James Lefevre; Diane Donovan; Nicholas J. Cavenagh; Aleš Drápal

Minimal and minimum size latin bitrades of each genus

Commentationes Mathematicae Universitatis Carolinae, Vol. 48 (2007), No. 2, 189--203

Persistent URL: `http://dml.cz/dmlcz/119649`

Comment.Math.Univ.Carolin. 48,2 (2007)189–203

Minimal and minimum size latin bitrades of each genus

James Lefevre, Diane Donovan, Nicholas Cavenagh, Aleš Drápal

Abstract. Suppose that T° and $T^\star$ are partial latin squares of order n, with the property that each row and each column of T° contains the same set of entries as the corresponding row or column of $T^\star$. In addition, suppose that each cell in T° contains an entry if and only if the corresponding cell in $T^\star$ contains an entry, and these entries (if they exist) are different. Then the pair $T = (T^\circ, T^\star)$ forms a *latin bitrade*. The *size* of T is the total number of filled cells in T° (equivalently $T^\star$). The latin bitrade is *minimal* if there is no latin bitrade $(U^\circ, U^\otimes)$ such that $U^\circ \subsetneq T^\circ$. Drápal (2003) represented latin bitrades in terms of row, column and entry cycles, which he proved formed a coherent digraph. This digraph can be considered as a combinatorial surface, thus associating each latin bitrade with an integer genus, which is a robust structural property of the latin bitrade. For each genus $g \geq 0$, we construct a latin bitrade of smallest possible size, and also a minimal latin bitrade of size $8g + 8$.

Keywords: latin trade, bitrade, genus

Classification: 05B15

1. Introduction

We define a *partial latin square* P° of order n to be a pair $(N, \circ)$, where $N = N(n) = \{0, 1, \ldots, n-1\}$, and $\circ$ is a binary operation mapping some subset of $N \times N$ to N, which satisfies the following conditions:

- if $i \circ j = i' \circ j$ then $i = i'$,
- if $i \circ j = i \circ j'$ then $j = j'$.

A *latin square* L° is a partial latin square in which $\circ$ is defined everywhere on $N \times N$. In this case $\circ$ is a well defined binary operation on N, and $L^\circ = (N, \circ)$ is a quasigroup. Note that a latin square is also a partial latin square. We adopt the convention that, for example, P° and Q° may denote different partial latin squares; that is, two partial latin squares may use the same symbol to denote different operators (although we use different symbols where confusion might occur).

We often consider a partial latin square P° in terms of its Cayley table: this will consist of an $n \times n$ array of cells which are partially filled with entries from

Donovan and Lefevre supported by grant DP0664030.
Drápal supported by grants DP0664030, LX0453416 and MSM0021620839.

N (together with a headline and sideline). From the above conditions, each entry will occur at most once in each row, and at most once in each column. If P° is a latin square, all the cells will be filled.

We may also (interchangeably) regard P° as a subset of $N \times N \times N$, with $(i,j,k) \in P^\circ$ if and only if $i \circ j = k$. We refer to i, j and k as the row, column and entry respectively. (Note that an *entry* of P° is one of the symbols in the array while an *element* of P° is an ordered triple.) Note that it is common to give the primary definition of a (partial) latin square in terms of either the set of ordered triples or the $n \times n$ array of entries (typically without the headline and sideline). When partial latin squares are used with set notation such as $\subseteq$ or $\cup$, the partial latin square should be interpreted as a triple set; thus $P^\circ \subseteq Q^\star$ if $i \circ j = k \Rightarrow i \star j = k$ (so if $i \star j = k$, then either $i \circ j = k$ or else $i \circ j$ is undefined).

A *latin bitrade* (of order n) is an ordered pair $(T^\circ, T^\star)$ of partial latin squares (of order n) such that for each $i, j, k \in N$ satisfying $i \circ j = k$ (respectively, $i \star j = k$), there exists:

- $i' \neq i$ such that $i' \star j = k$ (respectively, $i' \circ j = k$),
- $j' \neq j$ such that $i \star j' = k$ (respectively, $i \circ j' = k$),
- $k' \neq k$ such that $i \star j = k'$ (respectively, $i \circ j = k'$).

Thus, each row i of T° contains the same set of entries as row i of $T^\star$ (row i is *balanced*), and each column of T° contains the same set of entries as $T^\star$ (column j is *balanced*). Moreover $T^\star$ and T° occupy the same set of cells and are disjoint.

The first study of latin bitrades appeared in [DrKe1], where they are referred to as *exchangeable partial groupoids*. Later (and at first independently), latin bitrades were studied because of their connection to the intersection of latin squares ([5]). More recently, latin bitrades became of interest to researchers of critical sets (minimal defining sets of latin squares) ([2], [7], [1]). As discussed in [10], latin bitrades may be applied to the compact storage of large catalogues of latin squares. Results on other kinds of combinatorial trades may be found in [9] and [8].

We define the *size* of a partial latin square P°, denoted $|P^\circ|$, to be the number of filled cells in the Cayley table. Regarding P° as a set of ordered triples, this is just the standard notation for set size. We define the size of a latin bitrade $T = (T^\circ, T^\star)$, denoted by $|T|$, to be the size of the two component partial latin squares; so $|T| = |T^\circ| = |T^\star|$. The smallest possible size of a latin bitrade is four; we call a latin bitrade of this size an *intercalate*.

