Latin bitrades derived from groups

Nicholas J. Cavenagh
School of Mathematics
The University of New South Wales
NSW 2052 Australia

Aleš Drápal *
Department of Mathematics
Charles University
Sokolovská 83, 186 75 Praha 8
Czech Republic

Carlo Hämäläinen
Department of Mathematics
The University of Queensland
QLD 4072 Australia

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. Drápal ([8]) showed that a latin bitrade is equivalent to three derangements 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 from groups without specifying an independent group action. Properties of latin trades such as homogeneousness, minimality (via thinness) and orthogonality may also be encoded succinctly within the group structure. We apply the construction to a some well-known groups, constructing new classes of latin trades which are rich in symmetry. In particular, we show the existence of minimal, k-homogeneous

*This work was supported by Australian Research Council Linkage International Award LX0453416 and institutional grant MSM0021620839

latin trades for each odd $k \geq 3$. In some cases these are the smallest such known examples.

1 Introduction

One of the earliest studies of latin bitrades appeared in [9], 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],[12],[1]) and of the intersections between latin squares ([10]). As discussed in [17], 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 [16] and [13].

Drápal [8] showed the equivalence of a latin bitrade to 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 the result of Drápal 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 homogeneousness may be encoded concisely into the group structure, as shown in Section 3. Section 4 shows that many interesting 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 trades 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. The group theory notation used in this paper is consistent with most introductory texts, including [11].

2 Permutation Structure

In what follows let A_1, A_2 and A_3 be finite, pairwise-disjoint sets. A *partial quasigroup* is some $T^\circ \subset A_1 \times A_2 \times A_3$ such that the following conditions are all 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) 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.

We often represent T° as an array with rows indexed by A_1, columns indexed by A_2, and entry $a_3 \in A_3$ in cell (a_1, a_2) if and only if $(a_1, a_2, a_3) \in T^\circ$. The partial quasigroup operation here is $\circ$, so that $a_1 \circ a_2 = a_3$ if and only if $(a_1, a_2, a_3) \in T^\circ$.

Note that (P2) implies there are no "unused" elements of $A_1 \cup A_2 \cup A_3$. However if we relax (P2) and specify that $|A_1| = |A_2| = |A_3| = n$ for some integer n, then T° is precisely a *partial latin square*. In the literature it is sometimes specified that $A_1 = A_2 = A_3$. However, combinatorially, the difference between a partial latin square and a partial quasigroup is superficial. We simply request the reader to note the connection between the two, as latin bitrades are very commonly thought of in terms of latin squares. In this paper we choose the partial quasigroup definition for the sake of elegance in the following proofs.

Let $T^\circ, T^\star \subset A_1 \times A_2 \times A_3$ be two partial quasigroups. 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 $|T^\circ| = |T^\star|$.

An *isotopism* of a partial quasigroup allows any relabelling of the elements of A_1, A_2 and A_3. Combinatorial properties of partial quasigroups 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 2.1. *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:*

$T^\circ =$

$\circ$	c	d	e
a	f	g	h
b	g	h	f

$T^\star =$

$\star$	c	d	e
a	g	h	f
b	f	g	h

We may also write:

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

It turns out (as first shown by Drápal, [8]) that latin trades may be defined completely in terms of permutations. We first show how to derive permutations of T° from a given latin trade.

DEFINITION 2.2. *Define the map $\beta_r : T^\star \to T^\circ$ 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 $i \neq r$. (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 $\tau_1 = \beta_2\beta_3^{-1}$, $\tau_2 = \beta_3\beta_1^{-1}$ and $\tau_3 = \beta_1\beta_2^{-1}$. For each $i \in \{1, 2, 3\}$, let A_i be the set of cycles in τ_i.*

EXAMPLE 2.3. *Consider the latin trade constructed in Example* 2.1. *Here:*

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

LEMMA 2.4. *The permutations τ_1, τ_2 and τ_3 satisfy the following properties:*

(Q1) *If $\rho \in A_r$, $\mu \in A_s$, $1 \leq r < s \leq 3$, 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) $\tau_1\tau_2\tau_3 = 1$.

