A new representation of mutually orthogonal frequency squares

Jonathan Jedwab   Tabriz Popatia

8 March 2020 (revised 14 November 2020)

To Gary MacGillivray, in appreciation of his mathematics research, teaching, and service over several decades

Abstract

Mutually orthogonal frequency squares (MOFS) of type $F(m\lambda; \lambda)$ generalize the structure of mutually orthogonal Latin squares: rather than each of m symbols appearing exactly once in each row and in each column of each square, the repetition number is $\lambda \geq 1$. A classical upper bound for the number of such MOFS is $\frac{(m\lambda-1)^2}{m-1}$. We introduce a new representation of MOFS of type $F(m\lambda; \lambda)$, as a linear combination of $\{0, 1\}$ arrays. We use this representation to give an elementary proof of the classical upper bound, together with a structural constraint on a set of MOFS achieving the upper bound. We then use this representation to establish a maximality criterion for a set of MOFS of type $F(m\lambda; \lambda)$ when m is even and λ is odd, which simplifies and extends a previous analysis [3] of the case when $m = 2$ and λ is odd.

1   Introduction

Latin squares are a fundamental concept in combinatorial design theory, whose study is at least 300 years old [2, p. 12]. A frequency square is a generalization of a Latin square, introduced by MacMahon [15] in 1898 under the name "quasi-latin square", subsequently studied in the 1940s by Finney [5], and named in 1969 by Hedayat [7] (see [14] for a survey).

Definition 1. *A* frequency square (F-square) *of type $F(m\lambda; \lambda)$ is an $m\lambda \times m\lambda$ array with elements belonging to the symbol set $\{1, 2, \ldots, m\}$, where each symbol j appears exactly λ times in each row and in each column.*

We note that some authors write $F(m\lambda; \lambda^m)$ instead of $F(m\lambda; \lambda)$. The special case of an F-square of type $F(m; 1)$ is a Latin square of order m. An F-square of type $F(m\lambda; \lambda)$ corresponds to a statistical experimental design offering more flexibility than a design based on a Latin square [9, Section 2].

Definition 2. *Two F-squares S and S' of type $F(m\lambda; \lambda)$ are* orthogonal *if each ordered symbol pair (j, j') appears exactly λ^2 times in the superposition of S on S'.*

A set of pairwise orthogonal F-squares of type $F(m\lambda; \lambda)$ is a set of *mutually orthogonal frequency squares* (MOFS) of type $F(m\lambda; \lambda)$. The central question is:

> How large can a set of MOFS of type $F(m\lambda; \lambda)$ be?

The following result provides an upper bound.

Theorem 3 (Hedayat, Raghavarao, Seiden (1975) [8, Theorem 2.1])**.** *The number of MOFS of type $F(m\lambda; \lambda)$ is at most $\frac{(m\lambda-1)^2}{(m-1)}$.*

A set of MOFS attaining the upper bound in Theorem 3 is *complete*. The special case of a set of MOFS of type $F(m; 1)$ is the well-known concept of a set of mutually orthogonal Latin squares (MOLS) of order m (see [1] for background), and the existence of a complete set of $m - 1$ MOLS of order m is equivalent to the existence of a projective plane of order m and an affine plane of order m [1, Theorem 3.20]. Several ideas from the study of sets of MOLS have been adapted to investigate the existence pattern for sets of MOFS.

The following construction, which depends on symmetric factorial designs, provides a complete set of MOFS of type $F(m\lambda; \lambda)$ when m is a prime power.

Theorem 4 (Hedayat, Raghavarao, Seiden (1975) [8, Theorem 3.1])**.** *Let m be a prime power and h a positive integer. Then there exists a complete set of $\frac{(m^h-1)^2}{m-1}$ MOFS of type $F(m^h; m^{h-1})$.*

Other combinatorial designs have been used to construct complete sets of MOFS with the same parameters as in Theorem 4, including linear permutation polynomials over $\mathrm{GF}(m)$ [17] and affine designs [16].