The representation of a partial latin square as a set of ordered triples highlights a level of symmetry between the rows, columns and entries of a latin square or latin bitrade which is not clear in other representations. Given $P^\circ \in N \times N \times N$, the necessary and sufficient conditions for P° to be a partial latin square are

- if $(i,j,k), (i',j,k) \in P^\circ$ then $i = i'$,
- if $(i,j,k), (i,j',k) \in P^\circ$ then $j = j'$ and
- if $(i,j,k), (i,j,k') \in P^\circ$ then $k = k'$.

(The third condition corresponds to the operation $\circ$ being uniquely defined.) It follows that any consistent reordering of the triples in P° will produce another partial latin square of the same size. The definition of a latin bitrade given earlier is similarly symmetric with respect to rows, columns and entries; thus any consistent reordering of the triples in a latin bitrade will produce a second latin bitrade of the same size.

Next, given a latin bitrade $(T^\circ, T^\star)$ we define the following permutations on the elements of T°:

$$\begin{aligned}\tau_1((i,j,k)) &= (i,j',k') \text{ iff } (i,j,k') \in T^\star,\\ \tau_2((i,j,k)) &= (i',j,k') \text{ iff } (i',j,k) \in T^\star,\\ \tau_3((i,j,k)) &= (i',j',k) \text{ iff } (i,j',k) \in T^\star.\end{aligned}$$

Note that τ_1 is invariant on rows, τ_2 on columns and τ_3 on entries. In fact, it is easy to see that $\tau_1\tau_2\tau_3 = 1$ (evaluating permutations from the right).

Now, consider a digraph whose vertices are elements of T° and whose directed edges are the ordered pairs of the form $(v, \tau_i(v))$, where $v \in T^\circ$. Drápal ([3]) showed that this digraph is coherent (that is, each face is oriented in one direction), and thus, from Euler's formula, a latin bitrade may be associated with a non-negative, integer genus:

$$g = (2 + E - V - F)/2, \tag{1}$$

where V, F and E are the number of vertices, faces and edges in the digraph. Each cycle of τ_i, $i \in \{1,2,3\}$, contributes a face, and $\tau_1\tau_2\tau_3 = 1$ implies that, in addition, for each vertex there is a corresponding triangular face. Thus $F = |T| + \omega(\tau_1) + \omega(\tau_2) + \omega(\tau_3)$, where $\omega(\phi)$ denotes the number of cycles in the permutation ϕ. Then, since $V = |T|$ and $E = 3|T|$, equation (1) becomes:

$$g = (2 + |T| - \omega(\tau_1) - \omega(\tau_2) - \omega(\tau_3))/2. \tag{2}$$

A latin bitrade is said to be *separated* if each row, column and entry give rise to a unique cycle in τ_1, τ_2 and τ_3, respectively. So for a separated latin bitrade the genus is given by:

$$g = (2 + |T| - r - c - e)/2, \tag{3}$$

where r, c and e stand for the number of rows, columns and entries, respectively. Any latin bitrade may be made separated by a straightforward process of splitting rows, columns and entries. This process does not change the size of the latin bitrade, so for the purposes of this paper, we may assume that all latin bitrades are separated. We define $O(T) = \omega(\tau_1) + \omega(\tau_2) + \omega(\tau_3)$; provided that the latin bitrade is separated, this becomes $O(T) = r + c + e$. We noted above that a consistent reordering of the triples in a latin bitrade $(T^\circ, T^\star)$ will produce another latin bitrade of the same size. Such a consistent reordering will reorder the triple (τ_1, τ_2, τ_3), and will possibly invert each of these three permutations, but it will not alter $O(T)$, the genus, or whether the latin bitrade is separated.

The concept of genus has become an important and useful way of classifying and interpreting latin bitrades. We conjecture that any latin bitrade of genus 0 can be embedded in the Cayley table of an abelian group.

Example. Let $(T^\circ, T^\star)$ be the following *latin bitrade* of order 3 and size 6:

$T^\circ =$

$\circ$	0	1	2
0	0	1	2
1	1	2	0
2			

$T^\star =$

$\star$	0	1	2
0	1	2	0
1	0	1	2
2			

We may also write:

$$T^\circ = \{(0,0,0), (0,1,1), (0,2,2), (1,0,1), (1,1,2), (1,2,0)\} \text{ and}$$
$$T^\star = \{(0,0,1), (0,1,2), (0,2,0), (1,0,0), (1,1,1), (1,2,2)\}.$$

Next,

$$\tau_1 = ((0,0,0)\ (0,1,1)\ (0,2,2))((1,0,1)\ (1,2,0)\ (1,1,2)),$$
$$\tau_2 = ((0,0,0)\ (1,0,1))((0,1,1)\ (1,1,2))((0,2,2)\ (1,2,0)) \text{ and}$$
$$\tau_3 = ((0,0,0)\ (1,2,0))((0,1,1)\ (1,0,1))((0,2,2)\ (1,1,2)).$$

Thus the genus of this latin bitrade is equal to $(2 + 6 - 8)/2 = 0$. Indeed, its digraph is planar, as shown in Figure 1. (The edges from τ_1, τ_2 and τ_3 are shown with solid, dot-dash and dashed arrows, respectively.)

