of mutually orthogonal f-hyperrectangles. *Utilitas Math.*, 25:315—324, 1984.

[34] V. C. Mavron. Frequency squares and affine designs. *The Electronic Journal of Combinatorics*, 7(1):56, 2000.

[35] G. L. Mullen. Polynomial representation of complete sets of mutually orthogonal frequency squares of prime power order. *Discrete Mathematics*, 69(1):79–84, 1988.

[36] R. E. Paley. On orthogonal matrices. *Journal of Mathematics and Physics*, 12(1-4):311–320, 1933.

[37] C. R. Rao. Factorial experiments derivable from combinatorial arrangements of arrays. *Supplement to the Journal of the Royal Statistical Society*, 9(1):128–139, 1947.

[38] J. Williamson. Hadamard's determinant theorem and the sum of four squares. *Duke Mathematical Journal*, 11(1):65–81, 1944.

Chapter 3

Applications to Experimental Designs

3.1 Factorial Designs

Designing an experiment for statistical analysis has long been an integral part of research in most fields of science. Experiments in the fields of agriculture, medicine, manufacturing and other industries often involve the study of the effect of combinations of different input variables on the output product (for example, some real experiments are given in [10]). One of the common techniques to study such effects is by carrying out a *factorial experiment*. The variables under the study are called *factors* and the different settings for each variable are termed as *levels* of that variable. Below we give the formal definitions for these terms. The notations in this section are mostly consistent with [14].

Definition 3.1. Let $k \geq 2$. An experiment that involves the study of effects and interactions of k factors $F_1, F_2, \ldots, F_k$ that appear at $q_1, q_2, \ldots, q_k$ levels, respectively, is called a *factorial experiment*. If $q_1 = \cdots = q_k = q$ then we call such a factorial a *symmetrical* q^k *factorial* or simply a q^k *factorial*.

Let $[q] = \{0, 1, \ldots, q-1\}$. A *treatment combination* is a combination of levels of k factors that can be represented by the vector $(a_1, a_2, \ldots, a_k) \in [q]^k$.

Example 3.1. Consider an experiment in which we are testing the effect of four drugs D_1, D_2, D_3 and D_4 on the production of milk by cows. For each drug, there are two possibilities, either a cow has been treated with it or not. Thus we have four factors and each factor has two levels. There are 16 treatment combinations possible that can conveniently be represented by the binary strings of length four:

$$\begin{array}{cccccccc} 0000, & 0001, & 0010, & 0011, & 0100, & 0101, & 0110, & 0111, \\ 1000, & 1001, & 1010, & 1011, & 1100, & 1101, & 1110, & 1111. \end{array}$$

Here the treatment combination 1101, for example, represents that this particular group of cows is being treated with D_1, D_2 and D_4. Thus it is a 2^4 factorial experiment. Before proceeding any further we want to include the definition of treatment contrasts which are parametric functions used to determine factorial effects.

Definition 3.2. Let $\tau(a_1, a_2, \ldots, a_k)$ represent the treatment effect corresponding to the treatment combination $(a_1, a_2, \ldots, a_k)$. Then a *treatment contrast* is defined to be a function:

$$\sum_{(a_1,\ldots,a_k)\in[q]^k} l(a_1, \ldots, a_k)\tau(a_1, a_2, \ldots, a_k),$$

where $l(a_1, \ldots, a_k)$ are real numbers, not all zero and

$$\sum_{(a_1,\ldots,a_k)\in[q]^k} l(a_1, \ldots, a_k) = 0.$$

In the case of the above experiment, let $\tau(abcd)$ represent the mean amount of milk produced by the cows treated with the treatment combination $abcd$. The effect of D_1 at a particular combination bcd of D_2, D_3 and D_4 can be measured by the following expression:

$$L(D_1|_{bcd}) = \tau(1bcd) - \tau(0bcd).$$

Thus a way of obtaining the total effect $L(D_1)$, called the *main effect*, of drug D_1 is to take the mean of these differences over all the combinations of D_2, D_3

and D_4, that is:

$$\begin{aligned} L(D_1) &= \frac{1}{8}\sum_{bcd\in[1]^3}\{\tau(1bcd)-\tau(0bcd)\} \\ &= \frac{1}{8}\Big[\{\tau(1000)-\tau(0000)\}+\{\tau(1001)-\tau(0001)\}+\{\tau(1010)-\tau(0010)\} \\ &\quad +\{\tau(1100)-\tau(0100)\}+\{\tau(1011)-\tau(0011)\}+\{\tau(1101)-\tau(0101)\} \\ &\quad +\{\tau(1110)-\tau(0110)\}+\{\tau(1111)-\tau(0111)\}\Big] \end{aligned}$$

Note that the right-hand side of the above equation is a treatment contrast to estimate the main effect of drug D_1. The number 1/8 depends on further statistical aims (see Chapter 2 in [14]).

Now the interaction effect D_1D_2 of the drug D_1 with D_2 at a particular combination cd of the drugs D_3 and D_4 can be estimated by taking the difference $L(D_1|_{1cd}) - L(D_1|_{0cd})$. In turn, a treatment contrast to estimate the interaction effect $L(D_1D_2)$ is given by:

$$L(D_1D_2) = \frac{1}{8}\sum_{cd\in[1]^2}\{L(D_1|_{1cd}) - L(D_1|_{0cd})\}$$

The interaction of three factors $D_1D_2D_3$ can be defined in terms of the interaction of the interaction factor D_1D_2 with D_3 or D_1 with D_2D_3, which are essentially the same. There are some structural approaches to write treatment contrasts corresponding to factorial effects that can be found in [14]. For a detailed review of factorial design experiments, also see [16, 17].

3.2 Row-Column Factorial Designs

In the above experiment, one may also want to study the effect of different age groups of cows and breeds. Suppose that there are four age groups of cows and four breeds. This can be done by arranging the 16 treatment combinations in a 4×4 array such that each row represents a different breed and each column represents a different age group of cows as shown in Table 3.1 (this table is taken from [7]). The rows and columns of the design can be thought of as *blocking factors* and such a design is called a *full row-column factorial design.*

	Age 1	Age 2	Age 3	Age 4
Breed 1	1111	0100	0010	1001
Breed 2	0001	1010	1100	0111
Breed 3	1000	0011	0101	1110
Breed 4	0110	1101	1011	0000

Table 3.1: A regular row-column factorial design of type $I_4(4, 4; 2)$.

In Table 3.1 we have given an example of a row-column factorial design in which each treatment combination appears exactly once. However, in general, the treatment combinations can appear more than once. Formally,

Definition 3.3. An $m \times n$ row-column factorial design q^k is any arrangement of the elements of $\alpha \times [q]^k$ in an $m \times n$ array. Necessarily, mn must be a multiple of q^k.

A *blocking factor* is a partition (usually equipartition) of the treatment combinations of the factorial design. While blocking factors help study some additional information, balance in the treatment combinations within each block can help avoid estimation bias. Therefore the design needs a more careful arrangement of treatment combinations. There are several structured approaches in constructing factorial designs with blocking factors ([1, 2, 8, 9, 13]). However, as mentioned in [11], designs with two forms of blocking have not been investigated thoroughly.

Consider the design in Table 3.1 (with two forms of blocking). If we look closely we can see that in each row (or column) at any particular position $i \in [4]$ the entries 0 and 1 each appear twice. Thus half of the entries for a particular drug in each block are at a high level and half of them are at a low. These type of regularity properties in the design allows the unbiased estimation of the main effects; the four drugs, age and breed.

On the other hand, if we fix the first and the fourth coordinates, then pairs 01 and 10 do not appear in the first row. Similarly in the columns, if we choose

the second and the third coordinate, the design lacks this property. Therefore the interaction factor D_1D_4 *confounds* with the age groups and the interaction factor D_2D_3 is not estimable across the breeds.

We say that a row-column factorial design is of *strength* t if each of its columns is an orthogonal array of type $OA(m, k, q, t)$ and each of its rows is a transpose of an $OA(n, k, q, t)$. We denote such a design by $I_k(m, n, q, t)$. In the context of experimental design, in an $I_k(m, n, q, t)$ all subsets of interactions of size at most t can be estimated without confounding by the row and column blocking factors. Thus, the design in Table 3.1 is an $I_4(4, 4, 2, 1)$ but not an $I_4(4, 4, 2, 2)$. Here we want to remind the reader that, in Chapter 4 a *regular row-column design* $I_k(m, n, q)$ is equivalent to $I_k(m, n, q, 1)$.

In experimental design, there is a wide range of designs that can be considered row-column designs. Almost all of them have the property of being arranged in a rectangular array and typically (but not always) the rows and columns act as blocking factors. One of the earliest examples of a row-column factorial design can be found in [15] in which the following design was featured:

11111	10011	00110	01010	00101	10000	01001	11100
10010	11110	01011	00111	10001	00100	11101	01000
11011	10100	00001	01101	00010	10111	01110	11011
10101	11001	01100	00000	10110	00011	11010	01111
00011	01000	11010	10001	11111	01101	10100	00110
01001	00010	10000	11011	01100	11110	00111	10101
00100	01111	11011	10110	11011	01010	10011	00001
01110	00101	10111	11100	01011	11001	00000	10010

Table 3.2: A Row-column design for a 2^5-Factorial with 2 replicates

In practical use, sometimes a row-column design of strength 0 (non-regular) is also useful. The design in Table 3.3 containing six replicates of 4×8 factorial was used by CSIRO Division of Forestry [19]. The two factors were the

four salt-irrigation levels and eight different lots of seeds. It was known that the effect of growth varies with respect to the distance from the walls of the glasshouse and also from north to south. Therefore, the row-column design was constructed to analyse this two-dimensional physical effect.

3 8	2 2	1 7	4 3	1 5	2 1	3 6	4 4
1 4	3 1	2 3	1 8	2 6	4 2	4 5	2 7
4 1	4 7	3 5	2 4	3 3	1 6	2 8	1 2
2 7	1 3	4 6	3 2	4 8	3 4	1 1	2 5
1 5	1 7	2 3	3 2	2 8	3 4	4 6	4 1
3 7	4 8	3 6	2 5	4 2	1 3	1 1	2 4
2 6	3 1	1 8	4 4	3 3	4 5	2 7	1 2
4 3	2 2	4 7	1 6	1 4	2 1	3 8	3 5
4 5	1 8	2 3	1 7	3 2	3 4	2 1	4 6
2 2	2 7	4 8	3 6	1 4	4 1	1 5	3 3
1 6	3 1	3 5	2 8	4 7	1 3	4 2	2 4
3 8	4 3	1 1	4 4	2 6	2 5	3 7	1 2
4 3	2 2	3 6	3 5	1 4	1 7	4 8	2 1
3 2	4 6	1 1	2 7	2 8	4 5	3 4	1 3
2 6	1 5	2 3	4 4	4 1	3 8	1 2	3 7
1 8	3 1	4 7	1 6	3 3	2 4	2 5	4 2
2 4	3 7	4 1	1 3	1 6	2 5	3 2	4 8
4 6	1 5	3 8	4 7	2 3	3 4	2 1	1 2
3 3	2 8	1 4	3 6	4 2	1 1	4 5	2 7
1 7	4 4	2 6	2 2	3 1	4 3	1 8	3 5
4 7	1 2	2 6	3 1	2 4	4 5	3 8	1 3
3 2	3 7	4 1	2 5	4 3	1 6	1 4	2 8
2 3	4 8	3 5	1 7	1 1	2 2	4 6	3 4
1 5	2 1	1 8	4 4	3 6	3 3	2 7	4 2

Table 3.3: Row-column design for a 4×8 Factorial with 6 replicates

Unbiased estimation of factorial effects sometimes required the treatment combinations to be arranged in a way that coincides with the structure of a quasi-Latin rectangle.

Definition 3.4. A *quasi-Latin rectangle* $\mathrm{LR}(m, n; q)$ is an $m \times n$ array based on a symbol set of size q, where $q > m, n$ and q divides the product mn, such that each symbol appears λ times in the array and no symbol appears more than once in any row or column.

A quasi-Latin rectangle in which $m = n$ is called a *quasi-Latin square*.

Example 3.2. Table 3.4 and Table 3.5 are, respectively, a quasi-Latin square and a quasi-Latin rectangle based on the symbol set $\{0, 1, \ldots, 7\}$:

6	5	4	0
1	0	6	7
2	7	1	3
5	2	3	4

Table 3.4: LR$(4, 4; 8)$

1	2	3	4	5	6
7	0	1	2	3	4
5	6	7	0	1	2
3	4	5	6	7	0

Table 3.5: LR$(4, 6; 8)$

Quasi-Latin rectangles have been used to construct row-column factorial designs ([3]). Here if we consider each vector as a symbol then a row-column factorial design can be thought of a quasi-Latin rectangle. For example, the following 2^3 row-column design ($I_3(4, 4, 2, 1)$) featured in [3] corresponds to the quasi-Latin square given in Table 3.4.

0,1,1	1,0,1	1,1,0	0,0,0
1,0,0	0,0,0	0,1,1	1,1,1
0,1,0	1,1,1	1,0,0	0,0,1
1,0,1	0,1,0	0,0,1	1,1,0

Table 3.6: An $I_3(4, 4, 2, 1)$ design.

John and Lewis ([12]) describe a technique to generate row-column designs by using a generalized cyclic method. Some other examples and techniques to construct row-column designs are also given in [5], [6] and [4]. Wang [18] defines a technique to construct a row-column design involving k factors each with two levels, such that all the main effects are estimable. The procedure involves careful selection of treatment combinations to generate the first row and the first column of the design and then complete the table using component-wise addition modulo 2, to get an $I_k(2^M, 2^N, 2, 1)$ where $k = M + N$. For example,

$11111, 10100, 01100$ and $11110, 11101$ were used to span the first column and the first row, respectively, of the following design:

00000	**11110**	**11101**	00011
11111	00001	00010	11100
10100	01010	01001	10111
01100	10010	10001	01111
01011	10101	10110	01000
10011	01101	01110	10000
11000	00110	00101	11011
00111	11001	11010	00100

Table 3.7: An $I_5(2^3, 2^2, 2, 1)$ design.

A generalization of row-column design, called *generalized confounded row-column design (GCRC)*, was introduced by Datta et al. [7], in which the intersection of rows and columns can contain multiple treatment combinations. Their construction also utilizes the structure of a Latin square of suitable order. For example, the following design featured in [7] uses a Latin square of order four. Here each block corresponds to a cell of a Latin square.

0000	1011	1000	0100	0001	1010	0010	1001
0111	1100	0011	1111	0110	1101	0101	1110
1000	0100	0001	1010	0010	1001	0000	1011
0011	1111	0110	1101	0101	1110	0111	1100
0001	1010	0010	1001	0000	1011	1000	0100
0110	1101	0101	1110	0111	1100	0011	1111
0010	1001	0000	1011	1000	0100	0001	1010
0101	1110	0111	1100	0011	1111	0110	1101

Table 3.8: GCRC based on 2^4-factorial with block size 2^2

In [11], Godolphin described a method to construct row-column designs with two levels such that all main effects are estimable and the design also maximizes the possible number of two-factor interactions of interest. The construction uses a similar approach as in [7] by selecting specific treatment combinations to generate the first row and the first column of the design. The generating treatment combinations are grouped in the form of a matrix called *array generator matrix (AGM)*. In [11], the authors have also described the properties of the $AGMs$ which dictate the estimability of the main effects and two-factor interactions in the subsequent design. Consider the following AGM to construct a 2^5-factorial in a $2^2 \times 2^3$ array:

$$G = \left(\frac{G_c}{G_r}\right) = \left(\begin{array}{ccccc} 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ \hline 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

Since the matrix G has rank 5 (full) therefore the resulting design will consist of a full 2^5 factorial, and the number of treatment combinations in G_c and G_r corresponds to the dimension of the resulting array. Now by using the treatment combinations in G_c and G_r to span, respectively, the first column and the first row of the design and then completing the table using addition modulo 2 we get the following design:

00000	**10110**	**01101**	11011	**01001**	11111	00100	10010
11110	01000	10011	00101	10111	00001	11010	01100
11001	01111	10100	00010	10000	00110	11101	01011
00111	10001	01010	11100	01110	11000	00011	10101

Table 3.9: $2^2 \times 2^3$ full factorial row-column design

Since each column in the sub-matrices G_c and G_r is non-zero, the resulting array contains exactly half the number of zeroes and ones in each column and row (where the position is fixed). Thus the design in Table 3.9 is an

$I_5(2^2, 2^3, 2, 1)$. This property in the design enables the estimability of all main effects. The first two columns in G_c are the same, this leads to the appearance of only two types of pairs, either $\{10, 01\}$ or $\{11, 00\}$, in each column at the first and second coordinate. Thus the interaction factor F_1F_2 is confounded in the columns. Similarly, F_3F_4 is also confounded in the columns.

In matrix G_r, the first column is the same as the fourth and the second is the same as the fifth. This causes the interaction factors F_1F_4 and F_2F_5 to be confounded in the columns. In other words, the design in Table 3.9 lacks the strength 2 property in these positions and therefore these interaction factors are confounded.

In [11], the author has also provided an upper bound ω (defined below) on the maximal number of interaction factors that can be estimated together with all the main effects in a $2^p \times 2^q$ row-column design.

Let $n = \alpha(2^p - 1) + \beta$, where α and β are integers and $0 \leq \beta \leq 2^p - 2$. Then

$$\omega = \binom{n}{2} - \alpha\beta - (2^p - 1)\binom{\alpha}{2}. \tag{3.1}$$

If we plug in the values of the parameters of the design in Table 3.9 we get $\omega = 8$. However, the design only estimates the six interaction factors out of ten. If we take the AGM matrix such that each column of G_c is distinct then the resulting design would allow the estimation of the maximum number of interaction factors together with all main effects.

Example 3.3. [11] The following AGM matrix G_1 has the same G_c submatrix as in G but the G_r contains no identical columns. Therefore, the same interaction factors are confounded in the columns and there is no interaction factor confounded in the rows.

$$G = \left(\frac{G_c}{G_r}\right) = \left(\begin{array}{ccccc} 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ \hline 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{array}\right)$$

00000	**10101**	**01110**	11011	**01101**	11000	00011	10110
11110	01011	10000	00101	10011	00110	11101	01000
11001	01100	10111	00010	10100	00001	11010	01111
00111	10010	01001	11100	01010	11111	00100	10001

Table 3.10: An $I_5(2^2, 2^3, 2, 1)$ design.

References

[1] R. Bailey. Patterns of confounding in factorial designs. *Biometrika*, 64(3):597–603, 1977.

[2] R. Bailey. Factorial design and abelian groups. *Linear Algebra and its Applications*, 70:349–368, 1985.

[3] C. J. Brien, R. A. Bailey, T. T. Tran, and J. Boland. Quasi-latin designs. *Electronic Journal of Statistics*, 6:1900–1925, 2012.

[4] C.-S. Cheng and P.-W. Tsai. Templates for design key construction. *Statistica Sinica*, pages 1419–1436, 2013.

[5] K. C. Choi and S. Gupta. Confounded row–column designs. *Journal of statistical planning and inference*, 138(1):196–202, 2008.

[6] S. Dash, R. Parsad, and V. Gupta. Row–column designs for 2^n factorial 2-colour microarray experiments for estimation of main effects and two-factor interactions with orthogonal parameterization. *Agricultural research*, 2(2):172–182, 2013.

[7] A. Datta, S. Jaggi, E. Varghese, and C. Varghese. Generalized confounded row–column designs. *Communications in Statistics-Theory and Methods*, 46(12):6213–6221, 2017.

[8] A. Dean and S. Lewis. A unified theory for generalized cyclic designs. *Journal of Statistical Planning and Inference*, 4(1):13–23, 1980.

[9] A. Dean and S. Lewis. Multidimensional designs for two-factor experiments. *Journal of the American Statistical Association*, 87(420):1158–1165, 1992.

[10] A. Dean and D. Voss. *Design and Analysis of Experiments*. Springer Texts in Statistics. Springer New York, 2000.

[11] J. Godolphin. Construction of row–column factorial designs. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 81(2):335–360, 2019.

[12] J. John and S. Lewis. Factorial experiments in generalized cyclic row-column designs. *Journal of the Royal Statistical Society: Series B (Methodological)*, 45(2):245–251, 1983.

[13] A. Kobilinsky. Confounding in relation to duality of finite abelian groups. *Linear algebra and its applications*, 70:321–347, 1985.

[14] R. Mukerjee and C. J. Wu. *A modern theory of factorial design*. Springer Science & Business Media, 2007.

[15] C. R. Rao. Confounded factorial designs in quasi-latin squares. *Sankhyā: The Indian Journal of Statistics*, pages 295–304, 1946.

[16] A. Street and D. Street. *Combinatorics of experimental design*. Oxford science publications. Clarendon Press, 1987.

[17] B. G. Tabachnick and L. S. Fidell. *Experimental designs using ANOVA*. Thomson/Brooks/Cole Belmont, CA, 2007.

[18] P. Wang. Orthogonal main-effect plans in row–column designs for two-level factorial experiments. *Communications in Statistics-Theory and Methods*, 46(21):10685–10691, 2017.

[19] E. Williams and J. John. Row-column factorial designs for use in agricultural field trials. *Journal of the Royal Statistical Society: Series C (Applied Statistics)*, 45(1):39–46, 1996.

Chapter 4

Row-column factorial designs with multiple levels

4.1 Abstract

An $m \times n$ *row-column factorial design* is an arrangement of the elements of a factorial design into a rectangular array. Such an array is used in experimental design, where the rows and columns can act as blocking factors. Formally, for any integer q, let $[q] = \{0, 1, \ldots, q-1\}$. The q^k (full) factorial design with replication α is the multi-set consisting of α occurrences of each element of $[q]^k$; we denote this by $\alpha \times [q]^k$. A *regular* $m \times n$ *row-column factorial design* is an arrangement of the elements of $\alpha \times [q]^k$ into an $m \times n$ array (which we say is of *type* $I_k(m, n; q)$) such that for each row (column) and fixed vector position $i \in [k]$, each element of $[q]$ occurs n/q times (respectively, m/q times). Let $m \leq n$. We show that an array of type $I_k(m, n; q)$ exists if and only if (a) $q \mid m$ and $q \mid n$; (b) $q^k \mid mn$; (c) $(k, q, m, n) \neq (2, 6, 6, 6)$ and (d) if $(k, q, m) = (2, 2, 2)$ then 4 divides n. Godolphin (2019) showed the above is true for the case $q = 2$ when m and n are powers of 2.

In the case $k = 2$, the above implies necessary and sufficient conditions for the existence of a pair of mutually orthogonal frequency rectangles (or F-rectangles) whenever each symbol occurs the same number of times in a given

row or column.

Keywords: Row-column factorial design, blocking factor, double confounding, frequency square *or* F-square, frequency rectangle *or* F-rectangle, MOFS.

4.2 Introduction

For any integer q, let $[q] = \{0, 1, \ldots, q-1\}$. Consider the following example of an experimental design from [8]. Suppose we wish to study the effects of 4 drugs at two dosage levels while controlling for the effects of 4 breeds and 4 age groups. We could conduct 16 experiments based on the following row-column factorial design:

1111	0100	0010	1001
0001	1010	1100	0111
1000	0011	0101	1110
0110	1101	1011	0000

Table 4.1: A regular row-column factorial design of type $I_4(4, 4; 2)$.

Here the rows and columns correspond to age groups and breeds, respectively, of calves; with the binary vector in a cell indicating the dosage of each of the four drugs as one of two *levels*.

In the above the 16 vectors from $[2]^4$ are arranged in a 4×4 array, in such a way that for each row (column) and $i \in [4]$, the entries 0 and 1 each appear twice in position i of a vector in that row (respectively, column). In the context of experimental design, these properties of regularity mean that if we consider the set of six effects (the four drugs together with breed and age group), there is no *confounding* between any pair of these effects. On the other hand, if we ignore age and breed effects, the underlying factorial design allows us to also estimate the effects of any subset of the four types of drug (these are called

interactions) without confounding. We refer the reader to Chapter 9 of [15] for more detail of the application of row-column factorial designs to statistical experimental design.

Formally, the q^k (full) factorial design with replication α is the multi-set consisting of α occurrences of each element of $[q]^k$; we denote this by $\alpha \times [q]^k$. An $m \times n$ *row-column factorial design* q^k is any arrangement of the elements of $\alpha \times [q]^k$ into an $m \times n$ array. Necessarily, q^k must divide mn. Without loss of generality, we always assume $m \leq n$. We call such a design *regular* if for each row (column) and $i \in [q]$, each element of $[q]$ occurs n/q times (respectively, m/q times). Furthermore, we denote the type of such an array to be $I_k(m, n; q)$, where regularity is always assumed to hold. Observe that regularity implies that q divides both m and n. The above example is thus a regular 4×4 row-column factorial design 2^4, or equivalently an array of type $I_4(4, 4; 2)$. Note that an array of type $I_2(n, n; n)$ is equivalent to a pair of orthogonal Latin squares of order n.

We first review the impact of row-column factorial designs within experimental design literature. A *blocking factor* can be thought of as a partition of the blocks of a design, typically an equipartition (all subsets in the partition have equal size) with further properties of regularity to minimize confounding within the design structure. Blocking factors for factorial designs have been well-studied ([1], [2], [9], [10], [17]). However, as mentioned in [13], having two forms of blocking for a factorial design is less well-studied.

Within experimental design, a *row-column* design can refer to a variety of combinatorial designs, all with the property of being arranged in a rectangular array, where the rows and columns are typically (but not always) blocking factors. This is sometimes referred to as *double confounding* [13]. To ensure that certain effects can be estimated without confounding, regularity conditions are imposed. For example, in a Latin square each symbol occurs once per row and once per column. In practice non-regular row-column factorial designs are also sometimes of use. In [25], a non-regular row-column factorial design is given

which was used by the CSIRO Division of Forestry for a glasshouse experiment. Here the physical distance to the edge of the glasshouse is an important effect to consider.

A *quasi-Latin square* is an $n \times n$ array such that for some $k > n$ which divides n^2, each entry from $[k]$ occurs n^2/k times in the array, with no entry occurring more than once per row or column. Some of the literature on quasi-Latin squares features row-column factorial designs [3]. Here if we consider the vectors as the entries, a row-column factorial design can be thought of as a quasi-Latin square if no vector occurs more than once in a row or column (necessarily, $m, n < 2^k$). John and Lewis [16] describe a technique to cyclically generate some regular row-column factorial designs. Examples of regular row-column factorial designs are also given in [6], [7] and [5]. Wang [24] constructs $I_k(2^M, 2^N; 2)$ whenever $k = M + N$. A variation of row-column factorial designs is considered by [8]: a *generalized confounded row-column design* can be thought of as a factorial design arranged into a rectangular array where each cell contains a constant number of vectors.

Row-column factorial designs with two levels (that is, $q = 2$) are studied in [13]. As well as the result in Theorem 4.1 below, designs are also constructed to estimate paired interactions without confounding by row and column blocking factors.

Theorem 4.1. [13] *Let $1 \leq M \leq N$. An array of type $I_k(2^M, 2^N; 2)$ (i.e. a regular $2^M \times 2^N$ row-column factorial design 2^k) exists if and only if $k \leq M+N$ and $(k, M, N) \neq (2, 1, 1)$.*

We next describe the connection between regular row-column factorial designs and frequency rectangles. Given two vectors $\mathbf{v} = (v_0, v_1, \ldots, v_{s-1})$ and $\mathbf{w} = (w_0, w_1, \ldots, w_{t-1})$, we define $\mathbf{v} \oplus \mathbf{w}$ to be the concatenation of $\mathbf{v}$ and $\mathbf{w}$, that is:

$$\mathbf{v} \oplus \mathbf{w} := (v_0, v_1, \ldots, v_{s-1}, w_0, w_1, \ldots, w_{t-1}).$$

Next, let $A = [a_{ij}]$ and $B = [b_{ij}]$ be matrices of the same dimensions, where each entry of A is a vector of dimension k and each entry of B is a vector of

dimension ℓ. Then we define $C = A \oplus B$ to be the matrix given by $C = [c_{ij} := a_{ij} \oplus b_{ij}]$.

Now, an array of type $I_k(m, n; q)$ can be written in the form $F_0 \oplus F_1 \oplus \cdots \oplus F_{k-1}$, where each entry of each F_i, $i \in [k]$, has dimension 1. Since regularity is assumed, each element of $[q]$ occurs precisely n/q times per row and m/q times per column, for each of the arrays F_i, $i \in [k]$. These arrays are thus *frequency rectangles*.

Formally, a *frequency rectangle* (sometimes known as an *F-rectangle*) of type $FR(m, n; q)$ is an $m \times n$ array such that each element of $[q]$ occurs n/q times per row and m/q times per column. Thus, we may write any array of type $I_k(m, n; q)$ as $F_0 \oplus F_1 \oplus \cdots \oplus F_{k-1}$, where for each $i \in [k]$, F_i is a frequency rectangle of type $FR(m, n; q)$. We note here that frequency rectangles in the literature (most often *frequency squares* or *F-squares* when $m = n$) may have different row/column frequencies for distinct symbols. In this paper we restrict ourselves to the regular case.

Two frequency rectangles of type $FR(m, n; q)$ are orthogonal if, when superimposed, each ordered pair from $[q] \times [q]$ occurs exactly mn/q^2 times in the array. A set of pairwise orthogonal frequency rectangles are called *mutually orthogonal frequency rectangles*. These have mostly been studied in the case $m = n$, where such structures are called Mutually Orthogonal Frequency Squares or MOFS), and in particular the case $m = n = q$, where such structures are Mutually Orthogonal Latin Squares (MOLS).

The existence problem for pairs of MOFS has been completely solved; the following theorem is a special case of [18, p. 67]. The exceptions are precisely the two orders for which pairs of MOLS do not exist, as originally conjectured by Euler.

Theorem 4.2. *There exists a pair of MOFS of type $F(n, n; q)$ (equivalently, an array of type $I_2(n, n; q)$) if and only if $(n, q) \notin \{(2, 1), (6, 1)\}$.*

Hedayat, Raghavarao, et al. [14] showed that if a set of k MOFS of type $FR(n, n; q)$ exists then $k \leq (n-1)^2/(q-1)$. When k meets this upper bound

such a set is called *complete*. Complete sets of MOFS exist when $q = 2$ and if there exists a Hadamard matrix of order n [12]; otherwise they are only known to exist when n is a prime power [19, 20, 21, 23]. A complete set of MOFS does not exist when $q = 2$ and $n \equiv 2 \pmod 4$ [4].

Note that while an array of type $I_k(m, n; q)$ yields a set of k mutually orthogonal frequency rectangles, the converse is not always true for $k \geq 3$, as seen below. Here we see a set of three mutually orthogonal frequency rectangles of type $FR(6, 12; 2)$ (overlapped) which is not a regular row-column factorial design, as the binary sequences of even weights (000, 110, 101, 011) appear 12 times each and the sequences of odd weights (001, 010, 100, 111) appear 6 times each in the resulting array.

