Smallest critical sets for the groups of size eight

Peter Adams and A. Khodkar*
Centre for Combinatorics
Department of Mathematics
The University of Queensland
Queensland 4072
Australia

ABSTRACT. In this note, we computationally prove that the size of smallest critical sets for the quaternion group of order eight, the group $\mathbb{Z}_2 \times \mathbb{Z}_4$ and the dihedral group of order eight are 20, 21 and 22, respectively.

1 Introduction

A *(partial) latin square* L 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 (at most) precisely once in each row and column. We will sometimes talk of the (partial) latin square L as a set of ordered triples $(i, j; k)$, and read this to mean that element k occurs in position (i, j) of the (partial) latin square L. If a latin square L contains an $s \times s$ subarray S and if S is a latin square of order s, then we say that S is a *latin subsquare* of L. A *critical set* in a latin square L of order n, is a set $A = \{(i, j; k) \mid i, j, k \in \{1, 2, \dots, n\}\}$ such that,

(1) L is the only latin square of order n which has element k in position (i, j) for each $(i, j; k) \in A$.

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

A *smallest critical set* in a latin square L is a critical set of minimum cardinality.

*Research supported by the Australian Research Council

Let $P = \{(i,j;k) \mid i,j,k \in \{1,2,\ldots,n\}\}$ 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 cells $\{(i,j) \mid (i,j;k) \in P, \exists k \in \{1,2\ldots,n\}\}$ is said to determine the *shape* of P. Let P and P' be two partial latin squares of order n, with the same shape. Then P and 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 (and column) of P'. They are said to be *disjoint* if no cell in P contains the same entry as the corresponding cell in P'. Given two partial latin squares P and P' of order n, of the same size and shape, with the property that P and P' are disjoint and mutually balanced, P is said to be a *latin interchange* and P' is said to be a *disjoint mate* of P. Note that any latin subsquare, with order greater than one, of a latin square L is a latin interchange. The following lemma states the relation between critical sets and latin interchanges in a latin square.

Lemma 1.1 *Let L be a latin square and let A be a critical set in L. Then $|A \cap P| \geq 1$ for any latin interchange P in L.*

A latin square L' is said to be *isotopic* to the latin square L if L' can be obtained from L by permuting the rows and/or the columns and/or the symbols of L. Then the cell $(i,j;k)$ of L is transformed to the cell $(\theta(i),\phi(j);\psi(k))$ of L', where θ, ϕ and ψ are permutations. Let L' be isotopic to the latin square L; that is, $L' = \{(\theta(i),\phi(j);\psi(k)) \mid (i,j;k) \in L\}$. If P is a latin interchange (critical set) in L then $P' = \{(\theta(i),\phi(j);\psi(k)) \mid (i,j;k) \in P\}$ is a latin interchange (critical set) in L'.

A latin square which can be bordered with a headline and sideline in such a way that it becomes the multiplication table of a group G is said to be *based on* the group G. Clearly, any isotope of a latin square based on the group G is also based on G. The smallest size for critical sets in latin squares based on groups have been investigated in the past (for example, see [3, 4, 6, 9]). Table 1 shows some results on the smallest size of critical sets in the latin squares based on the groups.

In this note we deal with the remaining groups of order eight; namely the quaternion group (Q_8), the group $\mathbb{Z}_2 \times \mathbb{Z}_4$ and the dihedral group (D_4). We computationally prove that the smallest size of a critical set in a latin square based on Q_8 is 20, in a latin square based on $\mathbb{Z}_2 \times \mathbb{Z}_4$ is 21 and in a latin square based on D_4 is 22. Burgess [1] gives critical sets of size 20 for Q_8 and Sittampalam and Keedwell [9] produce critical sets of size 23 for D_4.

Groups	Smallest size for critical sets	References
$\mathbb{Z}_2$	1	Obvious
$\mathbb{Z}_3$	2	Obvious
$\mathbb{Z}_4$	4	[4]
$\mathbb{Z}_2 \times \mathbb{Z}_2$	5	[3]
$\mathbb{Z}_5$	6	[3]
$\mathbb{Z}_6$	9	[4]
S_3	12	[5]
$\mathbb{Z}_7$	12	[5]
$\mathbb{Z}_8$	16	[4]
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	25	[8]

Table 1

2 Technique

In this section we shall describe how to get close to a smallest critical set for a given latin square. This method was also used in [7, 8]. Let L be a latin square of order n with the entries on $\{1, 2, \dots, n\}$ and let $\{P_i\}_{i\in I}$ be a family of latin interchanges of L. Let $T_i = \{(r_i, s_i) \mid (r_i, s_i; t_i) \in P_i,\ \exists t_i \in \{1, 2 \dots, n\}\}$ be the shape of P_i. We form the inequality $\sum_{(r_i,s_i)\in T_i} x_{n(r_i-1)+s_i} \geq 1$ for each T_i.

