The maximum, supremum and spectrum for critical set sizes in $(0,1)$-matrices

Nicholas J. Cavenagh and Liam K. Wright,
Department of Mathematics,
The University of Waikato,
Private Bag 3105,
Hamilton 3240, New Zealand
nickc@waikato.ac.nz
liam.wright479@live.com

Abstract

If D is a partially filled-in $(0,1)$-matrix with a unique completion to a $(0,1)$-matrix M (with prescribed row and column sums), we say that D is a *defining set* for M. A *critical set* is a minimal defining set (the deletion of any entry results in more than one completion). We give a new classification of critical sets in $(0,1)$-matrices and apply this theory to Λ_{2m}^m, the set of $(0,1)$-matrices of dimensions $2m \times 2m$ with uniform row and column sum m.

The smallest possible size for a defining set of a matrix in Λ_{2m}^m is m^2 [3], and the infimum (the largest smallest defining set size for members of Λ_{2m}^m) is known asymptotically [4]. We show that no critical set of size larger than $3m^2-2m$ exists in an element of Λ_{2m}^m and that there exists a critical set of size k in an element of Λ_{2m}^m for each k such that $m^2 \leqslant k \leqslant 3m^2-4m+2$. We also bound the supremum (the smallest largest critical set size for members of Λ_{2m}^m) between $\lceil (3m^2-2m+1)/2 \rceil$ and $2m^2-m$.

Keywords: $(0,1)$-matrix, critical set, defining set, frequency square, F-square.

1 Introduction

Where convenient, we keep notation consistent with [2].

Let $R = (r_1, r_2, \ldots, r_m)$ and $S = (s_1, s_2, \ldots, s_n)$ be vectors of non-negative integers such that $\sum_{i=1}^{m} r_i = \sum_{j=1}^{n} s_j$. Then $\mathcal{A}(R, S)$ is defined to be the set of all $m \times n$ $(0,1)$-matrices with r_i 1's in row i and s_j 1's in column j, where $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$. If $M \in \mathcal{A}(R, S)$, we refer to R and S as the row sum and column sum vectors for M, respectively.

With R and S as above, we next define $\mathcal{A}'(R, S)$ to be the set of all $m \times n$ $(0, 1, \star)$-matrices with:

1. at most r_i 1's in row i,
2. at most $n - r_i$ 0's in row i,
3. at most s_j 1's in column j,
4. at most $m - s_j$ 0's in column j.

We call a matrix $M \in \mathcal{A}'(R, S)$ a *partial* $(0,1)$-matrix with row sum vector R and column sum vector S. If $M_{ij} = \star$ we say that position (i, j) is *empty*. Indeed, $\mathcal{A}(R, S) \subseteq \mathcal{A}'(R, S)$ and a partial $(0,1)$-matrix is a $(0,1)$-matrix if and only if it none of its positions are empty (equal to $\star$). (Note that our definition of a partial $(0,1)$-matrix allows for the possibility of a matrix $M \in \mathcal{A}'(R, S)$ which has *no* completion to a a $(0,1)$-matrix in $\mathcal{A}(R, S)$.)

We sometimes consider a partial $(0,1)$-matrix M as a set of triples

$$M = \{(i, j, M_{ij}) \mid 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n, M_{ij} \in \{0, 1\}\}.$$

Note that we naturally omit here the empty positions of M. It is usually clear by context whether we are considering a partial $(0,1)$-matrix as a matrix or as a set of ordered triples. For example, if we say that $M_1 \subseteq M_2$ for two partial $(0,1)$-matrices M_1 and M_2, we are considering M_1 and M_2 as sets. Similarly, the *size* of a partial $(0,1)$-matrix M refers to $|M|$ where M is a set (i.e. the number of 0's and 1's).

With this is mind, suppose that $M \in \mathcal{A}(R, S)$ and $D \in \mathcal{A}'(R, S)$. We say that D is a *defining set* for M if M is the unique member of $\mathcal{A}(R, S)$ such that $D \subseteq M$. We say that D is a *critical set* for M if it is minimal with respect to this property. That is, D is a critical set for M if it is a defining set for M and if $D' \subset D$, then D' is not a defining set for D.

This is analogous to the usual definition of defining sets and critical sets of Latin squares and other combinatorial designs ([5, 8]).

Given a $(0,1)$-matrix M, the size of the smallest (respectively, largest) critical set in M is denoted by $\mathrm{scs}(M)$ (respectively, $\mathrm{lcs}(M)$). For given row column sum vectors R and S, $\mathrm{scs}(\mathcal{A}(R,S))$ (respectively, $\mathrm{lcs}(\mathcal{A}(R,S))$) is the size of the smallest (respectively, largest) critical set for all members of the set $\mathcal{A}(R,S)$. More precisely,

$$\mathrm{scs}(\mathcal{A}(R,S)) = \min\{\mathrm{scs}(M) \mid M \in \mathcal{A}(R,S)\},$$

$$\mathrm{lcs}(\mathcal{A}(R,S)) = \max\{\mathrm{lcs}(M) \mid M \in \mathcal{A}(R,S)\}.$$

We also define a type of infimum and supremum, respectively:

$$\inf(\mathcal{A}(R,S)) = \max\{\mathrm{scs}(M) \mid M \in \mathcal{A}(R,S)\},$$

$$\sup(\mathcal{A}(R,S)) = \min\{\mathrm{lcs}(M) \mid M \in \mathcal{A}(R,S)\}.$$

We henceforth focus on the case when row and column sums are constant. To this end, let Λ_n^x be the set of $n \times n$ $(0,1)$-matrices with constant row and column sum x.

