Journal of Algebraic Combinatorics (2025) 62:30
https://doi.org/10.1007/s10801-025-01460-0

Latin bitrades derived from quasigroup autoparatopisms

Nicholas J. Cavenagh[1] · **Raúl M. Falcón**[2]

Received: 26 August 2023 / Accepted: 28 July 2025 / Published online: 4 September 2025

Abstract
In 2008, Cavenagh, Drápal and Hämäläinen described a method of constructing Latin trades using groups. The Latin trades that arise from this construction are entry-transitive (that is, there always exists an autoparatopism of the Latin trade mapping any ordered triple to any other ordered triple). Moreover, useful properties of the Latin trade can be established using properties of the group. However, the construction does not give a direct embedding of the Latin trade into any particular Latin square. In this paper , we propose a similar approach to the above to construct Latin trades embedded in a Latin square L, via the autoparatopism group of the quasigroup with Cayley table L. We apply this theory to identify non-trivial entry-transitive trades in some group operation tables as well as in Latin squares that arise from quadratic orthomorphisms.

Keywords Latin square · Quasigroup · Latin trade · Autoparatopism group · Automorphism group

Mathematics Subject Classification 05B15 · 05B30

1 Introduction

A *partial Latin square* of order n is an $n \times n$ partial array $P = (P[i, j])$, where each cell is either empty or contains an element from a finite set Q of n distinct symbols, so that each symbol appears at most once per row, and at most once per column. The number of non-empty cells in P is its *size*, which we denote by $|P|$. If $|P| = n^2$, then the array is a *Latin square* of order n. Furthermore, the partial Latin square P is uniquely identified

Nicholas J. Cavenagh and Raúl M. Falcón have contributed equally to this work.

✉ Raúl M. Falcón
rafalgan@us.es

Nicholas J. Cavenagh
nickc@waikato.ac.nz

[1] Department of Mathematics, The University of Waikato, Private Bag 3105, 3240 Hamilton, New Zealand

[2] Department of Applied Mathematics I, Universidad de Sevilla, Avenida Reina Mercedes 4 A, 41012 Sevilla, Spain

with its *set of entries* $\mathrm{Ent}(P) := \{(i, j, P[i, j]) \mid i, j, P[i, j] \in Q\}$. Observe that any two distinct entries of a partial Latin square agree in at most one coordinate. If $\mathrm{Ent}(P') \subseteq \mathrm{Ent}(P)$, for some other partial Latin square P' of the same order, then it is said that P' is *embedded* in P. This is denoted by $P' \subseteq P$.

A *Latin trade* in a Latin square L is any non-empty partial Latin square $T \subseteq L$ such that there is another partial Latin square T' of the same order satisfying the following three conditions: (1) $|T| = |T'|$; (2) $\mathrm{Ent}(T) \cap \mathrm{Ent}(T') = \emptyset$; and (3) the set $(\mathrm{Ent}(L) \backslash \mathrm{Ent}(T)) \cup \mathrm{Ent}(T')$ is the set of entries of a new Latin square. Not every Latin trade is embedded in a Latin square of the same order, but this can always be done for some higher order. (In particular, every partial Latin square of order n is embedded in a Latin square of order $m \geq 2n$ (see [16]).) Further, Condition (3) above is equivalent to the following: (3*) corresponding rows and columns of T and T' contain the same set of symbols. Conditions (1), (2) and (3*) above allow the definition of a Latin trade as a partial Latin square that is not embedded in any particular Latin square.

The partial Latin square T' is said to be a *disjoint mate* of T, and the pair (T, T') is called a *Latin bitrade* of size $|T|$. It is said to be *primary* if, whenever (U, U') is also a Latin bitrade such that $U \subseteq T$ and $U' \subseteq T'$, then $U = T$ and $U' = T'$. Furthermore, the Latin trade T is said to be *minimal* if, whenever (U, U') is a Latin bitrade such that $U \subseteq T$, then $U = T$. Finally, the Latin bitrade (T, T') is said to be *orthogonal* if, whenever $T[i, j] = T[i', j']$, with $i \neq i'$ and $j \neq j'$, then $T'[i, j] \neq T'[i', j']$.