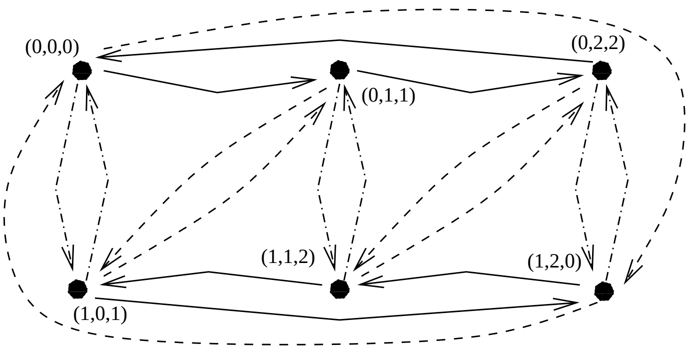

Figure 1: The planar digraph associated with $(T^\star, T^\circ)$

This paper explores the relationship between the genus and the size of a latin bitrade. We pose the question: For a given genus, what is the size of the smallest latin bitrade that has that genus? We give an exact answer to this question.

Theorem 1.2. *Let g be an arbitrary non-negative integer, and define $n \in \mathbb{Z}$ by $n = \lceil (3 + \sqrt{8g+1})/2 \rceil$. The minimum size of a latin bitrade of genus g is*

$$\begin{cases} 3n + 2g - 3, & \text{if } n \geq 2 + \sqrt{2g+1}; \\ 3n + 2g - 2, & \text{if } n < 2 + \sqrt{2g+1}. \end{cases}$$

A latin bitrade $(T^\circ, T^\star)$ is said to be *minimal* if there exists no latin bitrade $(U^\circ, U^\otimes)$ such that $U^\circ \subset T^\circ$. Note that for minimality we do not require that $U^\otimes \subset T^\star$. The property of minimality is relevant to the study of critical sets of latin squares, as a critical set must intersect every minimal latin trade within a latin square. For a recent survey on critical sets in latin squares, see [7]. In Section 4 we construct minimal bitrades of genus g and size $8g + 8$.

2. The lower bound

Let $T = \{T^\circ, T^\star\}$ be a separated latin bitrade of genus g. Rearranging equation (3),

$$|T| = O(T) + 2g - 2. \tag{4}$$

For a given genus, minimising $O(T) = r + c + e$ is equivalent to minimising $|T|$. Since any consistent reordering of the triples in a separated latin bitrade produces a second separated latin bitrade of the same size and genus, we assume without loss of generality that

$$2 \leq r \leq c \leq e. \tag{5}$$

There are at most rc cells in T°, so $|T| \leq rc$. Therefore

$$rc \geq r + c + e + 2g - 2. \tag{6}$$

We can produce a lower bound on $O(T)$ by minimising $r + c + e$ subject to the inequalities (5) and (6) (r, c and e must be integers of course).

Lemma 2.1. *Let g be a non-negative integer, and define $n = \lceil (3 + \sqrt{8g+1})/2 \rceil$. Given that r, c, e are integers satisfying inequalities* (5) *and* (6)*, the sum $r + c + e$ is minimised when*

$$\begin{cases} [r, c, e] = [n-1, n, n], & \text{if } n \geq 2 + \sqrt{2g+1}; \\ [r, c, e] = [n, n, n], & \text{if } n < 2 + \sqrt{2g+1}. \end{cases}$$

Proof: If $g = 0$, then $r = c = e = 2$ satisfies (5) and (6), and this solution minimises $r+c+e$ subject to (5). This proves the lemma for $g = 0$, so from here on we assume that $g \geq 1$. If $r = 2$, inequality (6) gives $2c \geq 2+c+e+2g-2 \geq 2c+2g$, contradicting $g \geq 1$; hence we may also assume that $3 \leq r \leq c \leq e$ for the remainder of the proof.

We begin by looking for solutions in which $r = c = e$. Inequality (6) becomes $r^2 \geq 3r+2g-2$. Since $g \geq 1$ and $r > 2$, this has the solution $r \geq (3+\sqrt{8g+1})/2$. Hence the integer solution to (5) and (6) in which r, c and e are equal and $r+c+e$ is minimised is $r = c = e = n$, where

$$n = \lceil (3 + \sqrt{8g+1})/2 \rceil.$$

In this case $r + c + e = 3n$.

We now look for solutions in which r, c, e are not equal. In order for such a solution to be an improvement upon the solution $r = c = e = n$, we require that $r + c + e < 3n$; by (5), it follows that $r < n$. Let $r = n - 1 - d$, where $d \geq 0$. Suppose that $c \leq n - 1 + d$ (we seek a contradiction). By (5) and (6) we have $rc \geq r+2c+2g-2$ and hence $c \geq (r+2g-2)/(r-2)$. Therefore, by assumption, $n+d-1 \geq (r+2g-2)/(r-2)$. Substituting $r = n-1-d$ and simplifying gives

$$n^2 - d - d^2 - 5n + 6 \geq 2g. \tag{7}$$

By the definition of n, we have $n - 1 < (3 + \sqrt{8g+1})/2$, and hence

$$(n-1)(n-4) < (\sqrt{8g+1} + 3)(\sqrt{8g+1} - 3)/4$$

(we have $r \geq 3$ and $r \leq n-1$, so $n \geq 4$). Rearranging this inequality gives $n^2 < 5n + 2g - 6$; with (7) this gives $-d - d^2 > 0$, contradicting the condition $d \geq 0$. Thus by contradiction we have $c \geq n + d$, and hence also $e \geq n + d$, giving $r + c + e \geq 3n - 1 + d$. It follows that the only possible solution in which $r + c + e < 3n$ is $r = n - 1$, $c = e = n$, giving $r + c + e = 3n - 1$.