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 ρ and μ act on distinct points $x = (x_1, x_2, x_3)$, y and intersect both these points. 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. So $x_1 = x_1''$, $x_2' \neq x_2$, and $x_3' = x_3''$, contradicting (P1). The cases $(r, s) = (1, 3)$ and $(2, 3)$ are similar.

(Q2) Each $\tau_i = \beta_s\beta_r^{-1}$ changes the t–th component of a triple on which it acts, where $t \notin \{s, r\}$.

(Q3) Observe that $\tau_1\tau_2\tau_3 = \beta_2\beta_3^{-1}\beta_3\beta_1^{-1}\beta_1\beta_2^{-1} = 1$. □

Thus from a given latin trade we may define a set of permutations with particular properties. It turns out that this relationship between latin trades and permutations is an isomorphism, as the process of Lemma 2.4 is invertible.

DEFINITION 2.5. *Let τ_1, τ_2, τ_3 be permutations on some set of size X and for $i \in \{1, 2, 3\}$, let 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* 2.4. *Next, define*

$$S^\circ = \{(\rho_1, \rho_2, \rho_3) \mid \rho_i \in A_i \text{ and the } \rho_i \text{ all act on a common point point of } X\}$$

and

$$S^\star = \{(\rho_1, \rho_2, \rho_3) \mid \rho_i \in A_i,\ x, x', x'' \text{ are distinct points of } X \text{ such that } x\rho_1 = x', \\ x'\rho_2 = x'', x''\rho_3 = x\}.$$

THEOREM 2.6 (Drápal [8]). *Then the pair of partial latin squares* $(S^\circ, S^\star)$ *is a latin bitrade of size* $|X|$ *with* $|A_1|$ *rows,* $|A_2|$ *columns and* $|A_3|$ *entries.*

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

¿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 $\rho_1 \in A_1$, $\rho_2 \in A_2$ and $\rho_3 \in A_3$ 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 ρ_1 and ρ_2 intersect in two points (x and x'), contradicting (Q1). By symmetry, $S^\star$ is also a partial quasigroup.

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' is a common point to ρ_1 and ρ_2 and x'' is a common point to ρ_2 and ρ_3. But ρ_1, ρ_2 and ρ_3 intersect in a common point y and at least one of $y \neq x'$, $y \neq x''$ is true. Without loss of generality suppose that $y \neq x''$ is true. Then ρ_2 and ρ_3 contain two common points, 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 be the common point to ρ_1, ρ_2 and ρ_3. Thus 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 A_1 that does not fix x and ρ_2 is the only permutation in A_2 that does not fix y. It follows from the observation in the second paragraph of the proof that there is a unique $\rho_3' \in A_3$ 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 $x''\rho_3 = x$. Thus x' is a common point to ρ_1 and ρ_2. Let ρ_3' be the unique cycle of A_3 that does not fix x'. Then $(\rho_1, \rho_2, \rho_3') \in S^\circ$. By symmetry (R3) is satisfied. $\square$

EXAMPLE 2.7. *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* 2.1.

DEFINITION 2.8. *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 2.9. *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 since we have not specified the disjoint mate of T° it is possible that a non-minimal latin trade may not partition into smaller, disjoint latin trades. So in effect the minimal property implies the primary property, but not necessarily vice versa. Minimal latin trades are important in the study of *critical sets* (minimal defining sets) of latin squares (see [12] for a recent survey).

So a 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. However, can we construct a latin trade from a group without an independent group action being specified? The following theorem shows us how.

DEFINITION 2.10. *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:

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

THEOREM 2.11. *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 2.6 with $X = G$, there exists a latin trade $(S^\circ, S^\star)$ 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 2.5,

$T^\circ = \{(g_1A, g_2B, g_3C) \mid |g_1A \cap g_2B \cap g_3C| = 1\}$ and
$T^\star = \{(g_1A, g_2B, g_3C) \mid h \in g_1A, h' \in g_2B, h'' \in g_3C, ha = h', h'b = h'', h''c = h\}$.

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 2.10 is a latin bitrade with size $|G|$.

