Available online at www.sciencedirect.com

ScienceDirect

Discrete Mathematics 308 (2008) 6189–6202

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Latin bitrades derived from groups

Nicholas J. Cavenagh[a,*], Aleš Drápal[b], Carlo Hämäläinen[c]

[a] *School of Mathematics, The University of New South Wales, NSW 2052, Australia*
[b] *Department of Mathematics, Charles University, Sokolovská 83, 186 75 Praha 8, Czech Republic*
[c] *Department of Mathematics, The University of Queensland, QLD 4072, Australia*

Received 4 July 2006; received in revised form 21 November 2007; accepted 22 November 2007
Available online 31 December 2007

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 set of entries. In [A. Drápal, On geometrical structure and construction of Latin trades, Advances in Geometry (in press)] it is shown that a Latin bitrade may be thought of as three derangements of the same set, whose product is the identity and whose cycles pairwise have at most one point in common. By letting a group act on itself by right translation, we show how some Latin bitrades may be derived directly from groups. Properties of Latin bitrades such as homogeneity, minimality (via thinness) and orthogonality may also be encoded succinctly within the group structure. We apply the construction to some well-known groups, constructing previously unknown Latin bitrades. In particular, we show the existence of minimal, k-homogeneous Latin bitrades for each odd $k \geq 3$. In some cases these are the smallest known such examples.

Keywords: Latin bitrade; Homogeneous Latin bitrade; Permutation group; Orthogonality

1. Introduction

One of the earliest studies of Latin bitrades appeared in [10], where they are referred to as *exchangeable partial groupoids*. Later (and at first independently), Latin bitrades became of interest to researchers of critical sets (minimal defining sets of Latin squares) [7,13,1] and of the intersections between Latin squares [11]. As discussed in [18], 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 [17,14].

In [9] it is shown that a Latin bitrade may be thought of as a set of three permutations with no fixed points, whose product is the identity and whose cycles have pairwise at most one point in common. By letting a group act on itself by right translation, in this paper we extend this result to give a construction of Latin bitrades directly from groups. This construction does not give every type of Latin bitrade; however the Latin bitrades generated in this way are rich in symmetry and structure. Furthermore Latin bitrade properties such as orthogonality, minimality and homogeneity may be encoded concisely into the group structure, as shown in Section 3. Section 4 shows that many interesting

* Corresponding author.
E-mail address: nicholas_cavenagh@yahoo.co.uk (N.J. Cavenagh).

0012-365X/$ - see front matter © 2008 Published by Elsevier B.V.
doi:10.1016/j.disc.2007.11.041

examples can be constructed, even from familiar examples of groups. Finally in Section 5 we give a table of known results of minimal k-homogeneous Latin bitrades for small, odd values of k.

Note that throughout this paper we compose permutations from left to right. Correspondingly, if a permutation ρ acts on a point x, $x\rho$ denotes the image of x. Given a group G acting on a set X, for each $g \in G$, $\mathrm{Fix}(g) = \{x \mid x \in X, xg = g\}$ and $\mathrm{Mov}(g) = \{x \mid x \in X, xg \neq g\}$. The group theory notation used in this paper is consistent with most introductory texts, including [12].

2. Permutation structure

Definition 2.1. Let A_1, A_2, and A_3 be finite, non-empty sets. A *partial Latin square* T is an $|A_1| \times |A_2|$ array with rows indexed by A_1, columns indexed by A_2, and entries from A_3, such that each $e \in A_3$ appears at most once in each row and at most once in each column. In this paper, we ignore unused rows, columns and symbols, so that A_1, A_2 and A_3 often have differing sizes. In the case where $|A_1| = |A_2| = |A_3| = n$ and each $e \in A_3$ appears exactly once in each row and once in each column, we say that T is a *Latin square* of order n.

We may view T as a set and write $(x, y, z) \in T$ if and only if symbol z appears in the cell at row x, column y. As a binary operation we write $x \circ y = z$ if and only if $(x, y, z) \in T$ $(=T^\circ)$. Equivalently, a partial Latin square T° is a subset $T^\circ \subseteq A_1 \times A_2 \times A_3$ such that the following conditions are satisfied:

(P1) If $(a_1, a_2, a_3), (b_1, b_2, b_3) \in T^\circ$, then either at most one of $a_1 = b_1$, $a_2 = b_2$ and $a_3 = b_3$ is true or all three are true.

(P2) The sets A_1, A_2, and A_3 are pairwise disjoint, and for all $\alpha \in \bigcup_i A_i$, there exists an $(a_1, a_2, a_3) \in T^\circ$ with $\alpha = a_i$ for some i.

Let $T^\circ, T^\star \subset A_1 \times A_2 \times A_3$ be two partial Latin squares. Then $(T^\circ, T^\star)$ is called a *Latin bitrade* if the following conditions are all satisfied.

(R1) $T^\circ \cap T^\star = \emptyset$.

(R2) For all $(a_1, a_2, a_3) \in T^\circ$ and all $r, s \in \{1, 2, 3\}$, $r \neq s$, there exists a unique $(b_1, b_2, b_3) \in T^\star$ such that $a_r = b_r$ and $a_s = b_s$.

(R3) For all $(a_1, a_2, a_3) \in T^\star$ and all $r, s \in \{1, 2, 3\}$, $r \neq s$, there exists a unique $(b_1, b_2, b_3) \in T^\circ$ such that $a_r = b_r$ and $a_s = b_s$.

Note that (R2) and (R3) imply that each row (column) of T° contains the same subset of A_3 as the corresponding row (column) of $T^\star$. We sometimes refer to T° as a *Latin trade* and $T^\star$ its *disjoint mate*. The *size* of a Latin bitrade is equal to $|T^\circ| = |T^\star|$.

Given any two distinct Latin squares L° and $L^\star$, each of order n, $(L^\circ \setminus L^\star, L^\star \setminus L^\circ)$ is a Latin bitrade. In this way, Latin bitrades describe the difference between two Latin squares. In fact, we may think of a Latin trade as a subset of a Latin square which may be replaced with a disjoint mate to obtain a new Latin square. An *isotopism* of a partial Latin square is a relabelling of the elements of A_1, A_2 and A_3. Combinatorial properties of partial Latin squares are, in general, preserved under isotopism (in particular, any isotope of a Latin bitrade is also a Latin bitrade), a fact we exploit in this paper.

Example 2.2. Let $A_1 = \{a, b\}$, $A_2 = \{c, d, e\}$ and $A_3 = \{f, g, h\}$. Then $(T^\circ, T^\star)$ is a *Latin bitrade*, where $T^\circ, T^\star \subset A_1 \times A_2 \times A_3$ are shown below:

$$T^\circ = \begin{array}{|c||c|c|c|}\hline \circ & c & d & e \\ \hline a & f & g & h \\ \hline b & g & h & f \\ \hline \end{array} \qquad T^\star = \begin{array}{|c||c|c|c|}\hline \star & c & d & e \\ \hline a & g & h & f \\ \hline b & f & g & h \\ \hline \end{array}.$$

We may also write

$$T^\circ = \{(a, c, f), (a, d, g), (a, e, h), (b, c, g), (b, d, h), (b, e, f)\} \quad \text{and}$$
$$T^\star = \{(a, c, g), (a, d, h), (a, e, f), (b, c, f), (b, d, g), (b, e, h)\}.$$

It turns out (as shown in [9]) that Latin bitrades may be defined in terms of permutations. We first show how to derive permutations of T° from a given Latin bitrade.

Definition 2.3. Define the map $\beta_r : T^\star \to T^\circ$ where $(a_1, a_2, a_3)\ \beta_r = (b_1, b_2, b_3)$ implies that $a_r \neq b_r$ and $a_i = b_i$ for $i \neq r$. (Note that by conditions (R2) and (R3) the map β_r and its inverse are well defined.) In particular, let $\tau_1, \tau_2, \tau_3 : T^\circ \to T^\circ$, where $\tau_1 = \beta_2^{-1}\beta_3$, $\tau_2 = \beta_3^{-1}\beta_1$ and $\tau_3 = \beta_1^{-1}\beta_2$. For each $i \in \{1, 2, 3\}$, let $\mathcal{A}_i$ be the set of cycles in τ_i. We will see these cycles as permutations of T°.

