

University of Manitoba Technical Report 06/01
On the spectrum of critical sets in latin squares of
order 2^n

Diane Donovan¹, James LeFevre¹ and G. H. John van Rees²

1. Centre for Discrete Mathematics and Computing

University of Queensland

St Lucia 4072 Australia

2. Department of Computer Science

University of Manitoba

Winnipeg, Manitoba

R3T 2N2

Canada

Abstract

Suppose that L is a latin square of order m and $P \subseteq L$ is a partial latin square. If L is the only latin square of order m which contains P , and no proper subset of P has this property, then P is a *critical set* of L . The critical set spectrum problem is to determine, for a given m , the set of integers t for which there exists a latin square of order m with a critical set of size t . We outline a partial solution to the critical set spectrum problem for latin squares of order 2^n .

The back circulant latin square of even order m has a well-known critical set of size $m^2/4$, and this is the smallest known critical set for a latin square of order m . The abelian 2-group of order 2^n has a critical set of size $4^n - 3^n$, and this is the largest known critical set for a latin square of order 2^n . We construct a set of latin squares with associated critical sets which are intermediate between the back circulant latin square of order 2^n and the abelian 2-group of order 2^n .

1 Introduction

Let m be a positive integer and let $X = \{0, 1, 2, \dots, m-1\}$. A *partial latin square* P of order m is a set of ordered triples of elements of X such that

1. if $(i, j, k), (i', j, k) \in P$, then $i = i'$,
2. if $(i, j, k), (i, j', k) \in P$, then $j = j'$, and
3. if $(i, j, k), (i, j, k') \in P$, then $k = k'$.

If $(i, j, k) \in P$ we say that *entry* k occurs in *row* i and *column* j . Thus we may think of P as an $m \times m$ array of integers chosen from X in such a way that

each element of X occurs at most once in each row and at most once in each column.

If every cell of the array contains an entry then the partial latin square is termed a latin square: every element of X must occur exactly once in each row and each column. In other words, given any pair (i, j) , (i, k) or (j, k) in $X \times X$, there exists exactly one element k , j or i respectively such that $(i, j, k) \in L$. Since a (partial) latin square is defined as a set, the usual set operations apply. The *size* of a (partial) latin square P is the quantity $|P|$ (clearly the size of a latin square of order m is m^2).

Suppose that L is a latin square of order m and $P \subseteq L$ is a partial latin square. If L is the only latin square of order m which contains P , then P is a *uniquely completable set* in L , and L is the *unique completion* of P . If, in addition, no proper subset of P has this property, then P is a *critical set* of L .

Here we are concerned with the spectrum of critical sets; that is, the study of

$$S(m) = \{t \mid \text{there exists a latin square of order } m \text{ with a critical set of size } t\}.$$

See [5], [3], [6] for discussion of this problem. The most important result known is the following:

Lemma 1.1. ([1] and [4]) *There exist critical sets of order m and size t , whenever $\lfloor m^2/4 \rfloor \leq t \leq (m^2 - m)/2$.*

In this paper we extend the upper limit on the known spectrum in the case where the order is a power of 2. We now state our main theorem, for which the proof is provided in the remainder of this paper.

Theorem 1.2. *Suppose that $n \geq 1$ and $4^{n-1} \leq t \leq 4^n - 3^n$. Then there exists a latin square of order 2^n which has a critical set of size t .*

Note that in the limit as n tends to infinity, the maximum size of the critical set as a proportion of the latin square tends to 1.

Two (partial) latin squares, L and M say, are said to be *isotopic* if there exists permutations α , β , γ on X such that $M = \{(\alpha(i), \beta(j), \gamma(k)) \mid (i, j, k) \in L\}$. That is, we may rearrange the row, columns and symbols of L to obtain M . If we apply the same permutations to a critical set of L (in the case where L and M are latin squares rather than partial latin squares), then we obtain a critical set of M .

A *latin bitrade* consists of a pair $\{T, T'\}$ of partial latin squares which satisfy the following property: if there exists a triple $(i, j, k) \in T$, then there exist distinct triples (i, j, k') , (i, j', k) and (i', j, k) in T' , where $i \neq i'$, $j \neq j'$ and $k \neq k'$, and if there exists a triple $(i, j, k) \in T'$, then there exist distinct triples (i, j, k') , (i, j', k) and (i', j, k) in T , where again $i \neq i'$, $j \neq j'$ and $k \neq k'$. Given a latin bitrade $\{T, T'\}$, we refer to T as a *trade*, and T' as the *disjoint mate* of T (and vice-versa). Note that the disjoint mate of a trade is not necessarily unique. The size of a trade T is the quantity $|T|$, as for any other partial latin square, and a trade of size 4, the smallest possible size other than zero, is known as an *intercalate*.

We use the following well-known results (see, for example, the discussion early in [6]):

Lemma 1.3. *Suppose that L is a latin square of order m and $P \subseteq L$ is a partial latin square. Then P is a uniquely completable set in L if and only if there is no trade $T \subseteq L \setminus P$.*

Lemma 1.4. *Suppose that L is a latin square of order m and $P \subseteq L$ is a partial latin square. Then P is a critical set in L if and only if P is a uniquely completable set in L and, for every $x \in P$, there is a trade T satisfying $x \in T$ and $T \setminus \{x\} \subseteq L \setminus P$.*

In this paper, we will be dealing specifically with latin squares of order $m = 2^n$, where n is a positive integer. Thus $X = \{0, 1, 2, \dots, 2^n - 1\}$. It will be useful to consider the binary representation for the elements of X , and so note that any $u \in X$ can be expressed as $u = u_1 \cdot 2^{n-1} + u_2 \cdot 2^{n-2} + \dots + u_{n-1} \cdot 2 + u_n$ and represented by $u = [u_1, u_2, \dots, u_n]$, where $u_i \in \{0, 1\}$ for $i = 1, 2, \dots, n$. We define r_n to be a permutation on the elements of X such that for all $u \in X$, $r_n(u) = r_n([u_1, u_2, \dots, u_{n-1}, u_n]) = [u_n, u_{n-1}, \dots, u_2, u_1]$. Given any element u of $X = \{0, 1, 2, \dots, 2^n - 1\}$, u and $u + 2^n$ may be regarded as elements of $\{0, 1, 2, \dots, 2^{n+1} - 1\}$. We have $u = [u_1, u_2, \dots, u_n] = [0, u_1, u_2, \dots, u_n]$ and $u + 2^n = [1, u_1, u_2, \dots, u_n]$, and thus $r_{n+1}(u) = 2r_n(u)$ and $r_{n+1}(u + 2^n) = 2r_n(u) + 1$.

We shall define two binary operations on the elements of X as follow: For $0 \leq u, v < 2^n$ with $u = [u_1, u_2, \dots, u_n]$ and $v = [v_1, v_2, \dots, v_n]$, define

$$\begin{aligned} u \oplus_n v &\equiv u + v \pmod{2^n}, \quad 0 \leq u \oplus_n v \leq 2^n - 1, \text{ and} \\ u \oplus v &= [(u_1 \oplus_1 v_1), (u_2 \oplus_1 v_2), \dots, (u_n \oplus_1 v_n)]. \end{aligned}$$

We are specifically interested in the latin squares corresponding to the cyclic group and the abelian 2-group of order 2^n defined, respectively, as:

$$\begin{aligned} C^n &= \{(i, j, i \oplus_n j) \mid i, j \in X\}, \\ Z^n &= \{(i, j, i \oplus j) \mid i, j \in X\}. \end{aligned}$$

At times it will be useful to partition a (partial) latin square into subsquares. This will be achieved as follows. A (partial) latin square L , of order 2^n , may be partitioned into four separate quadrants L_1, L_2, L_3, L_4 , each of order 2^{n-1} :

$$L = \begin{array}{|c|c|} \hline L_1 & L_2 \\ \hline L_3 & L_4 \\ \hline \end{array}.$$

We refer to L_1, L_2, L_3 and L_4 as the first, second, third and fourth quadrants of L respectively (to avoid confusion, we do not use subscripts with latin squares or partial latin squares except to denote quadrants). In general, the quadrants L_1, L_2, L_3 and L_4 will not be (partial) latin squares of order 2^{n-1} , because L contains entries from $X = \{0, 1, 2, \dots, 2^n - 1\}$ while the entries in a (partial) latin square of order 2^{n-1} must belong to the set $\{0, 1, 2, \dots, 2^{n-1} - 1\}$. However, if the quadrant L_i contains at most 2^{n-1} distinct entries, then we can obtain a (partial) latin square of order 2^{n-1} from L_i (and vice-versa) by using a consistent

bijjective relabelling of the entries. Note that if M and N are partial latin squares of order 2^n such that $M \subseteq N$, then $M_i \subseteq N_i$ for $i = 1, 2, 3, 4$.