Finally we have the (G3) condition. We start by considering the 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. Also, there are $|A|$ elements in this row. To see why, 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 $hB = ga^ib^jB = ga^iB$ and columns of this form have already been accounted for. If $(gA, ga^iB, ga^iC) \in T^\circ$ then $(gA, ga^iB, ga^{i-1}C) \in T^\star$ so row gA in the bitrade is precisely:

$\circ$	ga^0B	ga^1B	$\cdots$	$ga^{\lvert A\rvert-1}B$
gA	ga^0C	ga^1C	$\cdots$	$ga^{\lvert A\rvert-1}C$

$\star$	ga^0B	ga^1B	$\cdots$	$ga^{\lvert A\rvert-1}B$
gA	$ga^{-1}C$	ga^0C	$\cdots$	$ga^{\lvert A\rvert-2}C$

To avoid a notation clash with the τ_i, define $\nu_1 = \beta_2\beta_3^{-1}$, $\nu_2 = \beta_3\beta_1^{-1}$ and $\nu_3 = \beta_1\beta_2^{-1}$ where the β_r send $T^\star$ to T°. Reading row gA of the bitrade above, we find that $\nu_1(gA, ga^iB, ga^iC) = (gA, ga^{i+1}B, ga^{i+1}C)$. It follows that ν_1, ν_2, and ν_3 have cycles of size $|A|$, $|B|$, and $|C|$, respectively. This implies that the bitrade has $|G : A|$ rows (each with $|A|$ entries), $|G : B|$ columns (each with $|B|$ entries) and $|G : C|$ entries (each occurring $|C|$ times).

Now, 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 bitrade $(W^\circ, W^\star)$ such that $W^\circ \subset T^\circ$ and $W^\star \subset T^\star$ (by assumption this sub-bitrade is not trivial). Suppose that column gB lies in $(W^\circ, W^\star)$ for some $g \in G$. 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

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

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 $(W^\circ, W^\star) = (T^\circ, T^\star)$. $\square$

COROLLARY 2.12. *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 trade, as latin trades 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 2.13. *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 2.1.

3 Orthogonality, minimality and homogeneousness

In this section we describe how certain properties of latin trades constructed as in Theorem 2.11 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, 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* 2.11 *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 $g^{-1}h \in aCa^{-1} = C^a$. 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. □

Is it possible to encode minimality via our group construction? We do this by encoding a "thin" property of latin trades, 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. □

In general, the minimality of latin trades 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* 2.11 *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 $i = g_1A$, $j = g_2B$ for some g, $h \in G$. Since $i \circ j$ must be defined it follows that g_1A and g_2B intersect. By Corollary 2.12 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 following lemma is straightforward.

LEMMA 3.7. *A latin bitrade $(T^\circ, T^\star)$ constructed from a group $G = \langle a,b,c \rangle$ as in Theorem* 2.11 *is k-homogeneous if and only if $|A| = |B| = |C| = k$.*

A 2-homogeneous latin trade is trivially the union of latin squares of order 2. A construction for 3-homogeneous latin trades is given in [4]; moreover in [3] it is shown that this construction gives every possible primary 3-homogeneous latin trade. The problem of determining the spectrum of sizes of k-homogeneous latin trades 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] and [6]; however it is even an open problem to determine the possible sizes of a minimal 4-homogeneous latin trade. The theorems in the following section yield previously unknown cases of minimal k-homogeneous latin trades.

4 Examples

In this section we give some examples of groups which can generate latin bitrades using Theorem 2.11. This amounts to specifying a group, three cyclic subgroups, and showing that each of the (G1), (G2), and (G3) conditions are met. Note that all latin bitrades constructed satisfy will be primary, so by Lemma 3.4 thinness will imply minimality for these examples.

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 trades. 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):

- $A \cap B = \{(0,0)\}$.
- If there exists $(0,x) \in A \cap C$ with $x \neq 0$ then there must exist an integer k such that $k(p-1) \equiv 0 \pmod p$ and $k(p-1) \equiv x \pmod p$. So $x \equiv 0 \pmod p$, a contradiction.
- There is no $(x,0) \in B \cap C$ with $x \neq 0$ by similar reasoning.