In fact, elements of Λ_n^x may also be thought of as *frequency squares* (sometimes *F-squares*). Let $n, \alpha, \lambda_1, \lambda_2, \dots, \lambda_\alpha \in \mathbb{N}$ and $\sum_{i=1}^{\alpha} \lambda_i = n$. A *frequency square* or *F-square* $F(n; \lambda_1, \lambda_2, \dots, \lambda_\alpha)$ of *order* n is an $n \times n$ array on symbol set $\{s_1, s_2, \dots, s_\alpha\}$ such that each cell contains one symbol and symbol s_i occurs precisely λ_i times in each row and λ_i times in each column. Thus if we let $\alpha = 2$, $s_1 = 1$ and $s_2 = 0$, the frequency squares $F(n; x, n-x)$ are precisely the elements of Λ_n^x.

Critical and defining sets of frequency squares were first studied in [6]. Precise bounds for $\mathrm{scs}(\Lambda_n^x)$ were obtained in [6] for small values of x and upper bounds for general x, including $\mathrm{scs}(\Lambda_{2m}^m) \leqslant m^2$. In [3] it is shown that $\mathrm{scs}(\Lambda_n^x) \geqslant \min\{x^2, (n-x)^2\}$, a corollary of which is:

Theorem 1. $\mathrm{scs}(\Lambda_{2m}^m) = m^2$.

The following theorem was shown via constructing specific $(0,1)$-matrices which do not possess small defining sets.

Theorem 2. ([4]) *If m is a power of two,* $\inf(\Lambda_{2m}^m) \geqslant 2m^2 - O(m^{7/4})$.

This result is currently being generalized to arbitrary m as part of a more general result in [1]. Given that it is easy to show that any element of Λ_{2m}^m has a defining set (and hence critical set) of size at most $2m^2$ (simply take all the 1's), this result is in some sense asympotically optimal. The analogous question has been considered for Latin squares in [7], where it is shown that every Latin square of order n has a defining set of size at most $n^2 - \frac{\sqrt{\pi}}{2}n^{9/6}$ and that for each n there exists a Latin square L with no defining set of size less than $n^2 - (e + o(1))n^{10/6}$.

In this paper we first find a new way of describing a critical set in any $(0,1)$-matrix (Theorem 9). We then find asymptotically tight bounds for the largest critical set size:

$$3m^2 - 4m + 2 \leqslant \mathrm{lcs}(\Lambda_{2m}^m) \leqslant 3m^2 - 2m$$

(Corollary 12) as well as showing the existence of critical sets of each size between m^2 and $3m^2 - 4m + 2$ (Theorem 17). Finally, in Sections 4 and 5 we turn our attention to the supremum case, i.e. the function $\sup(\Lambda_{2m}^m)$. We show that

$$\lceil (3m^2 - 2m + 1)/2 \rceil \leqslant \sup(\Lambda_{2m}^m) \leqslant 2m^2 - m,$$

with the lower bound given by Theorem 18 and the upper bound given by Theorem 23.

2 Trades and critical sets in $(0,1)$-matrices

In this section we list the theory from [3] which is relevant to our paper, extending this theory with a new classification of critical sets in $(0,1)$-matrices. We define a *trade* to be a non-empty partial $(0,1)$-matrix T such that there exists a *disjoint mate* T' such that:

- T_{ij} is empty if and only if T'_{ij} is empty;
- if T_{ij} is non-empty, then $T_{ij} \neq T'_{ij}$;
- if 1 appears precisely k times in a row r (column c) of T, then 1 also appears k times in row r (column c) of T';
- if 0 appears precisely k times in a row r (column c) of T, then 0 also appears k times in row r (column c) of T';

We can analyse the properties of critical sets of $(0,1)$-matrices via the trade structure of $(0,1)$-matrices. We say that a trade T is a *cycle* if each row and each column of T contains either 0 or 2 non-empty positions. A cycle is analogous to what Brualdi calls a *minimal balanced matrix* ([2]) and hence we have the following.

Theorem 3. (Lemma 3.2.1 of [2]) *Any trade T in a $(0,1)$-matrix is a union of disjoint cycles.*

Lemma 4. *A partial $(0,1)$-matrix D is a defining set for a $(0,1)$-matrix M if and only if $D \subseteq M$ and $|D \cap T| \geqslant 1$ for every cycle $T \subseteq M$.*

Since a critical set is a minimal defining set, we have the following.

Corollary 5. *A partial $(0,1)$-matrix D is a critical set for a $(0,1)$-matrix M if and only if it is a defining set for M and for each $(i,j,D_{ij}) \in D$, there exists a cycle $T \in M$ such that $T \cap D = \{(i,j,D_{ij})\}$.*

Next we give a new classification of critical sets in $(0,1)$-matrices that will be useful for our purposes. We embed any element M of Λ_{2m}^{m} in the Euclidian plane with the top left-hand corner in the origin. Specifically, cell (i,j) of M becomes the unit square bordered by the lines $x = j-1$, $x = j$, $y = -i$ and $y = 1-i$. A *South East walk* in M is then the walk induced by a sequence of points $w_0 = (0,0), w_1, w_2, \ldots, w_{4m} = (2m, -2m)$, where either $w_{i+1} = w_i - (0,1)$ (a step *South*) or $w_{i+1} = w_i + (1,0)$ (a step *East*), for each i, $0 \leqslant i < 4m$. Observe that W begins at the top-left corner of M and finishes at the bottom-right corner of M.