Now consider the following integer programming problem.

$$\text{Minimize} \quad \sum_{j\in J} x_j, \quad \text{where } J = \{1, 2, \dots, n^2\}$$

subject to:

$$\sum_{(r_i,s_i)\in T_i} x_{n(r_i-1)+s_i} \geq 1 \ \ for\ all\ \ i \in I; \text{ and}$$

$$x_j = 0 \ or\ 1\ for\ all\ j \in J.$$

Let m be the integer optimal solution for the above integer programming problem. Then, by Lemma 1.1, the size of a smallest critical set for L cannot be less than m. Moreover, if $S = \{x_i\}_{i\in K}$ is a feasible solution for the above system such that $S \setminus \{x_i\}$ is not feasible for all $i \in K$, then the corresponding partial latin square with S is a critical set in L if it can uniquely be completed to L.

Example 2.1 Let L be the following latin square which is based on the group $\mathbb{Z}_4$.

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

Then consider the following integer programming problem. Note that each constraint corresponds to a latin interchange of L.

$$\text{Minimize} \quad \sum_{j \in J} x_j, \text{ where } J = \{1, 2, \dots, 16\}$$

subject to:

$$\begin{aligned} &x_1 + x_3 + x_9 + x_{11} \geq 1 \\ &x_2 + x_4 + x_{10} + x_{12} \geq 1 \\ &x_5 + x_7 + x_{13} + x_{15} \geq 1 \\ &x_6 + x_8 + x_{14} + x_{16} \geq 1 \\ &x_j = 0 \text{ or } 1 \text{ for all } j \in J. \end{aligned}$$

Obviously, the integer optimal solution for this system is four. On the other hand, each of the following partial latin squares in L has a unique completion. So the smallest size of critical sets in L is 4.

1	2		
2			
			3

1			
2			1
	4		

Table 2

We are now ready to describe a procedure for finding smallest critical sets for latin squares based on the groups Q_8, $\mathbb{Z}_2 \times \mathbb{Z}_4$ and D_4.

Procedure: Let the latin square L be based on the groups Q_8, $\mathbb{Z}_2 \times \mathbb{Z}_4$ or D_4. The procedure for finding a critical set with smallest size in L is as follows.

(1) Find all the latin subsquares of size two or four in L.

(2) Form the corresponding integer programming problem with these latin interchanges.

(3) Find the optimal integer solution for the system. Then form the corresponding partial latin square, P say, in L.

(4) Stop if P has only one completion, otherwise there is at least one latin interchange in L which does not intersect P (see Lemma 1.1).

(5) Using Lemma 3.1 (see Section 3) and P generate more latin interchanges in L. Add the corresponding constraints with the latin interchanges to the system and go to Step (3).

Applying this process we have obtained the following results.

Proposition 2.1 *The size of smallest critical sets in a latin square which is based on Q_8 is* 20.

Let the latin square L be based on Q_8 (see Table 3). Since there exist four non-overlapping latin subsquares of size four in L which are isotopic to $\mathbb{Z}_4$ it follows that (see Table 1) the size of smallest critical sets in L is at least 16. Applying the above technique we proved that the lower bound for the size of smallest critical sets is 20. Table 3 gives a critical set of size 20 in L.

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

Latin square L

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

critical set in L

Table 3

Proposition 2.2 *The size of smallest critical sets in a latin square which is based on $\mathbb{Z}_2 \times \mathbb{Z}_4$ is* 21.

Let the latin square L be based on $\mathbb{Z}_2 \times \mathbb{Z}_4$ (see Table 4). Since there exist four non-overlapping latin subsquares of size four in L which are isotopic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ it follows that (see Table 1) the size of smallest critical sets in L is at least 20. Applying the above technique we proved that the lower bound for the size of smallest critical sets is 21. Table 4 gives a critical set of size 21 in L.

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

Latin square L

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

critical set in L

Table 4

Proposition 2.3 *The size of smallest critical sets in a latin square which is based on D_4 is* 22.

Let the latin square L be based on D_4 (see Table 5). Since there exist four non-overlapping latin subsquares of size four in L which are isotopic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ it follows that (see Table 1) the size of smallest critical sets in L is at least 20. Applying the above technique we proved that the lower bound for the size of smallest critical sets is 22. Table 5 gives a critical set of size 22 in L.

