Uniform critical sets in Latin squares

Diane Donovan and Abdollah Khodkar
Centre for Discrete Mathematics and Computing
Department of Mathematics
The University of Queensland
Queensland 4072
Australia

Abstract

In this paper we introduce two new classes of critical sets, t-uniform and T-uniform (where t is a positive integer and T is a partial latin square). We identify, up to isomorphism, all t-uniform critical sets of order n, where $2 \leq n \leq 6$. We show that the completable product of two T-uniform critical sets is a T-uniform critical set for certain partial Latin squares T, and then apply this theorem to small examples to generate infinite families of T-uniform critical sets.

1 Introduction

In any combinatorial configuration it is possible to identify a subset which uniquely determines the structure of the configuration and is minimal with respect to this property. In this paper we focus on subsets, called critical sets, of a Latin square which uniquely determine the Latin square and are minimal with respect to this property. (Formal definitions of Latin squares and critical sets are given in Sections 2 and 3 of this paper.)

The concept of a critical set was first discussed in 1977 and in 1978 Curran and van Rees [3] exhibited examples of critical sets in the Latin squares corresponding to the addition table for the integers modulo n. One of the first major breakthroughs in the study of critical sets was documented in a paper by Stinson and van Rees [8], in 1982. They defined 2–critical sets and used these in conjunction with 'direct products' to construct critical sets in Latin squares of larger order. A critical set C in a Latin square L is said to be 2–critical if, for each $x \in C$, $C \setminus \{x\}$ is also contained in a Latin square L', where L' and L differ in only four cells. To this day, this construction is one of the most important tools developed in this area.

JCMCC 48 (2004), pp. 3-23

Recent computational results, presented in Section 5 of the current paper, indicate that there exists another class of critical sets which has interesting, and what appear to be useful, properties. We say a critical set C is uniform if, for each $x \in C$, $C \setminus \{x\}$ is contained in a fixed number of Latin squares L_i, and (in some cases) across all elements of the critical set, the differences between the L_i's are isotopic. In some sense we are saying that every element of the critical sets has uniform "weight" or "power". In addition, it is possible to show (see Section 4) that if we take two "uniform" critical sets in Latin squares of order m and n, then the "completable product" is also a "uniform" critical set. It is hoped that the study of this class of critical sets will enable us to extend our methods of construction and thus facilitate the classification of critical sets.

The results presented in this paper are related to work by Fitina, Seberry and Chaudhry [4] and Seberry and Street [7]. In these papers the authors define the nest, the power and the influence of elements of combinatorial configurations and relate this work back to strongboxes and secret sharing schemes.

2 Partial Latin squares

A *partial Latin square* P of order n is an $n \times n$ array containing symbols chosen from a set X of size n in such a way that each element of X occurs at most once in each row and at most once in each column of the array. Thus P 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 $\{(i, j; k) \mid \text{element } k \in X \text{ occurs in cell } (i, j) \text{ of the array}\}$. If all the cells of the array are filled, then the partial Latin square is termed a Latin square. That is, a *Latin square* L of order n is an $n \times n$ array with entries chosen from the set X, of size n, in such a way that each element of X occurs precisely once in each row and precisely once in each column of the array.

We say that the partial Latin square P of order n *completes* to the Latin square L of order n, if $P \subset L$. If L is the only Latin square of order n which has element k in cell (i, j) for each $(i, j; k) \in P$, then P is termed a *uniquely completable set* (UC) in the Latin square L.

Two partial Latin squares P and Q of order n are *isotopic* if there exists three bijections θ, ϕ and ρ, respectively, mapping the rows, columns, and symbols of P to the rows, columns, and symbols of Q. Formally, P and Q are isotopic if $Q = \{(\theta(i), \phi(j); \rho(k)) \mid (i, j; k) \in P\}$. Moreover, if $\theta = \phi = \rho$ then we say P and Q are isomorphic. We note that if the partial Latin squares P and Q of order ℓ are isotopic and there are precisely r

different Latin squares of order ℓ containing P then there are precisely r different Latin squares of order ℓ containing Q.

Let P be a partial Latin square of order n and $\{a,b,c\} = \{1,2,3\}$. Then the (a,b,c)-conjugate of P is denoted and defined by $P_{(a,b,c)} = \{(x_a, x_b; x_c) \mid (x_1, x_2; x_3) \in P\}$. For $\theta \in S_3$, the symmetric group on $\{1,2,3\}$, we define $\theta(x_1,x_2,x_3) = (x_{\theta(1)}, x_{\theta(2)}, x_{\theta(3)})$. It is immediate that P is UC to L if and only if $P_{(a,b,c)}$ is UC to $L_{(a,b,c)}$.

Let N be a Latin square of order n, with symbols chosen from the set $\{1,2,\ldots,n\}$. Let N^r be the array obtained from N by adding $(r-1)n$ to each of the symbols in cells of N. Consequently, N^r is a Latin square isomorphic to N and based on the set of symbols $\{(r-1)n+1,\ldots,(r-1)n+n\}$. If Q is a partial Latin square contained in N then Q^r is obtained by adding $(r-1)n$ to each symbol in the non–empty cells of Q, and consequently Q^r is a partial Latin square contained in N^r, isomorphic to Q, and based on the set of symbols $\{(r-1)n+1,\ldots,(r-1)n+n\}$.

Let M and N be Latin squares of order m and n, with symbols chosen from the sets $\{1,2,\ldots,m\}$ and $\{1,2,\ldots,n\}$, respectively. The *direct product* of M with N is the Latin square of order mn obtained by taking each cell of M containing symbol r, $1 \le r \le m$, and replacing it by the array N^r. Formally,

$$\begin{aligned} M \times N &= \{((a-1)n+d, (b-1)n+e; (c-1)n+f) \mid \\ &\quad (a,b;c) \in M \wedge (d,e;f) \in N\}. \end{aligned}$$

Lemma 1 Let M and N be two Latin squares of order m and n respectively. The direct product $M \times N$ is isomorphic to the direct product $N \times M$.