By (6), this is a solution if and only if $n(n-1) \geq 3n - 1 + 2g - 2$; that is, $n^2 - 4n + 3 \geq 2g$. Solving gives $n \geq 2 + \sqrt{2g+1}$ (since n and g are positive integers we can rule out the alternative solution, $n \leq 2 - \sqrt{2g+1}$).

Therefore $[r, c, e] = [n-1, n, n]$ is the minimal integer solution to inequalities (5) and (6) if and only if

$$n \geq 2 + \sqrt{2g+1}.$$

Otherwise, the minimal integer solution is $[r, c, e] = [n, n, n]$. □

With equation (4), we can convert this lower bound on $O(T) = r+c+e$ into a lower bound on $|T|$ (for a given genus). This is the bound given by Theorem 1.2; in the following section we prove that this bound is tight.

3. Constructions

We now wish to construct, for each $g \geq 0$, separated latin bitrades of genus g in which the number of rows, columns and entries correspond to the minimum values given by Lemma 2.1. We begin by reformulating the conditions slightly. By the definition of n in Lemma 2.1, we have $n-1 < (3+\sqrt{8g+1})/2 \leq n$. This is equivalent to $(n-2)(n-3)/2 < g \leq (n-1)(n-2)/2$. Likewise the condition $n \geq 2+\sqrt{2g+1}$ is equivalent to $g \leq (n-1)(n-3)/2$. Thus we can state the construction problem as follows: Let $n \geq 2$ be an integer; for every integer g satisfying

$$(n-1)(n-3)/2 < g \leq (n-1)(n-2)/2,$$

we must construct a separated latin bitrade of genus g with $[r,c,e] = [n,n,n]$, while for every integer g satisfying

$$(n-2)(n-3)/2 < g \leq (n-1)(n-3)/2,$$

we must construct a separated latin bitrade of genus g with $[r,c,e] = [n-1,n,n]$.

We can further restate the construction problem in terms of the size of the latin bitrade; this is the easiest form to check. By equation (4), we have $|T| = 3n+2g-2$ if $[r,c,e] = [n,n,n]$ and $|T| = 3n+2g-3$ if $[r,c,e] = [n-1,n,n]$. Note also that in the second case, we have $(n-2)(n-3)/2 < (n-1)(n-3)/2$, and hence $n \geq 4$; but $n = 4$ gives $1 < g \leq 3/2$, so in fact $n \geq 5$. Therefore:

Case 1: for every integer $n \geq 2$ and size S satisfying $S \equiv n \pmod 2$ and

$$n^2 - n + 1 < S \leq n^2,$$

we must construct a separated latin bitrade T with $[r,c,e] = [n,n,n]$ and $|T| = S$.

Case 2: for every integer $n \geq 5$ and size S satisfying $S \equiv n+1 \pmod 2$ and

$$n(n-1) - n + 3 < S \leq n(n-1),$$

we must construct a separated latin bitrade with $[r,c,e] = [n-1,n,n]$ and $|T| = S$.

Case 1:

We start with a well-known separated bitrade (see, for example, [6]). Let $n \geq 2$ be an integer. Taking all addition modulo n, define $C_n = (C_n^{\circ}, C_n^{\star})$, where

$$C_n^{\circ} = \{(i,j,i+j) \mid i,j \in \mathbb{Z}_n\},$$
$$C_n^{\star} = \{(i,j,i+j+1) \mid i,j \in \mathbb{Z}_n\}.$$

Then C_n is a latin bitrade of size n^2 with $r = c = e = n$. The row, column and symbol permutations τ_1, τ_2, τ_3 satisfy

$$\begin{aligned}\tau_1((i,j,i+j)) &= (i,j+1,i+j+1),\\ \tau_2((i,j,i+j)) &= (i-1,j,i+j-1),\\ \tau_3((i,j,i+j)) &= (i+1,j-1,i+j),\end{aligned}$$

for every $i, j \in \mathbb{Z}_n$. It follows that the permutation on each row, column and entry is a single cycle; that is, C_n is separated. Therefore C_n is the required construction for Case 1 when $S = n^2$ (corresponding to genus $g = (n-1)(n-2)/2$). To complete Case 1, we modify C_n to reduce the size while not altering $O(T)$; that is, the sum of the number of rows, columns and entries. We must also ensure that the modified bitrade is separated. We use the following lemma.

Lemma 3.1. *Suppose that a separated latin bitrade $T = (T^\circ, T^\star)$ satisfies*

$$\begin{aligned}A^\circ &= \{(i_1,j_1,k_1),(i_1,j_2,k_2),(i_2,j_1,k_2),(i_2,j_2,k_3)\} \subseteq T^\circ,\\ A^\star &= \{(i_1,j_1,k_2),(i_1,j_2,k_3),(i_2,j_1,k_3),(i_2,j_2,k_4)\} \subseteq T^\star.\end{aligned}$$

Let

$$\begin{aligned}B^\circ &= \{(i_1,j_1,k_1),(i_2,j_2,k_2)\},\\ B^\star &= \{(i_1,j_1,k_3),(i_2,j_2,k_4)\},\\ U^\circ &= (T^\circ \setminus A^\circ) \cup B^\circ,\\ U^\star &= (T^\star \setminus A^\star) \cup B^\star.\end{aligned}$$

Then $U = (U^\circ, U^\star)$ is a separated latin bitrade with the same number of rows, columns and entries as T, and with size $|U| = |T| - 2$.