Example 6. *Figure 1 gives an example of a South-East walk in a matrix from Λ_3^6. With respect to this walk,*

$$(w_0, w_1, \ldots, w_{12}) = ((0,0),(1,0),(1,-1),(2,-1),(2,-2),(3,-2),(3,-3),\\ (4,-3),(4,-4),(5,-4),(5,-5),(5,-6),(6,-6)),$$
$$(P_0, P_1, \ldots, P_{11}) = ((0,0),(1,0),(1,-1),(2,-1),(2,-2),(3,-2),(3,-3),\\ (4,-3),(4,-4),(5,-4)(5,-6),(6,-6)),$$

$L = 5$ and $L' = 6$. By Theorem 9, the elements in italics form a critical set in this matrix of size 14.

The following theorem was shown in [4].

1	0	*1*	*1*	0	0
1	1	0	0	0	*1*
0	*0*	1	0	*1*	*1*
0	1	*0*	1	0	*1*
1	*0*	1	*0*	1	0
0	1	*0*	1	1	0

Figure 1: A critical set of size 14 in an element of Λ_6^3

Theorem 7. *The set D is a defining set of a $(0,1)$-matrix M if and only if $D \subset M$ and the rows and columns can be rearranged so that there exists a South-East Walk W with only 1's below W and only 0's above W, within the cells of $M \setminus D$.*

Next, we work towards a refinement of the previous theorem to give an equivalent definition of a critical set in a $(0,1)$-matrix. To this end, let C be a critical set of a $(0,1)$-matrix M. From Theorem 7, we may assume that the rows and columns of $M \setminus C$ are rearranged so that there exists a South-East walk W with only 1's below W and only 0's above W. We rearrange the rows and columns of M identically. We assume, without loss of generality, that W includes the point $(1,0)$ (otherwise, swap 0's with 1's and take the transpose of M to obtain an equivalent walk).

We wish to define the *corners* of the walk W. These are the points where the walks changes direction from South to East (or vice versa). To this end, there is a uniquely-defined list of points $P_i = (r_i, c_i)$, $i \geqslant 0$, each on W and with integer coordinates, such that $P_0 = (0,0)$ and $P_\ell = (m, -m)$ and:

- If k is odd, $r_k = r_{k-1}$ and $c_k > c_{k-1}$;
- if k is even, $c_k = c_{k-1}$ and $r_k > r_{k-1}$.

If the last step is South, then $P_{2\ell} = (r_\ell, c_\ell)$ for some ℓ. In this case we define $L = L' = \ell$. Otherwise the last step is East and $P_{2\ell-1} = (r_{\ell-1}, c_\ell)$ for some ℓ; here we define $L = \ell - 1$ and $L' = \ell$. For each $1 \leqslant i \leqslant L$ and $1 \leqslant j \leqslant L'$, let $L_{i,j}$ be the *block* of cells defined as follows:

$$L_{i,j} := \{(r,c) \mid r_i < r \leqslant r_{i+1}, c_j < c \leqslant c_{j+1}\}.$$

The blocks defined above are simply the partition of M induced by the corners of the walk.

Lemma 8. *If C is a critical set, every cell in blocks of the form $L_{i,i}$ $(i \leqslant L)$ contains 1 and every cell in blocks of the form $L_{i,i+1}$ $(i \leqslant L' - 1)$ contains 0.*

Proof. Suppose, for the sake of contradiction, that cell (r, c) contains 0 and belongs to block $L_{i,i}$ for some i. Swap row r with $r_i + 1$ and column c with column $c_i + 1$. Observe that these swaps do not change any of the properties of W with respect to C - in particular C is still a defining set as in Theorem 7.

Next, modify the walk W to obtain the unique South-East walk W' such cell (r, c) is *above* W' but every cell not equal to (r, c) is below W' if and only if it is below W. Then W' is still a South-East walk and thus implies the existence of a defining set D' as in Theorem 7. But $D' \subset C$, so C is not a minimal defining set, a contradiction.

The case when a block of the form $L_{i,i+1}$ contains 0 is similar. □

We have the following.

Theorem 9. *A set C is a critical set of a $(0, 1)$-matrix M if and only if $C \subset M$ and the rows and columns of M (and C) can be rearranged so that there exists a South-East Walk W such that:*

- *The walk W begins in the top-left corner of M and finishes in the bottom-right corner of M;*
- *Within $M \setminus C$, there are only 1's below W and only 0's above W;*
- *Within M, each cell in a block bordering W from below contains 1;*
- *Within M, each cell in a block bordering W from above contains 0.*

Proof. From the discussion above it remains to show the final claim that these conditions are sufficient. From Theorem 7, such a subset C is a defining set of M, so from Corollary 5 and Theorem 3 it is sufficient to show that for each element of C there exists a cycle which intersects C only at that element. Let $(r, c, 0) \in C$. Then $(r, c, 0) \in L_{a,b}$ for some block such that $a < b$. Then there exists a cycle:

$$\{(r, c, 0), (r_a, c, 1), (r_a, c_{a+1}, 0), (r_{a+1}, c_{a+1}, 1), \ldots, (r_{b-1}, c_b, 0), (r, c_b, 1)\},$$

where (r_i, c_i) is any cell in block $L_{i,i}$ and (r_i, c_{i+1}) is any cell in block $L_{i,i+1}$, for each i where these cells are in the cycle. The case when $(r, c, 1) \in C$ is similar. □

Theorems 7 and 9 imply the following result, which was first proved in [3].

Theorem 10. *The complement of a minimal defining set in a* $(0,1)$*-matrix is a defining set.*

In fact, we can improve on this a little.

