Critical Sets For Latin Squares of order 7

Diane Donovan and Adelle Howse

Center for Combinatorics,
Mathematics Department,
The University of Queensland,
Queensland, 4072, Australia

Abstract

This paper provides a general method for finding a critical set for any latin square of order n. In particular, the algorithm is applied to all main classes of latin squares of order seven, thus producing a critical set for each latin square of order seven.

1. Introduction

A *latin square* of order n is an $n \times n$ array with entries chosen from a set N, of size n such that each element of N occurs precisely once in each row and column. Note that the multiplication table of any quasigroup with its headline and sideline removed forms a latin square.

Latin squares have historically been used in experimental design and more recently in cryptographic algorithms. In cryptography for example, latin squares may be encorporated in the design of encryption algorithms, such as DES (Data Encryption Standard). In [?] Carter, Dawson and Nielsen propose a variation for DES which replaces a binary bit-wise operation with a latin square. Further, they show that the resulting cipher is more resistant to differential and linear cryptanalysis than DES. In addition, message authentication codes [?] have been devised that are based on latin squares. The downfall of many of these systems is the implementation cost resulting from the need to store a large number of latin squares of significant order. Storage costs may be reduced if instead of retaining the entire latin square, only a minimal amount of vital information is kept from which the latin square can be reconstructed. It is pertinent to consider partial latin squares for this purpose.

A *partial latin square P*, of order n, is an $n \times n$ array where the entries in non-empty positions are chosen from a set N, in such a way that each element of N occurs at most once in each row and at most once in each column of the array. A *critical set* is a partial latin square which is contained in precisely one latin square, and for which the removal of any entry destroys this property. Critical sets attracted interest after they were introduced by Nelder in 1977 in [?]. Subsequently however, the determination of properties about them has appeared to be a complex problem. The known algorithms for producing critical sets for a given latin square, [?], are computationally intense and until now it has proved difficult to investigate critical sets generally for latin squares of order greater than 6.

This paper documents new and interesting ideas which significantly reduce the complexity of search algorithms. Consequently, examples of critical sets for all 147 main classes of latin squares of order 7 have been found. Arising from these ideas is the development of a procedure for constructing general families of critical sets. Consequently, the existence of new families of critical sets is documented in Section 4. The methods presented are the first to establish critical set constructions in latin squares other than the cyclic group or in latin squares that are partitionable into cyclic subsquares. Further, they provide a critical set of size 28 in a latin square of order 10, filling a hole in the classification produced in [**?**,]

The main results of this paper, are Theorem 1 in Section 3 and the general constructions given in Theorems 2, 3 and 4 in Section 4. At the end of the paper a table provides an example of a critical set for each main class of latin squares of order 7. Before tackling these however, some background information is needed.

2. Definitions

In what follows the set N is assumed to be $\{0, 1, \ldots, n-1\}$. Further, the representation of a latin square with a set of ordered triples $\{(i, j; k) \mid$ element k occurs in position $(i, j) \}$ will be used often.

Let $L_1 = \{(i_1, j_1; k_1) \mid i_1, j_1, k_1 \in N\}$ and $L_2 = \{(i_2, j_2; k_2) \mid i_2, j_2, k_2 \in N\}$ be two latin squares of order n. Then L_1 is said to be isotopic to L_2 if there exists permutations α, β and γ such that $L_2 = \{(i_1\alpha, j_1\beta; k_1\gamma) \mid (i_1, j_1; k_1) \in L_1\}$. In this case L_2 is said to be an *isotope* of L_1. If $\alpha = \beta = \gamma$ then L_1 is said to be *isomorphic* to L_2.

Each latin square $L = \{(i, j; k) \mid i, j, k \in N\}$ has five *conjugates* associated with it. Conjugates result by interchanging rows with columns and/or elements of L, and these are:

- $L^* = \{(j, i; k) \mid (i, j; k) \in L\}$;

- $^{-1}L = \{(k, j; i) \mid (i, j; k) \in L\}$;

- $L^{-1} = \{(i, k; j) \mid (i, j; k) \in L\}$;

- $^{-1}(L^{-1}) = \{(j, k; i) \mid (i, j; k) \in L\}$;

- $(^{-1}L)^{-1} = \{(k, i; j) \mid (i, j; k) \in L\}$.

For every latin square L of order n, the *main class* of L consists of all latin squares M where either M is a conjugate of L and/or M is isotopic to L. For more details on latin squares, isotopisms and conjugates, see [**?**].

