

Mutually orthogonal binary frequency squares

Thomas Britz

School of Mathematics and Statistics
UNSW Sydney
NSW 2052, Australia
britz@unsw.edu.au

Nicholas J. Cavenagh

Department of Mathematics
The University of Waikato
Private Bag 3105, Hamilton 3240, New Zealand
nickc@waikato.ac.nz

Adam Mammoliti

Ian M. Wanless

School of Mathematics
Monash University
VIC 3800, Australia

{adam.mammoliti,ian.wanless}@monash.edu

Submitted: Feb 17, 2020; Accepted: Jun 27, 2020; Published: Jul 10, 2020

© The authors. Released under the CC BY-ND license (International 4.0).

Abstract

A *frequency square* is a matrix in which each row and column is a permutation of the same multiset of symbols. We consider only *binary* frequency squares of order n with $n/2$ zeros and $n/2$ ones in each row and column. Two such frequency squares are *orthogonal* if, when superimposed, each of the 4 possible ordered pairs of entries occurs equally often. In this context we say that a set of k -MOFS(n) is a set of k binary frequency squares of order n in which each pair of squares is orthogonal.

A set of k -MOFS(n) must satisfy $k \leq (n-1)^2$, and any set of MOFS achieving this bound is said to be *complete*. For any n for which there exists a Hadamard matrix of order n we show that there exists at least $2^{n^2/4 - O(n \log n)}$ isomorphism classes of complete sets of MOFS(n). For $2 < n \equiv 2 \pmod{4}$ we show that there exists a set of 17-MOFS(n) but no complete set of MOFS(n).

A set of k -maxMOFS(n) is a set of k -MOFS(n) that is not contained in any set of $(k+1)$ -MOFS(n). By computer enumeration, we establish that there exists a set of k -maxMOFS(6) if and only if $k \in \{1, 17\}$ or $5 \leq k \leq 15$. We show that up to isomorphism there is a unique 1-maxMOFS(n) if $n \equiv 2 \pmod{4}$, whereas no 1-maxMOFS(n) exists for $n \equiv 0 \pmod{4}$. We also prove that there exists a set of 5-maxMOFS(n) for each order $n \equiv 2 \pmod{4}$ where $n \geq 6$.

Mathematics Subject Classifications: 05B15

1 Introduction

Rows and columns of an $n \times n$ array will be indexed by $N(n) = \{1, 2, \dots, n\}$. A *frequency square* L of *type* $(n; \lambda_0, \lambda_1, \dots, \lambda_{m-1})$ is an $n \times n$ array such that symbol i occurs λ_i times in each row and λ_i times in each column for each $i \in \{0, \dots, m-1\}$; necessarily $\sum_{i=0}^{m-1} \lambda_i = n$. In the case where $\lambda_0 = \lambda_1 = \dots = \lambda_{m-1} = \lambda$ we say that L is of type $(n; \lambda)$. A frequency square of type $(n; 1)$ is a *Latin square* of order n . Two frequency squares of type $(n; \lambda_0, \lambda_1, \dots, \lambda_{m-1})$ are *orthogonal* if each ordered pair (i, j) occurs $\lambda_i \lambda_j$ times when the squares are superimposed. A set of *mutually orthogonal frequency squares* (MOFS) is a set of frequency squares in which each pair of squares is orthogonal.

Research into frequency squares has focused mainly on constructing sets of MOFS, motivated originally by problems in statistical experiment design. Hedayat, Raghavarao and Seiden [13] showed that the maximum possible size of a set of MOFS of type $(n; \lambda)$ is $(n-1)^2/(m-1)$; such a set is called *complete*. A complete set of MOFS of type $(n; \lambda)$ for $n/\lambda > 2$ is only known to exist when n is a prime power [16, 17, 18, 20]; a unified theory for all known constructions is given in [15].

Starting with a set of mutually orthogonal Latin squares and replacing some subset of the symbols by zeros, and replacing all other symbols by ones, we can obtain a set of binary MOFS. A slightly less obvious connection between binary MOFS and other designs is the following. An *equidistant permutation array* $A(n, d; k)$ is a $k \times n$ array in which each row contains each integer from 1 to n exactly once and any two distinct rows differ in exactly d positions. One can construct k MOFS of type $(n; n-1, 1)$ by writing down the permutation matrices that correspond to the rows of an $A(n, n-1; k)$. It is known from [8] that there exists an $A(n, n-1; 2n-4)$ for any $n \geq 6$ and from [5] that there exists an $A(q^2 + q + 1, q^2 + q; q^3 + q^2)$ for any prime power q .

Two sets of MOFS are *isomorphic* if one can be obtained from the other by some sequence of the following operations:

- Applying the same permutation to the rows of all squares in the set.
- Applying the same permutation to the columns of all squares in the set.
- Transposing all squares in the set.
- Permuting the symbols in one of the squares.
- Permuting the squares within the set (in cases where we have imposed an order on the set).

Isomorphism is an equivalence relation and the equivalence classes that it induces are *isomorphism classes*.

For the remainder of this paper we restrict ourselves to frequency squares of type $(n; \lambda)$ where $n/\lambda = 2$. In other words, our squares have just two symbols, which we will take to be 0 and 1. We will not say it each time, but all subsequent mention of MOFS will refer to these binary MOFS. As we are assuming that both symbols must occur equally often within each row, the order of our MOFS must be even. We use $\text{MOFS}(n)$ to denote MOFS of order n . If there are k MOFS in the set then we write $k\text{-MOFS}(n)$.

The following result was proved by Federer [12]; see also [20].

Theorem 1. *If there exists a Hadamard matrix of order n , then there exists a complete set of MOFS(n).*

The Hadamard conjecture famously asserts the existence of Hadamard matrices for all orders that are divisible by 4. If true, this would imply the existence of a complete set of MOFS(n) for every n divisible by 4. Conversely, Theorem 4.6 in [7] gives the asymptotic result that if n is divisible by 4, then there exists a set of k -MOFS(n) where $k = n^2(1 - o(1))/9$, providing a quadratic lower bound on the size of the largest set of MOFS(n). No corresponding bound is known when $n/2$ is odd. Indeed, very little seems to be known about sets of MOFS(n) when $n \equiv 2 \pmod{4}$. Our primary aim in this paper is to shed some light on this case. For example, we will show in §2 that there are no complete sets of MOFS of this type, for $n > 2$. The corresponding problem for Latin squares is a famous problem that remains open; it would imply the non-existence of a finite projective plane of order $n \equiv 2 \pmod{4}$ with $n > 2$.

Maintaining consistency with Latin square terminology, a *bachelor* frequency square F is one such that there exists no frequency square F' orthogonal to F . In general, a set $\{F_1, F_2, \dots, F_k\}$ of k -MOFS(n) is said to be *maximal* if there does not exist a frequency square F that is orthogonal to F_i for each $1 \leq i \leq k$. If we wish to specify that a set of k -MOFS(n) is maximal we may write k -maxMOFS(n).

The structure of the paper is as follows. In §2 we demonstrate a condition that is sufficient to show that a set of MOFS is maximal. The condition is called a *relation* and is modelled on similar work that has been done for Latin squares. In §3 we show that bachelor frequency squares are unique up to isomorphism for orders that are $2 \pmod{4}$ and do not exist for orders that are $0 \pmod{4}$. The bachelor frequency squares are maximal because they satisfy a relation. The contrast with Latin squares is worth noting. It is known from [11, 21] that bachelor Latin squares exist for all orders $n > 3$. Moreover, there are vast numbers of bachelor Latin squares up to isomorphism [4]. In §4 we study small local changes that can convert a set of MOFS into a non-isomorphic set of MOFS. Using these “trades” we show that for any n for which there exists a Hadamard matrix of order n there are at least $2^{n^2/4 - O(n \log n)}$ isomorphism classes of complete sets of MOFS(n). This contrasts nicely with the result in §2 that there is no complete set of MOFS(n) when $n \equiv 2 \pmod{4}$ and $n > 2$. In §5 we report on computer enumerations for MOFS of small order. We find that aside from the unique bachelor there is no set of k -maxMOFS(6) with $k < 5$. Also, most but not all of the sets of 5-maxMOFS(6) satisfy a relation. The largest sets of k -MOFS(6) have size $k = 17$, and they also satisfy relations. In §6 we show how sets of k -MOFS(n) can sometimes be embedded in sets of k -MOFS(n') for some $n' > n$. Using this technique we show that there exists a set of 17-MOFS(n) for all $n \equiv 2 \pmod{4}$ such that $n > 2$. Then in §7 we use similar ideas to show that there exists a set of 5-maxMOFS(n) for all $n \equiv 2 \pmod{4}$ such that $n > 2$. Finally, in §8 we discuss some interesting questions that have been prompted by our work.

2 Relations

The technique of relations developed in this section is based on the techniques used in [9] and [10] (with origins in [19]) to analyse maximal sets of mutually orthogonal Latin squares.

A set $\{F_1, \dots, F_k\}$ of k -MOFS of order n can be written as an $n^2 \times (k+2)$ orthogonal array \mathcal{O} in which there is a row

$$[i, j, F_1[i, j], F_2[i, j], \dots, F_k[i, j]], \quad (1)$$

for each $i \in N(n)$ and $j \in N(n)$. In this context it is safest to consider MOFS to have an indexing that implies an ordering on the squares (and hence the order of the columns in \mathcal{O} is well-defined. Let Y_c be the set of symbols that occur in column c of \mathcal{O} . Then a *relation* is a $(k+2)$ -tuple (X_1, \dots, X_{k+2}) of sets such that $X_i \subseteq Y_i$ for $1 \leq i \leq k+2$, with the property that every row (1) of \mathcal{O} has an even number of columns c for which the symbol in column c is an element of X_c . A relation is *trivial on column c* if $X_c = \emptyset$ or $X_c = Y_c$. We will say that a relation is *non-trivial* if there is some column on which it is not trivial, and *full* if it is non-trivial on every column except possibly one of the first two. We say that a relation is an (a, b) -relation if $|X_1| = a$ and $|X_2| = b$. In the results below we will show certain restrictions on the kinds of relations that can be achieved.

If we start with a relation and two of the X_c 's are replaced by their complements, then we obtain another relation. In our context, $X_c \subseteq \{0, 1\}$ for $c \geq 3$. By complementing X_c and X_1 if necessary, we may assume that $X_c = \{1\}$ or $X_c = \emptyset$ for all $c \geq 3$. In the latter case, we have a relation on a proper subset of the MOFS. The choices of X_1 and X_2 govern which rows and columns of the MOFS are involved in the relation. However, we are only interested in properties of MOFS up to isomorphism. That means that only 3 quantities really matter to us for a relation: How many MOFS are involved, how many rows are involved and how many columns are involved. These observations will allow us to rule out existence of relations in a number of cases below. They also allow us to provide an easy characterisation of MOFS that satisfy a relation.