Given a triple (i, j, k) and integers a and b , we define

$$a(i, j, k) + b = (i, j, ak + b).$$

Given any (partial) latin square P , we likewise define

$$aP + b = \{(i, j, ak + b) \mid (i, j, k) \in P\}.$$

2 Preliminary constructions

Define

$$\begin{aligned} A^n &= \{(i, j, r_n(i) \oplus_n r_n(j)) \mid i, j \in X\} \text{ and} \\ B^n &= \{(i, j, r_n(i) \oplus r_n(j)) \mid i, j \in X\}. \end{aligned}$$

Note that r_n is its own inverse, so we may equivalently write

$$\begin{aligned} A^n &= \{(r_n(i), r_n(j), i \oplus_n j) \mid i, j \in X\} \text{ and} \\ B^n &= \{(r_n(i), r_n(j), i \oplus j) \mid i, j \in X\}. \end{aligned}$$

Therefore, for all positive integers n , the latin square A^n is isotopic to C^n and B^n is isotopic to Z^n ; in each case the rows and columns have been rearranged using the permutation r_n , but the entries are unchanged. Now $r_n(i) \oplus r_n(j) = r_n(i \oplus j)$, so we also have

$$B^n = \{(i, j, r_n(i \oplus j)) \mid i, j \in X\}.$$

Therefore we may also obtain B^n from Z^n by applying the permutation r_n to the entries, while leaving the rows and columns unchanged.

A known critical set of C^n ([2]) is

$$\begin{aligned} cr(C^n) &= \{(i, j, i \oplus_n j) \mid 0 \leq i, j \leq 2^{n-1} - 1, i \oplus_n j \leq 2^{n-1} - 1\} \\ &\cup \{(i, j, i \oplus_n j) \mid 2^{n-1} + 1 \leq i, j \leq 2^n - 1, i \oplus_n j \geq 2^{n-1}\}. \end{aligned}$$

Equivalently, using $[a, b]$ to denote the set of integers between a and b inclusive (if $b < a$, then $[a, b] = \emptyset$), we may write

$$cr(C^n) = \{(i, j, k) \mid (i, j, k) \in C^n, i + j \in [0, 2^{n-1} - 1] \cup [3 \cdot 2^{n-1}, 2^{n+1} - 2]\}.$$

By symmetry, an alternative critical set of C^n is

$$cr^*(C^n) = \{(i, j, k) \mid (i, j, k) \in C^n, i + j \in [0, 2^{n-1} - 2] \cup [3 \cdot 2^{n-1} - 1, 2^{n+1} - 2]\}.$$

Both of these critical sets have size 4^{n-1} .

We have shown that A^n may be obtained from C^n by applying the permutation r_n to both rows and columns. If we similarly permute the rows and columns of $cr(C^n)$, we obtain the partial latin square

$$cr(A^n) = \{(r_n(i), r_n(j), k) \mid (i, j, k) \in C^n, i + j \in [0, 2^{n-1} - 1] \cup [3 \cdot 2^{n-1}, 2^{n+1} - 2]\}.$$

Since $cr(C^n)$ is a critical set of C^n , then $cr(A^n)$ is a critical set of A^n . Using the fact that r_n is its own inverse, we may equivalently write

$$cr(A^n) = \{(i, j, k) \mid (i, j, k) \in A^n, r_n(i)+r_n(j) \in [0, 2^{n-1}-1] \cup [3 \cdot 2^{n-1}, 2^{n+1}-2]\}.$$

Similarly, the critical set of A^n corresponding to $cr^*(C^n)$ is

$$cr^*(A^n) = \{(i, j, k) \mid (i, j, k) \in A^n, r_n(i) + r_n(j) \in [0, 2^{n-1} - 2] \cup [3 \cdot 2^{n-1} - 1, 2^{n+1} - 2]\}.$$

Example 2.1. If we let $n = 3$, then $X = \{000, 001, 010, 011, 100, 101, 110, 111\}$ (in binary notation) and A^3 and B^3 are as follows: Note that the headline and sideline index the rows and columns and have been included for ease of checking.

A^3 (in binary notation)

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

A^3 (in base 10 notation)

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

B^3 (in base 10 notation)

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

B^3 (in binary notation)

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

We note that

$$A^3 = \begin{array}{|c|c|} \hline 2A^2 & 2A^2 + 1 \\ \hline 2A^2 + 1 & 2A^2 \oplus_3 2 \\ \hline \end{array}, \quad \text{and} \quad B^3 = \begin{array}{|c|c|} \hline 2B^2 & 2B^2 + 1 \\ \hline 2B^2 + 1 & 2B^2 \\ \hline \end{array},$$

where

$$A^2 = \begin{array}{|c|c|c|c|c|} \hline & 00 & 01 & 10 & 11 \\ \hline 00 & 00 & 10 & 01 & 11 \\ \hline 01 & 10 & 00 & 11 & 01 \\ \hline 10 & 01 & 11 & 10 & 00 \\ \hline 11 & 11 & 01 & 00 & 10 \\ \hline \end{array} \quad \text{and} \quad B^2 = \begin{array}{|c|c|c|c|c|} \hline & 00 & 01 & 10 & 11 \\ \hline 00 & 00 & 10 & 01 & 11 \\ \hline 01 & 10 & 00 & 11 & 01 \\ \hline 10 & 01 & 11 & 00 & 10 \\ \hline 11 & 11 & 01 & 10 & 00 \\ \hline \end{array}.$$

Example 2.2. Recall that we have defined two critical sets of the cyclic group C^n , namely $cr(C^n)$ and $cr^*(C^n)$, and the corresponding critical sets of A^n are $cr(A^n)$ and $cr^*(A^n)$ respectively. In the case $n = 2$, these critical sets are as follows (decimal notation has been used for ease of explanation):

$$\begin{array}{c} cr(C^2) \\ \begin{array}{|c|c|c|c|} \hline & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & & \\ \hline 1 & 1 & & & \\ \hline 2 & & & & \\ \hline 3 & & & & 2 \\ \hline \end{array} \end{array} \quad \begin{array}{c} cr(A^2) \\ \begin{array}{|c|c|c|c|} \hline & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & & 1 & \\ \hline 1 & & & & \\ \hline 2 & 1 & & & \\ \hline 3 & & & & 2 \\ \hline \end{array} \end{array},$$

$$\begin{array}{c} cr^*(C^2) \\ \begin{array}{|c|c|c|c|} \hline & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & & & \\ \hline 1 & & & & \\ \hline 2 & & & & 1 \\ \hline 3 & & & 1 & 2 \\ \hline \end{array} \end{array} \quad \begin{array}{c} cr^*(A^2) \\ \begin{array}{|c|c|c|c|} \hline & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & & & \\ \hline 1 & & & & 1 \\ \hline 2 & & & & \\ \hline 3 & & 1 & & 2 \\ \hline \end{array} \end{array}$$

Now consider the case $n = 3$; $cr(C^3)$ and $cr(A^3)$ are as follows:

$cr(C^3)$

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

$cr(A^3)$

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

We note that

$$cr(A^3) = \begin{array}{|c|c|} \hline 2cr(A^2) & 2cr(A^2) + 1 \\ \hline 2cr(A^2) + 1 & 2cr^*(A^2) \oplus_3 2 \\ \hline \end{array}.$$

These observations leads to the next lemma.

Lemma 2.3. *For all positive integers n , we have*

$$A^{n+1} = \begin{array}{|c|c|} \hline 2A^n & 2A^n + 1 \\ \hline 2A^n + 1 & 2A^n \oplus_{n+1} 2 \\ \hline \end{array}, \quad B^{n+1} = \begin{array}{|c|c|} \hline 2B^n & 2B^n + 1 \\ \hline 2B^n + 1 & 2B^n \\ \hline \end{array},$$

$$\text{and } cr(A^{n+1}) = \begin{array}{|c|c|} \hline 2cr(A^n) & 2cr(A^n) + 1 \\ \hline 2cr(A^n) + 1 & 2cr^*(A^n) \oplus_{n+1} 2 \\ \hline \end{array}.$$

Proof:

The elements of B^{n+1} have the form $(i, j, r_{n+1}(i) \oplus r_{n+1}(j))$, where $0 \leq i, j \leq 2^{n+1} - 1$. The elements of A^{n+1} have the form $(i, j, r_{n+1}(i) \oplus_{n+1} r_{n+1}(j))$, where $0 \leq i, j \leq 2^{n+1} - 1$; the elements of $cr(A^{n+1})$ have the same form but only occur when $r_{n+1}(i) + r_{n+1}(j) \in [0, 2^n - 1] \cup [3 \cdot 2^n, 2^{n+2} - 2]$.

The proof will be split into four separate cases:

- Case 1) $0 \leq i, j \leq 2^n - 1$,
- Case 2) $0 \leq i \leq 2^n - 1$ and $2^n \leq j \leq 2^{n+1} - 1$,
- Case 3) $2^n \leq i \leq 2^{n+1} - 1$ and $0 \leq j \leq 2^n - 1$,
- Case 4) $2^n \leq i, j \leq 2^{n+1} - 1$.

