An investigation of 2-critical sets in latin squares

Diane Donovan[1], Chin-Mei Fu[2] and Abdollah Khodkar[1]

[1]Department of Mathematics
The University of Queensland
Brisbane, 4072, Australia

[2]Department of Mathematics
Tamkang University
Tamsui, Taipei, Taiwan

Abstract

In this paper we focus on the existence of 2-critical sets in the latin square corresponding to the elementary abelian 2-group of order 2^n. It has been shown by Stinson and van Rees that this latin square contains a 2-critical set of volume $4^n - 3^n$. We provide constructions for 2-critical sets containing $4^n - 3^n + 1 - (2^{k-1} + 2^{m-1} + 2^{n-(k+m+1)})$ entries, where $1 \leq k \leq n$ and $1 \leq m \leq n - k$. That is, we construct 2-critical sets for certain values less than $4^n - 3^n + 1 - 3 \cdot 2^{\lfloor n/3 \rfloor - 1}$. The results raise the interesting question of whether, for the given latin square, it is possible to construct 2-critical sets of volume m, where $4^n - 3^n + 1 - 3 \cdot 2^{\lfloor n/3 \rfloor - 1} < m < 4^n - 3^n$.

1 Introduction

A critical set is a subset of entries of a latin square which uniquely determines the latin square and is minimal with respect to this property. Let $\mathcal{C}$ be the collection of all critical sets of a latin square L and define the spectrum to be $spec(L) = \{m \mid C \text{ is a critical set of } L \text{ and } |C| = m\}$. We say the spectrum contains a hole if there exist $\ell < m < p$ such that $\ell, p \in spec(L)$, but $m \notin spec(L)$. For the latin square $\mathcal{B}_n$ which corresponds to the addition table for the integers *mod* n, where n is even, we know there exist critical sets containing m entries where $m \in \{\frac{n^2}{4}, \frac{n^2}{4} + 2, \frac{n^2}{4} + 4, \ldots, \frac{n^2-n}{2} - n\}$ or where $\frac{n^2-n}{2} - (n-2) \leq m \leq \frac{n^2-n}{2}$, [**2**]. Bate and van Rees [**1**] have conjectured that for n even there exists no critical set in $\mathcal{B}_n$ containing $n^2/4 + 1$ entries and hence have conjectured that the spectrum for $\mathcal{B}_n$ contains a hole. In this paper we focus on the latin square corresponding to elementary abelian 2-group of order 2^n and prove the existence of general families of 2-critical sets (defined below) of various sizes. In an earlier paper [**3**] we have shown that for $n = 2$ there exist 2-critical sets containing 5 and 7 entries, but no 6 element 2-critical set exists. For $n = 3$, we exhibited examples which proved the existence of 2-critical sets containing m entries where $m \in \{37, 35, 34, \ldots, 27, 26\}$. We were not able to find a 2-critical set containing 25 or 36 entries. Note that a critical set in such a latin square has at least 25 entries, [**4**].

These results raise the question of whether there are holes in $spec(L)$ where L is the latin square corresponding to the elementary abelian 2-group of order 2^n. In this paper we seek to shed some light on this question by providing constructions for 2-critical sets containing $4^n - 3^n + 1 - (2^{k-1} + 2^{m-1} + 2^{n-(k+m+1)})$ entries, where $1 \le k \le n$ and $1 \le m \le n - k$.

2 Definitions

A *partial latin square* P of order v is a $v \times v$ array with entries chosen from the set $V = \{0, \ldots, v-1\}$ in such a way that each element of V occurs at most once in each row and at most once in each column of the array. Thus a partial latin square may contain a number of empty cells. For ease of exposition, a partial latin square P will be represented by a set of ordered triples $P = \{(i, j; P_{ij}) \mid \text{ element } P_{ij} \text{ occurs in cell } (i, j) \text{ of the array}\}$. The *volume* of the partial latin square is $|P|$; that is, the number of non-empty cells in P. Figure 1 provides examples of partial latin squares $P_1,\ P_2,\ P_3$, respectively, of orders 2, 4 and 8 and volumes 1, 7 and 37. If every cell of the $v \times v$ array is occupied the partial latin square is termed a latin square. That is, a *latin square* L of order v is a $v \times v$ array with entries chosen from the set $V = \{0, \ldots, v-1\}$ in such a way that each element of V occurs precisely once in each row and precisely once in each column of the array. Figure 1 provides examples of latin squares $L_1,\ L_2$ of orders 2 and 4 respectively.

The rows and columns of the array will be labelled 0 to $v - 1$. The set of cells $\mathcal{S}_P = \{(i, j) \mid (i, j; P_{ij}) \in P, \text{ for some } P_{ij} \in V\}$ is said to determine the *shape* of P. Thus $(x, y) \in \mathcal{S}_P$ implies that cell (x, y) is filled in the partial latin square P and $(x, y) \notin \mathcal{S}_P$ implies that cell (x, y) is empty in P.

