Critical sets for dihedral groups

A.G. Sittampalam and A.D. Keedwell
Department of Mathematical and Computing Sciences
University of Surrey, U.K.

In this paper, we obtain critical sets for the general dihedral group, but we are not able to decide whether they are minimal. We also show the existence of a weakly completable critical set in the latin square based on the dihedral group of order six. We believe this to be the smallest group based square to have such a set.

Introduction

A *latin square* of order n is an $n{\times}n$ square consisting of elements chosen from a set of size n, such that no element appears twice in any one row or column. Since this property is satisfied by the multiplication table of any group, we can form a latin square for any group.

We describe elements of a latin square by means of triples (i,j,k). The notation means that element k occurs in row i, column j.

A *latin subsquare* is a subset of the triples of a latin square which themselves form a latin square.

A *partial latin square* is a latin square with some triples left out.

A *uniquely completable (UC)* set is a set of triples which is a subset of the triples of only one latin square.

A *critical set* is a UC set which has the property that no proper subset of it is UC.

A *minimal critical set* for a particular latin square is a critical set which contains the least possible number of triples for that square.

When attempting to complete a square, we say that a triple $e=(r,c,s)$ is *forced* in the set S if

either (1) $\forall t \neq s, \exists p$ such that $(p,c,t) \in S$ or $(r,p,t) \in S$

or (2) $\forall t \neq c, \exists p$ such that $(p,t,s) \in S$ or $(r,t,p) \in S$

or (3) $\forall t \neq r, \exists p$ such that $(t,p,s) \in S$ or $(t,c,p) \in S$

A UC set C is called *strong* if we can define a sequence of sets of triples $C = F_1 \subset F_2 \subset \dots\dots\dots \subset F_k = L$, such that each triple e in $F_{i+1} - F_i$ is forced in F_i.

A strong UC set is *super-strong* if each triple in this sequence is forced only by virtue of property (1) in the above definition of forcing.

Note that the authors of [1] have used the terms *semi-strong* and *strong* in place of strong and super-strong as defined above. However, for consistency with previous papers we retain our earlier terminology.

A UC set which is not strong is *weak.*

In particular, a critical set may be weak, strong or super-strong.

A partial latin square which has m filled squares is said to be of *size m.* If the triples that make up the square are denoted (r_i, c_i, s_i), $1 \leq i \leq m$, then the set of pairs (r_i, c_i) determines the *shape* of the square.

Two partial latin squares P_1 and P_2 of the same size and shape are *mutually balanced* if the entries of the cells of each row (and column) of P_1 are the same as those in the corresponding row (and column) of P_2 and they are *disjoint* if $P_1 \cap P_2 \equiv \varnothing$.

A *critical partial latin square (CPLS)* for a latin square L is a partial latin square P of L which has a mutually balanced and disjoint partner.

An *intercalate* is a latin subsquare consisting of four elements.

To prove that a set S of triples is critical, we must prove that it is UC and that no proper subset of it is UC.

To prove that no proper subset is UC, it is enough to prove that $S-\{t\}$ is not UC $\forall t \in S$, since any proper subset of S must be a subset of one of these sets. The easiest way to show that a set T of triples is not UC is to exhibit a CPLS P such that $P \cap T \equiv \varnothing$. Intercalates are often the easiest CPLSs to find.

Many latin squares are constructed from groups by using the multiplication table for the group. For the group Z_n, Nelder [9] found two UC sets, which he conjectured to be critical. The larger set, which he conjectured to be a maximal critical set for Z_n, is described later. The smaller is of size $\lfloor n^2/4 \rfloor$. We shall denote it by Ω. An example for n=6 is shown in Figure 1. Nelder conjectured that Ω is a minimal critical set for Z_n. For n even, Curran and van Rees [4] showed it to be critical. Cooper, Donovan and Seberry [3] showed it to be minimal for n even, and proved criticality for n odd. It is not known whether Ω is minimal for n odd. However, Ω is in fact super-strong, and hence strong, and it has been proved in [1] that any strong critical set has size at least $\lfloor n^2/4 \rfloor$, so Ω is a minimal strong set. This does not rule out the existence of a smaller critical set which is weak. However, one of the present authors has conjectured that no weak critical sets exist for latin squares based on the cyclic group (see [6]).

Minimal critical sets have been found for all latin squares of order ≤5 (see [3]). A critical set of size 20 has been found for the Quaternion Group (see [2]), and a UC set of size 25 has been found for $Z_2 \times Z_2 \times Z_2$ (for the details see [6] and [8]), but so far as the authors are aware, no results valid for all orders, other than those for the cyclic group mentioned above, have hitherto been published.