Example 2.4. Consider the Latin bitrade constructed in Example 2.2. Here,

$$\tau_1 = ((a, c, f)(a, e, h)(a, d, g))((b, c, g)(b, d, h)(b, e, f))$$
$$\tau_2 = ((a, c, f)(b, c, g))((a, e, h)(b, e, f))((a, d, g)(b, d, h)) \quad \text{and}$$
$$\tau_3 = ((a, c, f)(b, e, f))((a, d, g)(b, c, g))((b, d, h)(a, e, h)).$$

Lemma 2.5. *The permutations τ_1, τ_2 and τ_3 satisfy the following properties:*

(Q1) *If $\rho \in \mathcal{A}_r$, $\mu \in \mathcal{A}_s$, $1 \le r < s \le 3$, then $|\mathrm{Mov}(\rho) \cap \mathrm{Mov}(\mu)| \le 1$.*
(Q2) *For each $i \in \{1, 2, 3\}$, τ_i has no fixed points.*
(Q3) $\tau_1\tau_2\tau_3 = 1$.

Proof. Observe that τ_i leaves the i-th coordinate of a triple fixed.

(Q1) Let $r = 1$, $s = 2$ and take ρ, μ as specified. Suppose that x and y are distinct points in $\mathrm{Mov}(\rho) \cap \mathrm{Mov}(\mu)$. Let $x = (x_1, x_2, x_3)$. Then $(x_1, x_2, x_3)\rho^i = (x_1, x_2', x_3') = y$ and $(x_1, x_2, x_3)\mu^j = (x_1'', x_2, x_3'') = y$ for some i, j. This implies that $x_2 = x_2'$, a contradiction to the fact that ρ leaves only the first coordinate fixed. The cases $(r, s) = (1, 3)$ and $(2, 3)$ are similar.
(Q2) Each $\tau_i = \beta_s^{-1}\beta_r$ changes the tth component of a triple x, where $t \in \{s, r\}$.
(Q3) Observe that $\tau_1\tau_2\tau_3 = \beta_2^{-1}\beta_3\beta_3^{-1}\beta_1\beta_1^{-1}\beta_2 = 1$. $\square$

Thus from a given Latin bitrade we may define a set of permutations with particular properties. It turns out that there exists a reverse process.

Definition 2.6. Let τ_1, τ_2, τ_3 be permutations on some set X and for $i \in \{1, 2, 3\}$, let $\mathcal{A}_i$ be the set of cycles of τ_i. Suppose that τ_1, τ_2, τ_3 satisfy Conditions (Q1), (Q2) and (Q3) from Lemma 2.5. Next, define

$$S^\circ = \{(\rho_1, \rho_2, \rho_3) \mid \rho_i \in \mathcal{A}_i \text{ and there exists } x \text{ such that } x \in \mathrm{Mov}(\rho_i) \text{ for all } i\}$$

and

$$S^\star = \{(\rho_1, \rho_2, \rho_3) \mid \rho_i \in \mathcal{A}_i,\ \text{there exist distinct points } x, x', x'' \text{ in } X \text{ such that}$$
$$x\rho_1 = x', x'\rho_2 = x'', x''\rho_3 = x\}.$$

Theorem 2.7 ([9]). *Then the pair of partial Latin squares $(S^\circ, S^\star)$ is a Latin bitrade of size $|X|$ with $|\mathcal{A}_1|$ rows, $|\mathcal{A}_2|$ columns and $|\mathcal{A}_3|$ entries.*

Proof. Condition (Q1) ensures that S° is a partial Latin square.

From (Q3), $\tau_1\tau_2\tau_3$ fixes every point in X. It follows that, for each point $x \in X$, there is a unique choice of $\rho_1 \in \mathcal{A}_1$ not fixing x, $\rho_2 \in \mathcal{A}_2$ not fixing $x\rho_1$, and $\rho_3 \in \mathcal{A}_3$ not fixing $x\rho_1\rho_2$, such that $x\rho_1\rho_2\rho_3 = x$. Suppose that $(\rho_1, \rho_2, \rho_3), (\rho_1, \rho_2, \rho_3') \in S^\star$, where $\rho_3 \neq \rho_3'$. Then from our previous observation, if $\rho_1\rho_2\rho_3$ fixes $x \in X$ and $\rho_1\rho_2\rho_3'$ fixes $x' \in X$, $x \neq x'$. But this implies that $x\rho_1, x'\rho_1 \in \mathrm{Mov}(\rho_1) \cap \mathrm{Mov}(\rho_2)$, contradicting (Q1). By symmetry, $S^\star$ is also a partial Latin square.

Next, suppose that $(\rho_1, \rho_2, \rho_3) \in S^\circ \cap S^\star$. Then there are distinct points x, x', x'' such that $x\rho_1 = x'$, $x'\rho_2 = x''$ and $x''\rho_3 = x$. Thus $x' \in \mathrm{Mov}(\rho_1) \cap \mathrm{Mov}(\rho_2)$ and $x'' \in \mathrm{Mov}(\rho_2) \cap \mathrm{Mov}(\rho_3)$. But there exists $y \in \mathrm{Mov}(\rho_1) \cap \mathrm{Mov}(\rho_2) \cap \mathrm{Mov}(\rho_3)$ and either $y \neq x'$ or $y \neq x''$ is true. Without loss of generality suppose that $y \neq x''$ is true. Then $|\mathrm{Mov}(\rho_2) \cap \mathrm{Mov}(\rho_3)| \ge 2$, contradicting (Q1). Thus $S^\circ \cap S^\star = \emptyset$ and (R1) is satisfied.

Next we show that (R2) is satisfied. So suppose that $(\rho_1, \rho_2, \rho_3) \in S^\circ$ and let $y \in \mathrm{Mov}(\rho_1) \cap \mathrm{Mov}(\rho_2) \cap \mathrm{Mov}(\rho_3)$. Then there is some x and z such that $x\rho_1 = y$ and $y\rho_2 = z$. But ρ_1 is the only permutation in $\mathcal{A}_1$ that does not fix x and ρ_2 is the only permutation in $\mathcal{A}_2$ that does not fix y. It follows from the observation in the second paragraph of the proof that there is a unique $\rho_3' \in \mathcal{A}_3$ such that $z\rho_3' = x$. Thus $(\rho_1, \rho_2, \rho_3') \in S^\star$. By symmetry (R2) is satisfied.

Finally we show that (R3) is satisfied. So let $(\rho_1, \rho_2, \rho_3) \in S^\star$. Then there are distinct points x, x', x'' such that $x\rho_1 = x'$, $x'\rho_2 = x''$ and $x''\rho_3 = x$. Then there exists $x' \in \mathrm{Mov}(\rho_1) \cap \mathrm{Mov}(\rho_2)$. Let ρ_3' be the unique cycle of $\mathcal{A}_3$ that does not fix x'. Then $(\rho_1, \rho_2, \rho_3') \in S^\circ$. By symmetry (R3) is satisfied.

Since each cycle in ρ_1, ρ_2, ρ_3 gives rise to a unique row, column, entry (respectively), the Latin bitrade $(S^\circ, S^\star)$ will have $|\mathcal{A}_1|$ rows, $|\mathcal{A}_2|$ columns and $|\mathcal{A}_3|$ entries. $\square$

Example 2.8. Let $\tau_1 = (123)(456)$, $\tau_2 = (14)(26)(35)$ and $\tau_3 = (16)(34)(25)$ be three permutations on the set $\{1, 2, 3, 4, 5, 6\}$. Then these permutations satisfy Conditions (Q1), (Q2) and (Q3), thus generating a Latin bitrade of size 6 with two rows, three columns and three different entries. In fact, this Latin bitrade is isotopic to the Latin bitrade given in Example 2.2.

A Latin bitrade is said to be *separated* if each row, column and entry gives rise to exactly one cycle of τ_1, τ_2 and τ_3, respectively (see Definition 2.3). The Latin bitrade given in Example 2.2 is separated. The next example gives a non-separated Latin bitrade.