A *latin trade*, $\mathcal{I} = \{I, I'\}$, of *volume* s, is a pair of two disjoint partial latin squares, of order v, such that
1. $\mathcal{S}_I = \mathcal{S}_{I'}$,
2. for each r, $0 \le r \le v-1$, $\{I_{rj} \mid I_{rj} \in V \wedge (r, j; I_{rj}) \in I\} = \{I'_{rj} \mid I'_{rj} \in V \wedge (r, j; I'_{rj}) \in I'\}$ and

0	

P_1

0	1
1	0

L_1

0	1	2	
1	0		
2		0	

P_2

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

L_2

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

P_3

Figure 1: P_1, P_2 and P_3 are partial latin squares of orders 2, 4 and 8 respectively, and L_1 and L_2 are latin squares of orders 2 and 4 respectively.

3. for each c, $0 \leq c \leq v-1$, $\{I_{ic} \mid I_{ic} \in V \wedge (i,c;I_{ic}) \in I\} = \{I'_{ic} \mid I'_{ic} \in V \wedge (i,c;I'_{ic}) \in I'\}$.

In this paper we will be concerned with latin trades of volume 4. Such latin trades correspond to 2×2 latin subsquares, which are called *intercalates.*

A *critical set* C of order v is a partial latin square which has the properties:
1. C is contained in precisely one latin square of order v;
2. For all $x \in C$, $C \setminus \{x\}$ is contained in at least two latin squares of order n.

If a partial latin square has property 1 above then it is said to have a *unique completion* (UC) and if a uniquely completable partial latin square has property 2 above then it is said that every entry is *essential* for unique completion. The following lemma is a well-know consequence of the definitions of critical sets and latin trades.

LEMMA 1 *Let L be a latin square of order v and $C \subset L$. The partial latin square C is a critical set if and only if*
1. *for all latin trades $\{I, I'\}$ of order v, such that $I \subset L$, $I \cap C \neq \emptyset$, and*
2. *for all $x \in C$, there exists a latin trade $\{I, I'\}$ of order v, with $I \subset L$, such that $I \cap C = \{x\}$.*

Given a critical set $C \subset L$ and an element $x \in C$, if there exists an intercalate $J \subset L$ such that $J \cap C = \{x\}$, then x is said to be 2-*essential.* A critical set C is said to be 2-*critical* if for all $x \in C$, x is 2-essential. The partial latin squares P_1, P_2 and P_3 given in Figure 1 are examples of 2-critical sets.

Let P_1 and L_1 be as defined in Figure 1. For $n \geq 2$, define

$$\begin{aligned} L_n = L_1 \times L_{n-1} \quad &= \quad \{(x,y;z),(x,y+2^{n-1};z+2^{n-1}), \\ &\quad\quad (x+2^{n-1},y;z+2^{n-1}),(x+2^{n-1},y+2^{n-1};z) \mid \\ &\quad\quad (x,y;z) \in L_{n-1}\}, \text{ and} \\ P_n = P_1 \otimes P_{n-1} \quad &= \quad \{(x,y;z),(u,v+2^{n-1};w+2^{n-1}), \\ &\quad\quad (u+2^{n-1},v;w+2^{n-1}),(u+2^{n-1},v+2^{n-1};w) \mid \\ &\quad\quad (u,v;w) \in P_{n-1} \text{ and } (x,y;z) \in L_{n-1}\}. \end{aligned}$$

It should be noted that L_n corresponds to the elementary abelian 2-group of order 2^n. The $2^n \times 2^n$ arrays, L_n and P_n, may be partitioned into four quadrants as illustrated in Figure 2. Note L^1_{n-1} and P^1_{n-1}, respectively, are isomorphic copies of L_{n-1} and P_{n-1}, however each symbol $x \in \{0, \ldots, 2^{n-1}-1\}$ has been replaced by $x + 2^{n-1}$.

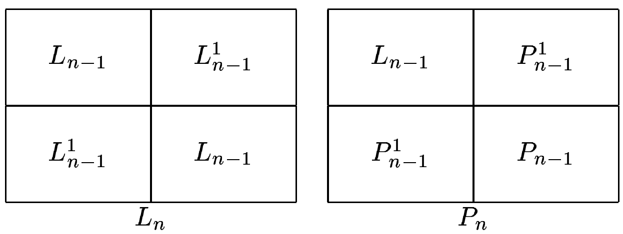

Figure 2: The partitioning of L_n and P_n.

In [**5**] Stinson and van Rees proved that P_n is a 2-critical set in L_n. In this paper we provide an alternative method of proof (Lemma 8). We shall then modify P_n to provide examples of families of 2-critical sets in L_n. The method of proof will be similar to that used for P_n. In doing so we will provide information about the spectrum of 2-critical sets in the latin square corresponding to the elementary abelian 2-group of order 2^n. However, before we present the proof of Lemma 8 we give two important definitions and prove four useful lemmas.