Proof: By assumption, T° and $T^\star$ contain the subsquares

$$\begin{array}{c|cc} \circ & j_1 & j_2 \\ \hline i_1 & k_1 & k_2 \\ i_2 & k_2 & k_3 \end{array} \qquad \text{and} \qquad \begin{array}{c|cc} \star & j_1 & j_2 \\ \hline i_1 & k_2 & k_3 \\ i_2 & k_3 & k_4 \end{array}$$

respectively. In U° and $U^\star$, these entries are replaced by

$$\begin{array}{c|cc} \circ & j_1 & j_2 \\ \hline i_1 & k_1 & \\ i_2 & & k_2 \end{array} \qquad \text{and} \qquad \begin{array}{c|cc} \star & j_1 & j_2 \\ \hline i_1 & k_3 & \\ i_2 & & k_4 \end{array}$$

respectively. It is easily verified that the rows and columns are still balanced, and hence $U = (U^\circ, U^\star)$ is a latin bitrade of size $|U| = |T| - 2$. So it only remains to prove that $O(U) = O(T)$ (and thus U is separated).

Let τ_1, τ_2 and τ_3 be respectively the row, column and symbol permutations of T, and let τ_1', τ_2' and τ_3' be respectively the row, column and symbol permutations of U.

By the definition of τ_1, the cycle corresponding to row i contains the segment

$$(\ldots(i_1,j_1,k_1)\ (i_1,j_2,k_2)\ (i_1,j_3,k_3)\ldots),$$

where $j_3 \notin \{j_1,j_2\}$. In τ_1', this segment is replaced by

$$(\ldots(i_1\ j_1,k_1)\ (i_1,j_3,k_3)\ldots).$$

Otherwise the cycle is unchanged; hence in τ_1', as in τ_1, there is exactly one cycle corresponding to row i_1.

The cycle in τ_1 corresponding to row i_2 contains the segment

$$(\ldots(i_2,j_1,k_2)\ (i_2,j_2,k_3)\ (i_2,j_4,k_4)\ldots)$$

where $j_4 \notin \{j_1,j_2\}$. In τ_1', this segment is replaced by

$$(\ldots(i_2,j_2,k_2)\ (i_2,j_4,k_4)\ldots).$$

Otherwise the cycle is unchanged, and hence in τ_1', as in τ_1, there is exactly one cycle corresponding to row i_2. Note that there is some $(i_2,j_5,k_2) \in T^\star$; we have $j_5 \neq j_1, j_2$, and hence also $(i_2,j_5,k_2) \in U^\star$. Thus by definition $\tau_1^{-1}((i_2,j_1,k_2)) = (\tau_1')^{-1}((i_2,j_2,k_2)) = (i_2,j_5,k_5)$, for some k_5.

Every other row cycle in τ_1' is identical to the corresponding row cycle in τ_1, and hence the total number of cycles in τ_1' is equal to the total number of cycles in τ_1. Similarly the total number of cycles in τ_2' is equal to the total number of cycles in τ_2.

In τ_3, the cycle corresponding to symbol k_2 contains the segment

$$(\ldots(i_1,j_2,k_2)\ (i_2,j_1,k_2)\ldots).$$

The entry k_2 occurs in row i_2 of T°; hence by the definition of a latin bitrade, there is some column j_6 such that $(i_2,j_6,k_2) \in T^\star$. We have $j_6 \notin \{j_1,j_2\}$, hence $(i_2,j_6,k_2) \in U^\star$ also. By the definition of the symbol permutation, $\tau_3((i_2,j_1,k_2)) = \tau_3'((i_2,j_2,k_2)) = (i_3,j_6,k_2)$, for some $i_3 \notin \{i_1,i_2\}$. Similarly $\tau_3^{-1}((i_1,j_2,k_2)) = (\tau_3')^{-1}((i_2,j_2,k_2))$, and thus the above segment is replaced by

$$(\ldots(i_2,j_2,k_2)\ldots)$$

in τ_3'; otherwise the cycle corresponding to symbol k_2 is unchanged. The cycle in τ_3 corresponding to symbol k_3 contains the segment

$$(\ldots(i_1,j_7,k_3)\ (i_2,j_2,k_3)\ (i_4,j_1,k_3)\ldots),$$

for some $i_4 \notin \{i_1, i_2\}$ and $j_7 \notin \{j_1, j_2\}$. In τ_3', this segment is replaced by

$$(\dots (i_1, j_7, k_3)\ (i_4, j_1, k_3) \dots);$$

otherwise the cycle is unchanged. Every other cycle in τ_3' is identical to the corresponding cycle in τ_3; thus we see that the total number of cycles in τ_3' is equal to the total number of cycles in τ_3. With the equivalent results for the row and symbol permutations, it follows that the order of U is equal to the order of T, so we are done. □

Using Lemma 3.1, we can complete the construction for Case 1.

Corollary 3.1. *For every integer $n \geq 2$ and size S satisfying $S \equiv n \pmod 2$ and*

$$n^2 - n + 1 < S \leq n^2,$$

there exists a separated latin bitrade T with $[r, c, e] = [n, n, n]$ and $|T| = S$.