Theorem 11. *Let* C *be a critical set of a matrix* M *in* Λ_{2m}^m*. Then there is a defining set* D *for* M *such that* $D \subset M \setminus C$ *and* $|D| \leqslant 4m^2 - 2m - |C|$*.*

Proof. Let C be a critical set of a matrix M in Λ_{2m}^m. Then the rows and columns of M can be arranged so that there exists a South-East walk satisfying the conditions of Theorem 9. Let $\{L_{i,j} \mid 1 \leqslant i \leqslant L, 1 \leqslant i \leqslant L'\}$ be the set of blocks with respect to the walk W. Next, let W' be the unique South-East walk such that:

- If $i > j$, block $L_{i,j}$ is below W'; and
- if $i \leqslant j$, block $L_{i,j}$ is above W'.

Since W' is a South-East walk, by Theorem 7, the set of cells below W' containing 1 and the set of cells above W' containing 0 form a defining set D of M. (Note that we are actually applying an equivalent version of Theorem 7 with 1's and 0's swapped.) Moreover, by construction D avoids all cells of C and all cells from the main diagonal of blocks (since by Theorem 9, such blocks contain no 0's). Indeed, $|D| = 4m^2 - |C| - \sum_{i=1}^{L} |L_{i,i}|$. But each row contains at least one element in the main diagonal of blocks, so $|D| \leqslant 4m^2 - 2m - |C|$. □

Corollary 12. *If* C *is a critical set in a matrix* M *in* Λ_{2m}^m*, then* $|C| \leqslant 3m^2 - 2m$*.*

Proof. For the sake of contradiction, suppose there exists a critical set C in a matrix M in Λ_{2m}^m and that $|C| > 3m^2 - 2m$. Then, by the previous theorem, there exists a defining set D in M (and thus a minimal defining set, i.e. a critical set) of size less than m^2. This contradicts Theorem 1. □

1	0	*1*	*1*	*1*	0	0	0
0	1	0	*1*	*1*	*1*	0	0
0	*0*	1	0	*1*	*1*	*1*	0
0	*0*	*0*	1	0	*1*	*1*	*1*
1	*0*	*0*	*0*	1	0	*1*	*1*
1	1	*0*	*0*	*0*	1	0	*1*
1	1	1	*0*	*0*	*0*	1	0
0	1	1	1	*0*	*0*	*0*	1

X_8

Figure 2: The matrix X_8 with elements of a critical set shown in italics.

3 The spectrum of critical set sizes

In this section we show that for each $m \geqslant 1$ and each k such that $m^2 \leqslant k \leqslant 3m^2 - 4m + 2$, there exists a critical set of size k in some matrix from Λ_{2m}^m. From Corollary 12, lcs(Λ_{2m}^m)$\leqslant 3m^2 - 2m$, so this result completes the spectrum with less than $2m$ possible exceptions. We conjecture that there are no exceptions and lcs$(\Lambda_{2m}^m) = 3m^2 - 4m + 2$.

We first show that lcs$(\Lambda_{2m}^m) \geqslant 3m^2 - 4m + 2$ by showing the existence of a critical set of such size for each m. By observation, such a critical set exists for $m = 1$. Otherwise, let $m \geqslant 2$. We define a $(0,1)$-matrix X_{2m} as follows. Cell (i, j) contains:

- 0 if $i - j \equiv k \pmod{2n}$ where $k \in \{1, 2, \dots, m-1, 2m-1\}$;
- 1 otherwise.

It is clear that $X_{2m} \in \Lambda_{2m}^m$. Now, let W be the unique South-East walk from the top left-hand corner of X_{2m} to the bottom right-hand corner of X_{2m} which borders the main diagonal from above.

By Theorem 9, this defines a critical set C which consists of each 0 below W and each 1 above W. Therefore we have the following.

Theorem 13. *Let $m \geqslant 1$. There exists a critical set in $X_{2m} \in \Lambda_{2m}^m$ of size $3m^2 - 4m + 2$.*

See Figure 2 for a demonstration of the previous theorem when $m = 4$. From Corollary 12 we have:

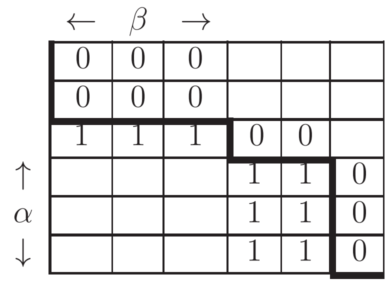

Figure 3: The walk W within the quadrant Q.

Corollary 14. $3m^2 - 4m + 2 \leqslant lcs(\Lambda_{2m}^m) \leqslant 3m^2 - 2m$.

Next, we fill the lower part of the spectrum.

Lemma 15. *Let $m \geqslant 1$. For each k, $m^2 \leqslant k \leqslant m^2 + (m-1)^2$, there exists a critical set of size k in some matrix from Λ_{2m}^m.*

Proof. We define a matrix $M(k) \in \Lambda_{2m}^m$ as follows. Let $k - m^2 = \alpha(m-1) + \beta$, where $\alpha \geqslant 0$ and $0 \leqslant \beta < m-1$. Let W be the unique South-East walk including the points:

$$(0,0), (m,0), (m, \alpha - m), (2m-1, \alpha - m), (2m-1, -m),$$
$$(2m, -m), (2m, -2m) \text{ (if } \beta = 0);$$

otherwise $\beta > 1$ and let W be the unique South-East walk including the points:

$$(0,0), (m,0), (m, \alpha + 1 - m), (m + \beta, \alpha + 1 - m), (m + \beta, \alpha - m),$$
$$(2m-1, \alpha - m), (2m-1, -m), (2m, -m), (2m, -2m).$$

Let Q be the quadrant of cells in $M(k)$ bordered by points $(m,0)$, $(m,-m)$, $(2m,-m)$ and $(2m,0)$, Place 1 in each cell of Q below W and 0 in each cell of Q above W. Next, for each cell $(i,j) \in Q$ containing entry e, let cell $(i-m, j-m)$ contain entry e, cell $(i-m, j)$ contain entry $1-e$ and cell $(i, j-m)$ contain entry $1-e$. We illustrate the walk W within Q (and its induced blocks) in Figure 3. A complete example of $M(k)$ is given in Figure 4.