A further construction of a complete set of MOFS of type $F(m\lambda; \lambda)$ depends on the existence of a Hadamard matrix of order $4n$ (which has long been conjectured for all positive integers n; see [10] for background).

Theorem 5 (Federer (1977) [4, Theorem 2.1]). *Let n be a positive integer and suppose a Hadamard matrix of order $4n$ exists. Then there exists a complete set of $(4n-1)^2$ MOFS of type $F(4n; 2n)$.*

All known constructions of complete sets of F-squares of type $F(m\lambda; \lambda)$ having $m > 2$ require m to be a prime power, and the only known examples having $m = 2$ are as described in Theorem 5. Jungnickel, Mavron and McDonough showed in 2001 how to unify all such constructions in terms of nets [13].

Whereas Theorem 5 shows the existence of a complete set of MOFS of type $F(2\lambda; \lambda)$ when λ is even (subject to the existence of a Hadamard matrix of order 2λ), a recent result established nonexistence when $\lambda > 1$ is odd by making a connection with resolvable designs.

Theorem 6 (Britz, Cavenagh, Mammoliti, Wanless (2019+) [3, Corollary 11]). *There is no complete set of MOFS of type $F(2\lambda; \lambda)$ when $\lambda > 1$ is odd.*

In view of Theorem 6, it is natural to ask:

Q1. What is the maximum size of a set of MOFS of type $F(m\lambda; \lambda)$ when $\lambda > 1$ is odd?

Q2. When is a set of MOFS of type $F(m\lambda; \lambda)$ maximal (that is, not extendible to a larger such set) but not complete?

These questions are explored in the recent paper by Britz et al. [3] when λ is odd. For example, it is shown computationally that for MOFS of type $F(6; 3)$, the maximum size of a set is 17 rather than the upper bound of 25 given by Theorem 3, and there are maximal sets of size t for each t satisfying $t \in \{1, 17\}$ or $5 \leq t \leq 15$.

In this paper, we introduce a representation of MOFS of type $F(m\lambda; \lambda)$ as a linear combination of $\{0, 1\}$ arrays (Section 2). We use this representation to give a new elementary proof of the upper bound of Theorem 3, together with a structural constraint on a complete set of MOFS (Section 3). We then use this representation to establish a maximality criterion for a set of MOFS of type $F(m\lambda; \lambda)$ when m is even and λ is odd (Section 4), extending the analysis of [3] for the case when $m = 2$ and λ is odd.

2 Indicator squares

We begin by introducing a representation of an F-square of type $F(m\lambda; \lambda)$ as a linear combination of $\{0, 1\}$ arrays. We shall use this representation

3

in Section 3 in the new proof of Theorem 3, and in Section 4 to establish maximality criteria. The *indicator function* of a condition X is the function

$$I[X] = \begin{cases} 1 & \text{if } X \text{ holds,} \\ 0 & \text{otherwise.} \end{cases}$$

Definition 7. *Let $S = (S_{ij})$ be an F-square of type $F(m\lambda; \lambda)$. For $a \in \{1, 2, \ldots, m\}$, the indicator square $I_a(S)$ of S with respect to a is the $\{0, 1\}$ array of size $m\lambda \times m\lambda$ whose (i, j) entry is $I[S_{ij} = a]$.*

Using Definition 7, an F-square S of type $F(m\lambda; \lambda)$ may be written as $\sum_{a=1}^{m} a I_a(S)$.

Example 8. *Let*

$$S = \begin{bmatrix} 1 & 2 & 3 & 1 & 2 & 3 \\ 3 & 1 & 2 & 3 & 2 & 1 \\ 2 & 3 & 1 & 2 & 1 & 3 \\ 1 & 1 & 2 & 3 & 3 & 2 \\ 3 & 3 & 1 & 2 & 1 & 2 \\ 2 & 2 & 3 & 1 & 3 & 1 \end{bmatrix}$$

be an F-square of type $F(6; 2)$. Then the indicator square of S with respect to 1, 2, 3 is

$$I_1(S) = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \quad I_2(S) = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$I_3(S) = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix},$$

respectively, and $S = I_1(S) + 2I_2(S) + 3I_3(S)$.