Example 2.9. Let $A_1 = \{a, b, c\}$, $A_2 = \{d, e, f, g\}$ and $A_3 = \{h, i, j, k\}$. Then $(T^\circ, T^\star)$ is a *Latin bitrade*, where $T^\circ, T^\star \subset A_1 \times A_2 \times A_3$ are shown below:

$T^\circ =$

$\circ$	d	e	f	g
a	h	i	j	k
b	i	l	k	
c	k	j	l	h

$T^\star =$

$\circ$	d	e	f	g
a	i	j	k	h
b	k	i	l	
c	h	l	j	k

.

Moreover, $(T^\circ, T^\star)$ is non-separated, by observation of row c.

The next theorem demonstrates that the process in Definition 2.6 is the inverse of the process in Definition 2.3 for separated Latin bitrades.

Theorem 2.10. *Let $(T^\circ, T^\star)$ be a separated Latin bitrade. Let τ_1, τ_2 and τ_3 be the corresponding set of permutations as given in Definition 2.3. In turn, let $(S^\circ, S^\star)$ be the Latin bitrade defined from τ_1, τ_2 and τ_3 via Definition 2.6. Then $(T^\circ, T^\star)$ and $(S^\circ, S^\star)$ are isotopic Latin bitrades.*

Proof. For each $i \in \{1, 2, 3\}$ and each $x \in A_i$, let $f_i(x) \in \mathcal{A}_i$ be the cycle in τ_i which includes x in each ordered triple. Since $(T^\circ, T^\star)$ is separated, each f_i is a 1–1 correspondence between A_i and $\mathcal{A}_i$. Indeed, if $(x_1, x_2, x_3) \in T^\circ$, then $(x_1, x_2, x_3) \in \mathrm{Mov}(f_1(x_1)) \cap \mathrm{Mov}(f_2(x_2)) \cap \mathrm{Mov}(f_3(x_3))$. Thus $(f_1(x_1), f_2(x_2), f_3(x_3)) \in S^\circ$.

Next, let $(y_1, y_2, y_3) \in T^\star$. Let $(y_1, y_2, y_3)\beta_1 = (y_1', y_2, y_3) \in T^\circ$, where $y_1' \neq y_1$. Define y_2' and y_3' similarly. Then $\tau_1 (= \beta_2^{-1}\beta_3)$ (in fact, its cycle $f_1(y_1)$) maps (y_1, y_2', y_3) to (y_1, y_2, y_3'). Similarly $f_2(y_2)$ maps (y_1, y_2, y_3') to (y_1', y_2, y_3) and $f_3(y_3)$ maps (y_1', y_2, y_3) to (y_1, y_2', y_3). It follows that $(f_1(y_1), f_2(y_2), f_3(y_3)) \in S^\star$. $\square$

Definition 2.11. A Latin bitrade $(T^\circ, T^\star)$ is said to be *primary* if whenever $(U^\circ, U^\star)$ is a Latin bitrade such that $U^\circ \subseteq T^\circ$ and $U^\star \subseteq T^\star$, then $(T^\circ, T^\star) = (U^\circ, U^\star)$.

It is not hard to show that a non-primary Latin bitrade may be partitioned into smaller, disjoint Latin bitrades.

Definition 2.12. A Latin trade T° is said to be *minimal* if whenever $(U^\circ, U^\star)$ is a Latin bitrade such that $U^\circ \subseteq T^\circ$ then $T^\circ = U^\circ$.

Note that for any primary bitrade $(T^\circ, T^\star)$, it is not necessarily true that T° or $T^\star$ is a minimal trade. Minimal Latin trades are important in the study of *critical sets* (minimal defining sets) of Latin squares (see [13] for a recent survey).

So a separated Latin bitrade may be identified with a set of permutations that act on a particular set X. Clearly, the permutations τ_1, τ_2, τ_3 generate some group G which acts on the set X. We now study the case where the set X is the set of elements of G.

Definition 2.13. Let G be a finite 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:

$$T^\circ = \{(gA, gB, gC) \mid g \in G\}, \qquad T^\star = \{(gA, gB, ga^{-1}C) \mid g \in G\}.$$

Theorem 2.14. *The pair of partial Latin squares $(T^\circ, T^\star)$ as defined above is a Latin bitrade with size $|G|$, $|G : A|$ rows (each with $|A|$ entries), $|G : B|$ columns (each with $|B|$ entries) and $|G : C|$ entries (each occurring $|C|$ times).*

If, in turn,

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

then the Latin bitrade is primary.

Proof. For each $g \in G$, define a map r_g on the elements of G by $r_g : x \mapsto xg$. Let $\tau_1 = r_a$, $\tau_2 = r_b$ and $\tau_3 = r_c$. Then (G1) implies (Q3) and (G2) implies (Q1). Since a, b and c are non-identity elements, each of r_a, r_b and r_c has no fixed points, so (Q2) is also satisfied. So from Theorem 2.7 with $X = G$, there exists a Latin bitrade $(S^\circ, S^\star)$ defined in terms of the cycles of r_a, r_b and r_c. A cycle in r_a is of the form $(g, ga, ga^2, \ldots, ga^{|A|-1})$ for some $g \in G$. Hence cycles of r_a (or r_b or r_c) permute the elements of the left cosets of A (or B or C, respectively).

Next relabel the triples of S° and $S^\star$, replacing each cycle with its corresponding (unique) left coset. Let this (isotopic) Latin bitrade be $(T^\circ, T^\star)$. Thus, from Definition 2.6,

$$T^\circ = \{(g_1A, g_2B, g_3C) \mid |g_1A \cap g_2B \cap g_3C| = 1\} \quad \text{and}$$
$$T^\star = \{(g_1A, g_2B, g_3C) \mid \text{ there exist elements } h \in g_1A, h' \in g_2B, h'' \in g_3C \text{ such that } ha = h', h'b = h'', h''c = h\}.$$

Consider an element $(g_1A, g_2B, g_3C) \in T^\circ$. Then there exists unique $g \in g_1A \cap g_2B \cap g_3C$. Thus $(g_1A, g_2B, g_3C) = (gA, gB, gC)$. Next, consider $(g_1A, g_2B, g_3C) \in T^\star$. In terms of h' we have $g_1A = h'A$ and $g_3C = h'a^{-1}C$. Letting $g = h'$ we have $(g_1A, g_2B, g_3C) = (gA, gB, ga^{-1}C)$. Thus $(T^\circ, T^\star)$ as given in Definition 2.13 is a Latin bitrade with size $|G|$.

From Theorem 2.7, the Latin bitrade $(T^\circ, T^\star)$ has $|G : A|$ rows, $|G : B|$ columns and $|G : C|$ entries. We next show that each row has $|A|$ entries. Consider an arbitrary row gA in $(T^\circ, T^\star)$. Since $ga^iA \cap ga^iB \cap ga^iC = \{ga^i\}$ for all i, we have $(ga^iA, ga^iB, ga^iC) \in T^\circ$ for all i. These entries are actually all on the same row since $ga^iA = gA$ for all i. Next, suppose that $ga^iB = ga^jB$ for some i, j. Then $a^iB = a^jB$ so $a^{i-j} \in B$ and $i = j$. So there are at least $|A|$ elements in the row. If there were more than $|A|$ elements in the row then there must be some h, x such that $gA \cap hB = \{x\}$. But then $x = ga^i = hb^j$ for some i, j and therefore $h = ga^ib^{-j}$ so $hB = ga^ib^{-j}B = ga^iB$ and columns of this form have already been accounted for. Similarly, each column has $|B|$ entries and each entry occurs $|C|$ times.

Finally we have the (G3) condition. For the sake of contradiction, suppose that $(T^\circ, T^\star)$ is not primary and $G = \langle a, b, c \rangle$. Then there is a (non-empty) bitrade $(W^\circ, W^\star)$ such that $W^\circ \subset T^\circ$ and $W^\star \subset T^\star$. Suppose that column gB lies in $(W^\circ, W^\star)$ for some $g \in G$.