Let P be a partial latin square of order n. Then $|P|$ is said to be the *size* of the partial latin square and the set of positions $\mathcal{S}_P = \{(i, j) \mid (i, j; k) \in P, \exists k \in N\}$ is said to determine the *shape* of P. Let P and P' be two partial latin squares of the same order, with the same size and shape. Then P are P' are said to be *mutually balanced* if the entries in each row (and column) of P are the same as those in the corresponding row

2

(and column) of P'. They are said to be *disjoint* if no position in P' contains the same entry as the corresponding position in P. A *latin interchange* I is a partial latin square for which there exists another partial latin square I', of the same order, size and shape with the property that I and I' are disjoint and mutually balanced. The partial latin square I' is said to be a *disjoint mate* of I. See Table 1 for an example.

$$
\begin{array}{ccc}
0 & * & 2 \\
2 & 3 & 4 \\
3 & 4 & 0
\end{array}
\qquad\qquad
\begin{array}{ccc}
2 & * & 0 \\
3 & 4 & 2 \\
0 & 3 & 4
\end{array}
$$

Table 1: A latin interchange of size 8 with its disjoint mate.

If a latin interchange contains precisely two entries in each non-empty row and column, then the latin interchange is said to be a *cycle*, see [?]. An *intercalate* is an example of a cycle of size four, and this is the smallest possible size for a latin interchange.

Lemma 1: *Suppose L is a latin square of order n, and $I, J \subset L$ are latin interchanges satisfying the following conditions.*

(i) *J is of the form $\{(r_1, c_1; k_1), (r_1, c_2; k_2), (r_2, c_1; k_2), (r_2, c_2; k_3), (r_3, c_1; k_3), (r_3, c_2; k_4),$ $\ldots, (r_s, c_1; k_s), (r_s, c_2; k_1)\}$;*

(ii) *$I \cap J = \{(r_1, c_1; k_1), (r_t, c_1; k_t)\}$, for some t, where $1 < t \leq s$, and*

(iii) *$\{(r_1, c_1; k_t), (r_t, c_1; k_1)\} \subset I'$, the disjoint mate of I.*

Then the latin square $L' = (L \setminus I) \cup I'$ contains two latin interchanges $J1$ and $J2$, such that $\mathcal{S}_{J1} \cap \mathcal{S}_{J2} = \emptyset$ and $\mathcal{S}_{J1}, \mathcal{S}_{J2} \subset \mathcal{S}_J$. (Note that requirement (iii) above is always satisfied if $|\{i \mid (r_i, c_1) \in \mathcal{S}_I\}| = 2$.)

Proof. Since $(r_1, c_1; k_t), (r_t, c_1; k_1) \in I' \subset L'$ it follows that $\{(r_1, c_1; k_t), (r_1, c_2; k_2),$ $(r_2, c_1; k_2), (r_2, c_2; k_3), \ldots, (r_{t-1}, c_1; k_{t-1}), (r_{t-1}, c_2; k_t)\} \subset L'$ and $\{(r_t, c_1; k_1), (r_t, c_2; k_{t+1}),$ $(r_{t+1}, c_1; k_{t+1}), (r_{t+1}, c_2; k_{t+2}), \ldots, (r_s, c_1; k_s), (r_s, c_2; k_1)\} \subset L'$ are two disjoint latin interchanges in $(L \setminus I) \cup I'$ satisfying the required properties.

Corollary 1: Suppose L is a latin square of order n, and $I, J \subset L$ are latin interchanges satisfying the following conditions.

(i) *J is a cycle of size $2s$ on the elements $k_1, k_2 \in N$;*

(ii) *$I \cap J = \{(r_1, c_1; k_1), (r_t, c_t; k_1)\}$, for some t where $1 < t \leq s$ and*

(iii) *$(r_1, c_t; k_1), (r_t, c_1; k_1) \in I'$, the disjoint mate of I.*

Then the latin square $L' = (L \setminus I) \cup I'$ contains two cycles $J1$ and $J2$, such that $\mathcal{S}_{J1} \cap \mathcal{S}_{J2} = \emptyset$ and $(\mathcal{S}_{J1} \setminus \{(r_1, c_t)\}) \subset (\mathcal{S}_J \setminus \{(r_1, c_1)\})$ and $(\mathcal{S}_{J2} \setminus \{(r_t, c_1)\}) \subset (\mathcal{S}_J \setminus \{(r_t, c_t)\})$.

3

Proof. This result is obtained by using the conjugate J^{-1} of the latin interchange, J, given in Lemma 1. This then gives $J1 = \{(r_1, c_2; k_2), (r_1, c_t; k_1)\} \cup \{(r_i, c_i; k_1), (r_i, c_{i+1}; k_2) \mid 2 \leq i \leq t-1\}$ and $J2 = \{(r_t, c_1; k_1), (r_t, c_{t+1}; k_2), (r_s, c_s; k_1), (r_s, c_1; k_2)\} \cup \{(r_i, c_i; k_1), (r_i, c_{i+1}; k_2) \mid t+1 \leq i \leq s-1\}$.