Proof: Let $Y = \{1,\ldots,mn\}$ and note that for each $x \in Y$ there exists unique integers x_1 and y_1, $1 \le x_1 \le m$ and $1 \le y_1 \le n$ such that $x = (x_1-1)n + y_1$. Define $f : Y \to Y$ such that $f(x) = f((x_1-1)n+y_1) = (y_1-1)m + x_1$. It can be shown that f is one to one and onto. If f is applied to the rows, columns and symbols of $M \times N$, we obtains a Latin square $N \times M$ isomorphic to $M \times N$, where

$$\begin{aligned} N \times M &= \{((d-1)m+a, (e-1)m+b; (f-1)m+c) \\ &\quad \mid ((a-1)n+d, (b-1)n+e; (c-1)n+f) \in M \times N\}. \end{aligned}$$

□

We may generalise this definition to the product of two partial Latin squares as follows.

Let M and N be two Latin squares of orders m and n, with symbols chosen from the sets $\{1,2,\ldots,m\}$ and $\{1,2,\ldots,n\}$, respectively. Suppose that P is a partial Latin square contained in M and Q is a partial Latin square contained in N. Then we define the *completable product* of P and Q, with respect to M and N, written $P \times Q$, to be the partial Latin square of order mn obtained by replacing each cell containing the entry r of P with the array N^r and each cell containing the entry s of $M \setminus P$ with the array Q^s. Formally the completable product of P with Q is

$$\begin{aligned} P \times Q \;=\; & \{((a-1)n+d,(b-1)n+e;(c-1)n+f) \mid \\ & (a,b;c) \in P \wedge (d,e;f) \in N\} \cup \\ & \{((a-1)n+d,(b-1)n+e;(c-1)n+f) \mid \\ & (a,b;c) \in M \setminus P \wedge (d,e;f) \in Q\}. \end{aligned}$$

We note that the partial Latin square $P \times Q$ is contained in $M \times N$.

Lemma 2 Let P be a partial Latin square in the Latin square M of order m and let Q be a partial Latin square in the Latin square N of order n. Then the completable product $P \times Q$ with respect to M and N is isomorphic to the completable product $Q \times P$ with respect to N and M.

Proof: The product $P \times Q$ is the set

$$\begin{aligned} P \times Q \;=\; & \{((a-1)n+d,(b-1)n+e;(c-1)n+f) \mid \\ & (a,b;c) \in P \wedge (d,e;f) \in N\} \cup \\ & \{((a-1)n+d,(b-1)n+e;(c-1)n+f) \mid \\ & (a,b;c) \in M \setminus P \wedge (d,e;f) \in Q\}. \end{aligned}$$

By Lemma 1 we know that $P \times Q$ is isomorphic to

$$\begin{aligned} \chi \;=\; & \{((d-1)m+a,(e-1)m+b;(f-1)m+c) \\ & \mid ((a-1)n+d,(b-1)n+e;(c-1)n+f) \in (P \times Q)\}. \end{aligned}$$

We leave the reader to prove that $\chi = Q \times P$. □

Finally, let P and Q be two partial Latin squares of order m and n, respectively. Then for a given cell (i,j) of P, define the *block position* (i,j) of $P \times Q$ to be the cells of $P \times Q$ corresponding to the intersection of rows $(i-1)n+1$ to $(i-1)n+n$ and columns $(j-1)n+1$ to $(j-1)n+n$.

3 Critical sets

A *critical set* in a Latin square L of order n is a partial Latin square C in L, such that

(1) C is a uniquely completable set in L, and

(2) no proper subset of C satisfies (1).

Let I be a partial Latin square of order n. The set of cells $S_I = \{(i,j) \mid (i,j;k) \in I\}$ is said to determine the *shape* of I. Two partial Latin squares I and I', of order n with $S_I = S_{I'}$, are said to be *mutually balanced* if the symbols in each row (and column) of I are the same as those in the corresponding row (and column) of I'. They are said to be *disjoint* if no cell in I contains the same symbol as the corresponding cell in I'. Given two partial Latin squares I and I' of order n, of the same shape, with the property that I and I' are disjoint and mutually balanced, then I is said to be a *Latin interchange* and I' is said to be a *disjoint mate* of I. An *intercalate* is a latin interchange of size four.

Let L be Latin square of order n and $I \subseteq L$ be Latin interchange with disjoint mate denoted I'. Then $(L \setminus I) \cup I'$ is a Latin square of order n distinct from L. Consequently, the definition of a critical set implies that if C is a critical set then for each $(i,j;k) \in C$ there exists a Latin interchange $I_{(i,j;k)}$ such that $I_{(i,j;k)} \cap C = \{(i,j;k)\}$.

A critical set C of order n is called *t-uniform* if for each $(i,j;k) \in C$ there are precisely t distinct Latin squares of order n containing $C \setminus \{(i,j;k)\}$.

Note that using the definition of *power*, as defined in [7], we are saying that each element of C has power t.

Let P be a partial Latin square and assume the cell (i,j) of P is empty. The addition of a triple $(i,j;k)$ to the partial Latin square P is said to be *forced* (see [6, 2]) if either

(1) $\forall h \neq k$, $\exists z$ such that $(i,z;h) \in P$ or $(z,j;h) \in P$; or

(2) $\theta(i,j,k)$ satisfies 1 in $P_{\theta(1,2,3)}$ for some $\theta \in S_3$.

The concept of "forced" has been extended to semi-forced by Bedford and Whitehouse [2]. To state their definition we need the following notation.

Let P be a partial Latin square of order n defined on an element set X. Then A_P is an *array of alternatives* for P if

1. A_P is an $n \times n$ array ;
2. whenever the $(i,j)^{\text{th}}$ cell of P is filled, the $(i,j)^{\text{th}}$ cell of A_P is empty; and
3. whenever the $(i,j)^{\text{th}}$ cell of P is empty, the $(i,j)^{\text{th}}$ cell of A_P contains all the elements of X which do not appear in the i^{th} row or j^{th} column of P.

