Critical Sets in a Family of Groups

Diane Donovan

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

D.G. Hoffman

Department of Discrete & Statistical Sciences
Auburn University
Auburn, AL36849–5307, USA

Dedicated to the memory of Derrick Breach, 1933–1996

Abstract

In this paper we construct critical sets for the multiplication tables of the groups of order $4h$, $h \geq 2$, with generating relations $a^{2h} = 1,\ b^2 = a^h$ and $ba = a^{-1}b$.

1 Introduction

A *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 precisely once in each row and column of the array. (See [**3**].) For example, the following array, H_1, is a latin square of order 8. Here $N = \{0, \ldots, 7\}$.

0	1	2	3	4	5	6	7
1	2	3	4	5	6	7	0
2	3	4	5	6	7	0	1
3	4	5	6	7	0	1	2
4	5	6	7	0	1	2	3
5	6	7	0	1	2	3	4
6	7	0	1	2	3	4	5
7	0	1	2	3	4	5	6

This latin square is the addition table for the integers modulo 8.

For convenience, we will sometimes talk of the latin square L as a set of ordered triples $\{(i,j;k) \mid \text{ cell } (i,j) \text{ contains } k\}$. In the above example the latin square can be represented by the set $\{(i,j;i+j(\text{mod } 8)) \mid i,j \in \{0,\ldots,7\}\}$.

A latin square L' is said to be *isotopic* to L if L' can be obtained from L by permuting the rows and/or the columns and/or the entries of L. That is, L' is said to be isotopic to L is there exists permutations $\alpha,\ \beta,\ \gamma$ such that $L' = \{(i\alpha, j\beta; k\gamma) \mid (i,j;k) \in L\}$. Then $(\alpha,\ \beta,\ \gamma)$ is said to be an *isotopism* from L to L'.

There are six conjugate latin squares associated with each latin square L. The reader will find the definition of these in [**3**]. In this paper we require one of these conjugates and so define it as follows:

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

is a conjugate of the latin square L. The first array $\mathcal{H}_2$, given below, is a conjugate of the multiplication table of the integers modulo 8 and $\mathcal{H}_2'$ can be obtained by applying the permutation $(0\ 7\ 6 \ldots 1)$ to the columns of $\mathcal{H}_2$. Hence $\mathcal{H}_2$ and $\mathcal{H}_2'$ are isotopic.

0	1	2	3	4	5	6	7
7	0	1	2	3	4	5	6
6	7	0	1	2	3	4	5
5	6	7	0	1	2	3	4
4	5	6	7	0	1	2	3
3	4	5	6	7	0	1	2
2	3	4	5	6	7	0	1
1	2	3	4	5	6	7	0

$\mathcal{H}_2$

1	2	3	4	5	6	7	0
0	1	2	3	4	5	6	7
7	0	1	2	3	4	5	6
6	7	0	1	2	3	4	5
5	6	7	0	1	2	3	4
4	5	6	7	0	1	2	3
3	4	5	6	7	0	1	2
2	3	4	5	6	7	0	1

$\mathcal{H}_2'$

If a latin square L contains an $s \times s$ subarray S and if S is a latin square of order s, then S is said to be a *latin subsquare* of L.

A *partial latin square* P, of order n, is an $n \times n$ array with some cells containing entries chosen from the 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 partial latin square $\mathcal{C} = \{(i,j;k) \mid \text{ cell } (i,j) \text{ contains } k\}$, of order n, is said to have a *unique completion* to a latin square L, if L is the only latin square of order n which has element k in cell (i,j), for each $(i,j;k) \in \mathcal{C}$.

A *critical set* in a latin square L, of order n, is a set $\mathcal{C} \subseteq L$ such that,

1. $\mathcal{C}$ has a unique completion to L, and
2. no proper subset of $\mathcal{C}$ satisfies 1.

For example, it can be shown that the following partial latin squares are critical sets. These two partial latin squares complete to H_1 and $\mathcal{H}_2'$ respectively. (Here $*$ indicates an empty cell.)

$$
\begin{array}{cccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & * \\
1 & 2 & 3 & 4 & 5 & 6 & * & * \\
2 & 3 & 4 & 5 & 6 & * & * & * \\
3 & 4 & 5 & 6 & * & * & * & * \\
4 & 5 & 6 & * & * & * & * & * \\
5 & 6 & * & * & * & * & * & * \\
6 & * & * & * & * & * & * & * \\
* & * & * & * & * & * & * & *
\end{array}
\qquad\qquad
\begin{array}{cccccccc}
* & * & * & * & * & * & * & 0 \\
* & * & * & * & * & * & * & * \\
7 & * & * & * & * & * & * & * \\
6 & 7 & * & * & * & * & * & * \\
5 & 6 & 7 & * & * & * & * & * \\
4 & 5 & 6 & 7 & * & * & * & * \\
3 & 4 & 5 & 6 & 7 & * & * & * \\
2 & 3 & 4 & 5 & 6 & 7 & * & *
\end{array}
$$

At various stages throughout this paper we will use the following results.

