VERSITA

Mathematica Slovaca

DOI: 10.2478/s12175-008-0103-2
Math. Slovaca **58** (2008), No. 6, 691–718

THE THEORY AND APPLICATION OF LATIN BITRADES: A SURVEY

Nicholas J. Cavenagh

(*Communicated by Peter Horák*)

ABSTRACT. A latin bitrade is a pair of partial latin squares which are disjoint, occupy the same set of non-empty cells, and whose corresponding rows and columns contain the same sets of symbols. This survey paper summarizes the theory of latin bitrades, detailing their applications to critical sets, random latin squares and existence constructions for latin squares.

1. Introduction

Over a brief period of time, a theory of latin bitrades has developed, with connections to permutation groups, geometry and topology. Applications of latin bitrades have broadened from their early purpose of studying critical sets to analysing and generating random latin squares and obtaining existence constructions. As latin bitrades describe the difference between two latin squares of the same order, a study of latin bitrades is equivalent to the study of the *connections* between distinct latin squares.

Definitions and terminology of latin bitrades and related structures are far from uniform across the literature. While part of the aim of this survey paper is to promote some terminological coherency, and in some cases citing this paper may remove the need for lengthy introductions to papers that mention latin

2000 Mathematics Subject Classification: Primary 05B15.
Keywords: latin square, latin bitrade, latin trade, critical set, random latin square, bachelor latin square.

bitrades, the definitions in this paper should not necessarily be set in stone, for a number of reasons.

Firstly, as outlined in later sections, different applications, in some instances, befit slightly different terminological approaches. Secondly, the youth of this research area means that the process of definition is arguably still a collective and organic process. Thirdly, the fact that latin trades (and indeed latin squares) may be defined in different ways is an essential part of their usefulness.

Observing various difference sets between two latin squares is, in a way, something implicitly present in many different papers, some of them very old. Two early results on intersections of latin squares are given in [33] and [42], both of which give implicit results on the possible sizes of latin bitrades. In [33], Drápal considers the problem of determining the least number of non-associative triples in a non-associative quasigroup (see next section for definitions). Around the same time (and independently), Fu's PhD thesis [42] included a study the spectrum of intersections of two latin squares.

The explicit theory of latin trades was, however, made possible by a shift of the perspective, when the difference set became an object in its own right. In this sense the earliest known published article of latin bitrades appeared in [38], where they are referred to as *exchangeable partial groupoids*. Later, latin bitrades became of interest to researchers of critical sets (minimal defining sets of latin squares) ([25], [51], [3]). (These two branches of research were initially independent, partly because they took place on opposing sides of the cold war in the 1970s and 1980s.) In some early papers, latin bitrades are referred to as *latin interchanges*.

It is impossible to give a comprehensive survey on the application of latin bitrades, mainly because latin bitrades are such a fundamental concept, that they are applied in many instances without the term "latin bitrade" ever being mentioned. The terms "swap", "move", "mapping" and "name-change" have each been used synonymously with "latin bitrade".

This is the case, for example, in much of the literature on random latin squares. One of the aims of this survey paper is to connect results that use latin bitrades, in the hope that better use might be made of existing latin bitrade theory. In turn, exposing applications of latin bitrades in the research literature motivates pure latin bitrade research.

This paper is split into two main sections. In Section 1 we analyse the *theory* of latin bitrades. This includes definitions and summarizes the study of latin bitrades for their own sake. Then, in Section 2, we look at applications of latin bitrades to research problems involving latin squares. The focus of this survey is to provide illustrative examples; for rigorous proofs of results, readers should refer to the original papers.

Those with an interest in latin bitrades should also obtain a copy of Keedwell's recent survey paper on critical sets [51], which includes information on latin bitrades not covered here.

2. The theory of latin bitrades

Sections 2.1, 2.2 and 2.3 provide an introduction to those unfamiliar with latin bitrades. In Section 2.4 we explore in detail the topology and geometry of latin bitrades. In Section 2.5 we show how some latin bitrades may be defined via groups. Section 2.6 surveys results on homogeneous latin bitrades and Section 2.7 analyses methods to construct and deconstruct latin bitrades.

2.1. What is a partial latin square?

A *latin square* L of order n is an $n \times n$ array, with the cells of the array occupied by elements of a set $S = \{s_0, s_1, \dots, s_{n-1}\}$ (of size n) of *symbols*, such that each symbol occurs precisely once in each row and once in each column. If we also index the rows and columns of L by the sets $R = \{r_0, r_1, \dots r_{n-1}\}$ and $C = \{c_0, c_1, \dots c_{n-1}\}$, respectively, then L may be thought of as a set of ordered (row,column,symbol) triples. It is this definition of L that will be used in this paper. Specifically, $(r_i, c_j, s_k) \in L$ if and only if symbol s_k occurs in row r_i and column c_j of the latin square.

If we let $R = C = S$, then a latin square is precisely the operation table for a *quasigroup*. A quasigroup is defined to be a closed binary operation which allows left and right cancellation. Furthermore, the rows and columns of a latin square may be reordered to allow an identity element. We say that such a latin sqaure is in *standard form*. Latin squares in standard form are equivalent to *loops*. A *loop* has all the properties of a group except for associativity. There is a rich algebraic study of loops and quasigroups. However, latin squares, considered in their most general sense, arguably behave combinatorially rather than algebraically. For example, the number of latin squares of order n grows superexponentially in n, and most latin squares have a trivial autotopism group ([55]). The focus of this survey is combinatorial. While algebraic applications typically specify that R,

C and S are equivalent sets; in combinatorial applications we sometimes wish these sets to be distinct. Unless (and frequently) otherwise stated, in this paper we let $R = C = S = \{0, 1, \dots, n-1\}$.

A *partial latin square* P of order n is an $n \times n$ array, with possibly empty cells, such that each symbol from S occurs *at most* once in each row and at most once in each column. Thus any subset of a latin square L is a partial latin square. The converse, however, is not true, as some partial latin squares have no completion to latin squares of the same order. (To see this, try and fill in a sudoku puzzle without employing any strategy!)

Clearly a partial latin square of order n may be extended to a partial latin square of any order $m > n$ by a process of adding empty rows and columns. In some instances we may wish to define a partial latin square $P \subset R \times C \times S$ such that R, C and S are of varying sizes, so that each element of R, C and S occurs *somewhere* within an ordered triple of P as a row, column or symbol, respectively. In this instance, the *order* of P may refer to any $n \geq \max(|R|, |C|, |S|)$. (An alternative approach is to ignore the concept of order for partial latin squares.)

Two partial latin squares are said to be *isotopic* if one may be obtained from the other by relabelling the sets R, C and S. However, isotopisms are not the only type of equivalence relation on partial latin squares.

Consider the following, equivalent definition of partial latin squares. A partial latin square P is a set of ordered triples from $R \times C \times S$ such that:

- if $(r_i, c_j, s_k), (r_i, c_j, s_{k'}) \in P$, then $k = k'$,
- if $(r_i, c_j, s_k), (r_i, c_{j'}, s_k) \in P$, then $j = j'$, and
- if $(r_i, c_j, s_k), (r_{i'}, c_j, s_k) \in P$, then $i = i'$.

It is clear from this definition that if we permute the sets R, C and S amongst themselves, the property of being a partial latin square is invariant. Such a relation is called a *conjugacy* or *parastrophy*. (The word *parastrophy* is sometimes used as conjugacy has a separate meaning in group theory.)

Specifically, a partial latin square P has six *parastrophes* (including the transpose P^T):

$$\begin{aligned} P,\ P^T = &\big\{(c_j, r_i, s_k) :\ (r_i, c_j, s_k) \in P\big\}, \\ &\big\{(r_i, s_k, c_j) :\ (r_i, c_j, s_k) \in P\big\},\ \big\{(c_j, s_k, r_i) :\ (r_i, c_j, s_k) \in P\big\}, \\ &\big\{(s_k, r_i, c_j) :\ (r_i, c_j, s_k) \in P\big\},\ \big\{(s_k, c_j, r_i) :\ (r_i, c_j, s_k) \in P\big\}. \end{aligned}$$

If two partial latin squares are equivalent to each either via isotopy and/or parastrophy, they are said to belong to the same *main class* or *species*.

2.2. Three ways to define a latin bitrade

We next give three equivalent definitions of a latin bitrade. We begin with the most intuitive.