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

Latin square L

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

critical set in L

Table 5

Computational details. The integer programming was carried out using CPLEX [2] on the Silicon Graphics Power Challenge supercomputer at the University of Queensland, Australia. Some computational statistics for each case are given in Table 6.

Groups	No. of constraints	CPU time (sec.)	No. of processors
Q_8	9650	1572108	4
$\mathbb{Z}_2 \times \mathbb{Z}_4$	6080	449374	4
D_4	320	540	4

Table 6

Summary: Let L be a latin square which is based on a group of order eight. Table 7 shows the relation between the number of latin subsquares of size two or four in L and the smallest size for the critical sets in L.

Groups	No. of latin subsquares isotopic to $\mathbb{Z}_2$	No. of latin subsquares isotopic to $\mathbb{Z}_4$	No. of latin subsquares isotopic to $\mathbb{Z}_2 \times \mathbb{Z}_2$	Size of smallest critical sets
$\mathbb{Z}_8$	16	4	0	16
Q_8	16	12	0	20
$\mathbb{Z}_2 \times \mathbb{Z}_4$	48	8	4	21
D_4	80	4	8	22
$(\mathbb{Z}_2)^3$	112	0	28	25

Table 7

3 An equivalence relation on partial latin squares

Let the latin square L be based on the group $(G, *)$; that is $L(a, b) = a * b$, where $a, b \in G$. For a partial latin square $P = \{(i, j; k) \mid i, j, k \in G\}$ in L we define $aPb = \{(a * i, j * b; a * k * b) \mid (i, j; k) \in P\}$, where $a, b \in G$. Obviously, aPb is a partial latin square in L. Now let $\mathcal{P}$ be the set of all partial latin squares of size m in L. We define a relation $\mathcal{R}$ on $\mathcal{P}$ as follows. For any $P_1, P_2 \in \mathcal{P}$, $(P_1, P_2) \in \mathcal{R}$ if and only if there exist $a, b \in G$ such that $P_1 = aP_2b$. It is easy to see that the relation $\mathcal{R}$ is an equivalence relation on $\mathcal{P}$. Therefore, $\mathcal{R}$ partitions $\mathcal{P}$ into equivalence classes.

Lemma 3.1 *Let the latin square L be based on the group $(G, *)$.*

(1) If P is a latin interchange in L then aPb is also a latin interchange in L for any $a, b \in G$.

(2) If A is a critical set in L then aAb is also a critical set in L for any $a, b \in G$.

Proof: (1) Let P be a latin interchange in L with disjoint mate P'. Then $aP'b$ is a disjoint mate of aPb for any $a, b \in G$.
(2) Let A be a critical set in L. suppose there exist $a, b \in G$ such that aAb is not a critical set in L. By Lemma 1.1 there exists a latin interchange P in L such that $P \cap (aAb) = \emptyset$. This implies $(a^{-1}Pb^{-1}) \cap A = \emptyset$. This is a contradiction since $a^{-1}Pb^{-1}$ is a latin interchange in L by (1).

Example 3.1 An exhaustive computer search shows that there are exactly 32 critical sets of size 4 in the latin square in Example 2.1. The relation $\mathcal{R}$ partitions these critical sets into two equivalence classes. Table 2 gives a representation for each class.

Example 3.2 The following latin square is based on the group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

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

An exhaustive computer search shows that there are exactly 96 critical sets of size 5 in this latin square. The relation $\mathcal{R}$ partitions these critical sets into six equivalence classes. Table 8 gives a representation for each class.

1	2		
			3
	4		
		2	

1	2		
			3
		1	
4			

1		3	
		4	
			2
	3		

1		3	
	1		
			2
4			

1			4
2			
		1	
	3		

1			4
	1		
3			
		2	

Table 8

Example 3.3 Let the latin square L be based on the group $\mathbb{Z}_8$ (see Table 9). Let P be a critical set of size 16 in L. Since L contains four non-overlapping latin subsquares isotopic to $\mathbb{Z}_4$ it follows that P must contain a critical set of size four in each of these subsquares. On the other hand, any subsquare isotopic to $\mathbb{Z}_4$ has exactly 32 critical sets of size four (see Example 3.1). An exhaustive computer search which uses the above fact shows that there are exactly 256 critical sets of size 16 in L . These critical sets fall into 16 equivalence classes with respect to the relation $\mathcal{R}$. Table 10 gives a representation for each class.