We denote the set of symbols in cell (i,j) of A_P by $A_P(i,j)$.

Let P be a partial Latin square. We will say that the element $k' \in A_P(i,j)$ is *forced out* of A_P if either:

(1) there exists $r > 0$ and $i_1, i_2, \ldots, i_r$ (all $\neq i$) with $k' \in A_P(i_1,j) \cup \ldots \cup A_P(i_r,j)$ and $|A_P(i_1,j) \cup \ldots \cup A_P(i_r,j)| = r$; or

(2) $\theta(i,j,k')$ satisfies 1 in $A_{P_{\theta(1,2,3)}}$ for some $\theta \in S_3$.

The reduced array of alternatives, RA_P, is the array obtained from A_P by successively removing elements which are forced out until it is not possible to force out any other elements. Then if $k \in RA_P(i,j)$, the addition of a triple $(i,j;k)$ to P is said to be *semi-forced* if either:

1. k is the only element in $RA_P(i,j)$; or
2. k occurs exactly once in either the i^{th} row or j^{th} column of RA_P.

Note that if a triple is forced it is also semi-forced.

A UC set U is *near-strong* UC to the Latin square L if there exists a sets of triples $U = S_1 \subset S_2 \subset \ldots \subset S_f = L$ such that each triple $t \in S_{v+1} \setminus S_v$ is semi-forced in S_v. Further, let P and Q be two partial Latin squares in L. The partial Latin square P is *near-strong completable* to Q if there exists a sequence of sets of triples $P = S_1 \subset S_2 \subset \ldots \subset S_f = Q$ such that each triple $t \in S_{v+1} \setminus S_v$ is semi-forced in S_v.

A critical set C is a *near-strong critical set* in L, if C is near-strong UC to L and no proper subset of C satisfies this property.

In [2] Bedford and Whitehouse prove the following lemma.

Lemma 3 Let P be a partial Latin square of order m that is UC to the Latin square M and let Q be a partial Latin square of order n that is UC to N. Let L be a Latin square to which $P \times Q$ completes. Suppose that the addition of the triple $(i,j;k)$ is semi-forced in P. Then L must contain a copy of N^k in block position (i,j).

A similar proof to that given in [2] for Lemma 3 leads to the following lemma which is crucial for the results in the next section.

Lemma 4 Let P be a partial Latin square of order m in the Latin square M and let Q be a partial Latin square of order n that is near-strong completable to a partial Latin square R in the Latin square N. Suppose that in the process of completing P to a Latin square the triple $(i,j;k)$ is semi-forced in P. Then in the process of completing $P \times Q$ to a Latin square the block position (i,j) in $P \times Q$ is semi-forced to contain a copy of R^k.

Let C be a near-strong critical set in L and let T be a partial Latin square in L. The critical set C is called T-uniform if for each $(i,j;k) \in C$

(i) there exists a partial Latin square $I_{(i,j;k)}$ in L isotopic to T such that $I_{(i,j;k)} \cap C = \{(i,j;k)\}$, and

(ii) $C \setminus \{(i,j;k)\}$ is near-strong completable to $L \setminus I_{(i,j;k)}$.

Once again this is related to the notion of the *influence* of a triple, as presented in [7]. For any two triples $(a,b;c)$ and $(d,e;f)$ in C, the sets $I_{(a,b;c)}$ and $I_{(d,e;f)}$ correspond to the influence of these triples and it is assumed that these partial latin squares are isotopic.

Lemma 5 *Let C be a T-uniform critical set in L. Then C is also t-uniform where,*

$$t = |\{M \mid M \text{ is a Latin square of order } n \text{ and } L \setminus T \subseteq M\}|.$$

Proof: Since for each $(i,j;k) \in C$ there exists a partial Latin square $I_{(i,j;k)}$ such that $I_{(i,j;k)}$ is isotopic to T, for any two triples $(a,b;c),(d,e;f) \in C$ there exist bijections θ, ϕ and ρ such that $I_{(d,e;f)} = \{(\theta(i),\phi(j);\rho(k)) \mid (i,j;k) \in I_{(a,b;c)}\}$. So if I is a latin interchange in $I_{(a,b;c)}$ it follows that $\{(\theta(i),\phi(j);\rho(k)) \mid (i,j;k) \in I\}$ is a latin interchange in $I_{(d,e;f)}$. Therefore there is a one-to-one correspondence between latin interchanges in $I_{(a,b;c)}$ and latin interchanges in $I_{(d,e;f)}$. On the other hand, if M is a latin square of order n containing $L \setminus I_{(a,b;c)}$ and different from L then $L \setminus M$ is a latin interchange in $I_{(a,b;c)}$. So the result follows. □

4 Theoretical results

In this section we study the completable product of T-uniform critical sets for certain partial Latin squares T.

Lemma 6 Let P be near-strong UC to a Latin square M of order m and let Q be near-strong UC to a Latin square N of order n. Let $(a,b;c) \in P$ and $(d,e;f) \in Q$ and assume that I and J are partial Latin squares in M and N, respectively, such that $P \setminus \{(a,b;c)\}$ is near-strong completable to $M \setminus I$ and $Q \setminus \{(d,e;f)\}$ is near-strong completable to $N \setminus J$. Then the partial Latin square $(P \times Q) \setminus \{\gamma\}$ is near-strong completable to

$$([(M \setminus I) \cup \{(a,b;c)\}] \times [(N \setminus J) \cup \{(d,e;f)\}]) \setminus \{\gamma\}$$

where $\gamma = ((a-1)n+d,(b-1)n+e;(c-1)n+f)$.