Definition 2.1. A *latin bitrade* (T, T') of order n is a pair of partial latin squares T and T' of order n such that:

- T and T' occupy the same set of filled-in cells,
- T and T' are disjoint sets, and
- each row (column) of T contains the same set of symbols as the corresponding row (column) of T'.

The *size* of a latin bitrade is equal to $|T|$, i.e. the number of filled-in cells in T (or, equivalently, T').

Example 2.2. The partial latin squares T and T' shown below together form a latin bitrade (T, T') of size 12 and order 4.

	1	2	3
1	0	3	
2		0	1
3	2		0

T

	2	3	1
3	1	0	
1		2	0
2	0		3

T'

If (T, T') is a latin bitrade, we may refer to T as a *latin trade* and T' as its *disjoint mate*. Equivalently, a *latin trade* is a partial latin square T for which there exists a disjoint mate T' such that (T, T') is a latin bitrade. It is possible that a latin trade may have more than one choice of disjoint mate. (The spectrum of sizes of latin trades with arbitrarily many disjoint mates is studied in [1].)

We now give an equivalent definition of a latin bitrade.

Definition 2.3. A *latin bitrade* (T, T') is a set of ordered triples from $R \times C \times S$ such that for each $(r_i, c_j, s_k) \in T$ (respectively, T'), there exists unique $i' \neq i$, $j' \neq j$ and $k' \neq k$ such that:

- $(r_{i'}, c_j, s_k) \in T'$ (respectively, T),
- $(r_i, c_{j'}, s_k) \in T'$, (respectively, T), and
- $(r_i, c_j, s_{k'}) \in T'$, (respectively, T).

Definition 2.3 is not as transparent as Definition 2.1, however it usefully highlights the symmetry of latin bitrades under conjugation. From this definition, it is immediate that any isotopism or conjugate of a latin bitrade is also a latin bitrade.

Our third and most succinct definition of a latin bitrade is as follows.

Definition 2.4. A *latin bitrade* is any ordered pair of the form $(L \setminus L', L' \setminus L)$, where L and L' are distinct latin squares of order n.

Definition 2.4 demonstrates that latin bitrades describe precisely the difference between two latin squares of the same order.

A clarification needs to be made about the *order* of a latin trade defined in this fashion. We note that not every latin trade of order n embeds into a latin square of order n. But since any partial latin square of order m embeds into a latin square of order $n \geq 2m$ ([41]), it is indeed possible to define any latin bitrade via Definition 2.4, as long as we allow the deletion of empty rows and columns.

Example 2.5. Consider the following latin squares:

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

L

0	2	3	1
3	1	0	2
1	3	2	0
2	0	1	3

L'

The latin bitrade $(L \setminus L', L' \setminus L)$ is equal to the latin bitrade (T, T') given in Example 2.2.

2.3. Elementary properties of latin bitrades

We note a few basic properties of latin bitrades. Firstly, (T, T') is a latin bitrade if and only if (T', T) is a latin bitrade. It is thus possible to think of a latin bitrade as an unordered pair $\{T_1, T_2\}$. In such an instance we refer to the latin bitrade as being *unordered*. Unless otherwise stated, it is assumed that latin bitrades are *ordered*.

Many applications are easier to explain if we consider latin bitrades as *ordered*. However, the number of isotopy classes of ordered pairs of latin bitrades is *not* necessarily twice the number of isotopy classes of unordered pairs of latin bitrades (see [62]). This is because some latin trades may be isotopic to their disjoint mates. (In fact T and T', as given in Example 2.2 above, are isotopic to each other.) Moreover, the equivalence given later in Theorem 2.14 involves unordered latin bitrades. For these reasons it seems to be counterproductive to set a definition of latin bitrades as either ordered or unordered pairs, except within a given paper as appropriate.

If (T, T') is a latin bitrade, it is not hard to see that each non-empty row and each non-empty column must contain at least two symbols, and that each symbol occurs at least twice (if at all) within T and T'. Drápal and Kepka [38] also showed the following:

Lemma 2.6. (Drápal and Kepka [38]) *Let (T, T') be a latin bitrade with no non-empty rows, columns or missing symbols. Then $3\sqrt{|T|} \leq |R| + |C| + |S|$.*

To see this, observe that $|T| \leq |R||C|$, $|T| \leq |R||S|$ and $|T| \leq |C||S|$. Thus, $9|T| \leq 3(|R||C| + |C||S| + |R||S|) \leq (|R| + |C| + |S|)^2$.

The smallest possible size of a latin bitrade is 4; such latin bitrades correspond to latin subsquares of order 2 and are called *intercalates*. No latin bitrades of size 5 exist; however Fu [42] showed that any size greater than 5 is possible.

A latin bitrade (T, T') is said to be *primary* (or *connected*) if there exists no latin bitrades (U, U') and (V, V') such that $T = U \cup V$ and $T' = U' \cup V'$. On the other hand, a latin trade T is said to be *minimal* if there exists no latin bitrade (U, U') such that $U \subset T$. So if (T, T') is a latin bitrade with T minimal, then certainly (T, T') is primary. However, if (T, T') is a primary latin bitrade, then T is not necessarily minimal.

As we shall see in a later section, minimal latin trades are of particular interest in the study of critical sets. The Appendix in [20] includes a primary latin bitrade (T, T') of size 40 such that T is a minimal latin trade but T' is not. In [62], a list of species representatives of all minimal latin trades of size at most 11 is given. (This updates a list given in [29], in which there is an omission.) Furthermore, [62] includes statistics on all latin bitrades of size up to 19.

2.4. The genus of separated latin bitrades

In this section we exclude from $R \cup C \cup S$ any rows, columns or symbols unused within any triple of a particular latin bitrade and we also assume that R, C and S are pairwise distinct.

Each row r of a latin bitrade (T, T') defines an alternating permutation of columns and symbols, where c_i is mapped to symbol s_j if and only if $(r, c_i, s_j) \in T$ and symbol s_j is mapped to column c_k if and only if $(r, s_j, c_k) \in T'$. If this permutation is a single cycle, then we say that the row r is *separated*. Similarly, we may classify each column and symbol as being either separated or non-separated. If every element of $R \cup C \cup S$ (excluding unused rows, columns and symbols) is separated, then we say that the latin bitrade (T, T') is *separated*.

Any non-separated latin bitrade may be transformed into a separated latin bitrade by a process of identifying each cycle in the permutation with a new row, column or symbol, as shown in the following example.

Example 2.7. The first row of the latin bitrade (T, T') is non-separated. The separated latin bitrade (U, U') is formed by splitting the first row of (T, T') into two rows.

	1_4	3_5	4_1	5_3
1_2	3_1	2_3		
2_1	4_3	5_2	1_4	3_5

(T, T')

	1_4		4_1	
		3_5		5_3
1_2	3_1	2_3		
2_1	4_3	5_2	1_4	3_5

(U, U')

Thus a classification of separated latin bitrades includes, in some sense, all latin bitrades.

Given a separated, primary latin bitrade (T, T'), we may construct a graph G whose vertex set is $R \cup C \cup S$ and whose edges are pairs of vertices that occur within some triple of T (or, equivalently, some triple of T'). If we define white and black faces of G to be the triples from T and T' (respectively), then we have a face 2-colorable triangulation of G in some surface.

We next orient the edges of G so that each white face contains directed edges from a row to a column vertex, a column to a symbol vertex and a symbol to a row vertex. It is immediate that each face (black or white) is labelled *coherently*; i.e. each triangular face has all 3 edges in either clockwise or anti-clockwise direction on the surface. Thus the surface in which G is embedded is *orientable*, and Euler's genus formula must give a non-negative, integer value for the genus g:

$$\begin{aligned} g &= (2+e-f-v)/2 \\ &= (2+3|T|-|T|-|T'|-|R|-|C|-|S|)/2 \\ &= (2+|T|-|R|-|C|-|S|)/2 \qquad (1) \end{aligned}$$

(where v, e and f are the number of vertices, edges and faces of G, respectively).

