Des Codes Crypt (2006) 40:131–135
DOI 10.1007/s10623-006-8168-9

The existence of latin squares without orthogonal mates

Ian M. Wanless · Bridget S. Webb

Received: 4 January 2006 / Accepted: 6 March 2006

Abstract A latin square is a bachelor square if it does not possess an orthogonal mate; equivalently, it does not have a decomposition into disjoint transversals. We define a latin square to be a *confirmed bachelor square* if it contains an entry through which there is no transversal. We prove the existence of confirmed bachelor squares for all orders greater than three. This resolves the existence question for bachelor squares.

Keywords Latin square · Bachelor square · MOLS · Transversal · Latin trade

AMS Classification 05B15

1. Introduction

We assume familiarity with the basic terminology of latin squares such as can be found in [3].

A *bachelor latin square* is a latin square which has no orthogonal mate; or equivalently, is a latin square with no decomposition into disjoint transversals. We define a *confirmed bachelor square* to be a latin square that contains an entry through which no transversal passes. Thus a confirmed bachelor square is necessarily a bachelor square.

The purpose of this note is to prove:

Theorem 1.1 *For any positive integer $n \notin \{1, 3\}$ there exists a confirmed bachelor square of order n.*

The existence of bachelor squares follows directly:

Communicated by D. Jungnickel.

I.M. Wanless(✉)
School of Mathematical Sciences,
Monash University, Vic 3800, Australia
e-mail: ian.wanless@sci.monash.edu.au

B.S. Webb
Department of Mathematics
The Open University,
Milton Keynes, MK7 6AA, UK
e-mail: b.s.webb@open.ac.uk

Corollary 1.1 *For any positive integer $n \notin \{1, 3\}$ there exists a bachelor square of order n.*

Despite a vast literature on orthogonal latin squares it seems the existence problem for bachelor latin squares has not been previously settled. For even orders the problem is simple, since there are many constructions for squares which have no transversals at all (see, e.g., [3, Section 12.3] and also Corollary 2.1). Some of these constructions can be traced as far back as Euler, who should therefore be credited with the first existence results for bachelor squares (although the name "bachelor square" seems to be comparatively recent [10]).

For odd orders the problem is harder because there are thought to be no latin squares without transversals. A conjecture to this effect is attributed to Ryser. Our Theorem 1.1 gives one indication why Ryser's conjecture is hard to prove (if indeed it is true). The existence of bachelor squares of orders $n \equiv 1 \bmod 4$ was shown by Mann [8], although he did not demonstrate the existence of any *confirmed* bachelors. Surprisingly, the case $n \equiv 3 \bmod 4$ has resisted proof until now. It is listed as an unsolved problem in a number of places, including [1, Section 3.3; 2, X. 8.13; 4; 7, p. 181; 10].

Throughout this note we shall assume that L is a latin square of order n, and all calculations will be in the cyclic group $\mathbb{Z}_n$. Our latin squares will use $\mathbb{Z}_n$ as their symbol set and we use the same set to index the rows and columns. We let $L[x, y]$ denote the symbol in row x and column y of a latin square L. It will prove convenient to think of a latin square of order n as a set of n^2 triples, or *elements*, of the form $(x, y, L[x, y])$. We denote by Z_n, the cyclic square of order n; this is the group table of $\mathbb{Z}_n$ under addition. Thus $Z_n[i, j] = i + j \bmod n$, for all i and j.

2. The Δ function

We define the following function on the elements (x, y, z) of L.

$$\Delta(x, y, z) = z - x - y \bmod n.$$

Summing the Δ values (mod n) for the elements of a row r of L, we get:

$$\sum_{i=0}^{n-1} \Delta\big(r, i, L(r, i)\big) = \sum_{i=0}^{n-1} \big(L(r, i) - r - i\big) = \sum_{i=0}^{n-1} i - \sum_{i=0}^{n-1} r - \sum_{i=0}^{n-1} i = nr = 0.$$

Of course, the corresponding result holds for columns. These results give a useful consistency check when calculating Δ values.

Now suppose that T is a transversal of L. The following simple Lemma is crucial.

Lemma 2.1 *The sum of the Δ values over the elements of T is $0 \bmod n$, if n is odd, and $\frac{1}{2}n \bmod n$, if n is even.*

Proof A transversal, by definition, comprises one element from each row, one element from each column, and one element from each symbol. Hence,

$$\sum_{e\in T} \Delta(e) = \sum_{i=0}^{n-1} i - \sum_{i=0}^{n-1} i - \sum_{i=0}^{n-1} i = -\tfrac{1}{2}n(n-1),$$

from which the Lemma follows. □

Since Δ is identically zero mod n on every element of Z_n, Lemma 2.1 immediately gives the following well known result:

Corollary 2.1 *The cyclic square Z_n has no transversal if n is even.*

If a latin square is nearly Z_n; that is, Z_n with a few elements amended, then Lemma 2.1 gives us significant restrictions on possible transversals through the amended entries. In another terminology, these amended entries are known as a *trade*. The key to our result is to find a trade in Z_n to create an entry with a Δ value which cannot satisfy Lemma 2.1. We do this in the next section.