Case 1: $0 \leq i, j \leq 2^n - 1$. We note that, for any such i and j , where $i = [i_1, i_2, \dots, i_{n+1}]$ and $j = [j_1, j_2, \dots, j_{n+1}]$, we have $i_1 = j_1 = 0$. Thus $r_{n+1}(i) = 2r_n(i)$ and $r_{n+1}(j) = 2r_n(j)$. It follows that $r_{n+1}(i) \oplus_{n+1} r_{n+1}(j) = 2(r_n(i) \oplus_n r_n(j))$, and hence the first quadrant of A^{n+1} is equal to $2A^n$. Furthermore, $r_{n+1}(i) + r_{n+1}(j) \in [0, 2^n - 1] \cup [3 \cdot 2^n, 2^{n+2} - 2]$ if and only if $r_n(i) + r_n(j) \in [0, 2^{n-1} - 1] \cup [3 \cdot 2^{n-1}, 2^n - 1]$, and hence the first quadrant of $cr(A^{n+1})$ is equal to $2cr(A^n)$.

Since $i_1 = j_1 = 0$, we also have $r_{n+1}(i) \oplus r_{n+1}(j) = 2(r_n(i) \oplus r_n(j))$, and thus the first quadrant of B^{n+1} is equal to $2B^n$.

Case 2: $0 \leq i \leq 2^n - 1$ and $2^n \leq j \leq 2^{n+1} - 1$. We note that, for any such i and j , where $i = [i_1, i_2, \dots, i_{n+1}]$ and $j = [j_1, j_2, \dots, j_{n+1}]$, we have $i_1 = 0$ and $j_1 = 1$. Thus $r_{n+1}(i) = 2r_n(i)$ and $r_{n+1}(j) = 2r_n(j - 2^n) + 1$. It follows that $r_{n+1}(i) \oplus_{n+1} r_{n+1}(j) = 2(r_n(i) \oplus_n r_n(j - 2^n)) + 1$, and hence the second quadrant of A^{n+1} is equal to $2A^n + 1$. Furthermore, $r_{n+1}(i) + r_{n+1}(j) \in [0, 2^n - 1] \cup [3 \cdot 2^n, 2^{n+2} - 2]$ if and only if $r_n(i) + r_n(j - 2^n) \in [0, 2^{n-1} - 1] \cup [3 \cdot 2^{n-1}, 2^{n+1} - 2]$, and hence the second quadrant of $cr(A^{n+1})$ is equal to $2cr(A^n) + 1$.

Since $i_1 = 0$ and $j_1 = 1$, we also have $r_{n+1}(i) \oplus r_{n+1}(j) = 2(r_n(i) \oplus r_n(j - 2^n)) \oplus 1 = 2(r_n(i) \oplus r_n(j - 2^n)) + 1$, and thus the second quadrant of B^{n+1} is equal to $2B^n + 1$.

Case 3: This case follows as in Case 2.

Case 4: $2^n \leq i, j \leq 2^{n+1} - 1$. We note that, for any such i and j , where $i = [i_1, i_2, \dots, i_{n+1}]$ and $j = [j_1, j_2, \dots, j_{n+1}]$, we have $i_1 = j_1 = 1$. Thus $r_{n+1}(i) = 2r_n(i - 2^n) + 1$ and $r_{n+1}(j) = 2r_n(j - 2^n) + 1$. It follows that $r_{n+1}(i) \oplus_{n+1} r_{n+1}(j) = 2(r_n(i - 2^n) \oplus_n r_n(j - 2^n)) \oplus_{n+1} 2$, and hence the fourth quadrant of A^{n+1} is equal to $2A^n \oplus_{n+1} 2$. Furthermore, $r_{n+1}(i) + r_{n+1}(j) \in [0, 2^n - 1] \cup [3 \cdot 2^n, 2^{n+2} - 2]$ if and only if $r_n(i - 2^n) + r_n(j - 2^n) \in [0, 2^{n-1} - 2] \cup [3 \cdot 2^{n-1} - 1, 2^{n+1} - 2]$, and hence the fourth quadrant of $cr(A^{n+1})$ is equal to $2cr^*(A^n) \oplus_{n+1} 2$.

Since $i_1 = j_1 = 1$, we also have $r_{n+1}(i) \oplus r_{n+1}(j) = 2(r_n(i - 2^n) \oplus r_n(j - 2^n))$, and thus the fourth quadrant of B^{n+1} is equal to $2B^n$.

Hence the result is true for all cases. \square

Definition 2.4. We iteratively define a partial latin square $cr(B^n)$ of order 2^n as follows:

- (i) $cr(B^1) = cr(A^1) = \{(0, 0, 0)\}$.
- (ii) For $n \in \mathbb{Z}^+$,

$$cr(B^{n+1}) = \begin{array}{|c|c|c|c|} \hline 2cr(B^n) & 2cr(B^n) + 1 & & \\ \hline 2cr(B^n) + 1 & 2B^n & & \\ \hline \end{array}.$$

Example 2.5. We give $cr(B^3)$:

$cr(B^3)$

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

Lemma 2.6. For all $n \in \mathbb{Z}^+$, $cr(B^n)$ is a critical set of B^n . Further, $|cr(B^n)| = 4^n - 3^n$.

Proof: This follows by induction on n , using the doubling construction in [7]. \square

Note that [7] gives a critical set for the abelian 2-group which has size $4^n - 3^n$, and $cr(B^n)$ is a version of this construction.

3 Main construction

We now give the principle construction, proving Theorem 1.2 for critical sets of size s where $s \equiv 1 \pmod{3}$ and $4^{n-1} \leq s \leq 4^n - 3^n$.

For every $n \in \mathbb{Z}^+$, and every s satisfying $s \equiv 1 \pmod{3}$ and $4^{n-1} \leq s \leq 4^n - 3^n$, we iteratively define a latin square $D^{n,s}$ of order 2^n , and a partial latin square $cr(D^{n,s}) \subseteq D^{n,s}$, with $|cr(D^{n,s})| = s$.

In the case $n = 1$, we have $s = 1$, and we define

$$D^{1,1} = \begin{array}{|c|c|} \hline 0 & 1 \\ \hline 1 & 0 \\ \hline \end{array} = \{(0,0,0), (0,1,1), (1,0,1), (1,1,0)\},$$

$$cr(D^{1,1}) = \{(0,0,0)\}.$$

Note that $D^{1,1} = B^1 = A^1$, and $cr(D^{1,1}) = cr(B^1) = cr(A^1)$.

For $n \geq 1$, we use one of two iterative definitions of $D^{n+1,s}$ and $cr(D^{n+1,s})$, depending on the value of s . By definition $s \equiv 1 \pmod{3}$ and $4^n \leq s \leq 4^{n+1} - 3^{n+1}$. We consider the two cases $4^n \leq s \leq 7 \cdot 4^{n-1} - 3$ and $7 \cdot 4^{n-1} \leq s \leq 4^{n+1} - 3^{n+1}$. If $n = 1$, then $3^n - 1 = 2 \cdot 4^{n-1}$, and hence inductively $3^n - 1 \leq 2 \cdot 4^{n-1}$ for all $n \geq 1$. Rearranging gives the inequality $7 \cdot 4^{n-1} - 3 \leq 13 \cdot 4^{n-1} - 3^{n+1}$. Therefore if $4^n \leq s \leq 7 \cdot 4^{n-1} - 3$ we have

$$3(4^{n-1}) + 4^{n-1} \leq s \leq 3(4^n - 3^n) + 4^{n-1}.$$

In the second case, $7 \cdot 4^{n-1} \leq s \leq 4^{n+1} - 3^{n+1}$, we can write

$$3(4^{n-1}) + 4^n \leq s \leq 3(4^n - 3^n) + 4^n.$$

Definition 3.1. If $4^n \leq s \leq 7 \cdot 4^{n-1} - 3$, and $s \equiv 1 \pmod{3}$, we choose integers s_1, s_2, s_3 satisfying $s_1 + s_2 + s_3 + 4^{n-1} = s$, with $4^{n-1} \leq s_i \leq 4^n - 3^n$ and $s_i \equiv 1 \pmod{3}$, for $i = 1, 2, 3$. We define

$$D^{n+1,s} = \begin{array}{|c|c|} \hline 2D^{n,s_1} & 2D^{n,s_2} + 1 \\ \hline 2D^{n,s_3} + 1 & 2A^n \oplus_{n+1} 2 \\ \hline \end{array},$$

$$cr(D^{n+1,s}) = \begin{array}{|c|c|} \hline 2cr(D^{n,s_1}) & 2cr(D^{n,s_2}) + 1 \\ \hline 2cr(D^{n,s_3}) + 1 & 2cr^*(A^n) \oplus_{n+1} 2 \\ \hline \end{array}.$$

Definition 3.2. If $7 \cdot 4^{n-1} \leq s \leq 4^{n+1} - 3^{n+1}$, and $s \equiv 1 \pmod{3}$, we choose integers s_1, s_2, s_3 satisfying $s_1 + s_2 + s_3 + 4^n = s$, with $4^{n-1} \leq s_i \leq 4^n - 3^n$

and $s_i \equiv 1 \pmod{3}$, for $i = 1, 2, 3$. We define

$$D^{n+1,s} = \begin{array}{|c|c|} \hline 2D^{n,s_1} & 2D^{n,s_2} + 1 \\ \hline 2D^{n,s_3} + 1 & 2B^n \\ \hline \end{array},$$

$$cr(D^{n+1,s}) = \begin{array}{|c|c|} \hline 2cr(D^{n,s_1}) & 2cr(D^{n,s_2}) + 1 \\ \hline 2cr(D^{n,s_3}) + 1 & 2B^n \\ \hline \end{array}.$$

It remains to prove that $cr(D^{n,s})$ is a critical set of $D^{n,s}$, for all $n \in \mathbb{Z}^+$, and every s satisfying $s \equiv 1 \pmod{3}$ and $4^{n-1} \leq s \leq 4^n - 3^n$.