A partial latin square $C = \{(i, j; k) \mid i, j, k \in N\}$, of order n is said to be *uniquely completable* (UC) (or to have *unique completion*) if there is precisely one latin square L of order n that has element k in position (i, j) for each $(i, j; k) \in C$. Note that any critical set is UC. A *minimal critical set* is a critical set for L of smallest possible size and hence is also the smallest UC set for L. An example is presented in Table 2. If C is a UC set, a triple $(i, j; k) \in L \setminus C$ will be said to be *forced*, if either $\forall h \neq i$, $\exists z$ such that $(h, j; z)$ or $(h, z; k) \in C$, or $\forall h \neq j$, $\exists z$ such that $(z, h; k)$ or $(i, h; z) \in C$, or $\forall h \neq k$, $\exists z$ such that $(i, z; h)$ or $(z, j; h) \in C$.

0	1	2	*	*	*	*
1	2	*	*	*	*	*
2	*	*	*	*	*	*
*	*	*	*	*	*	*
*	*	*	*	*	*	3
*	*	*	*	*	3	4
*	*	*	*	3	4	5

Table 2: A critical set of size 12 for a latin square of order 7.

Lemma 2: *Let $C \subset L$ denote a critical set for $L = \{(i, j; k) \mid i, j, k \in N\}$. If α, β, γ are permutations of N and $L' = \{(i\alpha, j\beta; k\gamma) \mid (i, j; k) \in L\}$ is an isotope of L, then $C' = \{(i\alpha, j\beta; k\gamma) \mid (i, j; k) \in C\}$ is a critical set for L'. Similarly, if L^c is some conjugate of L then the set C^c, the relevant conjugate of C, will be a critical set for L^c.*

Lemma 2 implies that if a critical set C is known for a latin square L, then a critical set for any latin square in the same main class as L can also be produced.

Lemma 3: *A partial latin square $C \subset L$, of size s and order n, is a critical set for a latin square L if and only if the following hold:*

  (i) C contains an element of every latin interchange that occurs in L;

  (ii) for each $(i, j; k) \in C$, there exists a latin interchange I_r in L so that $I_r \cap C = \{(i, j; k)\}$.

Proof.

  (i) If C does not contain an element from some latin interchange I, where I has the disjoint mate I', then C is also a partial latin square of $L' = (L \setminus I) \cup I'$. Hence C is not UC.

4

(ii) If no such latin interchange I_r can be found, then the position $(i, j; k)$ may be deleted from C and $C \setminus \{(i, j; k)\}$ will still be UC and thus a critical set for L.

If $N = \{0, 1, \ldots, n-1\}$ then a *back circulant* latin square has the integer $i + j \,(\text{mod } n)$ in position (i, j). The back circulant latin square of order n will be denoted by BC_n. The critical set in Table 2 completes to BC_7.

In 1978, Curran and van Rees [?] produced a UC set for BC_n of size $\frac{n^2-1}{4}$ for odd values of n. For even n, they produced a critical set of size $\frac{n^2}{4}$. These findings have been expanded on to provide the following general result.

Lemma 4. *(Donovan and Cooper [?].) The partial latin square*

$$
\begin{aligned}
S \;=\; & \{(i, j; i + j(\text{mod } n)) \mid 0 \leq i \leq a,\ 0 \leq j \leq a - i\} \cup \\
& \{(i, j; i + j(\text{mod } n)) \mid a + 2 \leq i \leq n - 1,\ n + 1 + a - i \leq j \leq n - 1\},
\end{aligned}
$$

where $\frac{n-3}{2} \leq a \leq n - 2$, is a critical set for BC_n.

3. Main Result

In this paper, techniques for constructing critical sets are given and critical sets are produced for all latin squares of order seven. This is accomplished by using the result of Lemma 2 and also by utilizing the following.

Theorem 1: If C is a critical set in a latin square L of order n, and I is a latin interchange in L (with disjoint mate I'), then the set $C' = (C \setminus I) \cup I'$ is a UC set for $L' = (L \setminus I) \cup I'$.

Proof. Clearly $C' = (C \setminus I) \cup I' \subseteq L'$. Suppose that $C' = (C \setminus I) \cup I'$ does not have a unique completion to L'. Then there must exist a latin interchange J in L' where $J \cap C' = \emptyset$. Since $\mathcal{S}_C \subseteq \mathcal{S}_{C'}$, it follows that $J \cap C = \emptyset$. However, this contradicts Lemma 3, as C must contain an element of every latin interchange occurring in L.