To avoid a notation clash with the τ_i, define $\nu_1 = \beta_2^{-1}\beta_3$, $\nu_2 = \beta_3^{-1}\beta_1$ and $\nu_3 = \beta_1^{-1}\beta_2$ where the β_r send $T^\star$ to T°. Since $(W^\circ, W^\star)$ is a subtrade, the permutations ν_i send elements of W° to itself. The cycles of ν_i are of length $|A|$, $|B|$, or $|C|$, so W° has $|A|$ entries per row and $|B|$ entries per column. In particular, if column gB intersects $(W^\circ, W^\star)$, then column ga^iB intersects $(W^\circ, W^\star)$ for any i. By a similar analysis of the rows, if row gA lies in $(W^\circ, W^\star)$ then row gb^jA lies in $(W^\circ, W^\star)$ for any j. It follows that

$$\begin{aligned} & (gA, gB, gC) \in W^\circ && \Rightarrow \quad (ga^iA = gA, ga^iB, ga^iC) \in W^\circ \\ \Rightarrow \quad & (ga^ib^jA, ga^ib^jB = ga^iB, ga^ib^jC) \in W^\circ && \Rightarrow \quad (ga^ib^jA, ga^ib^ja^kB, ga^ib^ja^kC) \in W^\circ, \end{aligned}$$

for any i, j and k. Thus if column gB lies in W°, then any column of the form $ga^ib^ja^kB$ lies in W°. By an iterative process, since any element of G can be written as a product of powers of a and b, it follows that W° includes every column of T° and $(W^\circ, W^\star) = (T^\circ, T^\star)$. □

Corollary 2.15. *The Latin trade T° in the previous theorem is equivalent to the set* $\{(g_1A, g_2B, g_3C) \mid g_1, g_2, g_3 \in G, |g_1A \cap g_2B \cap g_3C| = 1\}$, *which is in turn equivalent to* $\{(g_1A, g_2B, g_3C) \mid g_1, g_2, g_3 \in G, g_1A \cap g_2B = \{g_3\}\}$.

It should be noted that this construction does not produce *every* Latin bitrade, as Latin bitrades in general may have rows and columns with varying sizes. However, as the rest of the paper demonstrates, this technique produces many interesting examples.

Example 2.16. Let $G = \langle s, t \mid s^3 = t^2 = 1, ts = s^2t\rangle$, the symmetric group on three letters. $A = \langle s\rangle$, $B = \langle t\rangle$, $C = \langle ts^2\rangle$. Then (G1), (G2) and (G3) are satisfied. The left cosets are: $\langle s\rangle, t\langle s\rangle$; $\langle t\rangle, s\langle t\rangle, s^2\langle t\rangle$; $\langle ts^2\rangle, s\langle ts^2\rangle, s^2\langle ts^2\rangle$. Then the Latin bitrade is

$T^\circ =$

$\circ$	B	sB	s^2B
A	C	sC	s^2C
tA	s^2C	C	sC

$T^\star =$

$\star$	B	sB	s^2B
A	s^2C	C	sC
tA	C	sC	s^2C

.

Note that this Latin bitrade is isotopic to the one given in Example 2.2.

3. Orthogonality, minimality and homogeneity

In this section we describe how certain properties of Latin bitrades constructed as in Theorem 2.14 may be encoded in the group structure.

Definition 3.1. A Latin bitrade $(T^\circ, T^\star)$ is said to be *orthogonal* if whenever $i \circ j = i' \circ j'$ (for $i \neq i'$, $j \neq j'$), then $i \star j \neq i' \star j'$.

We use the term orthogonal because if $(T^\circ, T^\star)$ is a Latin bitrade and $T^\circ \subset L_1$, $T^\star \subset L_2$, where L_1 and L_2 are *mutually orthogonal Latin squares* (see [8] for a definition), then $(T^\circ, T^\star)$ is *orthogonal*.

Lemma 3.2. *A Latin bitrade $(T^\circ, T^\star)$ constructed from a group $G = \langle a, b, c\rangle$ as in Theorem 2.14 is orthogonal if and only if $|C \cap C^a| = 1$.*

Proof. First suppose that the Latin bitrade is not orthogonal. Then $gC = hC$ and $ga^{-1}C = ha^{-1}C$ for some $g, h \in G$ with $g \neq h$, as shown in the following diagram:

$\circ$	gB	hB
gA	gC	
hA		hC

$\star$	gB	hB
gA	$ga^{-1}C$	
hA		$ha^{-1}C$

Then $g^{-1}h \in C$ and $ag^{-1}ha^{-1} \in C$ which implies that $g^{-1}h \in a^{-1}Ca = C^a$. Thus $|C \cap C^a| \neq 1$.

Conversely, suppose that $x \in C \cap C^a$ where $x \neq 1$. Then we may write $x = h^{-1}g$ for some non-identity elements $g, h \in G$. We then reverse the steps in the previous paragraph to show that the Latin bitrade is not orthogonal. $\square$

Is it possible to encode minimality via our group construction? We do this by encoding a "thin" property of Latin bitrades, which, together with the primary property, implies minimality.

Definition 3.3. A Latin bitrade $(T^\circ, T^\star)$ is said to be *thin* if whenever $i \circ j = i' \circ j'$ (for $i \neq i'$, $j \neq j'$), then $i \star j'$ is either undefined, or $i \star j' = i \circ j$.

Lemma 3.4. *Let $(T^\circ, T^\star)$ be a thin and primary Latin bitrade. Then T° is a minimal Latin trade.*

Proof. Suppose, for the sake of contradiction, that $(T^\circ, T^\star)$ is thin but not minimal. Then there exists a Latin bitrade $(U^\circ, U^\otimes)$ such that $U^\circ \subset T^\circ$. Since $(U^\circ, U^\otimes)$ is a Latin bitrade, then for any i, j, k such that $i \otimes j = k$, there are i', j' such that $i \circ j' = i' \circ j = k$, where $i \neq i'$ and $j \neq j'$. By thinness of $(T^\circ, T^\star)$, it follows that $i \star j$ is either undefined or $i \star j = k$. However, $i \otimes j$ is defined, so $i \circ j$ is defined in both U° and T°. So $i \star j = k$ and we see that $U^\otimes \subset T^\star$, contradicting the primary property. $\square$

In general, the minimality of Latin bitrades can be complicated to check (see, for example, [6]), highlighting the elegance of the following lemma.

Lemma 3.5. *A Latin bitrade $(T^\circ, T^\star)$ constructed from a group $G = \langle a, b, c\rangle$ as in Theorem 2.14 is thin (and thus minimal) if and only if the only solutions to the equation $a^i b^j c^k = 1$ are $(i, j, k) = (0, 0, 0)$ and $(i, j, k) = (1, 1, 1)$, where i, j and k are calculated modulo $|A|$, $|B|$ and $|C|$, respectively.*

Proof. We first rewrite Definition 3.3 in terms of cosets. Let $i = g_1 A$, $j = g_2 B$ for some $g_1, g_2 \in G$. Since $i \circ j$ must be defined it follows that $g_1 A$ and $g_2 B$ intersect. By Corollary 2.15 this intersection is a unique element $g \in G$. Thus $i = gA$, $j = gB$. Similarly, $i' = hA$, $j' = hB$ for a unique $h \in G$. For a Latin bitrade to be thin we must have $i \star j' = i \circ j$ whenever $i \star j'$ is defined. In other words, the Latin bitrade is thin if $gC = hC$ implies that $gC = xa^{-1}C$ whenever there exists (a unique) $x \in gA \cap hB$.

$\circ$	gB	hB
gA	gC	xC
hA		hC

$\star$	gB	hB
gA	$ga^{-1}C$	$xa^{-1}C$
hA		$ha^{-1}C$

First suppose that the only solutions to $a^i b^j c^k = 1$ are $(i, j, k) = (0, 0, 0)$ and $(i, j, k) = (1, 1, 1)$. To check for thinness, suppose that $gC = hC$ and that there exists an $x \in gA \cap hB$. Then $x = ga^m = hb^{-n}$ for some m, n. Now $a^m b^n = g^{-1}h = c^{-p}$ for some p since $gC = hC$ implies that $g^{-1}h \in C$. So $a^m b^n c^p = 1$. If $m = n = p = 0$ then $g = h$ which is a contradiction. Otherwise $(m, n, p) = (1, 1, 1)$ so $x = ga$. Now $g^{-1}xa^{-1} = g^{-1}gaa^{-1} = 1 \in C$ so $gC = xa^{-1}C$ as required.