Let $A = (A_{ij})$ and $B = (B_{ij})$ be arrays of the same size. We write

$$A \circ B := \sum_{i,j} A_{ij} B_{ij}$$

for the sum of the entries of the elementwise product of A and B. With this notation, $A \circ J$ is the sum of the entries of A (where J is the all-ones

array whose size is given by context), and $A \circ A$ is the sum of squares of the entries of A. For an F-square S of type $F(m\lambda; \lambda)$, we have

$$I_a(S) \circ I_a(S) = I_a(S) \circ J = m\lambda^2 \quad \text{for each } a \in \{1, 2, \ldots, m\}, \qquad (1)$$

and F-squares S, S' of type $F(m\lambda; \lambda)$ are orthogonal if and only if

$$I_a(S) \circ I_b(S') = \lambda^2 \text{ for all } a, b \in \{1, 2, \ldots, m\}. \qquad (2)$$

3 Proof of Theorem 3 using indicator squares

The original proof of Theorem 3 by Hedayat, Raghavarao, and Seiden [8] uses an argument based on the matrix rank. Jungnickel, Mavron, and Mc-Donough [13, Theorem 3.5] give an alternative counting proof, making use of an equivalence between sets of MOFS and nets, and characterizing the case when equality holds (namely, that the set of MOFS is complete). In this section, we give a further elementary proof of Theorem 3 that provides a new structural constraint on the case when equality holds, using indicator squares. Our method is inspired by the proof of an upper bound for the number of rows of a difference matrix over a group given by van Greevenbroek and Jedwab [6, Theorem 2.1], which is in turn adapted from a more general result due to Jungnickel [12, Proposition 3.1].

Theorem 9. *Suppose $S_1, S_2, \ldots, S_t$ is a set of MOFS of type $F(m\lambda; \lambda)$. Relabel the F-squares if necessary so that $(S_k)_{11} = 1$ for each $k \in \{1, 2, \ldots, t\}$. Then $t \leq \frac{(m\lambda - 1)^2}{m-1}$, and equality holds if and only if*

$$\sum_k \sum_{a>1} I_a(S_k) = \begin{bmatrix} 0 & \lambda(m\lambda - 1) & \ldots & \lambda(m\lambda - 1) \\ \lambda(m\lambda - 1) & \lambda(m\lambda - 2) & \ldots & \lambda(m\lambda - 2) \\ \vdots & \vdots & \ddots & \vdots \\ \lambda(m\lambda - 1) & \lambda(m\lambda - 2) & \ldots & \lambda(m\lambda - 2) \end{bmatrix}.$$

Proof. Let $T = (T_{ij})$ be the $m\lambda \times m\lambda$ array given by

$$T = \sum_k \sum_{a>1} I_a(S_k).$$

We calculate the sum of the entries of T as

$$\sum_{i,j} T_{ij} = T \circ J$$

$$= \sum_k \sum_{a>1} I_a(S_k) \circ J$$

$$= t(m-1)m\lambda^2 \qquad (3)$$

5

from (1), and the sum of squares of the entries of T as

$$\sum_{i,j} T_{ij}^2 = T \circ T = \sum_{k,\ell} \sum_{a,b>1} I_a(S_k) \circ I_b(S_\ell)$$

$$= \sum_{k \neq \ell} \sum_{a,b>1} I_a(S_k) \circ I_b(S_\ell) + \sum_k \sum_{a,b>1} I_a(S_k) \circ I_b(S_k)$$

$$= t(t-1)(m-1)^2\lambda^2 + t(m-1)m\lambda^2$$

by (2) and (1), noting that $I_a(S_k) \circ I_b(S_k) = 0$ for all $a \neq b$. Therefore