Theorem 1 then provides us with a method for producing a critical set for every possible latin square of every order n. To see this, note that Lemma 4 provides a critical set, C, for the back circulant latin square (BC_n) for every value of n. Then for a given latin square L' of order n (in standard form), consider the set $I = \{(i, j; i+j) \mid (i, j; i+j) \notin L'\}$. That is, the set of positions in which BC_n and L' differ. This set of positions forms a latin interchange in BC_n, with corresponding disjoint mate, $I' = \{(i, j; k) \in L' \mid i + j \neq k\}$. From Theorem 1, the set $(C \setminus I) \cup I'$ is a UC set for L'. A critical set is embedded in every UC set. Hence, by removing elements sequentially, and testing for UC, a critical set is then found for L'. Using this method, we have identified a critical set for each of the 147 main classes of latin square, of order 7. The production of all the UC sets for each main class takes only seconds and the reduction, to a critical set, a further 22 minutes of CPU time on a Sun Ultra 220 machine. A representative of each main class is displayed at the end of the paper and the critical set produced for each is indicated with bold font. The largest critical set in this list is of size 19. Consequently, these results provide an upper bound, of 19, for the size of the minimal critical set for all latin squares of order 7.

5

The next lemma deals with the question of which elements of $(C \setminus I) \cap I'$ can be removed while still retaining the property of unique completion.

Lemma 5: Let C be a critical set in a latin square L of order n. Let $f = (i, j; k)$ be any initial element forced in the completion of C to L, and let I be a latin interchange, such that $(i, j; k) \in I$. Then, if I' denotes a disjoint mate of I and $(i, g; k) \in I'$ then the set $C' = (C \setminus I) \cup (I' \setminus (i, g; k))$ is a UC set for $L' = (L \setminus I) \cup I'$.

Proof. First suppose that element $(i, j; k)$ is forced by reason of $\forall h \neq j$, $\exists z$ such that $(i, h; z)$ or $(z, h; k) \in C$. Now note that if $(i, j; k)$ is forced in C, then for $h \neq j$, either column h contains element k or position (i, h) is filled. Then, if k occurred in column $h \neq g$ of I, k occurs in column h of I'. (Note that column j must contain k in I'.) If (i, h) was filled in I, $h \neq g$, then (i, h) will be filled in I' and also $(i, h) \in \mathcal{S}_{C'}$. For all other columns h, if k occurred in column h in C, it is unchanged and if (i, h) was filled, it will contain the same entry in $(C \setminus I) \cup (I' \setminus (i, g; k))$. Hence in all cases, it is impossible to place element k in any position of row i other than position (i, g).

An element $(i, j; k)$ may be forced for other reasons and the same argument applies in these cases.

Consequently $(i, g; k)$ is forced in the completion of C'. Now application of the proof of Theorem 1 establishes that $C' = (C \setminus I) \cup (I' \setminus (i, g; k))$ is a UC set for $L' = (L \setminus I) \cup I'$.

4. General Constructions

In Theorem 1 it was established that a UC set could easily be produced for any latin square, using the existence of a critical set in another latin square of the same order. It is then of interest to know what the size of the underlying critical sets might be. The following investigates this concept. In what follows, addition and subtraction is performed modulo n.

Theorem 2: When n is even and $n \geq 6$, there exist critical sets of size $\frac{n^2}{4} + 2$ and $\frac{n^2}{4} + 3$.

Proof. We shall begin by noting the following facts. When N has even order n, position (x, y) in the back circulant latin square BC_n, occurs in the intercalate $I_n = \{(x, y; x + y), (x, y + \frac{n}{2}; x + y + \frac{n}{2}), (x + \frac{n}{2}, y; x + y + \frac{n}{2}), (x + \frac{n}{2}, y + \frac{n}{2}; x + y)\}$. Thus there are precisely $\frac{n^2}{4}$ non-intersecting intercalates in BC_n, with each position (x, y) occurring in precisely one of these intercalates. In each case the set $L' = (BC_n \setminus I_n) \cup I'_n$, where I'_n is the disjoint mate of I_n, is a latin square of order n. From Lemma 4, with $a = \frac{n-3}{2}$, note that the set

$$
\begin{aligned}
C \ = \ & \{(i, j; i + j \pmod n) \mid 0 \leq i \leq \frac{n}{2} - 1, \ 0 \leq j \leq \frac{n}{2} - 1 - i\} \cup \\
& \{(i, j; i + j \pmod n) \mid \frac{n}{2} + 1 \leq i \leq n - 1, \ n + \frac{n}{2} - i \leq j \leq n - 1\},
\end{aligned}
$$

is a critical set for BC_n of size $\frac{n^2}{4}$.