DEFINITION 2 Let $0 \leq u < 2^n$ and $u_i \in \{0,1\}$ for $i = 1, 2, \ldots, n$. We say the vector $[u_1, u_2, \ldots, u_n]$ is the binary representation for u if $u = u_1 \cdot 2^{n-1} + u_2 \cdot 2^{n-2} + \ldots + u_{n-1} \cdot 2 + u_n$ and we write $u = [u_1, u_2, \ldots, u_n]$. Let $0 \leq v < 2^n$ with $v = [v_1, v_2, \ldots, v_n]$. Then by the direct sum $u \oplus v$ we mean the integer w whose binary representation is $[(u_1 \oplus v_1), (u_2 \oplus v_2), \ldots, (u_n \oplus v_n)]$. We let $\bar{u} = (2^n - 1) \oplus u$. Note that $0 \oplus 0 = 0 = 1 \oplus 1$ and $0 \oplus 1 = 1 = 1 \oplus 0$.

LEMMA 3 *Let $0 \leq x, y < 2^n$ with $x = [x_1, \ldots, x_n]$ and $y = [y_1, \ldots, y_n]$. Then $(x, y) \in \mathcal{S}_{P_n}$ if and only if there exists j, $1 \leq j \leq n$, such that $x_j = y_j = 0$. Moreover, the cell (x, y) contains the integer $x \oplus y$ in P_n.*

Proof: The result for $n = 1$ is trivial. Table 1 can be used to verify the result for $n = 2$. In Table 1 a headline and sideline have been added to P_2, these contain, respectively, column numbers and row numbers in binary form. Assume that the result is true for P_{n-1}. For all cells (x, y) of P_n

	[0, 0]	[0, 1]	[1, 0]	[1, 1]
[0, 0]	[0, 0]	[0, 1]	[1, 0]	
[0, 1]	[0, 1]	[0, 0]		
[1, 0]	[1, 0]		[0, 0]	
[1, 1]				

Table 1: P_2 in binary representation.

where $0 \leq x, y < 2^{n-1}$, we have $(x, y) \in \mathcal{S}_{P_n}$ and note that $x_1 = y_1 = 0$. For cell (x, y) where $0 \leq x < 2^{n-1}$ and $2^{n-1} \leq y < 2^n$, we have $x_1 \neq y_1$ and $(x, y) \in \mathcal{S}_{P_n}$ if and only if $(x, y - 2^{n-1}) \in \mathcal{S}_{P_{n-1}}$. Thus by the inductive hypothesis $(x, y) \in \mathcal{S}_{P_n}$ if and only if there exists j, $2 \leq j \leq n$, such that $x_j = y_j = 0$. Similarly one can verify the result for cell (x, y) where $2^{n-1} \leq x < 2^n$ and $0 \leq y < 2^{n-1}$. For cell (x, y) where $2^{n-1} \leq x, y < 2^n$, we have $x_1 = y_1 = 1$ and $(x, y) \in \mathcal{S}_{P_n}$ if and only if $(x - 2^{n-1}, y - 2^{n-1}) \in \mathcal{S}_{P_{n-1}}$. Hence by the inductive hypothesis $(x, y) \in \mathcal{S}_{P_n}$ if and only if there exists j, $2 \leq j \leq n$, such that $x_j = y_j = 0$.

By the inductive hypothesis, for $0 \leq x, y < 2^{n-1}$, the integer $w = (0 \oplus 0).2^{n-1} + (x_2 \oplus y_2).2^{n-2} + \ldots + (x_n \oplus y_n)$ occupies cell (x, y). For $0 \leq x < 2^{n-1}$ and $2^{n-1} \leq y < 2^n$, the integer $w = (0 \oplus 1).2^{n-1} + (x_2 \oplus y_2).2^{n-2} + \ldots + (x_n \oplus y_n)$ occupies cells (x, y) and (y, x), and for $2^{n-1} \leq x, y < 2^n$, the integer $w = (1 \oplus 1).2^{n-1} + (x_2 \oplus y_2).2^{n-2} + \ldots + (x_n \oplus y_n)$ occupies cell (x, y). Thus the result holds for all $n \geq 2$.

LEMMA 4 *Let $0 \leq x, y, z < 2^n$, such that $(x, y) \notin \mathcal{S}_{P_n}$ and $y < z$. Then $x \oplus z$ occurs in column y of P_n.*

Proof: Let $x = [x_1, \ldots, x_n]$, $y = [y_1, \ldots, y_n]$, and $z = [z_1, \ldots, z_n]$. Since $y < z$ there exists an $i \in \{1, 2, \ldots, n\}$ such that $y_i = 0$ and $z_i = 1$. On the other hand $(x, y) \notin \mathcal{S}_{P_n}$ implies that $x_i = 1$ by Lemma 3. So if $w = x \oplus y \oplus z$ and $w = [w_1, w_2, \ldots, w_n]$ then $w_i = 0$ which leads to $(w, y) \in \mathcal{S}_{P_n}$ by Lemma 3. Moreover, $w \oplus y = (x \oplus y \oplus z) \oplus y = x \oplus z$.

Since P_n is symmetric we have the following.