Clearly $M(k)$ thus defined is an element of Λ_{2m}^m. Observe also that the walk W defines a critical set C as in Theorem 9. Such a critical set consists

1	1	1	1	0	0	0	0
1	1	1	1	0	0	0	0
0	1	1	1	1	0	0	0
0	*0*	*0*	1	1	1	1	0
0	*0*	*0*	*0*	1	1	1	1
0	*0*	*0*	*0*	1	1	1	1
1	*0*	*0*	*0*	*0*	1	1	1
1	1	1	*0*	*0*	*0*	*0*	1

Figure 4: $M(4)$ with $m = 20$, $\alpha = \beta = 1$; the elements of the critical set are shown in italics.

of all occurrences 0 below the walk W. Thus every 0 in the first m columns belongs to C (a total of m^2), no 0 from Q occurs in C and each of the $\alpha(m-1)+\beta$ 0's in the quadrant below Q belongs to C. Thus C has size k, as required. $\square$

Lemma 16. *Let $m \geqslant 4$. For each k, $2m^2 - 5m + 15 \leqslant k \leqslant 3m^2 - 4m + 2$, there exists a critical set of size k in some matrix from Λ_{2m}^{m}.*

Proof. Let I be the following set of cells in X_{2m}:

$$I := \{(i,j) \mid m < i \leqslant 2m, 1 \leqslant j < m-2, m \leqslant i-j < 2m-1\}.$$

Observe that $|I| = m(m+1)/2 - 7$. For each cell $(i,j) \in I$, define a trade $T(i,j) \subset X_{2m}$ on the cells:

$$\{(i,j), (i-m+1, j), (i, i-j), (i-m+1, i-j)\}.$$

In Figure 5, the elements of I are shown in bold for the case $m = 5$.

We claim that the set $\{T(i,j) \mid (i,j) \in I\}$ forms a set of $|I|$ disjoint trades and that only one element of $T(i,j)$ (containing 1) lies above the walk W for each $(i,j) \in I$. It suffices to show disjointness and that for each $(i,j) \in I$:

- Cells (i,j) and $(i-(m-1), i-j)$ contain 1;
- Cells $(i, i-j)$ and $(i-(m-1), j)$ contain 0;
- Cell $(i-(m-1), j)$ lies above W and each other cell lies below.

1	0	*1*	*1*	*1*	*1*	0	0	0	0
0_A	1	0	*1*	1_A	*1*	*1*	0	0	0
0_B	0_E	1	0	1_E	1_B	*1*	*1*	0	0
0_C	0_F	*0*	1	0	1_F	1_C	*1*	*1*	0
0_D	0_G	*0*	*0*	1	0	1_G	1_D	*1*	*1*
$\mathbf{1_A}$	0_H	*0*	*0*	0_A	1	0	1_H	*1*	*1*
$\mathbf{1_B}$	$\mathbf{1_E}$	*0*	*0*	0_E	0_B	1	0	*1*	*1*
$\mathbf{1_C}$	$\mathbf{1_F}$	1	*0*	*0*	0_F	0_C	1	0	*1*
$\mathbf{1_D}$	$\mathbf{1_G}$	1	1	*0*	*0*	0_G	0_D	1	0
0	$\mathbf{1_H}$	1	1	1	*0*	*0*	0_H	*0*	1

Figure 5: The elements of I in the case $m = 5$; trades are shown by common subscripts.

Since $m \leqslant i - j < 2m - 1$, by the definition of X_{2m}, cell (i, j) contains 1 whenever $(i, j) \in I$. We also note that $i - j > 0$ for each $(i, j) \in I$, so each such cell (i, j) lies below W.

Next consider the cell $(i - (m - 1), i - j)$ where $(i, j) \in I$. Then $1 \leqslant j \leqslant m - 3$ implies that

$$-m \leqslant (i - (m - 1)) - (i - j) \leqslant -4.$$

Thus from the definition of X_m, cell $(i - (m - 1), i - j)$ contains 1. Since $2 \leqslant i - (m - 1) \leqslant m$, such cells lie above the main diagonal (and thus above W).

Next, since $m \leqslant i - j \leqslant 2m - 2$, we have:

$$-m + 1 \leqslant j - (i - (m - 1)) \leqslant -1,$$

so each cell of the form $(i - (m - 1), j)$ contains 0. Since $1 \leqslant j \leqslant m - 3$, such cells also lie below the main diagonal.

Finally, we check that cells of the form $(i, i - j)$ always contain 0. This follows from the fact that $1 \leqslant j \leqslant m - 3$. Since $m + 1 \leqslant i \leqslant 2m$, such cells also lie below the main diagonal.