Example 3.3. We have noted that if $n = 1$ then $s = 1$ and $D^{n,s} = B^n = A^n$, and $cr(D^{n,s}) = cr(B^n) = cr(A^n)$. Using the iterative construction, we can obtain $D^{n+1,s} = D^{2,s}$. We have $4^n = 4$ and $4^{n+1} - 3^{n+1} = 7$. Since $s \equiv 1 \pmod{3}$, the only possibilities are $s = 4$ and $s = 7$. If $s = 4$ then Definition 3.1 applies, and we obtain $D^{2,4} = A^2$ and $cr(D^{2,4}) = cr(A^2)$. If $s = 7$ then Definition 3.2 applies, and we obtain $D^{2,7} = B^2$ and $cr(D^{2,7}) = cr(B^2)$.

Putting $n = 2$, we can now use the iterative construction to obtain $D^{n+1,s} = D^{3,s}$. We have $4^n = 16$ and $4^{n+1} - 3^{n+1} = 37$. Thus there are 8 possible values of s ; we illustrate the construction for 2 cases, $s = 22$ and $s = 31$. If $s = 22$ then $s \leq 7 \cdot 4^{n-1} - 3 = 25$, so Definition 3.1 applies. We let $s_1 = s_2 = 7$ and $s_3 = 4$; note that $s_1 + s_2 + s_3 + 4^{n-1} = 22$. If $s = 31$ then $s \geq 7 \cdot 4^{n-1} = 28$, so Definition 3.2 applies. We let $s_1 = 7$ and $s_2 = s_3 = 4$; note that $s_1 + s_2 + s_3 + 4^n = 31$.

$$D^{3,22}$$

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

$$cr(D^{3,22})$$

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

$$D^{3,31}$$

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

$$cr(D^{3,31})$$

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

Note that if Definition 3.1 is used at every stage of the iterative construction, then we will have $D^{n,s} = A^n$ and $cr(D^{n,s}) = cr(A^n)$. If, on the other hand,

Definition 3.2 is used at every stage of the iterative construction, then we will have $D^{n,s} = B^n$ and $cr(D^{n,s}) = cr(B^n)$. In general, $D^{n,s}$ and $cr(D^{n,s})$ will be in some sense intermediate between A^n and $cr(A^n)$ on the one hand and B^n and $cr(B^n)$ on the other. We express this property in the following result:

Lemma 3.4. *For all $n \in \mathbb{Z}^+$, and every s satisfying $s \equiv 1 \pmod{3}$ and $4^{n-1} \leq s \leq 4^n - 3^n$, we have*

$$D^{n,s} \setminus cr(D^{n,s}) \subseteq A^n \setminus cr(A^n), \quad (1)$$

$$B^n \setminus cr(B^n) \subseteq D^{n,s} \setminus cr(D^{n,s}). \quad (2)$$

Proof:

The proof is by induction. Recall that if $n = 1$ then $s = 1$, and further $D^{1,1} = B^1 = A^1$, and $cr(D^{1,1}) = cr(B^1) = cr(A^1)$. It follows that equations (1) and (2) hold in the case $n = 1$.

Now assume that equations (1) and (2) hold in the case $n = k$, for some $k \geq 1$. Consider $A^{k+1} \setminus cr(A^{k+1})$. Using the iterative expressions for A^{n+1} and $cr(A^{n+1})$ given by Lemma 2.3, we have

$$\begin{aligned} & A^{k+1} \setminus cr(A^{k+1}) \\ = & \begin{array}{|c|c|} \hline 2A^k \setminus 2cr(A^k) & (2A^k + 1) \setminus (2cr(A^k) + 1) \\ \hline (2A^k + 1) \setminus (2cr(A^k) + 1) & (2A^k \oplus_{k+1} 2) \setminus (2cr^*(A^k) \oplus_{k+1} 2) \\ \hline \end{array} \\ = & \begin{array}{|c|c|} \hline 2(A^k \setminus cr(A^k)) & 2(A^k \setminus cr(A^k)) + 1 \\ \hline 2(A^k \setminus cr(A^k)) + 1 & 2(A^k \setminus cr^*(A^k)) \oplus_{k+1} 2 \\ \hline \end{array}. \end{aligned}$$

Similarly, using the iterative expressions in Lemma 2.3 and Definition 2.4, we have

$$B^{k+1} \setminus cr(B^{k+1}) = \begin{array}{|c|c|} \hline 2(B^k \setminus cr(B^k)) & 2(B^k \setminus cr(B^k)) + 1 \\ \hline 2(B^k \setminus cr(B^k)) + 1 & \emptyset \\ \hline \end{array}.$$

If $s \leq 7 \cdot 4^{k-1} - 3$, then by Definition 3.1 we have

$$D^{k+1,s} \setminus cr(D^{k+1,s}) = \begin{array}{|c|c|} \hline 2(D^{k,s_1} \setminus cr(D^{k,s_1})) & 2(D^{k,s_2} \setminus cr(D^{k,s_2})) + 1 \\ \hline 2(D^{k,s_3} \setminus cr(D^{k,s_3})) + 1 & 2(A^k \setminus cr^*(A^k)) \oplus_{k+1} 2 \\ \hline \end{array}.$$

If $s \geq 7 \cdot 4^{k-1}$, then by Definition 3.2 we have

$$D^{k+1,s} \setminus cr(D^{k+1,s}) = \begin{array}{|c|c|} \hline 2(D^{k,s_1} \setminus cr(D^{k,s_1})) & 2(D^{k,s_2} \setminus cr(D^{k,s_2})) + 1 \\ \hline 2(D^{k,s_3} \setminus cr(D^{k,s_3})) + 1 & \emptyset \\ \hline \end{array}.$$

In quadrant 4, equations (1) and (2) hold trivially. In the other three quadrants, the result follows inductively. \square

We use this result to prove that $cr(D^{n,s})$ is a critical set of $D^{n,s}$.

Lemma 3.5. *For all $n \in \mathbb{Z}^+$, and every s satisfying $s \equiv 1 \pmod{3}$ and $4^{n-1} \leq s \leq 4^n - 3^n$, the latin square $D^{n,s}$ is the unique completion of $cr(D^{n,s})$.*

Proof: We know that $cr(D^{n,s}) \subseteq D^{n,s}$. Thus by Lemma 1.3, $D^{n,s}$ is the unique completion of $cr(D^{n,s})$ provided there is no trade $T \subseteq D^{n,s} \setminus cr(D^{n,s})$. But if such a trade exists, then by equation (1) of Lemma 3.4 we also have $T \subseteq A^n \setminus cr(A^n)$, contradicting the fact that $cr(A^n)$ is a critical set of A^n . \square

Lemma 3.6. *For all $n \in \mathbb{Z}^+$, and every s satisfying $s \equiv 1 \pmod{3}$ and $4^{n-1} \leq s \leq 4^n - 3^n$, $cr(D^{n,s})$ is a critical set of $D^{n,s}$.*

Proof:

We prove this by induction on n . Recall that if $n = 1$ then $s = 1$, and further $D^{1,1} = B^1 = A^1$, and $cr(D^{1,1}) = cr(B^1) = cr(A^1)$. We know that $cr(A^1)$ is a critical set of A^1 , hence $cr(D^{1,1})$ is a critical set of $D^{1,1}$. We now assume that the result holds for $n = k$, where $k \geq 1$, and prove that it holds for $n = k + 1$.

By Lemma 3.5, $D^{k+1,s}$ is the unique completion of $cr(D^{k+1,s})$. Using Lemma 1.4, we just have to show that for any $x \in cr(D^{k+1,s})$, there exists a trade T with $x \in T$ and $T \setminus \{x\} \subseteq D^{k+1,s} \setminus cr(D^{k+1,s})$.