Observe that if L and L' are distinct Latin squares of the same order, then $\mathrm{Ent}(L) \setminus \mathrm{Ent}(L')$ is a Latin trade with disjoint mate given by $\mathrm{Ent}(L') \backslash \mathrm{Ent}(L)$. Thus the study of Latin trades in Latin squares is close to the study of the difference between Latin squares, sometimes known as the *Hamming distance* ([8, 11]). In particular, the minimum Hamming distance between group operation tables and other Latin squares has been a much studied topic [3, 10, 12, 13, 19]. Other applications of Latin trades include defining sets and randomization; see [4] for a survey.

The Latin trade T is said to be *k-homogeneous* if the set $\mathrm{Ent}(T)$ intersects each row, each column and each symbol in L either zero or k times. It is known [5] that there exist 3-homogeneous Latin trades embedded in the Cayley table of the elementary abelian 2-group $(\mathbb{Z}_2)^{2n}$, for all $n > 1$. Particular constructions of 3- and 4-homogeneous Latin trades are described in [6, 7], while the existence of k-homogeneous Latin trades of certain sizes has been dealt with in [1, 2].

In 2008, Cavenagh et al. [9] described a method to construct Latin bitrades via certain finite groups. These Latin bitrades satisfy (1), (2) and (3*) above and are not embedded in any particular Latin square. More specifically, rows, columns and entries are labeled as co-sets of subgroups of the group under consideration. The Latin bitrades constructed in the following result are also *entry-transitive*. (We define entry-transitive in the next section.)

Theorem 1.1 ([9, Theorem 2.14 and Lemma 3.2]) *Let G be a finite group with unit element 1 and three elements $a, b, c \in G \setminus \{1\}$ such that*

(G1) $abc = 1$, *and*
(G2) $|\langle a \rangle \cap \langle b \rangle| = |\langle a \rangle \cap \langle c \rangle| = |\langle b \rangle \cap \langle c \rangle| = 1$.

Let $A = \langle a \rangle$, $B = \langle b \rangle$ and $C = \langle c \rangle$. Then, the pair of partial Latin squares (T°, T^*), with respective set of entries

$$\mathrm{Ent}(T^\circ) := \{(gA, gB, gC) \mid g \in G\} \quad \text{and}$$
$$\mathrm{Ent}(T^*) := \{(gA, gB, ga^{-1}C) \mid g \in G\},$$

is a Latin bitrade of size $|G|$, with $|G : A|$ rows (each with $|A|$ entries), $|G : B|$ columns (each with $|B|$ entries), and $|G : C|$ entries (each occurring $|C|$ times). It is primary whenever $G = \langle a, b, c \rangle$. It is orthogonal whenever $|C \cap aCa^{-1}| = 1$.

In this paper, we propose a new method to construct Latin bitrades embedded in a given Latin square L, via subgroups of the autoparatopism group of L. This follows an approach similar to the construction described in Theorem 1.1, to which our proposal is identified under certain conditions. This new method is described in Sect. 3, where we also characterize the fundamental aspects of the Latin bitrades so constructed, as its size, homogeneity or orthogonality, among others. We finish that section with some examples illustrating all these results. A pair of more comprehensive examples based on the use of Mersenne primes, and on quadratic orthomorphisms over finite fields, are described in Sect. 4.2.

2 Preliminaries

In this section, we describe some basic concepts, notations and results on partial Latin squares that are used throughout the paper. See [18] for more details on this topic, and [4] for a survey on Latin bitrades.

Every Latin square of order n constitutes the Cayley table of a *quasigroup* of the same order. That is, a pair $Q_* := (Q, *)$ formed by a finite set Q of n elements that is endowed with a binary operation $*$, so that both equations $i * x = j$ and $y * i = j$ have unique solution $x, y \in Q$, for all $i, j \in Q$. Equivalently, the set Q is endowed with right- and left-division. If the operation $*$ is associative, then the quasigroup is indeed a group. From here on, whenever there is no confusion, we denote by Q the quasigroup Q_*, and we denote by ij the product $i * j$, for all $i, j \in Q$. In addition, we denote by $L(Q_*)$ (by $L(Q)$, if there is no confusion) the Latin square describing the Cayley table of the quasigroup Q_*.