We now check the disjointness of the trades. As cells of the form $(i - (m - 1), i - j)$ lie above W and cells of the form (i, j) lie below W, there is no intersection in cells containing 0. (It is straightforward to check that cells of the same form are distinct.) Finally since $j \leqslant m - 1 < i - j$, cells of the

1	0	*1*	*1*	*1*	*1*	0	0	0	0
0	1	0	*1*	*1*	*1*	*1*	0	0	0
0	*0*	1	0	*1*	*1*	*1*	*1*	0	0
0	*0*	*0*	1	0	*1*	*1*	*1*	0	*1*
0	*0*	*0*	*0*	1	0	*1*	*1*	*1*	*1*
1	*0*	*0*	*0*	*0*	1	0	*1*	*1*	*1*
1	1	*0*	*0*	*0*	*0*	1	0	*1*	*1*
1	1	1	*0*	*0*	*0*	*0*	1	0	*1*
1	1	1	1	*0*	*0*	*0*	*0*	1	0
0	1	1	1	1	*0*	*0*	*0*	1	0

Figure 6: The matrix Y_{10}

from $(i, i-j)$ and $(i-(m-1), j)$ are distinct. Again, it is straightforward to check the cells of the same such forms are distinct.

Thus, replacing exactly α of these trades by their disjoint mates creates a critical set of size $3m^2-4m+2-2\alpha$. Since $|I| = m(m+1)/2-7$, this yields critical sets of size $3m^2-4m+2-2\alpha$ whenever $0 \leqslant \alpha \leqslant m(m+1)/2-7$.

Define Y_{2m} to be the element of Λ_{2m}^m formed by swapping 0 and 1 in the cells $(m-1, 2m-1)$, $(m-1, 2m)$, $(2m, 2m-1)$ and $(2m, 2m)$. The matrix Y_{10} is given in Figure 6. Observe that Y_{2m} has a critical set of size $3m^2-4m+1$ by making a small adjustment to our South East walk so that cell $(2m, 2m)$ lies above the South East walk, with all other cells as before.

Moreover, the set of trades $\{T(i,j) \mid (i,j) \in I\}$ retains the same properties with respect to Y_{2m}. Thus there exists a critical set in Y_{2m} of size $3m^2-4m+1-2\alpha$ whenever $0 \leqslant \alpha \leqslant m(m+1)/2-7$. We are done. □

Theorem 17. *Let $m \geqslant 1$. For each k, $m^2 \leqslant k \leqslant 3m^2-4m+2$, there exists a critical set of size k in some matrix from Λ_{2m}^m.*

Proof. For $m \leqslant 4$, the result is given by Theorem 13, Lemma 15, Lemma 16 and Example 6, except for the following cases: $(m,k) \in \{(3,15),(3,16),(4,26)\}$. The case $m=3$ and $k=16$ can be found in Y_6 as in the previous proof; the remaining two cases are given in Figure 7. Otherwise $m \geqslant 5$ and $2m^2-5m+15 \leqslant m^2+(m-1)^2$ and the theorem follows from Lemmas 15 and 16. □

1	0	*1*	*1*	0	0
1	1	0	0	*1*	0
0	*0*	1	0	*1*	*1*
0	1	*0*	1	0	*1*
1	*0*	1	*0*	1	0
0	1	*0*	1	*0*	1

1	0	*1*	*1*	*1*	0	0	0
1	1	0	0	*1*	*1*	0	0
1	1	1	0	0	0	*1*	0
1	*0*	*0*	1	0	0	*1*	*1*
0	*0*	*0*	1	1	0	*1*	*1*
0	1	*0*	*0*	1	1	0	*1*
0	1	1	*0*	*0*	1	1	0
0	*0*	1	1	*0*	1	*0*	1

Figure 7: Critical sets of size 15 and 26.

4 A lower bound on the supremum

In this section we show that every element of Λ_{2m}^{m} contains a critical set of size greater than $3m(m-1)/2$. Thus:

Theorem 18. $\sup(\Lambda_{2m}^{m}) \geqslant \lceil (3m^2 - 2m + 1)/2 \rceil$.

In the following, let $M \in \Lambda_{2m}^{m}$. By rearranging rows and columns, we may assume that cells $(i, 0)$ and $(0, j)$ contain 1 whenever $i \leqslant m$ or $j \leqslant m$. Let $R_1 = C_1 = \{1\}$, $R_2 = C_2 = \{2, 3, \ldots, m\}$ and $R_3 = C_3 = \{m+1, m+2, \ldots, 2m\}$. These sets give partitions of the rows and columns, so that we may define the subarray $M_{i,j}$ to be the intersection of the rows from R_i and the columns from C_j.

Lemma 19. *Let M be any element of Λ_{2m}^{m}. Then there exists a critical set C_1 of M including:*

- $(1, 1, 1)$*;*
- *no elements from* $M_{1,2} \cup M_{1,3} \cup M_{2,1} \cup M_{3,1}$*;*
- *each* 0 *from* $M_{2,2} \cup M_{2,3} \cup M_{3,2}$*;*
- *no* 1*'s from* $M_{2,2} \cup M_{2,3} \cup M_{3,2} \cup M_{3,3}$.

Proof. First, let D be the subset of M defined as above with the extra property that *every* 0 from $M_{3,3}$ is included. We first show that D is a defining set for M. Let M' be any completion of D to a matrix in Λ_{2m}^{m}. Within D, there are m 0's in each row from R_2 and m 0's in each column from C_2, so

M' and M correspond in rows from R_2 and columns from C_2. In turn, M and M' each have m 1's in the first row and column within corresponding cells. Finally, M and M' have m 0's in corresponding cells of columns from C_3, so $M' = M$. Thus D is a defining set for M.

Next, recursively remove elements of D from $M_{3,3}$ to obtain a set C_1 such that:

- C_1 is a defining set of M; and
- there exists no element (r, c, e) of C_1 in $M_{3,3}$ such that $C_1 \setminus \{(r, c, e)\}$ is a defining set of M.