In this paper, we obtain critical sets for the general dihedral group, but we are not able to decide whether they are minimal. We also obtain a weak critical set for the latin square based on D_3. It is known that weak critical sets do not exist in latin squares of order 4 or less (see [7]) and so, in view of the conjecture about weak critical sets for cyclic groups mentioned above, we believe this to be the smallest group based square for which such a weak critical set exists. However, for a particular latin square of order 5 which is not isotopic to a group square, a weak critical set has been found (see [2]).

0	1	2	.	.	.
1	2	.	.	.	.
2	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	3
.	.	.	.	3	4

Figure 1

The Dihedral Group

The dihedral group D_n is defined by $\langle a,b{:}a^n = e, b^2 = e, ab = ba^{n-1}\rangle$. We can relabel the elements as integers from *0* to *2n-1*, and obtain a latin square from the group table. The latin square derived from the group D_n will also be known as D_n.

From a preliminary investigation, we determined several critical sets for D_3. Two of these are illustrated in Figure 2 and 4. The set (of 13 elements) shown in Figure 2 is interesting because it is a weak critical set (we shall prove this statement later in the paper). As we remarked in the Introduction, we conjecture that D_3 is the smallest group-based latin square in which weakly completable critical sets exist.

0	.	.	.	.	.
.	.	.	5	3	.
.	.	1	.	5	.
.	4	5	.	.	2
.	.	.	2	.	1
.	3	4	1	.	.

Figure 2

Remark: We are indebted to the referee for pointing out that a slightly modified version of Figure 2 can be constructed which provides a weak critical set of D_3 with one less element. With the referee's permission, we exhibit this set in Figure 3.

0	.	.	.	.	.
.	.	.	5	3	.
.	.	1	.	5	.
.	4	.	.	.	2
.	.	.	2	.	1
.	3	4	.	.	0

Figure 3

0	.	.	.	4	5
1	.	.	.	.	4
2	.	1	.	.	.
.	.	.	0	.	.
.	.	3	2	0	.
.	3	.	.	.	.

Figure 4

We managed to find a set which is critical for all values of n, based on the set shown in Figure 4. Although the set shown in Figure 4 does not generalise to higher orders in itself, a slightly modified version (which has 12 elements for the case of D_3 and which we illustrate in Figure 5 for the case of D_5) is uniquely completable for all values of n as we shall prove in Theorem 1 below. It is also critical (see Theorem 2 below) but we have been unable to determine whether it is a minimal critical set.

.	.	.	.	.	.	6	7	8	9
1	.	.	.	.	.	.	6	7	8
2	.	.	.	1	.	.	.	6	7
3	.	.	1	2	.	.	.	.	6
4	.	1	2	3	.	.	.	.	.
.	.	.	.	.	0	.	.	.	.
.	.	.	.	5	4	0	.	.	.
.	.	.	5	6	3	4	0	.	.
.	.	5	6	7	2	3	4	0	.
9	5	.	.	.	.	.	.	.	.

Figure 5

$(i, 0, i)$:	$1 \le i \le n\text{-}1$	
$(i, j, i{+}j{-}n)$:	$2 \le i \le n\text{-}1,$	$n\text{-}i{+}1 \le j \le n\text{-}1$
$(i, j{+}n, j{-}i{+}n)$:	$0 \le i \le n\text{-}2,$	$i{+}1 \le j \le n\text{-}1$
$(i{+}n, j, i{+}j)$:	$1 \le i \le n\text{-}2,$	$n\text{-}i \le j \le n\text{-}1$
$(2n\text{-}1, 0, 2n\text{-}1)$		
$(2n\text{-}1, 1, n)$		
$(i{+}n, j{+}n, j{-}i \bmod n)$:	$0 \le i \le n\text{-}2,$	$0 \le j \le i$

Theorem 1

The set C listed above, of which Figure 5 is an example, is uniquely completable for all values of n.

Proof

There must be a 0 somewhere in column 0. It cannot be in the bottom row, because this position is already filled. It cannot be anywhere else in the bottom half, because these rows already contain 0's. It must therefore be in row 0, because all other positions are filled.

We now use induction to fill the main diagonal of the top-right hand quarter of the square with *n*'s.

Row 0 must contain an *n*, which cannot be in the first half of the row because the first column is now filled and the other columns contain *n*'s. It cannot be anywhere in the second half except column *n*, because the positions are filled, so it must be in column *n*. Now assume that it is possible to insert the *n*'s up to and including row *r*-1. There must be an *n* somewhere in row *r*. It cannot be anywhere in the first half of the row, because the first column is filled and all the other columns already contain *n*'s. From the induction assumption, all columns from *n* to *n*+*r*-1 already contain *n*'s. All the columns from *n*+*r*+1 to 2*n*-1 are already filled, so column *n*+*r* must contain the *n*. This completes the induction argument.