Suppose that x occurs in the first quadrant of $cr(D^{k+1,s})$ (and thus also in the first quadrant of $D^{k+1,s}$). By either Definition 3.1 or Definition 3.2, the first quadrant of $D^{k+1,s}$ is $2D^{k,s_1}$, while the first quadrant of $cr(D^{k+1,s})$ is $2cr(D^{k,s_1})$. By assumption, $cr(D^{k,s_1})$ is a critical set of D^{k,s_1} . Therefore we have $x = 2x'$, where $x' \in cr(D^{k,s_1})$, and there is a trade U satisfying $x' \in U$ and $U \setminus \{x'\} \subseteq D^{k,s_1} \setminus cr(D^{k,s_1})$. It follows that $2U$ is a trade satisfying $x \in 2U$ and $2U \setminus \{x\} \subseteq D^{k+1,s} \setminus cr(D^{k+1,s})$, and we are done (if U' is the disjoint mate of U , then $2U'$ is the disjoint mate of $2U$).

If x occurs in the second or third quadrants of $D^{k+1,s}$, the result follows similarly. If x occurs in the fourth quadrant and Definition 3.1 applies, then the result also follows similarly, since we know that $cr^*(A^k)$ is a critical set of A^k . We are left with the case where x occurs in the fourth quadrant of $D^{k+1,s}$, and Definition 3.2 applies. Comparing Definitions 3.2 and 2.4, we note that the fourth quadrant of $cr(D^{k+1,s})$ is identical to the fourth quadrant of $cr(B^{k+1})$, and hence $x \in cr(B^{k+1})$. By Lemma 2.6, $cr(B^{k+1})$ is a critical set of B^{k+1} , therefore there is a trade T satisfying $x \in T$ and $T \setminus \{x\} \subseteq B^{k+1} \setminus cr(B^{k+1})$. By Equation (2) of Lemma 3.4, it follows that $T \setminus \{x\} \subseteq D^{k+1,s} \setminus cr(D^{k+1,s})$, and we are done. \square

4 Modified constructions

Here we modify the construction in the previous section, in order to produce critical sets of sizes congruent to 0 and 2 modulo 3. We alter several elements of $D^{n,s}$, and remove one or two of these elements from the partial latin square, in order to produce critical sets of size $s - 1$ or $s - 2$. We start by defining the modified latin squares and listing some key relationships, then calculate the values s for which these constructions are well-defined. In the remainder of the section we prove that the partial latin squares given are, in fact, critical sets.

Let $n \geq 2$. Consider the latin square $D^{n,s}$ of order 2^n and its critical set $cr(D^{n,s})$ of size s , as defined iteratively in the previous section. We will assume

that Definition 3.2 is used at the final stage of the iteration, and thus

$$D^{n,s} = \begin{array}{|c|c|} \hline 2D^{n-1,s_1} & 2D^{n-1,s_2} + 1 \\ \hline 2D^{n-1,s_3} + 1 & 2B^{n-1} \\ \hline \end{array}$$

and

$$cr(D^{n,s}) = \begin{array}{|c|c|} \hline 2cr(D^{n-1,s_1}) & 2cr(D^{n-1,s_2}) + 1 \\ \hline 2cr(D^{n-1,s_3}) + 1 & 2B^{n-1} \\ \hline \end{array},$$

where $s = s_1 + s_2 + s_3 + 4^{n-1}$. The fourth (bottom right) quadrants of both $D^{n,s}$ and $cr(D^{n,s})$ are equal to $2B^{n-1}$, so all elements in the fourth quadrant of $D^{n,s}$ occur in $cr(D^{n,s})$.

By the original definition of B^n , the set of four elements in the extreme bottom right of $D^{n,s}$ is $\{(2^n - 2, 2^n - 2, 0), (2^n - 1, 2^n - 2, 2^{n-1}), (2^n - 2, 2^n - 1, 2^{n-1}), (2^n - 1, 2^n - 1, 0)\}$. These elements are also members of $cr(D^{n,s})$. We modify $D^{n,s}$ and $cr(D^{n,s})$ by swapping the entries in these four triples, and then removing $(2^n - 1, 2^n - 1, 2^{n-1})$ from the partial latin square. That is,

$$\begin{aligned} E^{n,s} &= D^{n,s} \setminus \{(2^n - 2, 2^n - 2, 0), (2^n - 1, 2^n - 2, 2^{n-1}), \\ &\quad (2^n - 2, 2^n - 1, 2^{n-1}), (2^n - 1, 2^n - 1, 0)\} \\ &\cup \{(2^n - 2, 2^n - 2, 2^{n-1}), (2^n - 1, 2^n - 2, 0), \\ &\quad (2^n - 2, 2^n - 1, 0), (2^n - 1, 2^n - 1, 2^{n-1})\}, \end{aligned}$$

and

$$\begin{aligned} cr(E^{n,s}) &= cr(D^{n,s}) \setminus \{(2^n - 2, 2^n - 2, 0), (2^n - 1, 2^n - 2, 2^{n-1}), \\ &\quad (2^n - 2, 2^n - 1, 2^{n-1}), (2^n - 1, 2^n - 1, 0)\} \\ &\cup \{(2^n - 2, 2^n - 2, 2^{n-1}), (2^n - 1, 2^n - 2, 0), \\ &\quad (2^n - 2, 2^n - 1, 0)\}. \end{aligned}$$

Provided that $n \geq 3$, we can further modify this construction by replacing the first quadrant of $E^{n,s}$ with a copy of $2E^{n-1,s_1}$ (assuming that E^{n-1,s_1} exists). Recalling that L_i represents the i th quadrant of L , for $i = 1, 2, 3, 4$, define

$$F^{n,s} = \begin{array}{|c|c|} \hline 2E^{n-1,s_1} & E_2^{n,s} \\ \hline E_3^{n,s} & E_4^{n,s} \\ \hline \end{array}$$

and

$$cr(F^{n,s}) = \begin{array}{|c|c|} \hline 2cr(E^{n-1,s_1}) & cr(E^{n,s})_2 \\ \hline cr(E^{n,s})_3 & cr(E^{n,s})_4 \\ \hline \end{array}.$$

We may regard $F^{n,s}$ as $E^{n,s}$ with a second point of modification added, this time at the bottom right corner of the first quadrant.

It is easily verified that $E^{n,s}$ and $F^{n,s}$ are latin squares of order 2^n , and $cr(E^{n,s}) \subseteq E^{n,s}$ and $cr(F^{n,s}) \subseteq F^{n,s}$ are partial latin squares of size $s - 1$ and $s - 2$ respectively. We have not yet shown that these partial latin squares are critical sets. For convenience, we label the two elements which are ‘‘removed’’ from the partial latin square; let

$$\begin{aligned} p_1 &= (2^n - 1, 2^n - 1, 2^{n-1}), \\ p_2 &= (2^{n-1} - 1, 2^{n-1} - 1, 2^{n-1}). \end{aligned}$$

The following relationships follow from the definitions:

$$E^{n,s} \setminus cr(E^{n,s}) = D^{n,s} \setminus cr(D^{n,s}) \cup \{p_1\}. \quad (3)$$

$$F^{n,s} \setminus cr(F^{n,s}) = E^{n,s} \setminus cr(E^{n,s}) \cup \{p_2\} \quad (4)$$

$$= D^{n,s} \setminus cr(D^{n,s}) \cup \{p_1, p_2\}. \quad (5)$$

Before calculating the values of s for which these modified constructions are well defined, we must impose one extra condition, which is required for Lemma 4.2 below (if this condition did not hold then $E^{n,s} \setminus cr(E^{n,s})$ would contain an intercalate). Consider, in the case $n \geq 3$, the four by four subsquare in the upper left corner of $E^{n,s}$; that is, the triple set $\{(i, j, k) \mid (i, j, k) \in E^{n,s}, 0 \leq i, j \leq 3\}$. Since $n \geq 3$ this subsquare is identical to the corresponding subsquare in $D^{n,s}$; thus by the iterative construction of $D^{n,s}$ (using either Definition 3.1 or Definition 3.2 at each stage), this subsquare is equal to $2^{n-2}D^{2,s'}$. So s' is the number of triples in this subsquare which are placed in $cr(E^{n,s})$. As noted in Example 3.3, either $s' = 4$, in which case $D^{2,s'} = A^2$ and $cr(D^{2,s'}) = cr(A^2)$, or $s' = 7$, in which case $D^{2,s'} = B^2$ and $cr(D^{2,s'}) = cr(B^2)$. We impose the condition that $s' = 7$, and thus the entire fourth quadrant of this 4 by 4 subsquare is in the partial latin square; that is, $\{(i, j, k) \mid (i, j, k) \in E^{n,s}, 2 \leq i, j \leq 3\} \subseteq cr(E^{n,s})$. We consider the implications of this condition for the allowed values of s in Lemma 4.1 (i) below. In the case $n = 2$, this condition is redundant.