Proof: Consider the partial Latin square $P \setminus \{(a,b;c)\}$. Since $P \setminus \{(a,b;c)\}$ is near-strong completable to $M \setminus I$ there exists an empty cell, say (i,j), of $P \setminus \{(a,b;c)\}$ which is semi-forced to contain a specified symbol, say symbol k. So by Lemma 4 in the process of completing $(P \setminus \{(a,b;c)\}) \times (Q \setminus \{(d,e;f)\})$ to a Latin square the block position (i,j) in $(P \setminus \{(a,b;c)\}) \times (Q \setminus \{(d,e;f)\})$ is semi-forced to contain a copy of $(N \setminus J)^k$. Since $(P \setminus \{(a,b;c)\}) \times (Q \setminus \{(d,e;f)\}) \subseteq (P \times Q) \setminus \{\gamma\}$ it follows that in the process of completing $(P \times Q) \setminus \{\gamma\}$ to a Latin square the block position (i,j) is semi-forced to contain a copy of $(N \setminus J)^k$. Now since $Q^k \subseteq (N \setminus J)^k \cup \{((i-1)n+d, (j-1)n+e; (k-1)n+f)\}$, the block position (i,j) in $(P \times Q) \setminus \{\gamma\}$ contains $((i-1)n+d, (j-1)n+e; (k-1)n+f)$, and Q is near-strong completable to N we conclude that in the process of completing $(P \times Q) \setminus \{\gamma\}$ to a Latin square the block position (i,j) in $(P \times Q) \setminus \{\gamma\}$ is semi-forced to contain a copy of N^k. Continuing in this manner it can be shown that $(P \times Q) \setminus \{\gamma\}$ is near-strong completable to

$$[((M \setminus I) \cup \{(a,b;c)\}) \times Q] \setminus \{\gamma\}.$$

Note that every block position corresponding to a non–empty cell of $M \setminus I$ contains an isomorphic copy of N. So all these block positions are completely filled. Block position (a,b) is filled except for the triple $((a-1)n+d, (b-1)n+e; (c-1)n+f)$. All other block positions contain an isomorphic copy of Q.

By Lemma 2 we see that $(P \times Q) \setminus \{\gamma\}$ is isomorphic to $(Q \times P) \setminus \{\delta\}$ and $[((M \setminus I) \cup \{(a,b;c)\}) \times Q] \setminus \{\gamma\}$ (with respect to M and N) is isomorphic to $[Q \times ((M \setminus I) \cup \{(a,b;c)\})] \setminus \{\delta\}$ (with respect to N and M), where $\delta = ((d-1)m+a, (e-1)m+b; (f-1)m+c)$. So $(Q \times P) \setminus \{\delta\}$ is near-strong completable to $[Q \times ((M \setminus I) \cup \{(a,b;c)\})] \setminus \{\delta\}$.

Now since $Q \setminus \{(d,e;f)\}$ is near-strong completable to $N \setminus J$ there exists an empty cell, say (g,h) in $N \setminus Q$ which is semi-forced to contain a specific symbol, say symbol ℓ. So by Lemma 4 and an argument similar to that described above we see that in the process of completing $[Q \times ((M \setminus I) \cup \{(a,b;c)\})] \setminus \{\delta\}$ to a Latin square the block position (g,h) is semi-forced to contain a copy of M^ℓ. Continuing in this manner it can be shown that $(Q \times P) \setminus \{\delta\}$ is near-strong completable to $[((N \setminus J) \cup \{(d,e;f)\}) \times ((M \setminus I) \cup \{(a,b;c)\})] \setminus \{\delta\}$.

Once again Lemma 2 can be used to show that this partial Latin square is isomorphic to $[((M \setminus I) \cup \{(a,b;c)\}) \times ((N \setminus J) \cup \{(d,e;f)\})] \setminus \{\gamma\}$.

This completes the proof. □

Lemma 7 Let P be near-strong UC to a Latin square M of order m and let Q be near-strong UC to a Latin square N of order n. Let $(a,b;c) \in P$

and $(d,e;f) \notin Q$ and assume that I is a partial Latin square in M such that $P \setminus \{(a,b;c)\}$ is near-strong completable to $M \setminus I$. Then the partial Latin square $(P \times Q) \setminus \{\gamma\}$ is near-strong completable to

$$(M \setminus I) \times (N \setminus \{(d,e;f)\})$$

where $\gamma = ((a-1)n+d, (b-1)n+e; (c-1)n+f)$.

Proof: Consider the partial Latin square $P \setminus \{(a,b;c)\}$. Since $P \setminus \{(a,b;c)\}$ is near-strong completable to $M \setminus I$ there exists an empty cell, say (i,j), of $P \setminus \{(a,b;c)\}$ which is semi-forced to contain a specified symbol, say symbol k. So by Lemma 4 in the process of completing $(P \setminus \{(a,b;c)\}) \times Q$ to a Latin square the block position (i,j) in $(P \setminus \{(a,b;c)\}) \times Q$ is semi-forced to contain a copy of N^k. Since $(P \setminus \{(a,b;c)\}) \times Q \subseteq (P \times Q) \setminus \{\gamma\}$ it follows that in the process of completing $(P \times Q) \setminus \{\gamma\}$ to a Latin square the block position (i,j) is semi-forced to contain a copy of N^k. Continuing in this manner it can be shown that $(P \times Q) \setminus \{\gamma\}$ is near-strong completable to $[((M \setminus I) \cup \{(a,b;c)\}) \times Q] \setminus \{\gamma\}$.

By Lemma 2 we see that $(P \times Q) \setminus \{\gamma\}$ is isomorphic to $(Q \times P) \setminus \{\delta\}$ and $[((M \setminus I) \cup \{(a,b;c)\}) \times Q] \setminus \{\gamma\}$ is isomorphic to $[Q \times ((M \setminus I) \cup \{(a,b;c)\})] \setminus \{\delta\}$, where $\delta = ((d-1)m+a, (e-1)m+b; (f-1)m+c)$. So $(Q \times P) \setminus \{\delta\}$ is near-strong completable to $[Q \times ((M \setminus I) \cup \{(a,b;c)\})] \setminus \{\delta\}$.