Example 2.8. The following example shows an intercalate latin bitrade (T, T') and its corresponding graph G embedded in the plane. The triangles corresponding to T' are shaded. The triangle (r_0, c_0, s_0) is external.

	c_0	c_1
r_0	s_0	s_1
r_1	s_1	s_0

T

	c_0	c_1
r_0	s_1	s_0
r_1	s_0	s_1

T'

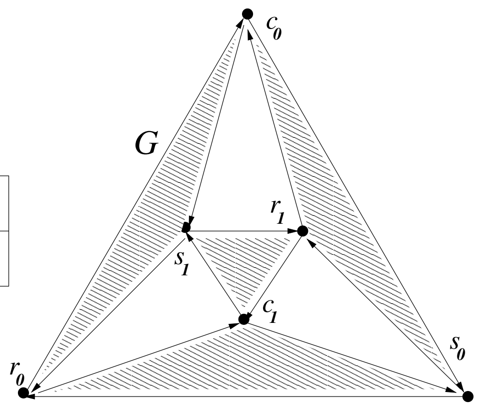


FIGURE 1. An intercalate (T, T') with its corresponding graph G

Let G^* be the dual of an embedding of a graph G of a separated, primary latin bitrade. Let D (on the same surface as G) be constructed from G^* as follows. Replace each 2-path from a white to a black to a white vertex by a single edge between white vertices, in the process removing the black vertices. This graph D has the same genus as G, and is the graph D r á p a l [36] uses when analysing the genus of a latin bitrade.

We next give a direct (and more informative) construction for D, which includes a coherent orientation of its edges. Throughout this paper, permutations are composed from left to right. Correspondingly, if permutation ρ acts on x then $x\rho$ denotes the image of x.

Definition 2.9. Let (T, T') be a primary and separated latin bitrade. Define the map $\beta_r\colon T \to T'$ where $\beta_r(a_1, a_2, a_3) = (b_1, b_2, b_3)$ implies that $a_r \neq b_r$ and $a_i = b_i$ for $i \neq r$. (From Definition 2.3 of a latin bitrade, the map β_r and its inverse are well defined.) In addition, let $\tau_1, \tau_2, \tau_3\colon T \to T$, where $\tau_1 = \beta_2\beta_3^{-1}$, $\tau_2 = \beta_3\beta_1^{-1}$ and $\tau_3 = \beta_1\beta_2^{-1}$. For each $i \in \{1, 2, 3\}$, let $\mathscr{A}_i$ be the set of cycles in τ_i.

Then we may define the graph D with vertex set T and directed edges corresponding to the mappings τ_1, τ_2 and τ_3.

Example 2.10. Consider the latin bitrade (T, T') in Example 2.2. Label the elements

$$(0,1,1),(0,2,2),(0,3,3),(1,0,1),(1,1,0),(1,2,3),$$
$$(2,0,2),(2,2,0),(2,3,1),(3,0,3),(3,1,2),(3,3,0)$$

of T with $A, B, C, D, E, F, G, H, I, J, K, L$ in that order. Then τ_1, τ_2 and τ_3 from Definition 2.9 are:

$$\tau_1 = (ACB)(DEF)(GHI)(JLK),$$
$$\tau_2 = (DJG)(AKE)(BFH)(CIL),$$
$$\tau_3 = (ADI)(BGK)(CJF)(ELH).$$

Figure 2 below shows the corresponding graph D embedded on the torus. To form the torus, the top of the rectangle is shifted half of its length before being glued to the bottom half. (So, for example, A is adjacent to E and K.) The left and right sides of the rectangle are glued together without any shift. The thick, dashed and thin lines represent τ_1, τ_2 and τ_3, respectively.

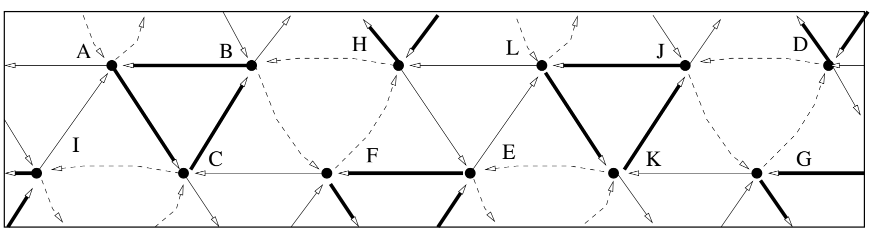


Figure 2. The graph D corresponding to the latin bitrade from Example 2.2

Theorem 2.11. (Drápal, [36]) *The mappings τ_1, τ_2 and τ_3 from* Definition 2.9 *satisfy the following conditions:*

(Q1) *If cycle ρ is in τ_r and cycle μ is in τ_s, $1 \le r < s \le 3$, then ρ and μ act on at most one common point.*

(Q2) *For each $i \in \{1,2,3\}$, τ_i has no fixed points.*

(Q3) $\tau_1\tau_2\tau_3 = 1$.

So we have seen how to derive a set of permutations from a separated and connected latin bitrade. In fact, this process is reversible:

Theorem 2.12. (Drápal, [36]) *Let τ_1, τ_2, τ_3 be permutations on some set X and for $i \in \{1,2,3\}$, let $\mathscr{A}_i$ be the set of cycles of τ_i. Suppose that τ_1, τ_2, τ_3 satisfy Conditions* (Q1), (Q2) *and* (Q3) *from* Theorem 2.11. *Next, let*

$$T = \{(\rho_1,\rho_2,\rho_3) :\ \rho_i \in \mathscr{A}_i \text{ and the } \rho_i \text{ all act on a common point of } X\}$$

and

$$T' = \{(\rho_1,\rho_2,\rho_3) :\ \rho_i \in \mathscr{A}_i,\ x, x', x'' \text{ are distinct points of } X \text{ such that } \\ x\rho_1 = x',\ x'\rho_2 = x'',\ x''\rho_3 = x\}.$$

Then (T,T') is a separated latin bitrade.

A proof of Theorems 2.11 and 2.12 may also be found in [21]. A consequence of the theorems above is that any primary, separated latin bitrade is equivalent to a set of permutations with particular properties.

Example 2.13. Let $X = \{A,B,C,D,E,F,G,H,I,J,K\}$ and

$$\begin{aligned}\tau_1 &= (ACB)(DEF)(GHI)(JLK),\\ \tau_2 &= (DJG)(AKE)(BFH)(CIL),\\ \tau_3 &= (ADI)(BGK)(CJF)(ELH).\end{aligned}$$

Observe that τ_1, τ_2 and τ_3 satisfy the conditions (Q1), (Q2) and (Q3) from Definition 2.12. In fact, the latin bitrade thus defined is isotopic to that given in Example 2.2.

A separated, primary latin bitrade of genus 0 is called a *planar* latin bitrade. Planar latin bitrades possess a number of interesting properties. A planar Eulerian triangulation is an Eulerian graph which has an embedding in the plane such that the faces of the graph are triangles. It turns out that such structures are equivalent to planar latin bitrades:

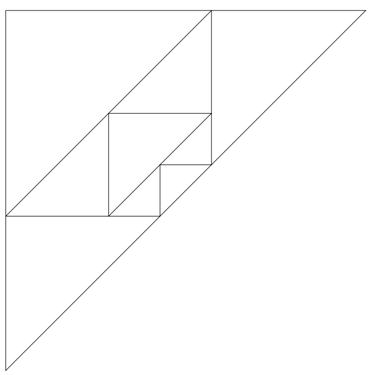
Theorem 2.14. (Cavenagh and Lisoněk, [23]) *Planar embeddings of* unordered *latin bitrades are equivalent to planar Eulerian triangulations.*

We define B_n to be the latin square that is precisely the addition table for the integers modulo n. Drápal shows how to construct planar latin bitrades in B_n geometrically.

Theorem 2.15. (Drápal, [34]) *Let m and n be positive integers. Suppose that we can partition the area of an equilateral triangle of side n into m smaller (integer-sided) equilateral triangles, such that each vertex of a triangle occurs as the vertex of at most 3 of the smaller triangles. Then there exists a planar latin bitrade (T, T') of size m such that T embeds into the addition table for the integers modulo n.*

We refer readers to [34] for a proof of this theorem, however we do include an example that is informal but hopefully informative.

Example 2.16. On the left in Figure 3 is a decomposition of an equilateral triangle into smaller equilateral triangles that satisfies the conditions of Theorem 2.15. (Note that we have applied a transformation so that each triangle is now right-angled and isoceles.) On the right is the corresponding planar latin trade in B_7 (constructed as in [34]), where the symbols of the latin trade are in bold and italic and the symbols of the disjoint mate are shown as subscripts.