000	111	000	101	011	110	000	111	000	101	011	110
111	000	000	011	110	101	111	000	000	011	110	101
000	000	111	110	101	011	000	000	111	110	101	011
101	011	110	010	100	001	101	011	110	010	100	001
011	110	101	100	001	010	011	110	101	100	001	010
110	101	011	001	010	100	110	101	011	001	010	100

Table 4.2: Three mutually orthogonal frequency rectangles of type $FR(6, 12; 2)$

However, if $k = 2$ an $I_k(m, n; q)$ is equivalent to a pair of mutually orthogonal frequency rectangles of type $F(m, n; q)$.

Theorem 4.3. [11] *Let q divide m and n. If $q \notin \{2, 6\}$ or at least one of n/q, m/q is even, there exists a pair of mutually orthogonal frequency rectangles of type $F(m, n; q)$ (equivalently, an array of type $I_2(m, n; q)$).*

A set of mutually orthogonal frequency rectangles can also be thought of as a type of mixed orthogonal array. In general, a *mixed orthogonal array* $\mathrm{OA}(N, s_1^{k_1} s_2^{k_2} \ldots s_v^{k_v}, t)$ is an array of size $N \times k$, where $k = \sum_{i=1}^{v} k_i$ in which k_i columns have symbols from the set $[s_i]$, such that in any $N \times t$ subarray every possible t-tuple occurs the same number of times. The parameter t is called the *strength* of the orthogonal array.

Given a set $F_1, F_2, \ldots, F_k$ of k mutually orthogonal frequency rectangles of type $F(m, n; q)$, for each cell $(i, j) \in [m] \times [n]$, create a row of an $mn \times (k + 2)$ array by placing the entry in cell (i, j) of F_ℓ in column ℓ, with i and j the entries, respectively, in the final two columns. The result is a mixed orthogonal array $\mathrm{OA}(mn, q^k, m^1, n^1, 2)$; in fact there is equivalence between the two combinatorial structures.

Thus, from above, an $I_k(m, n; q)$ is equivalent to a mixed orthogonal array only in the case $k = 2$. Mixed orthogonal arrays for $N \leq 100$ are classified in [22]. Consequently, it is known whether $I_2(m, n; q)$ exists for any m and n such that $mn \leq 100$.

In this paper our main result is to classify the parameters for which there exists a regular row-column factorial design, generalizing the results of Theorems 4.1, 4.2 and 4.3 above.

Theorem 4.4. *Let $m \leq n$. There exists an array of type $I_k(m, n; q)$ (that is, a regular $m \times n$ row-column factorial design q^k) if and only if q divides m, q divides n, q^k divides mn and neither of the following hold:*

(i) *$k = q = m = 2$ and $n \equiv 2 \pmod 4$.*

(ii) *$k = 2$ and $q = m = n = 6$.*

In Section 4, we generalize Theorem 4.3 to find necessary and sufficient conditions for the existence of an array of type $I_2(m, n; q)$. We prove the remaining cases of Theorem 4.4 in Section 5, using the recursive constructions from Section 2 and the finite field constructions from Section 3.

4.3 Recursive constructions

In this section we discuss ways in which row-column factorial designs can be built recursively. We begin with a straightforward lemma.

Lemma 4.5. *If there exist arrays of type $I_k(m, n; q)$ and $I_k(m', n; q)$ there exists an array of type $I_k(m+m', n; q)$. If there exist arrays of type $I_k(m, n; q)$ and $I_k(m, n'; q)$ there exists an array of type $I_k(m, n+n'; q)$.*

Next we consider a type of Kronecker Product. Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be two arrays of sizes $m \times n$ and $u \times v$, respectively. The *Kronecker product*, $A \otimes B$, of A and B is an $mu \times nv$ array defined by:

$$A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{pmatrix}$$

where $a_{lk}B$ is a $u \times v$ array with the entry (i, j) given by (a_{lk}, b_{ij}).

It is easy to see that if F and F' are two frequency rectangles of type $FR(m, n; q)$ and $FR(m', n'; q')$ respectively, then their Kronecker product $F \otimes F'$ is a frequency rectangle of type $FR(mm', nn'; qq')$, where the entries of $[q] \times [q']$ are mapped to $[qq']$ by some bijection f. In this fashion, let $D = F_0 \oplus F_1 \oplus \cdots \oplus F_{k-1}$ and $D' = F'_0 \oplus F'_1 \oplus \cdots \oplus F'_{k-1}$ be two row-column factorial designs of types $I_k(m, n; q)$ and $I_k(m', n'; q')$, respectively, where F_i and F'_i are frequency rectangles for each $i \in [k]$. Then we define $D \boxtimes D'$ to be the array given by $(F_0 \otimes F'_0) \oplus (F_1 \otimes F'_1) \oplus \cdots \oplus (F_{k-1} \otimes F'_{k-1})$.

Lemma 4.6. *If D and D' are arrays of type $I_k(m, n; q)$ and $I_k(m', n'; q')$, respectively, then $D \boxtimes D'$, as defined above, is an array of type $I_k(mm', nn'; qq')$.*

Proof. It suffices to show that the entries of the cells of $D \boxtimes D'$ form a regular factorial design. Let $D = F_0 \oplus F_1 \oplus \cdots \oplus F_{k-1}$ and $D' = F'_0 \oplus F'_1 \oplus \cdots \oplus F'_{k-1}$ as above.

Consider any $(\alpha_0, \alpha_1, \dots, \alpha_{k-1}) \in [qq']^k$ in a cell of $D \boxtimes D'$. Then for each $i \in [k]$, $\alpha_i = f(a_i, b_i)$, for some a_i and b_i belonging to the symbol sets of F_i

and F_i' respectively. Since D is of type $I_k(m, n; q)$, there are precisely mn/q^k cells containing a_i in F_i for each $i \in [k]$. Similarly, there are exactly $m'n'/(q')^k$ cells containing b_i in F_i' for each $i \in [k]$. From the definition of the Kronecker product, the sequence $(\alpha_0, \alpha_1, \ldots, \alpha_{k-1})$ appears exactly $mm'nn'/(qq')^k$ times in $D \boxtimes D'$. □

Example 4.7. Consider the two arrays D and D' of type $I_3(4, 2; 2)$ and $I_3(3, 9; 3)$ respectively.

000	011	101	110
111	100	010	001

D^T

000	011	022	101	112	120	202	210	221
111	122	100	212	220	201	010	021	002
222	200	211	020	001	012	121	102	110

D'

Then by taking the product $D \boxtimes D'$ and using the bijection $(a, b) \mapsto 3a + b$ to transform the symbol set, we get an array of type $I_3(12, 18; 6)$:

000	011	022	101	112	120	202	210	221	333	344	355	434	445	453	535	543	554
111	122	100	212	220	201	010	021	002	444	455	433	545	553	534	343	354	335
222	200	211	020	001	012	121	102	110	555	533	544	353	334	345	454	435	443
033	044	055	134	145	153	235	243	254	300	311	322	401	412	420	502	510	521
144	155	133	245	253	234	043	054	035	411	422	400	512	520	501	310	321	302
255	233	244	053	034	045	154	135	143	522	500	511	320	301	312	421	402	410
303	314	325	404	415	423	505	513	524	030	041	052	131	142	150	232	240	251
414	425	403	515	523	504	313	324	305	141	152	130	242	250	231	040	051	032
525	503	514	323	304	315	424	405	413	252	230	241	050	031	042	151	132	140
330	341	352	431	442	450	532	540	551	003	014	025	104	115	123	205	213	224
441	452	430	542	550	531	340	351	332	114	125	103	215	223	204	013	024	005
552	530	541	350	331	342	451	432	440	225	203	214	023	004	015	124	105	113

Table 4.3: An array of type $I_3(12, 18; 6)$

Corollary 4.8. *If there exist r arrays of types $I_k(m_i, n_i; q_i)$, where $i \in [r]$, then there exists an array of type $I_k(\prod_{i=0}^{r-1} m_i, \prod_{i=0}^{r-1} n_i; \prod_{i=0}^{r-1} q_i)$.*

Trivially there exists an array of type $I_k(m, n; 1)$ for any integers k, m, n. The following corollary is then immediate.

Corollary 4.9. *If there exists an array of type $I_k(m, n; q)$, then there exists an array of type $I_k(mm', nn'; q)$ for any integers $m', n' \geq 1$.*

4.4 Prime power constructions

In this section, we construct row-column factorial designs via finite fields of prime power order q. It is implicitly understood that field elements are relabelled to elements of $[q]$ as a final step in construction.

Lemma 4.10. *Let $M, N \geq 1$ and $q \geq 2$ a prime power, with $(M, N, q) \neq (1, 1, 2)$. Then there exists a linearly independent set of $M + N$ polynomials:*

$$f_r(x_0, ..., x_{M+N-1}) = a_{r,0}x_0 + a_{r,1}x_1 + \cdots + a_{r,M+N-1}x_{M+N-1};\ r \in [M + N]$$

over the field $\mathbb{F}_q$ which satisfy the following two conditions for each $r \in [M+N]$:

(i) $(a_{r,0}, ..., a_{r,M-1}) \neq (0, ..., 0)$*;*

(ii) $(a_{r,M}, ..., a_{r,M+N-1}) \neq (0, ..., 0)$.

Proof. We split the proof into cases.

Case I: When $M = N = 1$ and $q > 2$.

In this case we can take the following two polynomials:

$$\begin{aligned} f_0(x_0, x_1) &= x_0 + x_1 \\ f_1(x_0, x_1) &= x_0 + \alpha x_1, \end{aligned}$$

where α is a non-zero element in $\mathbb{F}_q$ other than the identity.

Case II (a): When $N \geq 2$ and q is a power of 2.

We remind the reader that since we are working over a field of order q, $1+1=0$ in this case. Consider the identity matrix I_{M+N} of order $M+N$. By performing the following two row operations sequentially:

$$\begin{aligned} &R_0 + R_s \to R_s \quad \text{for each } s \in \{1, 2, \ldots, M+N-1\}; \\ &R_s + (R_{M+N-1} + R_{M+N-2}) \to R_s \quad \text{for each } s \in [M], \end{aligned} \tag{4.1}$$

we get the following matrix:

$$\begin{array}{c} \\ R_0 \\ R_1 \\ \vdots \\ R_{M-1} \\ \hline R_M \\ R_{M+1} \\ \vdots \\ R_{M+N-1} \end{array} \left(\begin{array}{cccc:cccccc} c_0 & c_1 & \ldots & c_{M-1} & c_M & c_{M+1} & \ldots & c_{M+N-3} & c_{M+N-2} & c_{M+N-1} \\ 1 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & 1 & 1 \\ 1 & 1 & \ldots & 0 & 0 & 0 & \ldots & 0 & 1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 1 & 0 & \ldots & 1 & 0 & 0 & \ldots & 0 & 1 & 1 \\ \hdashline 1 & 0 & \ldots & 0 & 1 & 0 & \ldots & 0 & 0 & 0 \\ 1 & 0 & \ldots & 0 & 0 & 1 & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 1 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & 0 & 1 \end{array} \right)$$

Now corresponding to each row $R_s = (r_{s,0}, \ldots, r_{s,(M+N-1)})$ of the above matrix we define a polynomial $f_s = r_{s,0}x_0 + \cdots + r_{s,(M+N-1)}x_{M+N-1}$ in $\mathbb{F}_q$, where $s \in [M+N]$. Then these polynomials satisfy the conditions (i) and (ii) and are linearly independent.

Case II (b): When $N \geq 2$ and q is not a power of 2.

In this case again take the identity matrix I_{M+N} and by replacing the second row operation in (4.1) by $R_s + R_{M+N-1} \to R_s$ for each $s \in [M]$, we get the following matrix:

$$
\begin{array}{c}
 \\
R_0 \\
R_1 \\
\vdots \\
R_{M-1} \\
R_M \\
R_{M+1} \\
\vdots \\
R_{M+N-1}
\end{array}
\begin{array}{c}
\begin{array}{cccc:cccc} c_0 & c_1 & \dots & c_{M-1} & c_M & c_{M+1} & \dots & c_{M+N-2} & c_{M+N-1} \end{array} \\
\left(\begin{array}{cccc:cccc}
2 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 \\
2 & 1 & \dots & 0 & 0 & 0 & \dots & 0 & 1 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
2 & 0 & \dots & 1 & 0 & 0 & \dots & 0 & 1 \\
\hdashline
1 & 0 & \dots & 0 & 1 & 0 & \dots & 0 & 0 \\
1 & 0 & \dots & 0 & 0 & 1 & \dots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1
\end{array}\right)
\end{array}
$$

It is easy to see that the corresponding polynomials are linearly independent in $\mathbb{F}_q$ and satisfy the conditions (i) and (ii). □

Theorem 4.11. *Let $q \geq 2$ be a prime power. Let $M, N \geq 1$ and $(M, N, q) \neq (1, 1, 2)$. There exists an array of type $I_{M+N}(q^M, q^N; q)$.*

Proof. First we describe a method to construct a frequency rectangle of type $FR(q^M, q^N; q)$ corresponding to the polynomial f_r for each $r \in [M + N]$, as given by Lemma 4.10.

Label the rows and columns of a $q^M \times q^N$ array, respectively, by using the set of all M-tuples and N-tuples over the field $\mathbb{F}_q$. Now consider a polynomial

$$f_r(x_0, ..., x_{M+N-1}) = a_{r,0}x_{r,0} + \cdots + a_{r,M+N-1}x_{r,M+N-1}$$

over the field $\mathbb{F}_q$ that satisfies the conditions given in Lemma 4.10. We place the element $f(b_0, ..., b_{M-1}, c_0, ..., c_{N-1})$ in the intersection of row $(b_0, ..., b_{M-1})$ and column $(c_0, ..., c_{N-1})$ of the $q^M \times q^N$ array.

Now we show that the array obtained in this way is a frequency rectangle of type $FR(q^M, q^N; q)$, that is every element of $\mathbb{F}_q$ appears exactly q^{N-1} times

in each row and q^{M-1} times in each column. Consider a row which is labelled by $(b_0, ..., b_{M-1})$ and take an element $\alpha \in \mathbb{F}_q$. For this row, the equation

$$f_r(b_0, ..., b_{M-1}, x_M, ..., x_{M+N-1}) = \alpha$$

reduces to the equation

$$K + a_{r,M}x_M + ... + a_{r,M+N-1}x_{M+N-1} = \alpha \tag{4.2}$$

where K is a constant. Now by axiom (ii) of Lemma 4.10 there exists $i \in \{M, M+1, \ldots, M+N-1\}$ such that $a_{r,i} \neq 0$. We solve the equation (4.2) for x_i:

$$x_i = \frac{1}{a_{r,i}}(\alpha - K - a_{r,M}x_M - \cdots - a_{r,i-1}x_{i-1} - a_{r,i+1}x_{i+1} - \cdots - a_{r,M+N-1}x_{M+N-1}) \tag{4.3}$$

Since there are q elements in $\mathbb{F}_q$ and the $N-1$ variables on the right side of (4.3) can take any value from $\mathbb{F}_q$, the equation (4.3) has exactly q^{N-1} solutions in $\mathbb{F}_q$. This implies that the symbol α appears exactly at q^{N-1} places in the row $(b_0, ..., b_{M-1})$. By a similar argument, we can prove that each symbol appears exactly q^{M-1} times in each column. Thus the resulting array is a frequency rectangle of type $FR(q^M, q^N; q)$.

Now to construct an array of type $I_{M+N}(q^M, q^N; q)$. Consider a set of $M+N$ linearly independent polynomials

$$f_r(x_0, ..., x_{M+N-1}) = a_{r,0}x_0 + \cdots + a_{r,M+N-1}x_{M+N-1}; \quad r \in [M+N]$$

over the field $\mathbb{F}_q$, such that the coefficients satisfy the conditions (i) and (ii) of Lemma 4.10. As above, for each $r \in [M+N]$ we obtain a frequency rectangle F_r of type $FR(q^M, q^N; q)$

It remains to show that $F_0 \oplus F_1 \oplus \cdots \oplus F_{M+N-1}$ is an array of type $I_{M+N}(q^M, q^N; q)$. To this end, consider any $(\alpha_0, \alpha_1, ..., \alpha_{M+N-1}) \in (\mathbb{F}_q)^{M+N}$.

Since the polynomials above are linearly independent, the system of equations:

$$\begin{array}{lcl} a_{0,0}x_0 + \cdots + a_{0,M+N-1}x_{M+N-1} & = & \alpha_0 \\ a_{1,0}x_0 + \cdots + a_{1,M+N-1}x_{M+N-1} & = & \alpha_1 \\ \vdots \quad \ddots \quad \vdots & & \vdots \\ a_{M+N-1,0}x_0 + \cdots + a_{M+N-1,M+N-1}x_{M+N-1} & = & \alpha_{M+N-1} \end{array}$$

has rank $M+N$ and therefore has a unique solution in $\mathbb{F}_q$, which shows that $(\alpha_0, \alpha_1, ..., \alpha_{M+N-1})$ appears in exactly one cell of the array constructed. □

Corollary 4.9 implies the following:

Corollary 4.12. *If $(q, M, N) \neq (2, 1, 1)$, there exist an array of type $I_{M+N}(q^M b_1, q^N b_2; q)$, for any prime power q.*

4.4.1 "Sudoku" Frequency Rectangles

In this subsection we take the construction above and take it one step further. Specifically, we show in Theorem 4.18 that if q divides $b_1 b_2$ and q is a prime power, there exists an array of type $I_{M+N+1}(q^M b_1, q^N b_2; q)$.

First we describe a Latin square which has a Sudoku-type property with $q = q_1 q_2$ symbols, where q_1 and q_2 are positive integers and the symbol set is taken to be $[q]$. That is, such a Latin square can be partitioned into $q_1 \times q_2$ subarrays containing each element of $[q]$.

Theorem 4.13. *Let $q_1, q_2 \geq 1$. Then there exists a Latin square $L(q_1, q_2)$ of order $q_1 q_2$ such that for each $i \in [q_1]$ and $j \in [q_2]$, the set of cells*

$$\{(i', j') \mid i \equiv i' \pmod{q_1}, j \equiv j' \pmod{q_2}\}$$

contain each entry from $[q_1 q_2]$ exactly once.

Proof. In what follows, $q = q_1 q_2$. Let S_0 be the $q_1 \times q_2$ array where cell (i, j) of S contains the integer $i + jq_1$, for each $i \in [q_1]$ and $j \in [q_2]$. Thus the entries of S_0 are the elements of $[q]$, listed in ascending order from the first column:

0	q_1	$\dots$	$(q-q_1)$
1	q_1+1	$\dots$	$(q-q_1)+1$
$\vdots$	$\vdots$	$\ddots$	$\vdots$
q_1-1	$2q_1-1$	$\dots$	$q-1$

S_0

Now we define S_i to be the array obtained by adding the symbol $i \pmod q$ to each cell of S_0. Finally, define $L(q_1, q_2)$ to be the following array of order q:

	$\leftarrow\ q_2\ \rightarrow$	$\leftarrow\ q_2\ \rightarrow$	$\dots$	$\leftarrow\ q_2\ \rightarrow$
$\uparrow$ q_1 $\downarrow$	S_0	S_1	$\dots$	S_{q_1-1}
$\uparrow$ q_1 $\downarrow$	S_{q_1}	S_{q_1+1}	$\dots$	S_{2q_1-1}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\uparrow$ q_1 $\downarrow$	$S_{(q-q_1)}$	$S_{(q-q_1)+1}$	$\dots$	S_{q-1}

$L(q_1, q_2)$

Observe that each entry of $[q]$ occurs once per row and once per column; hence $L(q_1, q_2)$ is a Latin square. □

Example 4.14. We exhibit the construction in the previous theorem in the

case $q = 6, q_1 = 2$ and $q_2 = 3$:

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

The Latin square $L(2, 3)$ as defined in Theorem 4.13

Now, a Latin square of order q is also an array of type $I_1(q, q; q)$. Thus, from Corollary 4.9, we have the following corollary.

Corollary 4.15. *For any integers $\mu, \lambda, q_1, q_2 \geq 1$, there exists a frequency rectangle of type $FR(q\mu, q\lambda; q)$ (where $q = q_1q_2$) such that for each $i \in [\mu q_1]$ and $j \in [\lambda q_2]$, the set of cells*

$$\{(i', j') \mid i \equiv i' \pmod{\mu q_1}, j \equiv j' \pmod{\lambda q_2}\}$$

contain each entry from $[q_1q_2]$ exactly once.

Example 4.16. If L is the Latin square $L(2, 3)$, then $L \boxtimes I_1(2, 3; 1)$ yields a frequency rectangle of type $FR(12, 18; 6)$. The entries in bold show the elements of [6] occurring in cells of the form (i, j) where $i \equiv 1 \pmod 4$ and $j \equiv 2 \pmod 9$.

0	0	0	2	2	2	4	4	4	1	1	1	3	3	3	5	5	5
0	0	**0**	2	2	2	4	4	4	1	1	**1**	3	3	3	5	5	5
1	1	1	3	3	3	5	5	5	2	2	2	4	4	4	0	0	0
1	1	1	3	3	3	5	5	5	2	2	2	4	4	4	0	0	0
2	2	2	4	4	4	0	0	0	3	3	3	5	5	5	1	1	1
2	2	**2**	4	4	4	0	0	0	3	3	**3**	5	5	5	1	1	1
3	3	3	5	5	5	1	1	1	4	4	4	0	0	0	2	2	2
3	3	3	5	5	5	1	1	1	4	4	4	0	0	0	2	2	2
4	4	4	0	0	0	2	2	2	5	5	5	1	1	1	3	3	3
4	4	**4**	0	0	0	2	2	2	5	5	**5**	1	1	1	3	3	3
5	5	5	1	1	1	3	3	3	0	0	0	2	2	2	4	4	4
5	5	5	1	1	1	3	3	3	0	0	0	2	2	2	4	4	4

Table 4.4: A frequency rectangle of type $FR(12, 18; 6)$ by Corollary 4.15

Before we prove Theorem 4.18, we require the following number-theoretic observation.

Lemma 4.17. *Let b_1, b_2 and q be positive integers such that q divides the product b_1b_2. Then there exist positive integers q_1 and q_2 such that $q_1q_2 = q$ and q_1 divides b_2 and q_2 divides b_1.*

Proof. Let $q = p_0^{s_0} p_1^{s_1} \dots p_{m-1}^{s_{m-1}}$ be the prime factorization of q. Since q divides b_1b_2, b_1 and b_2 must be of the form:

$$b_1 = B_1\, p_0^{\alpha_0} p_1^{\alpha_1} \dots p_{m-1}^{\alpha_{m-1}},$$
$$b_2 = B_2\, p_0^{\beta_0} p_1^{\beta_1} \dots p_{m-1}^{\beta_{m-1}},$$

where p_i does not divide B_j and $\alpha_i + \beta_i \geq s_i$ for all $i \in [m]$ and $j \in \{1, 2\}$. Let

$$q_1 = p_0^{u_0} p_1^{u_1} \dots p_{m-1}^{u_{m-1}}$$

and

$$q_2 = p_0^{t_0} p_1^{t_1} \dots p_{m-1}^{t_{m-1}},$$

where $t_i := \max\{0, s_i - \beta_i\}$ and $u_i = s_i - t_i$ for all $i \in [m]$.

Since $\alpha_i + \beta_i \geq s_i$, $t_i \leq \alpha_i$ for each $i \in [m]$, which implies that q_2 divides b_1. Also $s_i - \beta_i \leq t_i$ implies that $u_i = s_i - t_i \leq \beta_i$ and thus q_1 divides b_2. Finally observe that $q_1 q_2 = q$. □

Theorem 4.18. *Let q be a divisor of $b_1 b_2$. If there exist an array of type $I_{M+N}(q^M, q^N; q)$, then there exists an array of type $I_{M+N+1}(q^M b_1, q^N b_2; q)$.*

Proof. By Lemma 4.17 we can choose q_1, q_2 such that $q_1 q_2 = q$ and q_1 divides b_2 and q_2 divides b_1.

Let I' be the array $I_1(q_2, q_1; 1) \boxtimes I_{M+N}(q^M, q^N; q)$ as shown in Table 4.5.

	$\leftarrow$ q^N $\rightarrow$	$\leftarrow$ q^N $\rightarrow$	$\dots$	$\leftarrow$ q^N $\rightarrow$
$\uparrow$ q^M $\downarrow$	I_{M+N}	I_{M+N}	$\dots$	I_{M+N}
$\uparrow$ q^M $\downarrow$	I_{M+N}	I_{M+N}	$\dots$	I_{M+N}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\uparrow$ q^M $\downarrow$	I_{M+N}	I_{M+N}	$\dots$	I_{M+N}

Table 4.5: $I' = I_1(q_2, q_1; 1) \boxtimes I_{M+N}(q^M, q^N; q)$

Applying Corollary 4.15 with $\mu = q^{M-1} q_2$ and $\lambda = q^{N-1} q_1$, there exists a rectangular array J' of type $I_1(q^M q_2, q^N q_1; q)$ such that for each $i \in [q^M]$ and

$j \in [q^N]$, the set of cells

$$\{(i', j') \mid i \equiv i' \pmod{q^M}, j \equiv j' \pmod{q^N}\}$$

contain each entry from $[q_1 q_2]$ exactly once. It follows that the array $I' \oplus J'$ contains each sequence of length $M+N+1$ exactly once. Thus $I' \oplus J'$ is of type $I_{M+N+1}(q^M q_2, q^N q_1; q)$. Finally, by Corollary 4.9, $I_1(b_1/q_2, b_2/q_1; 1) \boxtimes (I' \oplus J')$ is an array of type $I_{M+N+1}(q^M b_1, q^N b_2; q)$. □

4.5 The case $k = 2$

In this section we prove Theorem 4.4 in the case $k = 2$. Given Theorem 4.3, it suffices to consider the existence of an array of type $I_2(m, n; q)$ only in the case $q \in \{2, 6\}$ and m/q and n/q odd. From Theorem 4.2, arrays of type $I_2(2, 2; 2)$ and $I_2(6, 6; 6)$ do not exist. We next give another non-existence result.

Lemma 4.19. *There does not exist an array of type $I_2(2, n; 2)$ whenever $n/2$ is odd.*

Proof. Consider a frequency rectangle F of type $FR(2, n; 2)$. By permuting columns we can assume F is in the following form:

0	0	...	0	1	1	...	1
1	1	...	1	0	0	...	0

Now consider any other frequency rectangle F' of type $FR(2, n; 2)$. Now since $n \equiv 2 \pmod 4$, F' contains at least $\lfloor n/4 \rfloor + 1$ symbols of the same type (say 0) in the first $n/2$ cells of its first row. This implies there are at least $\lfloor n/4 \rfloor + 1$ $1's$ in the second half of the first row and consequently we have $\lfloor n/4 \rfloor + 1$ $0's$ in the second half of its second row. Thus if we superimpose F and F', we get at least $2 \times \lfloor n/4 \rfloor + 2 > n/2 = 2n/4$ ordered pairs of type $(0, 0)$. Which shows F and F' are not orthogonal. □

Lemma 4.20. *Let $m/2$ and $n/2$ be odd where $n \geq m > 2$. Then there exists an array of type $I_2(m, n; 2)$.*

Proof. Let $m = 2l_1$ and $n = 2l_2$, where l_1 and l_2 are odd and $l_2 \geq l_1 > 1$. Let $l_2 = l_1 + 2t$. Now by Theorem 4.2 there exists an array of type $I_2(2l_1, 2l_1; 2)$. By Theorem 4.11 and Corollary 4.9 there exists an array of type $I_2(2l_1, 4t; 2)$. Thus by Lemma 4.5, there exists an array of type $I_2(2l_1, 2l_2; 2)$. □

Next we consider when $q = 6$. An array of type $I_2(6, 12; 6)$ exists by Theorem 4.3. We also exhibit an array of type $I_2(6, 18; 6)$:

13	24	35	40	51	02	15	24	30	43	51	02	10	24	33	45	51	02
34	43	01	52	20	15	34	45	01	52	23	10	34	40	01	52	25	13
43	32	10	25	04	53	41	32	13	20	04	55	41	32	15	23	04	50
22	11	54	03	45	30	22	11	54	05	40	33	22	11	54	00	43	35
50	05	23	31	12	44	53	00	25	31	12	44	55	03	20	31	12	44
04	50	42	14	33	21	00	53	42	14	35	21	03	55	42	14	30	21

Table 4.6: An array of type $I_2(6, 18; 6)$.

By Lemma 4.5, we thus obtain the following.

Lemma 4.21. *There exists an array of type $I_2(6l_1, 6l_2; 6)$ if and only if $(l_1, l_2) \neq (1, 1)$.*

4.6 The case $k \geq 3$.

It now suffices to prove the case $k \geq 3$ in order to prove Theorem 4.4.

Theorem 4.22. *Let $k \geq 3$, $q|m$, $q|n$ and $q^k|mn$. Then there exist an array of type $I_k(m, n; q)$.*

Proof. Trivially, if an array of type $I_k(m,n;q)$ exists, then an array of type $I_\ell(m,n;q)$ exists for each $1 \leq \ell < k$. Thus we may assume that $k = \max\{t : q^t | mn\}$. Let $mn = q^k b$.

Consider the prime factorization of q:

$$q = p_0^{s_0} p_1^{s_1} \dots p_{l-1}^{s_{l-1}}.$$

For each $r \in [l]$, let $i_r = \max\{t : q_r^t | m\}$ and $j_r = \max\{t : q_r^t | n\}$, where $q_r = p_r^{s_r}$. Thus m and n can be expressed as:

$$m = q_0^{i_0} \dots q_{l-1}^{i_{l-1}}\ p_0^{\alpha_0} \dots p_{l-1}^{\alpha_{l-1}}\ a_1, \qquad n = q_1^{j_1} \dots q_l^{j_l}\ p_0^{\beta_0} \dots p_{l-1}^{\beta_{l-1}}\ a_2 \tag{4.4}$$

with $\alpha_r, \beta_r < s_r$ and $p_r \nmid a_1$ and $p_r \nmid a_2$ for each $r \in [l]$. Now for any $c \in [l]$ we have the following two cases:

Case I: When $\alpha_c + \beta_c < s_c$.

In this case, $i_c + j_c$ is the largest power of q_c which divides mn, and thus $i_c + j_c$ is the largest power of q_c which divides k. By Corollary 4.12, if $(i_c, j_c, q_c) \neq (1,1,2)$, there exists an array of type $I_k(q_c^{i_c} p_c^{\alpha_c}, q_c^{j_c} p_c^{\beta_c}; q_c)$, where $k = i_c + j_c$. However if $(i_c, j_c, q_c) = (1,1,2)$, then $s_c = 1$, $\alpha_c = \beta_c = 0$ and 2^3 does not divide mn, contradicting $k \geq 3$.

Case II: When $\alpha_c + \beta_c \geq s_c$.

Since $\alpha_c, \beta_c < s_c$, this implies $\alpha_c + \beta_c < 2s_c$ and therefore $i_c + j_c + 1$ is the largest power of q_c which divides k. By combining Theorem 4.11 and Theorem 4.18 we obtain an array of type $I_k(q_c^{i_c} p_c^{\alpha_c}, q_c^{j_c} p_c^{\beta_c}; q_c)$ where $k = i_c + j_c + 1$.