LEMMA 1.1 *If L is a latin square of order n, S a subsquare in L and C a critical set in L, then $C \cap S$ must have a unique completion in S.*

In 1995 Donovan, Cooper, Seberry and Nott [**4**] proved the following two results.

LEMMA 1.2 *Let L be a latin square with critical set C. Let (α, β, γ) be an isotopism from the critical set C onto C'. Then C' is a critical set in a latin square L' isotopic to L.*

LEMMA 1.3 *Let L be a latin square with critical set C and let C' be a conjugate of C. Then C' is a critical set in the corresponding conjugate L' of L.*

Recently Donovan and Cooper [**5**] extended work of Curran and van Rees [**2**] and Cooper, Donovan and Seberry [**1**] and constructed infinite families of critical sets in the addition tables for the integers modulo n. Their result is as follows

THEOREM 1.1 *Let L be the addition table for the integers modulo n, then the set*

$$
\begin{aligned}
C \;=\; & \{(i, j; i+j) \mid i = 0, \ldots, r \text{ and } j = 0, \ldots, r-i\} \cup \\
& \{(i, j; i+j) \mid i = r+2, \ldots, n-1 \text{ and } j = r+1-i, \ldots, n-1\}
\end{aligned}
$$

where $\frac{n-3}{2} \leq r \leq n-2$, is a critical set in L.

Recently Sittampalam (with Keedwell) [**9**] constructed an infinite class of critical sets for the multiplication tables of the dihedral groups. In addition a critical set for the quaternion group of order 8 has been found by Burgess, see [**8**]. This work has been taken up by Howse [**7**], and she has constructed two more infinite classes of critical sets for the multiplication tables of the dihedral groups.

The purpose of this paper is to construct an infinite family of critical sets for the multiplication tables of the groups of order $4h$, $h \geq 2$, with generating relations $a^{2h} = 1,\ b^2 = a^h$ and $ba = a^{-1}b$. (When h is a power of two, these groups are called generalized quaternion groups, see [**6**].) If we let $s(i)$ correspond to the element a^i and $t(i)$ correspond to $(a^{-i})b$, for i an element of the integers modulo $2h$, then multiplication is given by

$$
\begin{array}{rr}
s(i) * s(j) = s(i+j) & s(i) * t(j) = t(j-i) \\
t(i) * s(j) = t(i+j) & t(i) * t(j) = s(j-i+h).
\end{array}
$$

The latin square corresponding to the multiplication table for this group is

$$
\begin{aligned}
H = \{(s(i), s(j); s(i+j))\} \ \cup \ \{(s(i), t(j); t(j-i))\} \cup \\
\{(t(i), s(j); t(i+j))\} \ \cup \ \{(t(i), t(j); s(j-i+h))\}.
\end{aligned}
$$

The main result of this paper is:

THEOREM 1.2 *The partial latin square C_H*

$$
\begin{aligned}
&\{(s(i), s(j); s(i+j)) \mid i = 0, \ldots, 2h-2, j = 0, \ldots, 2h-2-i\} \quad \cup \\
&\{(s(0), t(0); t(0))\} \quad \cup \\
&\{(s(k), t(0); t(2h-k)) \mid k = h+1, \ldots, 2h-1\} \quad \cup \\
&\{(s(i), t(j); t(j-i)) \mid i = 2, \ldots, 2h-1, j = 1, \ldots, i-1\} \quad \cup \\
&\{(t(i), s(j); t(i+j)) \mid i = 1, \ldots, 2h-1, j = 2h-i, \ldots, 2h-1\} \quad \cup \\
&\{(t(i), t(j); s(j-i+h)) \mid i = 0, \ldots, 2h-2, j = i+1, \ldots, 2h-1\},
\end{aligned}
$$

is a critical set which has unique completion to the latin square H.