Lemma 2. *A set of MOFS satisfies a non-trivial relation if and only if some non-empty subset of the MOFS have a \mathbb{Z}_2 -sum that, up to permutation of the rows and columns, has the following structure of constant blocks:*

$$\begin{bmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{bmatrix}. \quad (2)$$

Proof. Suppose that the set of MOFS $\{F_1, \dots, F_k\}$ satisfies a full relation (X_1, \dots, X_{k+2}) . For $r, c \in N(n)$, let x_{rc} be the sum over the entries in the cell (r, c) of each of the squares. Then, by the definition of a relation, $x_{rc} \equiv 0 \pmod{2}$ if $r \in X_1$ and $c \in X_2$, or if $r \notin X_1$ and $c \notin X_2$, and $x_{rc} \equiv 1 \pmod{2}$ if exactly one of $r \in X_1$ and $c \in X_2$ holds. By permuting the rows and columns appropriately, the \mathbb{Z}_2 -sum of F_1, \dots, F_k has a structure of the form in (2).

If the set of MOFS $\{F_1, \dots, F_k\}$ has a \mathbb{Z}_2 -sum that is, up to permutation of the rows and columns, of the form (2), then let X_1 be the set of rows and X_2 be the set of

columns corresponding to the upper left $\mathbf{0}$ block in (2). Then it is easy to check that $(X_1, X_2, \dots, X_{k+2})$ with $X_c = \{1\}$ for $c \geq 3$ is a full relation on $\{F_1, \dots, F_k\}$.

Thus, we have shown that a set of MOFS $\{F_1, \dots, F_k\}$ satisfy a full relation if and only if the \mathbb{Z}_2 -sum of F_1, \dots, F_k is of the form (2) up to permutation of the rows and columns. As a set of MOFS satisfies a non-trivial relation if and only if a non-empty subset satisfies a full relation, the lemma follows. \square

We stress that the blocks in (2) are allowed to be degenerate. For example, here is a set of 2-MOFS(4) that satisfies a relation with $X_1 = \{1, 2\}$ and $X_2 = \emptyset$. Their \mathbb{Z}_2 -sum is also given.

$$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Lemma 3. *Let \mathcal{F} be a set of k -MOFS(2λ) and let $R = (X_1, \dots, X_{k+2})$ be a full relation on \mathcal{F} . Then $|X_1| \equiv |X_2| \equiv \lambda k \pmod{2}$.*

Proof. Let \mathcal{O} be the orthogonal array corresponding to \mathcal{F} . Let

$$s = |\{(r, c) \in N(4\lambda^2) \times N(k+2) : \mathcal{O}[r, 1] = 1, \mathcal{O}[r, c] \in X_c\}|$$

be the number of cells containing symbols in the relation among the rows of \mathcal{O} for which $i = 1$ in (1). By noting that $X_c = \{1\}$ for $c \geq 3$, one finds that $s = |X_2| + \lambda k + 2\lambda\delta$ where $\delta = 1$ if $1 \in X_1$ and $\delta = 0$ otherwise. By the definition of relations, it follows that $|X_2| + \lambda k$ is even. A similar argument on the first column of the MOFS shows that $|X_1| + \lambda k$ is even. \square

One reason to be interested in relations is that they can be used to diagnose maximality of a set of MOFS.

Theorem 4. *Suppose k and λ are both odd. Let \mathcal{F} be a set of k -MOFS(2λ) that satisfies a full relation. Then \mathcal{F} is maximal.*

Proof. Let $R = (X_1, \dots, X_{k+2})$ be a full relation of \mathcal{F} . By Lemma 3, we know that $|X_1|$ and $|X_2|$ are both odd. Suppose that \mathcal{F} can be extended by appending a square F . Let F have x ones in cells (r, c) where $r \in X_1$ and $c \in X_2$. Then F has $\lambda|X_1| - x$ ones in cells (r, c) where $r \in X_1$ and $c \notin X_2$ and $\lambda|X_2| - x$ ones in cells (r, c) where $r \notin X_1$ and $c \in X_2$. By orthogonality, the number of pairs $(F[r, c], F_i[r, c])$ such that $(F[r, c], F_i[r, c]) = (1, 1)$ is $k\lambda^2$. On the other hand, for a fixed pair (r, c) with $F[r, c] = 1$ the number of i 's such that $(F[r, c], F_i[r, c]) = 1$ is even if either $r \in X_1$ and $c \in X_2$ or $r \notin X_1$ and $c \notin X_2$, and is odd if exactly one of $r \in X_1$ and $c \in X_2$ holds. Therefore, we must have that

$$1 \equiv k\lambda^2 \equiv \lambda|X_1| - x + \lambda|X_2| - x \equiv 0 \pmod{2}.$$

This contradiction proves the theorem. \square

With Theorem 4 as motivation, we now consider what relations are possible. Our first result is a non-existence result.

Theorem 5. *Suppose that λ is odd and $k \not\equiv 1 \pmod{4}$. Then no set of k -MOFS(2λ) satisfies a full relation.*

Proof. Suppose that $\{F_1, \dots, F_k\}$ is a set of k -MOFS(2λ) that satisfies a full relation (X_1, \dots, X_{k+2}) . Let x_i be the number of k -tuples in the superposition of the k -MOFS(2λ) that contain exactly i ones. Since each square contains $2\lambda^2$ ones, we know that

$$2k\lambda^2 = \sum_{i=0}^k ix_i. \quad (3)$$

Also each pair of squares has λ^2 cells where both contain a one, so

$$\binom{k}{2}\lambda^2 = \sum_{i=0}^k \binom{i}{2}x_i. \quad (4)$$

Adding twice (4) to (3) we find that

$$k(k+1) \equiv k(k+1)\lambda^2 = \sum_{i=0}^k i^2x_i \equiv \sum_{\text{odd } i} x_i \pmod{4}. \quad (5)$$

However, by Lemma 3, the existence of the relation enforces the condition

$$\begin{aligned} \sum_{\text{odd } i} x_i &= |X_1|(2\lambda - |X_2|) + |X_2|(2\lambda - |X_1|) \\ &= 2\lambda(|X_1| + |X_2|) - 2|X_1||X_2| \\ &\equiv 2k^2 \pmod{4}. \end{aligned} \quad (6)$$

Equations (5) and (6) contradict each other when $k \equiv 2$ or $3 \pmod{4}$.

Next we rule out the case when k is even (thereby finding a second proof for the case $k \equiv 2 \pmod{4}$). So assume that k is even, and, hence, $|X_1|$ and $|X_2|$ are both even, by Lemma 3.

Let Ω_0 (respectively Ω_1) be the set of cells (r, c) for which $F_1[r, c] = 1$ and in which the superposition of F_1, \dots, F_k has an even (respectively, odd) number of ones. We claim that $|\Omega_1|$ is even, since it can be obtained by counting the (even) number of ones in the rows of F_1 with indices in X_1 , adding the (even) number of ones in the columns of F_1 with indices in X_2 , and subtracting twice the number of ones in the intersection. As $|\Omega_0| + |\Omega_1| = 2\lambda^2$, it follows that $|\Omega_0|$ is also even.

Now let p be the total number of pairs of ones in the superposition of F_1 with the other $(k-1)$ squares. Each square contributes λ^2 to p , so $p = (k-1)\lambda^2 \equiv 1 \pmod{2}$. However, each cell in Ω_0 contributes an odd number of times to p and each cell in Ω_1 contributes an even number, showing that $p \equiv |\Omega_0| \equiv 0 \pmod{2}$. This contradiction completes the proof. \square

In particular, Theorem 5 shows that $k = 5$ is the smallest k for which Theorem 4 says anything, aside from the fairly trivial case of $k = 1$. This will be significant later, but for the moment we just give an example to show that a relation can be achieved when $k = 5$. Consider the following set of 5-MOFS(6), shown superimposed on the left. Their \mathbb{Z}_2 -sum is shown on the right, demonstrating that they satisfy a $(5, 3)$ -relation and hence are maximal.

$$\begin{bmatrix} 11011 & 10111 & 01100 & 00001 & 00010 & 11100 \\ 10100 & 01111 & 11011 & 00010 & 11100 & 00001 \\ 01111 & 11000 & 10111 & 11100 & 00001 & 00010 \\ 01001 & 10001 & 00101 & 10110 & 01110 & 11010 \\ 10010 & 00110 & 01010 & 01101 & 11001 & 10101 \\ 00100 & 01000 & 10000 & 11011 & 10111 & 01111 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} \quad (7)$$

We next show that even in the case when $k \equiv 1 \pmod{4}$ there is another restriction on what relations are possible.

Theorem 6. *Let λ be odd. Suppose that there exists a set of k -MOFS(2λ) with a full relation $R = (X_1, \dots, X_{k+2})$. If $k \equiv 1 \pmod{8}$, then $|X_1||X_2| \equiv 1 \pmod{4}$ and if $k \equiv 5 \pmod{8}$, then $|X_1||X_2| \equiv 3 \pmod{4}$.*

Proof. Let $R = (X_1, \dots, X_{k+2})$ be a full relation on some set of k -MOFS(2λ). By Lemma 3, $|X_1|$ and $|X_2|$ are both odd. Let x_i be the number of k -tuples in the superposition of the k -MOFS(2λ) that contain exactly i ones. Let α be the number of ones in the superposition of the k -MOFS(2λ) that lie in some position (r, c) where $r \in X_1$ and $c \in X_2$. As R is a relation, α must be even. Then the total number of ones in the superposition of the k -MOFS(2λ) that lie in a position (r, c) such that exactly one of $r \in X_1$ and $c \in X_2$ is true is

$$\sum_{\text{odd } i} ix_i = \lambda k |X_1| - \alpha + \lambda k |X_2| - \alpha \equiv \lambda k (|X_1| + |X_2|) \pmod{4}. \quad (8)$$

Note that equations (3), (4) and (6) from the proof of Theorem 5 only depend on λ being odd and so each of them are still valid in the current setting. From (8) and (6) we have

$$\sum_{i \equiv 3 \pmod{4}} 2x_i \equiv \sum_{\text{odd } i} (i-1)x_i \equiv \lambda(k-2)(|X_1| + |X_2|) + 2|X_1||X_2| \pmod{4}. \quad (9)$$

By simplifying $2 \times (4) + (6) - (3)$, one finds that

$$\begin{aligned} k(k-3)\lambda^2 + 2\lambda(|X_1| + |X_2|) - 2|X_1||X_2| &= \sum_{i=0}^k i(i-2)x_i + \sum_{\text{odd } i} x_i \\ &\equiv \sum_{\text{odd } i} (i-1)^2 x_i \\ &\equiv \sum_{i \equiv 3 \pmod{4}} 4x_i \pmod{8}. \end{aligned} \quad (10)$$

By setting $2 \times (9) = (10)$ and noting that λ is odd, we see that

$$k(k-3) + 2\lambda(3-k)(|X_1| + |X_2|) - 6|X_1||X_2| \equiv 0 \pmod{8}. \quad (11)$$

Since k is odd, we see that $2\lambda(3-k)(|X_1| + |X_2|) \equiv 0 \pmod{8}$. Thus if $k \equiv 1 \pmod{8}$, then we must have $|X_1||X_2| \equiv 1 \pmod{4}$ and if $k \equiv 5 \pmod{8}$, then we must have $|X_1||X_2| \equiv 3 \pmod{4}$, by (11). \square

Having shown some restrictions on which relations are possible, our next goal is to show that certain relations are actually achievable. We first give a lemma characterising triples of MOFS.