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

Table 9

(1,1;1),(1,2;2),(1,3;3),(1,4;4),(2,1;2),(2,2;3),(2,3;4),(3,1;3),(3,2;4),(4,1;4),(6,8;5),(7,7;5),(7,8;6),(8,6;5),(8,7;6),(8,8;7)
(1,1;1),(1,2;2),(1,3;3),(2,1;2),(2,2;3),(3,1;3),(5,8;4),(6,7;4),(6,8;5),(7,6;4),(7,7;5),(7,8;6),(8,1;8),(8,2;1),(8,3;2),(8,4;3)
(1,1;1),(1,2;2),(1,3;3),(2,1;2),(2,2;3),(3,1;3),(5,8;4),(6,7;4),(6,8;5),(7,6;4),(7,7;5),(7,8;6),(8,5;4),(8,6;5),(8,7;6),(8,8;7)
(1,1;1),(1,2;2),(1,3;3),(1,8;8),(2,1;2),(2,2;3),(2,8;1),(3,1;3),(3,8;2),(4,8;3),(6,7;4),(7,6;4),(7,7;5),(8,5;4),(8,6;5),(8,7;6)
(1,1;1),(1,3;3),(1,4;4),(1,6;6),(2,7;8),(3,1;3),(3,4;6),(4,2;5),(4,5;8),(4,7;2),(6,1;6),(6,4;1),(6,6;3),(7,2;8),(7,7;5),(8,4;3)
(1,1;1),(1,3;3),(1,6;6),(2,4;5),(2,7;8),(3,1;3),(4,1;4),(4,3;6),(4,6;1),(4,8;3),(5,4;8),(6,1;6),(6,6;3),(7,2;8),(7,4;2),(7,7;5)
(1,1;1),(1,3;3),(1,6;6),(2,4;5),(2,7;8),(3,1;3),(4,2;5),(4,4;7),(4,5;8),(4,7;2),(5,4;8),(6,1;6),(6,6;3),(7,2;8),(7,4;2),(7,7;5)
(1,1;1),(1,3;3),(1,6;6),(1,8;8),(2,4;5),(3,1;3),(3,6;8),(4,2;5),(4,4;7),(4,7;2),(6,1;6),(6,3;8),(6,6;3),(7,4;2),(7,7;5),(8,1;8)
(1,1;1),(1,2;2),(2,1;2),(2,2;3),(2,8;1),(3,1;3),(3,2;4),(3,7;1),(3,8;2),(4,3;6),(4,4;7),(4,5;8),(5,3;7),(5,4;8),(6,3;8),(8,2;1)
(1,1;1),(2,3;4),(2,6;7),(3,1;3),(3,4;6),(3,7;1),(5,3;7),(5,6;2),(5,8;4),(6,1;6),(6,4;1),(7,6;4),(8,1;8),(8,2;1),(8,4;3),(8,7;6)
(1,1;1),(2,3;4),(2,6;7),(3,1;3),(3,4;6),(3,7;1),(5,3;7),(5,6;2),(5,8;4),(6,1;6),(6,4;1),(7,6;4),(8,3;2),(8,5;4),(8,6;5),(8,8;7)
(1,1;1),(2,1;2),(2,8;1),(3,1;3),(3,7;1),(3,8;2),(4,1;4),(4,6;1),(4,7;2),(4,8;3),(5,2;6),(5,3;7),(5,4;8),(6,2;7),(6,3;8),(7,2;8)
(1,1;1),(2,1;2),(2,8;1),(3,1;3),(3,7;1),(3,8;2),(4,2;5),(4,3;6),(4,4;7),(4,5;8),(5,2;6),(5,3;7),(5,4;8),(6,2;7),(6,3;8),(7,2;8)
(1,1;1),(1,4;4),(2,6;7),(3,1;3),(3,2;4),(3,4;6),(3,7;1),(4,1;4),(5,3;7),(5,6;2),(6,1;6),(6,4;1),(6,7;4),(8,3;2),(8,6;5),(8,8;7)
(1,1;1),(1,6;6),(2,3;4),(3,1;3),(3,4;6),(3,6;8),(3,7;1),(4,6;1),(5,3;7),(5,8;4),(6,1;6),(6,4;1),(6,6;3),(8,3;2),(8,5;4),(8,8;7)
(1,1;1),(1,8;8),(2,1;2),(2,7;8),(2,8;1),(3,1;3),(3,6;8),(3,7;1),(3,8;2),(4,2;5),(4,3;6),(4,4;7),(5,2;6),(5,3;7),(6,2;7),(8,1;8)

Table 10