Lastly, $G = \langle a, b, c \rangle$ since a and b generate G and c can be written as $-(a+b)$, so (G3) is satisfied. □

The latin trade 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, [11] 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.

REMARK 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* 2.11*. 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 $c = \beta^{-1}\alpha^{-1}$. 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 $\langle c\rangle \leq Z(G)$. For the converse we will rule out the two cases that $Z(G)$ has order p^2 or p^3. If $Z(G)$ has order p^3 then $G = Z(G)$ but we know that G is not abelian.

So suppose that $Z(G)$ has order p^2. Then there must be a group element w in $Z(G)$ but $w \notin \langle c\rangle$. By Lemma 4.2 we can write $w = a^ib^jc^k$ for some i, j, k. Then $(a^ib^jc^k)c^{-k} \in Z(G)$ since $c \in Z(G)$, which means that $a^ib^j \in Z(G)$. By Lemma 4.5, $a^ib^j = b^ja^i$. However, using (2) we have $a^ib^j = b^ja^ic^{ij}$ so it must be that $p \mid ij$. If $p \mid i$ then $w = b^jc^k$ 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 Lemma 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 nontrivial 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

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

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 $r \neq 1$ 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* 2.11. *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 Equation 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 $k = -2$. But then $(ab)^{-2} = b^{-1}a^{-1}b^{-1}$ which implies that $a = 1$, a contradiction.

It remains to show that this latin trade is q-homogeneous. To see this, $\beta^q = (ab)^q = b^q a^{r(r^q-1)/(r-1)} = b^q = 1$ as $r^q \equiv 1 \pmod{p}$. Next, from Equation 10,

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

$\square$

LEMMA 4.11. *The latin bitrade constructed in Theorem* 4.10 *is orthogonal.*

Proof. Observe that $\alpha\gamma\alpha^{-1} = b(b^{-1}a^{-1}b^{-1})b = a^{-1}$ so the order of $\langle\gamma\rangle^\alpha$ is p. Recalling that γ has order q, it follows that $\langle\gamma\rangle \cap \langle\gamma\rangle^\alpha = 1$ so by Lemma 3.2 the latin bitrade is orthogonal. $\square$

LEMMA 4.12. *The latin bitrade constructed in Theorem* 4.10 *is thin if and only if there exists no solution to*

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

apart from $i \equiv j \equiv 0 \pmod{q}$ *and* $i \equiv j \equiv 1 \pmod{q}$.

Proof. Assume that the latin bitrade in question is not thin. Then there exists some solution to $\alpha^i\beta^j\gamma^k = 1$ such that $(i,j,k) \notin \{(0,0,0),(1,1,1)\}$, where i, j and k are each calculated modulo q. Thus:

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

So $i + j \equiv 2k \pmod{q}$ and therefore

$$\begin{aligned}
& & r(r^j-1)/(r-1) - r(r^{2k}-1)/(r^2-1) &\equiv 0 \pmod{p} \\
&\Rightarrow & r(r^j-1)(r+1) - r(r^{i+j}-1) &\equiv 0 \pmod{p} \\
&\Rightarrow & r^2\left(r^j + r^{j-1} - r^{i+j-1} - 1\right) &\equiv 0 \pmod{p}.
\end{aligned}$$

If $p \mid r$ then $1 \equiv r^q \equiv 0 \pmod{p}$, a contradiction. So $r^j + r^{j-1} \equiv r^{i+j-1} + 1 \pmod{p}$ as required. $\square$

An example of a non-thin latin trade 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 trade 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 trade being thin. In particular, it can be shown that if $q = 3$ or if $p = r^q - 1$, then the latin trade 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 a and b act on $m+1$ common points. 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 [14] and [15].

THEOREM 4.14 ([14], 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 by B. Marggraff in 1889.

THEOREM 4.15 ([15], 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 at least the points that ab shifts (call this set M). 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

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

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 $G \leq A3m + 1$. □

THEOREM 4.17. *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* 2.11*. 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) is 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 a does not move the point $3m+1$, 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. Suppose that there exist integers i, j and k such that $\alpha^i\beta^j\gamma^k = 1$. Then $a^ib^j = c^k$. Since $(1)c^k = 1$ we have $(1)a^ib^j = 1$. For this to hold it must be that $(1)a^i \in \{1, 2, \ldots, m+1\}$ since b does not act on the points $\{m+2, m+3, \ldots, 2m+1\}$. Hence $i \equiv j \pmod{2m+1}$.