All the blank spaces left in the top-right hand quarter cannot contain any of the elements from 0 to *n*-1, because these are elsewhere in the corresponding rows or columns. It is therefore easy to complete the top right hand quarter square. We can then easily complete each of the other quarters.

Lemma 1

If a latin square L has a latin subsquare S, then if $S \cap C$ *is not UC in S, C will not be UC in L.*

Proof

Any CPLS found in the small square will be valid as a CPLS in the larger square.

Theorem 2

The set C (of which Figure 5 is an example) is critical for all values of n.

Proof

We have already shown *C* to be UC in Theorem 1. We must therefore prove that no proper subset of *C* is UC.

It suffices to prove that $\forall t \in C, C - \{t\}$ is not UC. To prove this, we find CPLSs $P\ \forall t \in C$ such that $P \cap C \equiv \{t\}$.

We can divide D_n into quarters, and each quarter will be a latin subsquare of D_n. Let us call the quarters S_1, S_2, S_3 and S_4, with "1" referring to the top-left quarter, "2" referring to the top-right quarter, "3" referring to the bottom-left quarter, and "4" referring to the bottom-right quarter. Let us denote $C \cap S_h$ by C_h.

Nelder conjectured in [9] that for the latin square which represents the cyclic group Z_n, the set M consisting of the upper left triangle entries bounded by, but not including, the main right to left diagonal, is critical (this is the conjectured maximal critical set referred to earlier). Donovan and Cooper have shown in [5] that this set is critical by giving a method for generating CPLSs for every element of the set.

The individual sets S_1, S_2, S_3 and S_4 are isomorphic to Cayley tables of the cyclic group, so we can make use of the CPLSs given by Donovan and Cooper if they are suitably transformed.

For $h \neq 3$, we can use the following mappings to transform Z_n onto S_h. These mappings also transform M into C_h.

$\underline{H}$	$(i, j, (i+j) \bmod n) \to$
1	$(n\text{-}1\text{-}i,\ (n\text{-}j) \bmod n,\ (\text{-}i\text{-}j\text{-}1) \bmod n)$
2	$(i,\ 2n\text{-}1\text{-}j,\ n+ (\text{-}1\text{-}I\text{-}j) \bmod n)$
3	$(2n\text{-}1\text{-}i,\ n\text{-}1\text{-}j,\ n+(\text{-}2\text{-}i\text{-}j) \bmod n)$
4	$(n+ (\text{-}2\text{-}i) \bmod n,\ n+j,\ (i+j+2) \bmod n)$

In order to show that C_h (h=1,2,3,4) is part of a critical set for D_n, we have to produce, for each triple of C_h, a CPLS which intersects C_h in that triple and in no other triple of C_h (or C).

Since, for $h \neq 3$, $\exists$ a mapping of Z_n onto S_h which maps M onto C_h, the images in S_h of the CPLS's which show that M is critical in Z_n may be used to show that C_h is critical in S_h.

For h=3, $\exists$ a mapping of Z_n onto S_3 which maps those cells of M which are not in the first row of Z_n onto those cells of C_3 which are not in the last row of S_3. Thus the CPLS's which cover those cells of M which are not in the first row of Z_n are transformed to CPLS's which cover the cells of C_3 which are not in the last row of S_3. Also, a CPLS can intersect M in only one place. So, since only one cell of the first row of Z_n does not belong to M and since a CPLS must have either zero or at least two cells in any particular row of Z_n, none of the transformed CPLS's has any entry in the last row of C_3. (An example of a CPLS obtained from Donovan and Cooper's paper and then transformed in the way described is given in Figure 6 (for the case n=5). The CPLS is shown in bold and the set C_3 is shown in italics.)

.	6	7	.	9
.	7	8	.	5
.	8	9	5	6
.	.	5	6	7
9	5	.	.	.

Figure 6

It remains to provide a CPLS in D_n which would be uncovered if the cell ($2n$-1,0,$2n$-1) of C_3 were omitted and also one which would be uncovered if the cell ($2n$-1,1,n) of C_3 were omitted. In the first case, the required CPLS is that consisting of all the cells of S_3 whose entries are $2n$-1 and $2n$-2. In the second case, the required CPLS is the intercalate of D_n whose cells are (0,1,1), (0,n,n), ($2n$-1,1,n) and ($2n$-1,n,1).

This completes the proof that C is a critical set for D_n.