Lemma 7. *For each triple t , let x_t count the number of cells where t occurs in the superimposition of three frequency squares F_1 , F_2 and F_3 of order 2λ . Then F_1 , F_2 and F_3 are orthogonal if and only if*

$$x_{000} = x_{011} = x_{101} = x_{110} \quad \text{and} \quad x_{001} = x_{010} = x_{100} = x_{111}. \quad (12)$$

Proof. Orthogonality requires that

$$\begin{aligned} \lambda^2 &= x_{000} + x_{001} = x_{010} + x_{011} = x_{100} + x_{101} = x_{110} + x_{111} \\ &= x_{000} + x_{010} = x_{001} + x_{011} = x_{100} + x_{110} = x_{101} + x_{111} \\ &= x_{000} + x_{100} = x_{001} + x_{101} = x_{010} + x_{110} = x_{011} + x_{111}, \end{aligned}$$

which is equivalent to (12). \square

We will say that two relations (X_1, \dots, X_{k+2}) and (X'_1, \dots, X'_{k+2}) are *equivalent* if $|X_i| = |X'_i|$ for $1 \leq i \leq k+2$.

Theorem 8. *Let $\Lambda = \{1, 2, \dots, \lambda\}$. For $k \leq 3$ the following relations are achieved, and every relation that is achieved is equivalent to one of these:*

- $k = 1$: $X_1 = X_2 = \Lambda$.
- $k = 2$: each of λ , $|X_1|$ and $|X_2|$ is even and either $X_1 = \Lambda$ or $X_2 = \Lambda$.
- $k = 3$: each of λ , $|X_1|$ and $|X_2|$ is even.

Proof. First suppose $k = 1$, so we are looking for a relation on a single frequency square F . Considering the fact that the first row of F contains λ zeros and λ ones we deduce that $|X_2| = \lambda$. Similar consideration of the first column of F shows that $|X_1| = \lambda$. So without loss of generality $X_1 = X_2 = \Lambda$. Moreover, this is achieved by a frequency square with four square blocks of order λ , in the pattern given in (2).

Next we consider the case when $k = 2$. Let $\{F_1, F_2\}$ be a set of 2-MOFS(2λ) and (X_1, X_2, X_3, X_4) be a relation on F_1 and F_2 . By orthogonality, the superposition of F_1 and F_2 must contain λ^2 occurrences of each of the pairs $(0, 1)$ and $(1, 0)$. It follows that $(2\lambda - |X_1|)|X_2| + (2\lambda - |X_2|)|X_1| = 2\lambda^2$, which implies that $|X_1| = \lambda$ or $|X_2| = \lambda$. Also,

$|X_1|$ and $|X_2|$ must be even, by Lemma 3. Therefore, the conditions in the theorem for $k = 2$ are necessary. To show sufficiency, we construct the superimposition of F_1 and F_2 :

$$\begin{bmatrix} \mathbf{00} & \mathbf{11} & \mathbf{01} & \mathbf{10} \\ \mathbf{11} & \mathbf{00} & \mathbf{10} & \mathbf{01} \\ \mathbf{01} & \mathbf{10} & \mathbf{00} & \mathbf{11} \\ \mathbf{10} & \mathbf{01} & \mathbf{11} & \mathbf{00} \end{bmatrix},$$

where the first two blocks on the diagonal have dimensions $|X_1|/2 \times |X_2|/2$, while the last two blocks on the diagonal have dimensions $(\lambda - |X_1|/2) \times (\lambda - |X_2|/2)$.

Lastly, consider the case $k = 3$. By Theorem 5 and Lemma 3, we see that λ , $|X_1|$ and $|X_2|$ must all be even. Thus, the conditions in the theorem for $k = 3$ are necessary.

Now we show sufficiency. For even integers y_1 and y_2 , let

$$\mathbf{B}_{y_1, y_2} = \begin{bmatrix} \mathbf{000} & \mathbf{011} & \mathbf{101} & \mathbf{110} \\ \mathbf{110} & \mathbf{101} & \mathbf{011} & \mathbf{000} \\ \mathbf{101} & \mathbf{110} & \mathbf{000} & \mathbf{011} \\ \mathbf{011} & \mathbf{000} & \mathbf{110} & \mathbf{101} \end{bmatrix},$$

where the first two blocks on the diagonal have dimensions $\lceil \frac{y_1}{4} \rceil \times \lceil \frac{y_2}{4} \rceil$ and the last two blocks on the diagonal have dimensions $\lfloor \frac{y_1}{4} \rfloor \times \lfloor \frac{y_2}{4} \rfloor$. Notice that every 3-tuple has an even number of ones and the pairs $(0, 0)$, $(0, 1)$, $(1, 0)$, $(1, 1)$ occur the same number of times when each tuple is restricted to 2 entries. The number of zeros and ones in each row is balanced on the 2nd and 3rd entries and number of zeros and ones in each column is balanced on the 1st and 2nd entries. For even integers y_1 and y_2 let \mathbf{B}_{y_1, y_2}^C be the complementary array to \mathbf{B}_{y_1, y_2} . That is,

$$\mathbf{B}_{y_1, y_2}^C = \begin{bmatrix} \mathbf{111} & \mathbf{100} & \mathbf{010} & \mathbf{001} \\ \mathbf{001} & \mathbf{010} & \mathbf{100} & \mathbf{111} \\ \mathbf{010} & \mathbf{001} & \mathbf{111} & \mathbf{100} \\ \mathbf{100} & \mathbf{111} & \mathbf{001} & \mathbf{010} \end{bmatrix},$$

where the dimensions of the diagonal blocks are the same as those in \mathbf{B}_{y_1, y_2} . For any even x_1 , x_2 and λ with $x_1, x_2 \leq 2\lambda$, we claim that the array

$$\begin{bmatrix} \mathbf{B}_{x_1, x_2} & \mathbf{B}_{x_1, 2\lambda - x_2}^C \\ \mathbf{B}_{2\lambda - x_1, x_2}^C & \mathbf{B}_{2\lambda - x_1, 2\lambda - x_2} \end{bmatrix}. \tag{13}$$

is the superposition of a set of 3-MOFS(2λ) that has a relation on $X_1 = \{1, \dots, x_1\}$ and $X_2 = \{1, \dots, x_2\}$. The fact that $x_2 \equiv 2\lambda - x_2 \pmod{4}$ ensures balance in the rows of the first square in (13). The fact that $x_1 \equiv 2\lambda - x_1 \pmod{4}$ ensures balance in the columns of the third square in (13). Other aspects of our claim are straightforward to check, using Lemma 7. \square

It is worth noting that Theorem 4 does not generalise to even λ . For example, if we take $x_1 = x_2 = \lambda \equiv 0 \pmod{4}$, then the MOFS in (13) satisfy a relation but are not

maximal, because they are orthogonal to the frequency square with the block structure given in (2).

To finish this section we consider the relations satisfied by complete sets of MOFS. A (v_*, k_*, λ_*) -design is a collection \mathcal{B} of k_* -subsets of a set V of size v_* such that each pair from V is contained in exactly λ_* blocks (we are using $*$ subscripts on variables here to distinguish them from similarly named variables used throughout the paper). Such a design is said to be *resolvable* if there is a partition of the blocks into *parallel classes* (i.e. partitions of V).

Our next result is implied by Theorem 3.5 from Jungnickel, et al [15], and the proof we give is basically the same as in that paper. We include a proof for completeness and because we want to squeeze a tiny bit more out of it.

Theorem 9. *Let $\mathcal{F} = \{F_1, F_2, \dots, F_k\}$ be a complete set of MOFS of order n where $k = (n - 1)^2$. Construct a multiset of blocks \mathcal{B} where for each $s \in \{0, 1\}$ and $1 \leq i \leq k$ there is a block $B_{s,i} \in \mathcal{B}$ that is the set of columns containing the entry s in the first row of F_i . Then \mathcal{B} is a resolvable $(n, n/2, (n - 1)(n - 2)/2)$ -design. Also, if $n \equiv 0 \pmod{4}$ then \mathcal{F} satisfies a $(0, n)$ -relation or an (n, n) -relation.*

Proof. Without loss of generality, consider a cell $(1, 1)$. For each cell $(r, c) \neq (1, 1)$, let $\theta_{r,c}$ be the number of frequency squares in \mathcal{F} such that cells $(1, 1)$ and (r, c) contain the same entry. Next, define

$$\alpha_1 = \sum_{c=2}^n \theta_{1,c} + \sum_{r=2}^n \theta_{r,1} \quad \text{and} \quad \alpha_2 = \sum_{r=2}^n \sum_{c=2}^n \theta_{r,c}.$$

In each frequency square, there are $n/2 - 1$ cells other than $(1, 1)$ in row (column) 1 containing the same entry as cell $(1, 1)$. Therefore, $\alpha_1 = 2k(n/2 - 1)$. By a similar argument, $\alpha_2 = k(n^2/2 - n + 1)$.