We briefly consider the implications of this condition for $F^{n,s}$ and $cr(F^{n,s})$. Suppose that $n \geq 4$. In order to remain consistent with equation (4), the above condition must also hold for $F^{n,s}$; that is, $\{(i, j, k) \mid (i, j, k) \in F^{n,s}, 2 \leq i, j \leq 3\} \subseteq cr(F^{n,s})$. But by definition, the first quadrant of $F^{n,s}$ is a relabelling of E^{n-1,s_1} . Since $n - 1 \geq 3$, it follows that this condition must hold in the first quadrant, and therefore in $F^{n,s}$ as a whole, without introducing any further constraints. In the case $n = 3$, the set $\{(i, j, k) \mid (i, j, k) \in F^{n,s}, 2 \leq i, j \leq 3\}$ comprises the fourth quadrant of the first quadrant of $F^{n,s}$. The first quadrant is a relabelling of E^{n-1,s_1} , and thus by the definition of $E^{n,s}$ the fourth quadrant of the first quadrant is contained in $cr(F^{n,s})$, except for the triple p_2 . The corresponding elements of $E^{n,s}$ are all contained in $cr(E^{n,s})$, so this is consistent with equation (4).

Lemma 4.1. *Let $E^{n,s}$, $cr(E^{n,s})$, $F^{n,s}$ and $cr(F^{n,s})$ be as defined above. Then*

- (i) $E^{n,s}$ and $cr(E^{n,s})$ are well-defined for all integers n and s satisfying $n \geq 2$, $7 \cdot 4^{n-2} + 3 \leq s \leq 4^n - 3^n$ and $s \equiv 1 \pmod{3}$, and also for $n = 2$, $s = 7$.
- (ii) $F^{n,s}$ and $cr(F^{n,s})$ are well-defined for all integers n and s satisfying $n \geq 3$, $31 \cdot 4^{n-3} + 3 \leq s \leq 4^n - 3^n$ and $s \equiv 1 \pmod{3}$, and also for $n = 3$, $s = 31$.

Proof.

- (i) We assumed that Definition 3.2 was used at the final stage of the iterative construction of $D^{n,s}$, and hence $s = s_1 + s_2 + s_3 + 4^{n-1}$ (this assumption also implies that $n \geq 2$). From Definition 3.2 we have $4^{n-2} \leq s_i \leq$

$4^{n-1} - 3^{n-1}$ and $s_i \equiv 1 \pmod{3}$, for $i = 1, 2, 3$, which implies that $7 \cdot 4^{n-2} \leq s \leq 4^n - 3^n$ and $s \equiv 1 \pmod{3}$. Since no additional constraints are placed on the second and third quadrants, s_2 and s_3 may take any values within the given range. If $n = 2$ then s_1 is similarly unconstrained, and hence s may take any value within the given range, and we are done. However, if $n \geq 3$ the allowed values of s_1 may be restricted by the condition introduced above. Recall that s' is the number of triples in the subsquare $\{(i, j, k) \mid (i, j, k) \in E^{n,s}, 0 \leq i, j \leq 3\}$ which occur in $cr(E^{n,s})$. Normally either $s' = 4$ or $s' = 7$, but we imposed the condition that $s' = 7$ only. Suppose that s_1 lies within the given range above, but that s_1 is inconsistent with the condition $s' = 7$; that is, we can only construct D^{n-1, s_1} with $s' = 4$. Then we can construct a D^{n-1, s_1+3} with $s' = 7$. It follows that, although we cannot have $s_1 = 4^{n-2}$, the values $s_1 = 4^{n-2} + 3$ and $s_1 = 4^{n-1} - 3^{n-1}$ are achievable, together with at least every second value in between (considering only values congruent to 1 modulo 3). Since we are free to vary s_2 and s_3 within the constraints imposed above, it follows that s may take any value satisfying $7 \cdot 4^{n-2} + 3 \leq s \leq 4^n - 3^n$ and $s \equiv 1 \pmod{3}$.

- (ii) Again we have $s = s_1 + s_2 + s_3 + 4^{n-1}$, with the same constraints on s_2 and s_3 . However, the first quadrant of $F^{n,s}$ is a relabelled copy of E^{n-1, s_1} . It follows from part (i) that $n-1 \geq 2$, $s_1 \equiv 1 \pmod{3}$ and either $7 \cdot 4^{n-3} + 3 \leq s_1 \leq 4^{n-1} - 3^{n-1}$ or else $n-1 = 2$ and $s_1 = 7$. Since there is no other constraint on s , the result follows. \square

In the remainder of this section, we prove that $cr(E^{n,s})$ is in fact a critical set of $E^{n,s}$, and $cr(F^{n,s})$ is a critical set of $F^{n,s}$. We will assume throughout that these four partial latin squares are well defined, with n and s being arbitrary integers within the constraints of Lemma 4.1. We begin with the harder part of the proof, showing that $E^{n,s}$ and $F^{n,s}$ are the unique completions of $cr(E^{n,s})$ and $cr(F^{n,s})$ respectively, but first we need the following results:

Lemma 4.2. *There is no intercalate I such that $p_1 \in I$ and $I \subseteq E^{n,s} \setminus cr(E^{n,s})$,*

Proof. Suppose that there exists such an intercalate I , with disjoint mate I' (we seek a contradiction). Then I and I' must have the form

$$\begin{aligned} I &= \{(2^n - 1, 2^n - 1, 2^{n-1}), (i, j, 2^{n-1}), (i, 2^n - 1, k), (2^n - 1, j, k)\}, \\ I' &= \{(2^n - 1, 2^n - 1, k), (i, j, k), (i, 2^n - 1, 2^{n-1}), (2^n - 1, j, 2^{n-1})\}, \end{aligned}$$

where i, j, k are some elements of X , not necessarily distinct. By equation (3), $I \setminus \{(2^n - 1, 2^n - 1, 2^{n-1})\} = I \setminus \{p_1\} \subseteq D^{n,s} \setminus cr(D^{n,s})$ and hence, by equation (1) of Lemma 3.4, we have $I \setminus \{p_1\} \subseteq A^n \setminus cr(A^n)$. By definition, the members of A^n have the form $(x, y, r_n(x) \oplus_n r_n(y))$. Thus we have $r_n(i) \oplus_n r_n(j) = 2^{n-1}$, and $r_n(i) \oplus_n r_n(2^n - 1) = r_n(2^n - 1) \oplus_n r_n(j) = k$. It follows that $r_n(i) = r_n(j) \in \{2^{n-2}, 2^{n-2} + 2^{n-1}\}$. Therefore $i = j \in \{2, 3\}$. But (for $n \geq 3$) we imposed the condition that $\{(i, j, k) \mid (i, j, k) \in E^{n,s}, 2 \leq i, j \leq 3\} \subseteq cr(E^{n,s})$. Thus $(i, j, 2^{n-1})$, which is a member of I , occurs in $cr(E^{n,s})$. This contradicts

the assumption that $I \subseteq E^{n,s} \setminus cr(E^{n,s})$, so we are done. In the case $n = 2$, the condition $i = j \in \{2, 3\}$ implies that the intercalate occurs entirely within the fourth quadrant, which is impossible since p_1 is the only member of $E^{n,s} \setminus cr(E^{n,s})$ in the fourth quadrant. \square

Corollary 4.3. *There is no intercalate I such that $p_1 \in I$ and $I \subseteq F^{n,s} \setminus cr(F^{n,s})$.*

Proof. Suppose that such an intercalate I exists. If $p_2 \notin I$, then equation (4) implies that $I \subseteq E^{n,s} \setminus cr(E^{n,s})$, which is a contradiction by Lemma 4.2; thus $p_1, p_2 \in I$. It follows that $I = \{(2^n - 1, 2^n - 1, 2^{n-1}), (2^{n-1} - 1, 2^{n-1} - 1, 2^{n-1}), (2^n - 1, 2^{n-1} - 1, z), (2^{n-1} - 1, 2^n - 1, z)\}$, for some z . By equations (5) and (1), $(2^n - 1, 2^{n-1} - 1, z), (2^{n-1} - 1, 2^n - 1, z) \in A^n \setminus cr(A^n)$ and thus $z = r_n(2^n - 1) \oplus_n r_n(2^{n-1} - 1) = 2^n - 3$. But by the original definition, $cr(A^n)$ contains these two triples, giving a contradiction. \square

Lemma 4.4. *The partial latin square $cr(E^{n,s})$ is uniquely completable to $E^{n,s}$.*

Proof. Using Lemma 1.3, we need to show that there is no trade $T \subseteq E^{n,s} \setminus cr(E^{n,s})$. We assume that such a trade exists, and seek a contradiction. Let T' be the disjoint mate of T , so that the pair $\{T, T'\}$ forms a latin bitrade. If T does not contain p_1 , then by equation (3) $T \subseteq D^{n,s} \setminus cr(D^{n,s})$, which is a contradiction since we know that $cr(D^{n,s})$ is a critical set of $D^{n,s}$; thus we can assume that $p_1 \in T$.