By Theorem 1 the set $(C \setminus I_n) \cup I_n'$ has a unique completion. For all elements $(i, j; k) \in C \setminus I_n$ there exists an intercalate P such that $P \cap C = \{(i, j; k)\}$, and $P \cap I_n = \emptyset$. It follows that each element of $C \setminus I_n$ is necessary for unique completion. We shall now determine which elements of I_n' are necessary for UC.

Consider intercalates I_n, containing positions (x, y) in C. Due to the symmetry of BC_n and C, only positions (x, y) on or above the diagonal need consideration. For $0 \leq x \leq \lfloor \frac{n-2}{4} \rfloor$ and $x \leq y \leq \frac{n}{2} - 1 - x$, observe from Corollary 1, that L' contains two cycles on the elements $x + y + \frac{n}{2}$, $x + y + \frac{n}{2} + 1$. The cycle on rows $x + 1$ to $x + \frac{n}{2}$ has positions $\{(x + \frac{n}{2}, y + \frac{n}{2}), (x + \frac{n}{2}, y + 1), (x + i, y + \frac{n}{2} - i), (x + i, y + \frac{n}{2} - i + 1) \mid 1 \leq i \leq \frac{n}{2} - 1\}$. This cycle intersects $(C \setminus I_n) \cup I_n'$ in $(x + \frac{n}{2}, y + \frac{n}{2}; x + y + \frac{n}{2})$ alone. Similarly, provided both x and y are not equal to 0, Corollary 1, can be used to show that L' contains two cycles on the elements $x + y + \frac{n}{2}$, $x + y + \frac{n}{2} - 1$. Further, the cycle on rows x to $x + \frac{n}{2} - 1$ intersects $(C \setminus I_n) \cup I_n'$ in $(x, y; x + y + \frac{n}{2})$ alone. Note that in the completion of C, the element $(0, \frac{n}{2}; \frac{n}{2})$ is forced, and so when $x = 0$ and $y = 0$, by Lemma 5, $(C \setminus I_n) \cup (I_n' \setminus (0, 0; \frac{n}{2}))$ has a unique completion.

Finally, provided $(x, y; x + y) \neq (0, \frac{n}{2} - 1, \frac{n}{2} - 1)$ Lemma 1 gives a latin interchange on rows x to $x + \frac{n}{2} - 1$ and columns $y + \frac{n}{2}$ and $y + \frac{n}{2} + 1$, which intersects $(C \setminus I_n) \cup I_n'$ in $(x, y + \frac{n}{2}; x + y)$ alone. Note that in the completion of C, the element $\frac{n}{2} - 1$ is forced to occur in $(\frac{n}{2}, n - 1)$. Hence $x = 0$ and $y = \frac{n}{2} - 1$, by Lemma 5, $(C \setminus I_n) \cup (I_n' \setminus (0, n - 1; \frac{n}{2} - 1))$ has unique completion.

Consequently when $(x, y; x + y) \in \{(0, 0; 0), (0, \frac{n}{2} - 1; \frac{n}{2} - 1), (\frac{n}{2} - 1, 0; \frac{n}{2} - 1)\}$, the sets $(C \setminus I_n) \cup (I_n' \setminus (0, 0; \frac{n}{2}))$, $(C \setminus I_n) \cup (I_n' \setminus (0, n - 1; \frac{n}{2} - 1))$ and $(C \setminus I_n) \cup (I_n' \setminus (n - 1, 0; \frac{n}{2} - 1))$ respectively are examples of critical sets of size $\frac{n^2}{4} + 2$. For all other values of x and y in the range $0 \leq x \leq \frac{n}{2} - 1$ and $0 \leq y \leq \frac{n}{2} - 1 - x$, the sets $(C \setminus I_n) \cup I_n'$ are examples of critical sets of size $\frac{n^2}{4} + 3$.

A similar argument can be used to show that for $\frac{n}{2} + 1 \leq x \leq n - 1$ and $n + \frac{n}{2} - x \leq y \leq n - 1$ the set $(C \setminus I_n) \cup I_n'$ is also a critical set of size $\frac{n^2}{4} + 3$.

