

On the spectrum of an F-square

L. F. Fitina and Jennifer Seberry

Centre for Computer Security Research
School of Information Technology and Computer Science
University of Wollongong
NSW 2522 Australia

Abstract

Given an F-square of some type $F(n; \alpha_0, \alpha_1, \dots, \alpha_{v-1})$, what critical set sizes can we obtain for this type? Such a question was considered by Donovan and Howse (1999), in the case of latin squares. In this note we solve this question for the type $F(n; 1, n-1)$, and also obtain partial results for type $F(n; 2, n-2)$.

1 Introduction

Let $n = \alpha_0 + \alpha_1 + \dots + \alpha_{v-1}$, where α_i is a natural number for each i . A *frequency square* or *F-square* of type $F = F(n; \alpha_0, \alpha_1, \dots, \alpha_{v-1})$ and of order n is an $n \times n$ array with entries chosen from the set $N = \{0, 1, \dots, v-1\}$, such that each element i occurs α_i times in each row and in each column. An F-square F can also be thought of as the set of ordered triples $F = \{(i, j; k)\}$ where element k occurs in position (i, j) . The set $\{0, 1, \dots, v-1\}$ is called the *underlying set* of F . A subset of F will also be called a *sub square* or *partial F-square*. A subset S of $F = F(n; \alpha_0, \alpha_1, \dots, \alpha_{v-1})$ is a *critical set* (of F) if

1. F is the only F-square of order n which has element k in position (i, j) for each $(i, j; k) \in S$. (We then say that F is *uniquely completable from S* , and that S is *uniquely completable to F*)

and

2. (a) every proper subset of S is contained in at least two F-squares of type $F(n; \alpha_0, \alpha_1, \dots, \alpha_{v-1})$
or
(b) for every $(i, j; k) \in S, \ell \in N, \ell \neq k \rightarrow$ there does not exist any F-square of type $F(n; \alpha_0, \alpha_1, \dots, \alpha_{v-1})$ which contains $(S \setminus \{(i, j; k)\}) \cup \{(i, j; \ell)\}$.

We say that a critical set has the same order as the original F -square.

A *latin square of order n* is an F -square of type $F(n; 1, 1, \dots, 1)$.

The *spectrum of type $F(n; \alpha_0, \alpha_1, \dots, \alpha_{v-1})$* , is denoted by $Sp(n; \alpha_0, \alpha_1, \dots, \alpha_{v-1})$ and defined as follows:

An integer s belongs to $Sp(n; \alpha_0, \alpha_1, \dots, \alpha_{v-1})$ if there is an F -square of type $F(n; \alpha_0, \alpha_1, \dots, \alpha_{v-1})$ which has a critical set of size s .

A collection \mathcal{K} of partial latin squares I is called a *latin collection* if the entries in the cells of each row (and column) of each $I \in \mathcal{K}$ are the same as those in the corresponding row (and column) of every other partial square in \mathcal{K} , and if the intersection of all the partial latin squares, regarded as sets of triples, is empty. A *latin interchange pair* is a latin collection of size 2. Elements of a latin interchange pair are called latin interchanges, and each is called the disjoint mate of the other.

Donovan and Howse [3] have studied the spectrum of type $F(n; 1, 1, \dots, 1)$.

2 Some Preliminary Results

The following is an adaptation of a result in Donovan and Howse[3]:

Lemma 1 *Let F be any F -square, and let \mathcal{C} be any latin collection in F . Let K be a critical set of F . If $I \in \mathcal{C}$ is such that $K \cup I$ has a unique completion to F , then $(K \setminus I) \cup I'$ has a unique completion to $(F \setminus I) \cup I'$, for every $I' \in \mathcal{C}, I' \neq I$.*

Proof. Let I' be any other set in \mathcal{C} . Every row/column in I' must contain the same elements as the corresponding row/column in I . Hence every unfilled cell outside of the set $(K \setminus I) \cup I'$ must be filled in precisely the same way, if $(K \setminus I) \cup I'$ was replaced by $K \cup I$. \square

The proofs of the following two lemmas are straightforward.

Lemma 2 *Let $F = F(n; \alpha_0, \alpha_1, \dots, \alpha_{n-1})$, with underlying multiset M and let $S \subseteq F$ be a partial F -square in F . Then an unfilled cell (i, j) in S can be uniquely filled if $M \setminus (R_i \cup C_j) \subseteq \{a, a, \dots, a\}$ for some $a \in \{0, 1, \dots, n-1\}$. \square*

Two F -squares of the same type are *isotopic* if one can be obtained from the other by permuting rows and columns or renaming elements.

Lemma 3 *Any two F -squares of type $F(n; 1, n-1)$ are isotopic. \square*

3 Spectrum of type $F(n; 1, n - 1)$

In this section we will consider only the spectrum of type $F(n; 1, n - 1)$.