COROLLARY 5 *Let $0 \leq x, y, z < 2^n$, such that $(x, y) \notin \mathcal{S}_{P_n}$ and $x < z$. Then $z \oplus y$ occurs in row x of P_n.*

DEFINITION 6 Let $0 \leq x, y < 2^n$ with $x = [x_1, x_2, \ldots, x_n]$ and $y = [y_1, y_2, \ldots, y_n]$. We define $x \star y$ to be the integer $z \in \{0, 1, 2, \ldots, 2^n - 1\}$ with binary representation $[z_1, z_2, \ldots, z_n]$, where for $i = 1, 2, \ldots, n$

$$z_i = \begin{cases} 1 \text{ if } x_i = y_i = 0 \text{ and} \\ x_i \text{ otherwise.} \end{cases}$$

It is easy to see that $x \star x = 2^n - 1$, $x \star (2^n - 1) = x$ and $(2^n - 1) \star x = 2^n - 1$. The next lemma places $\star$ in the context of P_n.

LEMMA 7 *Let $0 \leq u, v < 2^n$ such that $(u, v) \in \mathcal{S}_{P_n}$. Then*
(1) $u \star v \neq u$ and $v \star u \neq v$.
(2) $v \star u = \bar{u}$ if and only if $u \star v = \bar{v}$.
(3) $u \oplus (v \star u) = (u \star v) \oplus v$.
(4) $u \oplus v = (u \star v) \oplus (v \star u)$.
(5) $I = \{(u, v; u \oplus v), (u, v \star u; u \oplus (v \star u)), ((u \star v), v; (u \star v) \oplus v), (u \star v, v \star u; (u \star v) \oplus (v \star u))\}$ is an intercalate in L_n and $P_n \cap I = \{(u, v; u \oplus v)\}$.

Proof: Points 1, 2, 3 and 4 are easily verified and can be used to verify that $I \subseteq L_n$. We need to prove that $\{(u, v \star u; u \oplus (v \star u)), ((u \star v), v; (u \star v) \oplus v), (u \star v, v \star u; (u \star v) \oplus (v \star u))\} \cap P_n = \emptyset$.

Assume that $(u, w) \in \mathcal{S}_{P_n}$, where $w = v \star u$. Then there exists $j \in \{1, \ldots, n\}$ such that $u_j = 0 = w_j$. By the definition of $\star$ we see that if $w_j = 0$ then $v_j = 0$, but this gives a contradiction as $u_j = 0 = v_j$ implies $w_j = 1$. The other two cases can be dealt with in a similar manner.

LEMMA 8 *For all $n \geq 2$, the partial latin square P_n is a 2-critical set of volume $4^n - 3^n$.*

Proof: Fix $x \in \{0, \ldots, 2^n - 1\}$. Let R be a latin square of order 2^n such that $P_n \subseteq R$. Row x of P_n can be completed as follows. For $z = 2^n - 1, \ldots, 0$, assume $(x, z; x \oplus z) \in L_n \setminus P_n$. Lemma 4 implies for all $y < z$ either $(x, y) \in \mathcal{S}_{P_n}$ or entry $x \oplus z$ occurs in column y of P_n. So $(x, y; x \oplus z) \notin R$, for all $y < z$. Hence $(x, z; x \oplus z) \in R$. Consequently row x of P_n is UC to row x of L_n. As x takes all values $0, \ldots, 2^n - 1$ we see that P_n is UC to L_n. Property 5 of Lemma 7 ensures that each entry of P_n is 2-essential. Thus P_n is a 2-critical set in L_n.

3 New 2-critical sets

Since P_n is UC if we add an entry, say $(x, y; x \oplus y)$, then $P_n \cup \{(x, y; x \oplus y)\}$ is still UC. In this section we construct 2-critical sets which contain the entry $(x, y; x \oplus y)$ and for which the volume is strictly less than $4^n - 3^n$. For the remainder of this section it will be assumed that x and y are fixed integers such that $0 \leq x, y < 2^n$ and $(x, y) \notin \mathcal{S}_{P_n}$. In addition we will use the notation $x = [x_1, x_2, \ldots, x_n]$ for the binary expansion of an integer x, where $0 \leq x \leq 2^n - 1$. We shall define three important sets of columns $\mathcal{A}(x, y)$, $\mathcal{D}(x, y)$ and $\mathcal{D}'(x, y)$. The set $\mathcal{A}(x, y)$ is a set of columns which are used to identify the non-essential entries in row x of $P_n \cup \{(x, y; x \oplus y)\}$. It transpires that these entries can be identified with empty cells of the form (w, y), where $w \geq x$. Likewise, the set $\mathcal{A}(y, x)$ is a set of rows which are used to identify the non-essential entries in column y of $P_n \cup \{(x, y; x \oplus y)\}$ and corresponds to empty cells of the form (x, w), where $w \geq y$. In a similar, fashion $\mathcal{D}(x, y)$ identifies columns containing non-essential cells which contain the entry $x \oplus y$ and $\mathcal{D}'(x, y)$ identifies those which are essential.