Let x be a point in $X = \{1, 2, \ldots, m\}$. Since c^k does not act on any such x, we have $(x)a^ib^j = x$ for $x \in X$. Then it must be that $(x)a^i \in \{1, 2, \ldots, m+1\}$ otherwise b^j will be unable to act on $(x)a^i$ to return to x. In other words, the set $\{1, 2, \ldots, m\}$ has to be mapped into $\{1, 2, \ldots, m+1\}$. Thus $i \equiv j \equiv 0 \pmod{2m+1}$ or $i \equiv j \equiv 1 \pmod{2m+1}$. In the first case we find that $k \equiv 0 \pmod{2m+1}$. Otherwise, $ab = c^k = (ab)^k$ so $c^{k-1} = 1$ and $k \equiv 1 \pmod{2m+1}$, as required. □

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 $(2m+1)c^j a = 1$ 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. $\square$

EXAMPLE 4.20. *Letting $m = 1$, we construct a thin, orthogonal latin trade of size 12 as in this subsection. 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:*

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

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

$T^\circ =$

$\circ$	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

$T^\star =$

$\star$	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		$a^{-1}C$

As an aside, T° and $T^\star$ are completable to a pair of mutually orthogonal latin squares of order 4.

5 Minimal k-homogeneous latin trades

We conclude with a table of the sizes of smallest minimal k-homogeneous latin trades, 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 trade 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 trade is thin and thus minimal.

k	Thm 4.4	Thm 4.10	Thm 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	78	55
7	343	301 ($p = 43, q = 7, r = 4$)	1814400	133	133
9	N/A	N/A	3113510400	243	243
11	1331	979 ($p = 89, q = 11, r = 2$)	16!/2	407	407

Table of sizes of minimal k-homgoeneous latin trades

For arbitrary k (including even values), [6] gives the construction of minimal, k-homogeneous latin trades of size $1.75k^3 + 3$. If k is prime then Theorem 4.4 improves this result.

References

[1] J.A. Bate and 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 and E.S. Mahmoodian, k-homogeneous latin trades, Proc. Conference on Algebraic Combinatorics and Applications, Designs and Codes, Thurnau, 2005, Vol. 74, pp. 7–18, Bayreuther Mathemat. Schr., 2005.

[3] N.J. Cavenagh, A uniqueness result for 3-homogeneous latin trades, Commentationes Mathematicae Universitatis Carolinae, to appear.

[4] N.J. Cavenagh, D. Donovan and A. Drápal, 3-homogeneous latin trades, Discrete Mathematics, 300 (2005), 57–70.

[5] N.J. Cavenagh, D. Donovan and A. Drápal, 4-homogeneous latin trades, Australasian Journal of Combinatorics, 32 (2005), 285–303.

[6] N.J. Cavenagh, D. Donovan and E.Ş. Yazıcı, Minimal homogeneous latin trades, Discrete Mathematics, to appear.

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

[8] A. Drápal, Geometry of latin trades, manuscript circulated at the conference Loops ‘03, Prague 2003.

[9] A. Drápal and T. Kepka, Exchangeable Groupoids I, Acta Universitatis Carolinae - Mathematica et Physica, 24 (1983), 57–72.

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

[11] M.J. Hall, The theory of groups, New York, Macmillan Company, 1959.

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

[13] G.B. Khosrovshahi and C.H. Maysoori, On the bases for trades, Linear Algebra and its Applications, 226-228 (1995), 731–748.

[14] H. Wielandt, Finite Permutation Groups, Academic Press, London, 1964.

[15] J.D. Dixon and B. Mortimer, Permutation Groups, Springer, New York, 1996.

[16] A.P. Street, Trades and defining sets, in: C.J. Colbourn and J.H. Dinitz, ed., CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, Florida, 1996, 474–478.

[17] I.M. Wanless, Cycle switches in latin squares, Graphs and Combinatorics, 20 (2004), 545 – 570.