$$\sum_{i,j} T_{ij}^2 = t(m-1)\lambda^2\big(t(m-1)+1\big). \tag{4}$$

Since $(S_k)_{11} = 1$ for each k, we have $T_{11} = 0$ and therefore

$$\sum_{i>1} T_{i1} = \sum_i T_{i1}$$

$$= \sum_k \sum_{a>1} \sum_i I_a(S_k)_{i1}$$

$$= t(m-1)\lambda \tag{5}$$

because S_k is an F-square, and similarly

$$\sum_{j>1} T_{1j} = t(m-1)\lambda. \tag{6}$$

Now define an $m\lambda \times m\lambda$ array $U = (U_{ij})$ by

$$U_{ij} = \begin{cases} T_{11} + \lambda(m\lambda - 2) & \text{for } (i,j) = (1,1), \\ T_{ij} - \lambda & \text{for } (i > 1, j = 1) \text{ and } (i = 1, j > 1), \\ T_{ij} & \text{for } i, j > 1. \end{cases}$$

We calculate the sum of the entries of U as

$$\sum_{i,j} U_{ij} = \sum_{i,j} T_{ij} + \lambda(m\lambda - 2) - 2\lambda(m\lambda - 1)$$

$$= m\lambda^2(t(m-1) - 1) \tag{7}$$

by substitution from (3), and the sum of squares of the entries of U as

$$\sum_{i,j} U_{ij}^2 = \Big(T_{11} + \lambda(m\lambda - 2)\Big)^2 + \sum_{i>1}(T_{i1} - \lambda)^2 + \sum_{j>1}(T_{1j} - \lambda)^2 + \sum_{i,j>1} T_{ij}^2$$

$$= \sum_{i,j} T_{ij}^2 - 2\lambda\Big(\sum_{i>1} T_{i1} + \sum_{j>1} T_{1j}\Big) + \lambda^2(m\lambda - 2)^2 + 2\lambda^2(m\lambda - 1)$$

$$= t(m-1)\lambda^2\big(t(m-1)+1\big) - 2\lambda \cdot 2t(m-1)\lambda +$$
$$\lambda^2(m^2\lambda^2 - 2m\lambda + 2)$$

6

by substitution from (4), (5), and (6). Therefore

$$\sum_{i,j} U_{ij}^2 = \lambda^2 \Big(t^2(m-1)^2 - 3t(m-1) + m^2\lambda^2 - 2m\lambda + 2 \Big).$$

Substitute this and (7) into the Cauchy-Schwarz inequality

$$\left(\sum_{i,j} U_{ij} \right)^2 \leq m^2 \lambda^2 \sum_{i,j} U_{ij}^2 \qquad (8)$$

and simplify to obtain $t \leq \frac{(m\lambda-1)^2}{m-1}$. Equality holds in (8) if and only if the U_{ij} are equal for all i, j, in which case from (7) and $t = \frac{(m\lambda-1)^2}{m-1}$ we obtain $U_{ij} = \lambda(m\lambda - 2)$ for all i, j. In that case, by definition of U we have

$$T = \begin{bmatrix} 0 & \lambda(m\lambda-1) & \dots & \lambda(m\lambda-1) \\ \lambda(m\lambda-1) & \lambda(m\lambda-2) & \dots & \lambda(m\lambda-2) \\ \vdots & \vdots & \ddots & \vdots \\ \lambda(m\lambda-1) & \lambda(m\lambda-2) & \dots & \lambda(m\lambda-2) \end{bmatrix}.$$

□

4   A maximality criterion using indicator squares

In this section, we address question (Q2) of Section 1: when is a set of MOFS of type $F(m\lambda; \lambda)$ maximal (not extendible to a larger set) but not complete? As m and λ grow, it quickly becomes computationally infeasible to determine the maximality of a particular set of MOFS by direct comparison with all other F-squares. For example, the number of F-squares of type $F(6; 3)$ is 297 200 whereas the number of F-squares of type $F(8; 4)$ is 116 963 796 250 [11]. Nonetheless, Britz et al. [3] showed how to adapt parity arguments from the study of maximal sets of MOLS in order to obtain a theoretical criterion for the maximality of a set of MOFS of type $F(2\lambda; \lambda)$ when λ is odd. They also derived necessary conditions on the MOFS parameters for the criterion to hold. In this section, we extend the analysis of [3] to the case of MOFS of type $F(m\lambda; \lambda)$ for all even m and odd λ, using indicator squares as introduced in Section 2 and streamlining the arguments.