3. Existence of confirmed bachelor squares

We now prove the main theorem of this paper, Theorem 1.1.

Proof of Theorem 1.1 It is trivial to verify that bachelor squares do not exist for $n \in \{1, 3\}$. To show existence for all other orders we split into the three cases $n \equiv 0 \bmod 2$, $n \equiv 1 \bmod 4$ and $n \equiv 3 \bmod 4$.

Case $n \equiv 0 \bmod 2$

By Corollary 2.1, Z_n has no transversals, so it is a confirmed bachelor square.

Case $n \equiv 1 \bmod 4$

We define a latin square L of order $n \geq 5$ as follows, with the Δ value for each element given in parentheses.

$$
\begin{array}{ll}
L[i, j] = i + j \bmod n, & \text{except for the following entries:} \\
L[0, 0] = 1 & \quad (1), \\
L[0, 1] = 0 & \quad (-1) \\
\\
\text{for } i = 1, 3, \ldots, \frac{n-7}{2}, & \\
\quad L[i, 0] = i + 2 & \quad (2), \\
\quad L[i, 2] = i & \quad (-2), \\
\\
L[\frac{n-3}{2}, 0] = 0 & \quad (-\frac{n-3}{2}), \\
L[\frac{n-3}{2}, 2] = \frac{n-3}{2} & \quad (-2), \\
L[\frac{n-3}{2}, \frac{n+3}{2}] = \frac{n+1}{2} & \quad (-\frac{n-1}{2}), \\
\\
L[n-1, 1] = 1 & \quad (1), \\
L[n-1, 2] = \frac{n+1}{2} & \quad (\frac{n-1}{2}), \\
L[n-1, \frac{n+3}{2}] = 0 & \quad (\frac{n-1}{2}).
\end{array}
$$

Consider a possible transversal T which includes the element $e_2 = (n-1, 2, \frac{n+1}{2})$ which has $\Delta(e_2) = \frac{n-1}{2}$. Since T cannot include any other element which shares a row, column or symbol with e_2, the only elements of T which might have non-zero values of Δ are the elements e_0 and e_1 in columns 0 and 1, respectively. The only possibilities are $\Delta(e_0) \in \{0, 1, 2, -\frac{n-3}{2}\}$ and $\Delta(e_1) \in \{0, -1\}$. Also, it is impossible that both $\Delta(e_0) = -\frac{n-3}{2}$ and $\Delta(e_1) = -1$, since this would involve the symbol 0 being repeated in T. A simple list of the possible combinations shows that there is no way to achieve $\Delta(e_0) + \Delta(e_1) + \Delta(e_2) = 0 \bmod n$, so that T does not exist.

Case $n \equiv 3 \bmod 4$

We define a latin square L of order $n \geq 7$ as follows, with the Δ value for each element given in parentheses.

$$
\begin{array}{ll}
L[i,j] = i + j \bmod n, & \text{except for the following entries:} \\
L[0,0] = 1 & (1), \\
L[0,1] = 0 & (-1) \\
 & \\
\text{for } i = 1, 3, \ldots, \frac{n-5}{2}, & \\
\quad L[i,0] = i + 2 & (2), \\
\quad L[i,2] = i & (-2), \\
 & \\
L[\frac{n-1}{2}, 0] = 0 & (-\frac{n-1}{2}), \\
L[\frac{n-1}{2}, \frac{n+1}{2}] = \frac{n-1}{2} & (\frac{n-1}{2}), \\
 & \\
L[n-1, 1] = 1 & (1), \\
L[n-1, 2] = \frac{n-1}{2} & (\frac{n-3}{2}), \\
L[n-1, \frac{n+1}{2}] = 0 & (-\frac{n-1}{2}).
\end{array}
$$

Consider a possible transversal T which includes the element $e = (n-1, \frac{n+1}{2}, 0)$ which has $\Delta(e) = -\frac{n-1}{2}$. Since T cannot include any other element which shares a row, column or symbol with e, the only elements of T which might have non-zero values of Δ are the elements e_0 and e_2 in columns 0 and 2, respectively. The only possibilities are $\Delta(e_0) \in \{0, 1, 2\}$, and $\Delta(e_2) \in \{0, -2\}$. Since $|\Delta(e_0) + \Delta(e_2)| \leq 2$ and $\Delta(e) = -\frac{n-1}{2}$ there is no way to achieve $\Delta(e_0) + \Delta(e_2) + \Delta(e) = 0 \bmod n$ when $n \geq 7$, so that T does not exist. □

4. Concluding remarks

By analogous arguments to those used in the proof of Theorem 1.1 it can be shown that several (though not all) of the amended entries cannot have transversals through them. In particular, for any odd $n > 5$ the three amended entries in the last row of L cannot be in transversals. For $n = 5$ that result is not true, but by other means it can be shown that all transversals of L include the element $(0, 3, 3)$. We can therefore deduce that for all $n > 3$ there exists a latin square of order n which has no set of more than $n-3$ disjoint transversals.