Let $F, F' \in \mathcal{F}$. Then since F and F' are orthogonal, the number of cells $(r, c) \neq (1, 1)$ such that (r, c) and $(1, 1)$ share the same entry in F and F' is equal to $n^2/4 - 1$. Thus,

$$\sum_{(r,c) \neq (1,1)} \binom{\theta_{r,c}}{2} = \binom{k}{2} (n^2/4 - 1).$$

It follows that:

$$\sum_{(r,c) \neq (1,1)} \theta_{r,c}^2 = k(k - 1)(n^2/4 - 1) + \sum_{(r,c) \neq (1,1)} \theta_{r,c} = k(k - 1)(n^2/4 - 1) + \alpha_1 + \alpha_2. \quad (14)$$

Next, define $\theta_1 = (n/2 - 1)(n - 1)$ and $\theta_2 = (n^2/2 - n + 1)$ and observe that

$$\begin{aligned} & \sum_{c=2}^n (\theta_1 - \theta_{1,c})^2 + \sum_{r=2}^n (\theta_1 - \theta_{r,1})^2 + \sum_{r=2}^n \sum_{c=2}^n (\theta_2 - \theta_{r,c})^2 \\ &= 2(n - 1)\theta_1^2 + (n - 1)^2\theta_2^2 - 2\alpha_1\theta_1 - 2\alpha_2\theta_2 + \sum_{(r,c) \neq (1,1)} \theta_{r,c}^2 = 0, \end{aligned}$$

given (14) and the fact that $k = (n - 1)^2$. Thus, we must have $\theta_{1,c} = \theta_1 = \theta_{r,1}$ for each $r \neq 1$ and $c \neq 1$, and $\theta_{r,c} = \theta_2$ for all $r \geq 2$ and $c \geq 2$. In particular, for each column $c \neq 1$, the number of frequency squares which contain the same entry in both cells $(1, 1)$ and $(1, c)$ is constant and equal to θ_1 . The same is true if we replace $(1, 1)$ by any other fixed cell in the first row. Thus in the set \mathcal{B} as defined above, each pair of columns occurs in precisely θ_1 blocks. Also the blocks $B_{0,i}$ and $B_{1,i}$ are complementary sets, for each i . It follows that \mathcal{B} is a resolvable $(n, n/2, (n - 1)(n - 2)/2)$ -design.

Finally, we justify the claim that \mathcal{F} satisfies either a $(0, n)$ or (n, n) relation. Note that if $n \equiv 0 \pmod{4}$ then $(n - 1)^2 \equiv \theta_1 \equiv \theta_2 \equiv 1 \pmod{2}$. Hence, if we standardise \mathcal{F} by complementing any square that has a zero in cell $(1, 1)$ then the \mathbb{Z}_2 -sum of \mathcal{F} will be a matrix in which every entry is 1. Complementing any square in \mathcal{F} also complements the \mathbb{Z}_2 -sum of \mathcal{F} . \square

The method used in Theorem 9 would also show that if $n \equiv 2 \pmod{4}$ then \mathcal{F} must satisfy a relation. However, this is a moot point, given Corollary 11 below. The following theorem is stated in [5, Thm II.7.31]; again we include a short proof for completeness.

Theorem 10. *For odd positive integers $t \geq 1$ and $k > 1$, there does not exist a resolvable $(2k, k, t(k - 1))$ -design.*

Proof. Suppose such a design \mathcal{B} exists and let $\lambda_* = t(k - 1)$. For any subset W of V , let r_W be the number of blocks containing W as a subset. Suppose that $r_{\{x,y,z\}} = s$ for some distinct x, y and z . Then the number of blocks containing x but neither y nor z is $r_{\{x\}} - 2\lambda_* + s = t + s$. But for each such block B , the pair $\{y, z\}$ must be in the other block of the parallel class containing B . Thus $\lambda_* = r_{\{y,z\}} = t + 2s$. But λ_* is even, a contradiction. \square

Corollary 11. *There does not exist a complete set of MOFS of order n whenever $n/2$ is odd and $n > 2$.*

Proof. Taking $k = n/2$ and $t = n - 1$ in Theorem 10, we find that the design required by Theorem 9 does not exist when $n/2$ is odd. \square

For generalisations of some of the ideas and results in this section, see [14].

3 The lonely bachelor

In this section we show that for order $n = 2\lambda$, there are no bachelor frequency squares if λ is even and only one bachelor square (up to isomorphism) if λ is odd.

Let $A_{2\lambda}$ be the unique frequency square satisfying a (non-trivial) relation, as shown in Theorem 8. We will make use of the following well known corollary of Dirac's Theorem:

Theorem 12. *Let G be a simple graph with 2λ vertices and minimum degree at least λ . Then G has a perfect matching.*

Theorem 13. *Let B be a frequency square of type $(2\lambda; \lambda)$. Then B is a bachelor if and only if λ is odd and B is isomorphic to $A_{2\lambda}$.*

Proof. The fact that $A_{2\lambda}$ is a bachelor when λ is odd follows from Theorem 4. So it suffices to construct an orthogonal mate B' of type $(2\lambda; \lambda)$ for any B such that λ is even or B is not isomorphic to $A_{2\lambda}$.

With respect to any two distinct rows r and r' of B , we say that a column c is of type 1 if cells (r, c) and (r', c) contain the same entry; otherwise column c is of type 2. We say that a pair of distinct rows $\{r, r'\}$ in B is *bad* if every column is of type 2 with respect to that pair.

We aim to partition the rows of B into pairs so that no pair is bad. Observe that for a given row r , there are at most λ rows r' such that $\{r, r'\}$ is a bad pair. Suppose first that there exists a row r such that there are exactly λ rows r' for which $\{r, r'\}$ is a bad pair. Each of those λ rows must be identical, and it quickly follows that B is isomorphic to $A_{2\lambda}$. By our assumptions, λ must then be even, so we can easily avoid bad pairs by partitioning rows into pairs of identical rows.

Otherwise for each row r there exists *at most* $\lambda - 1$ rows r' such that $\{r, r'\}$ is a bad pair. Form a graph G where the vertices are the 2λ rows of B , and two rows r and r' are joined by an edge if and only if $\{r, r'\}$ is not a bad pair. The minimum degree of G is at least λ , so by Theorem 12, the graph G contains a perfect matching. Thus there exists a partition \mathcal{P} of the rows of B into pairs, none of which is bad.

For each $\{r, r'\} \in \mathcal{P}$, we next construct corresponding rows r and r' in B' so that:

- Rows r and r' in B' each contain λ ones and λ zeros;
- Each column in B' is of type 2 with respect to rows r and r' ; and
- When rows r and r' of B and B' are superimposed, the ordered pairs $(0, 0)$, $(0, 1)$ and $(1, 0)$ and $(1, 1)$ each occur λ times.

Assuming that these properties hold for every pair in \mathcal{P} , the first and second conditions guarantee that B' is a frequency square of type $(2\lambda; \lambda)$ while the third condition guarantees that B' is an orthogonal mate for B .

Hence, given $\{r, r'\} \in \mathcal{P}$ it remains to determine the entries of rows r and r' of B' satisfying these properties. We say that a column c is of type 1a (respectively, 1b) with respect to (r, r') if (r, c) and (r', c) each contain 0 (respectively, 1). We say that a column c is of type 2a (respectively, 2b) with respect to (r, r') if (r, c) contains 0 (respectively, 1) and (r', c) contains 1 (respectively, 0).

Within rows r and r' of B , let t_{1a} be the number of columns of type 1a, with t_{1b} , t_{2a} and t_{2b} defined similarly. Since each row contains λ zeros and λ ones,

$$t_{1a} + t_{2a} = t_{1b} + t_{2b} = t_{1b} + t_{2a} = t_{1a} + t_{2b} = \lambda,$$

from which it follows that $t_{1a} = t_{1b}$ and $t_{2a} = t_{2b}$. Since the pair of rows $\{r, r'\}$ is not bad, $t_{1a} = t_{1b} > 0$. Of the columns in B of types 1a, 1b, 2a and 2b, respectively, we place $\lambda - \lfloor t_{1a}/2 \rfloor - 2\lceil t_{2a}/2 \rceil$, $\lfloor t_{1a}/2 \rfloor$, $\lceil t_{2a}/2 \rceil$ and $\lceil t_{2a}/2 \rceil$ columns of type 2a in the corresponding positions in B' . That gives us λ columns of type 2a, and the other λ columns in B' are

made to be of type 2b. Note that

$$\begin{aligned} t_{1a} &\geq t_{1a} - \lfloor t_{1a}/2 \rfloor = \lambda - \lfloor t_{1a}/2 \rfloor - t_{2a} \\ &\geq \lambda - \lfloor t_{1a}/2 \rfloor - 2\lceil t_{2a}/2 \rceil \\ &\geq \lambda - \lfloor t_{1a}/2 \rfloor - t_{2a} - 1 = t_{1a} - \lfloor t_{1a}/2 \rfloor - 1 \geq 0 \end{aligned}$$

given that $t_{1a} \geq 1$. In particular, $t_{1a} \geq \lambda - \lfloor t_{1a}/2 \rfloor - 2\lceil t_{2a}/2 \rceil \geq 0$, which shows that our construction is feasible. Moreover, the ordered pairs $(0, 0)$, $(0, 1)$ and $(1, 0)$ and $(1, 1)$ each occur $t_{1a} + \lceil t_{2a}/2 \rceil + t_{2a} - \lfloor t_{2a}/2 \rfloor = \lambda$ times in rows $\{r, r'\}$ of the superposition of B and B' , as required. \square

4 Trades in MOFS

In this section we consider some transformations that can be used to alter the structure of a set of MOFS. The idea is to identify a comparatively small number of cells that can be changed, whilst preserving the property of being a set of MOFS. This leads to the idea of *trades*, which has been extensively studied for other designs [1, 3, 5], but we are not aware of any previous work regarding trades in binary MOFS.

Formally we define a trade in a set $\{F_1, \dots, F_k\}$ of MOFS to be a suitable set of cells C_i for each F_i in the set of MOFS. An individual C_i can be empty, but they should not all be empty. To *switch* the trade we change the entries in every cell in C_i in square F_i for each i . The test for whether the chosen cells are suitable is that the result of switching on the trade should again be a set of MOFS. We do not attempt to characterise the general case any further, but instead look at a simple special case which is already powerful enough to be interesting. In this special case the nonempty C_i are all equal.

Theorem 14. *Suppose that we have a set $\mathcal{F} = \{F_1, F_2, \dots, F_k\}$ of MOFS of order n and $\emptyset \neq C \subseteq N(n) \times N(n)$. For $1 \leq i \leq k$, let $C_i = C$ if F_i either agrees with F_1 on every cell in C or disagrees with F_1 on every cell in C , and let $C_i = \emptyset$ otherwise. Let $V_{i,a} = \{(x, y) \in C : F_i(x, y) = a\}$ for $1 \leq i \leq k$ and $a \in \{0, 1\}$. Then $T = (C_1, C_2, \dots, C_k)$ forms a trade if and only if*

- *Each row or column of F_1 contains equal numbers of zeros and ones within the cells in C .*
- *For each j such that $C_j = \emptyset$, we have $|V_{1,1} \cap V_{j,1}| = |V_{1,0} \cap V_{j,1}|$.*

Proof. We note that T is nonempty, because $C_1 = C \neq \emptyset$. Let $\{F'_1, F'_2, \dots, F'_k\}$ be the matrices produced by switching $\{F_1, F_2, \dots, F_k\}$ on T . First suppose that the two conditions are satisfied. The first condition guarantees that each F'_i is a frequency square. The two conditions together imply that $|V_{1,1} \cap V_{j,0}| = |V_{1,0} \cap V_{j,0}|$. Therefore, the two conditions ensure that F'_i is orthogonal to F'_j for all $1 \leq i < j \leq k$, since F_i is orthogonal to F_j . Thus, T is a trade if the two conditions are satisfied. Conversely, if T is a trade, then the first condition is satisfied, since F'_1 is a frequency square. Finally, for j such that $C_j = \emptyset$, F'_1 is orthogonal to $F'_j = F_j$ only if the second condition is satisfied. This completes the proof. \square

We call the trades described in Theorem 14, *basic trades*. There are some fairly trivial examples of basic trades where switching on the trade does not change the combinatorial structure of the set of MOFS.