We shall derive a maximality criterion in Theorem 13, depending on a sum of indicator squares having the regular block structure described in Definition 10. Write **0** for the all-zeroes array whose size is given by context, and as before write J for the all-ones array. For an array A, write A mod 2 for the elementwise reduction of A modulo 2.

Definition 10. *Let x, y be integers for which $0 \leq x, y \leq m\lambda$ and x, y do not both belong to $\{0, m\lambda\}$. A set $\{S_1, S_2, \ldots, S_t\}$ of F-squares of type $F(m\lambda; \lambda)$ satisfies a non-constant full relation with respect to x and y if, for some permutation of rows and columns, the array $\left(\sum_{k=1}^{t} I_1(S_k)\right) \bmod 2$ has block structure*

$$
\begin{array}{c c}
 & \begin{array}{cc} y \qquad\quad & m\lambda - y \end{array} \\
\begin{array}{c} x \\[2em] m\lambda - x \end{array} &
\left[\begin{array}{c|c} \mathbf{0} & J \\ \hline J & \mathbf{0} \end{array}\right]
\end{array}.
\tag{9}
$$

We present two preparatory results about a non-constant full relation in Lemmas 11 and 12.

Lemma 11. *Suppose that $\{S_1, S_2, \ldots, S_t\}$ is a set of F-squares of type $F(m\lambda; \lambda)$ satisfying a non-constant full relation with respect to x and y. Then*

(i) $x \equiv y \equiv t\lambda \pmod{2}$,

(ii) $m\lambda \equiv 0 \pmod{2}$.

Proof. Let $V = (V_{ij}) = \sum_k I_1(S_k)$. For each row i of V, we have

$$
\sum_j V_{ij} = \sum_k \sum_j I_1(S_k)_{ij} = \sum_k \lambda
$$

because S_k is an F-square of type $F(m\lambda; \lambda)$. Reduce modulo 2 to give

$$
\sum_j (V \bmod 2)_{ij} \equiv t\lambda \pmod{2} \quad \text{for each } i.
\tag{10}
$$

Similarly,

$$
\sum_i (V \bmod 2)_{ij} \equiv t\lambda \pmod{2} \quad \text{for each } j.
\tag{11}
$$

By symmetry, we may assume that $0 < x < m\lambda$. With reference to (9), take $i = x + 1$ in (10) to show that

$$
y \equiv t\lambda \pmod{2},
\tag{12}
$$

and take $i = 1$ in (10) to show

$$
m\lambda - y \equiv t\lambda \pmod{2}.
$$

8

Combining with (12) establishes (ii).

Next take $j = 1$ in (11). In the case $y = 0$, we obtain

$$x \equiv t\lambda \pmod{2},$$

which with (12) establishes (i). Otherwise $y > 0$, and then

$$m\lambda - x \equiv t\lambda \pmod{2},$$

which with (ii) and (12) establishes (i). $\qquad\square$

The condition in Definition 10 that x, y do not both belong to $\{0, m\lambda\}$ ensures that the array $\left(\sum_{k=1}^{t} I_1(S_k)\right) \bmod 2$ does not equal the constant array $\mathbf{0}$ or J. Without this condition, both conclusions (i) and (ii) of Lemma 11 can fail, for example for the three F-squares of type $F(3; 1)$ given by

$$S_1 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}, \quad S_2 = \begin{bmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}, \quad S_3 = \begin{bmatrix} 3 & 1 & 2 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{bmatrix},$$

which satisfy

$$I_1(S_1) + I_1(S_2) + I_1(S_3) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

and so fulfil all conditions of Definition 10 with $(x, y) = (3, 0)$ except that $x, y \in \{0, 3\}$.