Proof: We begin with the latin bitrade C_n (recall that this is the required construction for the case $S = n^2$). We may apply Lemma 3.1 repeatedly, using $i_1 = 0$, $i_2 = 1$, $j_1 = 2m$ and $j_2 = 2m + 1$, for $0 \leq m \leq \lfloor (n-2)/2 \rfloor$, reducing the size of the latin bitrade by two each time (so we modify 2×2 regions along the top of C_n° and $C_n^\star$). We may carry out repeated modifications since a different set of elements is replaced for each choice of j. The minimum size obtained in this way is $n^2 - 2(\lfloor (n-2)/2 \rfloor + 1) \leq n^2 - n + 1$, and we can obtain latin bitrades of any size with the same parity as n within this range. □

Case 2:

We begin with a variation of the latin bitrade C_n. Taking all addition modulo n (where $n \geq 5$), define $D_n = (D_n^\circ, D_n^\star)$, where

$$\begin{aligned} D_n^\circ &= \{(i, j, i+j) \mid 0 \leq i \leq n-2,\ 0 \leq j \leq n-1\}, \\ D_n^\star &= \{(i, j, i+j+1) \mid 0 \leq i \leq n-3,\ 0 \leq j \leq n-1\} \\ &\quad \cup \{(n-2, j, j) \mid 0 \leq j \leq n-1\}. \end{aligned}$$

Then D_n is a latin bitrade of size $n(n-1)$ with $r = n-1$ and $c = e = n$. The row, column and symbol permutations τ_1, τ_2, τ_3 satisfy

$$\tau_1((i, j, i+j)) = \begin{cases} (i, j+1, i+j+1), & \text{if } 0 \leq i \leq n-3, \\ (i, j+2, i+j+2), & \text{if } i = n-2, \end{cases}$$

$$\tau_2((i, j, i+j)) = \begin{cases} (i-1, j, i+j-1), & \text{if } 1 \leq i \leq n-2, \\ (n-2, j, j-2), & \text{if } i = 0, \end{cases}$$

$$\tau_3((i, j, i+j)) = \begin{cases} (i+1, j-1, i+j), & \text{if } 0 \leq i \leq n-3, \\ (0, j-2, j-2), & \text{if } i = n-2. \end{cases}$$

It follows that the permutation on each row, column and entry is a single cycle, with the possible exception of row $n-2$. If n is odd, the permutation on row $n-2$ is a single cycle, and hence the bitrade is separated; but if n is even, then the permutation on row $n-2$ consists of two cycles. If n is odd, we complete the construction as for Case 1.

Lemma 3.2. *For every odd integer $n \geq 5$ and size S satisfying $S \equiv n+1 \pmod 2$ and*

$$n(n-1) - n + 3 < S \leq n(n-1),$$

there exists a separated latin bitrade T with $[r,c,e] = [n-1,n,n]$ and $|T| = S$.

Proof: We begin with the latin bitrade D_n, which is separated since n is odd, and hence D_n is the required latin bitrade when $S = n(n-1)$. Note that the first two rows (and in fact the first $n-2$ rows) of both D_n° and $D_n^\star$ are identical to the corresponding rows of C_n° and $C_n^\star$ respectively. As in Corollary 3.1 (with C_n), we may apply Lemma 3.1 repeatedly to D_n, using $i_1 = 0$, $i_2 = 1$, $j_1 = 2m$ and $j_2 = 2m+1$, for $0 \leq m \leq (n-5)/2$, reducing the size of the latin bitrade by two each time. The minimum size obtained in this way is $n(n-1) - 2((n-3)/2) = n(n-1) - n + 3$, as required, and we can obtain latin bitrades of any size with the opposite parity to n within this range. $\square$

If n is even, we modify D_n to produce a separated latin bitrade. This modification will also reduce the size of the latin bitrade by one, which is necessary because in Case 2 the size has the opposite parity to n, and hence the maximum size is $n(n-1) - 1$.

By definition, D_n° and $D_n^\star$ contain the subsquares

$$\begin{array}{c|cc} \circ & 0 & 1 \\ \hline n-3 & n-3 & n-2 \\ n-2 & n-2 & n-1 \end{array} \qquad \text{and} \qquad \begin{array}{c|cc} \star & 0 & 1 \\ \hline n-3 & n-2 & n-1 \\ n-2 & 0 & 1 \end{array}$$

respectively. We modify the latin bitrade by replacing these entries with

$$\begin{array}{c|cc} \circ & 0 & 1 \\ \hline n-3 & n-3 & \\ n-2 & n-1 & n-2 \end{array} \qquad \text{and} \qquad \begin{array}{c|cc} \star & 0 & 1 \\ \hline n-3 & n-1 & \\ n-2 & 0 & 1 \end{array}$$

respectively. We label the modified latin bitrade $E_n = (E_n^\circ, E_n^\star)$; it is easily verified that E_n is a latin bitrade of size $n(n-1)-1$ with $[r,c,e] = [n-1,n,n]$, but it remains to be proved that E_n is separated.

Lemma 3.3. *For every even integer $n \geq 6$, the latin bitrade E_n is separated.*

Proof: We need to show that there is exactly one cycle in E_n corresponding to each of row $n-3$, row $n-2$, column 0, column 1, symbol $n-2$, and symbol $n-1$.