Note that every block position corresponding to a non–empty cell of Q contains an isomorphic copy of M. So all these block positions are completely filled. Now since Q is near-strong completable to N there exists an empty cell, say (g,h) in $N \setminus Q$ which is semi-forced to contain a specific symbol, say symbol ℓ. By Lemma 4 and an argument similar to that described in Lemma 6, if $(g,h) \neq (d,e)$ we see that in the process of completing $[Q \times ((M \setminus I) \cup \{(a,b;c)\})] \setminus \{\delta\}$ to a Latin square the block position (g,h) is semi-forced to contain a copy of M^ℓ. If $(g,h) = (d,e)$ then the block position (g,h) in $[Q \times ((M \setminus I) \cup \{(a,b;c)\})] \setminus \{\delta\}$ is semi-forced to contain a Latin subsquare which contains $(P \setminus \{(a,b;c)\})^\ell$ and is based on the set of symbols $(\ell-1)m+1, (\ell-1)m+2, \ldots, (\ell-1)m+m$. Therefore it will contain a copy of $(M \setminus I)^\ell$. Continuing in this manner it can be shown that $(Q \times P) \setminus \{\delta\}$ is near-strong completable to $[((N \setminus \{(d,e;f)\}) \times ((M \setminus I) \cup \{(a,b;c)\})] \setminus \{\delta\}$. We also note that

$$[((N \setminus \{(d,e;f)\}) \times ((M \setminus I) \cup \{(a,b;c)\})] \setminus \{\delta\} = (N \setminus \{(d,e;f)\}) \times (M \setminus I).$$

Once again Lemma 2 can be used to show that this partial Latin square is isomorphic to $(M \setminus I) \times (N \setminus \{(d,e;f)\})$.

This completes the proof. □

Lemma 8 Let P be near-strong UC to a Latin square M of order m and let Q be near-strong UC to a Latin square N of order n. Let $(a,b;c) \notin P$ and $(d,e;f) \in Q$ and assume that J is a partial Latin square in N such $Q \setminus \{(d,e;f)\}$ is near-strong completable to $N \setminus J$. Then the partial Latin square $(P \times Q) \setminus \{\gamma\}$ is near-strong completable to

$$(M \setminus \{(a,b;c)\}) \times (N \setminus J)$$

where $\gamma = ((a-1)n+d, (b-1)n+e; (c-1)n+f)$.

Proof: First by Lemma 7 $(Q \times P) \setminus \{\delta\}$ is near-strong completable to

$$(N \setminus J) \times (M \setminus \{(a,b;c)\})$$

where $\delta = ((d-1)n+a, (e-1)n+b; (f-1)n+c)$. Now by Lemma 2 $(Q \times P) \setminus \{\delta\}$ is isomorphic to $(P \times Q) \setminus \{\gamma\}$ and $(N \setminus J) \times (M \setminus \{(a,b;c)\})$ is isomorphic to $(M \setminus \{(a,b;c)\}) \times (N \setminus J)$. So the result follows. □

The proof of the following lemma is straightforward and we leave that for the reader.

Lemma 9 Consider the following partial Latin squares of order four.

$R =$

	2	3	
2	1		
3		1	

$S =$

	2	3	
2	1	4	3
3	4	1	2
	3	2	

Then R is near-strong completable to S.

Theorem 10 Let P and Q be T-uniform critical sets in Latin squares M and N, respectively, where T is an intercalate. Then $P \times Q$ is a T-uniform critical set in $M \times N$.

Proof: First since P and Q are near-strong critical sets in M and in N, respectively, it follows that $P \times Q$ is near-strong UC in $M \times N$ (see [2]). Now we prove for each $(i,j;k) \in (P \times Q)$ there exists an intercalate $I_{(i,j;k)}$ such that $(P \times Q) \setminus \{(i,j;k)\}$ is near-strong completable to $(M \times N) \setminus I_{(i,j;k)}$.

Case 1: Let $(a,b;c) \in P$ and $(d,e;f) \in Q$. By the assumptions there exist intercalates

$$\begin{aligned} I &= \{(a,b;c),(a,b';c'),(a',b;c'),(a',b';c)\}, \text{ and} \\ J &= \{(d,e;f),(d,e';f'),(d',e;f'),(d',e';f)\} \end{aligned}$$

in M and N, respectively, such that $P\setminus\{(a,b;c)\}$ is near-strong completable to $M\setminus I$ and $Q\setminus\{(d,e;f)\}$ is near-strong completable to $N\setminus J$. By Lemma 6, $(P\times Q)\setminus\{\gamma\}$ is near-strong completable to

$$\chi=[((M\setminus I)\cup\{(a,b;c)\})\times((N\setminus J)\cup\{(d,e;f)\})]\setminus\{\gamma\},$$

where $\gamma=((a-1)n+d,(b-1)n+e;(c-1)n+f)$. It will be shown that in χ there are only 10 empty cells. The empty cells must occur in block positions (a,b), (a,b'), (a',b) or (a',b'). So the set of empty cells must be a subset of the sixteen cells

$$\begin{aligned}R' &= \{((x-1)n+y,(z-1)n+w)\mid x\in\{a,a'\},\ y\in\{d,d'\},\\ &\quad z\in\{b,b'\},\ w\in\{e,e'\}\}\end{aligned}$$

in χ. But we know cells $((a-1)n+d,(b-1)n+e')$, $((a-1)n+d',(b-1)n+e)$, $((a-1)n+d',(b-1)n+e')$, $((a'-1)n+d,(b-1)n+e)$, $((a-1)n+d,(b'-1)n+e)$, $((a'-1)n+d,(b'-1)n+e)$ are all filled. Hence ten of the cells of R' are empty in χ and so R' forms a partial Latin square isotopic to the partial Latin square R given in Lemma 9. So by Lemma 9 of the ten empty cells six are semi-forced. The four unforced cells form an intercalate in $M\times N$.