Conversely, suppose that the Latin bitrade is thin and that $a^m b^n c^p = 1$ for some m, n, p. There is always a trivial solution $(0, 0, 0)$ so it suffices to check that $(1, 1, 1)$ is the only other possibility. Since $a^m b^n c^p = 1$ we can write $ga^m = (gc^{-p})b^{-n}$ for any $g \in G$. Define $h = gc^{-p}$ and $x = ga^m = hb^{-n}$. Now $hC = gc^{-p}C = gC$ and by definition $x \in gA \cap hB$ so $gA \star hB$ is defined. Now thinness implies that $gC = xa^{-1}C$, so $g^{-1}xa^{-1} \in C$. Then $g^{-1}ga^m a^{-1} = a^{m-1} \in C$ so $m = 1$. Since $abc = 1$,

$$1 = ab^n c^p = c^{-1}b^{-1}b^n c^p = c^{-1}b^{n-1}c^p \Rightarrow b^{n-1}c^{p-1} = 1$$

so $b^{n-1} = c^{1-p}$ and therefore $(m, n, p) = (1, 1, 1)$. □

Definition 3.6. A Latin trade T° is said to be (k-)*homogeneous* if each row and column contains precisely k entries and each entry occurs precisely k times within T°.

The next lemma follows from Theorem 2.14.

Lemma 3.7. *A Latin bitrade $(T^\circ, T^\star)$ constructed from a group $G = \langle a, b, c\rangle$ as in Theorem 2.14 is k-homogeneous if and only if $|A| = |B| = |C| = k$.*

A 2-homogeneous Latin bitrade is trivially the union of Latin squares of order 2. A construction for 3-homogeneous Latin bitrades is given in [4]; moreover in [3] it is shown that this construction gives every possible primary 3-homogeneous Latin bitrade. The problem of determining the spectrum of sizes of k-homogeneous Latin bitrades is solved in [2]; however if we add the condition of minimality this problem becomes far more complex. Some progress towards this has been made in [5,6]; however it is even an open problem to determine the possible sizes of a minimal 4-homogeneous Latin bitrade. The theorems in the following section yield previously unknown cases of minimal k-homogeneous Latin bitrades.

4. Examples

In this section we apply Theorem 2.14 to generate bitrades from various groups. All of the bitrades constructed will be primary, so by Lemma 3.4 thinness will imply minimality for each example.

4.1. Abelian groups

An abelian group G has the normaliser $N_G(C)$ equal to the entire group so $C = C^a$. By Lemma 3.2 abelian groups will not generate orthogonal bitrades. The next lemma gives an example of a Latin bitrade constructed from an abelian group.

Lemma 4.1. *Let p be a prime. Then $G = (\mathbb{Z}_p \times \mathbb{Z}_p, +)$ generates a Latin bitrade $(T^\circ, T^\star)$ using $a = (0, 1)$, $b = (1, 0)$ and $c = (p-1, p-1)$.*

Proof. First, $(0, 1) + (1, 0) + (p-1, p-1) = (0, 0)$ so (G1) is met. For (G2):

- $A \cap B = \{(0, 0)\}$.
- Note that $(0, x) \in C$ only when $x = 0$ so A and C intersect in the single element $(0, 0)$.
- There is no $(x, 0) \in B \cap C$ with $x \neq 0$ by similar reasoning.

Lastly, $G = \langle a, b, c\rangle$ follows from the definition of a and b so (G3) is satisfied. □

The Latin bitrade T° in the above lemma is in fact a Latin square so in some sense this example is degenerate.

4.2. A p^3-group example

It is well known (see, for example, [12, p. 52]) that for any odd prime p there exists a non-abelian group G of order p^3, with generators a, b, c and relations

$$a^p = b^p = c^p = 1, \tag{1}$$

$$ab = bac, \tag{2}$$

$$ca = ac, \tag{3}$$

$$cb = bc. \tag{4}$$

For convenience we let $z = c^{-1}$ throughout this section.

Lemma 4.2. *Any word $w \in G$ can be written in the form $a^i b^j c^k$. Further, the group operation can be defined in terms of the canonical representation*

$$(a^i b^j z^k)(a^r b^s z^t) = a^{i+r} b^{j+s} z^{k+t+jr}.$$

Lemma 4.3. *Let $\gamma = b^{-1}a^{-1}$. Then $\gamma^k = a^{-k} b^{-k} z^{k(k+1)/2}$ and γ has order p.*

Proof. First we show that $(a^{-1}b^{-1})^k = a^{-k}b^{-k}z^{k(k-1)/2}$ by induction on k. When $k = 1$ the statement is true. The inductive step is

$$\begin{aligned}(a^{-1}b^{-1})^{k+1} &= (a^{-1}b^{-1})(a^{-1}b^{-1})^k = (a^{-1}b^{-1})a^{-k}b^{-k}z^{k(k-1)/2}\\ &= a^{-(k+1)}b^{-(k+1)}z^{k(k-1)/2+k} = a^{-(k+1)}b^{-(k+1)}z^{(k+1)k/2}.\end{aligned}$$

Now we can evaluate γ^k:

$$\begin{aligned}\gamma^k &= (b^{-1}a^{-1})^k = (a^{-1}b^{-1}z)^k = (a^{-1}b^{-1})^k z^k\\ &= a^{-k}b^{-k}z^{k+k(k-1)/2} = a^{-k}b^{-k}z^{k(k+1)/2}.\end{aligned}$$

Since $\gamma^p = a^{-p}b^{-p}z^{p(p+1)/2} = 1$ we see that γ has order p. □

Theorem 4.4. *Let $\alpha = a$, $\beta = b$, $\gamma = b^{-1}a^{-1}$ where a, b, and c generate a group satisfying (1) through (4). Then α, β and γ satisfy conditions* (G1), (G2) *and* (G3) *of Theorem* 2.14. *Thus for each prime p, there exists a primary, p-homogeneous Latin bitrade of size p^3 given by*

$$(\{(g\langle\alpha\rangle, g\langle\beta\rangle, g\langle\gamma\rangle) \mid g \in G\}, \{(g\langle\alpha\rangle, g\langle\beta\rangle, g\alpha^{-1}\langle\gamma\rangle) \mid g \in G\}).$$

Proof. By definition $\alpha\beta\gamma = 1$ so (G1) is true. For (G2):

- The element a is of order p so any non-identity element of $\langle a\rangle$ generates $\langle a\rangle$. The same holds for b and $\langle b\rangle$. If $a^m = b^n$ for some $0 < m, n < p$ then $\langle a\rangle = \langle b\rangle$. So $b = a^r$ for some r and (2) becomes $a^{r+1} = a^{r+1}c$ so $c = 1$, a contradiction. Hence $\langle\alpha\rangle \cap \langle\beta\rangle = 1$.
- The subgroup $\langle a\rangle$ has order p and by Lemma 4.3 so does $\langle\gamma\rangle$. If $a^l = \gamma^k$ for some $0 < l, k < p$ then $\langle a\rangle = \langle\gamma\rangle$. The argument is now similar to the first case. Hence $\langle\alpha\rangle \cap \langle\gamma\rangle = 1$.

- Showing that $\langle\beta\rangle \cap \langle\gamma\rangle = 1$ is very similar to the first case.