Theorem 1 For any $n \geq 3$,

$$\{1, 2, \dots, n - 2\} \cap Sp(n; 1, n - 1) = \emptyset.$$

That is, none of $1, 2, \dots, n - 2$ belongs to the spectrum of type $F(n; 1, n - 1)$.

Proof. Let F be an F-square of type $F(n; 1, n - 1)$ and having the underlying multiset $M = \{0, 1, 1, \dots, 1\}$. By Theorem 2 of [4] there cannot exist a critical set of F of size less than or equal to $n - 2$. \square

Theorem 2 There exists a critical set in an F-square of type $F(n; 1, n - 1)$ with size

$$s + \frac{(n - s)(n - s - 1)}{2}$$

for each $s = 0, 1, 2, \dots, n - 1$.

Proof. Let $A(n, s)$ be the set

$$A(n, s) = \{(i, j; 1) : i = 0, 1, \dots, n - 1 - s; j = s + i + 1, \dots, n - 1\}$$

for $s = 0, 1, \dots, n - 2$ and $A(n, n - 1) = \emptyset$.

Let $B(n, s)$ be the set

$$B(n, s) = \{(p, q; 0) : p = n - s, \dots, n - 1; q = n - p - 1\}$$

for $s = 1, 2, \dots, n - 1$ and $B(n, 0) = \emptyset$.

Let

$$D(n, s) = A(n, s) + B(n, s).$$

We illustrate this set with the following example: here $n = 8$ and $s = 4$. The F-square of type $F(8; 1, 7)$ is on the right, and $D(8, 4)$ is on the left.

					1	1	1
						1	1
							1
			0				
		0					
	0						
0							

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

Each of the rows $n - s, n - s + 1, \dots, n - 1$ in $D(n, s)$ has a 0 in it, so each empty cell in each of these rows must be filled with the element 1. Column $n - 1$ now has the element 1 occurring in every cell, except cell $(n - s - 1, n - 1)$. Fill this cell with element 0. Now each of the empty cells in row $n - s - 1$ can be filled with element 1. Column $n - 2$ now has every cell filled with element 1, except cell $(n - s - 2, n - 2)$. Fill this cell with element 0, etc. Following this procedure, eventually the empty cells in $D(n, s)$ will be filled uniquely with either the element 1 or 0. Each row and column will have 0 occurring once and 1 occurring $n - 1$ times. Thus $D(n, s)$ completes uniquely to F .

We need now to show that each triple in $D(n, s)$ has a latin interchange associated with it. For each of the triples $(n - 1, 0; 0), \dots, (n - s, s - 1; 0)$ the latin interchange associated with a triple $(i, j; 0)$ is of the form:

$$I_{(i,j;0)}$$

	j	s
0	1	0
i	0	1

where the leftmost column gives the first coordinates of the triples, and the top row gives the second coordinates. Thus this diagram refers to the set $\{(0, j; 1), (0, s; 0), (i, j; 0), (i, s; 1)\}$.

It can be easily verified that each of these latin interchanges intersects $D(n, s)$ at $(i, j; 0)$.

For each of the triples $(i, j; 1) : i = 0, 1, \dots, n - s - 2; j = s + 1 + i, \dots, n - 1$, the latin interchange associated with each triple $(i, j; 1)$ is of the form:

$$I_{(i,j;1)}$$

	s+i	j
i	0	1
j-s	1	0

It is easy to verify that each such latin interchange intersects $D(n, s)$ at the given triple. Thus $D(n, s)$ is a critical set of F . □

Corollary 1 *Each of the numbers in the set $SP_1 = \{n - 1, n, n + 2, n + 5, \dots, \frac{1}{2}(n - 1)n\}$ belongs to the spectrum of $F(n; 1, n - 1)$.* □

Theorem 3 $n + 1$ does not belong to the spectrum of $F(n; 1, n - 1)$.

Proof. Let E be a subset of F of size $n + 1$. If E contains $n - 1$ or n triples of the form $(i, k; 0)$ then E must contain a critical set of size $n - 1$ (see Theorem 2). Thus E cannot be a critical set.

Suppose that E contains $n - 2$ triples of the form $(i, j; 0)$. Consider E now as a partial F-square. It has precisely one 0 each in $n - 2$ rows, and three cells filled with the entry 1. If at least one of these 1's does not fall in any of the rows that contain the 0's, then by Theorem 2 above, E will contain a critical set, and hence cannot be a critical set itself. Otherwise each of the 1's falls into a row that already contains a 0. In this case, having filled all the rows containing 0's, there will be four cells that cannot be uniquely filled. Each of these cells can be filled with either 0 or 1. In any case, E is not uniquely completable, and thus is not a critical set.