All other cycles are identical to the corresponding cycles in D_n, and hence there is exactly one cycle corresponding to each row, column and symbol.

The cycle in D_n corresponding to row $n-3$ contains the segment

$$(\dots(n-3,n-1,n-4)\ (n-3,0,n-3)\ (n-3,1,n-2)\ (n-3,2,n-1)\dots).$$

In E_n, this segment is replaced by

$$(\dots(n-3,n-1,n-4)\ (n-3,0,n-3)\ (n-3,2,n-1)\dots).$$

Similarly, the cycle in D_n corresponding to column 0 contains the segment

$$(\dots(0,0,0)\ (n-2,0,n-2)\ (n-3,0,n-3)\ (n-4,0,n-4)\dots),$$

which is replaced in E_n by

$$(\dots(0,0,0)\ (n-2,0,n-1)\ (n-3,0,n-3)\ (n-4,0,n-4)\dots);$$

the cycle in D_n corresponding to column 1 contains the segment

$$(\dots(0,1,1)\ (n-2,1,n-1)\ (n-3,1,n-2)\ (n-4,1,n-3)\dots),$$

which is replaced in E_n by

$$(\dots(0,1,1)\ (n-2,1,n-2)\ (n-4,1,n-3)\dots);$$

the cycle in D_n corresponding to entry $n-2$ contains the segment

$$(\dots(n-4,2,n-2)\ (n-3,1,n-2)\ (n-2,0,n-2)\ (0,n-2,n-2)\dots),$$

which is replaced in E_n by

$$(\dots(n-4,2,n-2)\ (n-2,1,n-2)\ (0,n-2,n-2)\dots);$$

and the cycle in D_n corresponding to entry $n-1$ contains the segment

$$(\dots(n-3,2,n-1)\ (n-2,1,n-1)\ (0,n-1,n-1)\dots),$$

which in E_n is replaced by

$$(\dots(n-3,2,n-1)\ (n-2,0,n-1)\ (0,n-1,n-1)\dots).$$

In each case we obtain a single cycle in E_n for the given row, column or entry.

We are left with row $n-2$. In D_n, there are two cycles on this row (since n is even), namely

$$((n-2,0,n-2)\ (n-2,2,0)\ (n-2,4,2)\dots(n-2,n-2,n-4))$$

and

$$((n-2,1,n-1)\ (n-2,3,1)\ (n-2,5,3)\dots(n-2,n-1,n-3)).$$

In E_n, these two cycles are replaced by the single cycle

$$((n-2,0,n-1)\ (n-2,2,0)\ (n-2,4,2)\dots(n-2,n-2,n-4)$$
$$(n-2,1,n-2)\ (n-2,3,1)\ (n-2,5,3)\dots(n-2,n-1,n-3)).$$

Therefore E_n is separated. $\square$

Corollary 3.2. *For every even integer $n \geq 6$ and size S satisfying $S \equiv n + 1 \pmod 2$ and*

$$n(n-1) - n + 3 < S \leq n(n-1) - 1,$$

there exists a separated latin bitrade T with $[r, c, e] = [n-1, n, n]$ and $|T| = S$.

PROOF: We begin with the separated latin bitrade E_n which is the required construction for Case 2 when n is even and $S = n(n-1) - 1$ (as noted earlier, there is no such latin bitrade for $S = n(n-1)$. Note that the first two rows (and in fact the first $n-3$ rows) of both D_n° and $D_n^\star$ are identical to the corresponding rows of C_n° and $C_n^\star$ respectively (by construction, the last row of D_n differs from C_n, while the last two rows of E_n differ from D_n; E_n has $n-1$ rows). As in Corollary 3.1 and Lemma 3.2 (with C_n and D_n respectively), we may apply Lemma 3.1 repeatedly to E_n, using $i_1 = 0$, $i_2 = 1$, $j_1 = 2m$ and $j_2 = 2m+1$, for $0 \leq m \leq (n-2)/2$, reducing the size of the latin bitrade by two each time. The minimum size obtained in this way is $n(n-1) - 1 - 2(n/2) \leq n(n-1) - n + 3$, as required, and we can obtain latin bitrades of any size with the opposite parity to n within this range. □

The constructions in this section prove that the bound given by Lemma 2.1 is tight. This completes the proof of Theorem 1.2.

4. Minimal latin bitrades of genus g and size $8g + 8$

In this section we introduce a complementary result which shows that minimal latin bitrades of genus g and size in the order of g (specifically, $8g + 8$) exist for each integer g. The latin bitrades in the previous section, while having *minimum* size for a given genus, are not *minimal* in general (see the definition at the end of Section 1). For example, recall that the first latin bitrade given was $\{C_n^\circ, C_n^\star\}$. Let $U^\circ = \{(0, j, j), (1, j, j+1) \mid j \in \mathbb{Z}_n\}$ and $U^\star = \{(0, j, j+1), (1, j, j) \mid j \in \mathbb{Z}_n\}$, where n is an integer and addition is taken $\bmod\, n$. Then $\{U^\circ, U^\star\}$ is a latin bitrade, and $U^\circ \subseteq C_n^\circ$ (in fact U° consists of the first two rows of C_n°), hence $\{C_n^\circ, C_n^\star\}$ is not minimal. The latin bitrade $\{C_n^\circ, C_n^\star\}$ was generalised by modifying the first two rows, but any two unmodified rows can be used in a similar way to form a latin bitrade. By contrast the constructions given here are minimal, but are not necessarily the smallest minimal latin bitrades of a given genus.