Thus in both cases for each $c \in [l]$ we obtain an array of type $I_k(q_c^{i_c} p_c^{\alpha_c}, q_c^{j_c} p_c^{\beta_c}; q_c)$ and by taking their Kronecker product (see Corollary 4.8), we can construct an array of type $I_k(\frac{m}{a_1}, \frac{n}{a_2}; q)$ where a_1 and a_2 are defined in equation (4.4). Finally, by applying Corollary 4.9 we obtain an array of type $I_k(m,n;q)$, which completes the proof. □

The previous section and Theorem 4.22 together imply Theorem 4.4.

References

[1] R. Bailey. Patterns of confounding in factorial designs. *Biometrika*, 64(3):597–603, 1977.

[2] R. Bailey. Factorial design and abelian groups. *Linear Algebra and its Applications*, 70:349–368, 1985.

[3] C. J. Brien, R. A. Bailey, T. T. Tran, and J. Boland. Quasi-latin designs. *Electronic Journal of Statistics*, 6:1900–1925, 2012.

[4] T. Britz, N. Cavenagh, A. Mammoliti, and I. Wanless. Mutually orthogonal binary frequency squares. *The Electronic Journal of Combinatorics*, 27(3):P3.7, 2020.

[5] C.-S. Cheng and P.-W. Tsai. Templates for design key construction. *Statistica Sinica*, pages 1419–1436, 2013.

[6] K. C. Choi and S. Gupta. Confounded row–column designs. *Journal of statistical planning and inference*, 138(1):196–202, 2008.

[7] S. Dash, R. Parsad, and V. Gupta. Row–column designs for 2^n factorial 2-colour microarray experiments for estimation of main effects and two-factor interactions with orthogonal parameterization. *Agricultural research*, 2(2):172–182, 2013.

[8] A. Datta, S. Jaggi, E. Varghese, and C. Varghese. Generalized confounded row–column designs. *Communications in Statistics - Theory and Methods*, 46(12):6213–6221, 2017.

[9] A. Dean and S. Lewis. A unified theory for generalized cyclic designs. *Journal of Statistical Planning and Inference*, 4(1):13–23, 1980.

[10] A. Dean and S. Lewis. Multidimensional designs for two-factor experiments. *Journal of the American Statistical Association*, 87(420):1158–1165, 1992.

[11] W. Federer, A. Hedayat, and J. Mandeli. Pairwise orthogonal f-rectangle designs. *Journal of statistical planning and inference*, 10(3):365–374, 1984.

[12] W. T. Federer. On the existence and construction of a complete set of orthogonal $f(4t; 2t, 2t)$-squares design. *The Annals of Statistics*, 5(3):561–564, 1977.

[13] J. Godolphin. Construction of row–column factorial designs. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 81(2):335–360, 2019.

[14] A. Hedayat, D. Raghavarao, and E. Seiden. Further contributions to the theory of f-squares design. *The Annals of Statistics*, 3:712–716, 1975.

[15] K. Hinkelmann and O. Kempthorne. *Design and analysis of experiments, vol. 2*. New York: Wiley, 2005.

[16] J. John and S. Lewis. Factorial experiments in generalized cyclic row-column designs. *Journal of the Royal Statistical Society: Series B (Methodological)*, 45(2):245–251, 1983.

[17] A. Kobilinsky. Confounding in relation to duality of finite abelian groups. *Linear algebra and its applications*, 70:321–347, 1985.

[18] C. Laywine and G. Mullen. *Discrete Mathematics Using Latin Squares*. 1484 Series. Wiley, 1998.

[19] C. F. Laywine and G. L. Mullen. A table of lower bounds for the number of mutually orthogonal frequency squares. *Ars Combinatoria*, 59:85–96, 2001.

[20] M. Li, Y. Zhang, and B. Du. Some new results on mutually orthogonal frequency squares. *Discrete Mathematics*, 331:175–187, 2014.

[21] V. C. Mavron. Frequency squares and affine designs. *The Electronic Journal of Combinatorics*, 7(1):56, 2000.

[22] N. Sloane. Table of orthogonal arrays of strength 2 with up to 100 runs. Accessed: May 2021. http://neilsloane.com/doc/cent4.html.

[23] D. Street. Generalized hadamard matrices, orthogonal arrays and f-squares. *Ars Combinatoria*, 8:131–141, 1979.

[24] P. Wang. Orthogonal main-effect plans in row–column designs for two-level factorial experiments. *Communications in Statistics-Theory and Methods*, 46(21):10685–10691, 2017.

[25] E. Williams and J. John. Row-column factorial designs for use in agricultural field trials. *Journal of the Royal Statistical Society: Series C (Applied Statistics)*, 45(1):39–46, 1996.

Chapter 5

Row-column factorial designs with strength at least 2

5.1 Abstract

The q^k (full) factorial design with replication λ is the multi-set consisting of λ occurrences of each element of each q-ary vector of length k; we denote this by $\lambda \times [q]^k$. An $m \times n$ *row-column factorial design* q^k of *strength* t is an arrangement of the elements of $\lambda \times [q]^k$ into an $m \times n$ array (which we say is of type $I_k(m, n, q, t)$) such that for each row (column), the set of vectors therein are the rows of an orthogonal array of degree k, size n (respectively, m), q levels and strength t. Such arrays are used in experimental design. In this context, for a row-column factorial design of strength t, all subsets of interactions of size at most t can be estimated without confounding by the row and column blocking factors.

In this manuscript, we study row-column factorial designs with strength $t \geq 2$. Our results for strength $t = 2$ are as follows. For any prime power q and assuming $2 \leq M \leq N$, we show that there exists an array of type $I_k(q^M, q^N, q, 2)$ if and only if $k \leq M + N$, $k \leq (q^M - 1)/(q - 1)$ and $(k, M, q) \neq (3, 2, 2)$. We find necessary and sufficient conditions for the existence of $I_k(4m, n, 2, 2)$ for small parameters. We also show that

$I_{k+\alpha}(2^\alpha b, 2^k, 2, 2)$ exists whenever $\alpha \geq 2$ and $2^\alpha + \alpha + 1 \leq k < 2^\alpha b - \alpha$, assuming there exists a Hadamard matrix of order $4b$.

For $t = 3$ we focus on the binary case. Assuming $M \leq N$, there exists an array of type $I_k(2^M, 2^N, 2, 3)$ if and only if $M \geq 5$, $k \leq M + N$ and $k \leq 2^{M-1}$. Most of our constructions use linear algebra, often in application to existing orthogonal arrays and Hadamard matrices.

Mathematics Subject Classification: 05B15, 05B20, 15B34.

Keywords: Row-column factorial design, Hadamard matrix, orthogonal array, Hadamard code, linear code, linear orthogonal array.

5.2 Introduction

For any integer s, let $[s] = \{0, 1, \ldots, s-1\}$. An *orthogonal array* of size N, degree k, q levels and strength t, denoted $\mathrm{OA}(N, k, q, t)$ is an $N \times k$ array with entries from $[q]$ such that in every $N \times t$ submatrix, every $1 \times t$ row vector appears N/q^t times. The q^k (full) factorial design with replication λ is the multi-set consisting of λ occurrences of each element of $[q]^k$; we denote this by $\lambda \times [q]^k$.

An $m \times n$ *row-column factorial design* q^k is any arrangement of the elements of $\lambda \times [q]^k$ into an $m \times n$ array. We say that such an array has *strength* t if for each row (column), the set of vectors therein are the rows of an orthogonal array of size k, degree n (respectively, m), q levels and strength t. That is, if we consider any subset of t positions within the vectors in a fixed row (or column), we obtain a $[q]^t$ full-factorial design with replication n/q^t (respectively, m/q^t). We denote such a row-column factorial design by $I_k(m, n, q, t)$, where the replication number or index λ of the design is given by $\lambda = mn/q^k$.

For example, in Table 5.1 the elements of $[3]^4$ are arranged into a 9×9 array such that the vectors in each row and column are the rows of an $\mathrm{OA}(9, 4, 3, 2)$. Thus this is an array of type $I_4(9, 9, 3, 2)$.

0000	1011	2022	0112	1120	2101	0221	1202	2210
0111	1122	2100	0220	1201	2212	0002	1010	2021
0222	1200	2211	0001	1012	2020	0110	1121	2102
1021	2002	0010	1100	2111	0122	1212	2220	0201
1102	2110	0121	1211	2222	0200	1020	2001	0012
1210	2221	0202	1022	2000	0011	1101	2112	0120
2012	0020	1001	2121	0102	1110	2200	0211	1222
2120	0101	1112	2202	0210	1221	2011	0022	1000
2201	0212	1220	2010	0021	1002	2122	0100	1111

Table 5.1: A row-column factorial design $I_4(9, 9, 3, 2)$.

Within experimental design, a *row-column* design can refer to a variety of combinatorial designs, all with the property of being arranged in a rectangular array, where regularity conditions may be imposed in order to estimate effects without confounding. Table 5.1, for example, could be used to study the effects of 4 drugs on cows, each at 3 dosage levels while controlling for the effects of 9 breeds (the rows) and 9 age groups (the columns). Here the vector $(2, 0, 2, 2)$ in the first row and third column indicates that the first breed and third age group are given the highest dosage of the first, third and fourth drug and the lowest dosage of the second drug. The property of being an array of type $I_4(9, 9, 3, 2)$ eliminates, for example, confounding between breed or age group and the interaction between any pair of drugs. We refer the reader to [13] and [7] for a literature review on the application of row-column factorial designs to statistical experimental design.

In this paper two arrays are *equivalent* under any: (a) reordering of rows; (b) reordering of columns; (c) reordering of levels (applied globally); and (d) reordering of the entries in each vector (with the same reordering applied

globally). It is also convenient to use the terms "array" and "matrix" interchangeably. When linear algebra is applied we often work over the field of order q, with an understanding that when q is a prime power, the levels are relabelled with $[q]$ as a final step.

By definition, if there exists an array of type $I_k(m, n, q, t)$ then $q^k | mn$ and there exists an OA(m, k, q, t) and there exists an OA(n, k, q, t). If (k, m, n, q, t) is a 5-tuple satisfying these three necessary conditions we say that (k, m, n, q, t) is *admissible*.

Necessary conditions for the existence of orthogonal arrays of strength t imply further necessary conditions for the existence of row-column factorial designs of strength t. It is impractical to list all known necessary conditions (in particular as t grows large); we refer the reader to surveys in III.6 and III.7 of the Handbook of Combinatorial Designs [4]. Elementary conditions imply that $t \leq k$ and q^t divides both m and n. In summary:

Lemma 5.1. *If (k, m, n, q, t) is admissible then $q^t \mid m$, $q^t \mid n$, $q^k \mid mn$ and $t \leq k$.*

Necessary and sufficient conditions for a row-column factorial design of strength 1 are given in [13], generalizing [7] and [16].

Theorem 5.2. [13] *Let $m \leq n$. There exists $I_k(m, n, q, 1)$ (that is, an $m \times n$ row-column factorial design q^k of strength 1) if and only if:*

i. $q \mid m$ and $q \mid n$;

ii. if $k = q = m = 2$ then 4 divides n; and

iii. $(k, m, n, q) \neq (2, 6, 6, 6)$.

Note that an array $I_k(n, n, q, t)$ implies the existence of a set of k mutually orthogonal frequency squares (MOFS) of size n based on a set of size q. Thus, the existence of row-column factorial designs also relates to the existence of frequency squares and Latin squares. For example, the exceptions in the previous theorem include pairs of orthogonal Latin squares of orders 2 and 6, which

are well-known not to exist. Some results, including a table of lower bounds, related to the existence of MOFS can be found in [2, 10, 11].

In this manuscript we focus on row-column factorial designs of strength 2 and higher. Binary row-column factorial designs of strength 1 which come as close as possible to strength 2 are studied in [7], in the case when the dimensions of the array are powers of 2. The motivation in [7] is to be able to estimate as many two-factor interactions as possible without confounding, given fixed parameters.

In the binary strength 2 case we will frequently make use of Hadamard matrices. A *Hadamard matrix* $H(n)$ is a square matrix of order n, having entries from the set $\{1, -1\}$ such that any two rows are orthogonal, i.e., it satisfies the equation: $H(n)H(n)^T = nI_n$. If a Hadamard matrix $H(n)$ exists, then either $n = 2$ or n is divisible by 4. However, the converse is an open problem known as the *Hadamard conjecture*; the smallest value for which it is not known whether a Hadamard matrix exists or not is 668 [6].

The following lemma gives a relationship between binary orthogonal arrays of strength 2 and 3 and the Hadamard matrices of order $4m$.

Lemma 5.3. [8, p. 148] *Let $m \geq 4$. Orthogonal arrays $OA(4m, 4m-1, 2, 2)$ and $OA(8m, 4m, 2, 3)$ exist if and only if there exists a Hadamard matrix order $4m$.*

It is worth mentioning how orthogonal arrays can be constructed from Hadamard matrices as per the previous lemma, as this idea is frequently applied in Sections 5 and 6, where we focus on binary arrays. Let H be a Hadamard matrix of order $4m$. Assume that H is in *normalized form*; that is, we assume the first row and column of H only contain the entry 1. Now delete the first column and replace each -1 with 0. The resultant array is an $\mathrm{OA}(4m, 4m-1, 2, 2)$. Next, consider the array $[H \mid -H]^T$ and again replace each -1 with 0; the resultant array is an $\mathrm{OA}(8m, 4m, 2, 3)$. The rows of such an array are the codewords of a code known as a *Hadamard code* [9].

For a binary vector $\mathbf{v}$, we often say that its *weight* $\omega(\mathbf{v})$ is equal to the

number of 1's in $\mathbf{v}$. It is also often convenient to say that two binary vectors $\mathbf{v}$ and $\mathbf{w}$ of length $4k$ are *orthogonal* if each has weight $2k$ and $\mathbf{v} \cdot \mathbf{w} = k$. So in a binary orthogonal array of strength 2, each pair of columns is necessarily orthogonal.

The previous lemma, together with the Bose-Bush bound for orthogonal arrays ([4]; [12] originally) implies the following necessary conditions for strength 2 row-column factorial designs.

Lemma 5.4. *Let $m \leq n$. If there exists an array of type $I_k(m, n, q, 2)$, then $k \leq (m-1)/(q-1)$. If there exists an array of type $I_{m-1}(m, n, 2, 2)$, then there is a Hadamard matrix of order m.*

Since the Hadamard conjecture is a well-studied but unsolved open problem, it is likely that generalizing Theorem 5.2 to the strength 2 case, that is finding necessary and sufficient conditions for the existence of a row-column factorial design of strength 2, is untenable even in the binary case.

The following result on strength 3 binary orthogonal arrays is well-known [4, 14].

Lemma 5.5. *If an $\mathrm{OA}(m, n, 2, 3)$ exists, then $m \leq 2^{n-1}$. Moreover, an $\mathrm{OA}(2^{n-1}, n, 2, 3)$ exists, the rows of which are all the binary vectors of length n and odd weight.*

Let C and R be orthogonal arrays each of degree k with q levels with the zero vector in the first row. We define $C \boxplus R$ to be the array such that row i and column j contains the vector sum, calculated in $\mathbb{F}_q$, of the ith row of C and the jth row of R. In turn, we call an array L of type $I_k(m, n, q, t)$ *abelian* if and only if there exists C and R such that $L = C \boxplus R$, where C is an $\mathrm{OA}(m, k, q, t)$ and R is an $\mathrm{OA}(n, k, q, t)$. (Here we use C and R to remind the reader that the first *C*olumn and first *R*ow of L are, respectively, the orthogonal arrays C and R.) If the replication is 1, then such an array is abelian if and only if it is the subarray of the addition table for $\mathbb{F}_q^k$. Most constructions in this paper are abelian, however Section 5 contains some non-abelian constructions.

In Section 2, we give some general recursive constructions that apply to all row-column factorial designs. In Section 3 we focus on the abelian case, using linear algebra to show that row-column factorial designs can be constructed from orthogonal arrays and matrices with certain independence properties. These are applied in Section 4 where we consider the strength 2 case with an arbitrary number of levels. We solve this case completely when the number of levels q is a prime power and the dimensions of the array are each a power of q; see Theorem 5.19. This generalizes the binary case solved in [7].

In Section 5 we find necessary and sufficient conditions for the existence of $I_k(4m, n, 2, 2)$ whenever $m \leq 5$; or m is odd assuming the existence of a Hadamard matrix of order $4m$, containing two sets of non-trivial columns such that their sums are orthogonal (see Conjecture 5.27). We also show that $I_{k+\alpha}(2^\alpha b, 2^k, 2, 2)$ exists whenever $\alpha \geq 2$ and $2^\alpha+\alpha+1 \leq k < 2^\alpha b-\alpha$, assuming there exists a Hadamard matrix of order $4b$ (Theorem 5.36). Finally in Section 6 we consider the strength 3 binary case, solving this whenever the dimensions are powers of 2 (Theorem 5.40).

5.3 General results

In this section we list some general observations and results that can be applied to row-column factorial designs of any strength.

We start with some straightforward lemmas.

Lemma 5.6. *If D is an array of type $I_k(m, n, q, t)$ then:*

- *D is also an array of type $I_k(m, n, q, t')$ for each t' such that $1 \leq t' \leq t$;*
- *there exists an array of type $I_{k'}(m, n, q, t')$ for each k' such that $1 \leq k' \leq k$.*

Lemma 5.7. *If there exist arrays of type $I_k(m, n, q, t)$ and $I_k(m', n, q, t)$ there exists an array of type $I_k(m + m', n, q, t)$. If there exist arrays of type $I_k(m, n, q, t)$ and $I_k(m, n', q, t)$ there exists an array of type $I_k(m, n + n', q, t)$.*

The proof of the following lemma is a Kronecker product construction based on a similar construction for orthogonal arrays (Theorem III.7.20 from [4], originally [3]).

Lemma 5.8. *If there exist arrays of type $I_k(m, n, q, t)$ and $I_k(m', n', q', t)$ then there exists an array of type $I_k(mm', nn', qq', t)$.*

Proof. Let D and D' be arrays of type $I_k(m, n, q, t)$ and $I_k(m', n', q', t)$, respectively. We construct an $mm' \times nn'$ array $D \boxtimes D'$ as follows. For each $(i, j) \in [mm'] \times [nn']$, write $i = xm' + x'$ and $j = yn' + y'$ where $x \in [m]$, $x' \in [m']$, $y \in [n]$, $y' \in [n']$, noting that the choices of x, x', y and y' are unique and depend on i and j. In cell (i, j) we place the vector $q'D(x, y) + D'(x', y')$, where $D(x, y)$ and $D'(x', y')$ are the vectors in cells (x, y) and (x', y') of D and D', respectively.

We next verify that $D \boxtimes D'$ is an array of type $I_k(mm', nn', qq', t)$. Fix a set T of t coordinates in column j of $D \boxtimes D'$ and let $(v_1, v_2, \ldots, v_t) \in [qq']^t$. As above, write $j = yn' + y'$ for unique $y \in [n]$, $y' \in [n']$. For each $\alpha \in [t]$, let $x_\alpha \in [q]$ and $x'_\alpha \in [q']$ be unique solutions to $v_\alpha = x_\alpha q' + x'_\alpha$.

Since D is of strength t, the vector $(x_1, x_2, \ldots, x_t)$ appears n/q^t times in column y of D in the set of positions T. Similarly, the vector $(x'_1, x'_2, \ldots, x'_t)$ appears $n'/(q')^t$ times in column y' of D' in the same set of positions T. Thus $(v_1, v_2, \ldots, v_t)$ appears precisely $nn'/(qq')^t$ times in column j of $D \boxtimes D'$. By the same argument in transpose, each vector in $[qq']^t$ appears $mm'/(qq')^t$ in each row of $D \boxtimes D'$.

It remains to show that each vector in $[qq']^k$ appears the same number of times in the array $D \boxtimes D'$. The idea is similar to above. Let $(v_1, v_2, \ldots, v_k) \in [qq']^k$. For each $\alpha \in [k]$, let $x_\alpha \in [q]$ and $x'_\alpha \in [q']$ be unique solutions to $v_\alpha = x_\alpha q' + x'_\alpha$. By the parameters of D and D', the vectors $(x_1, x_2, \ldots, x_k)$ and $(x'_1, x'_2, \ldots, x'_k)$ appear mn/q^k and $m'n'/(q')^k$ times, respectively, in the arrays D and D'. Thus $(v_1, v_2, \ldots, v_k)$ appears precisely $mm'nn'/(qq')^k$ times in the array $D \boxtimes D'$. □

The $m \times n$ matrix of $\mathbf{0}$ vectors of dimension k is trivially an array $I_k(m, n, 1, t)$ for any $1 \leq k \leq t$. The following corollary is then immediate.

Corollary 5.9. *If there exists an array $I_k(m, n, q, t)$, then there exists an array $I_k(mm', nn', q, t)$ for any integers $m', n' \geq 1$.*

5.4 Abelian row-column factorial designs

In this section, we find necessary and sufficient conditions on orthogonal arrays C and R such that $C \boxplus R$ is a row-column factorial design of strength t, where at least one of C or R is a vector space.

Since every row (column) in $C \boxplus R$ is equivalent to the first row (respectively, column), we have the following observation.

Lemma 5.10. *Let C be an $\mathrm{OA}(m, k, q, t)$ and let R be an $\mathrm{OA}(n, k, q, t)$. Then $L = C \boxplus R$ is an array of type $I_k(m, n, q, t)$ if and only if L is a row-column factorial design, that is, the multiset of entries of the cells of L is the $\lambda \times [q]^k$ factorial design.*

We next consider the extreme case when every row is a factorial design.

Lemma 5.11. *If there exists an orthogonal array $\mathrm{OA}(m, k, q, t)$ then there exists an array of type $I_k(m, q^k, q, t)$.*

Proof. Let R be an $\mathrm{OA}(q^k, k, q, t)$ where $t \leq k$ and the row vectors of R are the factorial design $[q]^k$. Let C be an $\mathrm{OA}(m, k, q, t)$. Since the entries in each row of $C \boxplus R$ are trivially $[q]^k$, by the previous lemma $C \boxplus R$ is an array of type $I_k(m, q^k, q, t)$. □

In the following, given a matrix A over the field $\mathbb{F}_q$, let $\langle A \rangle$ be a matrix whose row vectors are the row space of A; that is the vector space generated by the row vectors of A. An orthogonal array is called *linear* if its rows form a vector space (assuming without loss of generality that the zero vector is one of the rows). The theory of linear orthogonal arrays is closely related to that of linear codes; see for example Section 4.3 of [8].

The following lemma is in some ways a standard result in this area, stemming from the original result by Bose (1961) [1] which links the two theories. This lemma is also implied by Theorem 3.27 and Theorem 3.29 in [8]. We include a proof for thoroughness.

Henceforth we say that a set S of vectors is *t-independent* if every t-subset of S is linearly independent [5].

Lemma 5.12. *Let A be an $m \times n$ matrix of rank m over the field $\mathbb{F}_q$ where $m \leq n$. Let $2 \leq t \leq m$. Then $\langle A \rangle$ is an $\mathrm{OA}(q^m, n, q, t)$ if and only if the set of columns of A is t-independent.*

Proof. Let C be a subset of t distinct column vectors of A. Let B be the $m \times t$ sub-matrix which is A restricted to these columns.

If C is a dependent set, there exists a non-zero vector $\mathbf{w}$ such that $B\mathbf{w} = \mathbf{0}$. Then, by the fundamental theorem of linear algebra, the vector $\mathbf{w}$ does not occur in $\langle B \rangle$. In turn, within the set of vectors of $\langle A \rangle$, within the t positions determined by the columns of C, the ordered sequence $\mathbf{w}$ does not occur. Thus $\langle A \rangle$ does not have strength t.

Conversely, suppose that C is an independent set. Let $\mathbf{w} \in \mathbb{F}_q^t$. Since B has rank t, there are q^{m-t} vectors $\mathbf{v}$ such that $B\mathbf{v} = \mathbf{w}$. In turn, within the set of vectors of $\langle A \rangle$, within the t positions determined by the columns of C, each element of $(\mathbb{F}_q)^t$ occurs q^{m-t} times. □

Corollary 5.13. *Let K be a binary $m \times (n-m)$ matrix. Then $\langle [I \mid K] \rangle$ is an $\mathrm{OA}(2^m, n, 2, 2)$ if and only if the columns of K are distinct* and *each column of K contains at least 2 non-zero elements.*

Example 5.14. From the previous corollary, $\langle A \rangle$ is an $\mathrm{OA}(2^6, 8, 2, 2)$:

$$A = \left(\begin{array}{cccccc:cc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{array}\right)$$

Theorem 5.15. *Let G be an $m \times k$ matrix and let A be an $N \times k$ matrix of full rank, each over the field $\mathbb{F}_q$ where $N \leq k$. Let $A^{\perp}$ be a $k \times (k-N)$ matrix the columns of which are a basis for the nullspace of A. Then $G \boxplus \langle A \rangle$ is an $m \times q^N$ row-column factorial design if and only if $GA^{\perp}$ is an $\mathrm{OA}(m, k-N, q, k-N)$.*

Proof. Let $M = G \boxplus \langle A \rangle$ and let $\mathbf{v_i} \in \mathbb{F}_q^k$ denote the i^{th} row vector of G. Then the elements of the i^{th} row of M form the coset $\mathbf{v_i} + \langle A \rangle$ of $\langle A \rangle$ in $\mathbb{F}_q^k$. Note that $\langle A \rangle$ has exactly q^{k-N} distinct cosets in $\mathbb{F}_q^k$. We show that each of these cosets appears the same number of times as a set of entries in a row of M. To this end, observe that for $1 \leq i, j \leq m$:

$$\mathbf{v_i} + \langle A \rangle = \mathbf{v_j} + \langle A \rangle \iff \mathbf{v_i} - \mathbf{v_j} \in \langle A \rangle \iff \mathbf{v_i}A^{\perp} = \mathbf{v_j}A^{\perp}.$$

Thus the set of entries in two rows of M are identical if and only if the corresponding rows in $GA^{\perp}$ are identical. Thus M is a row-column factorial design (that is, the set of entries of M form a factorial design) if and only if each element of $(\mathbb{F}_q)^{k-N}$ occurs the same number of times as a row of $GA^{\perp}$. In turn, this is true if and only if $GA^{\perp}$ is an $\mathrm{OA}(m, k-N, q, k-N)$. □

Theorem 5.16. *Let G be an $\mathrm{OA}(m, k, q, t)$ and let $\langle A \rangle$ be an $\mathrm{OA}(q^N, k, q, t)$ where A is an $N \times k$ matrix of full rank and $N \leq k$. Let $A^{\perp}$ be a $k \times (k-N)$ matrix whose columns generate the nullspace of A. If $GA^{\perp}$ is an $\mathrm{OA}(m, k-N, q, k-N)$, then $G \boxplus \langle A \rangle$ is an array of type $I_k(m, q^N, q, t)$.*

Proof. Let $M = G \boxplus \langle A \rangle$. The result follows from Theorem 5.15 and Lemma 5.10. □

In the next example (and in Section 5) we make use of the result (well-known to coding theorists) that over any field, the nullspace of the matrix $[I \mid K]$ is equal to the columnspace of the matrix $[-K^T \mid I]^T$ (Remark 1.5, [4, p. 677]).

Example 5.17. We continue with Example 5.14 to show that $G \boxplus \langle A \rangle$ is an $I_8(12, 2^6, 2, 2)$, using Theorem 5.16 the following $G = \mathrm{OA}(12, 8, 2, 2)$.

$$A^{\perp} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \quad G = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \end{pmatrix} \quad GA^{\perp} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \\ 1 & 1 \\ 0 & 0 \\ 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$$

The following is a generalization of Theorem 5 in [13].

Theorem 5.18. *Let q be a prime power. Let $M, N \geq 1$ and $k \leq M + N$. Suppose there exists a $k \times M$ matrix A and a $k \times N$ matrix B such that:*

(a) *the $k \times (M + N)$ matrix $[A \mid B]$ has rank k;*

(b) *the rows of A are a t-independent set of vectors; and*

(c) *the rows of B are a t-independent set of vectors.*

Then there exists an abelian array of type $I_k(q^M, q^N, q, t)$.

Proof. Assuming the conditions of the theorem, the rows of $[A \mid B]$ are a linearly independent set of k vectors:

$$(a_{r,0} + a_{r,1} + \cdots + a_{r,M+N-1});\ r \in [k] \tag{5.1}$$

in the vector space $\mathbb{F}_q^{M+N}$ such that:

(i) The set of vectors $\{(a_{r,0}, ..., a_{r,M-1}) : r \in [k]\}$ is t-independent; and

(ii) the set of vectors $\{(a_{r,M}, ..., a_{r,M+N-1}) : r \in [k]\}$ is t-independent.

Corresponding to each vector in (5.1) we construct a $q^M \times q^N$ array A_r by using a polynomial f_r, where

$$f_r(x_0, ..., x_{M+N-1}) = a_{r,0}x_0 + \cdots + a_{r,M+N-1}x_{M+N-1}.$$

Label the rows and columns of A_r by using the set of all M-tuples and N-tuples, respectively, over the field $\mathbb{F}_q$. We place the element $f(b_0, ..., b_{M-1}, c_0, ..., c_{N-1})$ in the intersection of row $(b_0, ..., b_{M-1})$ and column $(c_0, ..., c_{N-1})$ of the array A_r.

We next form an array D by overlapping the arrays A_r, $r \in [k]$. That is, cell (i, j) of D contains a vector of dimension k the rth coordinate of which is the entry of cell (i, j) of A_r. We claim that the array D is an $I_k(q^M, q^N, q, t)$.

We first show that D is an array of strength t. Let T be a subset of $[k]$ of size t and consider a sequence $(\alpha_1, \ldots, \alpha_t)$ in $[q]^t$. For a fixed column in D, the system of equations

$$f_r(x_0, \ldots, x_{M+N-1}) = \alpha_r; \qquad r \in T$$

reduces to:

$$a_{r,0}x_0 + a_{r,1}x_1 + \cdots + a_{r,M-1}x_{M-1} = \alpha_r + K_r; \qquad r \in T$$

where K_r is a constant in $\mathbb{F}_q$ for each $r \in T$.

By condition (i), the above system with M variables has rank t. Therefore it has exactly q^{M-t} solutions in $\mathbb{F}_q$. Thus each column of D is an orthogonal array of type $\mathrm{OA}(q^M, k, q, t)$. Similarly, we can show that each row of D also forms an orthogonal array of type $\mathrm{OA}(q^N, k, q, t)$. Hence the strength t condition is satisfied.