Suppose E contains $n - 3$ triples of the form $(i, j; 0)$, then it has four triples in the form $(i, j; 1)$. Each of the empty cells in the rows that contains a 0 can be filled with element 1. There are now six cells that are either still empty, or that contain element 1, from the original subsquare E . One can permute the rows and columns so that these cells appear on the upper right hand corner of the partial F-square. One now needs to consider how to fill a 3×3 square with four 1's, into an F-square of type $F(3; 1, 2)$. But this can be done only if the partial F-square contains the following configuration (up to isotopy):

	1	1
		1

But then E , by Theorem 2 above, must contain a critical set, and is not itself a critical set. This is sufficient to show that no other configuration of elements of E will give a critical set.

An argument similar to that described above shows that if E contains $n - s$ 0's, $s \geq 4$ then E cannot be a critical set.

Thus there cannot exist a critical set of size $n + 1$, and $n + 1$ does not belong to the spectrum of $F(n; 1, n - 1)$. □

We rewrite one of the implications in the above proof, so as to help with proofs of the next theorems.

Lemma 4 *Let F be an F-square of type $F(n; 1, n - 1)$, $n \geq 3$. Then a subsquare H of F consisting of just 1's in every cell in H , is a critical set of F only if $|H| = \frac{1}{2}(n - 1)n$, and the elements of H are arranged in the following configuration:*

For each i , $0 \leq i \leq n - 1$, there exists exactly one row that contains i 1's, and for each j , $0 \leq j \leq n - 1$, there exists exactly one column that contains j 1's. □

Proof. We present below an example of such a 7×7 partial F-square and an isotope:

1	1	1	1	1	1	1
1	1	1	1	1		
1	1	1	1			
1	1	1				
1	1					
1						

1	1	1	1	1	1	1
1	1	1	1	1		
1	1		1	1		
1	1		1			
1	1					
1						

It is easy to show that with the above configuration H is a critical set. Suppose that H does not have the above configuration, that is, there exist at least two rows or two columns with the same number of 1's.

We assume the rows are arranged in decreasing size: that is, the rows with the most numbers of 1's at the top, etc. Suppose also that the columns are arranged in decreasing size; that is with the columns containing the most number of 1's to the left, etc.

Suppose that row 0 and row 1 have the same size. Row 0 is uniquely completable if it contains $n - 1$ 1's. Suppose that cell $(0, n - 1)$ is the only empty cell in row 0. Then this cell can be uniquely filled with element 0. If the empty cell in row 1 is also in column $n - 1$ then we get a contradiction. Suppose the empty cell in row 1 is not in column $n - 1$. Then cell $(1, n - 1)$ must contain a 1. But since element 0 must be forced into cell $(0, n - 1)$, this forces the element 1 into every other cell in column $n - 1$. Thus the 1 in cell $(1, n - 1)$ is redundant. That is, H is not the smallest uniquely completable set contained in itself, and so cannot be a critical set. Similarly, no other two rows can have the same size in H . Arguing similarly, no two columns can have the same size in H .

Thus H is a critical set only if it has the above configuration. □

By modifying the proof of the above theorem and using the above lemma, we have the following result:

Theorem 4 *No number outside of $\{(n - s) + \frac{1}{2}(s - 1)s : s = 2, 3, \dots, n\}$ belongs to the spectrum of $F(n; 1, n - 1)$.* □

Thus we have:

Theorem 5 *The spectrum of $F(n; 1; n)$ is precisely the set*

$$Sp(n; 1, n - 1) = \{(n - s) + \frac{1}{2}(s - 1)s : s = 2, 3, \dots, n\}.$$

□

4 Spectrum of type $F(n; 2, n - 2)$

4.1 Case $n = 2k + 1$ (Or n is odd)

For $i = 0, 2, \dots, 2(k - 1)$, form the subsquares

$$\begin{aligned} S_i &= \{(i, i; 0), (i, i + 1; 0), (i + 1, i; 0), (i + 1, i + 1; 0)\} \\ S'_i &= \{(i, i; 0), (i, i + 1; 0), (i + 1, i; 0)\} \\ S''_i &= \{(i, i; 0)\}. \end{aligned}$$

Form the subsquares

$$T_r = \{(i, j; 1) | i = r, r + 1, \dots, n - 1; j = n - i + r - 1, n - i + r, \dots, n - 1\},$$

for $r = 2, 3, 4, \dots, n - 1$ and $T_n = \emptyset$.

For $r = 0, 1, \dots, (k - 1)$, let

$$U''_{2r} = \bigcup_{p=0}^{r-1} S_{2p} \cup S''_{2r} \cup T_{2r+2}$$

and

$$U'_{2r} = \bigcup_{p=0}^{r-1} S_{2p} \cup S'_{2r} \cup T_{2r+3}.$$

Example 1 Let $n = 9$. Then $U''_0 = S''_0 \cup T_2$, $U'_0 = S'_0 \cup T_3$, and $U''_4 = S_0 \cup S_2 \cup S''_4 \cup T_6$, and $U'_4 = S_0 \cup S_2 \cup S'_4 \cup T_7$.