Weak Critical Sets

With regard to our second claim, it is easy to see that the set shown in Figure 2, which we will denote by W, is weak because when we consider $F_1=W$, we see that there are no forced triples. It remains to show that it is UC. Note first that the cell (3,0) can be filled with 1 or 3. Let us first try to complete W by defining $F_2^{'} = F_1 \cup (3,0,1)$. We find that

$$F_3^{'} = F_2^{'} \cup \{(0,4,1)^R,\ (1,1,1)^C,\ (3,3,3)^C,\ (3,4,0)^S\ \}$$

$$F_4^{'} = F_3^{'} \cup \{(0,3,4)^S,\ (2,3,0)^R,\ (4,4,4)^S,\ (5,4,2)^S,\ (5,5,0)^C\}$$

$$F_5^{'} = F_4^{'} \cup \{(0,5,5)^R,\ (1,2,0)^C,\ (1,5,4)^S,\ (2,1,2)^S,\ (4,1,0)^R,\ (5,0,5)^S\ \}$$

The superscripts after each element refer to the way in which each element is forced. 'S' indicates that the given symbol is the only possibility for this row/column combination, 'R' indicates that the given row is the only possibility for this column/symbol combination, and 'C' indicates that the given column is the only possibility for this row/symbol combination.

After constructing $F_5^{'}$, we have the situation shown in Figure 6. It is impossible to construct $F_6^{'}$ because cell (0,1) (marked with an 'x') cannot be filled. We therefore define $F_2 = F_1 \cup (3,0,3)$. We find that the square can then be filled uniquely by forcing.

0	X	.	4	1	5
.	1	0	5	3	4
.	2	1	0	5	.
1	4	5	3	0	2
.	0	.	2	4	1
5	3	4	1	2	0

Figure 6

To show that W is critical, we list the CPLSs for each element:

(0,0,0)	{(0,0,0), (0,5,5), (5,0,5), (5,5,0)}
(1,3,5)	{(0,3,3), (0,5,5), (1,3,5), (1,5,4), (2,3,4), (2,5,3)}
(1,4,3)	{(1,2,0), (1,4,3), (4,2,3), (4,4,0)}
(2,2,1)	{(0,1,1), (0,2,2), (1,0,1), (1,1,2), (2,0,2), (2,2,1)}
(2,4,5)	{(2,1,0), (2,4,5), (4,1,5), (4,4,0)}
(3,1,4)	{(2,1,0), (2,3,4), (3,1,4), (3,3,0)}
(3,2,5)	{(0,2,2), (0,3,3), (0,4,4), (0,5,5), (1,1,2), (1,2,0), (2,0,2), (2,1,0), (2,3,4), (2,5,3), (3,0,3), (3,2,5), (4,0,4), (4,2,3), (4,4,0), (5,0,5), (5,4,2), (5,5,0)}
(3,5,2)	{(2,0,2), (2,5,3), (3,0,3), (3,5,2)}
(4,3,2)	{(2,0,2), (2,3,4), (4,0,4), (4,3,2)}
(4,5,1)	{(1,0,1), (1,5,4), (4,0,4), (4,5,1)}
(5,1,3)	{(2,1,0), (2,5,3), (5,1,3), (5,5,0)}
(5,2,4)	{(1,2,0), (1,5,4), (5,2,4), (5,5,0)}
(5,3,1)	{(0,1,1), (0,3,3), (0,4,4), (0,5,5), (1,0,1), (1,1,2), (2,0,2), (2,1,0), (2,3,4), (2,5,3), (3,3,0), (3,4,1), (4,0,4), (4,1,5), (4,4,0), (5,0,5), (5,3,1), (5,5,0)}

This completes our proof that a weak critical set for D_3 exists.

(Note: The authors would like to thank the referee for some valuable suggestions.)

References

[1] J. A. Bate and G. H. J. van Rees, The Size of the Smallest Strong Critical Set in a Latin Square, (submitted).

[2] D. R. Burgess, Ph.D. Thesis, University of Surrey 1997, (submitted).

[3] J. Cooper, D. Donovan and J. Seberry, Latin squares and critical sets of minimal size, *Austral. J. Combin.* 4 (1994), 113-120.

[4] D. Curran and G. H. J. van Rees, Critical sets in latin squares. In Proc. 8th Manitoba Conference on Numerical Mathematics and Computing, *Congressus Numerantium* 22 (1978), 165-168.

[5] D. Donovan and J. Cooper, Critical Sets in Back Circulant Latin Squares, *Aequationes Math.* **52** (1996), 157-179

[6] A.D. Keedwell, Critical sets for latin squares, graphs and block designs: a survey, *Congressus Numerantium* **113** (1996), 231-245.

[7] A.D. Keedwell, What is the size of the smallest latin square for which a weakly completable critical set of cells exists?, *Ars Combinatoria*, to appear.

[8] M. Mahdian, The size of the minimum critical set in the $Z_2 \times Z_2 \times Z_2$ latin square is 25, *Bull. ICA* **21** (1997), 14-16.

[9] J. Nelder, Private communication to J. Seberry (January 1979).