Now to show that D is a q^k-full factorial design. Consider a sequence $(\alpha_0, \alpha_1, \ldots, \alpha_{k-1})$ in $\mathbb{F}_q^k$. Since the system of equations:

$$a_{r,0}x_0 + a_{r,1}x_1 + \cdots + a_{r,M+N-1}x_{M+N-1} = \alpha_r, \qquad r \in [k],$$

has $M + N$ variables and rank k, it has exactly q^{M+N-k} solutions in $\mathbb{F}_q$. Thus each sequence in $\mathbb{F}_q^k$ appears exactly q^{M+N-k} times in D. $\square$

5.5 Strength 2 with arbitrary number of levels

In this section we consider row-column factorial designs of the form $I_k(q^M, q^N, q, 2)$. We aim to prove the following theorem.

Theorem 5.19. *Let $2 \leq M \leq N$, let q be a prime power and let $k \geq 2$. Then there exists an array of type $I_k(q^M, q^N, q, 2)$ if and only if $k \leq M + N$, $k \leq (q^M - 1)/(q - 1)$ and $(k, M, q) \neq (3, 2, 2)$.*

Lemma 5.8 and the previous theorem imply the following corollary.

Corollary 5.20. *Let $q_1 \leq q_2 \leq \cdots \leq q_\alpha$ be powers of distinct primes and $(k, M, q_1) \neq (3, 2, 2)$. Let $q = q_1 q_2 \ldots q_\alpha$, $k \leq (q_1^M - 1)/(q - 1)$, $2 \leq M \leq N$ and $2 \leq k \leq M + N$. Then there exists an array of type $I_k(q^M, q^N, q, 2)$.*

The elements of $[2]^2$ form the rows of an $\mathrm{OA}(4, 2, 2, 2)$. In turn, Lemma 5.11 implies the existence of $I_2(4, 4, 2, 2)$. This observation, together with the following two lemmas and Theorem 5.18, will imply the Theorem 5.19.

Lemma 5.21. *Let $N \geq M \geq 2$ be integers and $q \geq 2$ be a prime power, with $M + N \leq (q^M - 1)/(q - 1)$ and $(M, q) \neq (2, 2)$. Then there exists an $(M + N) \times M$ matrix A and an $(M + N) \times N$ matrix B such that:*

(a) *$[A \mid B]$ has full rank;*

(b) *no two rows of A are parallel; and*

(c) *no two rows of B are parallel.*

Proof. We split the proof in different cases. In each case we describe a square matrix $L = [A \mid B]$ with the required properties.

Case I: When $M = 3$ and $q = 2$.

In this case, $3 \leq N \leq 4$. For $N = 4$ we define the matrix L to be,

$$L = \left(\begin{array}{ccc|ccc:c} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ \hdashline 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \tag{5.2}$$

The above matrix has full rank over $\mathbb{F}_2$ and also satisfies the conditions (b) and (c). Now for the case $N = 3$, we can take the 6×6 sub-matrix (as shown in (5.2)) of the above matrix obtained by deleting the final row and column. Observe that this matrix also has full rank and satisfies the conditions in the lemma.

For all other cases, we take L to be of the form:

$$L = \left(\begin{array}{c|c:c} I_M & I_M & \mathbf{O} \\ \hdashline C_M - I_M & C_M & \mathbf{O} \\ \hdashline S & \mathbf{O} & I_{N-M} \end{array}\right) \tag{5.3}$$

Where I_M is an identity matrix of order M and $\mathbf{O}$ is a matrix of zeroes of appropriate size. Matrices C_M and S are to be defined later.

Label the columns of the matrix L in (5.3) by $c_i,\ i \in [M+N]$. Note that for any choices of matrices C_M and S, the column operations;

$$c_{M+i} - c_i \longrightarrow c_{M+i}, \quad \text{for each} \quad i \in [M], \tag{5.4}$$

transfers the matrix L into a lower triangular matrix with entry 1 on the main diagonal. Thus condition (a) is satisfied for any choice of C_M and S.

Case II: When $M \geq 4$.

In this case let C_M be a $M \times M$ matrix with exactly one 0 in each row and column, 1's on the main diagonal and 1's in every other cell. Observe that

condition (c) is satisfied. Let D be the set of all rows in I_M and $C_M - I_M$. It is easy to see that no two vectors in D are parallel. Let W be the largest set of non-parallel vectors in $\mathbb{F}_q^M$ containing D. Then $|W| = (q^M - 1)/(q - 1) \geq M + N$. We define S to be the matrix each of whose row is a distinct element in $W \setminus D$. Thus condition (b) is satisfied.

In the remaining cases the matrix S can be obtained in the similar manner from the corresponding C_M, again satisfying condition (b).

Case III: When $2 \leq M \leq 3$ and q is odd.

In this case we define the matrices $C_M, M \in \{2, 3\}$ to be:

$$C_2 = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix} \quad \text{and} \quad C_3 = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}.$$

Case IV: When $M = 3$ and $q = 2^l,\ l \geq 2$.

In this case we define C_3 as follows.

$$C_3 = \begin{pmatrix} \alpha + 1 & 1 & 1 \\ 1 & \alpha + 1 & 1 \\ 1 & 1 & \alpha + 1 \end{pmatrix},$$

where α is a primitive element of the field $\mathbb{F}_q$. □

Lemma 5.22. *If b is odd, there does not exist an array of type $I_3(4, 4b, 2, 2)$.*

Proof. Suppose that an array D exists of type $I_3(4, 4b, 2, 2)$. Then each column of D is an $\mathrm{OA}(4, 3, 2, 2)$. By inspection, the vectors in any column of D are either all the vectors of even weight or all the vectors of odd weight; we refer to these columns as type A or B, respectively.

A
000
101
011
110

B
001
100
010
111

Since the vectors in A and B form a partition of $\mathbb{F}_2^3$ and the entries of D form a factorial design, D must contain exactly $2b$ columns of each type.

Now consider a row R in D; by permuting columns we may assume without any loss of generality that the first two coordinates of the entries in R have the following form:

$$\overbrace{00 \quad 00 \quad \dots \quad 00}^{B1} \mid \overbrace{01 \quad 01 \quad \dots \quad 01}^{B2} \mid \overbrace{10 \quad 10 \quad \dots \quad 10}^{B3} \mid \overbrace{11 \quad 11 \quad \dots \quad 11}^{B4}$$

where each Bi has size b. Let x be the number of zeros at the third coordinate in $B1$, then without loss of generality $x \geq (b+1)/2$. By the strength two property, the number of zeros in the third coordinate in $B2, B3$ and $B4$ is $b-x, b-x$ and x respectively. This implies that there are x vectors of type A in each Bi. Consequently, R contains $4x \geq 2b+2$ vectors of type A. This is a contradiction since D contains exactly $2b$ columns of each type. □

5.6 Binary row-column factorial designs of strength 2

In this section we restrict ourselves to the binary case. We exploit the theory developed in Section 3 to give existence results for arrays of the form $I_k(4m, n, 2, 2)$. We focus on the case where m is odd, however the next theorem is also true when m is even. The main results in this section are given in Theorems 5.36, 5.38 and 5.39.

Theorem 5.23. *Let $k \geq 5$. Let $m \geq 3$ be odd and suppose there exists an* $\mathrm{OA}(4m, k, 2, 2)$ *with two subsets of column vectors V and W such that:*

(i) $|V|, |W| \geq 3$*;*

(ii) *there exists $\mathbf{v} \in V \setminus W$ and $\mathbf{w} \in W \setminus V$ such that $V \setminus \{\mathbf{v}\} \neq W \setminus \{\mathbf{w}\}$;*

(iii) $(\sum_{\mathbf{x} \in V} \mathbf{x})$ *is orthogonal to* $(\sum_{\mathbf{y} \in W} \mathbf{y})$.

Then there exists an abelian $I_k(4m, 2^{k-2}, 2, 2)$.

Proof. Observe that the conditions (i) and (ii) imply $k \geq 5$. Let G be an $\mathrm{OA}(4m, k, 2, 2)$ satisfying the conditions of the theorem. Let $G = [\mathbf{v}_1|\mathbf{v}_2|\ldots|\mathbf{v}_k]$. Without loss of generality, assume that $\mathbf{v}_{k-1} \in V \setminus W$ and $\mathbf{v}_k \in W \setminus V$. Define a $(k-2) \times 2$ matrix K over $\mathbb{F}_2$ such that the first column of K contains a 1 in the jth row if and only if $\mathbf{v}_j \in V$. Similarly, the second column of K contains a 1 in the jth row if and only if $\mathbf{v}_j \in W$. Observe furthermore that $[K^T \mid I]^T$ has the same property.

Next, let A be the $(k-2) \times k$ matrix defined by $A = [I \mid K]$. If the columns of K are identical, then $V \setminus \{\mathbf{v}\} = W \setminus \{\mathbf{w}\}$, a contradiction. Moreover, since $|V|, |W| \geq 3$, the columns of K each have at least two 1's. Thus, by Corollary 5.13, $\langle A \rangle$ is an $\mathrm{OA}(2^{k-2}, k, 2, 2)$.

Define $A^\perp = [K^T \mid I]^T$. Observe that $GA^\perp$ is a $4m \times 2$ matrix with columns given by $\sum_{\mathbf{x} \in V} \mathbf{x}$ and $\sum_{\mathbf{y} \in W} \mathbf{y}$. By definition, $GA^\perp$ is an $\mathrm{OA}(4m, 2, 2, 2)$. Thus, by Theorem 5.16, $G \boxplus \langle A \rangle$ is an $I_k(4m, 2^{k-2}, 2, 2)$. □

Now, observe that the matrix G from Example 5.17 is an $\mathrm{OA}(12, 8, 2, 2)$ with the property that $\mathbf{v}_1+\mathbf{v}_3+\mathbf{v}_4+\mathbf{v}_6+\mathbf{v}_7$ is orthogonal to $\mathbf{v}_2+\mathbf{v}_3+\mathbf{v}_5+\mathbf{v}_6+\mathbf{v}_8$. Moreover, G embeds in the Hadamard matrix $H(12)$ of order 12 (`had.12`, [15]). Thus we have the following corollary.

Corollary 5.24. *There exists an abelian* $I_k(12, 2^{k-2}, 2, 2)$ *where* $8 \leq k \leq 11$.

Corollary 5.25. *There exists an abelian* $I_k(20, 2^{k-2}, 2, 2)$ *where* $8 \leq k \leq 19$.

Proof. The following is a transpose of an $\mathrm{OA}(20, 8, 2, 2)$ which has the property that $\mathbf{v}_1 + \mathbf{v}_3 + \mathbf{v}_4 + \mathbf{v}_6 + \mathbf{v}_7$ is orthogonal to $\mathbf{v}_2 + \mathbf{v}_3 + \mathbf{v}_5 + \mathbf{v}_6 + \mathbf{v}_8$. The result follows by Theorem 5.23.

$$\left[\begin{array}{cccccccccccccccccc}
1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1
\end{array}\right]$$

The above array consists of columns 2 to 9 of the Hadamard matrix (`had.20.toncheviv`, [15]) with the permutation $(2\ \ 4)(5\ \ 7)(3\ \ 8\ \ 6\ \ 9)$ applied to its columns. □

Corollary 5.26. *For any odd $m \geq 3$, there exists an $I_k(4m, 2^{k-2}, 2, 2)$ where $8 \leq k \leq 11$.*

Proof. By Theorem 5.19 there exists an $I_k(16, 2^{k-2}, 2, 2)$ where $8 \leq k \leq 15$. Thus the result follows by previous two corollaries and Lemma 5.7. □

Via a counting argument, Theorem 5.23 cannot work for m odd if $k \leq 6$. We outline this argument in the conclusion in Lemma 5.47. Moreover, computational results show that $k = 7$ does not work in the cases $m \in \{3, 5\}$.

The above and Theorem 5.23 thus motivate the following conjecture, which is stronger than the Hadamard conjecture.

Conjecture 5.27. *For each odd m, there exists a Hadamard matrix $4m$ which yields an orthogonal array $\mathrm{OA}(4m, 8, 2, 2)$ satisfying the conditions of Theorem 5.23.*

If the above conjecture is true, then by Theorem 5.23, there exists an $I_k(4m, 2^{k-2}, 2, 2)$ for any $8 \leq k \leq 4m - 1$.

We next focus on a strategy for the case $k \leq 7$. Our constructions are typically non-abelian. In the following, $\oplus$ is a binary operation that gives the concatenation of two vectors. That is,

$$(a_1, a_2, \ldots, a_r) \oplus (b_1, b_2, \ldots, b_s) = (a_1, a_2, \ldots, a_r, b_1, b_2, \ldots, b_s).$$

The following lemma is implied by the definition of an orthogonal array. Note that $\mathbf{1}$ is the vector containing only 1's.

Lemma 5.28. *Consider a set S of 2^k binary vectors of dimension $k+2$ with the following properties:*

- *For each $\mathbf{v} \in [2]^k$, the vector $\mathbf{v} \oplus (i,j) \in S$, for some $i,j \in [2]$;*
- *For each $(i,j) \in [2]^2$, there are precisely 2^{k-2} vectors in S of the form $\mathbf{v} \oplus (i,j)$ for some $\mathbf{v}$;*
- *The vector $\mathbf{v} \oplus (i,j) \in S$ if and only if $(\mathbf{1}+\mathbf{v}) \oplus (i,j) \in S$.*

Then the vectors of S are the rows of an $\mathrm{OA}(|S|, k+2, 2, 2)$.

Lemma 5.29. *Let $\{\mathbf{w}, \mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{1}\}$ be a set of linearly independent binary vectors of dimension $k \geq 5$. Consider the 4×2^k array of vectors of dimension $k+2$ given by $C \boxplus R$, where R is the set of 2^k vectors with 0 in the final two positions and*

$$C = (\mathbf{w} \oplus (0,0), \mathbf{x} \oplus (0,1), \mathbf{y} \oplus (1,0), \mathbf{z} \oplus (1,1))^T.$$

Then the elements in each column of $C \boxplus R$ can be rearranged so that each row is an $\mathrm{OA}(2^k, k+2, 2, 2)$.

Proof. Observe that H is a 4×8 subarray of $C \boxplus R$:

$$H = \begin{array}{|c|c|c|c|c|c|c|c|} \hline \mathbf{w} & \mathbf{x} & \mathbf{y} & \mathbf{z} & \mathbf{t} & \mathbf{u} & \mathbf{s} & \mathbf{v} \\ \hline \mathbf{x} & \mathbf{w} & \mathbf{t} & \mathbf{u} & \mathbf{y} & \mathbf{z} & \mathbf{v} & \mathbf{s} \\ \hline \mathbf{y} & \mathbf{t} & \mathbf{w} & \mathbf{s} & \mathbf{x} & \mathbf{v} & \mathbf{z} & \mathbf{u} \\ \hline \mathbf{z} & \mathbf{u} & \mathbf{s} & \mathbf{w} & \mathbf{v} & \mathbf{x} & \mathbf{y} & \mathbf{t} \\ \hline \end{array},$$

where $\mathbf{s} = \mathbf{w}+\mathbf{y}+\mathbf{z}$, $\mathbf{t} = \mathbf{w}+\mathbf{x}+\mathbf{y}$, $\mathbf{u} = \mathbf{w}+\mathbf{x}+\mathbf{z}$, $\mathbf{v} = \mathbf{x}+\mathbf{y}+\mathbf{z}$ and the vectors in the first, second, third and fourth rows are concatenated with $(0,0)$, $(0,1)$, $(1,0)$ and $(1,1)$, respectively.

Next, let H' be the 4×8 array formed by replacing each vector $\mathbf{a}$ in H with the vector $\mathbf{a} + (\mathbf{1} \oplus (0,0))$. We next arrange the entries in each column of $[H \mid H']$. We mark the elements of H as follows:

$$H = \begin{array}{|c|c|c|c|c|c|c|c|}\hline \underline{\mathbf{w}} & \mathbf{x}^{\circ} & \mathbf{y}^{*} & \mathbf{z} & \mathbf{t} & \mathbf{u}^{*} & \mathbf{s}^{\circ} & \underline{\mathbf{v}} \\ \hline \mathbf{x}^{*} & \mathbf{w} & \underline{\mathbf{t}} & \mathbf{u}^{\circ} & \mathbf{y}^{\circ} & \underline{\mathbf{z}} & \mathbf{v} & \mathbf{s}^{*} \\ \hline \mathbf{y} & \mathbf{t}^{*} & \mathbf{w}^{\circ} & \underline{\mathbf{s}} & \underline{\mathbf{x}} & \mathbf{v}^{\circ} & \mathbf{z}^{*} & \mathbf{u} \\ \hline \mathbf{z}^{\circ} & \underline{\mathbf{u}} & \mathbf{s} & \mathbf{w}^{*} & \mathbf{v}^{*} & \mathbf{x} & \underline{\mathbf{y}} & \mathbf{t}^{\circ} \\ \hline \end{array}.$$

Next, rearrange the elements in each column of H so that elements with the same mark are in the same row, with a corresponding permutation applied to each column of H'. Let the resultant 4×16 matrix be J.

Now, replace each vector of the form $\mathbf{a}$ in J with the vector $(\mathbf{v} \oplus (0,0)) + \mathbf{a}$ to obtain a 4×16 matrix J'. Observe that for each row of $K = [J \mid J']$ and for each $\mathbf{g} \in G = \langle \mathbf{w}, \mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{1} \rangle$, there exists i and j such that $\mathbf{g} \oplus (i,j)$ is in that row. Moreover, each column from K is a column from $C \boxplus R$ with elements permuted.

Let G, $\mathbf{z}_0 + G, \ldots, \mathbf{z}_{\alpha-1} + G$ be the cosets of G in $(\mathbb{F}_2)^k$, where $\alpha = 2^{k-5}$. For each $i \in [\alpha]$, let K_i be formed from K by replacing each entry $\mathbf{a}$ of K with $(\mathbf{z}_i \oplus (0,0)) + \mathbf{a}$.

Then, observe that $[K_0 \mid K_1 \mid \cdots \mid K_\alpha]$ can be formed from $C \boxplus R$ by permuting the elements in each column. Moreover, the resultant rows each now satisfy the conditions of Lemma 5.28. □

Example 5.30. Let $\mathbf{w} = 10000, \mathbf{x} = 10111, \mathbf{y} = 01101$, and $\mathbf{z} = 01011$. Then H and H' in the proof of above lemma are as follows:

$$H = \begin{array}{|c|c|c|c|c|c|c|c|}\hline \underline{1000000} & 1011100^{\circ} & 0110100^{*} & 0101100 & 0101000 & 0110000^{*} & 1011000^{\circ} & \underline{1000100} \\ \hline 1011101^{*} & 1000001 & \underline{0101001} & 0110001^{\circ} & 0110101^{\circ} & \underline{0101101} & 1000101 & 1011001^{*} \\ \hline 0110110 & 0101010^{*} & 1000010^{\circ} & \underline{1011010} & \underline{1011110} & 1000110^{\circ} & 0101110^{*} & 0110010 \\ \hline 0101111^{\circ} & \underline{0110011} & 1011011 & 1000011^{*} & 1000111^{*} & 1011111 & \underline{0110111} & 0101011^{\circ} \\ \hline \end{array}$$

$$H' = \begin{array}{|c|c|c|c|c|c|c|c|}\hline \underline{0111100} & 0100000^{\circ} & 1001000^{*} & 1010000 & 1010100 & 1001100^{*} & 0100100^{\circ} & \underline{0111000} \\ \hline 0100001^{*} & 0111101 & \underline{1010101} & 1001101^{\circ} & 1001001^{\circ} & \underline{1010001} & 0111001 & 0100101^{*} \\ \hline 1001010 & 1010110^{*} & 0111110^{\circ} & \underline{0100110} & \underline{0100010} & 0111010^{\circ} & 1010010^{*} & 1001110 \\ \hline 1010011^{\circ} & \underline{1001111} & 0100111 & 0111111^{*} & 0111011^{*} & 0100011 & \underline{1001011} & 1010111^{\circ} \\ \hline \end{array}.$$

Corollary 5.31. *Let $G = \mathrm{OA}(4m, k+2, 2, 2)$ be an orthogonal array such that the rows partition into sets of 4 vectors of the form*

$$\{\mathbf{w} \oplus (0,0), \mathbf{x} \oplus (0,1), \mathbf{y} \oplus (1,0), \mathbf{z} \oplus (1,1)\}$$

where $\{\mathbf{w}, \mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{1}\}$ is a linearly independent set. Let R be the set of 2^k vectors with 0 in the final two positions. Then the elements in each column of $G \boxplus R$ can be rearranged to create an $I_{k+2}(4m, 2^k, 2, 2)$.

Proof. From the previous lemma it suffices to check that $G \boxplus R$ is a factorial design. Let A be a $k \times (k+2)$ matrix of the form $[I \mid \mathbf{0}]$. Observe that $R = \langle A \rangle$. The nullspace of A is generated by the columns of $A^{\perp} = [\mathbf{0} \mid I]^T$. Thus the columns of $GA^{\perp}$ are the last two columns of G which are by definition orthogonal. The result then follows from Theorem 5.15. □

Corollary 5.32. *There exists $I_7(12, 32, 2, 2)$.*

Proof. We present an orthogonal array of type $\mathrm{OA}(12, 7, 2, 2)$ in Table 5.2, that satisfies the conditions of Corollary 5.31. The dashed lines partition the rows into three sets of the form $\{\mathbf{w} \oplus (0,0), \mathbf{x} \oplus (0,1), \mathbf{y} \oplus (1,0), \mathbf{z} \oplus (1,1)\}$ such that in each case $\{\mathbf{w}, \mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{1}\}$ is linearly independent.

$$\left(\begin{array}{ccccc:cc}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 1 & 1 \\
\hdashline
1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 1 & 1 \\
\hdashline
0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1
\end{array}\right)$$

Table 5.2: An orthogonal array of type $\mathrm{OA}(12, 7, 2, 2)$.

□

We next generalize the above ideas to the case where linear independence is not assumed.

Lemma 5.33. *Let $m = 2^\alpha$ where $\alpha \geq 2$ and $(\mathbb{F}_2)^\alpha = \{\mathbf{e}_i \mid i \in [m]\}$. That is, label the binary vectors of dimension α with $\mathbf{e}_0$, $\mathbf{e}_1, \ldots \mathbf{e}_{m-1}$. Let $\mathbf{v}_i$, $i \in [m]$ be any vectors (possibly non-distinct) of dimension $k \geq \alpha + m + 1$. Consider the $m \times 2^k$ array of vectors of dimension $k + \alpha$ given by $C \boxplus R$, where the rows of R are the set of 2^k vectors with 0 in the final α positions and the ith row of C is given by $\mathbf{v}_i \oplus \mathbf{e}_i$, where $i \in [m]$. Then the elements in each column of $C \boxplus R$ can be rearranged so that the vectors in each row form an $\mathrm{OA}(2^k, k + \alpha, 2, 2)$.*

Proof. r in Let $\mathbf{e}_0 = \mathbf{0}$ be the first row of R. Let G be the subgroup generated

by the set of vectors $\{\mathbf{v}_i : i \in [m]\} \cup \{\mathbf{1}\}$. Then $|G| = 2^\ell$ for some $1 \leq \ell \leq m+1$. Let $G = \{\mathbf{g}_i \mid i \in [2^\ell]\}$ where $\mathbf{g}_0 = \mathbf{0}$. Define a $2^\ell \times (k+\alpha)$ array R_0 so that row i of R_0 is $\mathbf{g}_i \oplus \mathbf{0}$, $i \in [2^\ell]$. Let K_0 be the $m \times 2^\ell$ array of vectors of dimension $k+\alpha$ given by $C \boxplus R_0$.

Next, let $\mathbf{z}_0 + G$, $\mathbf{z}_1 + G, \ldots, \mathbf{z}_{\beta-1} + G$ be the cosets of G in $(\mathbb{F}_2)^k$, where $\beta = 2^{k-\ell}$. For each $j \in [\beta]$, let K_j be formed from K_0 by adding $\mathbf{z}_j \oplus \mathbf{0}$ to each vector in K_0. Next, cyclically permute the elements in each column of K_j by j places (modulo m) to create K'_j.

Note that $L = [K'_0 \mid K'_1 \mid \cdots \mid K'_{\beta-1}]$ is equal to $C \boxplus R$ after a permutation of the elements in each column. Moreover, let S be the set of vectors of dimension $k+\alpha$ that occur in a given row of L. Then we claim the following:

(a) For each $\mathbf{w} \in [2]^k$, the vector $\mathbf{w} \oplus \mathbf{e}_i \in S$, for some $\mathbf{e}_i \in (\mathbb{F}_2)^\alpha$;

(b) For each $\mathbf{e}_i \in (\mathbb{F}_2)^\alpha$, there are precisely $2^{k-\alpha}$ vectors in S of the form $\mathbf{w} \oplus \mathbf{e}_i$ for some $\mathbf{w}$;

(c) For each $\mathbf{e}_i \in (\mathbb{F}_2)^\alpha$, the vector $\mathbf{w} \oplus \mathbf{e}_i \in S$ if and only if $(\mathbf{w}+\mathbf{1}) \oplus \mathbf{e}_i \in S$.

Similarly to Lemma 5.28, if this claim is true, it follows that the set of vectors in S form the rows of an orthogonal array of strength 2. So it suffices to show that the above claim is true.

To see (a), let $j \in [\beta]$. Observe that in every row of K_j and for every element $\mathbf{w} \in \mathbf{z}_j + G$, the vector $\mathbf{w} \oplus \mathbf{e}_i$ occurs in that row. The same property holds for K'_j. Next, from the conditions of the lemma, $\beta \geq m$; indeed m divides β. Thus (b) is true. Finally (c), is true because $\mathbf{1} \in G$. □

Corollary 5.34. *Let $\alpha \geq 2$ and $2^\alpha + \alpha + 1 \leq k$. Suppose there exists an $\mathrm{OA}(2^\alpha b, k+\alpha, 2, 2)$ such that the last α columns are an $\mathrm{OA}(2^\alpha b, \alpha, 2, \alpha)$. Then $I_{k+\alpha}(2^k, 2^\alpha b, 2, 2)$ exists.*

Proof. We shall construct the transpose design $I_{k+\alpha}(2^\alpha b, k, 2, 2)$. Let C be an $\mathrm{OA}(2^\alpha b, k+\alpha, 2, 2)$ such that the last α columns are an $\mathrm{OA}(2^\alpha b, \alpha, 2, \alpha)$. Note that C can be partitioned into subarrays C_0, $C_1, \ldots, C_{b-1}$, each of dimension

$2^\alpha \times (k+\alpha)$, such that for each $i \in [b]$, the last α columns of C_i contain each element of $(\mathbb{F}_2)^\alpha$ exactly once.

Next, let A be the $k \times (k+\alpha)$ matrix of the form $[I \mid \mathbf{0}]$ and let R be an orthogonal array whose rows are the elements of $\langle A \rangle$. Observe that the rows of R are the set of 2^k vectors with 0 in the final α positions. Moreover, the nullspace of A is generated by the columns of $A^\perp = [\mathbf{0} \mid I]^T$. Thus the columns of $CA^\perp$ are the last α columns of C.

Thus, by Theorem 5.15, $C \boxplus R$ is a row-column factorial design. Moreover, the columns of $C \boxplus R$ are each of strength 2 since C is of strength 2. Finally, apply the previous lemma with $m = 2^\alpha$ to rearrange the elements in each column of subarray $C_i \boxplus R$ so that $C \boxplus R$ becomes an $I_{k+\alpha}(2^\alpha b, 2^k, 2, 2)$ $\square$

The following lemma uses a standard doubling technique.

Lemma 5.35. *Suppose there exists a Hadamard matrix of order $4b$ for some integer b. Let $\alpha \geq 2$. Then there exists an $\mathrm{OA}(2^\alpha b, k+\alpha, 2, 2)$ such that the final α columns form an $\mathrm{OA}(2^\alpha b, \alpha, 2, \alpha)$, for any $\alpha \leq k+\alpha < 2^\alpha b$.*

Proof. We proceed by induction on α. Suppose $\alpha = 2$. The existence of a Hadamard matrix of order $4b$ implies the existence of an $\mathrm{OA}(4b, k+2, 2, 2)$ for any $k+2 \leq 4b-1$ by Lemmas 5.3 and 5.6. By the definition of the strength of an orthogonal array, the final two columns must contain each ordered pair b times, so the final two columns form an $\mathrm{OA}(4b, 2, 2, 2)$.

Next assume that the lemma is true for a fixed value of $\alpha \geq 2$. then there exists an $L = \mathrm{OA}(2^\alpha b, 2^\alpha b - 1, 2, \alpha)$ with the specified properties. Observe that the following matrix L' is an $\mathrm{OA}(2^{\alpha+1}b, 2^{\alpha+1}b-1, 2, 2)$:

$$L' = \left[\begin{array}{c|c|c} L & L & \mathbf{1} \\ \hline \overline{L} & L & \mathbf{0} \end{array}\right],$$

where $\overline{L}$ is formed from L by replacing each 0 with 1. Moreover, the final $\alpha+1$ columns of L' contain each binary sequence of dimension $\alpha+1$ exactly once. Thus the final $\alpha+1$ columns form an $\mathrm{OA}(2^{\alpha+1}b, \alpha+1, 2, \alpha+1)$. Hence an $\mathrm{OA}(2^{\alpha+1}b, k+\alpha+1, 2, \alpha+1)$ can be obtained for any k such that $k+\alpha+1 < 2^{\alpha+1}b$ by deletion of columns. This completes the induction and the proof. $\square$

From the previous lemma and Corollary 5.34, we have the following.

Theorem 5.36. *If there exists a Hadamard matrix $H(4b)$, then there exists $I_{k+\alpha}(2^\alpha b, 2^k, 2, 2)$ for any $2 \leq \alpha$; $2^\alpha + \alpha + 1 \leq k < 2^\alpha b - \alpha$.*

Before we completely deal with the case when m is odd and k is small, we need some constructions for specific parameters.

Lemma 5.37. *There exists $I_5(12, 8, 2, 2)$, $I_6(12, 16, 2, 2)$ and $I_4(12, 12, 2, 2)$.*

Proof. In Table 5.3 we present an abelian array of the form $C \boxplus R$, where R is the rowspace of the 3×5 matrix $[I_3 \mid 0]$ and C is an $\mathrm{OA}(12, 5, 2, 2)$ (constructed from 5 columns of a Hadamard matrix of order 12). Now, the columns of the matrix $C[I_3 \mid 0]^T$ are in turn distinct columns of C; thus $C[I_3 \mid 0]^T$ is an $\mathrm{OA}(12, 3, 2, 2)$. Hence, by Theorem 5.15, $C \boxplus R$ is a row-column factorial design. Moreover, each column is an orthogonal array of strength 2. We can then rearrange the elements in each column to create an $I_5(12, 8, 2, 2)$; the rearrangement is indicated by the use of superscripts. That is, we permute entries within each column so that vectors with the same superscript belong to the same row.