Lemma 15. *Below are three ways to define basic trades for which switching does not change the isomorphism class of the set of MOFS.*

- Let $C = N(n) \times N(n)$.
- Let C be the set of cells on which F_1 agrees with F_j for some fixed $j > 1$.
- Let C be the set of cells on which F_1 disagrees with F_j for some fixed $j > 1$.

Proof. If we take $C = N(n) \times N(n)$, then $C_1 = C$. However, $C_i = \emptyset$ for $i > 1$ since F_i cannot agree with F_1 on every cell or disagree with it on every cell, since F_i is orthogonal to F_1 . So, in this case the trade simply complements F_1 (interchanges zeros and ones within F_1).

Next consider what happens when we take C to be the set of cells on which F_1 disagrees with F_j . Since F_1 is orthogonal to F_j , C must consist of exactly half of all cells in these squares. Switching on these cells converts F_1 into F_j and vice versa. Let $i \in N(k) \setminus \{1, j\}$. We know that F_i is orthogonal to F_1 and hence agrees with F_1 on exactly half of its cells. If F_i disagrees with F_1 on every cell in C it would have to equal F_j . Also, if F_i agrees with F_1 on every cell in C it would have to disagree with F_j in every cell. Either option is impossible, since F_i is orthogonal to F_j . So we conclude that $C_i = \emptyset$. Moreover, Lemma 7 ensures that $|V_{1,1} \cap V_{i,1}| = |V_{1,0} \cap V_{i,1}|$, so the trade is valid, by Theorem 14. The result of switching on the trade is to interchange F_1 and F_j , resulting in an isomorphic set of MOFS.

Taking C to be the set of cells on which F_1 agrees with F_j works similarly. Switching on it is equivalent to interchanging F_1 and F_j and then complementing both squares. \square

However, switching on a basic trade often does change the structure:

Theorem 16. *Let $n > 2$ and let \mathcal{F} be a set of MOFS(n) in which every frequency square has the property that every pair of rows is either equal or complementary. Then \mathcal{F} has at least $(n/2)^4$ basic trades each of which produce a new set of MOFS that are not isomorphic to \mathcal{F} .*

Proof. Up to permutations of the rows and columns, each of the squares in \mathcal{F} has block structure (2). Choose C to be any of the “intercalates” in F_1 , that is, 2×2 submatrices that meet all four blocks in F_1 . There are $(n/2)^4$ choices for C . We claim each of them produces a basic trade. It is obvious that each row and column of F_1 has the same number of zeros and ones in cells in C . Moreover, in each F_i the number of ones that occur in cells in C must be even, since the two rows that meet C are either equal or complementary. If C induces an identity matrix or its complement in F_i , then $C_i = C$. In the other squares, C must induce a matrix with either constant rows or constant columns, and $C_i = \emptyset$. Either case satisfies the second condition in Theorem 14.

After switching on the trade, F_1 becomes a matrix with two rows that are neither equal nor complementary, so the new set of MOFS is not isomorphic to the original set. \square

Theorem 17. For any n for which there exists a Hadamard matrix of order n there exists at least $2^{n^2/4-O(n \log n)}$ isomorphism classes of complete sets of MOFS(n).

Proof. By Theorem 1, from a Hadamard matrix we can construct a complete set of MOFS of the same order. The construction used to prove that theorem ensures that every square in that set has the property that each pair of rows is equal or complementary. Any such square is determined by its first row and first column. We assume, without loss of generality, that the first square has block structure (2).

Say that a complete set $\{F_1, \dots, F_{(n-1)^2}\}$ of MOFS(n) is *standardised* if $F_i(1, 1) = 0$ for $1 \leq i \leq (n-1)^2$. An isomorphism class of MOFS contains $e^{O(n \log n)}$ standardised MOFS since the rows and columns can be permuted in $n!^2 = e^{O(n \log n)}$ ways and then there is a unique way to standardise the set by complementing any squares that have a one in their (1, 1) cell.

We make use of the basic trades described in Theorem 16. Consider the set of trades $\mathcal{T} = \{T_{r,c} : 2 \leq r \leq n/2, 2 \leq c \leq n/2\}$, where $T_{r,c}$ uses the cells

$$C = \{(r, c), (r + n/2, c), (r, c + n/2), (r + n/2, c + n/2)\}.$$

Observe that $T_{r,c}$ and $T_{r',c'}$ involve disjoint sets of cells unless $r = r'$ and $c = c'$. Hence we can switch on any subset of \mathcal{T} to obtain a new complete set of MOFS. As we have preserved the first row and column of each square, and these are unique to that square, we cannot produce two sets of MOFS that are the same but have their squares listed in a different order. Also, every set that we produce is standardised, so we have built $2^{|\mathcal{T}|} = 2^{n^2/4-O(n)}$ standardised complete sets of MOFS. The result now follows since the number of isomorphism classes is at least $2^{n^2/4-O(n)}/e^{O(n \log n)} = 2^{n^2/4-O(n \log n)}$. \square

5 Computational results

In this section we report the results of a computational exploration of maximality among sets of MOFS of small orders. Our results were each obtained by two independently written programs. The computations took several months of CPU time. In order to present sets of MOFS more compactly we adapt the notation used earlier. Rather than just superimposing the squares as we did in (7), we superimpose them and then convert the resulting entries from binary to decimal. For example, the first row of (7) would be written as [27,23,12,1,2,28] rather than [11011,10111,01100,00001,00010,11100].

All sets of MOFS(4) extend to a complete set, so there are no maximal sets of MOFS(4) that are not complete. There are three different complete sets of MOFS(4), up to isomorphism [5]. One of the 3 sets is related to the other two by basic trades that switch 4 cells in 4 squares:

$$\begin{bmatrix} 511 & 448 & 21 & 42 \\ 76 & 115 & 410 & 421 \\ 259 & 316 & 233 & 214 \\ 176 & 143 & 358 & 345 \end{bmatrix} \qquad \begin{bmatrix} 511 & 448 & 21 & 42 \\ 76 & 115 & 410 & 421 \\ 259 & 316 & 233 & 214 \\ 176 & 143 & 358 & 345 \end{bmatrix} \qquad (15)$$

A basic trade on the cells highlighted in the left hand copy above changes the last four frequency squares in the set. A basic trade on the cells highlighted in the right hand copy above changes the 4th, 5th, 6th and 7th frequency squares in the set. The basic trades both produce sets of MOFS that are not isomorphic to each other or the initial set of MOFS. There is no single basic trade that switches between the isomorphism classes of the sets of MOFS that result from the two basic trades highlighted in (15). The set of MOFS produced by the trade shown on the right in (15) are the ones produced from Theorem 1. They are the only ones in which every frequency square consists of rows which pairwise are either equal or complementary.

Up to equivalence, there are 6 frequency squares of type (6; 3) and 2435 pairs of MOFS of the same type. For each pair P we found and stored every “mate” that allows the pair to extend to a triple. The number of mates ranged from 5937 to 7413. A graph Γ_P was then constructed with the mates as its vertices, and edges indicating orthogonality. It was easily observed that every vertex in Γ_P had positive degree (indeed, the minimum degree ranged from 548 to 1369) and that every edge was in a triangle. It follows that aside from the unique bachelor (see Theorem 13), there are no maximal sets of MOFS of type (6; 3) containing fewer than 5 squares. There are a large number of maximal sets of 5 squares. By the above method we generated 577 418 387 (respectively, 1475) 5-maxMOFS(6) that do (respectively, do not) satisfy a relation. We did not store the former so we cannot say how many isomorphism classes they represent. However, we did store the 1475 sets of 5-maxMOFS(6) that do not satisfy a relation, and these come from 130 isomorphism classes. The most symmetric set of 5-maxMOFS(6) has an automorphism group of order 10. A representative of that class follows. Its \mathbb{Z}_2 -sum is the identity matrix.

$$\begin{bmatrix} 31 & 17 & 18 & 0 & 15 & 12 \\ 17 & 21 & 30 & 6 & 9 & 10 \\ 18 & 30 & 8 & 29 & 3 & 5 \\ 0 & 6 & 29 & 7 & 24 & 27 \\ 15 & 9 & 3 & 24 & 22 & 20 \\ 12 & 10 & 5 & 27 & 20 & 19 \end{bmatrix} \quad (16)$$

One of the sets of 5-maxMOFS(6) satisfying a relation was given in (7).

Next we used an elementary backtracking search to locate all cliques of size 15 or more in Γ_P . Each k -clique of Γ_P corresponds to a set of $(k + 2)$ -MOFS(6). Of the 2435 pairs of MOFS(6), there were 842 pairs that extended to a set of 17-MOFS(6) and no pair extended further. We conclude that the largest set of MOFS(6) has cardinality 17. There are 18 sets of 17-MOFS(6) up to isomorphism. We now present these 18 sets, starting with this example:

$$\begin{bmatrix} 72128 & 91655 & 44068 & 53560 & 731 & 131071 \\ 115574 & 15266 & 58249 & 15454 & 87221 & 101449 \\ 46877 & 54474 & 129267 & 84231 & 76344 & 2020 \\ 107666 & 39541 & 86604 & 28625 & 52654 & 78123 \\ 24107 & 100765 & 1395 & 107246 & 130880 & 28820 \\ 26861 & 91512 & 73630 & 104097 & 45383 & 51730 \end{bmatrix}$$

The 6 lightly shaded cells indicate a trade which changes the first 6 squares in the set, and the 6 darkly shaded cells indicate a trade which changes the last 6 squares in the set. Both trades result in non-isomorphic sets of 17-MOFS(6).