Since T and T' are partial latin squares of order 2^n , we may partition each of them into quadrants of order 2^{n-1} ; so we have

$$T = \begin{array}{|c|c|} \hline T_1 & T_2 \\ \hline T_3 & T_4 \\ \hline \end{array} \quad \text{and} \quad T' = \begin{array}{|c|c|} \hline T'_1 & T'_2 \\ \hline T'_3 & T'_4 \\ \hline \end{array}.$$

By assumption $T \subseteq E^{n,s} \setminus cr(E^{n,s})$, so T_i is a subset of the i th quadrant of $E^{n,s} \setminus cr(E^{n,s})$ (and thus of the i th quadrant of $E^{n,s}$), for $i = 1, 2, 3, 4$.

Let $E = \{2m \mid 0 \leq m < 2^{n-1} - 1\}$ and $O = \{2m + 1 \mid 0 \leq m < 2^{n-1} - 1\}$, so E and O partition X . By the iterative definition of $D^{n,s}$ (Definition 3.1 or 3.2), the entries in the first and fourth quadrants of $D^{n,s}$ are in E , while the entries in the second and third quadrants are in O . Therefore $E^{n,s}$ must also satisfy this property, and hence the entries in T_1 and T_4 are in E , while the entries in T_2 and T_3 are in O .

We know that p_1 is an element of T , specifically of T_4 . Now T_4 is a subset of the fourth quadrant of $E^{n,s} \setminus cr(E^{n,s})$ and by definition, the only triple in the fourth quadrant of $E^{n,s} \setminus cr(E^{n,s})$ is p_1 . Therefore $T_4 = \{p_1\}$, and hence $T'_4 = \{(2^n - 1, 2^n - 1, z)\}$, where $z \neq 2^{n-1}$. Since 2^{n-1} is the only even entry in row $2^n - 1$ of T , and hence T' , z is odd.

Let R_i be row i of T ; that is, R_i is the subset of triples from T with the form (i, j, k) , where j and k are arbitrary. Likewise, let R'_i be row i of T' . Each row and each column intersects two quadrants; assume without loss of generality that $i < 2^{n-1}$, so R_i intersects T_1 and T_2 , while R'_i intersects T'_1 and T'_2 (these

intersections may be empty). Suppose $j \in X$. By the definition of a latin trade, there is a triple $(i, j, k) \in T$ if and only if there is a triple $(i, j, k') \in T'$ (we often express this property by saying that T and T' have the same “shape”). Therefore $|R_i \cap T_1| = |R'_i \cap T'_1|$ and $|R_i \cap T_2| = |R'_i \cap T'_2|$. We know that the entries in $R_i \cap T_1$ are from E , while the entries in $R_i \cap T_2$ are from O . But the total number of even (odd) entries in R_i is equal to the total number of even (odd) entries in R'_i . It follows that the number of odd entries in $R'_i \cap T'_1$ is equal to the number of even entries in $R'_i \cap T'_2$. A similar property holds for every other row and column.

Rows 2^{n-1} to $2^n - 1$ intersect the third and fourth quadrants. The only triple in T'_4 is $(2^n - 1, 2^n - 1, z)$, which has an odd entry. Applying the above argument to every row from 2^{n-1} to $2^n - 1$, we see that there is exactly one even entry in T'_3 , and it occurs in row $2^n - 1$. This even entry also occurs in row $2^n - 1$ of T , therefore it is 2^{n-1} . Thus we have $(2^n - 1, y, 2^{n-1}) \in T'$, and similarly $(x, 2^n - 1, 2^{n-1}) \in T'$, where $0 \leq x, y < 2^{n-1}$, and these are the only even entries in T'_3 and T'_2 respectively.

Applying the same argument on rows 0 to $2^{n-1} - 1$, we see that there is exactly one odd entry in T'_1 , and it occurs in row x . Similarly (considering columns 0 to $2^{n-1} - 1$), the only odd entry in T'_1 occurs in column y . Thus we have $(x, y, z') \in T'$, where z' is the sole odd entry in T'_1 .

We now use a slightly different argument to prove that $z' = z$. For any $i \in X$, we know that a given entry occurs in R_i if and only if it occurs in R'_i . Aggregating over rows 2^{n-1} to $2^n - 1$, it follows that the number of occurrences of the entry z in $T_3 \cup T_4$ is equal to the number of occurrences of the entry z in $T'_3 \cup T'_4$. Let this total be t . Since z occurs 0 times in T_4 and 1 time in T'_4 , it occurs t times in T_3 and $t - 1$ times in T'_3 . Now z does not occur as an entry in T_1 , since it is odd, and thus z occurs t times in $T_1 \cup T_3$. By a similar argument as above, using columns 0 to $2^{n-1} - 1$, it follows that z occurs t times in $T'_1 \cup T'_3$, and hence exactly once in T'_1 . But the only odd entry in T'_1 is z' , hence $z = z'$.

We now know that T' contains the four triples $(2^n - 1, 2^n - 1, z)$, $(x, 2^n - 1, 2^{n-1})$, $(2^n - 1, y, 2^{n-1})$, and (x, y, z) . These triples form an intercalate, a trade of size 4. The disjoint mate can be obtained by swapping the entries z and 2^{n-1} . Thus if we let

$$T'' = T' \setminus \{(2^n - 1, 2^n - 1, z), (x, 2^n - 1, 2^{n-1}), (2^n - 1, y, 2^{n-1}), (x, y, z)\} \\ \cup \{(2^n - 1, 2^n - 1, 2^{n-1}), (x, 2^n - 1, z), (2^n - 1, y, z), (x, y, 2^{n-1})\},$$

then $T \setminus T''$ is a trade, with disjoint mate $T'' \setminus T$. This trade cannot have size zero, because that would imply that T is the intercalate $\{(2^n - 1, 2^n - 1, 2^{n-1}), (x, 2^n - 1, z), (2^n - 1, y, z), (x, y, 2^{n-1})\}$, in contradiction to Lemma 4.2. But $p_1 = (2^n - 1, 2^n - 1, 2^{n-1}) \in T''$. Recalling that $T \subseteq E^{n,s} \setminus cr(E^{n,s})$, it follows by equation (3) that we have $T \setminus T'' \subseteq D^{n,s} \setminus cr(D^{n,s})$. This is a contradiction since we know that $cr(D^{n,s})$ is a critical set of $D^{n,s}$. \square

Corollary 4.5. *The partial latin square $cr(F^{n,s})$ is uniquely completable to $F^{n,s}$.*

Proof. Assume that there is a trade $T \subseteq F^{n,s} \setminus cr(F^{n,s})$ (we seek a contradiction). First consider the case where T contains p_1 . Since p_2 has an even entry, $F^{n,s} \setminus cr(F^{n,s})$ has the property (like $E^{n,s} \setminus cr(E^{n,s})$), that all entries in the first and fourth quadrants are even, while all entries in the second and third quadrants are odd. Also p_1 is the only element in the fourth quadrant. Using Corollary 4.3 and the reasoning in the proof of Lemma 4.4, we can deduce the existence of a non-empty trade ($T' \setminus T$ in the proof of Lemma 4.4) which is contained in $F^{n,s} \setminus cr(F^{n,s})$ but does not contain p_1 ; thus we may assume without loss of generality that $p_1 \notin T$.

Let T' be the disjoint mate of T . Since $T \subseteq F^{n,s} \setminus cr(F^{n,s})$ and $p_1 \notin T$, the fourth quadrants of both T and T' are empty. The entries in the first quadrant of T must be even, while the entries in the second and third quadrants are odd. By the reasoning used in the second half of the proof of Lemma 4.4, it follows that the entries in the first quadrant of T' must also be even, while the entries in the second and third quadrants are odd. Letting T_1 and T'_1 be the first quadrants of T and T' respectively, it follows that T_1 is a trade with disjoint mate T'_1 . Since $T \subseteq F^{n,s} \setminus cr(F^{n,s})$, then $T_1 \subseteq 2(E^{n-1,s_1} \setminus cr(E^{n-1,s_1}))$. This is a contradiction, since by Lemma 4.4, $cr(E^{n-1,s_1})$ is uniquely completable to E^{n-1,s_1} . \square

Lemma 4.6. *The partial latin square $cr(E^{n,s})$ is a critical set of $E^{n,s}$, with size $s - 1$.*

Proof. In Lemma 4.4, we proved that $E^{n,s}$ is the unique completion of $cr(E^{n,s})$. Therefore (by Lemma 1.4), we just need to show that for any $x \in cr(E^{n,s})$, there exists a trade T with $x \in T$ and $T \setminus \{x\} \subseteq E^{n,s} \setminus cr(E^{n,s})$.