$\mathbf{00000}^A$	$\mathbf{10000}^C$	$\mathbf{01000}^D$	$\mathbf{11000}^B$	$\mathbf{00100}^D$	$\mathbf{10100}^B$	$\mathbf{01100}^A$	$\mathbf{11100}^C$
$\mathbf{00001}^B$	10001^D	01001^C	11001^A	00101^C	10101^A	01101^B	11101^D
$\mathbf{00110}^C$	10110^A	01110^B	11110^D	00010^B	10010^D	01010^C	11010^A
$\mathbf{01011}^D$	11011^B	00011^A	10011^C	01111^A	11111^C	00111^D	10111^B
$\mathbf{01100}^E$	11100^G	00100^F	10100^H	01000^H	11000^F	00000^G	10000^E
$\mathbf{01111}^F$	11111^H	00111^E	10111^G	01011^G	11011^E	00011^H	10011^F
$\mathbf{11001}^G$	01001^E	10001^H	00001^F	11101^F	01101^H	10101^E	00101^G
$\mathbf{11010}^H$	01010^F	10010^G	00010^E	11110^E	01110^G	10110^F	00110^H
$\mathbf{10010}^I$	00010^K	11010^J	01010^L	10110^J	00110^L	11110^I	01110^K
$\mathbf{10101}^J$	00101^L	11101^I	01101^K	10001^I	00001^K	11001^J	01001^L
$\mathbf{10111}^K$	00111^I	11111^L	01111^J	10011^L	00011^J	11011^K	01011^I
$\mathbf{11100}^L$	01100^J	10100^K	00100^I	11000^K	01000^I	10000^L	00000^J

Table 5.3: An array of type $I_5(12, 8, 2, 2)$, with rows indicated by superscripts.

In Table 5.4, first consider the matrix A formed by the first 4 columns. This matrix is abelian of the form $C \boxplus R$, where C is an $\mathrm{OA}(12, 4, 2, 2)$ and R is the rowspace of a 2×4 matrix. By Theorem 5.15 (or inspection if easier), $C \boxplus R$ is a row-column factorial design. Thus $[A \mid A \mid A]$, as shown in Table 5.4, is a row-column factorial design with each column an orthogonal array of strength 2. It thus remains to rearrange the elements within each column so that the rows are each of strength 2. The superscripts A, B, C and D indicate 4 rows of strength 2. The remaining rows are formed by cyclic shifts of each of these by 4 rows and then 8 rows; also indicated by superscripts. This results in the array given in Table 5.5.

$\mathbf{0000}^A$	$\mathbf{0001}^B$	$\mathbf{1111}^C$	$\mathbf{1110}^D$	$\mathbf{0000}^E$	$\mathbf{0001}^F$	$\mathbf{1111}^G$	$\mathbf{1110}^H$	$\mathbf{0000}^I$	$\mathbf{0001}^J$	$\mathbf{1111}^K$	$\mathbf{1110}^L$
$\mathbf{0110}^J$	0111^I	1001^A	1000^B	0110^B	0111^A	1001^E	1000^F	0110^F	0111^E	1001^I	1000^J
$\mathbf{1011}^B$	1010^A	0100^D	0101^C	1011^F	1010^E	0100^H	0101^G	1011^J	1010^I	0100^L	0101^K
$\mathbf{1101}^D$	1100^C	0010^B	0011^A	1101^H	1100^G	0010^F	0011^E	1101^L	1100^K	0010^J	0011^I
$\mathbf{0000}^L$	0001^K	1111^K	1110^L	0000^D	0001^C	1111^C	1110^D	0000^H	0001^G	1111^G	1110^H
$\mathbf{0111}^H$	0110^G	1000^G	1001^H	0111^L	0110^K	1000^K	1001^L	0111^D	0110^C	1000^C	1001^D
$\mathbf{0011}^C$	0010^D	1100^I	1101^J	0011^G	0010^H	1100^A	1101^B	0011^K	0010^L	1100^E	1101^F
$\mathbf{0101}^I$	0100^J	1010^J	1011^I	0101^A	0100^B	1010^B	1011^A	0101^E	0100^F	1010^F	1011^E
$\mathbf{1001}^K$	1000^L	0110^E	0111^F	1001^C	1000^D	0110^I	0111^J	1001^G	1000^H	0110^A	0111^B
$\mathbf{1110}^E$	1111^F	0001^F	0000^E	1110^I	1111^J	0001^J	0000^I	1110^A	1111^B	0001^B	0000^A
$\mathbf{1010}^G$	1011^H	0101^L	0100^K	1010^K	1011^L	0101^D	0100^C	1010^C	1011^D	0101^H	0100^G
$\mathbf{1100}^F$	1101^E	0011^H	0010^G	1100^J	1101^I	0011^L	0010^K	1100^B	1101^A	0011^D	0010^C

Table 5.4: A factorial row-column design with each row strength 2.

0000	**1010**	**1001**	**0011**	**0101**	**0111**	**1100**	**1011**	**1110**	**1101**	**0110**	**0000**
0110	0100	1010	1101	1100	1111	0001	0111	1011	0001	0010	1000
1011	0001	0010	1000	0110	0100	1010	1101	1100	1111	0001	0111
1101	0010	0100	1110	0000	1000	0101	1110	0111	1011	0011	1001
0000	1000	0101	1110	0111	1011	0011	1001	1101	0010	0100	1110
0111	1011	0011	1001	1101	0010	0100	1110	0000	1000	0101	1110
0011	1100	1111	0101	1001	0001	1111	0100	1010	0110	1000	0010
0101	0111	1100	1011	1110	1101	0110	0000	0000	1010	1001	0011
1001	0001	1111	0100	1010	0110	1000	0010	0011	1100	1111	0101
1110	1101	0110	0000	0000	1010	1001	0011	0101	0111	1100	1011
1010	0110	1000	0010	0011	1100	1111	0101	1001	0001	1111	0100
1100	1111	0001	0111	1011	0001	0010	1000	0110	0100	1010	1101

Table 5.5: An array of type $I_4(12, 12, 2, 2)$.

Finally, $I_6(12, 16, 2, 2)$ is given in the Appendix. Similarly to above, this is presented first as an abelian row-column factorial design where each column is of strength 2. The superscripts indicate how to permute the entries within each column. □

We can now give necessary and sufficient conditions for the case when the number of rows is congruent to 4 (mod 8), assuming the truth Conjecture 5.27.

Theorem 5.38. *Let m and b be odd. If Conjecture 5.27 is true, Then $I_k(4m, 2^a b, 2, 2)$ exists if and only if $(k, 4m, 2^a b, 2, 2)$ is admissible and*

$$(k, 4m, 2^a b, 2, 2) \notin \{(3, 4m, 4, 2, 2), (3, 4, 4m, 2, 2) \mid m \text{ is odd}\}.$$

Proof. Since $(k, 4m, 2^a b, 2, 2)$ is admissible, from Lemmas 5.1 and 5.4: $a \geq 2$, $k \leq a + 2$, $k \leq 4m - 1$ and $k \leq 2^a b - 1$.

Case 1: $a = 2$ and $b = 1$. Then $k \leq 3$. Suppose $k = 2$. Now, $[00, 01, 10, 11]^T$ is an OA$(4, 2, 2, 2)$, so by Lemma 5.11, there exists $I_2(4, 4, 2, 2)$.

Thus by Corollary 5.9, $I_2(4m, 4b, 2, 2)$ exists for any integers m and b. Otherwise $k = 3$. By Lemma 5.22, $I_3(4m, 4, 2, 2)$ does not exists for odd m.

Case 2: $a = 2$ and $b \geq 3$. If $m = 1$, this is the transpose of Case 1, so we may assume $m \geq 3$. Thus $k \leq 4$ implies admissibility. From Lemma 5.37, there exist $I_4(12, 12, 2, 2)$ and $I_5(12, 8, 2, 2)$. From Theorem 5.19, $I_6(8, 8, 2, 2)$ exists. In turn, by Lemma 5.6, $I_4(12, 8, 2, 2)$ and $I_4(8, 8, 2, 2)$ exist. By adjoining copies of $I_4(12, 12, 2, 2)$, $I_4(12, 8, 2, 2)$, $I_4(8, 12, 2, 2)$ and $I_4(8, 8, 2, 2)$ as needed using Lemma 5.7, there exists $I_4(4m, 4b, 2, 2)$ for any $m, b \geq 3$.

Case 3: $m = 1$ and $a \geq 3$. Since $m = 1$, $k \leq 3$. Then there exists $I_3(4, 8, 2, 2)$ by Theorem 5.19. Thus there exists $I_3(4, 2^a b, 2, 2)$ for any $a \geq 3$ by Corollary 5.9.

Case 4: $m \geq 3$ and $a \in \{3, 4\}$. Here $k \leq a + 2$ implies admissibility. Now, $I_{a+2}(12, 2^a, 2, 2)$ exists for each $a \in \{3, 4\}$ from Lemma 5.37. Next, $I_6(8, 8, 2, 2)$ exists by Theorem 5.19. Thus by Lemma 5.7, $I_{a+2}(4m, 2^a, 2, 2)$ exists for any odd integer m. In turn, $I_{a+2}(4m, 2^a b, 2, 2)$ exists by Corollary 5.9.

Case 5: $m \geq 3$ and $a = 5$. Then $k \leq 7$ implies admissibility. Now, $I_7(12, 2^5, 2, 2)$ exists by Corollary 5.32. Also, $I_7(8, 2^5, 2, 2)$ exists by Theorem 5.19. Thus by Lemma 5.7 and Corollary 5.9, $I_7(4m, 2^5 b, 2, 2)$ exists for all odd $m \geq 3$ and odd b.

Case 6: $m \geq 3$ and $a \geq 6$. From Corollary 5.26 and assuming the truth of Conjecture 5.27, $I_{a+2}(4m, 2^a, 2, 2)$ exists for all $6 \leq a \leq 4m - 3$. Thus $I_k(4m, 2^a b, 2, 2)$ exists for all $k \leq a + 2$. □

Observe that Conjecture 5.27 is not necessary for the validity of Theorem 5.38 when $a \leq 5$.

Theorem 5.39. *Let $m \leq 5$ and b odd. Then $I_k(4m, 2^a b, 2, 2)$ exists for all admissible*

$$(k, 4m, 2^a b, 2, 2) \notin \{(3, 4m, 4, 2, 2), (3, 4, 4m, 2, 2) \mid m \text{ is odd}\}.$$

Proof. From the previous theorem and the fact that Conjecture 5.27 is true for $m \in \{3, 5\}$, we can assume $m \in \{2, 4\}$.

Let $m = 2$. By Theorem 5.19 there exists $I_3(8, 4, 2, 2)$ and $I_7(8, 8, 2, 2)$. Also there exists $I_5(4b, 8, 2, 2)$ (and thus $I_5(8, 4b, 2, 2)$) by the previous theorem, where $b \geq 3$ is odd. The result then follows by Lemma 5.7 and Corollary 5.9.

Otherwise $m = 4$. Then by Theorem 5.19 there exists $I_3(16, 4, 2, 2)$ and $I_{a+4}(16, 2^a, 2, 2)$ for any $3 \leq a \leq 11$. Also there exists $I_6(16, 4b, 2, 2)$, where $b \geq 3$ is odd, by the previous theorem. The result then follows by Lemma 5.7 and Corollary 5.9. □

5.7 Binary row-column factorial designs with strength $t = 3$

In this section we restrict ourselves to binary row-column factorial designs of strength 3. We completely classify these when the dimensions of the arrays are powers of 2. The aim of this section is to prove the following theorem.

Theorem 5.40. *Let $M \leq N$. Then an array of type $I_k(2^M, 2^N, 2, 3)$ exists if and only if $3 \leq k \leq M + N$, $3 \leq M$, $k \leq 2^{M-1}$ and $(k, M, N) \notin \{(4, 3, 3), (8, 4, 4)\}$.*

Lemma 5.41. *Let $M \leq N$. Then $(k, 2^M, 2^N, 2, 3)$ is admissible if and only if $3 \leq k \leq M + N$, $3 \leq M$ and $k \leq 2^{M-1}$.*

Proof. By Lemma 5.1, $3 \leq k \leq M + N$ and $3 \leq M$. The bound $k \leq 2^{M-1}$ (and sufficiency) follows by Lemma 5.5. □

To establish the two exceptions in Theorem 5.40, we first need the following result on orthogonal arrays. This result is a fairly standard observation for researchers in Hadamard codes but we include a proof for thoroughness.

Lemma 5.42. *Let $M \geq 3$. In any $\mathrm{OA}(2^M, 2^{M-1}, 2, 3)$, the weight of any two rows has the same parity.*

Proof. Let K be an $\mathrm{OA}(2^M, 2^{M-1}, 2, 3)$. Without loss of generality assume that, restricting ourselves to the first two columns of K, the first 2^{M-2} rows contain the ordered pairs $(1,1)$, the next 2^{M-2} rows contain the ordered pairs $(1,0)$, the next 2^{M-2} rows contain the ordered pairs $(0,1)$ and the final 2^{M-2} rows contained the ordered pairs $(0,0)$.

Let K' be the array obtained from K by replacing 0s with -1s. It follows, from the strength 3 property of the orthogonal array, that: (a) the first 2^{M-1} rows of K' form a Hadamard matrix; (b) the last 2^{M-1} rows of K' form a Hadamard matrix; and (c) the first 2^{M-2} rows together with the third set of 2^{M-2} rows of K' forms a Hadamard matrix.

Now, in a normalized Hadamard matrix of order at least 4, the weight of any row or column is even. Equivalent Hadamard matrices are formed by rearranging rows or columns, taking a transpose or swapping 0 with 1 in any row or column. All of these equivalences preserve the property that the weight of each pair of rows shares the same parity. The result follows. □

Corollary 5.43. *There exists neither an array of type* $I_4(8,8,2,3)$ *nor an array of type* $I_8(16,16,2,3)$.

Proof. If an array of type $I_4(8,8,2,3)$ exists, then the vectors in any row or column, by definition, form an $\mathrm{OA}(8,4,2,3)$. Thus, from the previous lemma, the weight of every vector in the array has the same parity. Hence the vectors in all the cells of the array do not form a factorial design. Similarly, there does not exist an array of type $I_8(16,16,2,3)$. □

We now focus on proving Theorem 5.40 in the case where $M \geq 5$. We will use Theorem 5.18 for this case. We first need some preliminary lemmas.

We remind the reader that a set S of vectors is t-independent if and only if each subset of S of size t is independent.

Lemma 5.44. *Let* C *be a set consisting of* M *cyclic permutations of the vector* $(1,1,1,1,0,0,\ldots,0)$ *over* $\mathbb{F}_2^M$, *where* $M \geq 5$ *and* $M \neq 6$. *Let*

$B = \{\mathbf{e_1}, \ldots, \mathbf{e_M}\}$ *be the standard basis for* $\mathbb{F}_2^M$. *Then the set* $W = B \cup C$ *is* $3-$*independent.*

Proof. We first show that the set C is $3-$independent. Note that all the vectors in C have weight 4. Also, any three vectors $\mathbf{t}, \mathbf{u}, \mathbf{v}$ in $(\mathbb{F}_2)^M$ are linearly dependent if and only if $\mathbf{u} + \mathbf{v} = \mathbf{t}$. Now for any two vectors $\mathbf{u}$ and $\mathbf{v}$ in C we have the following possibilities:

Case I: There is at most one i such that $u_i = v_i = 1$. In this case $\omega(\mathbf{u} + \mathbf{v}) \geq 6$ and therefore $\mathbf{u} + \mathbf{v} \notin C$.

Case II: There are exactly two values of i for which $u_i = v_i = 1$. In this case $\omega(\mathbf{u} + \mathbf{v}) = 4$ and $M \geq 7$ (since $M \neq 6$). However, notice that the vector $\mathbf{u} + \mathbf{v}$ contains the values $1, 1, 0, 0, 1, 1, 0$ at seven consecutive positions (modulo n) and therefore does not belong to C.

Case III: There are exactly three values of i for which $u_i = v_i = 1$. In this case $\omega(\mathbf{u} + \mathbf{v}) = 2$.

From above the weight of the sum of any two elements in C is at least 2 therefore $W = B \cup C$ is also $3-$independent. □

Lemma 5.45. *For* $N \geq M \geq 5$ *there exists an* $I_k(2^M, 2^N, 2, 3)$ *if and only if* $(k, 2^M, 2^N, 2, 3)$ *is admissible.*

Proof. From Lemma 5.41 and Corollary 5.9, it suffices to assume $k = \min\{2^{M-1}, M + N\}$.

We split the proof into different cases. In each case we define a matrix L satisfying the required conditions of Theorem 5.18.

Case I: $M \neq 6$. Let C_M be an $M \times M$ matrix such that the rows are the elements of the set C defined in Lemma 5.44 with the main diagonal of C_M containing only entry 1. Let D be the set of all the rows in I_M and $C_M - I_M$. Let W be the set of all vectors of odd weight in $\mathbb{F}_2^M$. By Lemma 5.5, W is a 3-independent set of vectors. Let S be a $(k - 2M) \times M$ matrix such that each

row is a distinct element in $W \setminus D$. Then the matrix L is as follows.

$$L = \left(\begin{array}{c|c:c} I_M & I_M & \mathbf{0} \\ \hdashline C_M - I_M & C_M & \mathbf{0} \\ \hdashline S & \mathbf{0} & I_{k-2M} \end{array}\right) \tag{5.5}$$

Case II: When $M = 6$. In this case we can take the above matrix L using the following C_M:

$$C_M = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

□

Lemma 5.46. *There exist* $I_3(8, 8, 2, 3)$, $I_4(8, 16, 2, 3)$, $I_7(16, 16, 2, 3)$ *and* $I_8(16, 32, 2, 3)$.

Proof. The eight binary vectors of dimension 3 give the rows of an $\mathrm{OA}(8, 3, 2, 3)$. Thus by Lemma 5.11, there exists an array of type $I_3(8, 8, 2, 3)$. Next, the 8 binary vectors of dimension 4 and even weight give the rows of an $\mathrm{OA}(8, 4, 2, 3)$. Using Lemma 5.11 again, there exists an array of type $I_4(8, 16, 2, 3)$.

By Theorem 5.18 and the following array L, there exists $I_8(16, 32, 2, 3)$. Moreover, we get $I_7(16, 16, 2, 3)$ for free by deleting the last row and column,

as indicated by dotted lines.

$$L = \left(\begin{array}{cccc:cccc:c} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ \hdashline 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \end{array}\right).$$

□

We now have all the tools, base cases and exceptions we need to prove Theorem 5.40. From Lemma 5.45, we may restrict ourselves to the case $M \in \{3, 4\}$ and $N \geq M$. If $M = 3$ then by Lemma 5.41, $3 \leq k \leq 2^{M-1} = 4$. An $I_3(8, 8, 2, 3)$ exists by the previous lemma. Thus by Corollary 5.9, there exists $I_3(2^M, 2^N, 2, 3)$ whenever $M, N \geq 3$. Next, $I_4(8, 8, 2, 3)$ does not exist by Corollary 5.43. However $I_4(8, 16, 2, 3)$ exists by the previous lemma. Thus by Corollary 5.9 there exists an array of type $I_4(2^M, 2^N, 2, 3)$ whenever $M \geq 3$ and $N \geq 4$.

Finally suppose that $N \geq M = 4$. By Lemma 5.41, $3 \leq k \leq 8$. Now, $I_8(16, 16, 2, 3)$ does not exist by Corollary 5.43 but $I_7(16, 16, 2, 3)$ exists by the previous lemma and $I_8(16, 32, 2, 3)$. The result then follows by Corollary 5.9.

5.8 Conclusion

We first discuss some limitations to the approach given in Section 5. Firstly, the idea in Theorem 5.23 cannot work for theoretical reasons when $k \leq 6$, and for computational reasons (inspection of possible cases) when $k = 7$ and $m \in \{3, 5\}$. The reason that $k \geq 7$ is necessary for the approach is as follows. The counting argument in the following lemma shows that if m is odd, then in any OA$(4m, n, 2, 2)$, if the sum of ℓ columns has weight $2m$ (that is, contains $2m$ occurrences of 1), then $\ell \equiv 1$ or 2 (mod 4). Consider the OA$(4m, l, 2, 2)$

formed from the columns of V satisfying the conditions of Theorem 5.23. Then Lemma 5.47 implies the size of V and W are each at least 5 meaning k is at least 7.

Lemma 5.47. *Let H be an* $\mathrm{OA}(4m, \ell, 2, 2)$*, where m is an odd integer. Let $\boldsymbol{v}$ be the sum of columns of H.*

- *If* $\ell \equiv 0$ *or* $3 \pmod 4$ *then* $\omega(\boldsymbol{v}) \equiv 0 \pmod 4$.
- *If* $\ell \equiv 1$ *or* $2 \pmod 4$ *then* $\omega(\boldsymbol{v}) \equiv 2 \pmod 4$.

Proof. Let x_i be the weight of the ith row of H. The total number of $(1,1)$ pairs such that both of them lie in the same row is given by $\sum_{i=1}^{4m} \binom{x_i}{2}$. Also, since each pair of columns contain exactly m $(1,1)$ pairs, therefore this number can also be given by $m\binom{\ell}{2}$. Thus we have,

$$\sum_{i=1}^{4m} \binom{x_i}{2} = m\binom{\ell}{2}$$

Since the number of 1s in the array is $2m\ell$, $\sum x_i = 2m\ell$. Therefore,

$$\sum_{i=1}^{4m} x_i^2 = m\ell(\ell+1). \tag{5.6}$$

Also notice that, $x_i^2 \equiv 1 \pmod 4$ if x_i is odd and $x_i^2 \equiv 0 \pmod 4$ otherwise. Thus we have:

$$\omega(\mathbf{v}) = \sum_{i=1}^{4m}(x_i \pmod 2) = \sum_{i=1}^{4m}(x_i^2 \pmod 2) = \sum_{i=1}^{4m}(x_i^2 \pmod 4).$$

The result is now follows from (5.6) and the fact that m is odd. □

We have intentionally structured our paper so that abelian and non-abelian constructions are distinguished. By inspection, we have determined that there does not exist an abelian $I_5(12, 8, 2, 2)$; a non-abelian example is given in Lemma 5.37. However we do not know at this stage whether there are infinitely many parameters for which their exists only a non-abelian binary strength 2 row-column factorial design.

As observed in the introduction, finding necessary and sufficient conditions for the existence of a strength 2 binary row-column factorial design depends on the Hadamard conjecture. However, the following may be more within reach.

Conjecture 5.48. *If there exists a Hadamard matrix of order* $4m$*, then there exists an* $I_k(4m, 4n, 2, 2)$ *for any* $n \geq m$*,* $2^k \mid 16mn$ *and* $k \leq 4m - 1$*, with the exception* $m = 1$ *and* n *is odd.*

From Theorem 5.39, the above conjecture is true for $m \leq 5$. For $m = 6$, the unknown cases with minimal parameters are: $I_{k+3}(24, 2^k, 2, 2); 5 \leq k \leq 11$. From Theorem 5.36 and the existence of a Hadamard matrix of order 12, $I_{k+3}(24, 2^k, 2, 2)$ exists for $12 \leq k \leq 20$.

Appendix: $I_6(12, 16, 2, 2)$

$\mathbf{000000}^A$	$\mathbf{100000}^B$	$\mathbf{010000}^C$	$\mathbf{001000}^D$	$\mathbf{000100}^A$	$\mathbf{001100}^D$	$\mathbf{010100}^C$	$\mathbf{011000}^B$	$\mathbf{101000}^C$	$\mathbf{100100}^B$	$\mathbf{110000}^D$	$\mathbf{011100}^B$	$\mathbf{101100}^C$	$\mathbf{110100}^D$	$\mathbf{111000}^A$	$\mathbf{111100}^A$
$\mathbf{110101}^B$	010101^A	100101^D	111101^C	110001^B	111001^C	100001^D	101101^A	011101^D	010001^A	000101^C	101001^A	011001^D	000001^C	001101^B	001001^B
$\mathbf{110010}^C$	010010^D	100010^A	111010^B	110110^C	111110^B	100110^A	101010^D	011010^A	010110^D	000010^B	101110^D	011110^A	000110^B	001010^C	001110^C
$\mathbf{000011}^D$	100011^C	010011^B	001011^A	000111^D	001111^A	010111^B	011011^C	101011^B	100111^C	110011^A	011111^C	101111^B	110111^A	111011^D	111111^D
$\mathbf{001100}^E$	101100^E	011100^H	000100^F	001000^G	000000^H	011000^F	010100^G	100100^F	101000^G	111100^H	010000^E	100000^H	111000^F	110100^G	110000^E
$\mathbf{010101}^F$	110101^H	000101^E	011101^E	010001^H	011001^G	000001^G	001101^F	111101^G	110001^F	100101^G	001001^H	111001^E	100001^E	101101^H	101001^F
$\mathbf{011110}^G$	111110^F	001110^G	010110^H	011010^E	010010^F	001010^E	000110^H	110110^E	111010^H	101110^F	000010^F	110010^G	101010^H	100110^E	100010^G
$\mathbf{011011}^H$	111011^G	001011^F	010011^G	011111^F	010111^E	001111^H	000011^E	110011^H	111111^E	101011^E	000111^G	110111^F	101111^G	100011^F	100111^H
$\mathbf{111000}^I$	011000^J	101000^K	110000^J	111100^K	110100^L	101100^I	100000^L	010000^I	011100^L	001000^L	100100^J	010100^K	001100^J	000000^K	000100^I
$\mathbf{101001}^J$	001001^I	111001^I	100001^L	101101^L	100101^J	111101^K	110001^K	000001^K	001101^K	011001^J	110101^I	000101^I	011101^L	010001^L	010101^J
$\mathbf{100110}^K$	000110^L	110110^L	101110^I	100010^I	101010^K	110010^J	111110^J	001110^J	000010^J	010110^K	111010^L	001010^L	010010^I	011110^I	011010^K
$\mathbf{101111}^L$	001111^K	111111^J	100111^K	101011^J	100011^I	111011^L	110111^I	000111^L	001011^I	011111^I	110011^K	000011^J	011011^K	010111^J	010011^L

Table 5.6: An array of type $I_6(12, 16, 2, 2)$.

References

[1] R. Bose. On some connections between the design of experiments and information theory. *Bull. Inst. Inter. Statist.*, 38:257–271, 1961.

[2] T. Britz, N. Cavenagh, A. Mammoliti, and I. Wanless. Mutually orthogonal binary frequency squares. *The Electronic Journal of Combinatorics*, 27(3):P3.7, 2020.

[3] K. Bush. A generalization of a theorem due to MacNeish. *Ann. Math. Statist.*, 23(2):293–295, 1933.

[4] C. J. Colbourn and J. H. Dinitz. *Handbook of Combinatorial Designs, Second Edition (Discrete Mathematics and Its Applications)*. Chapman & Hall/CRC, 2006.

[5] S. Damelin, G. Michalski, and G. L. Mullen. The cardinality of sets of k-independent vectors over finite fields. *Monatshefte für Mathematik*, 150(4):289–295, 2007.

[6] D. Z. Djokovic. Hadamard matrices of order 764 exist. *Combinatorica*, 28:487–489, 2008.

[7] J. Godolphin. Construction of row–column factorial designs. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 81(2):335–360, 2019.

[8] S. Hedayat, Sloane. *Orthogonal Arrays*. Springer, New York, NY, 1999.

[9] K. J. Horadam. *Hadamard matrices and their applications*. Princeton university press, 2012.

[10] C. F. Laywine and G. L. Mullen. A table of lower bounds for the number of mutually orthogonal frequency squares. *Ars Combinatoria*, 59:85–96, 2001.

[11] M. Li, Y. Zhang, and B. Du. Some new results on mutually orthogonal frequency squares. *Discrete Mathematics*, 331:175–187, 2014.

[12] R. Plackett and J. Burman. The design of optimum multifactorial experiments. *Biometrika*, (33):305–325, 1943–1946.

[13] F. Rahim and N. J. Cavenagh. Row-column factorial designs with multiple levels. *Journal of Combinatorial Designs*, 29:750–764, 2021.

[14] C. R. Rao. Factorial experiments derivable from combinatorial arrangements of arrays. *Supplement to the Journal of the Royal Statistical Society*, 9(1):128–139, 1947.

[15] N. J. Sloane. A library of hadamard matrices. Accessed Apr 2022. http://neilsloane.com/hadamard/.

[16] P. Wang. Orthogonal main-effect plans in row–column designs for two-level factorial experiments. *Communications in Statistics-Theory and Methods*, 46(21):10685–10691, 2017.

Chapter 6

Mutually orthogonal frequency rectangles

6.1 Abstract

A *frequency rectangle* of type FR$(m, n; q)$ is an $m \times n$ matrix such that each symbol from a set of size q appears n/q times in each row and m/q times in each column. Two frequency rectangles of the same type are said to be orthogonal if, upon superimposition, each possible ordered pair of symbols appear the same number of times. A set of k frequency rectangles in which every pair is orthogonal is called a set of *mutually orthogonal frequency rectangles*, denoted by k–MOFR$(m, n; q)$. We show that a k–MOFR$(2, 2n; 2)$ and an orthogonal array OA$(2n, k, 2, 2)$ are equivalent. We also show that an OA$(mn, k, 2, 2)$ implies the existence of a k–MOFR$(2m, 2n; 2)$. We construct $(4a-2)$–MOFR$(4, 2a; 2)$ assuming the existence of a Hadamard matrix of order $4a$.

A k–MOFR$(m, n; q)$ is said to be *t–orthogonal*, if each subset of size t, when superimposed, contains each of the q^t possible ordered t-tuples of entries exactly mn/q^t times. A set of vectors over a finite field $\mathbb{F}_q$ is said to be *t-independent* if each subset of size t is linearly independent. We describe a method to obtain a set of t–orthogonal k–MOFR(q^M, q^N, q) corresponding to a set of t–independent vectors in $(\mathbb{F}_q)^{M+N}$. We also discuss upper and lower

bounds on the sizes of sets of t–independent vectors and give a table of values for binary vectors of length $N \leq 16$.

A frequency rectangle of type FR$(n, n; q)$ is called a frequency square and a set of k mutually orthogonal frequency squares is denoted by k–MOFS$(n; q)$ or k–MOFS(n) when there is no ambiguity about the symbol set. For p an odd prime, we show that there exists a set of $(p-1)$ binary MOFS$(2p)$, hence improving the lower bounds in (Britz et al. 2020) for $p \geq 19$.

MSC 2010 Codes: 05B15

Keywords: Frequency square; frequency rectangle or F-rectangle; MOFR; MOFS; Hadamard matrix; Orthogonal array.

6.2 Introduction

A *frequency rectangle* (also called *F-rectangle*) of type FR$(m, n; q)$ is an $m \times n$ array based on a symbol set S of size q, such that each element of S appears exactly n/q times in each row and m/q times in each column. Two frequency rectangles, F_1 and F_2, of the same type, are said to be *orthogonal* if each possible ordered pair of symbols appear the same number of times when F_1 and F_2 are superimposed. A set of k frequency rectangles in which every pair is orthogonal is called a set of *mutually orthogonal frequency rectangles*, denoted by k–MOFR$(m, n; q)$.