  Lastly, $G = \langle \alpha, \beta, \gamma \rangle$ since $a = \alpha$, $b = \beta$, and $c = \alpha^{-1}\beta^{-1}\gamma^{-1}$. Thus (G3) is satisfied. □

Lemma 4.5. *Let G be a finite group and $g, h \in G$. If the product gh is in $Z(G)$ then $gh = hg$.*

Proof. Since $gh \in Z(G)$ it must commute with any element of G. Thus $(gh)g^{-1} = g^{-1}(gh) = h$ so $gh = hg$. □

Lemma 4.6. *Let G be the group defined by (1) through (4). Then $Z(G) = \langle c \rangle$.*

Proof. Since c is in $Z(G)$ we know that $\langle c \rangle \le Z(G)$. For the converse, suppose that there is a group element w in $Z(G)$ but $w \notin \langle c \rangle$. By Lemma 4.2 we can write $w = a^i b^j c^k$ for some i, j, k. Then $(a^i b^j c^k)c^{-k} \in Z(G)$ since $c \in Z(G)$, which means that $a^i b^j \in Z(G)$. By Lemma 4.5, $a^i b^j = b^j a^i$. However, using (2) we have $a^i b^j = b^j a^i c^{ij}$ so it must be that $p \mid ij$. If $p \mid i$ then $w = b^j c^k$ which implies that $b \in Z(G)$, a contradiction. Similarly, if $p \mid j$ then $a \in Z(G)$, another contradiction. □

Lemma 4.7. *Latin bitrades constructed as in Theorem 4.4 are thin.*

Proof. Suppose that $\alpha^i \beta^j \gamma^k = 1$ for some i, j, k. Then by Lemmas 4.2 and 4.3

$$\begin{aligned} 1 &= a^i b^j \gamma^k = a^i b^j \left(a^{-k} b^{-k} z^{k(k+1)/2}\right) \\ &= a^{i-k} b^{j-k} z^{k(k+1)/2 - jk}. \end{aligned} \tag{5}$$

By Lemma 4.6, $a^{i-k}b^{j-k} \in Z(G)$ and by Lemma 4.5, $a^{i-k}b^{j-k} = b^{j-k}a^{i-k}$. Using (2) a total of $(i-k)(j-k)$ times we have $a^{i-k}b^{j-k} = b^{j-k}a^{i-k}c^{(i-k)(j-k)}$ so $c^{(i-k)(j-k)} = 1$. Since p is prime there are two cases:

1. If $p \mid i - k$ then (5) reduces to $1 = b^{j-k}z^{k(k+1)/2-jk}$ so $p \mid j - k$.
2. If $p \mid j - k$ then (5) reduces to $1 = a^{i-k}z^{k(k+1)/2-jk}$ so $p \mid i - k$.

Thus $p \mid i - k$ and $p \mid j - k$. Now $i \equiv k \pmod p$ and $j \equiv k \pmod p$ which implies $i \equiv j \equiv k \pmod p$, and (5) becomes

$$1 = z^{k(k+1)/2 - k^2} \quad \Rightarrow \quad 1 = z^{k(k-1)/2},$$

so $p \mid \frac{1}{2}k(k-1)$. If $p \mid k$ then $(i, j, k) \equiv (0, 0, 0)$. Otherwise, $p \mid \frac{1}{2}(k-1)$ and $(i, j, k) \equiv (1, 1, 1)$. By Lemma 3.5 the Latin bitrade is thin. □

Lemma 4.8. *The Latin bitrade constructed in Theorem 4.4 is orthogonal.*

Proof. Suppose for the sake of contradiction (see Lemma 3.2) that $\langle\gamma\rangle$ and $\langle\gamma\rangle^\alpha$ have a non-trivial intersection. Since $\langle\gamma\rangle$ and $\langle\gamma\rangle^\alpha$ are cyclic of order p, it must be that $\langle\gamma\rangle = \langle\gamma\rangle^\alpha$ so $\alpha^{-1}\gamma^k\alpha = \gamma$ for some k. Hence

$$\begin{aligned} & \alpha^{-1}\gamma^k\alpha = b^{-1}a^{-1} \\ \Rightarrow \quad & (ab)a^{-1}\left(a^{-k}b^{-k}z^{k(k+1)/2}\right)a = 1 \\ \Rightarrow \quad & aba^{-k}b^{-k}z^{k(k+1)/2-k} = 1 \\ \Rightarrow \quad & a^{-k+1}b^{-k+1}z^{k(k+1)/2-2k} = 1. \end{aligned}$$

Now $a^{-k+1}b^{-k+1} \in Z(G)$ so by Lemma 4.5, $a^{-k+1}b^{-k+1} = b^{-k+1}a^{-k+1}$. From (2) we can deduce that $a^{-k+1}b^{-k+1} = b^{-k+1}a^{-k+1}c^{(-k+1)(-k+1)}$; hence $k \equiv 1 \pmod p$. Now

$$a^{-1}\gamma a = \gamma \quad \Rightarrow \quad a^{-1}b^{-1}a^{-1}a = b^{-1}a^{-1} \quad \Rightarrow \quad ab = ba,$$

which is a contradiction since a and b do not commute with each other. □

4.3. $|G| = pq$, where p and q are primes and G is non-abelian

Let p and q be primes such that $p > q > 2$ and q divides $p - 1$. Let $G = \langle a, b \rangle$ be the non-abelian group of order pq defined by

$$a^p = b^q = 1 \quad \text{and} \tag{6}$$

$$b^{-1}ab = a^r, \tag{7}$$

where $r \in \{2, 3, \ldots, p-1\}$ is some solution to $r^q \equiv 1 \pmod p$. The following remark may be verified by induction.

Remark 4.9. Let G be the group defined by (6) and (7). Then for any integers i, j, k, l,

$$b^i a^j b^k a^l = b^{i+k} a^m, \tag{8}$$

$$(ab)^k = b^k a^{r(r^k-1)/(r-1)}, \tag{9}$$

$$(bab)^k = b^{2k} a^{r(r^{2k}-1)/(r^2-1)}, \tag{10}$$

where $m = jr^k + l$.

Theorem 4.10. *Let $\alpha = b$, $\beta = ab$ and $\gamma = b^{-1}a^{-1}b^{-1}$ where a and b generate a group that satisfies (6) and (7). Then α, β and γ satisfy conditions* (G1), (G2) *and* (G3) *of Theorem* 2.14. *Thus for each pair of primes p, q such that $q > 2$ and q divides $p-1$, there exists a q-homogeneous Latin bitrade of size pq given by*

$$(\{(g\langle\alpha\rangle, g\langle\beta\rangle, g\langle\gamma\rangle) \mid g \in G\}, \{(g\langle\alpha\rangle, g\langle\beta\rangle, g\alpha^{-1}\langle\gamma\rangle) \mid g \in G\}).$$

Proof. Clearly $\alpha\beta\gamma = 1$, thus satisfying (G1). It is also clear that α and β together generate G, so (G3) is satisfied. We next check (G2).

- If $\langle\alpha\rangle \cap \langle\beta\rangle \neq 1$, then $b^k = ab$ for some k. This implies that $b^{k-1} = a$ so $a \in \langle b\rangle$. Then a and b must generate the same cyclic subgroup of prime order, a contradiction since $p \neq q$.
- If $\langle\alpha\rangle \cap \langle\gamma\rangle \neq 1$, then $b^k = b^{-1}a^{-1}b^{-1}$ for some k, or equivalently $a^{-1} = b^{k+2}$. So $a \in \langle b\rangle$, a contradiction.
- If $\langle\beta\rangle \cap \langle\gamma\rangle \neq 1$, $(ab)^k = b^{-1}a^{-1}b^{-1}$ for some k. Then $(ab)^{k+1} = b^{-1}$. Therefore from Eq. (9) we have $b^{k+1}a^{r(r^{k+1}-1)/(r-1)} = b^{-1}$ so $b^{k+2}a^{r(r^{k+1}-1)/(r-1)} = 1$. The subgroups $\langle a\rangle$ and $\langle b\rangle$ only intersect in the identity, so $k \equiv -2 \pmod q$. But
$$(ab)^q = b^q a^{r(r^q-1)/(r-1)} = b^q = 1$$
as $r^q \equiv 1 \pmod p$. Thus $(ab)^k = (ab)^{-2} = b^{-1}a^{-1}b^{-1}$ which implies that $a = 1$, a contradiction.