Let S_3 and S_Q denote the respective symmetric groups on the sets of symbols $\{1, 2, 3\}$ and Q. The quasigroup Q_* is *paratopic* to a quasigroup $Q_\circ := (Q, \circ)$ if there exist a permutation $\pi \in S_3$ and a triple $f := (f_1, f_2, f_3) \in S_Q \times S_Q \times S_Q$ such that,

$$f_{\pi(1)}(e_{\pi(1)}) \circ f_{\pi(2)}(e_{\pi(2)}) = f_{\pi(3)}(e_{\pi(3)}),$$

for every entry $e := (e_1, e_2, e_3) \in \mathrm{Ent}(L(Q_*))$. The pair $(\pi; f)$ is a *paratopism* from Q_* to $Q_\circ$. It acts on the set $\mathrm{Ent}(L(Q_*))$ in the following way.

- First, we apply the isotopism f by permuting the rows of $L(Q_*)$ according to the bijection f_1, its columns according to f_2, and its symbols according to f_3, giving rise to an intermediate Latin square of set of entries $\{f(e) := (f_1(e_1),\ f_2(e_2),\ f_3(e_3)) \mid e \in \mathrm{Ent}(L(Q_*))\}$.
- Then, we permute the coordinates of each entry in this intermediate Latin square according to the permutation π, so that we get the set of entries

$$\mathrm{Ent}(L(Q_\circ)) = \left\{(\pi; f)(e) := f^{\pi^{-1}}\left(e_{\pi(1)},\ e_{\pi(2)},\ e_{\pi(3)}\right) \mid e \in \mathrm{Ent}(L(Q_*))\right\}, \tag{1}$$

where for each permutation $\rho \in S_3$, we denote from here on

$$f^\rho := \left(f_{\rho^{-1}(1)}, f_{\rho^{-1}(2)}, f_{\rho^{-1}(3)}\right).$$

That is,

$$\mathrm{Ent}(L(Q_\circ)) = \left\{\left(f_{\pi(1)}(e_{\pi(1)}),\ f_{\pi(2)}(e_{\pi(2)}),\ f_{\pi(3)}(e_{\pi(3)})\right) \mid e \in \mathrm{Ent}(L(Q_*))\right\}.$$

In particular,

$$(f^\pi)^\rho = f^{\rho\pi}. \tag{2}$$

Note that the composition from the right to the left of two paratopisms is again a paratopism. More specifically, if $(\rho; g)$ is a paratopism from the quasigroup $Q_\circ$ to a third quasigroup $Q_\diamond := (Q, \diamond)$, then, for each entry $e \in \mathrm{Ent}(L(Q_*))$, we have from (1) and (2)

$$\begin{aligned}((\rho; g)(\pi; f))(e) &= (\rho; g)\left(f_{\pi(1)}(e_{\pi(1)}),\ f_{\pi(2)}(e_{\pi(2)}),\ f_{\pi(3)}(e_{\pi(3)})\right)\\ &= g^{\rho^{-1}} f^{(\pi\rho)^{-1}}\left(e_{\pi(\rho(1))},\ e_{\pi(\rho(2))}, e_{\pi(\rho(3))}\right)\\ &= g^{(\pi\rho)^{-1}\pi} f^{(\pi\rho)^{-1}}\left(e_{\pi(\rho(1))},\ e_{\pi(\rho(2))}, e_{\pi(\rho(3))}\right)\\ &= \left(\pi\rho; g^\pi f\right)(e).\end{aligned}$$

That is,

$$(\rho; g)(\pi; f) := \left(\pi\rho; g^\pi f\right). \tag{3}$$

This conforms with the standard law for a semidirect product $S_3^{\mathrm{op}} \ltimes (S_Q \times S_Q \times S_Q)$, where op refers to the opposite group. We illustrate all the previous notions by focusing on quasigroups with entries in $\mathbb{Z}_4$.

Example 2.1 Let $\mathbb{Z}_{4*}$, $\mathbb{Z}_{4\circ}$ and $\mathbb{Z}_{4\diamond}$ be three quasigroups of respective Cayley tables

$$L(\mathbb{Z}_{4*}) \equiv \begin{array}{|c|c|c|c|}\hline 1&3&0&2\\\hline 0&2&1&3\\\hline 2&0&3&1\\\hline 3&1&2&0\\\hline\end{array}, \qquad L(\mathbb{Z}_{4\circ}) \equiv \begin{array}{|c|c|c|c|}\hline 0&1&2&3\\\hline 3&2&1&0\\\hline 2&3&0&1\\\hline 1&0&3&2\\\hline\end{array} \quad \text{and} \quad L(\mathbb{Z}_{4\diamond}) \equiv \begin{array}{|c|c|c|c|}\hline 2&3&0&1\\\hline 3&2&1&0\\\hline 1&0&3&2\\\hline 0&1&2&3\\\hline\end{array}.$$