We claim that C_1 is in fact a critical set of M. It remains to show that the removal of any element of C_1 not in $M_{3,3}$ results in more than one completion.

First consider $(1, 1, 1) \in C_1$. Now, $(1, m+1, 0) \in M \setminus C_1$ and there exists a row $i \geqslant m$ such that $(r, m+1, 1) \in M \setminus C_1$ (otherwise there are more than m 0's in column $m+1$). Next observe that $(r, 1, 0) \in M \setminus C_1$. Thus

$$\{(1, 1, 1), (1, m+1, 0), (r, m+1, 1), (r, 1, 0)\}$$

is a cycle in M intersecting C_1 only at $(1, 1, 1)$. Swapping the entries in the cycle gives an alternate completion of $M \setminus \{(1, 1, 1)\}$.

Next, let $(i, j, 0) \in C_1 \cap M_{2,3}$. Then there exists row $i' \in R_3$ such that $(i', j, 1) \in M \setminus C_1$ (otherwise, as above, there are more than m 0's in column j). Then:

$$\{(i, j, 0), (i', j, 1), (i', 1, 0), (i, 1, 1)\}$$

is a cycle intersecting C_1 only at $(i, j, 0)$. The case when $(i, j, 0) \in C_1 \cap M_{3,2}$ is similar. Finally, let $(i, j, 0) \in C_1 \cap M_{2,2}$. Let (i', j') be any cell of $M_{3,3}$ containing 1. Then:

$$\{(i, j, 0), (i', j', 1), (i', 1, 0), (1, j', 0), (i, 1, 1), (j, 1, 1)\}$$

intersects C_1 only at $(i, j, 0)$. □

Lemma 20. *Let M be any element of Λ_{2m}^{m}. There exists a critical set C_2 of M including:*

- *no elements from $M_{1,1} \cup M_{1,2} \cup M_{1,3} \cup M_{2,1} \cup M_{3,1}$;*
- *each 1 from $M_{3,3} \cup M_{2,3} \cup M_{3,2}$;*

- *no* 0*'s from* $M_{2,2} \cup M_{2,3} \cup M_{3,2} \cup M_{3,3}$.

Proof. First, let D be the subset of M defined as above with the extra property that *every* 1 from $M_{3,3}$ is included.

We claim that D is a defining set for M. Let M' be any completion of D to a matrix in Λ_{2m}^{m}. Within D, there are m 1's in each row from R_3 and m 1's in each column from C_3, so M' and M correpsond in rows from R_3 and columns from C_3. In turn, M and M' each have m 0's in the first row and column within corresponding cells. Finally, M and M' have m 1's in corresponding cells of columns from C_2, so $M' = M$. Thus our claim is true.

Recursively remove elements of D from $M_{2,2}$ to obtain a set C_2 such that:

- C_2 is a defining set of M; and
- there exists no element (r, c, e) of C_2 in $M_{2,2}$ such that $C_2 \setminus \{(r, c, e)\}$ is a defining set of M.

We claim that C_2 is in fact a critical set of M. It remains to show that the removal of any element of C_2 not in $M_{2,2}$ results in more than one completion.

First, let $(i, j, 1) \in C_2 \cap M_{3,3}$. Then, the intersection of

$$\{(i, j, 1), (i, 1, 0), (1, j, 0), (1, 1, 1)\}$$

with C_2 is $\{(i, j, 1)\}$. Next, let $(i, j, 1) \in C_2 \cap M_{2,3}$. Let (i, j') be a cell of $M_{2,2}$ containing 0. Then the intersection of

$$\{(i, j, 1), (i, j', 0), (1, j, 0), (1, j', 1)\}$$

with C_2 is $\{(i, j, 1)\}$. The case $(i, j, 1) \in C_2 \cap M_{3,2}$ is similar. □

Now we are ready to prove Theorem 18. Let α be the number of 0's in subarray $M_{2,2}$. Then there are $m(m-1) - \alpha$ 0's in $M_{2,3}$ and in turn, α 0's in $M_{3,3}$. Thus there are $m^2 - \alpha$ 1's in $M_{3,3}$. Let C_1 and C_2 be critical sets given by Lemmas 19 and 20 above. Then C_1 and C_2 are disjoint and:

$$|C_1| + |C_2| \geqslant |M_{2,3}| + |M_{3,2}| + \alpha + (m^2 - \alpha) + 1 = 3m^2 - 2m + 1.$$

Theorem 18 follows.

5 An upper bound for the supremum

Define $B_{2m} \in \Lambda_{2m}^m$ to be the matrix such that cell (i,j) contains the element $(\lfloor (i-1)/m \rfloor, \lfloor (j-1)/m \rfloor)$, where $1 \leqslant i, j, \leqslant 2m$. Observe that each quadrant of B_{2m} contains either only 0 or only 1. Via Theorem 9 we can classify all critical sets in B_{2m}. This in turn will yield an upper bound for $\sup(\Lambda_{2m}^m)$.

Let C be a critical set of B_{2m}. Let W be a walk as in Theorem 9, with the "corners" of W and blocks defined as in Section 2. Within B_{2m}, whenever the entries of cells (i,j), (i',j), (i',j') are known, the entry of cell (i,j') is uniquely determined. It follows that each cell of $L_{i,j}$ contains 1 if $i+j$ is even and 0 otherwise.