Case 2: Let $(a,b;c)\in P$ and $(d,e;f)\notin Q$. By the assumptions there exists an intercalate I in M such that $P\setminus\{(a,b;c)\}$ is near-strong completable to $M\setminus I$. So by Lemma 7 $(P\times Q)\setminus\{\gamma\}$ is near-strong completable to $(M\setminus I)\times(N\setminus\{(d,e;f)\})$. By Lemma 2 this partial latin square is isomorphic to $(N\setminus\{(d,e;f)\})\times(M\setminus I)$. In this partial latin square every block position $(i,j)\neq(d,e)$ contains an isomorphic copy of M and the block position (d,e) contains an isomorphic copy of $M\setminus I$. So in partial latin square $(M\setminus I)\times(N\setminus\{(d,e;f)\})$ there are only four empty cells and these cells form an intercalate in $M\times N$.

Case 3: Let $(a,b;c)\notin P$ and $(d,e;f)\in Q$. By the assumptions there exists an intercalate J in N such that $Q\setminus\{(d,e;f)\}$ is near-strong completable to $N\setminus J$. So by Lemma 8 $(P\times Q)\setminus\{\gamma\}$ is near-strong completable to $(M\setminus\{(a,b;c)\})\times(N\setminus J)$. In this partial Latin square there are only four empty cells and these cells form an intercalate in $M\times N$.

This completes the proof. □

Lemma 11 Let $2\leq n\leq 6$ and let T be an intercalate. Then the only T-uniform critical sets of order n are the trivial critical set of order 2 and the critical sets 4.2.1, 4.2.2, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6 and 6.7.3 listed in Section 5.

Proof: See Section 5. □

The other 2-uniform critical sets listed in Section 3 are not T-uniform for any T. So there are 2-uniform critical sets which are not T-uniform for any T.

Applying Theorem 10 and Lemma 11 we obtain the following result.

Corollary 12 There exist infinite families of T-uniform critical sets, where T is an intercalate. Therefore, there exist infinite families of 2-uniform critical sets.

Lemma 13 The completable product $S \times S$ is a T-uniform (hence a 4-uniform) critical set in $L \times L$, where

$L =$

1	2	3
2	3	1
3	1	2

$S =$

1		
	3	

$T =$

	2	3
2	3	1
3	1	2

Proof: First note that S is a T-uniform in L. Moreover, by [2] $S \times S$ is near-strong UC to $L \times L$. Now we prove that for each $(i, j; k) \in (S \times S)$ there is a partial Latin square $I_{(i,j;k)}$ in $L \times L$ and isotopic to T such that $(S \times S) \setminus \{(i, j; k)\}$ is near-strong completable to $(L \times L) \setminus I_{(i,j;k)}$. Consider $(S \times S) \setminus \{(1, 1; 1)\}$. It is straightforward to see that $(S \times S) \setminus \{(1, 1; 1)\}$ is near-strong completable to

	2	3	4		6	7	8	
2	3	1	5	6	4	8	9	7
3	1	2	6	4	5	9	7	8
4	5	6	7	8	9	1	2	3
	6	4	8	9	7	2	3	
6	4	5	9	7	8	3	1	2
7	8	9	1	2	3	4	5	6
8	9	7	2	3	1	5	6	4
	7	8	3		2	6	4	

This is $(L \times L) \setminus I_{(1,1;1)}$, where

$$I_{(1,1;1)} = \{(1, 1; 1), (1, 5; 5), (1, 9; 9), (5, 1; 5), (5, 9; 1), (9, 1; 9), (9, 5; 1), (9, 9; 5)\}.$$

Note that $I_{(1,1;1)}$ is isotopic to T.

An argument similar to that described above can be applied for the triples $(2, 2; 3)$, $(4, 4; 7)$ and $(5, 5, 9)$ of $S \times S$.

The other triples of $S \times S$ are of the form $(3(a-1)+d, 3(b-1)+e; 3(c-1)+f)$ where $(a,b;c) \in S$ and $(d,e;f) \notin S$ or $(a,b;c) \notin S$ and $(d,e;f) \in S$. The reader may apply Lemma 7 and Lemma 8, respectively, for these two cases. □

Theorem 14 Let P and Q be T-uniform critical sets in Latin squares M and N, respectively, where T is as in Lemma 13. Then $P \times Q$ is a T-uniform critical set in $M \times N$.

Proof: First since P and Q are near-strong critical sets in M and in N, respectively, it follows that $P \times Q$ is near-strong UC to $M \times N$ (see [2]).

We now prove that for each $(i,j;k) \in (P \times Q)$ there exists a partial Latin square $I_{(i,j;k)}$, isotopic to T, in $M \times N$ such that $(P \times Q) \setminus \{(i,j;k)\}$ is near-strong completable to $(M \times N) \setminus I_{(i,j;k)}$.

Case 1: Let $(a,b;c) \in P$ and $(d,e;f) \in Q$. By the assumptions there exist partial Latin squares I and J, both isotopic to T, in M and N, respectively, such that $P \setminus \{(a,b;c)\}$ is near-strong completable to $M \setminus I$ and $Q \setminus \{(d,e;f)\}$ is near-strong completable to $N \setminus J$. By Lemma 6 $(P \times Q) \setminus \{\gamma\}$ is near-strong completable to

$$\chi = [((M \setminus I) \cup \{(a,b;c)\}) \times ((N \setminus J) \cup \{(d,e;f)\})] \setminus \{\gamma\},$$

where $\gamma = ((a-1)n+d, (b-1)n+e; (c-1)n+f)$. It is straightforward to verify that $\chi \cup \{\gamma\}$ contains a partial Latin subsquare isotopic to $S \times S$, where S is as in Lemma 13. Moreover, all the empty cells of χ are contained in this partial Latin subsquare. Now the result follows by Lemma 13.