$\boldsymbol{0}_{4}$	1	2	3	$\boldsymbol{4}_{0}$	5	6
1	2	3	4	5	6	0
2	3	$\boldsymbol{4}_{6}$	5	$\boldsymbol{6}_{4}$	0	1
3	4	5	$\boldsymbol{6}_{0}$	$\boldsymbol{0}_{6}$	1	2
$\boldsymbol{4}_{0}$	5	$\boldsymbol{6}_{4}$	$\boldsymbol{0}_{6}$	1	2	3
5	6	0	1	2	3	4
6	0	1	2	3	4	5

B_7

Figure 3. A latin trade in B_7 constructed as in Theorem 2.15

Next, observe that we can overlap the triangle decomposition with B_7 on the right, so that each right-angle vertex of a smaller triangle overlaps with one of the black symbols. Thus we observe a $1-1$ correspondence between the filled cells of the latin bitrade and the smaller triangles. Next, take any symbol s in the disjoint mate and find its corresponding right-angle vertex. Look at the other two vertices of the triangle and observe that s occurs in the corresponding positions within the original latin trade. (In this process we identify the three vertices of the original triangle with the cell $(0,0)$.)

In [40] (and in [13] for a later, alternative proof) it is shown that any latin trade within B_n has size at least $\mathrm{e}\log p+3$, where p is the smallest prime that divides n. Conversely, Drápal has shown (via the triangle construction above) that B_n contains a latin trade of size $O((\log n)^2)$ for any positive integer n. It is conjectured that B_n contains a latin trade of size $O(\log n)$ for each integer n; this is an open problem which appears difficult to solve.

Theorem 2.15 suggests a possible connection between the genus of a latin trade and the type of latin square it may be embedded into. Not all planar latin bitrades embed into $(\mathbb{Z}_n,+)$; however we conjecture the following.

Conjecture 2.17. *If (T,T') is a planar latin bitrade, then T embeds into the operation table for some abelian group.*

(Here we allow the abelian group to have possibly larger order than T.) Wanless has verified this conjecture computationally for the 10000 planar latin bitrades of smallest size.

The smallest latin bitrade (T,T') of genus 1 has size 9 with T equal to a latin square of order 3. This is generalized in [53] to the following:

Theorem 2.18. (Lefevre, et al. [53]) *Let g be an arbitrary non-negative integer, and define $n=\lceil(3+\sqrt{8g+1})/2\rceil$. Then the minimum size of a latin bitrade of genus g is:*

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

The smallest latin bitrade (T,T') of genus 1 such that T is minimal is given by Example 2.2.

2.5. Latin bitrades via groups

Theorem 2.12 from the previous section showed how to define a separated latin bitrade from a set of permutations with particular properties. By letting a group act on itself by right translation, some latin bitrades may be defined from groups without specifying an independent group action.

Theorem 2.19. ([21]) *Let G be some group. Let a, b, c be non-identity elements of G and let $A = \langle a \rangle$, $B = \langle b \rangle$ and $C = \langle c \rangle$ such that:*

(G1) $abc = 1$ *and*

(G2) $|A \cap B| = |A \cap C| = |B \cap C| = 1$.

Next, define:

$$T = \{(gA, gB, gC) : \ g \in G\}, \qquad T' = \{(gA, gB, ga^{-1}C); \ g \in G\}.$$

The pair of partial latin squares (T, T') as defined above is a latin bitrade with size $|G|$, $|G : A|$ rows (each with $|A|$ symbols), $|G : B|$ columns (each with $|B|$ symbols) and $|G : C|$ entries (each occurring $|C|$ times).

If, in turn,

(G3) $\langle a, b, c \rangle = G$,

then the latin bitrade is primary.

This construction does not give *every* separated latin bitrade, since not every separated latin bitrade has the same number of symbols in each row or column. However it provides a very succinct way of defining latin bitrades which are highly symmetric in structure. In fact any latin bitrade defined from a group in this fashion possesses a transitive autotopism group. Moreover, various properties of the latin bitrades may be encoded in the group structure succinctly, as shown in [21].

Example 2.20. We construct a latin bitrade of size 12 as in Theorem 2.19. Here $a = (123)$, $b = (214)$ and $c = (234)$. We use the following cosets of $A = \langle a \rangle$, $B = \langle b \rangle$ and $C = \langle c \rangle$ within the alternating group A_4:

$$\begin{aligned} A &= \{1, (123), (132)\} & B &= \{1, (142), (124)\} \\ cA &= \{(234), (134), (12)(34)\} & aB &= \{(123), (234), (14)(23)\} \\ c^{-1}A &= \{(234), (124), (13)(24)\} & a^{-1}B &= \{(134), (132), (13)(24)\} \\ bA &= \{(142), (143), (14)(23)\} & c^{-1}B &= \{(243), (143), (12)(34)\} \end{aligned}$$

$$\begin{aligned} C &= \{1, (234), (243)\} \\ aC &= \{(123), (143), (13)(24)\} \\ a^{-1}C &= \{(132), (12)(34), (142)\} \\ b^{-1}C &= \{(124), (134), (14)(23)\} \end{aligned}$$

$T =$

$\circ$	B	aB	$a^{-1}B$	$c^{-1}B$
A	C	aC	$a^{-1}C$	
cA		C	$b^{-1}C$	$a^{-1}C$
$c^{-1}A$	$b^{-1}C$		aC	C
bA	$a^{-1}C$	$b^{-1}C$		aC

$T' =$

$\star$	B	aB	$a^{-1}B$	$c^{-1}B$
A	$a^{-1}C$	C	aC	
cA		$b^{-1}C$	$a^{-1}C$	C
$c^{-1}A$	C		$b^{-1}C$	aC
bA	$b^{-1}C$	aC		$a^{-1}C$

The latin bitrade (T, T') is in fact isotopic to the one given in Example 2.2.

2.6. Homogeneous latin bitrades

The latin bitrade in Example 2.2 has the property that each row contains 3 symbols, each column contains 3 symbols and each symbol occurs 3 times, and is thus (3-)*homogeneous*.

Similarly we may define (k-)homogeneous latin bitrades in the obvious fashion. A 2-homogeneous latin bitrade is precisely a union of intercalates. From Equation 1, any primary 3-homogeneous latin bitrade has genus 1. A geometric construction for 3-homogeneous latin bitrades is given in [16]. The construction uses a packing of the Euclidean plane with circles, which are split into arcs that are identified with either rows, columns or symbols.

Perhaps surprisingly, this construction yields *every possible* 3-homogeneous latin bitrade, as shown in [12]. (In fact, it has since been pointed out to me that the result in [12] is implied by a more general result by Negami [58], which states that any 6-connected graph with genus 1 is uniquely embeddable on the torus.)

A geometric construction for minimal 4-homogeneous latin bitrades is given in [17], however this does not give every possible 4-homogeneous latin bitrade. Constructions of k-homogeneous latin bitrades are given in [6] for each $k \geq 2$. In [19], *minimal* k-homogeneous latin trades of size km are constructed for each $k \geq 3$ and $m \geq 1.75d^2 + 3$.

Homogeneous latin bitrades are of interest because of their symmetry; they are commonly found in the latin squares corresponding to the groups $((\mathbb{Z}_2)^n, +)$. For instance, the latin trade T given in Example 2.5 is a subset of the latin square L which is isotopic to the operation table for $((\mathbb{Z}_2)^2, +)$. In [11] it is shown that there are infinitely many 3-homogeneous latin trades which embed in $((\mathbb{Z}_2)^n, +)$ for some n.

Example 2.21. Below (in italics) is my all-time favourite latin trade T, an old friend which I discovered in 1995. It is 4-homogeneous, minimal, with unique disjoint mate T' (shown in subscripts) and, as shown below, embeds into a latin square L which is isotopic to the operation table for $((\mathbb{Z}_2)^3, +)$. The latin bitrade (T, T') may also be defined as in Theorem 2.19 via a semidirect product of $\mathbb{Z}_4 \times \mathbb{Z}_2$ with $\mathbb{Z}_2$.

Moreover, T is isotopic to $L \setminus T$, and $T \cup \{(i, j, k)\}$ contains a critical set of L of size $|T|$ (see Section 3.1 for a definition of a critical set) for *any* choice of $(i, j, k) \notin T$.