A *frequency square* of type F$(n; q)$ is a frequency rectangle of type FR$(n, n; q)$. In the literature, a frequency square of type F$(n; q)$ is usually denoted by F$(n; \lambda)$, where $\lambda = n/q$ is the frequency of each symbol in each row or each column. However, we stick to the notation F$(n; q)$ where q is the size of the symbol set to remain consistent with the rest of the notations used. The definition of orthogonality between two frequency squares is analogous to frequency rectangles. A set of frequency squares in which each pair is orthogonal is called a set of *mutually orthogonal frequency squares* or MOFS, denoted by k–MOFS$(n; q)$ or simply by k–MOFS(n) when there is no ambiguity about

the symbol set.

In the theory of frequency squares, most of the work has been dedicated to constructing the largest possible sets of MOFS. The upper bound, $k \leq (n-1)^2/(q-1)$, for a k–MOFS$(n;q)$ was first determined by Hedayat, Raghavarao, and Seiden [12]. The following theorem is a particular case of a more general result proved in [18]. However, we have included the proof here for thoroughness. The proof is similar to the one given in [12] for frequency squares.

Theorem 6.1. [18] *If a* k–MOFR$(m,n;q)$ *exists, then:*

$$k \leq \frac{(m-1)(n-1)}{(q-1)}. \tag{6.1}$$

Proof. Let $F_1, F_2, \ldots, F_k$ be the elements of k–MOFR$(m,n;q)$. Corresponding to each F_α we define an $mn \times q$ matrix $H_\alpha = (h_{(ij),\beta})$, where $i = 1,2,\ldots,m; j = 1,2,\ldots,n$, β runs over the symbols set, and

$$h_{(ij),\beta} = \begin{cases} 1 & \textit{if the entry in the } (i,j)^{th} \textit{ cell of } F_\alpha \textit{ is } \beta \\ 0 & \textit{otherwise.} \end{cases}$$

Observe that each column of H_α contains mn/q 1's. Let M be an $(mn) \times (kq)$ matrix defined as follows:

$$M = (H_1 \mid H_2 \mid \cdots \mid H_k).$$

Since each row of M corresponds to a fixed position (i,j) of the set of frequency rectangles, by using the properties of frequency rectangles there are at least $(m-1)+(n-1)$ dependent rows in M. Therefore the rank of M,

$$\text{Rank}(M) \leq \min\{(m-1)(n-1)+1, kq\}.$$

Observe that $H_r^T H_s = (mn/q)I_q$ when $r = s$ and $H_r^T H_s = (mn/q^2)J_q$ when $r \neq s$, where I_q is an identity matrix of order q and J_q is a $q \times q$ matrix of ones.

Thus we have the following matrix of dimensions $(kq) \times (kq)$;

$$M^T M = \begin{pmatrix} n\lambda I_q & \lambda\lambda' J_q & \dots & \lambda\lambda' J_q \\ \lambda\lambda' J_q & n\lambda I_q & \dots & \lambda\lambda' J_q \\ \vdots & \vdots & \ddots & \vdots \\ \lambda\lambda' J_q & \lambda\lambda' J_q & \dots & n\lambda I_q \end{pmatrix},$$

where $\lambda = m/q$ and $\lambda' = n/q$. The eigenvalues of $M^T M$ are $n\lambda k, n\lambda$ and 0 with multiplicities $1, k(q-1)$ and $k-1$ respectively (see Appendix 6.7 for details). Since the sum of multiplicities of non-zero eigenvalues gives the rank of $M^T M$,

$$kq - k + 1 = R(M^T M) = R(M) \leq \min\{(m-1)(n-1)+1, kq\},$$

which gives the required result. □

A k–MOFR$(m, n; q)$ or k–MOFS$(n; q)$ is said to be *complete* if k reaches the upper bound described in the above theorem. Complete sets of MOFR of type FR$(q^M, q^N; q)$ are known to exist when q is a prime power [9]. For q a prime power, Mandeli [17] describes a method to construct a complete set of MOFR$(q^M, 2q^N, q)$. For $m = 4a$ and $n = 4b$, Cheng [4] showed the existence of a complete set of MOFR$(m, n; 2)$ provided that Hadamard matrices of order $4a$ and $4b$ exist. Also, assuming the existence of a Hadamard matrix of order $4b$, Federer, Hedayat, and Mandeli [9] describe a method to construct a complete set of MOFR$(2, 4b; 2)$.

In Section 6.3, we include results that further describe the relationship between Hadamard matrices, orthogonal arrays, and frequency rectangles. An *orthogonal array* OA(N, k, q, t) of strength t is an $N \times k$ matrix of symbols based on a set of size q, such that in any $N \times t$ submatrix, each possible ordered t–tuple appears the same number of times as a row. We show that an orthogonal array OA$(n, k, 2, 2)$ is equivalent to k–MOFR$(2, 2n; 2)$. We also show that if there exists an orthogonal array OA$(mn, k, 2, 2)$ then there exists k–MOFR$(2m, 2n; 2)$ and the existence of a Hadamard matrix of order $4a$ implies the existence of $(4a-2)$–MOFR$(4, 2a; 2)$.

Complete sets of MOFS of type F$(q^N; q)$ are also known to exist when q

is a prime power [15, 16, 19, 22]. A complete set of MOFS of type $\mathrm{F}(4a; 2)$ can be constructed by using a Hadamard matrix of order $4a$ [10]. However, no complete sets of MOFS for any other set of parameters are known to exist. In 2001, Laywine and Mullen [15] formulated a table of lower bounds for the maximum known values for the frequency squares of type $\mathrm{F}(n; q)$ where $n \leq 100$. Later the table was improved by Li et al. [16] in 2014. Recently, in [3], the lower bounds in the case of k–MOFS$(n; q)$, where $n \equiv 2 \pmod 4$ and $q = 2$ have been improved to $k \geq 17$ and it is also shown there that complete sets do not exist for these parameters. In Section 6.5, we give a method to construct a set of $(p-1)$–MOFS$(2p; 2)$ where p is an odd prime, thus improving the lower bounds in [16] and [3] for such $p \geq 19$.

We next describe a stronger form of orthogonality for a set of frequency rectangles. A set M of frequency rectangles of type $\mathrm{FR}(m, n; q)$ is said to be *t–orthogonal*, $t \geq 2$, if upon superimposition of any t elements in M, each of the possible q^t ordered t–tuples occurs the same number of times in the resulting array. By definition k–MOFR$(m, n; q)$ is 2–orthogonal and any t–orthogonal set is also t'–orthogonal for any $2 \leq t' \leq t$.

Here we include an example to illustrate the definition further.

Example 6.2. Consider the set $M = \{F_1, F_2, \ldots, F_6\}$, where each F_i is given in Table 6.1.

0	0	1	1
0	0	1	1
1	1	0	0
1	1	0	0

F_1

0	1	0	1
0	1	0	1
1	0	1	0
1	0	1	0

F_2

0	1	0	1
1	0	1	0
1	0	1	0
0	1	0	1

F_3

0	1	0	1
1	0	1	0
0	1	0	1
1	0	1	0

F_4

0	0	1	1
1	1	0	0
1	1	0	0
0	0	1	1

F_5

0	0	1	1
1	1	0	0
0	0	1	1
1	1	0	0

F_6

Table 6.1: 3–orthogonal 6–MOFR$(4, 4; 2)$.

Now if we superimpose any three elements of M, then each of the 2^3 possible ordered 3–tuples occurs twice in the resultant array, as shown in Table 6.2 for the case of F_1, F_2, F_3 and F_1, F_4, F_6. We leave it to the reader to verify that it is true for the rest of the cases. Thus M is 3–orthogonal. However, M is not 4–orthogonal, since the sequences of odd weights do not occur when the arrays F_1, F_2, F_3, and F_5 are superimposed (see Table 6.2).

000	011	100	111
001	010	101	110
111	100	011	000
110	101	010	001

F_1, F_2, F_3

000	010	101	111
011	001	110	100
100	110	001	011
111	101	010	000

F_1, F_4, F_6

0000	0110	1001	1111
0011	0101	1010	1100
1111	1001	0110	0000
1100	1010	0101	0011

F_1, F_2, F_3, F_5

Table 6.2: Superimposed arrays from 6–MOFR$(4, 4; 2)$

In [20] and [21], row-column factorial designs of strength s are discussed. A row-column factorial design of strength s, denoted by $I_k(m, n, q, s)$, is an arrangement of mn/q^k copies of the q^k–factorial design (that is, all the k-tuples over a set of size q) in an $m \times n$ array such that the elements in each row (column) forms an orthogonal array OA(n, k, q, s) (OA(m, k, q, s)). By definition, the existence of an $I_k(m, n, q, s)$ (for any $s \geq 1$) implies the existence of k–orthogonal k–MOFR$(m, n; q)$. Conversely, if there exists a k–orthogonal k-MOFR$(m, n; q)$ then there exists an $I_k(m, n, q, 1)$. Since necessary and sufficient conditions are known for the existence of $I_k(m, n, q, 1)$, we have the following theorem.

Theorem 6.3. [20] *Let $m \leq n$. There exists k–orthogonal k–*MOFR$(m, n; q)$ *if and only if:*

(i) $q|m$ *and* $q|n$*;*

(ii) *if* $k = q = m = 2$ *then* $n \equiv 0 \pmod 4$*; and*

(iii) $(k, m, n, q) \neq (2, 6, 6, 6)$.

A set of vectors over a field $\mathbb{F}_q$ is said to be *t–independent* if each subset of size t is linearly independent. In Section 6.4, we describe a relationship between a set of t–independent vectors over a finite field $\mathbb{F}_q$ and a set of t–orthogonal MOFR(q^M, q^N, q). We also exhibit a table that shows the maximum known values for numbers of t–independent vectors over $\mathbb{F}_2$ by using existence results for linear codes and some other known results in the literature. We also show that the existence of an orthogonal array OA$(2m, k, 2, t)$ implies a t–orthogonal k–MOFR$(2m, 2m, 2)$.

6.3 Orthogonal Arrays and Frequency Rectangles

In this section, we use Hadamard matrices and orthogonal arrays to construct MOFR. A *Hadamard matrix* $H(n)$ is a square matrix of order n, having entries from the set $\{1, -1\}$ such that any two rows are orthogonal; that is it satisfies the equation:

$$H(n)H(n)^T = nI_n.$$

It has been conjectured that a Hadamard matrix of order $4n$ exists for each n [8, 13, 14]. A Hadamard matrix with all the entries in its first column and first row equal to 1 is called a *normalized Hadamard matrix*. Any Hadamard matrix is equivalent to a normalized Hadamard matrix. A normalized Hadamard matrix has the following combinatorial properties.

Lemma 6.4. *Let* $\mathbf{a} = (a_1, \ldots, a_n)$ *and* $\mathbf{b} = (b_1, \ldots, b_n)$ *be two distinct rows, other than the first, of a normalized Hadamard matrix of order* n, $n > 2$. *Then*

(i) *half of the entries* a_i *are* $+1's$ *and half of them are* $-1's$.

(ii) *the multiset* $\{(a_i, b_i) : i = 1, 2, \ldots, n\}$ *contains each type of order pair exactly* $n/4$ *times.*

(iii) *the conditions (i) and (ii) are also true for any two distinct columns, other than the first, of a normalized Hadamard matrix.*

A *partial Hadamard matrix* or *Hadamard rectangle* is a $k \times n$ matrix ($k \leq n$), having entries from the set $\{1, -1\}$ such that any two rows are orthogonal. Analogously to a normalized Hadamard matrix we can define a normalized Hadamard rectangle. The conditions (i) and (ii) in the Lemma 6.4 are also true for a normalized Hadamard rectangle, however, (iii) does not necessarily hold in the case of a rectangle.

An orthogonal array $\mathrm{OA}(4a, 4a-1, 2, 2)$ can be obtained from a normalized Hadamard matrix by removing the first column and replacing -1's with 0's. The following lemma that describes the relationship between the two structures is a generalization of the Theorem 7.5 given in [13, p. 148] for the rectangular case.

Lemma 6.5. *Let $k < 2b$. There exists an $\mathrm{OA}(2b, k-1, 2, 2)$ if and only if there exists a $k \times 2b$ Hadamard rectangle. In particular, there exists an $\mathrm{OA}(2b, 2b-1, 2, 2)$ if and only if there exists a Hadamard matrix $H(2b)$.*

If B is a binary array then we define $\overline{B}$ to be the array obtained by interchanging 0's and 1's in B.

Theorem 6.6. *Suppose there exists an $\mathrm{OA}(mn, k, 2, 2)$. Then there exist k–$\mathrm{MOFR}(2m, 2n; 2)$.*

Proof. Let M be an orthogonal array $\mathrm{OA}(mn, k, 2, 2)$. Let $\mathbf{b} = (b_1, \ldots, b_{mn})$ be any column of M. Define an $m \times n$ array B corresponding to this column as follows:

$$B = \begin{bmatrix} b_1 & b_2 & \ldots & b_n \\ b_{n+1} & b_{n+2} & \ldots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n(m-1)+1} & b_{n(m-1)+2} & \ldots & b_{mn} \end{bmatrix}$$

Now, let $L_{\mathbf{b}}$ be the following array:

$$L_{\mathbf{b}} = \left[\begin{array}{c|c} B & \overline{B} \\ \hline \overline{B} & B \end{array}\right]$$

Then L_b is a frequency rectangle of type FR$(2m, 2n; 2)$. Thus, by constructing an array corresponding to each column of M we obtain a set of k frequency rectangles of type FR$(2m, 2n; 2)$. The orthogonality of these arrays follows from the orthogonality of the columns of M. □

Corollary 6.7. *Suppose there exists a Hadamard matrix $H(mn)$ where 4 divides mn. Then there exist $(mn-1)$–*MOFR$(2m, 2n; 2)$.

Lemma 6.8. *There exist k–*MOFR$(2, 2n; 2)$ *if and only if there exists an* OA$(2n, k, 2, 2)$.

Proof. Suppose there exists k–MOFR$(2, 2n; 2)$ and denote this set by M. Let $L_1, \ldots, L_k \in M$. Let $\mathbf{r}_i$ be the first row of L_i. We claim that $[\mathbf{r}_1{}^T|\mathbf{r}_2{}^T|\ldots|\mathbf{r}_k{}^T]$ is an OA$(2n, k, 2, 2)$. It is sufficient to show that $\mathbf{r}_1$ and $\mathbf{r}_2$ are orthogonal. Without loss of generality, we may assume that L_1 has the following form:

$$L_1 = \begin{array}{|cccc|cccc|} \hline 0 & 0 & \ldots & 0 & 1 & 1 & \ldots & 1 \\ \hline 1 & 1 & \ldots & 1 & 0 & 0 & \ldots & 0 \\ \hline \end{array}$$

Suppose that $\mathbf{r}_2$ contains x zeros in the first n positions. Then by the definition of frequency rectangle the second row of L_2, that is $\overline{\mathbf{r}_2}$, contains x zeros in the last n positions. Therefore, the total number of $(0, 0)$ pairs when L_1 and L_2 are superimposed is $2x$. Since L_1 and L_2 are orthogonal, $2x = n$ or $x = n/2$. Thus $\mathbf{r}_1$ and $\mathbf{r}_2$ when superimposed contain each type of pair the same number of times since $x = n - x$.

Conversely, corresponding to each column $\mathbf{c}$ of an OA$(2n, k, 2, 2)$ we generate a frequency square $L_{\mathbf{c}}$ which contains $\mathbf{c}$ and $\overline{\mathbf{c}}$ as its first and second row respectively. □

Theorem 6.9. *Suppose there exists a Hadamard matrix $H(4a)$. Then there exists $(4a-2)$–*MOFR$(4, 2a; 2)$.

Proof. Let H be a Hadamard matrix of order $4a$ in normalized form. Replace -1's with 0's in H. Let $c_i, i \in \{1, \ldots, 4a\}$ be the columns of H. Without loss

of generality we may assume that c_1 and c_2 have the following form:

c_1	c_2
1	1
1	1
⋮	⋮
1	1
1	0
1	0
⋮	⋮
1	0

Since the columns $\mathbf{c_2}, \ldots, \mathbf{c_{4a}}$ of H form an OA$(4a, 4a-1, 2, 2)$, the columns $\mathbf{c_3}, \ldots, \mathbf{c_{4a}}$ have the property that each contains exactly a zeroes and a ones in the first $2a$ positions. Let $\mathbf{c_i} = (b_1, \ldots, b_{4a})$ for some $i \in \{3, \ldots, 4a\}$. Define a $2 \times 2a$ array B_i corresponding to $\mathbf{c_i}$ as follows:

$$B_i = \begin{bmatrix} b_1 & b_2 & \ldots & b_{2a} \\ b_{2a+1} & b_{2a+2} & \ldots & b_{4a} \end{bmatrix}$$

Now,

$$L_i = \left[\begin{array}{c} B \\ \hline \overline{B} \end{array}\right]$$

is a FR$(4, 2a; 2)$. Observe that the set $\{L_i : 3 \leq i \leq 4a\}$ forms a $(4a-2)$–MOFR$(4, 2a; 2)$. □

6.4 t–orthogonal frequency rectangles

Recall that a k–MOFR$(m, n; q)$ is *t–orthogonal* if each subset of size t, upon superimposition, gives mn/q^t copies of the full factorial design. A set of vectors is said to be *t–independent* if each subset of size t is linearly independent. In this section, we describe a relationship between a set of t–independent vectors and a set of t–orthogonal frequency rectangles. We also include some results from the literature about the known bounds for the size of a set of t–independent vectors. At the end of this section, we formulate a table that

provides lower bounds on k for a set of t–orthogonal k–MOFR$(m, n; 2)$, by using existence results on binary linear codes.

Let $\mathbf{u} = (u_1, u_2, \ldots, u_M)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_N)$ be vectors over the field $\mathbb{F}_q$ of length M and N, respectively. Then we define $\mathbf{u} \oplus \mathbf{v} = (u_1, u_2, \ldots, u_M, v_1, v_2, \ldots, v_N)$ to be the vector of length $M + N$ obtained by the concatenation of $\mathbf{u}$ and $\mathbf{v}$. By a *cyclic shift* of $\mathbf{v}$ we mean the vector $\mathbf{v}' = (v_N, v_1, v_2, \ldots, v_{N-1})$.

We first give here a result that uses orthogonal arrays to construct a set of t–orthogonal frequency rectangles.

Theorem 6.10. *If there exists an* OA$(2m, k, 2, t)$ *then there exists a* t–*orthogonal* k–MOFR$(2m, 2m; 2)$.

Proof. Let $\mathbf{v}$ be a column vector of an OA$(2m, k, 2, t)$. Construct a frequency square $F_{\mathbf{v}}$ where column i is the ith cyclic shift of $\mathbf{v}$. Clearly $F_{\mathbf{v}}$ is a frequency rectangle of type FR$(2m, 2m; 2)$. Now the t–orthogonality of these arrays follows from the definition of t in OA$(2m, k, 2, t)$. □

The converse of the above theorem is not true in general. In Example 6.2 the arrays F_1, F_2 and F_3 form a 3–orthogonal 3–MOFR$(4, 4; 2)$ but there does not exist an OA$(4, 3, 2, 3)$. However, we have the following result.

Theorem 6.11. *If there exists a* t–*orthogonal* k–MOFR$(m, n; q)$, *then there exists an orthogonal array* OA(mn, k, q, t).

Proof. Let $S = \{F_1, \ldots, F_k\}$ be a t–orthogonal k–MOFR$(m, n; q)$. Corresponding to each $F_i \in S$, we construct a vector $\mathbf{f}_i$ of length mn as follows. Let $\mathbf{v}_1, \ldots, \mathbf{v}_m$ be, in sequential order, the row vectors of F_i. Let $\mathbf{f}_i = \mathbf{v}_1 \oplus \mathbf{v}_2 \oplus \cdots \oplus \mathbf{v}_m$. Let M be the $(mn) \times k$ array which contains each element of $\{\mathbf{f}_i : 1 \leq i \leq k\}$ as a column vector. Observe that M is an OA(mn, k, q, t). □

Theorem 6.12. *Let* S *be a set of* k t*-independent vectors in* $(\mathbb{F}_q)^{M+N}$ *such that for each* $\mathbf{v} = (v_1, \ldots, v_{M+N}) \in S$

(i) $(v_1, \ldots, v_M) \neq (0, \ldots, 0)$,

(ii) $(v_{M+1}, \ldots, v_{M+N}) \neq (0, \ldots, 0)$,

*then there exists a t–orthogonal k–*MOFR$(q^M, q^N; q)$.

Proof. Corresponding to each vector $\mathbf{v} \in S$ we construct a frequency rectangle $F_{\mathbf{v}}$ as follows. Let $\mathbf{v} = (v_1, \ldots, v_{M+N})$. We define a polynomial,

$$f_{\mathbf{v}} = \sum_{i=1}^{M+N} v_i x_i.$$

Now we label the rows and columns of a $q^M \times q^N$ array by using all M–tuples and N–tuples, respectively, over the field $\mathbb{F}_q$. Let the cell in the intersection of row $(r_1, \ldots, r_M)$ and column $(c_1, \ldots, c_N)$ contain the entry $f_{\mathbf{v}}(r_1, \ldots, r_M, c_1, \ldots, c_N)$.

To show that $F_{\mathbf{v}}$ is a frequency rectangle, fix a column $\mathbf{c}$ of $F_{\mathbf{v}}$, labeled by $(c_1, \ldots, c_N)$. Let $\beta \in \mathbb{F}_q$. The number of appearances of β in $\mathbf{c}$ is equal to the number of solutions to the following equation over $\mathbb{F}_q$:

$$f_{\mathbf{v}}(x_1, ..., x_M, c_1, \ldots, c_N) = \beta \tag{6.2}$$

By (i) there is at least one $i \in \{1, \ldots, M\}$ for which $v_i \neq 0$, thus equation (6.2) has exactly q^{M-1} solutions over $\mathbb{F}_q$. This shows that β occurs exactly q^{M-1} times in $\mathbf{c}$. Similarly, we can show that each element of $\mathbb{F}_q$ occurs q^{N-1} times in each row of $F_{\mathbf{v}}$.

Thus $\{F_{\mathbf{v}} : \mathbf{v} \in S\}$ is a set of k frequency rectangles of type FR$(q^M, q^N; q)$. It remains to show that this set is t–orthogonal. Let S' be a subset of S of size t and consider a t-tuple $\alpha = (\alpha_1, \ldots, \alpha_t)$ in $\mathbb{F}_q$. Now consider the following system of equations:

$$HX = \alpha^T$$

where, $X = (x_1, \ldots, x_{M+N})^T$ and H is a $t \times (M+N)$ matrix that contains each element of S' as a row. Since S is a t–independent set of vectors, this system of equations has rank t and therefore there are exactly q^{M+N-t} solutions for each $\alpha \in (\mathbb{F}_q)^t$. Thus the set $\{F_{\mathbf{v}} : \mathbf{v} \in S\}$ is t–orthogonal k–MOFR$(q^M, q^N; q)$. $\square$

Corollary 6.13. *Let $t \geq 1$. If there exists a set of k t–independent vectors in $(\mathbb{F}_q)^M$ then there exists a t–orthogonal k–MOFR$(q^M, q^N; q)$, where $N \geq M$.*

Proof. Let S be a set of k t–independent vectors. Since $t \geq 1$, $\mathbf{0} \notin S$. For each $\mathbf{v} = (v_1, \ldots, v_M) \in S$, we define $\mathbf{v}' = \mathbf{v} \oplus \mathbf{v} \oplus \mathbf{0}$ of length $M + N$, where $\mathbf{0}$ is a zero vector of length $N - M$. Let $S' = \{\mathbf{v}' : \mathbf{v} \in S\}$. Observe that S' is t–independent and satisfies the conditions (i) and (ii) of Theorem 6.12. □

Theorem 6.14. *Suppose there exists a set of k_1 3–independent vectors of length M and a set of k_2 3–independent vectors of length N over the field $\mathbb{F}_q$. Then there exists a 3–orthogonal (k_1k_2)–MOFR$(q^M, q^N; q)$.*

Proof. Let S and T be sets of 3–independent vectors of length M and N, respectively, where $|S| = k_1$ and $|T| = k_2$. Define $S' = \{\mathbf{u} \oplus \mathbf{v} : \mathbf{u} \in S, \mathbf{v} \in T\}$. Observe that S' satisfies the conditions (i) and (ii) in Theorem 6.12 and $|S'| = k_1k_2$. We claim that S' is also 3–independent.

Let $\mathbf{x}, \mathbf{y}, \mathbf{z}$ be three distinct elements in S'. Then $\mathbf{x} = \mathbf{a} \oplus \mathbf{d}$, $\mathbf{y} = \mathbf{b} \oplus \mathbf{e}$, and $\mathbf{z} = \mathbf{c} \oplus \mathbf{f}$, where $\mathbf{a}, \mathbf{b}, \mathbf{c} \in S$ and $\mathbf{d}, \mathbf{e}, \mathbf{f} \in T$. Without loss of generality, we have the following three cases to consider:

Case I: $\mathbf{a}, \mathbf{b}, \mathbf{c}$ are all distinct. In this case, $\{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ is 3–independent (and thus linearly independent) so in turn $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ is linearly independent.

Case II: $\mathbf{a} = \mathbf{b} \neq \mathbf{c}$. Observe that $\mathbf{d} \neq \mathbf{e}$ in this case. Suppose that there exist $\alpha, \beta, \gamma \in \mathbb{F}_q$ such that:

$$\alpha\mathbf{x} + \beta\mathbf{y} + \gamma\mathbf{z} = \mathbf{0}$$

Then we have:

$$\alpha\mathbf{a} + \beta\mathbf{a} + \gamma\mathbf{c} = \mathbf{0} \tag{6.3}$$

$$\alpha\mathbf{d} + \beta\mathbf{e} + \gamma\mathbf{f} = \mathbf{0} \tag{6.4}$$

From equation (6.3), $(\alpha + \beta)\mathbf{a} = -\gamma\mathbf{c}$. Since $\mathbf{a}$ and $\mathbf{c}$ are linearly independent, $\gamma = 0$ and $\alpha = -\beta$. But then equation (6.4) implies $\mathbf{d} = \mathbf{e}$, which is a contradiction.

Case III: $\mathbf{a} = \mathbf{b} = \mathbf{c}$. In this case $\mathbf{d}, \mathbf{e}, \mathbf{f}$ are all distinct and thus $\{\mathbf{d}, \mathbf{e}, \mathbf{f}\}$ is 3–independent. In turn $\mathbf{x}, \mathbf{y}, \mathbf{z}$ are linearly independent. □

The above results indicate that there is a close relationship between a set of t–independent vectors over $\mathbb{F}_q$ and a set of t–orthogonal frequency rectangles. This motivates an exploration of the maximum size of sets of t–independent vectors corresponding to different sets of parameters. For particular values of N, q and t, let $\mathrm{Ind}_q(N,t)$ denote the maximum possible size of a set of t–independent vectors of length N over a finite field $\mathbb{F}_q$. In the case of $q = 2$, we drop q and simply write $\mathrm{Ind}(N,t)$. As we know that any two vectors are linearly independent if and only if one is not a scalar multiple of the other, it is easy to see that $\mathrm{Ind}_q(N,2) = (q^N - 1)/(q-1)$. Also for any $t \geq 2$, $\mathrm{Ind}_q(N,t-1) \geq \mathrm{Ind}_q(N,t)$. The values $\mathrm{Ind}_q(N,t)$ when $t \geq 3$ are of interest to researchers in coding theory, combinatorics, and matroid theory [1, 2, 6, 7]. The following result in the case $q = 2$ is taken from [6].

Theorem 6.15. *For $q = 2$ the following formulae hold:*

(a)

$$\mathrm{Ind}(N,3) = 2^{N-1}, \qquad for\ \ N \geq 3. \tag{6.5}$$

(b)

$$\mathrm{Ind}(N, N-r) = N+1, \qquad for\ \ N \geq 3r+2, \quad r \geq 0. \tag{6.6}$$

(c)

$$\mathrm{Ind}(N, N-r) = N+2, \qquad for\ N = 3r+i,\ i = 0,1, \quad r \geq 2. \tag{6.7}$$

Part (b) of the above theorem was later generalized in [7].

Theorem 6.16. [7] *Let $2 \leq t \leq N$. Then $\mathrm{Ind}_q(N,t) = N+1$ if and only if*

$$\frac{q}{q+1}(N+1) \leq t.$$

The next two results discuss the upper bounds on $\mathrm{Ind}_q(N,t)$ in the case when $t = N$.

Theorem 6.17. [1] *Let $q = p^h$, where p is a prime. Then*

(a)

$$\mathrm{Ind}_q(N, N) \leq q + 1, \qquad if\ N \leq p. \tag{6.8}$$

(b)

$$\mathrm{Ind}_q(N, N) \leq q + N - p, \qquad if\ q \geq N \geq p + 1 \geq 4. \tag{6.9}$$

Theorem 6.18. [2] *Let $q = p^h$, where p is a prime, and let $N \leq 2p-2$. Then*

(a)

$$\mathrm{Ind}_q(N, N) \leq q + 2, \qquad if\ q \text{ is even and } N = 3 \text{ or } N = q - 1. \tag{6.10}$$

(b)

$$\mathrm{Ind}_q(N, N) \leq q + 1, \qquad otherwise. \tag{6.11}$$

The following values of $\mathrm{Ind}_q(N, t)$ for $q = 3$ are listed in [23]:

- $\mathrm{Ind}_3(5, 3) = 20$
- $\mathrm{Ind}_3(5, 4) = 11$
- $\mathrm{Ind}_3(6, 3) = 56$
- $\mathrm{Ind}_3(6, 4) = 13$
- $\mathrm{Ind}_3(6, 5) = 13$

Next, we discuss the connection between t–independent vectors and the field of coding theory. In the rest of this section, we restrict ourselves to the binary case.

A *linear code* C of length n, dimension k is a subspace of $(\mathbb{F}_q)^n$ of dimension k. Let $c_1, c_2 \in C$. The *hamming distance* $d(c_1, c_2)$ between the codewords c_1 and c_2 is the number of positions at which they differ. The minimum hamming distance d is defined as follows.

$$d = \min\{d(c_1, c_2) : c_1, c_2 \in C\}$$

A code with length n, dimension k, and minimum hamming distance d is called an $[n, k, d]$-code. The following result shows the relationship between a set of t–independent vectors and a linear $[n, k, d]$-code.

Lemma 6.19. [5] *There exists a linear $[n, k, d]$-code if and only if there exists a $(n-k)\times n$ matrix H such that any $d-1$ columns of H are linearly independent, but there exists a set of d columns which are not linearly independent.*

Corollary 6.20. *If there exists a linear $[n, k, d]$-code, then $\mathrm{Ind}(n-k, d-1) \geq n$.*

Lemma 6.21. *If $\mathrm{Ind}(n-k, d-1) \geq n$, then there exists a linear $[n, k, d']$-code for some $d' \geq d$.*

Proof. Suppose $\mathrm{Ind}(n-k, d-1) \geq n$. Then there exists a set of n vectors, each of length $n-k$ such that any subset of $d-1$ vectors is linearly independent. Let H be the $(n-k)\times n$ matrix whose columns are these vectors. Let d' be the smallest integer such that there exists a set of d' linearly dependent columns in H. Clearly $d' \geq d$. Moreover, any subset of $d'-1$ columns of H is linearly independent. Thus by Lemma 6.19, there exists a linear $[n, k, d']$-code. □

The following corollary is the contrapositive of the previous lemma.

