Defining sets for latin squares given that they are based on groups

David Bedford
Department of Mathematics, Keele University,
Keele, Staffordshire, ST5 5BG, U.K.

Matthew Johnson
Department of Mathematics, University of Reading,
P.O. Box 220 Reading, Berkshire, RG6 6AX, U.K.

M. A. Ollis
School of Mathematical Sciences, Queen Mary, University of London,
Mile End Road, London, E1 4NS, U.K.

Abstract

We investigate defining sets for latin squares where we are given that the latin square is the Cayley table for some group. Our main result is that the proportion of entries in a smallest defining set approaches zero as the order of the group increases without bound.

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 exactly once in each row and column. The Cayley table of a group G is a latin square and we will use G to denote both the group and its Cayley table. Without loss of generality we may take $N = \{1, 2, \ldots, n\}$ and assume that rows and columns are indexed by N. We may also represent a latin square by a set of n^2 triples (i, j, k) such that element k appears in row i and column j.

A *partial latin square* P 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 once in each row and column. We shall also use the corresponding set of triples to represent a partial latin square.

If (θ, ϕ, ψ) are permutations on N, then the (θ, ϕ, ψ)-*isotope* of P is denoted and defined by $(\theta, \phi, \psi)P = \{(\theta(i), \phi(j), \psi(k)) : (i, j, k) \in P\}$.

If $\{a, b, c\} = \{1, 2, 3\}$, then the (a, b, c)-*conjugate* of P is denoted and defined by $P_{(a,b,c)} = \{(x_a, x_b, x_c) : (x_1, x_2, x_3) \in P\}$.

The set of all partial latin squares isotopic to a given partial latin square P is called the *isotopy class* of P; the isotopy class of P together with all of the conjugates of its members forms the *main class* of P and will be denoted $M(P)$. For the Cayley table of a group it is known that its isotopy and main classes are equal.

A set of triples defining a partial latin square, P, of order n is *uniquely completable (UC)*, or a *defining set*, if there is only one latin square, L, of order n that contains P. If L is the only latin square in the main class $M(L)$ that contains P, then we will say that P is uniquely completable in $M(L)$. A UC set is *critical* (in $M(L)$) if none of its proper subsets is UC (in $M(L)$). It is immediate that P is UC (in $M(L)$) to L if and only if $((\theta,\phi,\psi)P)_{(a,b,c)}$ is UC (in $M(L)$) to $((\theta,\phi,\psi)L)_{(a,b,c)}$. We define the *density* of a partial latin square of order n to be its size divided by n^2.

At present it is not known whether any latin square of order n has a critical set smaller than $\lfloor n^2/4 \rfloor$; Mahmoodian [8] and Bates and van Rees [1] have independently conjectured that no such latin square exists. With regard to group-based latin squares Donovan et al [4] have proved that the density of a critical set for C_2^r is at least 3/8, and in [5] Keedwell conjectured that for all group-based latin squares, except those based on a cyclic group, the density of a smallest critical set tends to 1/2 as the order of the square tends to infinity. In this paper we construct the smallest critical sets in $M(C_2 \times C_2)$ and $M(C_5)$, and prove that if G is a group of order n, then the density of a smallest defining set in $M(G)$ approaches 0 as $n \to \infty$. The latter result is extended to unique completion within the set of all group-based latin squares of order n. Finally we show that Keedwell's conjecture is false by constructing a defining set of density 7/16 for each member of an infinite class of non-cyclic groups.

2 Critical sets in $M(C_2 \times C_2)$ and $M(C_5)$

In [6] Keedwell considered the problem of finding critical sets for orthogonal latin squares and, as part of his investigations, showed that four entries are sufficient to define a partial latin square of order 4 that completes to exactly one isotope of $C_2 \times C_2$ (in [7] Keedwell had previously shown that a smallest critical set for $C_2 \times C_2$ has size 5). In our terminology Keedwell showed that there exists a set of size 4 that is UC in $M(C_2 \times C_2)$. Keedwell's example is displayed below.

1		3	
			2
4			

Keedwell's argument for unique completion in $M(C_2 \times C_2)$ was to show that there are exactly three latin squares of order 4 that contain the above partial latin square and that two of these are isotopic to C_4 leaving just one isotopic to $C_2 \times C_2$. We will give an alternative argument using the following lemma.

Lemma 1 *In $M(C_2^r)$ every pair of elements from the same row (or column) lies in an intercalate (i.e. a 2×2 latin subsquare).*

Proof: Since C_2^r is a group and latin subsquares are preserved by isotopy, it is sufficient to establish the result for C_2^r. Suppose that the cells $(a, f), (a, g)$ contain x and y respectively. Let (b, f) be the cell containing y in column f. So $af = x, ag = y, bf = y$. Since in C_2^r every element is its own inverse, $b = yf$ and $g = ay$. It follows that $bg = (yf)(ay) = af = x$.