Van Rees [10] has conjectured that the proportion of latin squares of order n which are bachelors tends to one as $n \to \infty$. However, this conjecture was based on a study of very small orders. Our experience in studying slightly larger orders leads us to the opposite conclusion; that the proportion of bachelors probably tends quickly to zero. Some experimental evidence in this direction has been obtained by McKay et al. [9], who tested 10 million random latin squares of order 10 and found that a minority of them were bachelors. It may even be true that the average, over all latin squares L of order n, of the size of the largest set of MOLS involving L tends to infinity as $n \to \infty$. However, even testing this proposition experimentally seems difficult at this stage.

Although elementary, Lemma 2.1 seems to be a useful tool for studying transversals. We have used it to demonstrate the existence of confirmed bachelor squares, but it can also be used for solving other problems. For example, it has been used in [5] to show existence results for latin squares with particular generalised transversals. We finish by applying Lemma 2.1 to a latin square of order 11 which has a transversal through every entry, but nonetheless is a bachelor square.

Let L be the following symmetric latin square (in which the borders indicate the indices for the rows and columns):

	0	1	4	5	9	3	10	7	6	2	8
0	0	1	4	5	9	3	10	7	6	2	8
1	1	6	5	10	2	4	0	8	7	3	9
4	4	5	2	9	7	8	3	0	10	6	1
5	5	10	9	8	3	6	4	1	0	7	2
9	9	2	7	3	10	1	8	5	4	0	6
3	3	4	8	6	1	7	2	10	9	5	0
10	10	0	3	4	8	2	9	6	5	1	7
7	7	8	0	1	5	10	6	3	2	9	4
6	6	7	10	0	4	9	5	2	1	8	3
2	2	3	6	7	0	5	1	9	8	4	10
8	8	9	1	2	6	0	7	4	3	10	5

Let E denote the set of elements in L which have non-zero values of Δ. There are 15 elements in E and they all occur in rows and columns indexed by non-zero quadratic residues in $\mathbb{Z}_{11}$. The Δ values for those entries are as follows:

	1	4	5	9	3
1	4	0	4	3	0
4	0	5	0	5	1
5	4	0	−2	0	−2
9	3	5	0	3	0
3	0	1	−2	0	1

It is a simple matter to check that no non-zero value of Δ can be repeated on a transversal. Hence, by Lemma 2.1, any transversal T which includes an element of E must include five elements of E, with Δ values being $1, -2, 3, 4$, and 5 in some order. This accounts for all elements of T which lie in rows or columns indexed by non-zero quadratic residues. It follows that the only place T can include the symbol 0 is in the element $(0, 0, 0)$. Thus every transversal through an element of E includes $(0, 0, 0)$, so it is impossible to decompose L into disjoint transversals. Although L is a bachelor square, it is easy to check with a computer that it is not a confirmed bachelor.

Acknowledgments The authors are grateful for discussions with Peter Danziger and Aleš Drápal during the early stages of the investigation. After submitting this paper we received a preprint [6] in which Evans has independently obtained our Corollary 1.1 using a variation of our technique.

References

1. Beth T, Jungnickel D, Lenz H (1986) Design theory. Cambridge University Press, Cambridge
2. Beth T, Jungnickel D, Lenz H (1999) Design theory, 2nd edn, vol. II. Cambridge University Press, Cambridge
3. Dénes J, Keedwell AD (1974) Latin squares and their applications. Akadémiai Kiadó, Budapest
4. Drake DA, van Rees GHJ, Wallis WD (1999) Maximal sets of mutually orthogonal latin squares. Discrete Math 194:87–94
5. Egan JA, Wanless IM (2006) Latin squares with no small odd k-plexes, preprint
6. Evans AB (2006) Latin squares without orthogonal mates. Des Codes Crypt 40:121–130
7. Jungnickel D (1990) Latin squares, their geometries and their groups: a survey. In: Ray-Chaudhuri D (ed) Coding theory and design theory. Part II. Design Theory. Springer-Verlag, New York, pp 166–225
8. Mann HB (1944) On orthogonal latin squares. Bull Amer Math Soc 50:249–257
9. McKay BD, Meynert A, Myrvold W (2006) Small latin squares, quasigroups and loops. J Combin Des to appear http://dx.doi.org/10.1002/jcd.20105
10. van Rees GHJ (1990) Subsquares and transversals in latin squares. Ars Combin 29B:193–204