It can readily be checked that the pairs

$$\Theta = ((123);\ ((01), (123), \mathrm{Id})) \qquad \text{and} \qquad \Theta' = ((23);\ ((0132), (12), (03)))$$

are respective paratopisms from $\mathbb{Z}_{4*}$ to $\mathbb{Z}_{4\circ}$, and from $\mathbb{Z}_{4\circ}$ to $\mathbb{Z}_{4\diamond}$. Then, we have from (3) that

$$\Theta'\Theta = ((12);\ ((013), (01), (12)))$$

is a paratopism from $\mathbb{Z}_{4*}$ to $\mathbb{Z}_{4\diamond}$. ◁

In what follows, let $\Theta = (\pi;\ f)$ be a paratopism from Q_* to $Q_\circ$. If $f = \mathrm{Id}_Q$ has the trivial permutation on Q as its three components, then Θ is said to be a *parastrophism* from Q_* to its *parastrophe* $Q_\circ$. In particular, we have from (3)

$$(\rho;\ \mathrm{Id}_Q)(\pi;\ \mathrm{Id}_Q) = (\pi\rho;\ \mathrm{Id}_Q).$$

In many papers the term "conjugate" is used for parastrophe. However, since group theory conjugates are used in this paper, we adhere to the term parastrophe to avoid confusion. If this is the case, the entries of $L(Q_\circ)$ coincide with those ones of $L(Q_*)$ after interchanging the role of rows, columns and symbols according to the permutation $\pi \in S_3$. The quasigroup Q_* is *totally symmetric* if it is identical to each of its six parastrophes.

The paratopism $(\pi;\ f)$ is an *isotopism* if π is the trivial permutation Id in the symmetric group S_3, in which case, the quasigroups Q_* and $Q_\circ$ are said to be *isotopic*, and the pair $(\mathrm{Id};\ f)$ is denoted only by f. In particular, we have from (3)

$$(\mathrm{Id};\ g)(\mathrm{Id};\ f) = (\mathrm{Id};\ gf).$$

The isotopism $(\mathrm{Id};\ f)$ is an *isomorphism* if $f_1 = f_2 = f_3$. If this is the case, then, by abuse of notation, we identify f with its three components.

The paratopism $(\pi;\ f)$ constitutes therefore the composition of a parastrophism and an isotopism. More specifically, we have from (3)

$$(\pi;\ \mathrm{Id}_Q)(\mathrm{Id};\ f) = (\pi;\ f) \qquad \text{and} \qquad (\pi^{-1};\ \mathrm{Id}_Q)(\mathrm{Id};\ f)(\pi;\ \mathrm{Id}_Q) = (\mathrm{Id};\ f^\pi).$$

Furthermore, if $Q_* = Q_\circ$, then the paratopism (respectively, the isotopism or the isomorphism) is an *autoparatopism* (respectively, an *autotopism* or an *automorphism*). We denote by $\mathrm{Apar}(Q_*)$ (respectively, $\mathrm{Atop}(Q_*)$ and $\mathrm{Aut}(Q_*)$) the set of autoparatopisms (respectively, the sets of autotopisms and automorphisms) of the quasigroup Q_*. (We remove the index $*$ if there is no confusion.) The three sets have group structure. More specifically, the set of autoparatopisms is a subgroup of the semidirect product $S_3^{\mathrm{op}} \ltimes (S_Q \times S_Q \times S_Q)$ with the composition described in (3). In particular, the inverse of a paratopism $(\pi;\ f)$ is

$$(\pi;\ f)^{-1} := \left(\pi^{-1};\ \left(f^{-1}\right)^{\pi^{-1}}\right). \tag{4}$$

Both the set of autotopisms and the set of automorphisms of a quasigroup Q have group structure with the component-wise composition of permutations. These groups are, respectively, called the *autoparatopism group*, the *autotopism group* and the *automorphism group* of the quasigroup Q. In particular, $\mathrm{Aut}(Q) \leq \mathrm{Atop}(Q) \trianglelefteq \mathrm{Apar}(Q)$ (see [17, Lemma 1]). This paper focuses on the subgroup

$$\mathrm{Apar}_{(12)}(Q) := \mathrm{Atop}(Q) \cup \{(f; (12)) \in \mathrm{Apar}(Q)\} \leq \mathrm{Apar}(Q).$$