It remains to show that this Latin bitrade is q-homogeneous. To see this, note that $\beta^q = (ab)^q = 1$. Next, from Eq. (10),

$$\gamma^q = (b^{-1}a^{-1}b^{-1})^q = ((bab)^q)^{-1} = \left(b^{2q}a^{r(r^{2q}-1)/(r^2-1)}\right)^{-1} = 1. \quad \square$$

Lemma 4.11. *The Latin bitrade constructed in Theorem* 4.10 *is orthogonal.*

Proof. Suppose for the sake of contradiction (see Lemma 3.2) that $\langle\gamma\rangle$ and $\langle\gamma\rangle^\alpha$ have a non-trivial intersection. Since $\langle\gamma\rangle$ and $\langle\gamma\rangle^\alpha$ are cyclic of order q, it must be that $\langle\gamma\rangle = \langle\gamma\rangle^\alpha$ so $\alpha^{-1}\gamma^k\alpha = \gamma$ for some k. Observe that $\alpha^{-1}\gamma\alpha = b^{-1}(b^{-1}a^{-1}b^{-1})b = b^{-2}a^{-1} = a^{-r^2}b^{-2}$. So, for some integer k, we must have that $\gamma^k = (b^{-1}a^{-1}b^{-1})^k = a^{-r^2}b^{-2}$. From Eq. (10), this implies that

$$a^{(r^4-r^2-r^{2k+1}+r)/(r^2-1)} = b^{2k-2}.$$

Thus $k \equiv 1 \pmod q$, so $r^k \equiv r \pmod p$. So,

$$a^{(r^4-r^2-r^{2k+1}+r)/(r^2-1)} = a^{r^2-r}.$$

Thus $r^2 \equiv r \pmod p$, which, in turn, implies that $r \equiv 1 \pmod p$, a contradiction. $\square$

Lemma 4.12. *The Latin bitrade constructed in Theorem* 4.10 *is thin if and only if the solutions to*

$$r^j + r^{j-1} \equiv r^{i+j-1} + 1 \pmod p$$

are precisely $i \equiv j \equiv 0 \pmod q$ and $i \equiv j \equiv 1 \pmod q$.

Proof. By Lemma 3.5 the Latin bitrade is *not* thin if and only if $\alpha^i\beta^j\gamma^k = 1$ has a non-trivial solution in i, j, k. In general, we can simplify $\alpha^i\beta^j\gamma^k = 1$ as follows:

$$\begin{aligned}
& & \alpha^i\beta^j\gamma^k &= 1\\
\Leftrightarrow & & b^i(ab)^j(b^{-1}a^{-1}b^{-1})^k &= 1\\
\Leftrightarrow & & b^{i+j}a^{r(r^j-1)/(r-1)}\left(b^{2k}a^{r(r^{2k}-1)/(r^2-1)}\right)^{-1} &= 1\\
\Leftrightarrow & & b^{i+j}a^{r(r^j-1)/(r-1)}a^{-r(r^{2k}-1)/(r^2-1)}b^{-2k} &= 1\\
\Leftrightarrow & & a^{r(r^j-1)/(r-1)-r(r^{2k}-1)/(r^2-1)} &= b^{2k-(i+j)}.
\end{aligned}$$

Since a and b are elements of different prime order, $\alpha^i\beta^j\gamma^k = 1$ if and only if $i + j \equiv 2k \pmod{q}$ and

$$\begin{aligned}
& \frac{r(r^j-1)}{(r-1)} - \frac{r(r^{2k}-1)}{(r^2-1)} \equiv 0 \pmod{p}\\
\Leftrightarrow \quad & r((r^j-1)(r+1) - r^{2k} + 1) \equiv 0 \pmod{p}\\
\Leftrightarrow \quad & r^j + r^{j-1} - 1 - r^{2k-1} \equiv 0 \pmod{p}.
\end{aligned}$$

The result follows. $\square$

An example of a non-thin Latin bitrade is the case $q = 11$, $p = 23$ and $r = 4$, as $4^5 + 4^6 \equiv 4^9 + 1 \pmod{23}$. It is an open problem to predict when the Latin bitrade in this subsection is thin (and indeed, minimal). In general, if the ratio p/q is large there seems to be more chance of the Latin bitrade being thin. In particular, it can be shown that if $q = 3$ or if $p = r^q - 1$, then the Latin bitrade is always thin.

4.4. *The alternating group on $3m + 1$ letters*

Let $m \geq 1$ and define permutations a and b on the set $[3m + 1] = \{1, 2, \ldots, 3m + 1\}$:

$$a = (1, 2, \ldots, 2m + 1) \tag{11}$$

$$b = (m + 1, m, \ldots, 1, 2m + 2, 2m + 3, \ldots, 3m + 1). \tag{12}$$

So $|\mathrm{Mov}(a) \cap \mathrm{Mov}(b)| = m + 1$. These permutations in fact generate the alternating group:

Lemma 4.13. *Let $G = \langle a, b\rangle$. Then $G = A_{3m+1}$.*

To prove the above lemma, we will require some results from the study of permutation groups. Relevant definitions can be found in [15,16].

Theorem 4.14 ([15], p. 19). *Let G be transitive on Ω and $\alpha \in \Omega$. Then G is $(k + 1)$-fold transitive on Ω if and only if G_α is k-fold transitive on $\Omega \setminus \alpha$.*

We say that $\Gamma \subseteq \Omega$ is a *Jordan set* and its complement $\Delta = \Omega \setminus \Gamma$ a *Jordan complement* if $|\Gamma| > 1$ and the pointwise stabiliser $G_{(\Delta)}$ acts transitively on Γ. The next theorem is a modern version of a result given by B. Marggraff in 1889.

Theorem 4.15 ([16], Theorem 7.4B, p. 224). *Let G be a group acting primitively on a finite set Ω of size n, and suppose that G has a Jordan complement of size m, where $m > n/2$. Then $G \geq A_\Omega$.*

Here are a few important elements of the group $G = \langle a, b\rangle$:

$$\begin{aligned}
r &= [a, b] = aba^{-1}b^{-1} = (1, 2m + 1)(m + 1, 3m + 1),\\
s &= (ab)^{-1}r(ab) = (1, 2m + 2)(m + 1, m + 2),\\
t &= rs = (1, 2m + 1, 2m + 2)(m + 1, 3m + 1, m + 2),\\
v_k &= a^{-k}ra^k = (1a^k, (2m + 1)a^k)((m + 1)a^k, 3m + 1),\\
u &= v_m = a^{-m}ra^m = (m, m + 1)(2m + 1, 3m + 1).
\end{aligned}$$

Lemma 4.16. *The group $G = \langle a, b\rangle$ is primitive.*

Proof. Consider the subgroup $G_1 = \{g \in G \mid 1g = 1\}$. The product

$$ab = (m+1, m+2, \ldots, 2m+1, 2m+2, \ldots, 3m+1)$$

is in G_1 so G_1 is transitive on $M = \{m+1, m+2, \ldots, 3m+1\}$. For $m = 1$, G is obviously 2-transitive. Otherwise suppose that $m > 1$.