Corollary 6.22. *Suppose that for all $d' \geq d$, there does not exist a linear $[n, k, d']$-code. Then $\mathrm{Ind}(n-k, d-1) < n$.*

Corollary 6.23. *Let D be the maximum value such that a linear $[n, k, D]$-code exists. Then $\mathrm{Ind}(n-k, D) < n$.*

Now we present some known values and bounds on $\mathrm{Ind}(N, t)$ for $N \leq 16$ in Table 6.3. Since $\mathrm{Ind}(N, 2) = 2^N - 1$ and $\mathrm{Ind}(N, 3) = 2^{N-1}$ (from Theorem 6.15(a)), we restrict ourselves to the values $t \geq 4$. Let $D(n, k)$ be the maximum value d such that a linear $[n, k, d]$-code exists.

Most of the results in Table 6.3 are obtained using an online repository for linear codes [11] in conjunction with Corollary 6.20 and Corollary 6.23. Some are obtained using the above results and [23]. The reasoning for each case is provided in the description. Also, the notation "a – b" in column $\mathrm{Ind}(N, t)$ implies $a \leq \mathrm{Ind}(N, t) \leq b$.

Let us compute $\mathrm{Ind}(9,4)$ as an example. From [11], a $[23,14,5]$-code exists; by Corollary 6.20 this implies $\mathrm{Ind}(9,4) \geq 23$. Also from [11], $D(24,15) = 4$. Thus by Corollary 6.23, $\mathrm{Ind}(9,4) < 24$. Consequently, we have $\mathrm{Ind}(9,4) = 23$.

Table 6.3: Values for $\mathrm{Ind}(N,t)$ for $N \leq 16$

N	t	$\mathbf{Ind}(N,t)$	**Description**
5	4	6	[23]
	5	6	Theorem 6.16
6	4	8	[23]
	5, 6	7	Theorem 6.16
7	4	11	[23]
	5	9	[23]
	6, 7	8	Theorem 6.16
8	4	17	[23]
	5	12	A $[12,4,6]$-code exists and $D(13,5) = 5$ ([11]).
	6	9	Theorem 6.15(b)
	7, 8	9	Theorem 6.16
9	4	23	A $[23,14,5]$-code exists and $D(24,15) = 4$ ([11]).
	5	18	A $[18,9,6]$-code exists and $D(19,10) = 5$ ([11]).
	6	11	A $[11,2,7]$-code exists and $D(12,3) = 6$ ([11]).
	7, 8, 9	10	Theorem 6.16

Table 6.3: (continued)

N	t	**Ind**(N,t)	**Description**
10	4	33	A $[33,23,5]$-code exists and $D(34,24)=4$ ([11]).
	5	24	A $[24,14,6]$-code exists and $D(25,15)=5$ ([11]).
	6	15	A $[15,5,7]$-code exists and $D(16,6)=6$ ([11]).
	7	12	Theorem 6.15(c)
	$8,9,10$	11	Theorem 6.16
11	4	$47-57$	A $[47,36,5]$-code exists and $D(58,47)=4$ ([11]).
	5	34	A $[34,23,6]$-code exists and $D(35,24)=5$ ([11]).
	6	23	A $[23,12,7]$-code exists and $D(24,13)=6$ ([11]).
	7	16	A $[16,5,8]$-code exists and $D(17,6)=7$ ([11]).
	8	12	Theorem 6.15(b)
	$9,10,11$	12	Theorem 6.16
12	4	$65-88$	A $[65,53,5]$-code exists and $D(89,77)=4$ ([11]).
	5	$48-58$	A $[48,36,6]$-code exists and $D(59,47)=5$ ([11]).
	6	24	A $[24,12,8]$-code exists and $D(25,13)=6$ ([11]).
	7	24	A $[24,12,8]$-code exists and $D(25,13)=6$ ([11]).
	8	14	Theorem 6.15(c)
	$9,\ldots,12$	13	Theorem 6.16

Table 6.3: (continued)

N	t	**Ind**(N,t)	**Description**
13	4	81 – 124	A $[81,68,5]$-code exists and $D(125,112)=4$ ([11]).
	5	66 – 89	A $[66,53,6]$-code exists and $D(90,77)=5$ ([11]).
	6	27	A $[27,14,7]$-code exists and $D(28,15)=6$ ([11]).
	7	25	A $[25,12,8]$-code exists and $D(26,13)=7$ ([11]).
	8	15	A $[15,2,10]$-code exists and $D(16,3)=8$ ([11]).
	9	15	A $[15,2,10]$ Theorem 6.15(c)
	$10,\ldots,13$	14	A $[15,2,10]$ Theorem 6.16
14	4	128 – 178	A $[128,114,5]$-code exists and $D(179,165)=4$ ([11]).
	5	82 – 125	A $[82,68,6]$-code exists and $D(126,112)=5$ ([11]).
	6	31 – 40	A $[31,17,7]$-code exists and $D(41,27)=6$ ([11]).
	7	28	A $[28,14,8]$-code exists and $D(29,15)=7$ ([11]).
	8	17	A $[17,3,9]$-code exists and $D(18,4)=8$ ([11]).
	9	16	A $[16,2,10]$-code exists and $D(17,3)=9$ ([11]).
	$10,\ldots,14$	15	Theorem 6.15(b)

Table 6.3: (continued)

N	t	$\mathbf{Ind}(N,t)$	**Description**
15	4	151 – 253	A $[151, 136, 5]$-code exists and $D(254, 239) = 4$ ([11]).
	5	129 – 179	A $[129, 114, 6]$-code exists and $D(180, 165) = 5$ ([11]).
	6	37 – 53	A $[37, 22, 7]$-code exists and $D(54, 39) = 6$ ([11]).
	7	32 – 41	A $[32, 17, 8]$-code exists and $D(42, 27) = 7$ ([11]).
	8	20	A $[20, 5, 9]$-code exists and $D(21, 6) = 8$ ([11]).
	9	18	A $[18, 3, 10]$-code exists and $D(19, 4) = 9$ ([11]).
	10	17	Theorem 6.15(c)
	$11, \ldots, 15$	16	Theorem 6.16
16	4	≥ 256	A $[256, 240, 5]$-code exists.
	5	152 – 254	A $[152, 136, 6]$-code exists and $D(255, 239) = 5$ ([11]).
	6	47 – 69	A $[47, 31, 7]$-code exists and $D(70, 54) = 6$ ([11]).
	7	38 – 54	A $[38, 22, 8]$-code exists and $D(55, 39) = 7$ ([11]).
	8	23	A $[23, 7, 9]$-code exists and $D(24, 8) = 8$ ([11]).
	9	21	A $[21, 5, 10]$-code exists and $D(22, 6) = 9$ ([11]).
	10	18	A $[18, 2, 12]$-code exists and $D(19, 3) = 10$ ([11]).
	11	18	Theorem 6.15(c)
	$12, \ldots, 16$	17	Theorem 6.16

If we know the value $\mathrm{Ind}_q(N,t)$ then by using Corollary 6.13 we can construct a set of $k = \mathrm{Ind}_q(N,t)$ t–orthogonal MOFR$(q^N, q^M; q)$, where $M \geq N$. However this method provides a lower bound that is, in general, not close to the actual upper bound. Consider the case when $q = 2, t = 3$ and $N = M = 2$. In this case, $\mathrm{Ind}(2,3)$ does not exist and hence does not provide a lower bound.

However, by Theorem 6.15(a) we know $\mathrm{Ind}(4,3) = 8$ and one such set is the set O (given below) of vectors of odd weight in $(\mathbb{F}_2)^4$.

$$O = \{1000, 0100, 0010, 0001, 1110, 1101, 1011, 0111\}.$$

Observe that only 4 elements of O satisfy the conditions of Theorem 6.12. Thus we can construct a set of 4–MOFR$(4,4;2)$ that is 3–orthogonal by using these elements in O. On the other hand, by inspection, we have found the following set:

$$W = \{1010, 1001, 1101, 0101, 1110, 0110, 0001, 0010\}$$

which is 3–independent and has 6 elements that satisfy the conditions of Theorem 6.12. In fact, the first 6 elements listed in W were used to construct 3–orthogonal 6-MOFR$(4,4,2)$ in Example 6.2.

This motivates us to propose the following problem.

Problem 6.24. *Let $S \subseteq (\mathbb{F}_q)^{M+N}$. For each set of admissible parameters t, M, N, and q, determine the maximum size of S such that:*

(i) *S is t–independent.*

(ii) *For each $\mathbf{v} = (v_1, \ldots, v_{M+N}) \in S$, $(v_1, \ldots, v_M) \neq (0, \ldots, 0)$ and $(v_{M+1}, \ldots, v_{M+N}) \neq (0, \ldots, 0)$.*

6.5 $p-1$ binary MOFS of size $2p$

In this section, our aim is to describe a method to construct a set of $p-1$ mutually orthogonal frequency squares of order $2p$, where p is an odd prime. The construction starts by generating a set of $p-1$ frequency squares which are almost orthogonal. Then we make some small changes in each frequency square in order to make the set orthogonal. Here we set out some notations that we use frequently in this section.

Let $[n] = \{0, 1, \ldots, n-1\}$, where n is an integer. Let H be an $m \times n$ array. The rows and columns of H are indexed using $[m]$ and $[n]$. The entry

in the intersection of row i and column j of the array H is denoted by $h(i,j)$. As previously, if H is a binary array then $\overline{H}$ is the array obtained from H by interchanging zeroes and ones.

Let A and B be two $m \times n$ binary arrays. We use the notation $|AB|_{(x,y)}$, where $x, y \in \{0,1\}$, to denote the total number of ordered pairs (i,j) such that $a(i,j) = x$ and $b(i,j) = y$, that is the total number of ordered pairs of type (x,y) obtained when A and B are superimposed. The term *orthogonality* between the arrays A and B means a sequence that contains the numbers $|AB|_{(x,y)}$ for all $x, y \in \{0,1\}$. However, the term *orthogonal* has its usual meaning, i.e., A and B are said to be orthogonal if each type of ordered pair appears the same number of times upon superimposition.

Recall that if $\mathbf{c} = (c_0, c_1, \ldots, c_r)$ is a vector then by the cyclic shift of $\mathbf{c}$ we mean the vector $\mathbf{c}' = (c_r, c_0, c_1, \ldots, c_{r-1})$. Let p be an odd prime. Let $\mathbf{v} \in (\mathbb{F}_2)^p$ be the vector $\mathbf{v} = (1, 1, \ldots, 1, 0, 0, \ldots, 0)$ of weight $(p+1)/2$. Let $\mathbf{v}_i$ denote the vector obtained from $\mathbf{v}$ by performing i cyclic shifts. Throughout this section $\Omega = \{1, \ldots, p-1\}$ and $K = \{1, \ldots, \frac{p-1}{2}\}$. We include here some observations related to the vectors $\mathbf{v}_i$.

Lemma 6.25. *Let $z \in [(p+1)/2]$. Upon superimposing $\mathbf{v}_i\mathbf{v}_j$, the following are equivalent:*

(a) $|\mathbf{v}_i\mathbf{v}_j|_{(1,0)} = z$.

(b) $|\mathbf{v}_i\mathbf{v}_j|_{(0,1)} = z$.

(c) $|\mathbf{v}_i\mathbf{v}_j|_{(0,0)} = \frac{p-1}{2} - z$.

(d) $|\mathbf{v}_i\mathbf{v}_j|_{(1,1)} = \frac{p+1}{2} - z$.

Proof. Each vector contains exactly $(p-1)/2$ zeroes. □

Corollary 6.26. *Superimposing $\mathbf{v}_i$ and $\mathbf{v}_j$ in either order yields the same number of ordered pairs of each type, i.e., $|\mathbf{v}_i\mathbf{v}_j|_{(x,y)} = |\mathbf{v}_j\mathbf{v}_i|_{(x,y)}$.*

Lemma 6.27. *For $i \in [(p+1)/2]$,*

(a) $|\mathbf{v}_0\mathbf{v}_i|_{(1,0)} = |\mathbf{v}_0\mathbf{v}_i|_{(0,1)} = i$.

(b) $|\mathbf{v}_0\mathbf{v}_i|_{(0,0)} = \frac{p-1}{2} - i$.

(c) $|\mathbf{v}_0\mathbf{v}_i|_{(1,1)} = \frac{p+1}{2} - i$.

Lemma 6.28. *For any $i, j \in [p]$ and $x, y \in \{0, 1\}$, we have the following:*

(a) $|\mathbf{v}_0\mathbf{v}_i|_{(x,y)} = |\mathbf{v}_0\mathbf{v}_{p-i}|_{(x,y)}$.

(b) $|\mathbf{v}_i\mathbf{v}_j|_{(x,y)} = |\mathbf{v}_0\mathbf{v}_r|_{(x,y)}$, *where* $r \in [p]$, $r \equiv j - i \pmod{p}$.

Proof. This follows from Corollary 6.26 and the observation $|\mathbf{v}_i\mathbf{v}_j|_{(x,y)} = |\mathbf{v}_{i+1}\mathbf{v}_{j+1}|_{(x,y)}$. □

Now we define a set of $p - 1$ arrays each of which consists of a different permutation of the vectors $\mathbf{v}_i$. These arrays will be our primary building blocks in defining our frequency squares. Formally, for each $\alpha \in \Omega$, let A_α be a $p \times p$ binary array such that for each $i \in [p]$ its row i is $\mathbf{v}_r$, where $r \in [p]$ is the unique solution to $r \equiv \alpha i \pmod{p}$. The next lemma records the total number of order pairs of each type obtained when these arrays are superimposed.

Lemma 6.29. *Let $\alpha, \beta \in \Omega$ and $\alpha \neq \beta$. Then:*

(a) $|A_\alpha A_\beta|_{(1,0)} = |A_\alpha A_\beta|_{(0,1)} = (p^2 - 1)/4$.

(b) $|A_\alpha A_\beta|_{(0,0)} = (p - 1)^2/4$.

(c) $|A_\alpha A_\beta|_{(1,1)} = (p + 1)^2/4$.

Proof. When we superimpose $A_\alpha A_\beta$ the corresponding rows are $\mathbf{v}_{r_1(i)}\mathbf{v}_{r_2(i)}$ where $r_1(i), r_2(i) \in [p]$ and $r_1(i) \equiv \alpha i \pmod{p}$, $r_2(i) \equiv \beta i \pmod{p}$ for each $i \in [p]$. Thus,

$$
\begin{aligned}
|A_\alpha A_\beta|_{(x,y)} &= \sum_{i=0}^{p-1} |\mathbf{v}_{r_1(i)}\mathbf{v}_{r_2(i)}|_{(x,y)} \qquad r_1(i), r_2(i) \in [p], \\
&\qquad\qquad r_1(i) \equiv \alpha i \pmod{p}, \quad r_2(i) \equiv \beta i \pmod{p} \\
&= \sum_{i=0}^{p-1} |\mathbf{v}_0\mathbf{v}_{r(i)}|_{(x,y)} \qquad r(i) \in [p], \\
&\qquad\qquad r(i) \equiv (\beta - \alpha)i \pmod{p} \qquad \text{(by Lemma 6.28(b))}.
\end{aligned}
$$

Since $\alpha \not\equiv \beta \pmod{p}$, $\{r(i) : i \in [p]\}$ forms a complete set of residues modulo p. Thus by using Lemma 6.28(a) we have:

$$|A_\alpha A_\beta|_{(x,y)} = \sum_{i=0}^{p-1} |\mathbf{v}_0 \mathbf{v}_i|_{(x,y)} = |\mathbf{v}_0 \mathbf{v}_0|_{(x,y)} + 2 \sum_{i=1}^{(p-1)/2} |\mathbf{v}_0 \mathbf{v}_i|_{(x,y)} \tag{6.12}$$

Now by using the values of $|\mathbf{v}_0 \mathbf{v}_i|_{(x,y)}$ from Lemma 6.27 we get:

$$|A_\alpha A_\beta|_{(1,0)} = |A_\alpha A_\beta|_{(0,1)} = 0 + 2 \sum_{i=1}^{(p-1)/2} i = (p^2-1)/4,$$

$$|A_\alpha A_\beta|_{(0,0)} = \frac{p-1}{2} + 2 \sum_{i=1}^{(p-1)/2} \left(\frac{p-1}{2} - i \right) = \frac{p(p-1)}{2} - 2 \sum_{i=1}^{(p-1)/2} i = \frac{(p-1)^2}{4}.$$

Now (c) follows since:

$$\sum_{x,y \in \{0,1\}} |A_\alpha A_\beta|_{(x,y)} = p^2.$$

□

Corollary 6.30. *Let $\alpha, \beta \in \Omega$ and $\alpha \neq \beta$. Then:*

(a) $|\overline{A}_\alpha \overline{A}_\beta|_{(1,0)} = |\overline{A}_\alpha \overline{A}_\beta|_{(0,1)} = (p^2-1)/4.$

(b) $|\overline{A}_\alpha \overline{A}_\beta|_{(0,0)} = (p+1)^2/4.$

(c) $|\overline{A}_\alpha \overline{A}_\beta|_{(1,1)} = (p-1)^2/4.$

Now let us construct a set of $p-1$ frequency squares. Corresponding to each $\alpha \in \Omega$ we construct a binary frequency square L_α of order $2p$ as follows.

$$L_\alpha = \left[\begin{array}{c|c} A_\alpha & \overline{A_\alpha} \\ \hline \overline{A_\alpha} & A_\alpha \end{array}\right] \tag{6.13}$$

For $\alpha \neq \beta$, by Lemma 6.29 and Corollary 6.30 the total number of ordered pairs (x, y) when L_α and L_β superimposed are as follows:

$$\begin{aligned} |L_\alpha L_\beta|_{(1,0)} &= |L_\alpha L_\beta|_{(0,1)} = p^2 - 1 \\ |L_\alpha L_\beta|_{(0,0)} &= |L_\alpha L_\beta|_{(1,1)} = p^2 + 1 \end{aligned} \tag{6.14}$$

Thus we have a set of $p-1$ frequency squares that are almost orthogonal. Now we will make some small changes in order to make these squares pairwise

orthogonal. Specifically, in the first and the fourth quadrant, we will flip some entries in a way that some of these arrays will become orthogonal to each other without disrupting the orthogonality between other pairs.

We introduce some more terminology here that we will use often in the rest of this section. Let $H_1, \ldots, H_n$ be a set of n binary arrays. Let $h_\alpha(i,j)$ denote the entry in the intersection of row i and column j of H_α, where $i, j \in [n]$. Let s_α be a 2×2 sub-array of H_α. Then the arrays $s_1, \ldots, s_n$ are said to be *coincident* if for each $\alpha \in \{1, \ldots, n\}$, s_α is of the form:

$$s_\alpha = \begin{pmatrix} h_\alpha(i,j) & h_\alpha(i,j') \\ h_\alpha(i',j) & h_\alpha(i',j') \end{pmatrix}, \qquad \text{for some fixed } i, j, i', j' \in [n]$$

that is, each s_α is a sub-square of H_α and all s_α correspond to the same positions within H_α.

The next lemma describes the effect on the orthogonality between any two binary arrays when we flip the entries of a 2×2 sub-array of one of them.

Lemma 6.31. *Let A and B be two binary arrays of size $m \times n$, where $m, n \geq 2$. Let s_1, s_2 be two 2×2 coincident sub-arrays of A and B, respectively. Let B' be the array obtained from B in which s_2 is replaced by $\overline{s_2}$, where $s_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.*

1. *If $s_1 = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, then:*

   (a) $|AB'|_{(x,y)} = |B'A|_{(x,y)} = |AB|_{(x,y)} + 1$, *where $x, y \in \{0,1\}$ and $x \neq y$.*

   (b) $|AB'|_{(x,x)} = |B'A|_{(x,x)} = |AB|_{(x,x)} - 1$, *where $x \in \{0,1\}$.*

2. *If $s_1 = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 0 \end{smallmatrix}\right)$, then $|AB'|_{(x,y)} = |B'A|_{(x,y)} = |AB|_{(x,y)}$, for all $x, y \in \{0,1\}$.*

3. *If B is a binary frequency square then B' is a binary frequency square.*

In what follows it will be useful to give an explicit formula for the entry of each cell in A_α.

Lemma 6.32. *Let $a_\alpha(i,j)$ denote the entry in the intersection of row i and column j of A_α, where $i,j \in [p]$. Then*

$$a_\alpha(i,j) = \begin{cases} 0 & \text{if} \quad (1-p)/2 \le j-r \le -1 \quad \text{or} \quad (p+1)/2 \le j-r \le p-1 \\ 1 & \text{otherwise,} \end{cases}$$

where $r \equiv \alpha i \pmod p$ and $0 \le r \le p-1$.

Now we describe different sets of coincident sub-arrays of A_α that we will use later on to alter the orthogonality between the arrays. Formally, let $a_\alpha(i,j)$ denote the entry in the intersection of row i and column j of A_α, where $i,j \in [p]$. For each $h \in K$ and $\alpha \in \Omega$ we define:

$$s_{(\alpha,h)} = \begin{pmatrix} a_\alpha(0,h) & a_\alpha(0,\frac{p-1}{2}+h) \\ a_\alpha(1,h) & a_\alpha(1,\frac{p-1}{2}+h) \end{pmatrix} \tag{6.15}$$

Then for each $h \in K$ the set $\{s_{(\alpha,h)} : \alpha \in \Omega\}$ forms a set of coincident sub-arrays of A_α. The configuration of each sub-array is given in the following lemma.

Lemma 6.33. *For each $h,k \in K$ and $\beta \in \Omega \setminus \{h, h+1, \ldots, h+\frac{p-1}{2}\}$ we have:*

$$s_{(h,h)} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad s_{(h+k,h)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad s_{(\beta,h)} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}.$$

Proof. This follows by Lemma 6.32. □

We next verify that the coincident arrays that we later use do not overlap. The following lemma follows from the definition (6.15) of $s_{(\alpha,h)}$.

Lemma 6.34. *Let $h,h' \in K$ such that $h \neq h'$. Then for each $\alpha \in \Omega$, the set of cells in $s_{(\alpha,h)}$ is disjoint from the set of cells in $s_{(\alpha,h')}$.*

Consider the set $\{A_\alpha : \alpha \in \Omega\}$ in the first quadrant of the arrays L_α (given in 6.13). By Lemma 6.33 and Lemma 6.31, for each $h \in K$, if we replace $s_{(h+k,h)}$ with $\overline{s}_{(h+k,h)}$ for all $k \in K$, the array L_h becomes orthogonal to each

array in the set $\{L_{h+1}, L_{h+2}, \ldots, L_{h+(p-1)/2}\}$, while the orthogonality between rest of the arrays remains unchanged. However, this does not cover the whole spectrum of the pairs which are subsets of $\{L_\alpha : \alpha \in \Omega\}$. Our next step is to apply similar transformations to the arrays A_α in the fourth quadrant of L_α. To ensure that we are covering the whole spectrum without repetitions, we will use the analogy of a complete graph. That is we want to establish a one-to-one correspondence between the edges of a complete graph with $p-1$ vertices such that each vertex represents a unique frequency square and an edge between two vertices implies that the two arrays are orthogonal. We start with the following result from graph theory.

Lemma 6.35. *Let G_{p-1} be the complete graph with vertex set $V = \{\infty\} \cup \{0, 1, \ldots, p-3\}$. Let S_i be the star with edge-set $\{\{i, \infty\}, \{i, i+1\}, \{i, i+2\}, \ldots, \{i, i+\frac{p-3}{2}\}\}$ (working modulo $(p-2)$ with residues in $\{0, 1, \ldots, p-3\}$). Then $\{S_1, S_2, \ldots, S_{p-2}\}$ is a partition of the edge set of G_{p-1}.*

Next, we relabel the vertices of the graph G_{p-1} by the mapping $f : V \to \Omega$ defined as follows:

$$f(z) = \begin{cases} (p+1)/2 & \text{if} \quad z = \infty \\ p-1 & \text{if} \quad z = 0 \\ z & \text{if} \quad 1 \leq z \leq (p-1)/2 \\ z+1 & \text{if} \quad (p+1)/2 \leq z \leq p-3. \end{cases}$$

The relabelling of vertices by using f is shown in the figure given below.

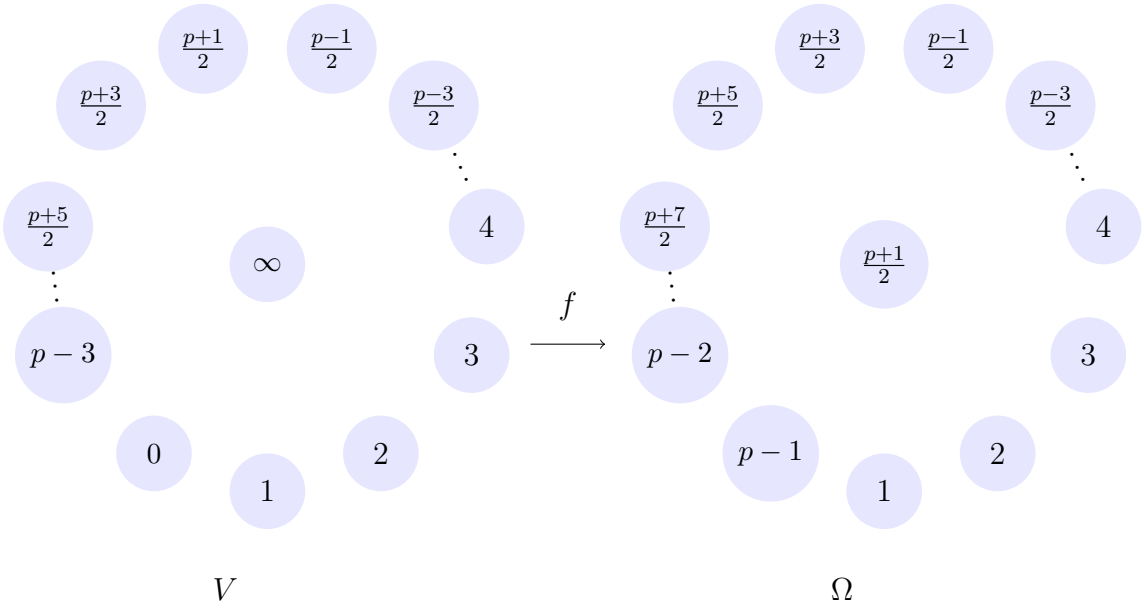


Figure 1

For each star:

$$S_i = \{\{i, \infty\}, \{i, i+1\}, \{i, i+2\}, \ldots, \{i, i+(p-3)/2\}\},$$

we define

$$f(S_i) = \{\{f(i), f(\infty)\}, \{f(i), f(i{+}1)\}, \{f(i), f(i{+}2)\}, \ldots, \{f(i), f(i{+}(p{-}3)/2)\}\}.$$

Then the set of stars S_i for $1 \leq i \leq (p-1)/2$ are transformed as described in the next lemma.

Lemma 6.36. *For* $1 \leq i \leq (p-1)/2$, $f(S_i) = \{\{i, i+1\}, \{i, i+2\}, \ldots, \{i, i+(p-1)/2\}\}$.

Proof. Observe that it is true for $i = 1$. Now for $2 \leq i \leq (p-1)/2$, S_i

transforms as follows:

$$\begin{array}{ccc} S_i & \xrightarrow{f} & f(S_i) \\ \{i, i+1\} & & \{i, i+1\} \\ \{i, i+2\} & & \{i, i+2\} \\ \vdots & & \vdots \\ \{i, (p-1)/2\} & & \{i, (p-1)/2\} \\ \{i, \infty\} & & \{i, (p+1)/2\} \\ \{i, (p+1)/2\} & & \{i, (p+3)/2\} \\ \vdots & & \vdots \\ \{i, i+(p-3)/2\} & & \{i, i+(p-1)/2\} \end{array}$$

Thus we have the required result. □

Consider the following permutation on the set Ω.

$$\rho(z) = \begin{cases} z & \text{if} \quad z = (p+1)/2 \\ 1 & \text{if} \quad z = (p-1)/2 \\ (z + \frac{p+1}{2}) \pmod p & \text{otherwise.} \end{cases}$$

By the definition of f and ρ, the remaining set of stars, $f(S_i)$ where $(p+1)/2 \leq i \leq p-2$ can be expressed as follows.

Lemma 6.37. *For* $1 \leq i \leq (p-3)/2$, $f(S_{i+(p-1)/2}) = \rho(f(S_i))$.

Proof. Let $j = i+(p-1)/2$, where $1 \leq i \leq (p-3)/2$. Then $(p+1)/2 \leq j \leq p-2$. We want to show that $f(S_j) = \rho(f(S_i))$. By using the definitions of f and ρ the transformations are as follows:

$$
\begin{array}{ccccc}
S_j & \xrightarrow{f} & f(S_j) & & \rho(f(S_i)) & \xleftarrow{\rho} & f(S_i) \\
\{j,\infty\} & & \{j+1,(p+1)/2\} & = & \{j+1,(p+1)/2\} & & \{i,(p+1)/2\} \\
\{j,j+1\} & & \{j+1,j+2\} & = & \{j+1,i+1+(p+1)/2\} & & \{i,i+1\} \\
\vdots & & \vdots & & \vdots & & \vdots \\
\{j,p-3\} & & \{j+1,p-2\} & = & \{j+1,(p-5)/2+(p+1)/2\} & & \{i,(p-5)/2\} \\
\{j,0\} & & \{j+1,p-1\} & = & \{j+1,(p-3)/2+(p+1)/2\} & & \{i,(p-3)/2\} \\
\{j,1\} & & \{j+1,1\} & = & \{j+1,1\} & & \{i,(p-1)/2\} \\
\{j,2\} & & \{j+1,2\} & = & \{j+1,(p+3)/2+(p+1)/2\} & & \{i,(p+3)/2\} \\
\vdots & & \vdots & & \vdots & & \vdots \\
\{j,j+(p-3)/2\} & & \{j+1,j+(p-3)/2\} & = & \{j+1,i\} & & \{i,i+(p-1)/2\}
\end{array}
$$

Hence the result. □

By combining Lemma 6.36 and Lemma 6.37 we have the following result.

Lemma 6.38. *The set of stars* $\{f(S_i) : i \in K\} \cup \{\rho(f(S_i)) : 1 \leq i \leq (p-3)/2\}$ *partitions the edge-set of the complete graph* G_{p-1} *with the vertex set* Ω.

Now consider the set of sub-arrays $\{s_{(\alpha,h)} : \alpha \in \Omega, h \in K\}$ defined in (6.15). Let $\{A^*_\alpha : \alpha \in \Omega\}$ be the set of arrays obtained by replacing $s_{(h+k,h)}$ with $\overline{s}_{(h+k,h)}$ in A_{h+k} for each $h, k \in K$. Then we have the following.