(In a similar way, one can also define the subgroups $\mathrm{Apar}_{(13)}(Q)$ and $\mathrm{Apar}_{(23)}(Q)$, for which analogous results to those ones described in the subsequent sections arise trivially by parastrophism.) The *stabilizer* of an entry $e \in \mathrm{Ent}(L(Q))$ with respect to a subgroup $G \leq \mathrm{Apar}_{(12)}(Q)$ is the subgroup

$$G_e := \{(\pi; f) \in G \mid (\pi; f)(e) = e\} = G_e^{\mathrm{row}} \cap G_e^{\mathrm{col}} \cap G_e^{\mathrm{sym}} \leq G,$$

where

$$\begin{aligned} G_e^{\mathrm{row}} &:= \{(\pi; f) \in G \mid f_{\pi(1)}(e_{\pi(1)}) = e_1\}, \\ G_e^{\mathrm{col}} &:= \{(\pi; f) \in G \mid f_{\pi(2)}(e_{\pi(2)}) = e_2\}, \\ G_e^{\mathrm{sym}} &:= \{(\pi; f) \in G \mid f_{\pi(3)}(e_{\pi(3)}) = e_3\}. \end{aligned}$$

By abuse of notation, we also define the stabilizer of an element $i \in Q$ with respect to a subgroup $G \leq \mathrm{Aut}(Q)$ as the subgroup

$$G_i := \{f \in G \mid f(i) = i\} \leq G.$$

Based on (1), all the previous concepts and notations are naturally translated to partial Latin squares. Furthermore, we say that two Latin bitrades (T_1, T_1') and (T_2, T_2') are paratopic if there exists a paratopism mapping both T_1 to T_2 and T_1' to T_2'. In this sense, we say that a partial Latin square P is *entry-transitive* if the group $\mathrm{Apar}(P)$ acts transitively on $\mathrm{Ent}(P)$.

3 The constructive method

Let Q be a quasigroup. Based on an approach similar to the construction described in Theorem 1.1, we describe in this section a new method to construct Latin bitrades via a subgroup of the autoparatopism group $\mathrm{Apar}(Q)$. The following lemma is useful to this end. (Remind here, and in the subsequent results, the respective notations $e = (e_1, e_2, e_3)$ and $f = (f_1, f_2, f_3)$ for each entry e and each isotopism f associated to any partial Latin square.)

Lemma 3.1 *Let $G \leq \mathrm{Apar}(Q)$ and $e \in \mathrm{Ent}(L(Q))$. For each autotopism $(\pi; f) \in G$, there is a bijection between*

1. *G_e^{row} and the set $S_1 := \left\{(\rho; g) \in G \mid g_{\rho\pi^{-1}(1)}(e_{\rho\pi^{-1}(1)}) = f_1(e_1)\right\}$.*

2. G_e^{col} *and the set* $S_2 := \left\{(\rho; g) \in G \mid g_{\rho\pi^{-1}(2)}(e_{\rho\pi^{-1}(2)}) = f_2(e_2)\right\}$.

Proof We prove the first statement. (The second one follows similarly.) To this end, we define the map

$$\begin{array}{rccc} \phi: & S_1 & \to & G_e^{\mathrm{row}} \\ & (\rho; g) & \mapsto & (\pi; f)^{-1}(\rho; g). \end{array}$$

We first show that ϕ is well-defined. To see this, note from (3), (4) and (2) that

$$\begin{aligned} (\pi; f)^{-1}(\rho; g) &= \left(\pi^{-1}; \left(f^{-1}\right)^{\pi^{-1}}\right)(\rho; g) \\ &= \left(\rho\pi^{-1}; \left(f^{-1}\right)^{\rho\pi^{-1}} g\right). \end{aligned}$$

Since $(\rho; g) \in S_1$, we have

$$\begin{aligned} \left(\left(f^{-1}\right)^{\rho\pi^{-1}} g\right)_{\rho\pi^{-1}(1)} \left(e_{\rho\pi^{-1}(1)}\right) &= \left(f^{-1}\right)_{\rho\pi^{-1}(1)}^{(\pi\rho^{-1})^{-1}} \left(g_{\rho\pi^{-1}(1)}\left(e_{\rho\pi^{-1}(1)}\right)\right) \\ &= f_1^{-1}(f_1(e_1)) \\ &= e_1. \end{aligned}$$