Corollary 2: When n is even, critical sets exist of sizes

1. $\frac{n^2}{4} + 3t$ for $t = 0, 1, 2, \ldots, w$, where $w = \begin{cases} \frac{n-2}{4} & \text{for } n \equiv 2 \, (\mathrm{mod} 4) \\ \frac{n-4}{4} & \text{for } n \equiv 0 \, (\mathrm{mod} 4) \end{cases}$;

2. $\frac{n^2}{4} + 2 + 3t$ for $t = 0, 1, 2, \ldots, w$, where $w = \begin{cases} \frac{n-6}{4} & \text{for } n \equiv 2 \, (\mathrm{mod} 4) \\ \frac{n-4}{4} & \text{for } n \equiv 0 \, (\mathrm{mod} 4) \end{cases}$;

3. $\frac{n^2}{4} + 4 + 3t$ for $t = 0, 1, 2, \ldots, w$, where $w = \begin{cases} \frac{n-6}{4} & \text{for } n \equiv 2 \, (\mathrm{mod} 4) \\ \frac{n-8}{4} & \text{for } n \equiv 0 \, (\mathrm{mod} 4) \end{cases}$.

Proof. The result applies by progressively interchanging intercalates that intersect with element $\frac{n}{2} - 1$ in C. The values of w then correspond to the number of times element $\frac{n}{2} - 1$ can be used. In particular, for the set of sizes in (1), select t distinct values of i where $1 \leq i \leq w$, and interchange the intercalates I_i that intersect $(2i - 1, \frac{n}{2} - 2i)$. For

each intercalate I_i, a new critical set C_i is produced where $C_i = (C_{i-1} \setminus I_i) \cup (I_i')$. Each intercalate I_i has positions $\{(2i-1, \frac{n}{2} - 2i), (2i-1, n - 2i), (2i + \frac{n}{2} - 1, \frac{n}{2} - 2i), (2i + \frac{n}{2} - 1, n - 2i)\}$ and hence is at least two rows and columns away from intercalate I_{i-1}. Each set C_i has size $|C_{i-1}| + 3$ and each element is still necessary in C_i, due to the following latin interchanges. The element in position $(2i-1, \frac{n}{2} - 2i)$ is necessary as it is the only element in C_i that intersects the latin interchange on rows $2i-1$ and $2i$ and columns $\frac{n}{2} - 2i$ to $n - 1 - 2i$. This latin interchange is the transpose of that described in Lemma 1. The element in position $(2i-1, n-2i)$ is necessary as it is the only element in C_i that intersects the latin interchange as per Lemma 1 on columns $n - 2i$ and $n - 2i + 1$ and rows $2i-1$ to $2i + \frac{n}{2} - 2$. Position $(2i + \frac{n}{2} - 1, \frac{n}{2} - 2i)$ occurs uniquely in the transpose of the latin interchange from Lemma 1 in rows $2i + \frac{n}{2} - 1$ and $2i + \frac{n}{2}$ and columns $\frac{n}{2} - 2i$ to $n - 1 - 2i$. Finally, position $(2i + \frac{n}{2} - 1, n - 2i)$ occurs uniquely in the latin interchange from Lemma 1 in rows $2i$ through to $2i + \frac{n}{2} - 1$ and columns $n - 1 - 2i$ and $n - 2i$.

For the set of sizes in (2), this time use the latin interchange with $(x, y) = (0, \frac{n}{2} - 1)$ to produce a critical set of size $\frac{n^2}{4} + 2$. Then select t distinct values of i where $1 \leq i \leq w$, and interchange intercalates I_i which contain position $(2i, \frac{n-2}{2} - 2i)$. Again each new critical set C_i has size $|C_{i-1}| + 3$ and the relative latin interchanges as used in (1) ensures that all elements of C_i are necessary.

For the third set of sizes, use the two latin interchanges on $(0, \frac{n}{2} - 1)$ and $(\frac{n}{2} - 1, 0)$. This provides a critical set of size $\frac{n^2}{4} + 4$. Then select t values of i where $1 \leq i \leq w$, and interchange the intercalates that intersect $(2i, \frac{n-2}{2} - 2i)$. Again, the same argument as for (1) and (2) applies to the size of C_i and the result follows.

$\Box$

We shall now apply a similar technique to the back circulant latin squares of odd order.

Theorem 4: When n is odd, and $n \geq 5$, there exists a critical set of size $\frac{n^2 - 1}{4} + 2$.