Lemma 12. *Let λ be odd, and suppose that $\{S_1, S_2, \ldots, S_t\}$ is a set of MOFS of type $F(m\lambda; \lambda)$ satisfying a non-constant full relation. Then t is odd.*

Proof. Let the relation be with respect to x and y, and let $V = \sum_k I_1(S_k)$. Using (2), the orthogonality of S_1 with each S_k for $k > 1$ gives

$$(t - 1)\lambda^2 = \sum_{k>1} I_1(S_k) \circ I_1(S_1)$$
$$= \sum_{k} I_1(S_k) \circ I_1(S_1) - I_1(S_1) \circ I_1(S_1)$$
$$= V \circ I_1(S_1) - m\lambda^2$$

by (1). By Lemma 11 (ii) and the assumption that λ is odd, reduction modulo 2 gives

$$t - 1 \equiv (V \bmod 2) \circ I_1(S_1) \pmod{2}. \tag{13}$$

Since S_1 is an F-square of type $F(m\lambda; \lambda)$, the sum of the entries of the blocks of $I_1(S_1)$ corresponding to the blocks of $V \bmod 2$ shown in (9) is

$$
\begin{array}{c}
\quad\; y \qquad\qquad\quad m\lambda - y \\
\begin{array}{cc}
x \\
\\
m\lambda - x
\end{array}
\left[
\begin{array}{c|c}
\alpha & x\lambda - \alpha \\
\hline
y\lambda - \alpha & m\lambda^2 - (x + y)\lambda + \alpha
\end{array}
\right]
\end{array}
\tag{14}
$$

for some non-negative integer α. Therefore from (13) we obtain

$$
\begin{aligned}
t - 1 &\equiv (x\lambda - \alpha) + (y\lambda - \alpha) \\
&\equiv 0 \pmod{2}
\end{aligned}
$$

by Lemma 11 (i), so t is odd. $\qquad\square$

We now use Lemmas 11 and 12 to prove the desired maximality criterion.

Theorem 13. *Let λ be odd, and suppose that $\{S_1, S_2, \ldots, S_t\}$ is a set of MOFS of type $F(m\lambda; \lambda)$ satisfying a non-constant full relation. Then $\{S_1, S_2, \ldots, S_t\}$ is a maximal set of MOFS.*

Proof. Let the relation be with respect to x and y, and let $V = \sum_k I_1(S_k)$. Suppose, for a contradiction, that S is an F-square of type $F(m\lambda; \lambda)$ that is orthogonal to each S_k. Then by (2),

$$
t\lambda^2 = \sum_k I_1(S_k) \circ I_1(S) = V \circ I_1(S).
$$

By Lemma 12 and the assumption that λ is odd, reduction modulo 2 gives

$$
1 \equiv (V \bmod 2) \circ I_1(S) \pmod{2}. \tag{15}
$$

Since S is an F-square of type $F(m\lambda; \lambda)$, the sum of the entries of the blocks of $I_1(S)$ corresponding to the blocks of $V \bmod 2$ shown in (9) is as shown in (14) for some non-negative integer α. Therefore from (15),

$$
1 \equiv (x\lambda - \alpha) + (y\lambda - \alpha) \equiv 0 \pmod{2}
$$

by Lemma 11 (i), which is a contradiction. $\qquad\square$

The criterion of Theorem 13 for a set of MOFS of type $F(m\lambda; \lambda)$ to be maximal requires the set to satisfy a non-constant full relation, and we know from Lemma 11 (ii) that this requires m to be even. We now derive a more restrictive necessary condition for this criterion to hold.