Case 2: Let $(a,b;c) \in P$ and $(d,e;f) \notin Q$. By the assumptions there exists a partial Latin square I in M, isotopic to T, such that $P \setminus \{(a,b;c)\}$ is near-strong completable to $M \setminus I$. So by Lemma 7 $(P \times Q) \setminus \{\gamma\}$ is near-strong completable to $(M \setminus I) \times (N \setminus \{(d,e;f)\})$. By Lemma 2, this partial latin square is isomorphic to $(N \setminus \{(d,e;f)\}) \times (M \setminus I)$. Clearly, the cells

$$\{((d-1)m+i, (e-1)m+j) \mid (i,j;k) \in I\}$$

form a partial latin square isotopic to T in $N \times M$. Now since $(N \setminus \{(d,e;f)\}) \times (M \setminus I)$ is isomorphic to $(M \setminus I) \times (N \setminus \{(d,e;f)\})$ the result follows.

Case 3: Let $(a,b;c) \notin P$ and $(d,e;f) \in Q$. By the assumptions there exists a partial Latin square J in N, isotopic to T, such that $Q \setminus \{(d,e;f)\}$

is near-strong completable to $N \setminus J$. So by Lemma 8 $(P \times Q) \setminus \{\gamma\}$, is near-strong completable to $(M \setminus \{(a, b; c)\}) \times (N \setminus J)$. Clearly, the cells

$$\{((a-1)m + d, (b-1)m + e) \mid (d, e; f) \in J\}$$

form a partial Latin square isotopic to T in $M \times N$.

This completes the proof. □

One can apply Lemma 13 and Theorem 14 to generate infinite families of 4-uniform critical sets as follows.

Corollary 15 Let L_1 and S_1 be the Latin square L and the critical set S given in Lemma 13, respectively. For $n \geq 2$ we define $L_n = L_1 \times L_{n-1}$ and $S_n = S_1 \times S_{n-1}$ (with respect to L_1 and L_{n-1}). Then S_n is a T-uniform (hence 4-uniform) critical set of order 3^n in L_n for all $n \geq 1$, where T is as given in Lemma 13.

5 Computational results

The authors of [1] found all the critical sets of different sizes in the Latin squares of order at most six. They also counted the number of main and isotopy classes of these critical sets and classified critical sets from the main classes into various "strengths". Using computer programs we examined these main classes and found all the possible m-uniform and T-uniform critical sets of order not larger than six. Here we list these critical sets.

The only T-uniform critical sets of order $2 \leq n \leq 6$, where T is an intercalate, are the trivial critical set of order 2 and the critical sets 4.2.1, 4.2.2, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6 and 6.7.3.

The only T-uniform critical set of order $2 \leq n \leq 6$, where T is as in Lemma 13, is the critical set 3.1.2.

5.1 Latin squares of order 3

There is only one main class for Latin squares of order three. The critical set 3.1.1 is 2-uniform and the critical set 3.1.2 is 4-uniform. Up to isotopism there is no other m-uniform critical set of order 3, for any m.

1	2	3
2	3	1
3	1	2

3.1

1	2	
2		

3.1.1

1		
	3	

3.1.2

5.2 Latin squares of order 4

There are two main classes for Latin squares of order four.

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

4.1

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

4.2

There does not exist any m-uniform critical set in Latin square labelled 4.1.

The following 2-uniform critical sets are in the Latin square labelled 4.2. Up to isotopism there is no other m-uniform critical set in the Latin square labelled 4.2.

1	2		
		4	3
		1	
	3		

4.2.1

1	2	3	
2	1		
3		1	

4.2.2

5.3 Latin squares of order 5

There are two main classes for Latin squares of order five.

1	2	3	4	5
2	3	4	5	1
3	4	5	1	2
4	5	1	2	3
5	1	2	3	4

5.1

1	2	3	4	5
2	1	4	5	3
3	4	5	1	2
4	5	2	3	1
5	3	1	2	4

5.2

There is no uniform critical set in the Latin square labelled 5.2.

Up to isotopism the following 32-uniform critical set is the only uniform critical set in the Latin square labelled 5.1.

1	2			
2				
				3
			3	4

5.1.1

5.4 Latin squares of order 6

There are twelve main classes for Latin squares of order six.

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

6.1

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

6.2

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

6.3

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

6.4

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

6.5

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

6.6

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

6.7

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

6.8

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

6.9

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

6.10

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

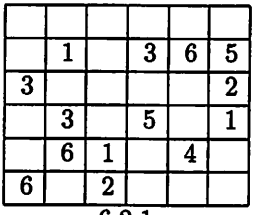
6.11

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

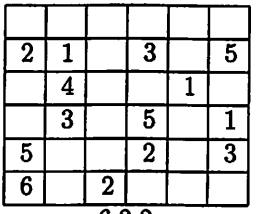
6.12

There is no uniform critical set in the Latin squares labelled 6.1, 6.8, 6.9, 6.10, 6.11 and 6.12.

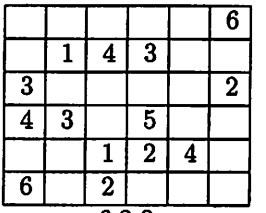
There are precisely ten (four of size 14 and six of size 15) uniform critical sets in the Latin square labelled 6.2. All are 2-uniform.



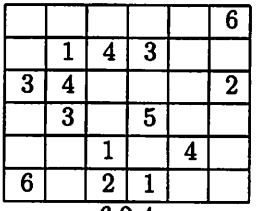
6.2.1



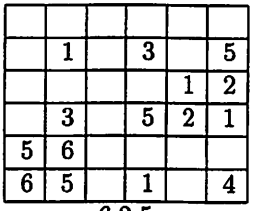
6.2.2



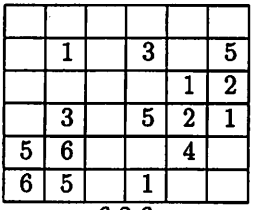
6.2.3



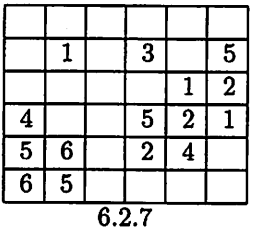
6.2.4



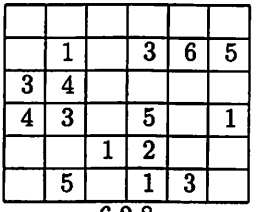
6.2.5



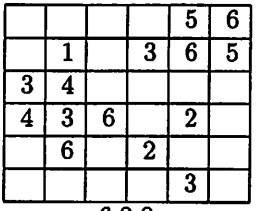
6.2.6



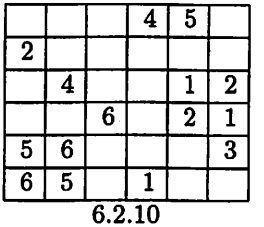
6.2.7



6.2.8



6.2.9



6.2.10

There are precisely ten (one of size 14, six of size 15 and three of size 16) uniform critical sets in the Latin square labelled 6.3. All are 2-uniform.