DEFINITION 9 Let $0 \leq x, y \leq 2^n - 1$ such that $(x, y) \notin \mathcal{S}_{P_n}$. If $x = 2^n - 1$ we define $\mathcal{A}(x, y) = \emptyset$. Otherwise, let $x_i = 0$ if and only if $i \in \{i_1, i_2, \ldots, i_k\}$, where $i_k = \max\{i_1, i_2, \ldots, i_k\}$. In addition, let $E = \{i \mid x_i = y_i = 1\}$. Define $\mathcal{A}(x, y)$ to be the set of integers $z = [z_1, z_2, \ldots, z_n]$ such that, for $i = 1, \ldots, n$,

$$z_i = \begin{cases} 1 & \text{if} \quad i \in E \\ 0 & \text{if} \quad i \notin (\{i_1, i_2, \ldots, i_{k-1}\} \cup E). \end{cases}$$

We note that for all $z \in \mathcal{A}(x, y)$ we have $z_{i_k} = x_{i_k} = 0$, where x and z are as in Definition 9. So $(x, z; x \oplus z) \in P_n$ by Lemma 3.

LEMMA 10 *Let $z \in \mathcal{A}(x, y) \neq \emptyset$ and $(x, w) \notin \mathcal{S}_{P_n}$.*
(1) If $y < w$, then $(x \oplus w \oplus z, z; x \oplus w) \in P_n$.
(2) If $w < y$, then $(x \oplus z \oplus w, w; x \oplus z) \in P_n$.

Proof: (1) Since $y < w$ there exists an $i \in \{1, 2, \ldots, n\}$ such that $y_i = 0$ and $w_i = 1$. Now $(x, y) \notin \mathcal{S}_{P_n}$ implies that $x_i = 1$. So $z_i = 0$ by Definition 9. Therefore, $x_i \oplus w_i \oplus z_i = z_i = 0$ and the result follows by Lemma 3.

(2) Since $w < y$ there exists an $i \in \{1, 2, \ldots, n\}$ such that $w_i = 0$ and $y_i = 1$. Now $(x, w) \notin \mathcal{S}_{P_n}$ implies that $x_i = 1$. So $z_i = 1$ by Definition 9. Therefore, $x_i \oplus z_i \oplus w_i = w_i = 0$ and the result follows by Lemma 3.

Since P_n is symmetric we have the following.

COROLLARY 11 *Let* $z \in \mathcal{A}(y,x) \neq \emptyset$ *and* $(w,y) \notin \mathcal{S}_{P_n}$.
(1) *If* $x < w$, *then* $(z, y \oplus w \oplus z; y \oplus w) \in P_n$.
(2) *If* $w < x$, *then* $(w, y \oplus z \oplus w; y \oplus z) \in P_n$.

LEMMA 12 *If* $z, w \in \mathcal{A}(x,y)$, *then* $(x \oplus z \oplus w, z; x \oplus w), (x \oplus z \oplus w, w; x \oplus z) \in P_n$.

Proof: Let $x_i = 0$ if and only if $i \in \{i_1, \ldots, i_k\}$ and $i_k = \max\{i_1, \ldots, i_k\}$. By Definition 9 for all $z, w \in \mathcal{A}(x,y)$ we have $z_{i_k} = w_{i_k} = 0$. Consequently, $x_{i_k} \oplus z_{i_k} \oplus w_{i_k} = 0$ and $(x \oplus z \oplus w, z), (x \oplus z \oplus w, w) \in \mathcal{S}_{P_n}$. The result now follows.

Since P_n is symmetric we have the following.

COROLLARY 13 *If* $z, w \in \mathcal{A}(y,x)$, *then* $(z, y \oplus z \oplus w; y \oplus w), (w, y \oplus z \oplus w; y \oplus z) \in P_n$.

DEFINITION 14 Let $(x,y) \notin \mathcal{S}_{P_n}$ and $k = \max\{i \mid x_i = y_i = 1\}$. If $y = \bar{x}$, define $\mathcal{D}(x,y) = \emptyset$, otherwise define $\mathcal{D}(x,y)$ to be the set of integers $z = [z_1, \ldots, z_n]$ such that, for $i = 1, \ldots, n$,

$$z_i = \begin{cases} 1 & \text{if} \quad x_i = 0, \\ 0 & \text{if} \quad y_i = 0, \\ 0 & \text{if} \quad i = k. \end{cases}$$

We also define $\mathcal{D}'(x,y) = \emptyset$ if $y = \bar{x}$, otherwise we define $\mathcal{D}'(x,y)$ to be the set of integers $z = [z_1, \ldots, z_n]$ such that, for $i = 1, \ldots, n$,

$$z_i = \begin{cases} 1 & \text{if} \quad x_i = 0, \\ 0 & \text{if} \quad y_i = 0, \\ 1 & \text{if} \quad i = k. \end{cases}$$

LEMMA 15 *Let* x, y *be as in Definition* 14. *Then* $\mathcal{D}(x,y)$ *is well-defined. Moreover, if* $z \in \mathcal{D}(x,y)$ *and* $u = x \oplus y \oplus z$ *then*
(1) $\bar{x} \in \mathcal{D}(x,y)$ *and* $\bar{x} \leq z < y$,
(2) $(x,z), (u,y) \notin \mathcal{S}_{P_n}$, *and*
(3) $(u,z) \in \mathcal{S}_{P_n}$.