Lemma 6.39. *Let* $\{A^*_\alpha : \alpha \in \Omega\}$ *be the set of arrays described above.*

1. *If* $\{\alpha, \beta\} \in f(S_i)$ *for some* $1 \leq i \leq (p-1)/2$, *then:*
   (a) $|A^*_\alpha A^*_\beta|_{(x,y)} = |A_\alpha A_\beta|_{(x,y)} + 1$, *where* $x, y \in \{0,1\}$ *and* $x \neq y$.
   (b) $|A^*_\alpha A^*_\beta|_{(x,x)} = |A_\alpha A_\beta|_{(x,x)} - 1$, *where* $x \in \{0,1\}$.
2. *Otherwise:* $|A^*_\alpha A^*_\beta|_{(x,y)} = |A_\alpha A_\beta|_{(x,y)}$.

Proof. This follows by Lemma 6.33 and Lemma 6.31. □

Now we define another set of arrays $\{A'_\alpha : \alpha \in \Omega\}$ that we will use in the fourth quadrant of our final arrays. Formally, let $\{A'_\alpha : \alpha \in \Omega\}$ be the set of arrays obtained by replacing $s_{(h+k,h)}$ with $\overline{s}_{(h+k,h)}$ in A_{h+k} for each $h \in$

$\{1, 2, \ldots, \frac{p-3}{2}\}$ and $k \in K$. Observe that the array $A'_\alpha = A^*_\alpha$ for $\alpha \in \Omega \setminus \{(p+1)/2, \ldots, p-1\}$ and for $\alpha \in \{(p+1)/2, \ldots, p-1\}$, the only difference between A'_α and A^*_α is that the array A'_α contains $s_{(\alpha,h)}$ and A^*_α contains $\overline{s}_{(\alpha,h)}$ for $h = (p-1)/2$. Thus we have a similar result as Lemma 6.39 for the set $\{A'_\alpha : \alpha \in \Omega\}$.

Lemma 6.40. *Let $\{A'_\alpha : \alpha \in \Omega\}$ be the set of arrays described above.*

1. *If $\{\alpha, \beta\} \in f(S_i)$ for some $1 \le i \le (p-3)/2$, then:*
   (a) $|A'_\alpha A'_\beta|_{(x,y)} = |A_\alpha A_\beta|_{(x,y)} + 1$, *where $x, y \in \{0, 1\}$ and $x \neq y$.*
   (b) $|A'_\alpha A'_\beta|_{(x,x)} = |A_\alpha A_\beta|_{(x,x)} - 1$, *where $x \in \{0, 1\}$.*
2. *Otherwise: $|A'_\alpha A'_\beta|_{(x,y)} = |A_\alpha A_\beta|_{(x,y)}$.*

Now we give our main result.

Theorem 6.41. *Let $p \ge 3$ be a prime. Then there exists a set of $p-1$ binary MOFS of order $2p$.*

Proof. Corresponding to each $\alpha \in \Omega$ we construct a binary frequency square L_α of order $2p$ as follows.

$$F_\alpha = \left[\begin{array}{c|c} A^*_\alpha & \overline{A}_\alpha \\ \hline \overline{A}_\alpha & A'_{\rho^{-1}(\alpha)} \end{array}\right] \tag{6.16}$$

Let $\alpha, \beta \in \Omega$. Let $\alpha' = \rho^{-1}(\alpha)$ and $\beta' = \rho^{-1}(\beta)$. Then, for all $x, y \in \{0, 1\}$:

$$|F_\alpha F_\beta|_{(x,y)} = |A^*_\alpha A^*_\beta|_{(x,y)} + 2|\overline{A}_\alpha \overline{A}_\beta|_{(x,y)} + |A'_{\alpha'} A'_{\beta'}|_{(x,y)} \tag{6.17}$$

Now consider the following two cases:

Case I: $\{\alpha, \beta\} \in f(S_i)$ for some $i \in K$. Then, by Lemma 6.38, $\{\alpha, \beta\} \notin \rho(f(S_i))$ for all $i \in \{1, \ldots, (p-3)/2\}$. This implies $\{\rho^{-1}(\alpha), \rho^{-1}(\beta)\} \notin f(S_i)$ for all $i \in \{1, \ldots, (p-3)/2\}$. Thus by Lemma 6.39 and Lemma 6.40 we have:

$$|A^*_\alpha A^*_\beta|_{(x,y)} = |A_\alpha A_\beta|_{(x,y)} + 1 \qquad \text{whenever } x \neq y$$

$$|A^*_\alpha A^*_\beta|_{(x,y)} = |A_\alpha A_\beta|_{(x,y)} - 1 \qquad \text{when } x = y$$

$$|A'_{\alpha'} A'_{\beta'}|_{(x,y)} = |A_{\alpha'} A_{\beta'}|_{(x,y)} = |A_\alpha A_\beta|_{(x,y)} \quad \text{for all } x, y \in \{0, 1\}.$$

Therefore, by using Lemma 6.29 and Corollary 6.30 in (6.17) we get:

$$|F_\alpha F_\beta|_{(x,y)} = p^2 \quad \text{for all } x, y \in \{0, 1\}.$$

Case II: $\{\alpha, \beta\} \notin f(S_i)$ for all $i \in K$. Then, by Lemma 6.38, $\{\alpha, \beta\} \in \rho(f(S_i))$ for some $i \in \{1, \ldots, (p-3)/2\}$. This implies $\{\rho^{-1}(\alpha), \rho^{-1}(\beta)\} \in f(S_i)$ for some $i \in \{1, \ldots, (p-3)/2\}$. Thus by Lemma 6.39 and Lemma 6.40 we have:

$$|A'_{\alpha'} A'_{\beta'}|_{(x,y)} = |A_{\alpha'} A_{\beta'}|_{(x,y)} + 1 = |A_\alpha A_\beta|_{(x,y)} + 1 \quad \text{whenever } x \neq y$$

$$|A'_{\alpha'} A'_{\beta'}|_{(x,y)} = |A_{\alpha'} A_{\beta'}|_{(x,y)} - 1 = |A_\alpha A_\beta|_{(x,y)} - 1 \quad \text{when } x = y$$

$$|A^*_\alpha A^*_\beta|_{(x,y)} = |A_\alpha A_\beta|_{(x,y)} \quad \text{for all } x, y \in \{0, 1\}.$$

Therefore, again by using Lemma 6.29 and Corollary 6.30 in (6.17) we get:

$$|F_\alpha F_\beta|_{(x,y)} = p^2 \quad \text{for all } x, y \in \{0, 1\}.$$

This completes the proof. □

Next, we include an example here to further illustrate the construction.

Example 6.42. Let us construct a set of 6 binary MOFS of order 14. Here $p = 7$, $\Omega = \{1, \ldots, 6\}$, $K = \{1, 2, 3\}$ and $\mathbf{v} = (1, 1, 1, 1, 0, 0, 0)$. The set of A_α for $\alpha \in \Omega$ is given in Table 6.4.

1	1	1	1	0	0	0
0	1	1	1	1	0	0
0	0	1	1	1	1	0
0	0	0	1	1	1	1
1	0	0	0	1	1	1
1	1	0	0	0	1	1
1	1	1	0	0	0	1

A_1

1	1	1	1	0	0	0
0	0	1	1	1	1	0
1	0	0	0	1	1	1
1	1	1	0	0	0	1
0	1	1	1	1	0	0
0	0	0	1	1	1	1
1	1	0	0	0	1	1

A_2

1	1	1	1	0	0	0
0	0	0	1	1	1	1
1	1	0	0	0	1	1
0	0	1	1	1	1	0
1	1	0	0	0	1	1
0	1	1	1	1	0	0
1	0	0	0	1	1	1

A_3

1	1	1	1	0	0	0
1	0	0	0	1	1	1
0	1	1	1	1	0	0
1	1	0	0	0	1	1
0	0	1	1	1	1	0
1	1	1	0	0	0	1
0	0	0	1	1	1	1

A_4

1	1	1	1	0	0	0
1	1	0	0	0	1	1
0	0	0	1	1	1	1
0	1	1	1	1	0	0
1	1	1	0	0	0	1
1	0	0	0	1	1	1
0	0	1	1	1	1	0

A_5

1	1	1	1	0	0	0
1	1	1	0	0	0	1
1	1	0	0	0	1	1
1	0	0	0	1	1	1
0	0	0	1	1	1	1
0	0	1	1	1	1	0
0	1	1	1	1	0	0

A_6

Table 6.4: Set of A_α to construct 6–MOFS(14)

Now consider the set of coincident arrays $\{s_{(\alpha,1)} : \alpha \in \Omega\}$ described in (6.15), shown as highlighted cells in Table 6.4. Then A_1 contains $\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$, $A_2, \ldots, A_4$ contain $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ and the rest of A_α contain $\left(\begin{smallmatrix}1&0\\1&0\end{smallmatrix}\right)$ at this position. We replace $s_{(\alpha,1)} = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ with $\overline{s}_{(\alpha,1)} = \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ in A_α for $\alpha \in \{2,3,4\}$. Similarly, by replacing $s_{(h+k,h)}$ with $\overline{s}_{(h+k,h)}$ in A_{h+k} for $h \in \{2,3\}$ and $k \in K$, we get the set $\{A^*_\alpha : \alpha \in \Omega\}$. The first two rows of $A^*_\alpha, \alpha \in \Omega$ are shown in Table 6.5.

1	1	1	1	0	0	0
0	1	1	1	1	0	0

A^*_1

1	0	1	1	1	0	0
0	1	1	1	0	1	0

A^*_2

1	0	0	1	1	1	0
0	1	1	1	0	0	1

A^*_3

1	0	0	0	1	1	1
1	1	1	1	0	0	0

A^*_4

1	1	0	0	0	1	1
1	1	1	1	0	0	0

A^*_5

1	1	1	0	0	0	1
1	1	1	1	0	0	0

A^*_6

Table 6.5: First two rows of A^*_α to construct 6–MOFS(14)

Now to obtain the set $\{A'_\alpha : \alpha \in \Omega\}$, we repeat the same procedure as above only this time we do not replace $s_{(h+k,h)}$ with $\overline{s}_{(h+k,h)}$ when $h = (p-1)/2$. The

first two rows of A'_α are shown in Table 6.6. Observe the difference between A^*_α and A'_α for $\alpha \in \{4, 5, 6\}$ in the highlighted cells of Table 6.5 and Table 6.6.

1	1	1	1	0	0	0
0	1	1	1	1	0	0

A'_1

1	0	1	1	1	0	0
0	1	1	1	0	1	0

A'_2

1	0	0	1	1	1	0
0	1	1	1	0	0	1

A'_3

1	0	0	1	1	1	0
1	1	1	0	0	0	1

A'_4

1	1	0	1	0	1	0
1	1	1	0	0	0	1

A'_5

1	1	1	1	0	0	0
1	1	1	0	0	0	1

A'_6

Table 6.6: First two rows of A'_α to construct 6–MOFS(14)

Now consider the permutation ρ on the set Ω.

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 4 & 2 & 3 \end{pmatrix}$$

Thus we get a set $\{F_\alpha : \alpha \in \Omega\}$ of 6 binary MOFS of order 14, where F_α is of the form:

$$F_\alpha = \left[\begin{array}{c|c} A^*_\alpha & \overline{A}_\alpha \\ \hline \overline{A}_\alpha & A'_{\rho^{-1}(\alpha)} \end{array}\right]$$

A complete description of each frequency square F_α is given in Appendix A (6.6).

6.6 Appendix A: 6 binary MOFS(14)

1	1	1	1	0	0	0	0	0	0	0	1	1	1
0	1	1	1	1	0	0	1	0	0	0	0	1	1
0	0	1	1	1	1	0	1	1	0	0	0	0	1
0	0	0	1	1	1	1	1	1	1	0	0	0	0
1	0	0	0	1	1	1	0	1	1	1	0	0	0
1	1	0	0	0	1	1	0	0	1	1	1	0	0
1	1	1	0	0	0	1	0	0	0	1	1	1	0
0	0	0	0	1	1	1	1	0	0	1	1	1	0
1	0	0	0	0	1	1	0	1	1	1	0	0	1
1	1	0	0	0	0	1	1	1	1	0	0	0	1
1	1	1	0	0	0	0	0	0	1	1	1	1	0
0	1	1	1	0	0	0	1	1	0	0	0	1	1
0	0	1	1	1	0	0	0	1	1	1	1	0	0
0	0	0	1	1	1	0	1	0	0	0	1	1	1

F_1

1	0	1	1	1	0	0	0	0	0	1	1	1	
0	1	1	1	0	1	0	1	1	0	0	0	0	1
1	0	0	0	1	1	1	0	1	1	1	0	0	0
1	1	1	0	0	0	1	0	0	0	1	1	1	0
0	1	1	1	1	0	0	1	0	0	0	0	1	1
0	0	0	1	1	1	1	1	1	1	0	0	0	0
1	1	0	0	0	1	1	0	0	1	1	1	0	0
0	0	0	0	1	1	1	1	0	1	0	0	1	0
1	1	0	0	0	0	1	1	1	1	0	0	0	1
0	1	1	1	0	0	0	0	0	1	1	1	1	1
1	0	0	0	1	1	1	0	1	1	1	0	0	0
1	1	1	0	0	0	0	1	1	1	0	0	0	1
0	0	1	1	1	0	0	0	0	1	1	1	1	0
0	0	1	1	1	1	0	0	0	1	1	1	1	0

F_2

1	0	0	1	1	1	0	0	0	0	0	1	1	1
0	1	1	1	0	0	1	1	1	1	0	0	0	0
1	1	1	0	0	0	1	0	0	0	1	1	1	0
0	0	1	1	1	1	0	1	1	0	0	0	0	1
1	1	0	0	0	1	1	0	0	1	1	1	0	0
0	1	1	1	1	0	0	1	0	0	0	0	1	1
1	0	0	0	1	1	1	0	1	1	1	0	0	0
0	0	0	0	1	1	1	1	1	1	0	0	0	1
1	1	1	1	0	0	0	1	1	1	0	0	0	1
0	0	0	1	1	1	0	1	1	0	0	0	1	1
1	1	0	0	0	0	1	1	0	0	0	1	1	1
0	0	1	1	1	0	0	0	0	0	1	1	1	1
1	0	0	0	0	1	1	0	0	1	1	1	1	0
0	1	1	1	0	0	0	0	1	1	1	1	0	0

F_3

1	0	0	0	1	1	1	0	0	0	0	1	1	1
1	1	1	1	0	0	0	0	1	1	1	0	0	0
0	1	1	1	1	0	0	1	0	0	0	1	1	1
1	1	0	0	0	1	1	0	0	1	1	1	0	0
0	0	1	1	1	1	0	1	1	1	0	0	0	1
1	1	1	0	0	0	1	0	0	0	1	1	1	0
0	0	0	1	1	1	1	1	1	1	0	0	0	0
0	0	0	0	1	1	1	1	0	0	0	1	1	1
0	1	1	1	0	0	0	1	1	1	0	0	0	1
1	0	0	0	1	1	1	0	1	1	0	0	0	1
1	1	0	0	0	0	1	1	0	0	1	1	1	0
0	0	1	1	1	0	0	0	1	1	0	0	1	1
1	1	0	0	0	0	1	0	0	1	1	1	1	0
0	1	1	1	0	0	0	1	1	0	0	0	1	1

F_4

1	1	0	0	0	1	1	0	0	0	0	1	1	1
1	1	1	1	0	0	0	0	0	1	1	1	0	0
0	0	0	1	1	1	1	1	1	1	0	0	0	0
0	1	1	1	1	0	0	1	0	0	0	0	1	1
1	1	1	0	0	0	1	0	0	0	1	1	1	0
1	0	0	0	1	1	1	0	1	1	1	0	0	0
0	0	1	1	1	1	0	1	1	0	0	0	0	1
0	0	0	0	1	1	1	1	1	1	0	0	0	0
0	0	1	1	1	0	0	0	1	1	1	0	0	0
1	1	1	1	0	0	0	1	1	0	0	0	1	1
1	1	0	0	0	1	1	1	0	0	1	1	1	0
0	0	1	1	1	1	0	0	1	1	0	0	0	1
1	0	0	0	0	1	1	0	1	1	0	0	1	1

F_5

1	1	1	0	0	0	1	0	0	0	0	1	1	1
1	1	1	1	0	0	0	0	0	0	1	1	1	0
1	1	0	0	0	1	1	0	0	1	1	1	0	0
1	0	0	0	1	1	1	0	1	1	1	0	0	0
0	0	0	1	1	1	1	1	1	1	0	0	0	0
0	0	1	1	1	1	0	1	1	0	0	0	0	1
0	1	1	1	1	0	0	1	0	0	0	0	1	1
0	0	0	0	1	1	1	1	0	1	1	1	0	0
0	0	1	1	1	0	0	0	1	1	0	1	1	0
0	0	0	1	1	1	0	0	1	1	1	0	0	1
0	0	1	1	1	0	0	1	0	0	0	1	1	1
0	1	1	1	0	0	0	1	1	1	0	0	0	1
1	1	1	0	0	0	0	0	1	1	1	0	0	1
1	1	0	0	0	0	1	0	0	0	1	1	1	1

F_6

Table 6.7: A set of 6 binary MOFS of order 14.

6.7 Appendix B: Eigenvalues

The eigenvalues of the matrix M^TM in the proof of Theorem 6.1 can be obtained from Lemma 6.44 by substituting $c = n\lambda$ and $d = \lambda\lambda'$, where $\lambda = m/q$ and $\lambda' = n/q$.

Lemma 6.43. *Let $H = aI_q + bJ_q$ be a $q \times q$ matrix, where I_q is an identity matrix of order q and J_q is a matrix of ones of order q. Then $a+bq$ and a are eigenvalues of H with multiplicities 1 and $q-1$ respectively.*

Proof. Observe that the matrix,

$$H = \begin{pmatrix} a+b & b & \dots & b \\ b & a+b & \dots & b \\ \vdots & \vdots & \ddots & \vdots \\ b & b & \dots & a+b \end{pmatrix}$$

can be reduced to the following lower triangular matrix:

$$\begin{pmatrix} a+qb & 0 & 0 & \dots & 0 \\ b & a & 0 & \dots & 0 \\ b & 0 & a & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b & 0 & 0 & \dots & a \end{pmatrix}$$

Thus the eigenvalues $a+qb$ and a have multiplicities 1 and $q-1$, respectively.

□

Lemma 6.44. *Let N be a $(kq) \times (kq)$ matrix of the following form:*

$$N = \begin{pmatrix} cI_q & dJ_q & \dots & dJ_q \\ dJ_q & cI_q & \dots & dJ_q \\ \vdots & \vdots & \ddots & \vdots \\ dJ_q & dJ_q & \dots & cI_q \end{pmatrix},$$

where I_q and J_q are defined in Lemma 6.43. Then N has eigenvalues $c+q(k-1)d$, $c-qd$, and c with multiplicities 1, $k-1$, and $k(q-1)$ respectively.

Proof. By row operations we can row-reduce N to the following matrices (where $\mathbf{0}$ is a $q \times q$ matrix of zeroes):

$$\begin{pmatrix} cI_q & dJ_q - cI_q & dJ_q - cI_q & \dots & dJ_q - cI_q \\ dJ_q & cI_q - dJ_q & \mathbf{0} & \dots & \mathbf{0} \\ dJ_q & \mathbf{0} & cI_q - dJ_q & \dots & \mathbf{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ dJ_q & \mathbf{0} & \mathbf{0} & \dots & cI_q - dJ_q \end{pmatrix},$$

$$\begin{pmatrix} cI_q + (k-1)dJ_q & \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} \\ dJ_q & cI_q - dJ_q & \mathbf{0} & \dots & \mathbf{0} \\ dJ_q & \mathbf{0} & cI_q - dJ_q & \dots & \mathbf{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ dJ_q & \mathbf{0} & \mathbf{0} & \dots & cI_q - dJ_q \end{pmatrix}.$$

Now by using Lemma 6.43 the matrix $cI_q + (k-1)dJ_q$ has eigenvalues $c + q(k-1)d$ and c with multiplicities 1 and $q-1$, respectively. And the matrix $cI_q - dJ_q$ has eigenvalues $c-qd$ and c with multiplicities 1 and $q-1$, respectively. Consequently the matrix N has eigenvalues $c + q(k-1)d$, $c - qd$, and c with multiplicities 1, $k-1$, and $k(q-1)$ respectively. □

References

[1] S. Ball. On sets of vectors of a finite vector space in which every subset of basis size is a basis. *Journal of the European Mathematical Society*, 14:733–748, 2012.

[2] S. Ball and J. De Beule. On sets of vectors of a finite vector space in which every subset of basis size is a basis ii. *Designs, Codes and Cryptography*, 65:5–14, 2012.

[3] T. Britz, N. J. Cavenagh, A. Mammoliti, and I. M. Wanless. Mutually orthogonal binary frequency squares. *The electronic journal of combinatorics*, 27(3), 2020.

[4] C.-S. Cheng. Orthogonal arrays with variable numbers of symbols. *The Annals of Statistics*, 8:447–453, 1980.

[5] C. J. Colbourn and J. H. Dinitz. *Handbook of Combinatorial Designs, Second Edition (Discrete Mathematics and Its Applications)*. Chapman & Hall/CRC, 2006.

[6] S. Damelin, G. Michalski, G. Mullen, and D. Stone. The number of linearly independent binary vectors with applications to the construction of hypercubes and orthogonal arrays, pseudo (t, m, s)-nets and linear codes. *Monatshefte für Mathematik*, 141(4):277–288, 2004.

[7] S. Damelin, G. Michalski, and G. L. Mullen. The cardinality of sets of k-independent vectors over finite fields. *Monatshefte für Mathematik*, 150(4):289–295, 2007.

[8] D. Z. Djokovic. Hadamard matrices of order 764 exist. *Combinatorica*, 28:487–489, 2008.

[9] W. Federer, A. Hedayat, and J. Mandeli. Pairwise orthogonal f-rectangle designs. *Journal of statistical planning and inference*, 10(3):365–374, 1984.

[10] W. T. Federer. On the existence and construction of a complete set of orthogonal $f(4t; 2t, 2t)$-squares design. *The Annals of Statistics*, 5(3):561–564, 1977.

[11] M. Grassl. Code tables: Bounds on the parameters of various types of codes. Accessed Nov 2022. http://codetables.markus-grassl.de/.

[12] A. Hedayat, D. Raghavarao, and E. Seiden. Further contributions to the theory of f-squares design. *The Annals of Statistics*, 3:712–716, 1975.

[13] S. Hedayat, Sloane. *Orthogonal Arrays*. Springer, New York, NY, 1999.

[14] K. J. Horadam. *Hadamard matrices and their applications*. Princeton university press, 2012.

[15] C. F. Laywine and G. L. Mullen. A table of lower bounds for the number of mutually orthogonal frequency squares. *Ars Combinatoria*, 59:85–96, 2001.

[16] M. Li, Y. Zhang, and B. Du. Some new results on mutually orthogonal frequency squares. *Discrete Mathematics*, 331:175–187, 2014.

[17] J. Mandeli. Complete-sets of mutually orthogonal frequency rectangle designs having twice a prime power number of columns. *Utilitas Mathematica*, 41:151–160, 1992.

[18] J. Mandeli and W. Federer. On the construction of mutually orthogonal f-hyperrectangles. *Utilitas Math.*, 25:315—324, 1984.

[19] V. C. Mavron. Frequency squares and affine designs. *The Electronic Journal of Combinatorics*, 7(1):56, 2000.

[20] F. Rahim and N. J. Cavenagh. Row-column factorial designs with multiple levels. *Journal of Combinatorial Designs*, 29:750–764, 2021.

[21] F. Rahim and N. J. Cavenagh. Row-column factorial designs with strength at least 2. *arXiv preprint arXiv:2207.02397*, 2022.

[22] D. Street. Generalized hadamard matrices, orthogonal arrays and f-squares. *Ars Combinatoria*, 8:131–141, 1979.

[23] T. Tassa and J. L. Villar. On proper secrets,(t, k)-bases and linear codes. *Designs, Codes and Cryptography*, 52(2):129–154, 2009.

Chapter 7

Conclusion

In this conclusion, we explore some open problems and ideas for future work. We also identify key challenges and potential methods or approaches that could be used to address these open problems and further our understanding.

In Chapter 4, necessary and sufficient conditions for the existence of row-column factorial designs of strength 1 have been established. Further work in this direction could be to explore designs of strength 1 containing the maximum possible number of rows and columns with strength 2 property, that is, a design in which all main effects are estimable and contains the maximum number of two-factor estimable interactions. Similarly, we could investigate designs of strength 2 with the maximum number of estimable three-factor interactions. In [2] binary designs of strength 1 with the maximum number of estimable two-factor interactions are discussed where the dimension of design is a power of 2. Theorem 5.18 could be helpful in the above, however, it would not prove the maximality of the number of interactions.

In Theorem 5.38 we assumed that the Conjecture 5.27 is true. That is, we assumed the existence of a Hadamard matrix of order $4m$, containing two non-trivial sets of columns, such that their sums are orthogonal. By inspection, we notice this conjecture is true for $m = 3$ and $m = 5$. This conjecture could be explored computationally and/or theoretically for larger values of m.

While constructing binary strength 2 row-column factorial designs we clas-

sified these designs into two categories: abelian and non-abelian on the basis of construction. In Lemma 5.37, we have given the following non-abelian row-column designs: $I_5(12, 8, 2, 2)$, $I_6(12, 16, 2, 2)$ and $I_4(12, 12, 2, 2)$. By inspection, we determined that an abelian $I_5(12, 8, 2, 2)$ does not exist. However, we do not know whether there are infinitely many parameters for which there exists only a non-abelian binary strength 2 row-column factorial design.

In Chapter 5 we utilized Hadamard matrices in order to construct binary row-column factorial designs of strength 2. In future work, these constructions might be generalizable to non-binary designs by using results on generalised Hadamard matrices.

In Section 6.4, we established a relationship between sets of t-independent vectors and sets of t–orthogonal frequency rectangles. We also formulated a table of known values for $\mathrm{Ind}(N, t)$ which provides lower bounds for a set of t-orthogonal frequency rectangles. However, stronger lower bounds might be obtainable by investigating Problem 6.24.

In Chapter 6, we gave various constructions for a set of MOFR. A further step in this direction could be to computationally classify all binary MOFR of small orders; this has already been done in the case of MOFS [1]. We also showed that a set of $p-1$ binary MOFS of order $2p$ exists whenever p is an odd prime. Additionally, we could look into generalising this construction when p is odd and composite.

Finally, in this thesis, we only considered designs with symmetrical factorials, that is, factorials in which each factor has the same number of levels. Future work could include extending this work to designs with asymmetrical factorials.

References

[1] T. Britz, N. J. Cavenagh, A. Mammoliti, and I. M. Wanless. Mutually orthogonal binary frequency squares. *The electronic journal of combinatorics*, 27(3), 2020.

[2] J. Godolphin. Construction of row–column factorial designs. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 81(2):335–360, 2019.

Appendix

Co-Authorship Forms

The co-authorship forms related to the three articles included in this thesis are provided on the following pages.

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

Co-Authorship Form

School of Graduate Research
The University of Waikato
Private Bag 3105
Hamilton 3240, New Zealand
Phone +64 7 838 5096
Email: SGR@waikato.ac.nz
Website: http://www.waikato.ac.nz/students/research-degree

This form is to accompany the submission of any PhD that contains research reported in published or unpublished co-authored work. **Please include one copy of this form for each co-authored work.** Completed forms should be included in your appendices for all the copies of your thesis submitted for examination and library deposit (including digital deposit).

Please indicate the chapter/section/pages of this thesis that are extracted from a co-authored work and give the title and publication details or details of submission of the co-authored work.

Chapter 4: Row-column factorial designs with multiple levels

Published in Journal of Combinatorial Desisgns, doi: https://doi.org/10.1002/jcd.21799

Nature of contribution by PhD candidate	Innovation, Key ideas, Writing and Reviewing
Extent of contribution by PhD candidate (%)	75

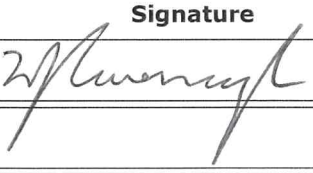
CO-AUTHORS

Name	Nature of Contribution
Nicholas Cavenagh	Conceptualization, Reviewing and some proofs were collaborative

Certification by Co-Authors

The undersigned hereby certify that:

- the above statement correctly reflects the nature and extent of the PhD candidate's contribution to this work, and the nature of the contribution of each of the co-authors; and
- that the candidate wrote all or the majority of the text.

Name	Signature	Date
Nicholas Cavenagh		February 01, 2023

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

Co-Authorship Form

School of Graduate Research
The University of Waikato
Private Bag 3105
Hamilton 3240, New Zealand
Phone +64 7 838 5096
Email: SGR@waikato.ac.nz
Website: http://www.waikato.ac.nz/students/research-degree

This form is to accompany the submission of any PhD that contains research reported in published or unpublished co-authored work. **Please include one copy of this form for each co-authored work.** Completed forms should be included in your appendices for all the copies of your thesis submitted for examination and library deposit (including digital deposit).

Please indicate the chapter/section/pages of this thesis that are extracted from a co-authored work and give the title and publication details or details of submission of the co-authored work.

Chapter 5: Row-column factorial designs with strength at least 2
Submitted for publication in Linear Algebra and Its Applications

Nature of contribution by PhD candidate	Writing, Reviewing and collaboration in research
Extent of contribution by PhD candidate (%)	65

CO-AUTHORS

Name	Nature of Contribution
Nicholas Cavenagh	Conceptualization, Reviewing and many proofs were collaborative

Certification by Co-Authors

The undersigned hereby certify that:

- the above statement correctly reflects the nature and extent of the PhD candidate's contribution to this work, and the nature of the contribution of each of the co-authors; and
- that the candidate wrote all or the majority of the text.

Name	Signature	Date
Nicholas Cavenagh		February 01, 2023

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

Co-Authorship Form

School of Graduate Research
The University of Waikato
Private Bag 3105
Hamilton 3240, New Zealand
Phone +64 7 838 5096
Email: SGR@waikato.ac.nz
Website: http://www.waikato.ac.nz/students/research-degree

This form is to accompany the submission of any PhD that contains research reported in published or unpublished co-authored work. **Please include one copy of this form for each co-authored work.** Completed forms should be included in your appendices for all the copies of your thesis submitted for examination and library deposit (including digital deposit).

Please indicate the chapter/section/pages of this thesis that are extracted from a co-authored work and give the title and publication details or details of submission of the co-authored work.

Chapter 6: Mutually Orthogonal Frequency Rectangles

Submitted for publication in Discrete Mathematics

Nature of contribution by PhD candidate	Most of the writing, reviewing and ideas
Extent of contribution by PhD candidate (%)	75

CO-AUTHORS

Name	Nature of Contribution
Nicholas Cavenagh	Conceptualization, Reviewing and some proofs were collaborative

Certification by Co-Authors

The undersigned hereby certify that:

- the above statement correctly reflects the nature and extent of the PhD candidate's contribution to this work, and the nature of the contribution of each of the co-authors; and
- that the candidate wrote all or the majority of the text.

Name	Signature	Date
Nicholas Cavenagh		February 01, 2023