Since $v_m = (m+1, m)(2m+1, 3m+1)$ we see that G_1 is transitive on $M' = M \cup \{m\}$. Using v_{m-1}, $v_{m-2}, \ldots, v_2 = (3, 2)(m+3, 3m+1)$, all of which are in G_1, shows that G_1 is transitive on $[3m+1] \setminus \{1\}$. By Theorem 4.14 with $k = 1$, G is 2-transitive, and hence primitive. □

Proof of Lemma 4.13. The cases $m = 1, 2, 3$, and 4 can be checked by explicitly constructing an isomorphism from G to A_{3m+1}. So we assume that $m \geq 5$ and define a Jordan set

$$\Gamma = \{1, m, m+1, m+2, 2m+1, 2m+2, 3m+1\}$$

and its complement $\Delta = [3m+1] \setminus \Gamma$. Then $|\Delta| = 3m-6 > (3m+1)/2$ when $m \geq 5$ so Δ is large enough. The pointwise stabiliser $G_{(\Delta)}$ consists of all group elements g such that $xg = x$ for $x \in \Delta$. Hence t and u are in $G_{(\Delta)}$ so $G_{(\Delta)}$ is transitive on Γ. By Theorem 4.15, $G \geq A_\Omega$. Lastly, an odd cycle can be written as a product of an even number of transpositions so $G \leq A_{3m+1}$. □

Theorem 4.17. *Let a and b be given as in Eqs. (11) and (12), and let $c = ab$, $\alpha = a$, $\beta = b$, $\gamma = c^{-1}$ be elements of $G = A_{3m+1}$, the alternating group on $3m+1$ elements. Then α, β, and γ satisfy conditions* (G1), (G2) *and* (G3) *of Theorem 2.14. Thus for each $m \geq 1$, there exists a primary $(2m+1)$-homogeneous Latin bitrade of size $(3m+1)!/2$ given by*

$$(\{(g\langle\alpha\rangle, g\langle\beta\rangle, g\langle\gamma\rangle) \mid g \in G\}, \{(g\langle\alpha\rangle, g\langle\beta\rangle, g\alpha^{-1}\langle\gamma\rangle) \mid g \in G\}).$$

Proof. Clearly (G1) holds. Next we verify (G2). Suppose that $\langle\alpha\rangle \cap \langle\beta\rangle \neq 1$. Then $a^i = b^j$ for some i, j. In particular, $(3m+1)a^i = (3m+1)b^j$. Since $3m+1 \in \mathrm{Fix}(a)$, it must be that $(3m+1)b^j = 3m+1$, so $j \equiv 0 \pmod{2m+1}$. Then $a^i = 1$ so $i \equiv j \equiv 0 \pmod{2m+1}$, a contradiction. By considering the action on the point 1 we can also show that $\langle\alpha\rangle \cap \langle\gamma\rangle \neq 1$ and $\langle\beta\rangle \cap \langle\gamma\rangle \neq 1$. Lastly (G3) is given by Lemma 4.13. □

Lemma 4.18. *The Latin bitrade constructed in Theorem 4.17 is thin.*

Proof. Let x be a point in $X = \{1, 2, \ldots, m\}$. Since c^k fixes x, we have $xa^ib^j = x$ for $x \in X$. Then it must be that $xa^i \in \{1, 2, \ldots, m+1\}$ otherwise b^j will be unable to map xa^i onto x. Thus $i \equiv 0$ or $1 \pmod{2m+1}$. If $i \equiv 0 \pmod{2m+1}$, then we must have $xb^j = x$ for each $x \in X$. Thus $j \equiv 0 \pmod{2m+1}$ which in turn implies that $k \equiv 0 \pmod{2m+1}$. Otherwise $i \equiv 1 \pmod{2m+1}$, which similarly implies that $j \equiv k \equiv 1 \pmod{2m+1}$. □

Lemma 4.19. *The Latin bitrade constructed in Theorem 4.17 is orthogonal.*

Proof. From Lemma 3.2, the Latin bitrade is orthogonal if and only if $|C \cap C^a| = 1$. So suppose that $c^i = a^{-1}c^ja$ for some integers i, j. Then

$$(1)c^i = 1 = (1)a^{-1}c^ja = (2m+1)c^ja.$$

For $(2m+1)c^ja = 1$ we must have $(2m+1)c^j = 2m+1$ so $j \equiv 0 \pmod{2m+1}$ which also implies that $i \equiv 0 \pmod{2m+1}$. Hence $|C \cap C^a| = 1$ as required. □

Example 4.20. Letting $m = 1$, we construct a thin, orthogonal Latin bitrade of size 12 as in this subsection. Here $a = (123)$, $b = (214)$ and $c = (243)$. We use the following cosets of $A = \langle a\rangle B = \langle b\rangle$ and $C = \langle c\rangle$ within the

Table 1
Sizes of minimal k-homogeneous Latin bitrades

k	Theorem 4.4	Theorem 4.10	Theorem 4.17	[6]	Smallest known
3	27	21 ($p = 7, q = 3, r = 2$)	12	21	12
5	125	55 ($p = 11, q = 5, r = 3$)	2520	75	55
7	343	203 ($p = 29, q = 7, r = 7$)	1814400	133	133
9	N/A	N/A	3113510400	243	243
11	1331	737 ($p = 67, q = 11, r = 14$)	16!/2	407	407

alternating group A_4:

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

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

$T^{\circ} =$

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

$T^{\star} =$

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

5. Minimal k-homogeneous Latin bitrades

Table 1 lists the sizes of the smallest minimal k-homogeneous Latin bitrades, where k is odd and $3 \leq k \leq 11$. We give the smallest such sizes for each of Theorems 4.4, 4.10 and 4.17, comparing these to the smallest sizes given by Lemma 17 and Table 2 of [6]. It is known that the smallest possible size of a minimal 3-homogeneous bitrade is 12; in any case the final column gives the smallest known example in the literature. When applying Theorem 4.10 we use Lemma 4.12 to verify that the Latin bitrade is thin and thus minimal. For arbitrary k (including even values), [6] gives the construction of minimal, k-homogeneous Latin bitrades of size $\lceil 1.75k^2 + 3 \rceil k$. (This paper also improves this bound for small values of k.) If k is prime then Theorem 4.4 improves this result.

Acknowledgements

The second author's work was supported by Australian Research Council Linkage International Award LX0453416 and institutional grant MSM0021620839.

References

[1] J.A. Bate, G.H.J. van Rees, Minimal and near-minimal critical sets in back circulant Latin squares, Australasian Journal of Combinatorics 27 (2003) 47–61.
[2] R. Bean, H. Bidkhori, M. Khosravi, E.S. Mahmoodian, k-homogeneous Latin trades, in: Proc. Conference on Algebraic Combinatorics and Applications, Designs and Codes, Thurnau, 2005, in: Bayreuther Mathemat. Schr., vol. 74, 2005, pp. 7–18.
[3] N.J. Cavenagh, A uniqueness result for 3-homogeneous Latin trades, Commentationes Mathematicae Universitatis Carolinae 47 (2006) 337–358.
[4] N.J. Cavenagh, D. Donovan, A. Drápal, 3-homogeneous Latin trades, Discrete Mathematics 300 (2005) 57–70.
[5] N.J. Cavenagh, D. Donovan, A. Drápal, 4-homogeneous Latin trades, Australasian Journal of Combinatorics 32 (2005) 285–303.
[6] N.J. Cavenagh, D. Donovan, E.Ş. Yazıcı, Minimal homogeneous Latin trades, Discrete Mathematics 306 (2006) 2047–2055.
[7] J. Cooper, D. Donovan, J. Seberry, Latin squares and critical sets of minimal size, Australasian Journal of Combinatorics 4 (1991) 113–120.
[8] C.J. Colbourn, J.H. Dinitz (Eds.), CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, Florida, 1996.
[9] A. Drápal, On geometrical structure and construction of Latin trades, Advances in Geometry (in press).
[10] A. Drápal, T. Kepka, Exchangeable Groupoids I, Acta Universitatis Carolinae - Mathematica et Physica 24 (1983) 57–72.

[11] H.-L. Fu, On the construction of certain type of Latin squares with prescribed intersections, Ph.D. Thesis, Auburn University, 1980.
[12] M.J. Hall, The Theory of Groups, Macmillan Company, New York, 1959.
[13] A.D. Keedwell, Critical sets in Latin squares and related matters: An update, Utilitas Mathematica 65 (2004) 97–131.
[14] G.B. Khosrovshahi, C.H. Maysoori, On the bases for trades, Linear Algebra and its Applications 226–228 (1995) 731–748.
[15] H. Wielandt, Finite Permutation Groups, Academic Press, London, 1964.
[16] J.D. Dixon, B. Mortimer, Permutation Groups, Springer, New York, 1996.
[17] A.P. Street, Trades and defining sets, in: C.J. Colbourn, J.H. Dinitz (Eds.), CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, Florida, 1996, pp. 474–478.
[18] I.M. Wanless, Cycle switches in Latin squares, Graphs and Combinatorics 20 (2004) 545–570.