Proof: Since $(x,y) \notin \mathcal{S}_{P_n}$ by Lemma 3 there is no $i \in \{1, 2, \ldots, n\}$ such that $x_i = y_i = 0$. So $\mathcal{D}(x,y)$ is well-defined. Parts (1) and (2) are easy to see. For Part (3) note that $u_k = x_k \oplus y_k \oplus z_k = 1 \oplus 1 \oplus z_k = z_k = 0$. Now the result follows by Lemma 3.

Similar to Lemma 10 we have the following result.

LEMMA 16 *Let* $z \in \mathcal{D}(x,y) \neq \emptyset$, $u = x \oplus y \oplus z$ *and* $(u,w) \notin \mathcal{S}_{P_n}$.
(1) *If* $y < w$ *then* $(u \oplus w \oplus z, z; u \oplus w) \in P_n$.
(2) *If* $w < y$ *then* $(u \oplus z \oplus w, w; u \oplus z) \in P_n$.

Proof: (1) Since $y < w$ there exists an $i \in \{1, 2, \ldots, n\}$ such that $y_i = 0$ and $w_i = 1$. So $x_i = 1$ since $(x,y) \notin \mathcal{S}_{P_n}$ and $z_i = 0$ by Definition 14. Therefore, $u_i = x_i \oplus y_i \oplus z_i = 1$. This implies $u_i \oplus w_i \oplus z_i = z_i = 0$. Now the result follows by Lemma 3.

(2) Since $w < y$ there exists an $i \in \{1, 2, \ldots, n\}$ such that $w_i = 0$ and $y_i = 1$. So $u_i = 1$ since $(u,w) \notin \mathcal{S}_{P_n}$. Now $u_i = x_i \oplus y_i \oplus z_i$ implies that $x_i = z_i$. This leads to $x_i = z_i = 1$ by Definition 14. Therefore, $u_i \oplus z_i \oplus w_i = w_i = 0$. Now the result follows by Lemma 3.

We are now in a position to prove our main result.

THEOREM 17 *Let* $(x,y) \notin \mathcal{S}_{P_n}$. *Then*

$$\begin{aligned} P_n(x,y) \quad = \quad & (P_n \cup \{(x,y; x \oplus y)\}) \setminus (\{(x,z; x \oplus z) \mid z \in \mathcal{A}(x,y)\} \\ & \cup \{(z,y; z \oplus y) \mid z \in \mathcal{A}(y,x)\} \cup \{(x \oplus y \oplus z, z; x \oplus y) \mid \\ & z \in \mathcal{D}(x,y)\}) \end{aligned}$$

is a 2*-critical set.*

Proof: Let R be a latin square, of order 2^n, such that $P_n(x,y) \subseteq R$. First we prove

$$\{(x,z; x \oplus z) \mid z \in \mathcal{A}(x,y)\} \cup \{(z,y; z \oplus y) \mid z \in \mathcal{A}(y,x)\} \subseteq R.$$

For $w = 2^n - 1, \ldots, y + 1$, let $(x, w; x \oplus w) \in L_n \setminus P_n$. If $(x,v) \notin \mathcal{S}_{P_n}$ and $v < w$ then Lemma 4 implies that $x \oplus w$ occurs in column v of P_n. So $(x, v; x \oplus w) \notin R$. Part (1) of Lemma 10 implies that $x \oplus w$ occurs in column z of P_n for all $z \in \mathcal{A}(x,y)$. So $(x, z; x \oplus w) \notin R$. Hence $(x, w; x \oplus w) \in R$ for $w = 2^n - 1, \ldots, y + 1$.

Now if $z \in \mathcal{A}(x,y)$ then by Lemma 12 for all $w \in \mathcal{A}(x,y) \setminus \{z\}$ we have $(x \oplus z \oplus w, w; x \oplus z) \in P_n$. So $(x, w; x \oplus z) \notin R$. In addition, Part (2) of Lemma 10 implies that for all $w < y$ such that $(x,w) \notin \mathcal{S}_{P_n}$ we have $(x \oplus z \oplus w, w; x \oplus z) \in P_n$. So $(x, w; x \oplus z) \notin R$. Hence $(x, z; x \oplus z) \in R$ for $z \in \mathcal{A}(x,y)$.