$\mathit{0}_{4}$	1	$\mathit{2}_{0}$	3	$\mathit{4}_{6}$	5	$\mathit{6}_{2}$	7
1	$\mathit{0}_{4}$	3	$\mathit{2}_{0}$	5	$\mathit{4}_{6}$	7	$\mathit{6}_{2}$
2	$\mathit{3}_{0}$	$\mathit{0}_{5}$	1	$\mathit{6}_{3}$	7	4	$\mathit{5}_{6}$
$\mathit{3}_{0}$	2	1	$\mathit{0}_{5}$	7	$\mathit{6}_{3}$	$\mathit{5}_{6}$	4
$\mathit{4}_{7}$	5	6	$\mathit{7}_{2}$	0	$\mathit{1}_{4}$	$\mathit{2}_{1}$	3
5	$\mathit{4}_{7}$	$\mathit{7}_{2}$	6	$\mathit{1}_{4}$	0	3	$\mathit{2}_{1}$
6	$\mathit{7}_{3}$	4	$\mathit{5}_{7}$	2	$\mathit{3}_{1}$	0	$\mathit{1}_{5}$
$\mathit{7}_{3}$	6	$\mathit{5}_{7}$	4	$\mathit{3}_{1}$	2	$\mathit{1}_{5}$	0

2.7. Constructions and deconstructions of latin bitrades

It is useful to consider techniques of "decomposing" latin bitrades into smaller ones. Such methods may lead to inductive proofs of properties of latin bitrades. We describe one method of decomposition in detail and briefly describe the others.

Donovan and Mahmoodian [32] outlined a method of "adding" latin bitrades as follows. Let (T, T') and (U, U') be two latin bitrades of the same order n, such that if (i, j) is a filled cell in both T and U, then either $(i, j, k) \in T \cap U'$ or $(i, j, k) \in T' \cap U$ for some symbol k. Suppose, furthermore, that if symbol k occurs in row (or column) i of both T and U, then it occurs in either the same cell of T and U' or in the same cell of T' and U. Then, the operation $\oplus$ gives a well-defined latin bitrade:

$$(T, T') \oplus (U, U') = (\{T \cup U\} \setminus \{T' \cup U'\}, \{T' \cup U'\} \setminus \{T \cup U\}).$$

In fact, Donovan and Mahmoodian [32] showed that any latin bitrade may be expressed as a "sum" of intercalates under the operation $\oplus$.

Example 2.22. Below a latin bitrade of size 8 is expressed as the sum ($\oplus$) of three intercalates. For each latin bitrade, the disjoint mate is shown in subscripts.

$$\begin{array}{|c|c|c|c|}\hline 1_4 & & & 4_1 \\ \hline & & 4_1 & 1_4 \\ \hline & 4_1 & 1_4 & \\ \hline 4_1 & 1_4 & & \\ \hline \end{array} = \begin{array}{|c|c|c|c|}\hline & & 1_4 & 4_1 \\ \hline & & 4_1 & 1_4 \\ \hline & & & \\ \hline & & & \\ \hline \end{array} \oplus \begin{array}{|c|c|c|c|}\hline 1_4 & & 4_1 & \\ \hline & & & \\ \hline & & & \\ \hline 4_1 & & 1_4 & \\ \hline \end{array} \oplus \begin{array}{|c|c|c|c|}\hline & & & \\ \hline & & & \\ \hline & 4_1 & 1_4 & \\ \hline & 1_4 & 4_1 & \\ \hline \end{array}.$$

Note that in the above example, the intercalates in some cases have filled-in cells which become empty when we take the sum ($\oplus$). In fact, some latin bitrades cannot be expressed as the sum ($\oplus$) of an intercalate plus a latin bitrade which has a strictly smaller size. (Example 2.2 gives such a latin bitrade.)

With this obstacle in mind, in [15] a decomposition of an arbitrary latin bitrade into smaller ones is given, such that in the deconstruction process the size strictly decreases, and in the construction process non-empty cells do not become empty cells.

A process by which any primary, separated latin bitrade of genus greater than 0 may be decomposed into two latin bitrades, each of smaller genus, is given in [37]. Batagelj [2] shows how to construct planar Eulerian triangulations inductively; from Theorem 2.14 this implies, in turn, the existence of an inductive construction process for planar latin bitrades.

3. Applications of latin bitrades

3.1. Critical sets

A *critical set* C of order n is a partial latin square of order n that is a subset of a unique latin square L of order n, and furthermore is minimal with respect to this property. More formally, if $C \subset L'$ and L' is a latin square (of order n)

then $L' = L$; and for any $C' \subset C$, there must exist a latin square $L' \neq L$ (of order n) such that $C' \subset L'$.

Example 3.1. The following partial latin square C is a critical set of B_5.

0	1			
1				
				2
			2	3

C

The study of critical sets is closely related to the study of latin trades. To see this, observe that if C is a critical set of a latin square L, then any latin trade $T \subseteq L$ must intersect C in at least one element. (For, if not, C is contained in the latin square $(L \setminus T) \cup T'$, where T' is a disjoint mate of T.) In fact, for each element of C, there must exist a unique (minimal) latin trade T such that $|C \cap T| = 1$. It is no surprise, then, that most results on critical sets make heavy use of latin trades ([18], [49], [45], [26], [24]).

A much studied open problem is to determine the smallest possible size of a critical set of order n. We denote this value by $\mathrm{scs}(n)$. It is conjectured that the correct value for $\mathrm{scs}(n)$ is equal to $\lfloor n^2/4 \rfloor$. (This has been verified computationally for $n \leq 8$ ([4])). Critical sets of such size are known to exist in B_n for each $n \geq 1$ ([25], [30]). Example 3.1 shows such a construction for B_5.

We now discuss how the evolution of latin trades has lead to improvements on lower bounds for $\mathrm{scs}(n)$. Let T be the set of elements in two rows of a latin square L. Then T is a latin trade within L, with disjoint mate T' formed by swapping these two rows. It follows immediately that any critical set of a latin square has at most one empty row. In other words, $\mathrm{scs}(n) \geq n - 1$.

Indeed, any two rows of a latin square of order n give rise to a derangement (a permutation with no fixed points) of size n. The cycles of this derangement lead to a partition of the two rows of the latin square into disjoint latin trades. The example below shows two rows of a latin square that partition into three latin trades, shown in plain, bold and italic fonts. The subscripts denote the entries of the disjoint mates.

$\mathbf{1_2}$	$\mathit{6_7}$	3_{10}	10_8	$\mathbf{2_5}$	$\mathit{7_6}$	9_4	$\mathbf{5_1}$	4_3	8_9
$\mathbf{2_1}$	$\mathit{7_6}$	10_3	8_{10}	$\mathbf{5_2}$	$\mathit{6_7}$	4_9	$\mathbf{1_5}$	3_4	9_8

These latin bitrades are called *cycle switches* and also arise from pairs of columns or pairs of symbols. The existence of many cycle switches in a particular latin square L gives information about the possible sizes of critical sets in L. However, many latin squares, including B_n when n is prime, contain no non-trivial cycle switches. That is, each cycle switch exchanges *entire* rows and columns. (Such latin squares are said to be *atomic* ([9]). It is an open problem to determine whether atomic latin squares exist for non prime-power order.)

The first significant improvement on this lower bound was by Fu, Fu and Rodger, who showed that $\mathrm{scs}(n) \geq \lfloor (7n-3)/6 \rfloor$. Their proof uses results on embeddings of partial latin squares. By studying latin trades which occur in arbitrary sets of *three* rows in latin squares, Cavenagh [10] showed that any critical set with an empty row has size at least $2n-4$. The result on latin bitrades which underpins this is the following:

Theorem 3.2. ([10, Corollary 7]) *In any set of three rows in any latin square of order n, there exists a latin trade within these three rows with an empty column.*

Note that the corresponding result for two rows is false; consider a pair of rows from an atomic latin square. In [5], Bean analysed latin trades within three or four rows of latin squares of order at most 9, establishing that $\mathrm{scs}(n) \geq 2n-4$ if $n \leq 9$.

With an analysis of trades that occur within the union of three rows and three columns of a latin square, Horak, Aldred and Fleischner [47] showed that $\mathrm{scs}(n) \geq \lfloor (4n-8)/3 \rfloor$. Recently, a superlinear lower bound for $\mathrm{scs}(n)$ has been established by Cavenagh [14], who showed that for all n, $\mathrm{scs}(n) \geq n\lfloor (\log n)^{1/3}/2 \rfloor$. In this paper it is also shown that $\mathrm{scs}(n) \geq 2n-32$ and if $n \geq 25$, $\mathrm{scs}(n) \geq \lceil (3n-7)/2 \rceil$.