Similarly, the following matrices represent sets of 17-MOFS(6) where the shading shows 6 cells where there is a trade that changes the first 6 frequency squares and leaves the other 11 unchanged. Each such trade leads to a non-isomorphic set of 17-MOFS(6).

$$\begin{bmatrix} 94304 & 36518 & 26456 & 37249 & 67615 & 131071 \\ 60811 & 119066 & 11061 & 13558 & 120429 & 68288 \\ 107059 & 80348 & 130181 & 24122 & 1513 & 49990 \\ 23468 & 25671 & 37595 & 117109 & 81666 & 107704 \\ 71639 & 47721 & 82094 & 108300 & 59890 & 23569 \\ 35932 & 83889 & 105826 & 92875 & 62100 & 12591 \end{bmatrix}$$

$$\begin{bmatrix} 7199 & 11745 & 123152 & 98958 & 21088 & 131071 \\ 110272 & 119623 & 6837 & 38266 & 92315 & 25900 \\ 61612 & 88540 & 79467 & 52305 & 110390 & 899 \\ 120753 & 41015 & 47562 & 92781 & 2012 & 89090 \\ 67942 & 79384 & 53005 & 31666 & 62663 & 98553 \\ 25435 & 52906 & 83190 & 79237 & 104745 & 47700 \end{bmatrix}$$

$$\begin{bmatrix} 25649 & 117472 & 70400 & 41438 & 7183 & 131071 \\ 47762 & 83118 & 59717 & 70263 & 54648 & 77705 \\ 89554 & 13765 & 124446 & 54185 & 76409 & 34854 \\ 110765 & 31324 & 18875 & 77154 & 100244 & 54851 \\ 36716 & 104731 & 14058 & 20117 & 123075 & 94516 \\ 82767 & 42803 & 105717 & 130056 & 31654 & 216 \end{bmatrix}$$

In the next example the set of 17-MOFS(6) has two trades which lead to non-isomorphic sets of 17-MOFS(6). The first trade consists of switching the first and last rows of the first square in the set. The second trade consists of switching the first and last columns of the first square in the set.

$$\begin{bmatrix} 105968 & 128645 & 75835 & 27623 & 53258 & 1884 \\ 69126 & 32895 & 29592 & 98689 & 131071 & 31840 \\ 94557 & 12170 & 50789 & 122426 & 73952 & 39319 \\ 21283 & 124242 & 105164 & 19673 & 43828 & 79023 \\ 59598 & 72553 & 83382 & 46380 & 5843 & 125457 \\ 42681 & 22708 & 48451 & 78422 & 85261 & 115690 \end{bmatrix}$$

Similarly, in the following two examples there is a trade consisting of switching the first and last rows of the first square in the set:

$$\begin{bmatrix} 125836 & 97351 & 66937 & 6902 & 46890 & 49297 \\ 32895 & 100227 & 31152 & 26176 & 71692 & 131071 \\ 8097 & 127032 & 41678 & 56607 & 91893 & 67906 \\ 113233 & 21466 & 117926 & 82733 & 11419 & 46436 \\ 87274 & 36404 & 78615 & 110040 & 53701 & 27179 \\ 25878 & 10733 & 56905 & 110755 & 117618 & 71324 \end{bmatrix}$$

$$\begin{bmatrix} 96320 & 74526 & 120239 & 6329 & 53090 & 42709 \\ 32895 & 126601 & 8084 & 119634 & 76268 & 29731 \\ 26544 & 103540 & 43595 & 77095 & 86683 & 55756 \\ 98689 & 19706 & 96885 & 18253 & 45734 & 113946 \\ 131071 & 39713 & 66754 & 59542 & 13657 & 82476 \\ 7694 & 29127 & 57656 & 112360 & 117781 & 68595 \end{bmatrix}$$

Finally, we present two more sets of 17-MOFS(6) which have no basic trades other than those of the type covered by Lemma 15.

$$\begin{bmatrix} 65567 & 67553 & 62976 & 51608 & 14438 & 131071 \\ 89932 & 37271 & 10972 & 95538 & 42667 & 116833 \\ 47401 & 53876 & 109907 & 90797 & 87258 & 3974 \\ 107764 & 27950 & 17275 & 7361 & 129941 & 102922 \\ 29635 & 125130 & 103852 & 40575 & 68400 & 25621 \\ 52914 & 81433 & 88231 & 107334 & 50509 & 12792 \end{bmatrix}$$

$$\begin{bmatrix} 65567 & 51334 & 30488 & 47201 & 67552 & 131071 \\ 97457 & 26213 & 41298 & 119452 & 40399 & 68394 \\ 123843 & 81164 & 39861 & 1663 & 28842 & 117840 \\ 55078 & 19417 & 88171 & 107913 & 109108 & 13526 \\ 40520 & 111354 & 77447 & 19890 & 86357 & 57645 \\ 10748 & 103731 & 115948 & 97094 & 60955 & 4737 \end{bmatrix}$$

This completes the specification of the 18 isomorphism classes of sets of 17-MOFS(6). No pair of these classes is connected by basic trades unless our description specified such a relationship.

All 18 sets of 17-MOFS(6) satisfy a (3, 3)-relation, thereby demonstrating that they are maximal by Theorem 4. We next consider the relations satisfied by sets of k -MOFS(6) for $1 < k < 17$. By Theorem 5, we need only consider $k \in \{5, 9, 13\}$. Also, by Theorem 6, when $k \in \{5, 13\}$ we only need to consider (r, s) -relations where

$$(r, s) \in \{(1, 3), (3, 1), (3, 5), (5, 3)\}. \tag{17}$$

A set of k -MOFS(6) having any of the relations in (17) can easily be converted into an isomorphic set satisfying any of the other 3 kinds of relations. Transposing all the

squares in a set of MOFS interchanges r and s , and complementing both X_1 and X_3 transforms a set of MOFS with an (r, s) -relation into one with an $(n - r, n - s)$ -relation. Thus the only question is whether there exists a set with any of the relations in (17) or not. We have already demonstrated a set of 5-maxMOFS(6) satisfying a $(5, 3)$ -relation in (7). Similarly, here is a set of 13-maxMOFS(6) satisfying a $(5, 3)$ -relation. The shaded cells indicate a basic trade which can be switched to reach a set of 13-maxMOFS(6) that do not satisfy any relation.

$$\begin{bmatrix} 4095 & 4196 & 4539 & 3587 & 7708 & 448 \\ 1576 & 2266 & 7495 & 4847 & 4881 & 3508 \\ 2181 & 7289 & 1910 & 5266 & 1001 & 6926 \\ 6442 & 1923 & 6832 & 2397 & 1126 & 5853 \\ 5457 & 798 & 3784 & 5548 & 2231 & 6755 \\ 4822 & 8101 & 13 & 2928 & 7626 & 1083 \end{bmatrix} \quad (18)$$

Switching the trade only changes the first square in the set of MOFS.

For sets of 9-MOFS(6) there were more possibilities, *a priori*. By Theorem 6, we need to consider (r, s) -relations where

$$(r, s) \in \{(1, 1), (5, 5)\} \cup \{(1, 5), (5, 1)\} \cup \{(3, 3)\}. \quad (19)$$

Here we have partitioned the possibilities into sets of relations that can be transformed into each other by the moves described above. As already noted, only the last possibility is achieved by sets of 17-MOFS(6). However, there are sets of 9-MOFS(6) achieving all of the options in (19). We start by giving a set of 9-MOFS(6) with a $(1, 1)$ -relation then a set of 9-MOFS(6) with a $(1, 5)$ -relation:

$$\begin{bmatrix} 284 & 511 & 259 & 4 & 224 & 251 \\ 433 & 288 & 335 & 126 & 154 & 197 \\ 206 & 338 & 444 & 483 & 9 & 53 \\ 457 & 108 & 113 & 27 & 438 & 390 \\ 55 & 135 & 170 & 464 & 365 & 344 \\ 98 & 153 & 212 & 429 & 343 & 298 \end{bmatrix} \quad \begin{bmatrix} 257 & 270 & 18 & 228 & 249 & 511 \\ 333 & 419 & 127 & 148 & 194 & 312 \\ 436 & 220 & 481 & 11 & 47 & 338 \\ 110 & 471 & 21 & 426 & 409 & 96 \\ 179 & 56 & 458 & 375 & 324 & 141 \\ 218 & 97 & 428 & 345 & 310 & 135 \end{bmatrix}$$

Next we give a set of 9-maxMOFS(6) that satisfies a $(3, 3)$ -relation.

$$\begin{bmatrix} 449 & 106 & 180 & 307 & 93 & 398 \\ 180 & 449 & 106 & 398 & 307 & 93 \\ 106 & 180 & 449 & 93 & 398 & 307 \\ 511 & 7 & 280 & 169 & 210 & 356 \\ 280 & 511 & 7 & 356 & 169 & 210 \\ 7 & 280 & 511 & 210 & 356 & 169 \end{bmatrix} \quad (20)$$

If the first and last rows of the first square in (20) are switched, then the result is a set of 9-maxMOFS(6) that do not satisfy any relation.

In (16), (20) and (18) we have described sets of k -maxMOFS(6) for $k \in \{5, 9, 13\}$ that do not satisfy a relation. In fact we found sets of k -maxMOFS(6) for all $5 \leq k \leq 15$ that do not satisfy a relation. There are no sets of 16-maxMOFS(6). Here we give sets of k -maxMOFS(6) for $k \in \{6, 7, 8, 10, 11, 12, 14, 15\}$:

$$\begin{array}{cc}
 \begin{bmatrix} 63 & 33 & 34 & 1 & 28 & 30 \\ 36 & 45 & 50 & 14 & 19 & 25 \\ 43 & 54 & 25 & 60 & 0 & 7 \\ 8 & 10 & 61 & 7 & 54 & 49 \\ 23 & 21 & 4 & 56 & 43 & 42 \\ 16 & 26 & 15 & 51 & 45 & 36 \end{bmatrix} & \begin{bmatrix} 127 & 64 & 67 & 5 & 56 & 62 \\ 73 & 84 & 106 & 31 & 36 & 51 \\ 86 & 111 & 53 & 112 & 11 & 8 \\ 25 & 26 & 124 & 6 & 99 & 101 \\ 32 & 45 & 14 & 121 & 87 & 82 \\ 38 & 51 & 17 & 106 & 92 & 77 \end{bmatrix} \\
 \\
 \begin{bmatrix} 255 & 128 & 129 & 14 & 114 & 125 \\ 145 & 175 & 214 & 58 & 76 & 97 \\ 170 & 220 & 107 & 229 & 19 & 20 \\ 53 & 54 & 248 & 9 & 199 & 202 \\ 66 & 89 & 31 & 240 & 173 & 166 \\ 76 & 99 & 36 & 215 & 184 & 155 \end{bmatrix} & \begin{bmatrix} 1023 & 513 & 526 & 51 & 452 & 504 \\ 584 & 698 & 855 & 230 & 305 & 397 \\ 677 & 884 & 427 & 920 & 79 & 82 \\ 219 & 213 & 992 & 44 & 794 & 807 \\ 256 & 363 & 124 & 963 & 701 & 662 \\ 310 & 398 & 145 & 861 & 738 & 617 \end{bmatrix} \\
 \\
 \begin{bmatrix} 2047 & 1025 & 1038 & 119 & 920 & 992 \\ 1200 & 1378 & 1691 & 462 & 597 & 813 \\ 1372 & 1773 & 850 & 1841 & 170 & 135 \\ 451 & 413 & 1956 & 56 & 1638 & 1627 \\ 516 & 762 & 245 & 1923 & 1353 & 1342 \\ 555 & 790 & 361 & 1740 & 1463 & 1232 \end{bmatrix} & \begin{bmatrix} 4095 & 2055 & 2105 & 194 & 1864 & 1972 \\ 2448 & 2788 & 3407 & 798 & 1137 & 1707 \\ 2794 & 3384 & 1747 & 3909 & 421 & 30 \\ 769 & 891 & 3732 & 253 & 3210 & 3430 \\ 1063 & 1490 & 492 & 3624 & 2975 & 2641 \\ 1116 & 1677 & 802 & 3507 & 2678 & 2505 \end{bmatrix} \\
 \\
 \begin{bmatrix} 16383 & 8207 & 8433 & 1814 & 6432 & 7880 \\ 8746 & 11717 & 13136 & 3512 & 5743 & 6295 \\ 11284 & 14248 & 7203 & 15067 & 965 & 382 \\ 2788 & 4754 & 15694 & 1097 & 10683 & 14133 \\ 4441 & 3955 & 2958 & 14885 & 13468 & 9442 \\ 5507 & 6268 & 1725 & 12774 & 11858 & 11017 \end{bmatrix} \\
 \\
 \begin{bmatrix} 32767 & 16415 & 16865 & 3622 & 13896 & 14736 \\ 22147 & 19288 & 31844 & 4602 & 11141 & 9279 \\ 22568 & 26566 & 12819 & 32157 & 2294 & 1897 \\ 11123 & 7461 & 25276 & 4813 & 21778 & 27850 \\ 1236 & 15018 & 3467 & 26416 & 29039 & 23125 \\ 8460 & 13553 & 8030 & 26691 & 20153 & 21414 \end{bmatrix}
 \end{array}$$

For orders larger than 6 it is not feasible to do exhaustive computations. However, we did a partial enumeration of sets of MOFS(10) inspired by the example in (20). The idea was to impose a block circulant structure similar to that example. Each square was assumed to be composed of 4 circulant blocks. Under this (strong) assumption, we found that the largest set of MOFS(10) that is possible has size 17. Every such example satisfies a (5, 5)-relation, and hence is maximal by Theorem 4. The first and sixth rows of one

such example are

$$\begin{bmatrix} 52452 & 86882 & 89113 & 107209 & 108822 & 26453 & 27322 & 38362 & 39725 & 79015 \\ 131071 & 127 & 3971 & 29068 & 46640 & 63555 & 72404 & 77160 & 115121 & 116238 \end{bmatrix}.$$

In light of Theorem 6, the only other k for which we might hope to find a block circulant set of k -MOFS(10) satisfying a (5,5)-relation are $k = 1$ and $k = 9$. The former case is rather trivially handled by Theorem 13, whilst for $k = 9$ we did find a (necessarily maximal) set with the following first and sixth rows

$$\begin{bmatrix} 210 & 332 & 353 & 404 & 427 & 110 & 117 & 157 & 162 & 283 \\ 511 & 1 & 14 & 55 & 248 & 201 & 312 & 338 & 420 & 455 \end{bmatrix}.$$

6 Embeddings

As discussed in the introduction, the Hadamard conjecture implies the existence of a complete set of MOFS of type $(n; n/2)$ whenever n is divisible by 4. In this section we explore the case $n \equiv 2 \pmod{4}$ via embeddings of sets of MOFS, building on the computational results in the previous section. The following lower bounds for the size of sets of binary MOFS of order $n \equiv 2 \pmod{4}$ for small values of n are given in [16, 17]:

Theorem 18. *There exist sets of k -MOFS(n) whenever (k, n) is an element of*

$$\begin{aligned} &\{(8, 6), (4, 10), (4, 14), (8, 18), (4, 22), (4, 26), (8, 30), (4, 34), \\ &(4, 38), (8, 42), (5, 46), (6, 50), (7, 54), (5, 58), (6, 62), (7, 66), \\ &(6, 70), (7, 74), (7, 78), (8, 82), (6, 86), (8, 90), (7, 94), (6, 98)\}. \end{aligned}$$

Theorem 25 at the end of this section improves each of the lower bounds in Theorem 18 to $k = 17$.

Let s, n be positive even integers with $s < n$. We define an *incomplete frequency square* of type $(n; s)$ to be an $n \times n$ array F , indexed by $N(n)$, such that:

1. the subarray indexed by $N(s) \times N(s)$ is empty and all other cells of F contain 0 or 1, and
2. each row and column is *balanced* in the sense that it contains equal numbers of the symbols 0 and 1.

We say that two incomplete frequency squares are *orthogonal* if, when superimposed, each of the four possible ordered pairs $(0, 0)$, $(0, 1)$, $(1, 0)$ and $(1, 1)$ occurs the same number of times. We use the notation k -IMOFS($n; s$) to denote k incomplete frequency squares, each pair of which is orthogonal in the above sense. We will present sets of IMOFS in superimposed format, similar to (7). Note that similar results to ours below could be developed for sets of IMOFS with multiple holes; however a single hole is enough for the purposes of this paper.

In the following, for any binary vector \mathbf{r} , we write $\bar{\mathbf{r}}$ for the complement of \mathbf{r} , that is, the vector formed by replacing each entry e with $1 - e$. The array $I(\mathbf{r})$ is the 2×2 array defined by

$$I(\mathbf{r}) = \begin{bmatrix} \mathbf{r} & \bar{\mathbf{r}} \\ \bar{\mathbf{r}} & \mathbf{r} \end{bmatrix}.$$

An important property of $I(\mathbf{r})$ is that its rows and columns are balanced.

Lemma 19. *If there exists a set of 2-IMOFS($n; n - 2$), then the bottom right-hand corner must be isomorphic to*

$$\begin{bmatrix} 00 & 01 \\ 10 & 11 \end{bmatrix}.$$

Proof. The number of filled cells in a pair of IMOFS($n; n - 2$) is equal to $4n - 4$. Therefore there are an odd number of cells filled with \mathbf{r} for each of the four choices of \mathbf{r} . Observe that to achieve balance in any row or column, the number of occurrences of \mathbf{r} must equal the number of occurrences of $\bar{\mathbf{r}}$ for each possible \mathbf{r} . Let M be the 2×2 subarray in the bottom right-hand corner. Suppose, for the sake of contradiction, that there exists an ordered pair \mathbf{r} which does not occur in M . Then, without loss of generality (considering the transpose if necessary), \mathbf{r} occurs α times within the first $n - 2$ rows where α is odd. Now, each of the first $n - 2$ rows contains \mathbf{r} if and only if it contains $\bar{\mathbf{r}}$. Thus, $\bar{\mathbf{r}}$ occurs α times within the first $n - 2$ rows. Since \mathbf{r} and $\bar{\mathbf{r}}$ must occur the same number of times in the final two columns, $\bar{\mathbf{r}}$ cannot occur in M . However, considering the final column, there must be an equal number of occurrences of \mathbf{r} and $\bar{\mathbf{r}}$, contradicting the fact that α is odd. Thus each possibility for \mathbf{r} occurs in M exactly once. Next, suppose that \mathbf{r} and $\bar{\mathbf{r}}$ occur in the final column of M . Then \mathbf{r} occurs an even number of times in the first $n - 2$ rows. However, \mathbf{r} must occur an odd number of times in the first $n - 2$ columns. Thus \mathbf{r} occurs an even number of times altogether, a contradiction. A similar argument shows that \mathbf{r} and $\bar{\mathbf{r}}$ cannot occur in any row or column of M , from which the result follows. \square

Lemma 20. *There does not exist a set of 3-IMOFS($n; n - 2$).*

Proof. From Lemma 19, without loss of generality the bottom right-hand corner must be isomorphic to:

$$\begin{bmatrix} 000 & 01a \\ 10b & 11c \end{bmatrix}$$

Considering the first and third IMOFS in light of Lemma 19, we must have $a = c = 1$. However, considering the second and third IMOFS, we get $a = 0$, a contradiction. \square

We now turn our attention to existence results.

Lemma 21. *There exists a pair of IMOFS($n; n - 2$) for each even $n \geq 4$.*

Proof. We first exhibit a set of 2-IMOFS(4, 2):

$$\begin{bmatrix} \cdot & \cdot & 01 & 10 \\ \cdot & \cdot & 11 & 00 \\ 10 & 11 & 00 & 01 \\ 01 & 00 & 10 & 11 \end{bmatrix}.$$

For $n \geq 6$, the above structure can be placed in the bottom right-hand corner. Fill the remaining cells in the last two rows with copies of $I(00)$ and the remaining cells in the last two columns with copies of $I(01)$. \square

A (v_*, k_*, λ_*) orthogonal array is a $\lambda_* v_*^2 \times k_*$ array with entries chosen from a set X of size v_* such that in every pair of columns of the array, each ordered pair from X occurs exactly λ_* times. Let H be a Hadamard matrix of order $4\lambda_*$ in normalised form (so that the first column are all 1's). Then by the definition of a Hadamard matrix, the remaining columns of H form a $(2, 4\lambda_* - 1, \lambda_*)$ orthogonal array (with $X = \{1, -1\}$). Existence results for Hadamard matrices (see [5]) yield the following:

Lemma 22. *There exists a $(2, 4\lambda_* - 1, \lambda_*)$ orthogonal array whenever $1 \leq \lambda_* < 167$ or λ_* is a power of 2.*

Theorem 23. *If there exists a $(2, k_*, \lambda_*)$ orthogonal array and $4\lambda_*$ divides $b(n - b)$, then there exists a set of k_* -IMOFS($n; n - 2b$).*

Proof. There are $4b(n - b)$ non-empty cells in an IMOFS($n; n - 2b$). Let $\alpha = 4b(n - b)/16\lambda_*$. Fill the non-empty cells using α copies of $I(\mathbf{r})$ for each row \mathbf{r} of the $(2, k_*, \lambda_*)$ orthogonal array (we are assuming without loss of generality that the symbols of the orthogonal array are 0 and 1). \square

By Lemma 22 and Theorem 23, we get:

Corollary 24. *If 2^β divides $b(n - b)$, then a set of $(2^\beta - 1)$ -IMOFS($n; n - 2b$) exists.*

It is worth noting that if b is odd, the previous theorem is of little use. That is, the embedding approach in this section is not apparently helpful in obtaining set of MOFS of order not divisible by 4 from sets of MOFS of order divisible by 4, the latter of which are far easier to construct.