Similarly one can prove that $(z, y; z \oplus y) \in R$ for $z \in \mathcal{A}(y,x)$. Hence

$$(P_n(x,y) \cup \{(x,z; x \oplus z) \mid z \in \mathcal{A}(x,y)\} \cup \{(z,y; z \oplus y) \mid z \in \mathcal{A}(y,x)\}) \subseteq R.$$

Secondly, we prove $\{(x \oplus y \oplus z, z; x \oplus y) \mid z \in \mathcal{D}(x,y)\} \subseteq R$. For $w = 2^n - 1, \ldots, y+1$, let $(x \oplus y \oplus z, w; x \oplus y \oplus z \oplus w) \in L_n \setminus P_n$, where $z \in \mathcal{D}(x,y)$. If

$(x\oplus y\oplus z, v) \notin \mathcal{S}_{P_n}$ and $v < w$ then Lemma 4 implies that $x\oplus y\oplus z\oplus w$ occurs in column v of P_n. So $(x \oplus y \oplus z, v; x \oplus y \oplus z \oplus w) \notin R$. Part (1) of Lemma 16 implies that $x \oplus y \oplus z \oplus w$ occurs in column z of P_n for all $z \in \mathcal{D}(x, y)$. So $(x \oplus y \oplus z, z; x \oplus y \oplus z \oplus w) \notin R$. Hence $(x \oplus y \oplus z, w; x \oplus y \oplus z \oplus w) \in R$ for $w = 2^n - 1, \ldots, y + 1$.

Now Part (2) of Lemma 16 implies that if $z \in \mathcal{D}(x, y)$ then $x \oplus y$ occurs in column w for all $w < y$ such that $(x \oplus y \oplus z, w) \notin \mathcal{S}_{P_n}$. So $(x\oplus y\oplus z, w; x\oplus y) \notin R$. Hence $(x\oplus y\oplus z, z; x\oplus y) \in R$. Therefore $P_n \subseteq R$. Now by Lemma 8 we must have $R = L_n$.

To prove every entry is 2-essential we divide the elements of $P_n(x, y)$ into five groups:
Group G1, the entry $(x, y; x \oplus y)$;
Group G2, $(u, v; u\oplus v) \in P_n(x, y)$ such that $u\oplus v = x\oplus y$ and $v \in \mathcal{D}'(x, y)$.
Group G3, $(x, v; x \oplus v) \in P_n(x, y)$ such that $v \neq y$ and $v \star x = y$.
Group G4, $(u, y; u \oplus y) \in P_n(x, y)$ such that $u \neq x$ and $u \star y = x$.
Group G5, all other entries.

For the entry $(x, y; x \oplus y)$ we proceed as follows. If $y \neq \bar{x}$ we take $z \in \mathcal{D}(x, y)$ and define

$$I = \{(x, y; x \oplus y), (x \oplus y \oplus z, z; x \oplus y), (x \oplus y \oplus z, y; x \oplus z), (x, z; x \oplus z)\}.$$

Then I is the required intercalate by Lemma 15. If $y = \bar{x}$ and $x \neq 2^n - 1$ then we take $z \in \mathcal{A}(x, y)$ and define

$$I = \{(x, y; x \oplus y), (x \oplus y \oplus z, z; x \oplus y), (x \oplus y \oplus z, y; x \oplus z), (x, z; x \oplus z)\}.$$

If $y = \bar{x}$ and $x = 2^n - 1$ then we take $z \in \mathcal{A}(y, x)$ and define

$$I = \{(x, y; x \oplus y), (z, x \oplus y \oplus z; x \oplus y), (x, x \oplus y \oplus z; y \oplus z), (z, y; z \oplus y)\}.$$

Consider an entry $(u, v; u\oplus v)$ of Group $G2$. Since $v \in \mathcal{D}'(x, y)$ it follows that $\bar{u} \in \mathcal{D}(x, y)$. In addition, $u \oplus v = x \oplus y$ implies $\bar{v} = x \oplus y \oplus \bar{u}$. Define

$$I = \{(u, v; x \oplus y), (\bar{v}, \bar{u}; x \oplus y), (u, \bar{u}; 2^n - 1), (\bar{v}, v; 2^n - 1)\}.$$

Then I is the required intercalate.

Consider an entry $(x, v; x \oplus v)$ of Group $G3$. Let $x = [x_1, x_2, \ldots, x_n]$, $x_i = 0$ if and only if $i \in \{i_1, i_2, \ldots, i_k\}$ and let $i_k = \max\{i_1, i_2, \ldots, i_k\}$. Since $v\star x = y$ and $(x, y) \notin \mathcal{S}_{P_n}$ it follows that $v_i = y_i$ for $i \notin \{i_1, i_2, \ldots, i_k\}$ and if for some i we have $x_i = y_i = 1$ then $v_i = 1$. This information and the fact $v \notin \mathcal{A}(x, y)$ imply $v_{i_k} = 1$. Let $z = \bar{x}\oplus v$. Then it is straightforward to see that $z \in \mathcal{A}(x, y)$. Moreover, $x \oplus z \oplus v = x \oplus \bar{x} \oplus v \oplus v = 2^n - 1$. Define

$$I = \{(x, v; x \oplus v), (x \oplus z \oplus v, z; x \oplus v), (x, z; x \oplus z), (x \oplus z \oplus v, v; x \oplus z)\}.$$

Then I is the required intercalate.

One can prove that the entries of Group $G4$ are also 2-essential in a similar manner.

The intercalates given in Part 5 of Lemma 7 prove that each of the entries in Group $G5$ are 2-essential.

Therefore $P_n(x,y)$ is a 2-critical set.