The proof in [14] uses latin trades that exist in the union of two rows and two columns in arbitrary latin squares. We describe the structure of these latin trades as follows. Let r and r' be any two rows of a latin square L. Rearrange the columns of L so that each cycle switch within these rows lies on an adjacent set of columns, and furthermore so that if c_k and c_{k+1} are columns in the same cycle switch, then cell (r', c_k) contains the same symbol as (r, c_{k+1}). For illustrative purposes, we arrange the columns of the two rows above in such an order:

	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}
r	$\mathbf{1_2}$	$\mathbf{2_5}$	$\mathbf{5_1}$	$\mathit{6}_7$	$\mathit{7}_6$	3_{10}	10_8	8_9	9_4	4_3
r'	$\mathbf{2_1}$	$\mathbf{5_2}$	$\mathbf{1_5}$	$\mathit{7}_6$	$\mathit{6}_7$	10_3	8_{10}	9_8	4_9	3_4

Then, for any columns c_k and c_{k+l} that lie in the same cycle switch, there exists a latin trade whose elements are each contained in either column c_k, column c_{k+l}, or in rows r and r' between columns c_k and c_{k+l}.

Example 3.3. In the latin square below we can observe two examples of such latin trades. The second example, in bold, is also a cycle switch.

	c_1	c_2	c_3	c_4	c_5	c_6
r	3	1_2	2_1	4	$\mathbf{6_5}$	$\mathbf{5_6}$
r'	1_2	2_1	3	6	$\mathbf{5_4}$	$\mathbf{4_5}$
	5	3	4	1	$\mathbf{2_6}$	$\mathbf{6_2}$
	2_6	4	6_2	5	1	3
	6_1	5	1_6	3	$\mathbf{4_2}$	$\mathbf{2_4}$
	4	6	5	2	3	1

From above, it is clear that knowledge of latin trades that occur within *arbitrary* latin squares is helpful to obtain information on $\mathrm{scs}(n)$. We shall see in later sections that such latin trades are useful for a variety of problems.

The converse problem is to determine $\mathrm{lcs}(n)$, the *largest* possible size of a critical set of order n. Various upper and lower bounds for $\mathrm{lcs}(n)$ have been given, but a precise value is undetermined for general n. Stinson and van Rees [60] showed via a "doubling" construction, that $\mathrm{lcs}(2^m) \geq 4^m - 3^m$, for each $m \geq 1$. So far these are the critical sets with relatively the largest number of filled cells. Each element of these critical sets is contained in an intercalate within the latin square that intersects the critical set precisely at that element; such critical sets are called 2-*critical sets*.

Hatami and Mahmoodian showed that $\mathrm{lcs}(n) \geq n^2-(2+\ln 2)n^2/\ln n+o(n^2/\ln n)$. This was improved by Ghandehari et al. to $\mathrm{lcs}(n) \geq n^2 - (\mathrm{e}+o(1))n^{5/3}$. Both results have been obtained using non-constructive methods.

As for an upper bound on $\mathrm{lcs}(n)$, trivially $\mathrm{lcs}(n) \leq n^2 - n$, since each row or column of a critical set must contain an empty cell. This was improved by Bean and Mahmoodian [8] to $\mathrm{lcs}(n) \leq n^2 - 3n + 3$. The best upper bound so far for $\mathrm{lcs}(n)$ is by Horak and Dejter [48], who have shown that $\mathrm{lcs}(n) \leq n^2 - \lfloor (7n - \sqrt{n} - 20)/2 \rfloor$.

A related question is to consider the spectrum of possible sizes of critical sets of order n. In [28] and [7] it is shown that there exist critical sets of order n and size t for each t such that $\lfloor n^2/4 \rfloor \leq t \leq (n^2 - n)/2$. Recently, Donovan, Lefevre, et al. [31] have shown that if $4^{m-1} \leq t \leq 4^m - 3^m$, then there exists a critical set of size t and order 2^m.

For a more extensive treatise on critical sets in latin squares, see the recent survey by Keedwell [51].

3.2. Generating random latin squares efficiently

In practice, the process of generating a random latin square efficiently is straightforward if the number of configurations of a particular order is small. For example, there are exactly twelve latin squares of order 3:

$$\begin{array}{|c|c|c|}\hline 1&2&3\\\hline 2&3&1\\\hline 3&1&2\\\hline\end{array}\quad\begin{array}{|c|c|c|}\hline 1&2&3\\\hline 3&1&2\\\hline 2&3&1\\\hline\end{array}\quad\begin{array}{|c|c|c|}\hline 3&1&2\\\hline 1&2&3\\\hline 2&3&1\\\hline\end{array}\quad\begin{array}{|c|c|c|}\hline 3&1&2\\\hline 2&3&1\\\hline 1&2&3\\\hline\end{array}\quad\begin{array}{|c|c|c|}\hline 2&3&1\\\hline 3&1&2\\\hline 1&2&3\\\hline\end{array}\quad\begin{array}{|c|c|c|}\hline 2&3&1\\\hline 1&2&3\\\hline 3&1&2\\\hline\end{array}$$

$$\begin{array}{|c|c|c|}\hline 1&3&2\\\hline 2&1&3\\\hline 3&2&1\\\hline\end{array}\quad\begin{array}{|c|c|c|}\hline 1&3&2\\\hline 3&2&1\\\hline 2&1&3\\\hline\end{array}\quad\begin{array}{|c|c|c|}\hline 3&2&1\\\hline 1&3&2\\\hline 2&1&3\\\hline\end{array}\quad\begin{array}{|c|c|c|}\hline 3&2&1\\\hline 2&1&3\\\hline 1&3&2\\\hline\end{array}\quad\begin{array}{|c|c|c|}\hline 2&1&3\\\hline 3&2&1\\\hline 1&3&2\\\hline\end{array}\quad\begin{array}{|c|c|c|}\hline 2&1&3\\\hline 1&3&2\\\hline 3&2&1\\\hline\end{array}$$

So to generate a random latin square of order 3, it suffices to index the above set of squares in a list of size 12, then select, at random, an integer from 1 to 12. However, McKay and Wanless [55] recently showed that the number of latin squares of order 11 is:

$$776966836171770144107444346734230682311065600000.$$

It is computationally infeasible to store a list of latin squares of that size. Thus a different method is required.

One approach is to employ Markov chain Monte Carlo methods ([50]). Here we start with a specific latin square, locate (at random) one of a restricted class of latin trades within the latin square and replace it with its disjoint mate. We repeat this process a large number of times, creating a Markov chain of latin squares. If certain simple conditions are satisfied, this Markov chain will generate a uniformly random latin square.

Firstly, we require a restricted set of latin trades such that each latin square of order n possesses a small number (polynomial in n) of such trades. Secondly, the overall process must be connected, in that it must be possible to change one latin square to any other latin square of the same order by a series of trades in this restricted class. Thirdly, it must be possible to locate these trades within a latin square in polynomial time. Next, the overall network on which the random walk is conducted should have diameter (longest minimal path between vertices) bounded by a polynomial in n. Lastly, the Markov chain should be *rapidly mixing* (informally, it should approach the uniform random distribution quickly).

As in the case of studying critical sets, we require latin trades which occur in any type of latin square. Therefore combinatorial trades which are relatively simple are the most appropriate to use. However, cycle switches are insufficient as it is not always possible to "walk" between any two latin squares via cycle switches alone, as shown in [61].

Two classes of latin trades have been given which satisfy the above requirements for an efficient algorithm (except that there is to date no proof that the algorithms are rapidly mixing). We describe the types of latin bitrades that are used below.

The first algorithm, developed by Jacobson and Matthews [50], uses a type of "move" that goes outside the set of all latin squares. An example of one of these moves is shown in bold in the diagram below:

$$\begin{array}{|c|c|c|c|}\hline \mathbf{a} & \mathbf{b} & c & d \\ \hline \mathbf{b} & \mathbf{c} & d & a \\ \hline c & d & a & b \\ \hline d & a & b & c \\ \hline \end{array} \quad \Longrightarrow \quad \begin{array}{|c|c|c|c|}\hline \mathbf{b} & \mathbf{a} & c & d \\ \hline \mathbf{a} & \mathbf{b}+\mathbf{c}-\mathbf{a} & d & a \\ \hline c & d & a & b \\ \hline d & a & b & c \\ \hline \end{array}$$

Notice that while the array on the right is no longer a latin square, the symbols in each row and column still add up to $a+b+c+d$. Jacobson and Matthews use a series of these moves to transform one latin square into another (and thus the process is equivalent to replacing a latin trade with one of its disjoint mates).