Returning to Keedwell's example: the entries $(1, 4, 4)$ and $(1, 2, 2)$ may be filled in immediately and, by Lemma 1, consideration of the four corner cells leads to the entry $(4, 4, 1)$; similarly we must have $(3, 2, 4)$. The resulting partial latin square is UC.

Keedwell did not show that no smaller set can be UC in $M(C_2 \times C_2)$ but since such a set must cover at least 3 rows, 3 columns and 3 symbols, any such set of size 3 is isotopic to P (shown below) which is contained in the two distinct members of $M(C_2 \times C_2)$ displayed alongside P.

P :

1			
	2		
		3	

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

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

It is well known that the smallest critical set for C_5 has size 6; in [6] Keedwell made the following conjecture.

A smallest UC set in $M(C_5)$ has size 6.

By exploiting the concepts of isotopy and conjugacy it is possible to prove this conjecture without the aid of a computer.

Theorem 1 *No set of 5 (or fewer) entries is UC in $M(C_5)$.*

Proof: The following are all members of $M(C_5)$:

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

L_1

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

L_2

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

L_3

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

L_4

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

L_5

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

L_6

[Note that the latin squares of order 5 partition into two main classes and that $L \in M(C_5)$ if and only if L does not contain an intercalate.]

Any putative UC set in $M(C_5)$ of 5 entries must cover at least 4 distinct rows, columns and symbols. We need to identify the main classes of partial latin squares of this type; by conjugacy it is sufficient to consider the following cases.

Case 1: exactly 5 rows, 5 columns and 5 elements covered.

Case 2: exactly 4 rows, 5 columns and 5 elements covered.

Case 3: exactly 4 rows, 4 columns and 5 elements covered.

Case 4: exactly 4 rows, 4 columns and 4 elements covered.

For each main class of partial latin squares we will either show that its members do not complete in $M(C_5)$ or write down a representative of the class that completes to two members of $L_1, \ldots, L_6$.

Case 1: Any such partial latin square is isotopic to the following which completes to both L_1 and L_2.

1				
	2			
		3		
			4	
				5

Case 2: Any such partial latin square is isotopic to

1				
	2			
		3		
			4	5

This does not complete in $M(C_5)$ because C_n for odd n has the property that any set of $n-1$ cells from distinct rows and columns and containing distinct elements extends to a transversal (i.e. a set of n cells from distinct rows and columns and containing distinct elements).

In cases 3 and 4 we distinguish between two types of partial latin square containing 5 entries in 4 rows and 4 columns. Those of type (a) have one entry with the property that there are further entries in the same row and column. The remaining partial latin squares are of type (b). We illustrate these types

below where * denotes a non-empty cell.

*			*	
	*			
		*		
			*	

*				
*				
	*	*		
			*	

Type (a) Type (b)

Case 3: Up to isotopism there is only one partial latin square of each of types (a) and (b), the following representatives each have two distinct completions among $L_1, \ldots, L_6$.

1			5	
	2			
		3		
			4	

	4			
	2			
		3	1	
				5

Case 4: The partial latin squares of type (a) partition into 4 main classes; a representative that completes to two members of $L_1, \ldots, L_6$ is given below for each class. Note that we may permute rows and columns so that 4 non-empty cells lie on the main diagonal; there is one main class when the entries in these cells are distinct and three where an element is repeated. In the latter case the three classes are distinguished by the number of times that the repeated element occurs in the row and column containing the non-empty cell off the main diagonal.

1		2		
	2			
		3		
			4	

1	4			
	1			
		2		
			3	

1				
	1	4		
		2		
			3	

1				
	1			
		2	4	
			3	

There are two non-isotopic partial latin squares of type (b) but they are $(3, 1, 2)$-conjugate to latin squares of type (a). We give representatives from each isotopy class with the property that their $(3, 1, 2)$-conjugates appear above:

1				
2				
	3		2	
		4		

1				
2				
	3			
		4	3	

3 Defining sets in group-based latin squares

In this section we prove that for a group G the density of a smallest critical set in $M(G)$ approaches 0 as the order of G increases without bound. In

fact the partial latin squares we construct have the stronger property that they are UC over all group-based latin squares. A fundamental property of a group-based latin square is the so called *quadrangle criterion* which states that a latin square L is based on a group if and only if for all pairs of sets $\{(h_1, j_1, a), (h_1, k_1, b), (i_1, j_1, c), (i_1, k_1, d)\}$ and $\{(h_2, j_2, a), (h_2, k_2, b), (i_2, j_2, c), (i_2, k_2, x)\}$ we have that $x = d$ (see [3] for details). In the following theorem we construct partial latin squares that complete to a group-based latin square by considering quadrangles only. Such a partial latin square is not only UC in $M(G)$ but also UC over all group-based latin squares. In Theorem 3 we prove that the density of this partial latin square tends to 0 as the order of the group increases without bound.