Thus, $\phi((\rho; g)) \in G_e^{\mathrm{row}}$ and hence, the map ϕ is well-defined. It is one-to-one because of the group structure of $\mathrm{Apar}(Q)$. In order to prove that it is also onto, for each autoparatopism $(\sigma; h) \in G_e^{\mathrm{row}}$, we consider the autoparatopism

$$(\sigma\pi; f^{\sigma} h) = (\pi; f)(\sigma; h) \in G.$$

It belongs to S_1 because

$$\begin{aligned} \left(f^{\sigma} h\right)_{(\sigma\pi)\pi^{-1}(1)} \left(e_{(\sigma\pi)\pi^{-1}(1)}\right) &= \left(f^{\sigma} h\right)_{\sigma(1)} \left(e_{\sigma(1)}\right) \\ &= f_{\sigma(1)}^{\sigma} \left(h_{\sigma(1)}\left(e_{\sigma(1)}\right)\right) \\ &= f_1(e_1). \end{aligned}$$

Then,

$$\phi\left((\sigma\pi; f^{\sigma} h)\right) = (\pi; f)^{-1}(\sigma\pi; f^{\sigma} h) = (\pi; f)^{-1}\left((\pi; f)(\sigma; h)\right) = (\sigma; h).$$

□

The following result describes the main constructive method to be studied in this paper.

Theorem 3.2 *Let* $G \leq \mathrm{Apar}_{(12)}(Q)$ *and* $\tau := (e, \Theta, \overline{\Theta}) \in \mathrm{Ent}(L(Q)) \times G \times G$ *be such that*

(C1) $\Theta \in G_e^{\text{row}} \setminus G_e^{\text{col}}$;
(C2) $\overline{\Theta} \in G_e^{\text{col}}$; *and*
(C3) $\overline{\Theta}^{-1}\Theta \in G_e^{\text{sym}}$.

If $\Theta := (\pi; f)$, *then the pair of partial Latin squares* $(T_{\tau,G}, T'_{\tau,G})$, *with respective set of entries*

$$\text{Ent}(T_{\tau,G}) := \left\{\Theta'(e) \mid \Theta' \in G\right\}$$

and

$$\text{Ent}(T'_{\tau,G}) := \left\{\Theta'\left((e_1, e_2, f_3(e_3))\right) \mid \Theta' \in G\right\}$$

is a Latin bitrade of size $|G|/|G_e|$.

Proof Since $G \leq \text{Apar}_{(12)}(Q)$, both partial Latin squares $T_{\tau,G}$ and $T'_{\tau,G}$ occupy the same cells. Further, the set $\text{Ent}(T_{\tau,G})$ constitutes the orbit of the cell (e_1, e_2) under the action of the subgroup $G \leq \text{Apar}_{(12)}(Q)$ on the set of cells of the Latin square $L(Q)$. Thus, $T_{\tau,G} \subseteq L(Q)$, and we have from the orbit-stabilizer and Lagrange's theorems, that $|T_{\tau,G}| = |G|/|G_e|$.

Next, we prove that $\text{Ent}(T_{\tau,G}) \cap \text{Ent}(T'_{\tau,G}) = \emptyset$. Otherwise, there are two autoparatopisms $\Theta_1, \Theta_2 \in G$ such that $\Theta_1(e) = \Theta_2((e_1, e_2, f_3(e_3))) \in \text{Ent}(L(Q))$. Then, we have that $(e_1, e_2, f_3(e_3)) \in \text{Ent}(L(Q))$. Since $e \in \text{Ent}(L(Q))$ and any two distinct entries in a Latin square agree in at most one coordinate, it must be $f_3(e_3) = e_3$. But (C1) implies that $f_3(e_3) = f_{\pi(1)}(e_{\pi(1)})f_{\pi(2)}(e_{\pi(2)}) = e_1 f_{\pi(2)}(e_{\pi(2)}) \neq e_1 e_2 = e_3$, which is a contradiction. Thus, $\text{Ent}(T_{\tau,G}) \cap \text{Ent}(T'_{\tau,G}) = \emptyset$.