The second type, developed by Pittenger [59] uses principally the following result. (In this paper the process of replacing a latin trade with a disjoint mate is called a "mapping" or "name-change"; we have reworded the lemma in terms of latin trades).

Theorem 3.4. ([59, Lemma 2.4]) *Given any two cells (i,j) and (i',j') in a latin square L that contain the same symbol k, there exists a latin bitrade (T,T') such that $T \subset L$ uses at most three distinct symbols* and *$(L \setminus T) \cup T'$ contains symbol k in cells (i,j') and (i',j).*

3.3. Analysing properties of random latin squares

The properties of random latin squares may be analysed via computational enumeration; however as we saw in the previous section this approach is feasible for small orders only. An alternative approach is to employ *switchings*. The concept of switchings was developed by McKay and Wormald (e.g., [57]).

We describe, informally, how the switchings method may be applied to latin squares. Let A and B be two sets of latin squares. Suppose that we also have a set of latin bitrades which describe the differences between latin squares in A and latin squares in B. If we think of the latin squares as vertices and the bitrades as edges, then we obtain a bipartite graph with partite sets of size $|A|$ and $|B|$. Suppose we know, in turn, that the degree of each vertex in A (equivalently, the number of latin trades in A from our restricted set) is bounded below by a_{MIN} and above by a_{MAX}, defining b_{MIN} and b_{MAX} similarly. Then, by counting the number of edges in the graph in two different ways, we have that:

$$\frac{b_{\mathrm{MIN}}}{a_{\mathrm{MAX}}} \leq \frac{|A|}{|B|} \leq \frac{b_{\mathrm{MAX}}}{a_{\mathrm{MIN}}}.$$

Thus, we can approximate the ratio $|A|/|B|$ using information about bitrades *without* knowing the sizes of $|A|$ and $|B|$ explicitly.

If we know, for example, that A consists of all configurations having a property (P) and B contains all remaining configurations, then we can estimate the probability that a *random* configuration has property (P). The trick in this process is to find a suitable class of latin bitrades, and then to exploit techniques from combinatorial enumeration. As in the previous section, we need to use latin trades that can be found in any type of latin square.

McKay and Wanless [56] apply the switching method using pairs of cycle switches of size 6. One of the main results in [56] is that almost all latin squares possess many 2×2 subsquares. In a submitted work by C. Greenhill, I. Wanless and I [22], latin bitrades of the type shown in Example 3.3 are used. In doing so we have shown that two rows of a random latin square share many properties of a random derangement (a permutation with no fixed points).

3.4. Existence constructions

Suppose that we wish to construct a latin square (or an infinite family of latin squares) with a specific property (P). One approach is to start with a latin square L that has a well-known structure and an abundance of latin trades. (Suitable candidates for L may be the back circulant latin square B_n or the latin square corresponding to another group operation table.) We then identify a latin bitrade (T, T') such that $T \subseteq L$ and $L' = (L \setminus T) \cup T'$ possesses property (P).

Since latin bitrades describe the difference between any two latin squares of the same order, it is possible to define *any* existence construction for latin squares as a problem involving latin bitrades. However it is somewhat absurd to claim that such an approach is always practical or feasible. But this approach can become feasible when the latin bitrade (T, T') has an easily defined structure.

We give an example where this is the case. In [63] the term "latin bitrade" is unused; however as we shall see it is possible to analyse the constructions from [63] in terms of latin bitrades. A *bachelor latin square* is one which possesses no orthogonal mate (equivalently, a latin square which cannot be decomposed into transversals). If n is even, then B_n is a bachelor latin square. However if n is odd, then B_n possesses an orthogonal mate for any $n \geq 3$. The existence of bachelor latin squares of odd order n for each $n \geq 5$ is shown in [63] by Wanless and Webb. Their construction may be thought of in terms of identifying a latin bitrade (T, T') such that $T \subset B_n$ and $(B_n \setminus T) \cup T'$ is a bachelor latin square. The case $n = 9$ is given below, with the latin trade T shown in italics and the disjoint mate T' as subscripts.

$\mathit{0}_{\mathit{1}}$	$\mathit{1}_{\mathit{0}}$	2	3	4	5	6	7	8
$\mathit{1}_{\mathit{3}}$	2	$\mathit{3}_{\mathit{1}}$	4	5	6	7	8	0
2	3	4	5	6	7	8	0	1
$\mathit{3}_{\mathit{0}}$	4	$\mathit{5}_{\mathit{3}}$	6	7	8	$\mathit{0}_{\mathit{5}}$	1	2
4	5	6	7	8	0	1	2	3
5	6	7	8	0	1	2	3	4
6	7	8	0	1	2	3	4	5
7	8	0	1	2	3	4	5	6
8	$\mathit{0}_{\mathit{1}}$	$\mathit{1}_{\mathit{5}}$	2	3	4	$\mathit{5}_{\mathit{0}}$	6	7

It can be shown (see [63] for details) that the element $(8, 2, 5) \in (B_n \setminus T) \cup T'$ belongs to no transversal within $(B_n \setminus T) \cup T'$. Thus the transformed latin square is a bachelor latin square. We might think of the latin bitrade (T, T') as "destroying" the property of B_n having an orthogonal mate. As the above example demonstrates, a knowledge of latin bitrades within highly structured latin squares such as B_n can be useful for existence constructions.

REFERENCES

[1] ADAMS, P.—BILLINGTON, E. J.—BRYANT, D. E.—MAHMOODIAN, E. S.: *On the possible volumes of μ-way latin trades*, Aequationes Math. **63** (2002), 303–320.

[2] BATAGELJ, V.: *An improved inductive definition of two restricted classes of triangulations of the plane*. In: Combinatorics and Graph Theory (Warsaw, 1987), Banach Center Publ. 25, PWN, Warsaw, 1989, pp. 11–18.

[3] BATE, J. A.—VAN REES, G. H. J.: *Minimal and near-minimal critical sets in back circulant latin squares*, Australas. J. Combin. **27** (2003), 47–61.

[4] BEAN, R.: *The size of the smallest uniquely completable set in order 8 latin squares*, J. Combin. Math. Combin. Comput. **52** (2005), 159–168.

[5] BEAN, R.: *Latin trades on three or four rows*, Discrete Math. **306** (2006), 3028–3041.

[6] BEAN, R.—BIDKHORI, H.—KHOSRAVI, M.—MAHMOODIAN, E. S.: *k-homogeneous latin trades*. In: Proc. Conference on Algebraic Combinatorics and Applications, Designs and Codes, Thurnau 2005, Vol. 74, Bayreuther Mathemat. Schr., Bayreuth, 2005, pp. 7–18.

[7] BEAN, R.—DONOVAN, D.: *Closing a gap in the spectrum of critical sets*, Australas. J. Combin. **22** (2000), 191–200.

[8] BEAN, R.—MAHMOODIAN, E. S.: *A new bound on the size of the largest critical set in a latin square*, Discrete Math. **267** (2003), 13–21.

[9] BRYANT, D.—MAENHAUT, B.—WANLESS, I. M.: *New families of atomic latin squares and perfect* 1*-factorizations*, J. Combin. Theory Ser. A **113** (2006), 608–624.

[10] CAVENAGH, N. J.: *Latin trade algorithms and the smallest critical set in a latin square*, J. Automat. Lang. Combin. **8** (2003), 567–578.

[11] CAVENAGH, N. J.: *Embedding* 3*-homogeneous latin trades into abelian* 2*-groups*, Commentat. Math. Univ. Carolin. **45** (2004), 194–212.

[12] CAVENAGH, N. J.: *A uniqueness result for* 3*-homogeneous latin trades*, Comment. Math. Univ. Carolin. **47** (2006), 337–358.

[13] CAVENAGH, N. J.: *The size of the smallest latin trade in the back circulant latin square*, Bull. Inst. Combin. Appl. **38** (2003), 11–18.