For $g \geq 0$, we define partial latin squares:

$$\begin{aligned} M^\circ = \{&(0, 4i, 2i), (1, 4i+1, 2i), (0, 4i+2, 2i+1), \\ &(1, 4i+3, 2i+1), (2, 4i+1, 2i+1), (3, 4i, 2i+1), \\ &(2, 4i+2, 2i+2), (3, 4i+3, 2i+2) \mid 0 \leq i \leq g\} \\ M^\star = \{&(0, 4i, 2i+1), (1, 4i+1, 2i+1), (0, 4i+2, 2i+2), \\ &(1, 4i+3, 2i+2), (2, 4i+1, 2i), (3, 4i, 2i), \\ &(2, 4i+2, 2i+1), (3, 4i+3, 2i+1) \mid 0 \leq i \leq g\} \end{aligned}$$

where arithmetic is calculated modulo $2g+2$.

Example 4.1. We give the pair $(M^\circ, M^\star)$ for $g=1$:

$\circ$	0	1	2	3	4	5	6	7
0	0		1		2		3	
1		0		1		2		3
2		1	2			3	0	
3	1			2	3			0

M°

$\circ$	0	1	2	3	4	5	6	7
0	1		2		3		0	
1		1		2		3		0
2		0	1			2	3	
3	0			1	2			3

$M^\star$

Lemma 4.1. *The ordered pair of partial latin squares $(M^\circ, M^\star)$ forms a separated, minimal latin bitrade of size $8g+8$ and genus g.*

Proof: It is clear that M° and $M^\star$ are disjoint. Each column of $(M^\circ, M^\star)$ contains exactly two entries, so the columns are both balanced and separated. Each row contains the set of entries $\{0, 1, \ldots, 2g+1\}$ so the rows are balanced. Thus $(M^\circ, M^\star)$ is a latin bitrade.

Next, there are four cycles of τ_1, corresponding to the four rows of M°:

$$\begin{aligned}
&((0,0,0)(0,2,1)\ldots(0,4i,2i)(0,4i+2,2i+1)\ldots)\\
&((1,1,0)(1,3,1)\ldots(1,4i+1,2i)(1,4i+3,2i+1)\ldots)\\
&((2,4g+2,2g+2)(2,4g+1,2g+1)\ldots(2,4i+2,2i+2)(2,4i+1,2i+1)\ldots)\\
&((3,4g+3,2g+2)(3,4g,2g+1)\ldots(3,4i+3,2i+2)(3,4i,2i+1)\ldots)
\end{aligned}$$

Thus the rows are separated.

Consider an odd entry $2i+1$. Within τ_3 the corresponding cycle is:

$$((0,4i+2,2i+1)(3,4i,2i+1)(1,4i+3,2i+1)(2,4i+1,2i+1)).$$

It is clear that each odd entry gives one cycle of τ_3. A similar result can be shown for the even entries, so the entries are separated.

Thus the entire latin bitrade is separated, and its genus is:

$$(8g+8-4-(4g+4)-(2g+2)+2)/2 = g.$$

□

Via more sophisticated constructions it should be possible to improve this result. That is, we conjecture that there should be some constant $c < 8$ such that there exists a minimal latin bitrade of genus g and size at most cg for each $g \geq 0$. It is an open problem to determine the least such c. However, the results in the earlier sections prove that any upper bound for the minimum size is, at best, linear with respect to g.

References

[1] Bate J.A., van Rees G.H.J., *Minimal and near-minimal critical sets in back circulant latin squares*, Australasian J. Combin. **27** (2003), 47–61.

[2] Cooper J., Donovan D., Seberry J., *Latin squares and critical sets of minimal size*, Australasian J. Combin. **4** (1991), 113–120.

[3] Drápal A., *Geometry of latin trades*, manuscript circulated at the conference Loops '03, Prague, 2003.

[4] Drápal A., Kepka T., *Exchangeable partial groupoids I*, Acta Univ. Carolin. Math. Phys. **24** (1983), 57–72.

[5] Fu H.-L., *On the construction of certain type of latin squares with prescribed intersections*, Ph.D. Thesis, Auburn University, 1980.

[6] Grannell M.J., Griggs T.S., Knor M., *Biembeddings of latin squares and hamiltonian decompositions*, Glasg. Math. J. **46** (2004), 443–457.

[7] Keedwell A.D., *Critical sets in latin squares and related matters: an update*, Utilitas Math. **65** (2004), 97–131.

[8] Khosrovshahi G.B., Maysoori C.H., *On the bases for trades*, Linear Algebra Appl. **226-228** (1995), 731–748.

[9] Street A.P., *Trades and defining sets*, in: C.J. Colbourn and J.H. Dinitz, Eds., CRC Handbook of Combinatorial Designs (CRC Press, Boca Raton, FL., 1996), pp. 474–478.

[10] Wanless I.M., *Cycle switches in latin squares*, Graphs Combin. **20** (2004), 545–570.

J. Lefevre, D. Donovan:
Centre for Discrete Mathematics and Computing, University of Queensland, St Lucia 4072, Australia

N. Cavenagh:
School of Mathematics, The University of New South Wales, Sydney 2052, Australia

A. Drápal:
Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 83, 186 75 Prague 8, Czech Republic

(*Received* September 6, 2006, *revised* February 6, 2007)