Proposition 14. *Let λ be odd, and suppose that $\{S_1, S_2, \ldots, S_t\}$ is a set MOFS of type $F(m\lambda; \lambda)$ satisfying a non-constant full relation with respect to x and y. Then $t \equiv m(x + y) - (m + 1) \pmod 8$.*

Proof. Let $V = \sum_k I_1(S_k)$, and let x_r be the number of occurrences of r in the array V. We shall calculate expressions for the four quantities $\sum_r r x_r$ and $\sum_r r^2 x_r$ and $\sum_{r \text{ odd}} x_r$ and $\sum_{r \text{ odd}} r x_r$, and substitute them into the congruence

$$\sum_r (2r - r^2) x_r \equiv \sum_{r \text{ odd}} r(2 - r) x_r \pmod 8$$

$$\equiv \sum_{r \text{ odd}} (2r - 1) x_r \pmod 8. \tag{16}$$

We have

$$\sum_{r=0}^{t} r x_r = V \circ J$$

$$= \sum_k I_1(S_k) \circ J$$

$$= t m \lambda^2$$

by (1), and

$$\sum_{r=0}^{t} r^2 x_r = V \circ V$$

$$= \sum_{k,\ell} I_1(S_k) \circ I_1(S_\ell)$$

$$= \sum_{k \neq \ell} I_1(S_k) \circ I_1(S_\ell) + \sum_k I_1(S_k) \circ I_1(S_k)$$

$$= t(t - 1)\lambda^2 + t m \lambda^2$$

by (2) and (1).

The expression $\sum_{r \text{ odd}} x_r$ is the sum of the entries of V mod 2, so with reference to the block structure of (9) we have

$$\sum_{r \text{ odd}} x_r = x(m\lambda - y) + y(m\lambda - x).$$

Since each S_k is an F-square of type $F(m\lambda; \lambda)$, the sum of the entries

11

of $V = \sum_{k=1}^{t} I_1(S_k)$ has the block structure

$$
\begin{array}{c}
 \\
x \\
\\
m\lambda - x
\end{array}
\begin{array}{c}
y \qquad\qquad m\lambda - y \\
\left[
\begin{array}{c|c}
\beta & tx\lambda - \beta \\
\hline
ty\lambda - \beta & tm\lambda^2 - t(x+y)\lambda + \beta
\end{array}
\right]
\end{array}
\tag{17}
$$

for some non-negative integer β. The expression $\sum_{r \text{ odd}} r x_r$ is the sum of the odd entries of V, so

$$
\sum_{r \text{ odd}} r x_r = V \circ (V \bmod 2)
$$
$$
= (tx\lambda - \beta) + (ty\lambda - \beta)
$$

from (17) and (9).

Substitute the four calculated quantities into (16) to give

$$
t\lambda^2(m + 1 - t) \equiv 2t(x + y)\lambda - 4\beta - m(x + y)\lambda + 2xy \quad (\bmod\ 8). \tag{18}
$$

By comparison of (17) with (9), we see that β is even. Also λ is odd by assumption, and m is even and x, y, t are odd by Lemmas 11 and 12. Note that for integers a and b with $a \equiv 0 \pmod 4$ and b odd,

$$
ab \equiv a \equiv -a \quad (\bmod\ 8). \tag{19}
$$

Therefore (18) simplifies to

$$
t(m + 1) - 1 \equiv m(x + y) + 2(x + y + xy) \quad (\bmod\ 8).
$$

Since x and y are odd we have $2(x + y + xy) = 2(x + 1)(y + 1) - 2 \equiv -2$ (mod 8), so that

$$
t(m + 1) \equiv m(x + y) - 1 \quad (\bmod\ 8).
$$

Multiply by the odd integer $m + 1$ and use (19) to give

$$
t \equiv m(x + y) - (m + 1) \quad (\bmod\ 8).
$$

$\square$

Corollary 15. *Let λ be odd, and suppose that $\{S_1, S_2, \ldots, S_t\}$ is a set of MOFS of type $F(m\lambda; \lambda)$ satisfying a non-constant full relation. Then $t \equiv m - 1 \pmod 4$.*

Proof. Let the relation be with respect to x and y. By Lemma 11 we have that $x + y$ and m are even. Reduce modulo 4 the conclusion of Proposition 14. ∎

By taking the special case $m = 2$ of Theorem 13, Proposition 14, Corollary 15 (and noting that in this case the condition in Definition 10 that x, y do not both belong to $\{0, m\lambda\}$ can be removed), we recover Theorems 4, 6, 5 of [3], respectively. These theorems were obtained in [3] by regarding a set of MOFS of type $F(2\lambda; \lambda)$ as an orthogonal array and using counting arguments. The analysis presented here, using indicator squares, streamlines the arguments of [3] and allows us to deal with all even $m > 2$.