Proof. Let

$$
\begin{aligned}
C &= \{(i, j; i + j) \mid 0 \leq i \leq \frac{n-3}{2}, 0 \leq j \leq \frac{n-3}{2} - i\} \\
&\cup \{(i, j; i + j) \mid \frac{n+1}{2} \leq i \leq n - 1, \frac{n-1}{2} - i \leq j \leq n - 1\}
\end{aligned}
$$

and $I = \{(0, 0; 0), (i, \frac{n-1}{2} - i; \frac{n-1}{2}), (i, \frac{n+1}{2} - i; \frac{n+1}{2}), (\frac{n-1}{2}, \frac{n+1}{2}; 0) \mid i = 0, \ldots, \frac{n-1}{2}\}$. It will be shown that the set

$$
C' = (C \setminus I) \cup \{(0, \frac{n+1}{2}; 0), (\frac{n-1}{2}, 0; 0), (\frac{n-1}{2}, \frac{n+1}{2}; \frac{n+1}{2})\}
$$

is a critical set of size $\frac{n^2 - 1}{4} + 2$, for $L' = (L \setminus I) \cup I'$ where $I' = \{(0, 0; \frac{n-1}{2}), (i, \frac{n-1}{2} - i; \frac{n+1}{2}), (i + 1, \frac{n-1}{2} - i; \frac{n-1}{2}), (\frac{n-1}{2}, 0; 0), (\frac{n-1}{2}, \frac{n+1}{2}; \frac{n+1}{2}), (0, \frac{n+1}{2}; 0) \mid i = 0, 1, \ldots, \frac{n-3}{2}\}$.

To show that C' has unique completion, we need only show that the cells of $\mathcal{S}_I$ must contain a unique entry and then invoke Theorem 1.

To begin, note that $\left(\frac{n-1}{2}, 0; \frac{n-1}{2}\right)$ was forced in the completion of C, and it follows that $\left(0, 0; \frac{n-1}{2}\right)$ is forced in the completion of C'. Now for $i = \frac{n-1}{2}$ downto 1, the entry $\left(\frac{n-1}{2} - i, i; \frac{n+1}{2}\right)$ is forced. Then, for $i = \frac{n-1}{2}$ downto 1, the entry $\left(\frac{n+1}{2} - i, i; \frac{n-1}{2}\right)$ is forced and unique completion follows.

Corollary 1 and the cycle on elements 0 and $n-1$ can be used to show that both of the entries $\left(0, \frac{n+1}{2}; 0\right), \left(\frac{n-1}{2}, 0; 0\right)$ are necessary for unique completion. Also using Lemma 1, it is easy to see that a latin interchange exists on the elements in rows $\frac{n-3}{2}$, and $\frac{n-1}{2}$ and columns 1 to $\frac{n+1}{2}$. This latin interchange intersects C' in the entry $\left(\frac{n-1}{2}, \frac{n+1}{2}; \frac{n+1}{2}\right)$ alone.

Next consider the element $(0, 1; 1)$. For $n > 5$ the latin interchange $\{(0, 1; 1), (0, n-1; n-1), (1, n-2; n-1), (1, n-1; 0), (2, n-2; 0), (2, n-1; 1), (3+2i, n-2-2i; 1), (3+2i, n-4-2i; n-1)\}$, for $i = 0, \ldots, \frac{n-5}{2}$ intersects C' in $(0, 1; 1)$ alone. For $n = 5$, element $(0, 1; 1)$ is needed as it is the only entry in columns 1 and 2. For element $(1, 0; 1)$, take the transpose of the latin interchange used for $(0, 1; 1)$, and this now also applies for $n = 5$.

The entries $\left(i, \frac{n+1}{2} - i; \frac{n-1}{2}\right), (i, n-i; 0), \left(\frac{n-1}{2} + i, \frac{n+1}{2} - i; 0\right), \left(\frac{n-1}{2} + i, n-i; \frac{n-1}{2}\right)$, for $i = 1$ to $\frac{n-3}{2}$, form an intercalate which intersects C' in $\left(\frac{n-1}{2} + i, n-i; \frac{n-1}{2}\right)$ alone. Similarly $\left(i, \frac{n-1}{2} - i; \frac{n+1}{2}\right), (i, n-i; 0), \left(\frac{n+1}{2} + i, \frac{n-1}{2} - i; 0\right), \left(\frac{n+1}{2} + i, n-i; \frac{n+1}{2}\right)$, for $i = 1$ to $\frac{n-3}{2}$, form an intercalate which intersects C' in $\left(\frac{n+1}{2} + i, n-i; \frac{n+1}{2}\right)$ alone.