Now, we show that each non-empty row of $T_{\tau,G}$ and $T'_{\tau,G}$ contains the same set of symbols. From the first statement of Lemma 3.1, it suffices to show this for row e_1. To this end, since $\Theta \in G_e^{\text{row}}$, note that

$$G_e^{\text{row}} = \left\{\Theta'\Theta \mid \Theta' \in G_e^{\text{row}}\right\}.$$

Then, from (3), row e_1 of $T_{\tau,G}$ contains the set of symbols

$$\left\{g_3\left(e_3\right) \mid (\rho; g) \in G_e^{\text{row}}\right\} = \left\{g_3 f_3(e_3) \mid (\rho; g) \in G_e^{\text{row}}\right\},$$

which is the set of symbols in row e_1 of $T'_{\tau,G}$.

Finally, we show that each non-empty column of $T_{\tau,G}$ and $T'_{\tau,G}$ contains the same set of symbols. From the second statement of Lemma 3.1, it suffices to show this for column e_2. To this end, suppose that $\overline{\Theta} := \left(\overline{f}; \overline{\pi}\right)$. From (C2), we have that

$$G_e^{\text{col}} = \left\{\Theta'\overline{\Theta} \mid \Theta' \in G_e^{\text{col}}\right\}.$$

In addition, we have from (C3) that $\left(\Theta'\overline{\Theta}\right)^{-1}\left(\Theta'\Theta\right) \in G_e^{\text{sym}}$, for all $\Theta' \in G$. From (3), this is equivalent to the fact that $g_3 f_3\left(e_3\right) = g_3 \overline{f}_3\left(e_3\right)$, for all $(g; \rho) \in G$. Hence,

column e_2 of $T_{\tau,G}$ contains the set of symbols

$$\left\{g_3\,(e_3) \mid (g;\rho) \in G_e^{\mathrm{col}}\right\} = \left\{g_3\overline{f}_3(e_3) \mid (\rho;g) \in G_e^{\mathrm{col}}\right\} = \left\{g_3 f_3(e_3) \mid (\rho;g) \in G_e^{\mathrm{col}}\right\}$$

which is the set of symbols in column e_2 of $T'_{\tau,G}$. □

Example 3.3 Let Q be the quasigroup of Cayley table

$$L(Q) \equiv \begin{array}{|c|c|c|c|}\hline 0&2&3&1\\\hline 1&3&2&0\\\hline 3&1&0&2\\\hline 2&0&1&3\\\hline\end{array}.$$

Its autotopism group is generated by

$$((0123),\ (13),\ (0132)) \qquad \text{and} \qquad ((23),\ (0132),\ (0213))\,.$$

Together with the autoparatopism

$$\Theta := ((12);\ ((0132),\ (23),\ (023)))\,,$$

they generate the group $\mathrm{Apar}_{(12)}(Q)$. In particular, $|\mathrm{Atop}(Q)| = 96$ and $|\mathrm{Apar}_{(12)}(Q)| = 192$. Let us consider the entry $e := (0,0,0) \in \mathrm{Ent}(L(Q))$ and the subgroup $G \leq \mathrm{Apar}_{(12)}(Q)$ of size 16 that is generated by Θ and the following autoparatopism of Q.

$$\overline{\Theta} = ((12);\ ((12),\ (0312),\ (023)))$$

We have from (3) and (4) that

$$\overline{\Theta}^{-1} = ((12);\ ((0213),\ (12),\ (032))) \qquad \text{and}$$
$$\overline{\Theta}^{-1}\Theta = (\mathrm{Id};\ ((02)(13),\ (02)(13),\ \mathrm{Id}))\,.$$

Then, it is readily verified that Conditions (C1)–(C3) in Theorem 3.2 hold and hence, the pair of partial Latin squares $(T_{\tau,G}, T'_{\tau,G})$, with $\tau := (e, \Theta, \overline{\Theta})$ constitute a Latin bitrade. Its entries are highlighted in bold type within $L(Q)$ as follows, with entries in $T'_{\tau,G}$ shown as subscripts. (It is the way in which we represent Latin bitrades throughout the paper.)