For each k, $1 \leqslant k \leqslant L$, let $s_k := r_k - r_{k-1}$ and for each k, $1 \leqslant k \leqslant L'$, let $t_k := c_k - c_{k-1}$. Observe that for each i and j such that $1 \leqslant i \leqslant L$ and $1 \leqslant j \leqslant L'$, $|L_{i,j}| = s_i t_j$. The size of critical set C is equal to:

$$\sum_{i+j \equiv 1 \mod 2, i>j} |L_{i,j}| + \sum_{i+j \equiv 0 \mod 2, i<j} |L_{i,j}|.$$

The following lemma is immediate.

Lemma 21. *The size of any critical set C of B_{2m} is equal to:*

$$\sum_{i+j \equiv 1 \mod 2, i>j} s_i t_j + \sum_{i+j \equiv 0 \mod 2, i<j} s_i t_j.$$

In the extreme case when $s_1 = s_2 = \cdots = s_{2m} = t_1 = t_2 = \cdots = t_{2m} = 1$, we have the following.

Corollary 22. *There exists a critical set in B_{2m} of size $2m^2 - m$.*

As per the above corollary, we exhibit a critical set of size 28 in B_8 in Figure 5.

Our next aim is to prove that there is no critical set in B_{2m} of larger size.

Since there are m 1's and m 0's in each row and column, we have the

1	0	*1*	0	*1*	0	*1*	0
0	1	0	*1*	0	*1*	0	*1*
1	*0*	1	0	*1*	0	*1*	0
0	1	*0*	1	0	*1*	0	*1*
1	*0*	1	*0*	1	0	*1*	0
0	1	*0*	1	*0*	1	0	*1*
1	*0*	1	*0*	1	*0*	1	0
0	1	*0*	1	*0*	1	*0*	1

Figure 8: A critical set of size 28 in B_8 (entries shown in italics)

following:

$$m - \sum_{i=0}^{\lfloor (L-1)/2 \rfloor} s_{2i+1} = 0 \tag{1}$$

$$m - \sum_{i=0}^{\lfloor (L'-1)/2 \rfloor} t_{2i+1} = 0 \tag{2}$$

$$m - \sum_{i=1}^{\lfloor L/2 \rfloor} s_{2i} = 0 \tag{3}$$

$$m - \sum_{i=1}^{\lfloor L'/2 \rfloor} t_{2i} = 0. \tag{4}$$

Theorem 23. *The largest critical set in B_{2m} has size $2m^2 - m$.*

Proof. We know a critical set of such size exists by Corollary 22.

We first consider a special case: L is odd and $L' = L + 1 = 2m$. Then we must have each s_i and t_j equal to 1 except $s_{2k} = 2$ for presciely one value of k. From Lemma 21, it then follows that $|C| = 2m^2 - m$.

In all other cases, we apply the method of Lagrange multipliers to maximize the formula given by Lemma 21 subject to the constraints 1, 2, 3 and 4 given above. (Note that we don't assume the constraints: $s_i \geqslant 1$ and $t_j \geqslant 1$, $1 \leqslant i \leqslant L$, $1 \leqslant j \leqslant L'$.)

In the case $L = L'$, this yields $s_1 = s_2 = \cdots = s_{L-1} = s$ for some s and $t_2 = t_3 = \cdots = t_L = t$ and $t_1 = 2m - (L-1)t$ for some t. If L is even, from the constraints it follows that $s_L = s$, $t_1 = t$ and $s = t = 2m/L$. From Lemma 21, we then have

$$|C| \leqslant (2m/L)^2(L-1)L/2 = 2m^2(L-1)/L \leqslant m(2m-1)$$

since $L \leqslant 2m$. If L is odd, from the constraints it follows that $s_L = 0$, $t_1 = 0$, so this reduces to the previous case.

In the case L is odd, $L' = L+1$ and $L+1 \leqslant 2m-2$, by allowing s_{L+1} to be defined, the upper bound in the previous paragraph can be applied, so that

$$|C| \leqslant 2m^2L/(L+1) \leqslant m^2(2m-3)/(m-1) < 2m^2 - m.$$

Otherwise $L' = L+1$ and L is even. Again, we apply the Lagrangian method to obtain $s_1 = s_2 = \cdots = s_L = s$ for some s and $t_2 = t_3 = \cdots = t_L$ for some t. From the constraints, $t_1 + t_{L+1} = t$. Thus $|C| \leqslant stL(L-2)/2 + (t_1 + t_{L+1})m = stL(L-2)/2 + tm$. But $s, t \leqslant 2m/L$ so

$$|C| \leqslant 2m^2(L-1)/L \leqslant m(2m-1).$$

□

References

[1] C. Bodkin, A. Liebenau and I. Wanless, *Most binary matrices have no small defining set*, In progress.

[2] R.A. Brualdi, Combinatorial Matrix Classes, (Encyclop. Mathem. Appl. 108), Cambridge University Press, 2006.

[3] N. Cavenagh, *Defining sets and critical sets in* $(0,1)$*-matrices*, J. Combin. Des. **21** (2013), 253–266.

[4] N. Cavenagh and R. Ramadurai, *Constructing* $(0,1)$*-matrices with large minimal defining sets*, Linear Algebra Appl. **537** (2018), 38–47.

[5] D. Donovan, E.S. Mahmoodian, C. Ramsay and A.P. Street, *Defining sets in combinatorics: a survey*, Surveys in Combinatorics, London Math. Soc. Lecture Note Ser. **307**, (Cambridge Univ. Press, Cambridge, 2003), 115–174.

[6] L.F. Fitina, J. Seberry and D. Sarvate, *On F-squares and their critical sets*, Australas. J. Combin. **19** (1999), 209–230.

[7] M. Ghandehari, H. Hatami and E.S. Mahmoodian, *On the size of the minimum critical set of a Latin square*, Discrete Math. **293** (2005), 121–127.

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