Theorem 2 *Let G be a group of order n with a set of generators of size k. Then there is a partial latin square of order n with $n + (n-1)(k+1)$ entries which is uniquely completable to a Cayley table of G, given that we know that the partial latin square must complete to the Cayley table of some group.*

Proof: Let $\{g_1, g_2, \ldots, g_k\}$ be a set of generators of G. To construct the partial latin square take the Cayley table of G and delete all of the entries apart from one complete row and all occurrences of elements from $\{e, g_1, g_2, \ldots, g_k\}$. This gives a partial latin square with $n + (n-1)(k+1)$ entries.

As we know that the full latin square must be the Cayley table of a group we can use the quadrangle criterion to fill in entries of the square.

Suppose we have all occurrences of x and y for some $x, y \in G$. Then we have the full quadrangle

	u^{-1}	$u^{-1}y$
xu	x	xy
u	e	y

for some u, where x and xy are entries in the full row of our partial latin square. We can now use the quadrangle criterion to fill in the remaining $n-1$ occurrences of xy.

Let $g \in G$, then $g = g_{i_1} g_{i_2} \cdots g_{i_m}$ for some m, where the g_{i_j} are generators. As we have all occurrences of the generators we can fill in all occurrences of $g_{i_1} g_{i_2}$ and then all occurrences of $g_{i_1} g_{i_2} g_{i_3}$ and so on until finally all occurrences of g are entered. This applies to any $g \in G$ so the partial latin square completes to the Cayley table of G as required.

Theorem 3 *Let G be a group of order n and k be the size of a minimal set of generators of G. Then*

$$\lim_{n \to \infty} \frac{n + (n-1)(k+1)}{n^2} = 0.$$

Proof: Let $\{g_1, g_2, \ldots, g_k\}$ be a minimal set of generators of G. There are 2^k elements of the form $g_{i_1} g_{i_2} \cdots g_{i_m}$ where $0 \leq m \leq k$ and $i_j < i_{j'}$ whenever $j < j'$. These elements must all be different or we would be able to reduce the

size of the set of generators (for example, if $g_1g_2 = g_3g_4$ then $g_1 = g_3g_4{g_2}^{-1}$ and we could omit g_1 from the set of generators).

So we have that $k \leq \log_2 n$ and hence

$$\lim_{n\to\infty} \frac{n + (n-1)(k+1)}{n^2} \quad \leq \quad \lim_{n\to\infty} \frac{2n + n\log_2 n - \log_2 n - 1}{n^2} = 0.$$

In [10] Weaver has used the above result and a consideration of special cases to show that every group of order $n > 8$ has a defining set over group-based latin squares of size less than $\lfloor n^2/4 \rfloor$.

4 Keedwell's conjecture

As previously stated, Keedwell [5] has conjectured that for all group-based latin squares, except those based on a cyclic group, the density of a smallest critical set tends to 1/2 as the order of the square tends to infinity. To disprove this conjecture we consider $C_2 \times C_m$ for even m. We way write the Cayley for $C_2 \times C_m$ as follows:

C_m	C_m^1
C_m^1	C_m

where C_m^1 is the array obtained by adding m to each entry of C_m. It is easy to see that

P_m	P_m^1
P_m^1	C_m

is a defining set for $C_2 \times C_m$ where $P_m = \{(i, j, (i + j) \bmod m : i + j < (n - 1)/2 \text{ or } i + j \geq (3n - 1)/2\}$ and P_m^1 is the array obtained by adding m to each entry of P_m. The density of the above partial latin square is 7/16 for all m (P_m is the well known critical set for C_m of density 1/4 introduced by Nelder [9] and shown to be critical by Curren and van Rees [2]).

The above reasoning may be extended in various ways to cover other direct products of cyclic groups and non-cyclic groups with a subgroup of index 2, but the above is sufficient for our purposes.

References

[1] J. A. Bate and G. H. J. van Rees, *The size of the smallest strong critical set in a latin square*, Ars Combinatoria, 53(1999), pp 73–83.

[2] D. Curren and G. H. J. van Rees, *Critical sets in latin squares*, Congr. Num. 22(1978), pp 165–168.

[3] J. Dénes and A. D. Keedwell, *Latin Squares and their Applications.* (Akadémiai Kiadó, Budapest/English Universities Press, London/Academic Press, New York, 1974.)

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

[5] A. D. Keedwell, Critical sets and critical partial latin squares, in "Graph Theory, Combinatorics, Algorithms and Applications" (Proc. Third China-USA Internat. Conf. Beijing, June 1–5, 1993), pp. 111-124, World Scientific Publ. Co., Singapore, 1994.

[6] A. D. Keedwell, *Critical sets for orthogonal latin squares of small order,* Congressus Numerantium **125** (1997), pp. 51–64.

[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, 51(1999), pp 97–104.

[8] E. S. Mahmoodian, *Some problems in graph colourings,* in Proc. 26th Annual Iranian Math. Conference, S. Javadpour and M. Radjabalipour, eds., Kerman, Iran, Mar. 1995, Iranian Math. Soc. University of Kerman, pp 215–218.

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

[10] H. Weaver, *Defining sets for Cayley tables of groups*, Research Report 01-?, Department of Mathematics, Keele University, 2001.