Theorem 25. *There exists a set of 17-MOFS(n) for each order $n \equiv 2 \pmod{4}$ where $n \geq 6$.*

Proof. From §5, there is a set of 17-MOFS(6) and a set of 17-MOFS(10). By Lemma 22, there exist a $(2, k_*, \lambda_*)$ orthogonal array with $k_* \geq 17$ for $\lambda_* \in \{6, 14, 24, 36, 50, 66\}$. By Theorem 23, there thus exists a set of 17-IMOFS($10 + 4B; 10$) for $1 \leq B \leq 6$. So, by “plugging” the hole of size 10 with a set of 17-MOFS(10), there exists a set of 17-MOFS(n) for each $n \equiv 2 \pmod{4}$ such that $14 \leq n \leq 34$.

Next, if 16 divides b , then by Corollary 24, there exists a set of 31-IMOFS ($n; n - 2b$) for any $n > 2b$. The result follows recursively. \square

7 Maximal sets of MOFS

We now show the following existence result.

Theorem 26. *There exists a set of 5-maxMOFS(n) for each $n \equiv 2 \pmod{4}$ where $n \geq 6$.*

Proof. Our starting point is the set of 5-maxMOFS(6) satisfying a (5, 3)-relation that was given in (7). We now embed that set of 5-maxMOFS(6) into a set of 5-maxMOFS($4\kappa + 2$), for each $\kappa > 1$. In the process we will add each binary 5-tuple the same number of times, thereby ensuring that orthogonality is preserved. Also the resulting 5-MOFS($4\kappa + 2$) will satisfy a $(2\kappa + 3, 2\kappa + 1)$ -relation, ensuring that it is maximal, by Theorem 4. Let X_1 be the set of the first $2\kappa + 3$ rows and X_2 the set of the first $2\kappa + 1$ columns. Let X'_1 and X'_2 be the sets of rows and columns not in X_1 and X_2 , respectively. Our set of MOFS will have \mathbb{Z}_2 -sum given by (2), where the top left block has rows X_1 and columns X_2 .

Next we describe the placement of the set of 5-maxMOFS(6). These are placed in the first three columns of each of X_2 and X'_2 , the first 5 rows of X_1 and the first row of X'_1 . Let C be the set of cells which do not include the 36 cells just specified. Then $|C| = (4\kappa + 2)^2 - 6^2 = 16(\kappa^2 + \kappa - 2)$. Excluding the first four rows of C , observe that the remaining cells may be partitioned into intercalates in (2), with one row in each of X_1 and X'_1 and one column in each of X_2 and X'_2 .

We complete our construction by describing how to fill the remaining cells in each frequency square. We do so by first describing how to fill the first four rows then the remaining cells of C using a partition of intercalates as described above.

First suppose that $\kappa \equiv 1$ or $2 \pmod{4}$. Then 64 divides $|C|$; let $c = |C|/64$. Observe that $c = (\kappa^2 + \kappa - 2)/4 \geq \kappa - 1$. We fill the cells of C in the first 4 rows with $\kappa - 1$ copies of the following array so that the tuples with an even number of ones occur in columns in X_2 and tuples with an odd number of ones occur in columns in X'_2 :

$$\begin{bmatrix} 00011 & 00011 & 11100 & 11100 \\ 01100 & 01100 & 10011 & 10011 \\ 10001 & 10001 & 01110 & 01110 \\ 11110 & 11110 & 00001 & 00001 \end{bmatrix} \quad (21)$$

Note that this array has balanced rows and columns. There are 24 binary 5-tuples not in (21), which in turn partition into 12 complementary pairs. Let \mathbf{r}_i for $1 \leq i \leq 12$ be the representatives from these pairs which contain an even number of ones.

To fill the intercalates we first add $\kappa - 1$ copies of each $I(\mathbf{r}_i)$ to C . We have thus far filled $64(\kappa - 1)$ cells of C , including the cells in the first 4 rows, with each binary 5-tuple occurring exactly $2(\kappa - 1)$ times. To fill the remaining $64(c - \kappa + 1)$ cells of C , we partition all 32 binary 5-tuples into 16 complementary pairs, represented by \mathbf{r}_i for $1 \leq i \leq 16$, and add $c - \kappa + 1 \geq 0$ copies of $I(\mathbf{r}_i)$ for each of the 16 possible values of i . It is now routine to check that the construction indeed results in a set of 5-MOFS($4\kappa + 2$) whose \mathbb{Z}_2 -sum is (2).

Otherwise $\kappa \equiv 3$ or $0 \pmod{4}$. In this case $16(\kappa^2 + \kappa - 2) \equiv 32 \pmod{64}$. Consider the following array B :

$$\begin{bmatrix} 11100 & 11010 & 11111 & 11001 \\ 10011 & 10101 & 10000 & 10110 \\ 01110 & 01011 & 00111 & 01101 \\ 00001 & 00100 & 01000 & 00010 \end{bmatrix}$$

This array has balanced columns and includes every binary 5-tuple with an odd number

of 1's. Therefore, if we take the complement of each tuple we obtain an array \overline{B} including every 5-tuple with an even number of 1's. Place exactly one copy of B and \overline{B} in the first 4 rows of C , with \overline{B} in columns of X_2 and B in columns of X'_2 . Note that this is possible since $\kappa \geq 3$. The number of remaining cells is divisible by 64 so we can proceed as in the previous case. \square

8 Concluding remarks

Theorem 13 showed that for $n \equiv 2 \pmod{4}$ there is a unique bachelor frequency square. Our computations showed that there is no other maximal set of k -MOFS(6) with $k < 5$. It would be very interesting to know whether this generalises to larger $n \equiv 2 \pmod{4}$. Note that we do know that there is a maximal set of 5-MOFS(n), by Theorem 26. For $n \equiv 0 \pmod{4}$, the question of how small a maximal set of MOFS(n) can be, is wide open. If it turns out that there are no maximal sets with fewer than 5 MOFS aside from those in Theorem 13 then that would be a significant difference from Latin squares. It is known [6] that maximal pairs of mutually orthogonal Latin squares exist for all orders $n > 6$ that are not twice a prime.

In Theorem 17 we gave a lower bound on the number of complete sets of MOFS(n) for $n \equiv 0 \pmod{4}$ (assuming the Hadamard conjecture). It would be interesting to obtain a corresponding upper bound. In particular, it would be nice to know whether the exponent in our bound is of the correct order. Note that substantial progress has very recently been made on the corresponding problem for Latin squares [2].

Two interesting directions for possible generalisation of our results are to frequency squares with 2 symbols that do not occur equally often or to frequency squares with more than 2 symbols. In particular, how many symbols does it take before bachelor frequency squares become common and other small maximal sets become possible?

Acknowledgements

This work was supported in part by Australian Research Council grant DP150100506. The first author thanks Daniel Mansfield for invaluable C programming help.

References

- [1] E. J. Billington, Combinatorial trades: a survey of recent results, in: W.D. Wallis (Ed.), *Designs 2002: Further Computational and Constructive Design Theory*, Kluwer, Boston, 2002, pp. 47–67.
- [2] S. Boyadzhyska, S. Das and T Szabó, Enumerating extensions of mutually orthogonal Latin squares, *Des. Codes Cryptogr.*, 2020. <https://doi.org/10.1007/s10623-020-00771-6>
- [3] N. J. Cavenagh, The theory and application of Latin bitrades: a survey, *Math. Slovaca* **58** (2008), 691–718.

- [4] N. J. Cavenagh and I. M. Wanless, Latin squares with no transversals, *Electron. J. Combin.* **24(2)** (2017), #P2.45.
- [5] C. J. Colbourn and J. H. Dinitz (eds.), *Handbook of Combinatorial Designs* (2nd ed.), Chapman & Hall/CRC, Boca Raton, 2007.
- [6] P. Danziger, I. M. Wanless and B. S. Webb, Monogamous Latin squares, *J. Combin. Theory Ser. A* **118** (2011), 796–807.
- [7] W. de Launey, On the asymptotic existence of partial complex Hadamard matrices and related combinatorial objects, *Discrete Appl. Math.* **102** (2000), 37–45.
- [8] M. Deza and S. A. Vanstone, Bounds for permutation arrays, *J. Statist. Plann. Inference* **2** (1978), 197–209.
- [9] S. T. Dougherty, A coding theoretic solution to the 36 officer problem, *Des. Codes Cryptogr.* **4** (1994), 123–128.
- [10] P. Dukes and L. Howard, Group divisible designs in MOLS of order 10, *Des. Codes Cryptogr.* **71** (2014), 283–291.
- [11] A. B. Evans, Latin squares without orthogonal mates, *Des. Codes Cryptogr.* **40** (2006), 121–130.
- [12] W. T. Federer, On the existence and construction of a complete set of orthogonal $F(4t; 2t, 2t)$ -squares design, *Ann. Statist.* **5** (1977), 561–564.
- [13] A. Hedayat, D. Raghavarao and E. Seiden, Further contributions to the theory of F -squares design, *Ann. Statist.* **3** (1975), 712–716.
- [14] J. Jedwab and T. Popatia, A new representation of mutually orthogonal frequency squares, submitted for publication, 2020. [arXiv:2003.03920](https://arxiv.org/abs/2003.03920)
- [15] D. Jungnickel, V. C. Mavron and T. P. McDonough, The geometry of frequency squares, *J. Combin. Theory Ser. A* **96** (2001), 376–387.
- [16] C. F. Laywine and G. L. Mullen, A table of lower bounds for the number of mutually orthogonal frequency squares, *Ars Combin.* **59** (2001), 85–96.
- [17] M. Li, Y. Zhang and B. Du, Some new results on mutually orthogonal frequency squares, *Discrete Math.* **331** (2014), 175–187.
- [18] V. C. Mavron, Frequency squares and affine designs, *Electron. J. Combin.* **7** (2000), #R56.
- [19] D. Stinson, A short proof of the non-existence of a pair of orthogonal Latin squares of order six, *J. Combin. Theory Ser. A* **36** (1984), 373–376.
- [20] D. J. Street, Generalized Hadamard matrices, orthogonal groups and F -squares, *Ars Comb.* **8** (1979), 131–141.
- [21] I. M. Wanless and B. S. Webb, The existence of Latin squares without orthogonal mates, *Des. Codes Cryptogr.*, **40** (2006), 131–135.