We display these subsquares below:

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

U''_0

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

U'_0

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

U''_4

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

U'_4

□

The proof of the following theorem is similar to the proofs of similar theorems in the previous section.

Theorem 6 The sets U''_{2r} and U'_{2r} defined above are critical sets of type $F(n; 2, n-2)$.

□

It is easy to verify that:

Theorem 7

$$|U''_{2r}| = 4r + 1 + \frac{1}{2}(n - 2r - 2)(n - 2r - 1)$$

and

$$|U'_{2r}| = 4r + 3 + \frac{1}{2}(n - 2r - 3)(n - 2r - 2).$$

□

Thus we have:

Theorem 8 Let $n = 2k + 1$. Then the spectrum of $F(n; 2, n - 2)$ contains each of the following numbers:

$$4k - 1 + \frac{1}{2}(n - 2k - 1)(n - 2k), \quad 4k - 3 + \frac{1}{2}(n - 2k)(n - 2k + 1), \quad \dots, \quad 7 + \frac{1}{2}(n - 5)(n - 4), \quad 5 + \frac{1}{2}(n - 4)(n - 3), \quad 3 + \frac{1}{2}(n - 3)(n - 2), \quad 1 + \frac{1}{2}(n - 2)(n - 1),$$

or

$$i + \frac{1}{2}(n - \frac{1}{2}i - \frac{3}{2})(n - \frac{1}{2}i - \frac{1}{2}), \quad i = 1, 3, 5, \dots, 4k - 1.$$

□

Example 2 Let $n = 9$. Then $k = 4$ and $\{14, 15, 17, 20, 24, 29\} \subseteq Sp(9; 2, 7)$.

□

4.2 Case $n = 2k$ (Or n is even)

For $i = 0, 2, \dots, 2(k - 2)$, form the subsquares

$$S_i = \{(i, i; 0), (i, i + 1; 0), (i + 1, i; 0), (i + 1, i + 1; 0)\},$$

the subsquares

$$S'_i = \{(i, i; 0), (i, i + 1; 0), (i + 1, i; 0)\}$$

and the subsquares

$$S''_i = \{(i, i; 0)\}.$$

Form the subsquare

$$T_r = \{(i, j; 1) \mid i = r, r + 1, \dots, n - 1; j = n - i + r - 1, n - i + r, \dots, n - 1\},$$

for $r = 2, 3, 4, \dots, n - 1$ and $T_n = \emptyset$.

For $r = 0, 1, \dots, (k - 2)$, let

$$U''_{2r} = \bigcup_{p=0}^{r-1} S_{2p} \cup S''_{2r} \cup T_{2r+2},$$

$$U'_{2r} = \bigcup_{p=0}^{r-1} S_{2p} \cup S'_{2r} \cup T_{2r+3}.$$

For $r = k - 2$, let

$$U_{2(k-2)} = \bigcup_{p=0}^{k-2} S_{2p}.$$

We state the following theorem without proof, as it is similar to theorems in the last two sections.

Theorem 9 *The sets U'_{2r}, U''_{2r} and $U_{2(k-2)}$ are critical sets of type $F(n; 2, n - 2)$, where n is an even number. \square*

Theorem 10 *If n is even then the spectrum of $F(n; 2, n - 2)$ contains the numbers $|U''_{2r}|, |U'_{2r}|, |U_{2(k-2)}|, r = 0, 1, \dots, (k - 2)$. \square*

Example 3 If $n = 10$ then $\{20, 21, 23, 26, 30, 41, 48, 56\} \subset Sp(10; 2, 8)$. \square

5 Conclusion

In this paper we have solved the spectrum of type $F(n; 1, n - 1)$ and also obtained partial solutions to the spectrums of $F(n; 2, n - 2)$ for n even and n odd. It is quite possible that we have in fact obtained all the spectrums of type $F(n; 2, n - 2)$ for n odd.

References

- [1] D. Curran and G.H.J. Van Rees, *Critical sets in latin squares*, Congr. Num., 22 (1979), 165–168.
- [2] D. Donovan and Joan Cooper, *Critical sets in back circulant latin squares*, Aequationes Mathematicae, 52 (1996), 157–179.
- [3] Diane Donovan and Adelle Howse, *Towards the spectrum of critical sets*, Australas. J. Combin., 21 (2000), 107–130.
- [4] L.F. Fitina, Jennifer Seberry and Dinesh Sarvate, *On F -squares and their critical sets*, Australas. J. Combin., 19 (1999), 209–230.

(Received 26/7/99; revised 9/6/2000)