If $x \in cr(D^{n,s})$, then the result follows immediately, since $cr(D^{n,s})$ is a critical set of $D^{n,s}$ and, by equation (3), $D^{n,s} \setminus cr(D^{n,s}) \subseteq E^{n,s} \setminus cr(E^{n,s})$. Thus we may assume that $x \in cr(E^{n,s}) \setminus cr(D^{n,s}) = \{(2^n - 2, 2^n - 2, 2^{n-1}), (2^n - 2, 2^n - 1, 0), (2^n - 1, 2^n - 2, 0)\}$. If $x = (2^n - 2, 2^n - 1, 0)$, then we let

$$\begin{aligned} T = & \{(0, 1, 2^{n-1}), (1, 1, 0), \\ & (2^n - 2, 1, 2^n - 1), (2^n - 1, 1, 2^{n-1} - 1), \\ & (0, 2^n - 1, 2^n - 1), (1, 2^n - 1, 2^{n-1} - 1), \\ & (2^n - 2, 2^n - 1, 0), (2^n - 1, 2^n - 1, 2^{n-1})\}, \end{aligned}$$

and

$$\begin{aligned} T' = & \{(0, 1, 2^n - 1), (1, 1, 2^{n-1} - 1), \\ & (2^n - 2, 1, 0), (2^n - 1, 1, 2^{n-1}), \\ & (0, 2^n - 1, 2^{n-1}), (1, 2^n - 1, 0), \\ & (2^n - 2, 2^n - 1, 2^n - 1), (2^n - 1, 2^n - 1, 2^{n-1} - 1)\}. \end{aligned}$$

The partial latin square T is a trade, with disjoint mate T' . We have $x \in T$, but we also need to show that every other triple in T occurs in $E^{n,s} \setminus cr(E^{n,s})$. By equation (3), we have $(2^n - 1, 2^n - 1, 2^{n-1}) \in E^{n,s} \setminus cr(E^{n,s})$. The remaining six triples in T each occur in $A^n \setminus cr(A^n)$ (by the original definitions of A^n and $cr(A^n)$). They all occur in the first or second row, or in the first or second

column. If we compare the iterative form of A^n and $D^{n,s}$ (given by Lemma 2.3 and Definition 3.1 or 3.2), and recall that $D^{1,1} = A^1$, then inductively we see that the first two rows and first two columns of $D^{n,s}$ are identical to the first two rows and first two columns of A^n . Likewise the first two rows and first two columns of $cr(D^{n,s})$ are identical to the first two rows and first two columns of $cr(A^n)$. Therefore the remaining six triples of T occur in $D^{n,s} \setminus cr(D^{n,s})$ and hence, by equation (3), in $E^{n,s} \setminus cr(E^{n,s})$. Thus T is the required trade in the case $x = (2^n - 2, 2^n - 1, 0)$. The transpose of this trade is the required trade for $x = (2^n - 1, 2^n - 2, 0)$. Similarly, the required trade for $x = (2^n - 2, 2^n - 2, 2^{n-1})$ is U , with disjoint mate U' , where

$$\begin{aligned} U = & \{(0, 1, 2^{n-1}), (1, 0, 2^{n-1}), \\ & (2^n - 1, 0, 2^n - 1), (2^n - 2, 1, 2^n - 1), \\ & (0, 2^n - 1, 2^n - 1), (1, 2^n - 2, 2^n - 1), \\ & (2^n - 2, 2^n - 2, 2^{n-1}), (2^n - 1, 2^n - 1, 2^{n-1})\}, \end{aligned}$$

and

$$\begin{aligned} U' = & \{(0, 1, 2^n - 1), (1, 0, 2^n - 1), \\ & (2^n - 1, 0, 2^{n-1}), (2^n - 2, 1, 2^{n-1}), \\ & (0, 2^n - 1, 2^{n-1}), (1, 2^n - 2, 2^{n-1}), \\ & (2^n - 2, 2^n - 2, 2^n - 1), (2^n - 1, 2^n - 1, 2^n - 1)\}, \end{aligned}$$

□

Corollary 4.7. *The partial latin square $cr(F^{n,s})$ is a critical set of $F^{n,s}$, with size $s - 2$.*

Proof. In Corollary 4.4, we proved that $F^{n,s}$ is the unique completion of $cr(F^{n,s})$. Therefore (by Lemma 1.4), we just need to show that for any $x \in cr(F^{n,s})$, there exists a trade T with $x \in T$ and $T \setminus \{x\} \subseteq F^{n,s} \setminus cr(F^{n,s})$.

Outside the first quadrant, $F^{n,s}$ and $cr(F^{n,s})$ are identical to $E^{n,s}$ and $cr(E^{n,s})$ respectively. Thus if $x \in cr(F^{n,s})$ is not in the first quadrant, then $x \in cr(E^{n,s})$ and hence by Lemma 4.6 we have a trade T with $x \in T$ and $T \setminus \{x\} \subseteq E^{n,s} \setminus cr(E^{n,s})$. Then by equation (4), $T \setminus \{x\} \subseteq F^{n,s} \setminus cr(F^{n,s})$, so we are done. This leaves the case where x is in the first quadrant of $cr(F^{n,s})$. By Lemma 4.6, $cr(E^{n-1,s_1})$ is a critical set of E^{n-1,s_1} , therefore the required trade exists within the first quadrant. □

5 Proof of Theorem 1.2

In Section 3, and in particular Lemma 3.6, we prove Theorem 1.2 for $t \equiv 1 \pmod{3}$. The necessary critical set is $cr(D^{n,s})$, with $t = s$. Note that for $n = 1$, the only possible value for t is 1; thus we can now assume that $n \geq 2$.

In Lemma 4.6 (with Lemma 4.1 (i)), we prove Theorem 1.2 for $t \equiv 0 \pmod{3}$ and $t \geq 7 \cdot 4^{n-2} + 2$. The necessary critical set is $cr(E^{n,s})$, with $t = |cr(E^{n,s})| =$

$s - 1$. We complete the case $t \equiv 0 \pmod{3}$ using Lemma 1.1. This lemma states that there exist critical sets of order m and size t , whenever $\lfloor m^2/4 \rfloor \leq t \leq (m^2 - m)/2$. Given order $m = 2^n$, this is $4^{n-1} \leq t \leq 2^{2n-1} - 2^{n-1}$. Since $(7 \cdot 4^{n-2} + 2) - 3 = 2^{2n-1} - 2^{2n-4} - 1 \leq 2^{2n-1} - 2^{n-1}$, for $n \geq 2$, we are done.

When $t \equiv 2 \pmod{3}$, Lemma 1.1 gives the case $n = 2$ and $t = 5$, so we may assume that $n \geq 3$. Corollary 4.7 (with Lemma 4.1 (ii)) gives the required critical sets for $t \geq 31 \cdot 4^{n-3} + 1$, and also $n = 3$, $t = 29$. The critical set is $cr(F^{n,s})$, with $t = |cr(F^{n,s})| = s - 2$. Combined with Lemma 1.1, which gives sizes up to $2^{2n-1} - 2^{n-1}$, this leaves only the case $n = 4$ and $t = 122$ undetermined. This case is given by example in the appendix.

Appendix

The following partial latin square is a critical set of order 2^4 and size 122.

0		4		2		6		1		5		3		7	
4		0	8	6		2	10	5				7			
		8	0			10	2				9				11
2		6						3		7		5			
					4		8								9
6		2	10				4	7							
		10	2		8	4	12				11		9		13
1		5		3		7		0	8	4	12	2	10	6	14
								8	0	12	4	10	2	14	6
5				7				4	12	0	8	6	14	2	10
			9				11	12	4	8	0	14	6	10	2
3		7		5				2	10	6	14	0	8	4	12
							9	10	2	14	6	8	0	12	4
7								6	14	2	10	4	12	8	0
			11		9		13	14	6	10	2	12	4	0	

References

- [1] R. Bean and D. Donovan, *Closing a gap in the spectrum of critical sets*, Australasian Journal of Combinatorics **22** (2000), 191–200.
- [2] D. Curran and G.H.J. van Rees, *Critical sets in latin squares*, Proc. Eighth Manitoba Conf. on Numerical Math. and Comput., Congressus Numerantium **23** (1978), 165–168.
- [3] D. Donovan, *The completion of partial Latin squares*, Australasian Journal of Combinatorics **22** (2000), 247–264.
- [4] D. Donovan and A. Howse, *Towards the spectrum of critical sets*, Australasian Journal of Combinatorics **21** (2000), 107–130.

- [5] A.D. Keedwell, *Critical sets for latin squares, graphs and block designs: a survey*, *Congressus Numerantium* **113** (1996), 231–245.
- [6] A.D. Keedwell, *Critical sets in latin squares and related matters: an update*, *Utilitas Mathematica* **65** (2004), 97–131.
- [7] D.R. Stinson and G.H.J. van Rees, *Some large critical sets*, *Congressus Numerantium* **34** (1982), 441–456.