By way of example we may take $h = 4$, and represent $s(i)$ by i and $t(i)$ by $8+i$. Then the following array forms a latin square of the given type.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	3	4	5	6	7	0	15	8	9	10	11	12	13	14
2	3	4	5	6	7	0	1	14	15	8	9	10	11	12	13
3	4	5	6	7	0	1	2	13	14	15	8	9	10	11	12
4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	6	7	0	1	2	3	4	11	12	13	14	15	8	9	10
6	7	0	1	2	3	4	5	10	11	12	13	14	15	8	9
7	0	1	2	3	4	5	6	9	10	11	12	13	14	15	8
8	9	10	11	12	13	14	15	4	5	6	7	0	1	2	3
9	10	11	12	13	14	15	8	3	4	5	6	7	0	1	2
10	11	12	13	14	15	8	9	2	3	4	5	6	7	0	1
11	12	13	14	15	8	9	10	1	2	3	4	5	6	7	0
12	13	14	15	8	9	10	11	0	1	2	3	4	5	6	7
13	14	15	8	9	10	11	12	7	0	1	2	3	4	5	6
14	15	8	9	10	11	12	13	6	7	0	1	2	3	4	5
15	8	9	10	11	12	13	14	5	6	7	0	1	2	3	4

The array given below is an example of the partial latin square C_H when $h = 4$.

0	1	2	3	4	5	6	*	8	*	*	*	*	*	*	*
1	2	3	4	5	6	*	*	*	*	*	*	*	*	*	*
2	3	4	5	6	*	*	*	*	15	*	*	*	*	*	*
3	4	5	6	*	*	*	*	*	14	15	*	*	*	*	*
4	5	6	*	*	*	*	*	*	13	14	15	*	*	*	*
5	6	*	*	*	*	*	*	11	12	13	14	15	*	*	*
6	*	*	*	*	*	*	*	10	11	12	13	14	15	*	*
*	*	*	*	*	*	*	*	9	10	11	12	13	14	15	*
*	*	*	*	*	*	*	*	*	5	6	7	0	1	2	3
*	*	*	*	*	*	*	8	*	*	5	6	7	0	1	2
*	*	*	*	*	*	8	9	*	*	*	5	6	7	0	1
*	*	*	*	*	8	9	10	*	*	*	*	5	6	7	0
*	*	*	*	8	9	10	11	*	*	*	*	*	5	6	7
*	*	*	8	9	10	11	12	*	*	*	*	*	*	5	6
*	*	8	9	10	11	12	13	*	*	*	*	*	*	*	5
*	8	9	10	11	12	13	14	*	*	*	*	*	*	*	*

PROOF of Theorem 1.2.

We shall begin by verifying that if any element of the set C_H is removed then it is not possible to obtain a unique completion.

From the structure of the latin square H we see that it can be partitioned into four latin subsquares

$$\begin{aligned}
H_1 &= \{(s(i), s(j); s(i+j)) \mid 0 \le i, j \le 2h-1\} \\
H_2 &= \{(s(i), t(j); t(j-i)) \mid 0 \le i, j \le 2h-1\} \\
H_3 &= \{(t(i), s(j); t(i+j)) \mid 0 \le i, j \le 2h-1\} \\
H_4 &= \{(t(i), t(j); s(j-i+h)) \mid 0 \le i, j \le 2h-1\}.
\end{aligned}$$

Each of these subsquares is isotopic to the multiplication table for the integers modulo $2h$ or to a conjugate of that latin square.

Theorem 1.1 can be used to show that the set of elements

$$\{(s(i), s(j); s(i+j)) \mid i = 0, \ldots, 2h-2, j = 0, \ldots, 2h-2-i\}$$

forms a critical set in H_1. Therefore if any of these elements are removed this set will not have a unique completion to H_1 and hence by Lemma 1.1 each of these elements is necessary to complete C_H uniquely to H.

Likewise it can be shown that each of the elements of the set

$$\{(t(i), s(j); t(i+j)) \mid i = 1, \ldots, 2h-1, j = 2h-i, \ldots, 2h-1\}$$

is necessary to complete C_H uniquely to H.

The subsquare H_4 is isotopic to a conjugate of the multiplication table of the integers modulo $2h$ and so using Lemmas 1.1, 1.2 and 1.3 and Theorem 1.1 it can be shown that each of the elements of the set

$$\{(t(i), t(j); s(j-i+h)) \mid i = 0, \ldots, 2h-2, j = i+1, \ldots, 2h-1\}$$

is necessary to complete C_H uniquely to H.

Finally we must consider the elements of the set $C_H \cap H_2$. The subsquare H_2 is a conjugate of the multiplication table of the integers modulo $2h$ and using Theorem 1.1 and Lemmas 1.2 and 1.3 we can show that the set

$$\{(s(0),t(0);t(0))\} \;\cup\; \{(s(i),t(j);t(j-i)) \mid i=2,\ldots,2h-1, j=1,\ldots,i-1\}$$

is a critical set in H_2. If one refers back to Donovan and Cooper's paper [**5**], Theorem 3, it can be seen that each of these entries is necessary for a unique completion to H_2 irrespective of whether of not the cells $(s(k),t(0))$, $k=h+1,\ldots,2h-1$, are empty. Therefore each of the elements of the set

$$\{(s(0),t(0);t(0))\} \;\cup\; \{(s(i),t(j);t(j-i)) \mid i=2,\ldots,2h-1, j=1,\ldots,i-1\}$$

is necessary for $C_H \cap H_2$ to complete uniquely to H_2 and hence each of these elements are necessary to complete C_H uniquely to H.