[14] CAVENAGH, N. J.: *A superlinear lower bound for the size of a critical set in a latin square*, J. Combin. Des. **15** (2007), 269–282.

[15] CAVENAGH, N. J.—DONOVAN, D.—DRÁPAL, A.: *Constructing and deconstructing latin trades*, Discrete Math. **284** (2004), 97–105.

[16] CAVENAGH, N. J.—DONOVAN, D.—DRÁPAL, A.: *3-homogeneous latin trades*, Discrete Math. **300** (2005), 57–70.

[17] CAVENAGH, N. J.—DONOVAN, D.—DRÁPAL, A.: *4-homogeneous latin trades*, Australas. J. Combin. **32** (2005), 285–303.

[18] CAVENAGH, N. J.—DONOVAN, D.—KHODKAR, A.: *On the spectrum of critical sets in back circulant latin squares*, Ars Combin. **82** (2007), 287–319.

[19] CAVENAGH, N. J.—DONOVAN, D.—YAZICI, E. Ş.: *Minimal homogeneous latin trades*, Discrete Math. **306** (2006), 2047–2055.

[20] CAVENAGH, N. J.—DONOVAN, D.—YAZICI, E. Ş.: *Minimal homogeneous Steiner 2-$(v, 3)$ trades*, Discrete Math. **308** (2008), 741–752.

[21] CAVENAGH, N. J.—DRÁPAL, A.—HÄMÄLÄINEN, C.: *Latin bitrades derived from groups*, Discrete Math. (To appear).

[22] CAVENAGH, N. J.—GREENHILL, C.—WANLESS, I.: *The cycle structure of two rows in a random latin square*, Random Structures Algorithms **33** (2008), 286–309.

[23] CAVENAGH, N. J.— LISONĚK, P.: *Planar Eulerian triangulations are equivalent to spherical latin bitrades*, J. Combin. Theory Ser. A **115** (2008), 193–197.

[24] COOPER, J.—DONOVAN, D.—GOWER, R. A. H.: *Critical sets in direct products of back circulant latin squares*, Util. Math. **50** (1996), 127–162.

[25] COOPER, J.—DONOVAN, D.—SEBERRY, J.: *Latin squares and critical sets of minimal size*, Australas. J. Combin. **4** (1991), 113–120.

[26] CURRAN, D.—VAN REES, G. H. J.: *Critical sets in latin squares.* In: Proc. Eighth Manitoba Conf. on Numerical Math. and Comput.. Congr. Numer. **23** (1978), 165–168.

[27] DONOVAN, D.: *Critical sets in latin squares of order less than 11*, J. Combin. Math. Combin. Comp. **29** (1999), 223–240.

[28] DONOVAN, D.—HOWSE, A.: *Towards the spectrum of critical sets*, Australas. J. Combin. **21** (2000), 107–130.

[29] DONOVAN, D.—HOWSE, A.—ADAMS, P.: *A discussion of latin interchanges*, J. Combin. Math. Combin. Comput. **23** (1997), 161–182.

[30] DONOVAN, D.—COOPER, J.: *Critical sets in back circulant latin squares*, Aequationes Math. **52** (1996), 157–179.

[31] DONOVAN, D.—LEFEVRE, J.—VAN REES, G. H. J.: *On the spectrum of critical sets in latin squares of order 2^n*, J. Combin. Des. **16** (2008), 25–43.

[32] DONOVAN, D.—MAHMOODIAN, E. S.: *An algortihm for writing any latin interchange as a sum of intercalates*, Bull. Inst. Combin. Appl. **34** (2002), 90–98.

[33] DRÁPAL, A.: *On quasigroups rich in associative triples*, Discrete Math. **44** (1983), 251–265.

[34] DRÁPAL, A.: *On a planar construction of quasigroups*, Czechoslovak Math. J. **41** (1991), 538–548.

[35] DRÁPAL, A.: *Hamming distances of groups and quasi-groups*, Discrete Math. **235** (2001), 189–197.

[36] DRÁPAL, A.: *Geometry of latin trades.* Manuscript circulated at the conference Loops '03, Prague 2003.

[37] DRÁPAL, A.: *On geometrical structure and construction of latin trades* (Submitted).

[38] DRÁPAL, A.—KEPKA, T.: *Exchangeable partial groupoids I*, Acta Univ. Carolin. Math. Phys. **24** (1983), 57–72.

[39] DRÁPAL, A.—KEPKA, T.: E*xchangeable partial groupoids II*, Acta Univ. Carolin. Math. Phys. **26** (1985), 3–9.

[40] DRÁPAL, A.—KEPKA, T.: *On a distance of groups and latin squares*, Comment. Math. Univ. Carolin. **30** (1989) 621–626.

[41] EVANS, T.: *Embedding incomplete latin squares*, Amer. Math. Monthly **67** (1960), 958–961.

[42] FU, H-L.: *On the Construction of Certain Type of Latin Squares with Prescribed Intersections.* Ph.D. Thesis, Auburn University, 1980.

[43] FU, C-M.—FU, H-L.—RODGER, C. A.: *The minimum size of critical sets in latin squares*, J. Statist. Plann. Inference **62** (1997), 333–337.

[44] GHANDEHARI, M.—HATAMI, H.—MAHMOODIAN, E. S.: *On the size of the minimum critcal set of a latin square*, Discrete Math. **293** (2005), 121–127.

[45] GOWER, R. A. H.: *Critical sets in products of latin squares*, Ars Combin. **55** (2000), 293–317.

[46] HATAMI, H.—MAHMOODIAN, E. S.: *A lower bound for the size of the largest critical sets in latin squares*, Bull. Inst. Combin. Appl. **38** (2003), 19–22.

[47] HORAK, P.—ALDRED, R. E. L.—FLEISCHNER, H.: *Completing latin squares: critical sets*, J. Combin. Des. **10** (2002), 419–432.

[48] HORAK, P.—DEJTER, I. J.: *Completing latin squares: critical sets II*, J. Combin. Des. **15** (2007), 77–83.

[49] HOWSE, A.: *Families of critical sets for the dihedral group*, Util. Math. **54** (1998), 175–191.

[50] JACOBSON, M. T.—MATTHEWS, P.: *Generating uniformly distributed random latin squares*, J. Combin. Des. **4** (1996), 405–437.

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

[52] KHOSROVSHAHI, G. B.—MAYSOORI, C. H.: *On the bases for trades*, Linear Algebra Appl., **226-228** (1995), 731–748.

[53] LEFEVRE, J.—DONOVAN, D.—CAVENAGH, N.—DRÁPAL, A.: *Minimal and minimum size latin bitrades of each genus*, Comment. Math. Univ. Carolin. **48** (2007), 189–203.

[54] LINDNER, C. C.—RODGER, C. A.: *Generalized embedding theorems for partial latin squares*, Bull. Inst. Combin. Appl. **5** (1992), 81–99.

[55] MCKAY, B. D.—WANLESS, I. M.: *On the number of latin squares*, Ann. Combin. **9** (2005), 335–344.

[56] MCKAY, B. D.—WANLESS, I.: *Most latin squares have many subsquares*, J. Combin. Theory Ser. A **86** (1999), 323–347.

[57] MCKAY, B. D.—WORMAD, N. C.: *Uniform generation of random latin rectangles*, J. Combin. Math. Combin. Comput. **9** (1991), 179–186.

[58] NEGAMI, S.: *Uniqueness and faithfuless of embedding of toroidal gaphs*, Discrete Math. **44** (1983), 161–180.

[59] PITTINGER, A.: *Mappings of latin squares*, Linear Algebra Appl. **261** (1997), 251–268.

[60] STINSON, D. R.—VAN REES, G. H. J.: *Som large critical sets*, Congr. Numer. **34** (1982), 441–456.

[61] WANLESS, I. M.: *Cycle switching in latin squares*, Graphs Combin. **20** (2004), 545–570.

[62] WANLESS, I. M.: *A computer enumeration of small latin trades*, Australas. J. Combin. **39** (2007), 247–258.

[63] WANLESS, I. M.—WEBB, B. S.: *The existence of latin squares without orthogonal mates*, Des. Codes Cryptogr. **40** (2006), 131–135.

Received 29. 8. 2007
Revised 24. 10. 2007

School of Mathematics and Statistics
The University of New South Wales
NSW 2052
AUSTRALIA