Acknowledgements

References

[1] R.J.R Abel, C.J. Colbourn, and J.H. Dinitz. Mutually orthogonal Latin squares (MOLS). In C.J. Colbourn and J.H. Dinitz, editors, *Handbook of Combinatorial Designs*, chapter III.3, pages 160–192. Chapman & Hall/CRC, Bocan Raton, 2nd edition, 2007.

[2] I. Anderson, C.J. Colbourn, J.H. Dinitz, and T.S. Griggs. Design theory: Antiquity to 1950. In C.J. Colbourn and J.H. Dinitz, editors, *Handbook of Combinatorial Designs*, chapter I.2, pages 11–22. Chapman & Hall/CRC, Bocan Raton, 2nd edition, 2007.

[3] T. Britz, N.J. Cavenagh, A. Mammoliti, and I.M. Wanless. Mutually orthogonal binary frequency squares. *Electron. J. Combin.*, 27(#P3.7), 2020. 26 pages.

[4] W.T. Federer. On the existence and construction of a complete set of orthogonal $F(4t; 2t, 2t)$-squares design. *Ann. Statist.*, 5:561–564, 1977.

[5] D.J. Finney. Some orthogonal properties of the 4×4 and 6×6 Latin squares. *Ann. Eugen.*, 12:213–219, 1943.

[6] K. van Greevenbroek and J. Jedwab. A new structure for difference matrices over abelian p-groups. In K.-U. Schmidt and A. Winterhof,

editors, *Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications*, Radon Series on Computational and Applied Mathematics 23, pages 79–108. de Gruyter, 2019.

[7] A. Hedayat. *On the theory of the existence, non-existence, and the construction of mutually orthogonal F-squares and latin squares.* PhD thesis, Cornell Univ., 1969.

[8] A. Hedayat, D. Raghavarao, and E. Seiden. Further contributions to the theory of F-squares design. *Ann. Statist.*, 3:712–716, 1975.

[9] A. Hedayat and E. Seiden. F-square and orthogonal F-squares design: a generalization of Latin square and orthogonal Latin squares design. *Ann. Math. Statist.*, 41:2035–2044, 1970.

[10] K.J. Horadam. *Hadamard matrices and their applications.* Princeton University Press, Princeton and Oxford, 2006.

[11] OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences. Available at `http://oeis.org/A058527`, 2020.

[12] D. Jungnickel. On difference matrices, resolvable transversal designs and generalized Hadamard matrices. *Math. Z.*, 167:49–60, 1979.

[13] D. Jungnickel, V.C. Mavron, and T.P. McDonough. The geometry of frequency squares. *J. Combin. Theory Ser. A*, 96:376–387, 2001.

[14] C.F. Laywine and G.L. Mullen. Frequency squares and hypercubes. In C.J. Colbourn and J.H. Dinitz, editors, *Handbook of Combinatorial Designs*, chapter VI.22, pages 465–471. Chapman & Hall/CRC, Bocan Raton, 2nd edition, 2007.

[15] P.A. MacMahon. A new method in combinatory analysis, with application to Latin squares and associated questions. *Trans. Cambridge Phil. Soc.*, 16:262–290, 1898.

[16] V.C. Mavron. Frequency squares and affine designs. *Electron. J. Combin.*, 7(#R56), 2000. 6 pages.

[17] G.L. Mullen. Polynomial representation of complete sets of mutually orthogonal frequency squares of prime power order. *Discrete Math.*, 69:79–84, 1988.