That leaves us to prove that the elements of the set $\{(s(k),t(0);t(2h-k)) \mid k = h+1,\ldots,2h-1\}$ are necessary for the unique completion. To see this take an element of the form $(s(k),t(0);t(2h-k))$ where $k \in \{h+1,\ldots,2h-1\}$. The elements

$$\begin{array}{ccc}
 & \{(s(k-h),s(h-k);s(0)) & (s(k-h),t(0);t(h-k)) \\
(s(k),s(2h-k);s(0)), & (s(k),s(h-k);s(h)), & (s(k),t(0);t(2h-k)) \\
(t(0),s(2h-k);t(2h-k)), & (t(0),s(h-k);t(h-k)), & (t(0),t(0);s(h)) \\
(t(h),s(2h-k);t(h-k)), & & (t(h),t(0);s(0))\}
\end{array}$$

intersects C_H in the single element $(s(k),t(0);t(2h-k))$. If this entry is removed from C_H then what is left will complete to H but also to the latin square which differs from H in the following entries.

$$\begin{array}{ccc}
 & \{(s(k-h),s(h-k);t(h-k)) & (s(k-h),t(0);s(0)) \\
(s(k),s(2h-k);t(2h-k)), & (s(k),s(h-k);s(0)), & (s(k),t(0);s(h))) \\
(t(0),s(2h-k);t(h-k)), & (t(0),s(h-k);s(h)), & (t(0),t(0);t(2h-k)) \\
(t(h),s(2h-k);s(0)), & & (t(h),t(0);t(h-k))\}
\end{array}$$

Thus each of the entries $(s(k),t(0);t(2h-k))$ where $k \in \{h+1,\ldots,2h-1\}$ is necessary to complete C_H uniquely to H.

At this point we have shown that each of the elements of C_H is necessary for a unique completion to H. It remains to be shown that the given set is sufficient to force the unique completion of C_H to H.

The notation $x\ R\ y\ C\ z$ denotes that symbol x must occur in row y, and column z is the only place for it, and $x\ C\ y\ R\ z$ means symbol x must occur in column y, and row z is the only place for it. Then the following steps justify the unique completion of C_H.

$t(0)\ R\ t(0)\ C\ s(0)$.

For $i = 1$ to $2h-1$,	$t(0)\ C\ t(i)\ R\ s(i)$.
For $i = 0$ to $2h-1$,	$s(2h-i-2)\ R\ s(2h-1)\ C\ s(2h-i-1)$.
For $i = 1$ to $2h-1$,	$t(i)\ C\ s(0)\ R\ t(i)$.
For $i = 1$ to $2h-1$, for $j = i$ to $2h-1$,	$t(i)\ C\ t(j)\ R\ s(j-i)$.
For $i = 1$ to $2h-1$, for $j = 2h-1$ downto i,	$s(h-i+1)\ C\ t(j-i+1)\ R\ t(j)$.
For $i = 2h-2$ downto $h+1$, for $j = 2h-1$ downto $2h-i-1$,	$s(i+j)\ R\ s(i)\ C\ s(j)$.
For $i = 0$ to $2h-1$,	$s(h-i)\ R\ t(i)\ C\ t(0)$

Now H_1, H_2 and H_3 have unique completions by Theorem 1.1 .

Hence C_H is a critical set in the latin square H.

References

[1] Joan Cooper, Diane Donovan and Jennifer Seberry, *Latin squares and critical sets of minimal size*, Australas. J. Combin., **4**, 1991, pp. 113–120.

[2] 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, pp. 165–168.

[3] J. Dénes and A.D. Keedwell, Latin Squares and their Applications, The English Universities Press Ltd, London (1974).

[4] Diane Donovan, Joan Cooper, D.J. Nott and Jennifer Seberry *Latin squares: critical sets and their lower bounds*, Ars Comb., **39**, (1995), pp 33–48.

[5] Diane Donovan and Joan Cooper, *Critical sets in back circulant latin squares*, Aequationes Math., (to appear).

[6] Marshall Hall, Jr., The Theory of Groups, Macmillan, 1959, p. 187.

[7] Adelle Howse, *Families of critical sets for dihedral groups*, private communication.

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

[9] A.G. Sittampalam (with A.D. Keedwell), *Critical sets for dihedral groups* (submitted).

(Received 2/9/96)