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

6.3.1

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

6.3.2

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

6.3.3

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

6.3.4

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

6.3.5

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

6.3.6

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

6.3.7

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

6.3.8

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

6.3.9

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

6.3.10

There are precisely three (all of size 14) uniform critical sets in the Latin square labelled 6.4. All are 2-uniform.

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

6.4.1

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

6.4.2

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

6.4.3

There is precisely one uniform critical sets in the Latin square labelled 6.5. This is of size 14 and it is 2-uniform.

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

6.5.1

There are precisely nineteen (all of size 15) uniform critical sets in the Latin square labelled 6.6. All are 2-uniform.

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

6.6.1

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

6.6.2

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

6.6.3

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

6.6.4

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

6.6.5

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

6.6.6

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

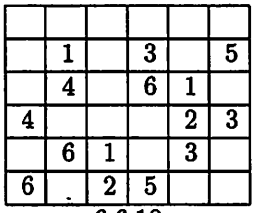
6.6.7

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

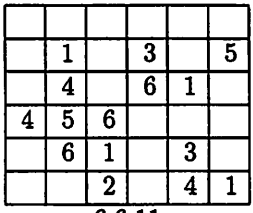
6.6.8

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

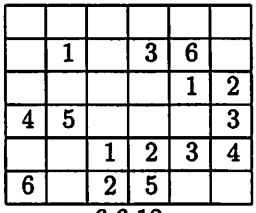
6.6.9



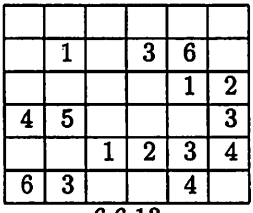
6.6.10



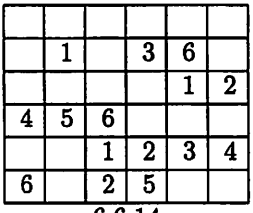
6.6.11



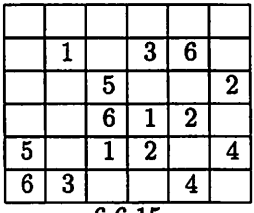
6.6.12



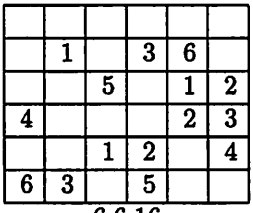
6.6.13



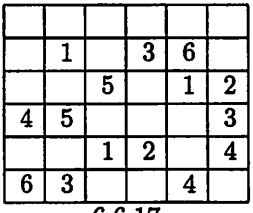
6.6.14



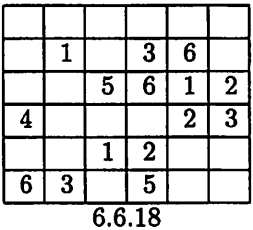
6.6.15



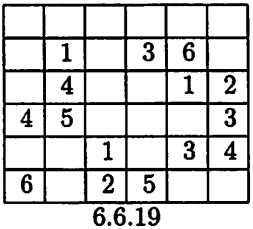
6.6.16



6.6.17

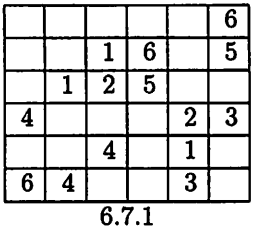


6.6.18

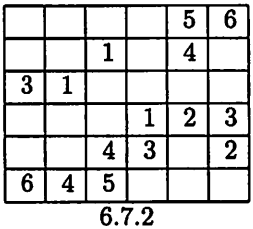


6.6.19

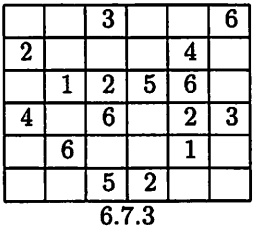
There are precisely three (two of size 15 and one of size 16) uniform critical sets in Latin square labelled 6.7. All are 2-uniform.



6.7.1



6.7.2



6.7.3

References

[1] P. Adams, R. Bean and A. Khodkar, *A census of critical sets in the Latin squares of order at most six*, (submitted).

[2] D. Bedford and D. Whitehouse, *Products of uniquely completable partial Latin squares* Utilitas Mathematica **58** (2000), 195–201.

[3] D. Curran and G.H.J. van Rees, *Critical sets in latin squares*, Proc. 8th Manitoba Conference on Numerical Mathematics and Computing, (Congressus Numerantium XXII), Utilitas Math. Pub., Winnipeg, 1978, 165–168.

[4] L.F. Fitina, Jennifer Seberry and Ghulam R. Chaudhry, *Back circulant Latin squares and the influence of a set*, The Australasian Journal of Combinatorics **20** (1999), 163–180.

[5] R.A.H. Gower, *Critical sets in products of Latin squares*, Ars Combinatoria **55** (2000), 293–317.

[6] A.D. Keedwell. *What is the size of the smallest Latin square for which a weakly completable critical set of cells exists?*, Ars Combinatoria **51** (1999), 97–104.

[7] Jennifer Seberry and Anne Penfold Street, *Strongbox Secured Secret Sharing Schemes*, Utilitas Mathematica **57** (2000), 147–163,

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