COROLLARY 18 *Let $0 \le x \le y \le 2^n - 1$ and $(x,y) \notin \mathcal{S}_{P_n}$. Suppose that $x = [x_1, x_2, \ldots, x_n]$ and $y = [y_1, y_2, \ldots, y_n]$, where $x_i = 0$ if and only if $i \in \{i_1, i_2, \ldots, i_k\}$ and $y_j = 0$ if and only if $j \in \{j_1, j_2, \ldots, j_m\}$. Then there exists a 2-critical set of volume $\phi(x,y)$ and order 2^n, where*

$$\phi(x,y) = \begin{cases} 4^n - 3^n + 1 - (2^{k-1} + 2^{m-1} + 2^{n-(k+m+1)}) \\ \quad \text{if } x \neq \bar{y} \text{ and } y \neq 2^n - 1; \\ 4^n - 3^n + 1 - (2^{k-1} + 2^{n-(k+1)}) \\ \quad \text{if } x \neq 0 \text{ and } y = 2^n - 1; \\ 4^n - 3^n + 1 - 2^{n-1} \\ \quad \text{if } x = 0 \text{ or } 2^n - 1, \text{ and } y = 2^n - 1. \end{cases}$$

Proof: First note that if $x = 2^n - 1$ then $|\mathcal{A}(x,y)| = 0$ otherwise $|\mathcal{A}(x,y)| = 2^{k-1}$ by Definition 9 and if $x = \bar{y}$ then $|\mathcal{D}(x,y)| = 0$ otherwise $|\mathcal{D}(x,y)| = 2^{n-(k+m+1)}$ by Definition 14. Now the result follows by Theorem 17.

REMARK 19 *Let $0 \le a, b \le 2^n - 1$.*

1. Let $n \equiv 0 \pmod 3$, $a_i = 0$ if and only if $i \in \{1, 2, \ldots, n/3\}$ and $b_j = 0$ if and only if $j \in \{n/3 + 1, \ldots, 2n/3\}$. Then for all $x, y \in \{0, 1, \ldots, 2^n - 1\}$ we have

$$\phi(x,y) \le \phi(a,b) = 4^n - 3^n + 1 - 3 \cdot 2^{n/3-1}.$$

2. Let $n \equiv 1 \pmod 3$, $a_i = 0$ if and only if $i \in \{1, 2, \ldots, \lfloor n/3 \rfloor\}$ and $b_j = 0$ if and only if $j \in \{\lfloor n/3 \rfloor + 1, \ldots, 2 \cdot \lfloor n/3 \rfloor\}$. Then for all $x, y \in \{0, 1, \ldots, 2^n - 1\}$ we have

$$\phi(x,y) \le \phi(a,b) = 4^n - 3^n + 1 - 4 \cdot 2^{(n-1)/3-1}.$$

3. Let $n \equiv 2 \pmod 3$, $a_i = 0$ if and only if $i \in \{1, 2, \ldots, \lfloor n/3 \rfloor + 1\}$ and $b_j = 0$ if and only if $j \in \{\lfloor n/3 \rfloor + 2, \ldots, 2 \cdot \lfloor n/3 \rfloor + 2\}$. Then for all $x, y \in \{0, 1, \ldots, 2^n - 1\}$ we have

$$\phi(x,y) \le \phi(a,b) = 4^n - 3^n + 1 - 5 \cdot 2^{(n-2)/3-1}.$$

In summary, if we use the above techniques to construct 2-critical sets in the latin square corresponding to the elementary abelian 2-group of order 2^n, then the volume of the 2-critical set is less than or equal to $4^n - 3^n + 1 - 3 \cdot 2^{\lfloor n/3 \rfloor - 1}$. Essentially, we took the 2-critical set of order 2^n and volume $4^n - 3^n$, constructed by Stinson and van Rees [**5**], added an entry and obtained a new 2-critical set by deleting at least $2^{\lfloor n/3 \rfloor} + 2^{\lfloor n/3 \rfloor - 1} - 1$ entries. These results raise the interesting question of whether, in the latin square corresponding to the elementary abelian 2-group of order 2^n, there exists a 2-critical set of volume m where $4^n - 3^n + 1 - 3 \cdot 2^{\lfloor n/3 \rfloor - 1} < m < 4^n - 3^n$.

References

[1] J.A. Bate and G.H.J. van Rees, *Minimal and near-minimal critical sets in back-circulant latin squares*, (submitted).

[2] N. Cavenagh, D. Donovan and A. Khodkar, *On the spectrum of critical sets in back circulant latin squares*, (submitted).

[3] D. Donovan, C.M. Fu and A. Khodkar, *A discussion of 2-critical sets in Abelian 2-groups*, Proceedings of the Twelfth Austalasian Workshop on Combinatorial Algorithms (AWOCA2001), Ed. Edy Tri Baskoro, Institut Teknologi, Bandung Indonesia, 2001, 88–97.

[4] A. Khodkar, *On smallest critical sets for the elementary abelian 2-group*, Utilitas Mathematica **54** (1998), 45–50.

[5] D.R. Stinson and G.H.J. van Rees, *Some large critical sets*, Congressus Numerantium **34** (1982), 441–456.