For $n \geq 9$ and $n \equiv 1 \pmod 4$, the entries $\left(2, \frac{n-3}{2}; \frac{n-1}{2}\right), \left(2, \frac{n-1}{2}; \frac{n+3}{2}\right), \left(2, \frac{n+1}{2}; \frac{n+5}{2}\right), \left(3, \frac{n-3}{2}; \frac{n+3}{2}\right), \left(3, \frac{n-1}{2}; \frac{n+5}{2}\right), \left(3, \frac{n+1}{2}; \frac{n+7}{2}\right), \left(3+2i, \frac{n-3}{2}; \frac{n+3}{2} + 2i\right), \left(3+2i, \frac{n+1}{2}; \frac{n+7}{2} + 2i\right), \left(n-2, \frac{n-1}{2}; \frac{n-5}{2}\right), \left(n-1, \frac{n-3}{2}; \frac{n-5}{2}\right), \left(n-1, \frac{n-1}{2}; \frac{n-3}{2}\right), \left(n-1, \frac{n+1}{2}; \frac{n-1}{2}\right)$, for $i = 1$ to $\frac{n-5}{2}$, form a latin interchange which intersects C' in $\left(n-1, \frac{n+1}{2}; \frac{n-1}{2}\right)$ alone. For $n \geq 7$ and $n \equiv 3 \pmod 4$, the latin interchange $\{\left(2, \frac{n-3}{2}; \frac{n-1}{2}\right), \left(2, \frac{n+1}{2}; \frac{n+5}{2}\right), \left(2i, \frac{n-3}{2}; 2i + \frac{n-3}{2}\right), \left(2i, \frac{n+1}{2}; 2i + \frac{n+1}{2}\right) \mid 2 \leq i \leq \frac{n-1}{2}\}$ intersects C' in $\left(n-1, \frac{n+1}{2}; \frac{n-1}{2}\right)$ alone. For $n = 5$ the latin interchange $\{(1, 2; 2), (1, 3; 4), (2, 1; 2), (2, 2; 4), (i, j; i+j) \mid i = 3, 4; j = 1, 2, 3\}$ has the required property.

Finally, for all other entries $(x, y; x+y)$ of C', there exists a latin interchange, of the form $\{(x, y; x+y), \left(x+i, y-i+\frac{n-1}{2}; x+y+\frac{n-1}{2}\right), \left(x+i, y-i+\frac{n+1}{2}; x+y+\frac{n+1}{2}\right), \left(x+\frac{n-1}{2}, y+\frac{n+1}{2}; x+y\right)\}$, for $i = 0$ to $\frac{n-1}{2}$, which intersects C' in a single entry.

Thus C' is a critical set for L'.

References

[1] S Bakhtiari, R Safavi–Naini, J Pieprzyk. A message authentication code based on latin squares. *ACISP'97, Sydney, 1997*, in Lecture Notes in Computer Science, **1270** (1997), 194–203.

[2] G Carter, E Dawson, and L Nielsen. DESV: A Latin Square Variation of DES. *SAC'95*, (1995), 158–172.

[3] D Curran and GHJ van Rees. Critical sets in latin squares. In *Proc. 8th Manitoba Conference on Numerical Mathematics and Computing*, 165–168, Winnipeg, 1978. Utilitas Math. Pub.

[4] J Denes and AD Keedwell. *Latin squares and their applications*. The English Universities Press Ltd, London, 1974.

[5] Diane Donovan and Joan Cooper. Critical sets in back circulant latin squares. *Aequationes Math*, **52** (1996), 157–179.

[6] J.R. Elliot and P.B. Gibbons The construction of subsquare free Latin squares by simulated annealing. *Austras. J. of Combin.*, **5** (1992), 209–228.

[7] Adelle Howse. Minimal critical sets for some small latin squares. *Austras. J. of Combin.*, (submitted).

[8] BD McKay. Private communication.

[9] J Nelder. Critical sets in latin squares. In *CSIRO Division of Math. and Stats., Newsletter 38*, 1977.

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

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

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

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

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

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

11

Table 1:

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

Table 2:

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

Table 3:

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

Table 4:

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

Table 5:

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

Table 6:

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

Table 7:

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

Table 8:

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

Table 9:

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

Table 10:

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

Table 11:

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

Table 12:

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

Table 13:

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

Table 14:

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

Table 15:

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

Table 16:

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

Table 17:

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

Table 18:

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

Table 19:

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

Table 20:

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

Table 21:

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

Table 22:

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

Table 23:

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

Table 24:

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

Block row 1

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

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

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

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

Block row 2

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

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

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

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

Block row 3

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

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

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

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

Block row 4

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

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

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

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

Block row 5

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

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

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

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

Block row 6

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

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

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

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

Grid row 1:

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

Grid row 2:

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

Grid row 3:

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

Grid row 4:

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

Grid row 5:

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

Grid row 6:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

15

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

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

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

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

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

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

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

Table 3: The main classes of latin squares of order 7