$\mathbf{0_2}$	$\mathbf{2_3}$	$\mathbf{3_0}$	1
1	$\mathbf{3_0}$	$\mathbf{2_3}$	$\mathbf{0_2}$
$\mathbf{3_0}$	1	$\mathbf{0_2}$	$\mathbf{2_3}$
$\mathbf{2_3}$	$\mathbf{0_2}$	1	$\mathbf{3_0}$

◁

In what follows, we characterize some fundamental aspects of the Latin bitrade described in Theorem 3.2. First, we establish the number of entries in the Latin trade $T_{\tau,G}$.

Lemma 3.4 *The Latin trade $T_{\tau,G}$ satisfies the following statements.*

1. *Each non-empty row has $|G_e^{\text{row}}|/|G_e|$ entries.*
2. *Each non-empty column has $|G_e^{\text{col}}|/|G_e|$ entries.*
3. *Each entry appears $|G_e^{\text{sym}}|/|G_e|$ times.*

Hence, the Latin trade $T_{\tau,G}$ is k-homogeneous, if and only if $|G_e^{\text{row}}| = |G_e^{\text{col}}| = |G_e^{\text{sym}}| = k \cdot |G_e|$.

Proof We prove the first statement. (The remaining ones hold by parastrophism, while the consequence holds readily from the three statements.) From Lemma 3.1, it is enough to determine the number of entries in the row e_1. Note to this end that the set of entries in the row e_1 in $T_{\tau,G}$ is the orbit of the entry e under the action of the subgroup of autoparatopisms in G preserving the row e_1, which contains in turn the set G_e. From the orbit-stabilizer and Lagrange's theorems, we have that the row e_1 in $T_{\tau,G}$ contains $|G_e^{\text{row}}|/|G_e|$ entries. □

Now, we characterize the orthogonality of our Latin bitrade.

Lemma 3.5 *The Latin bitrade $(T_{\tau,G}, T'_{\tau,G})$ is orthogonal if and only if*

$$G_e^{\text{sym}} \cap G^{\text{sym}}_{((e_1,e_2,f_3(e_3)))} \subseteq G_e. \tag{5}$$

Proof First suppose that (5) is true. Let $(\rho; g)$ and $\left(\rho'; g'\right)$ be two autoparatopisms in G such that $g_{\rho(i)}\left(e_{\rho(i)}\right) \neq g'_{\rho'(i)}\left(e_{\rho'(i)}\right)$, for $i \in \{1, 2\}$, and $g_3(e_3) = g'_3(e_3)$. Then,

$$\left(\rho'; g'\right)^{-1}(\rho; g) \in G_e^{\text{sym}} \setminus G_e.$$

From (5), this composition does not belong to $G^{\text{sym}}_{((e_1,e_2,f_3(e_3)))}$. Hence, $g_3 f_3(e_3) \neq g'_3 f_3(e_3)$. Thus, the Latin bitrade $(T_{\tau,G}, T'_{\tau,G})$ is orthogonal.

Conversely, suppose the existence of an autoparatopism

$$(\rho; g) \in \left(G_e^{\text{sym}} \cap G^{\text{sym}}_{((e_1,e_2,f_3(e_3)))}\right) \setminus G_e.$$

Since $(\rho; g) \in G_e^{\text{sym}}$, we have that $g_3(e_3) = e_3$. As a consequence, since $(\rho; g) \notin G_e$ and every two distinct entries in a Latin trade agree in at most one coordinate, it must be that $g_{\rho(1)}(e_{\rho(1)}) \neq e_1$ and $g_{\rho(2)}(e_{\rho(2)}) \neq e_2$. Further, since $(\rho; g) \in G^{\text{sym}}_{((e_1,e_2,f_3(e_3)))}$, we have that $g_3 f_3(e_3) = f_3(e_3)$. In summary, (e_1, e_2, e_3) and $(g_{\rho(1)}(e_{\rho(1)}), g_{\rho(2)}(e_{\rho(2)}), e_3)$ are distinct entries of $T_{\tau,G}$ while $(e_1, e_2, f_3(e_3))$ and $(g_{\rho(1)}(e_{\rho(1)}), g_{\rho(2)}(e_{\rho(2)}), f_3(e_3))$ are distinct entries of $T'_{\tau,G}$ containing the same symbol. This contradicts orthogonality. □

Next, we characterize those intermediate subgroups between G and $\mathrm{Apar}(Q)$ under whose action the Latin trade $T_{\tau,G}$ is a block.

Lemma 3.6 *Under the assumptions of Theorem 3.2, let $B \leq \mathrm{Apar}_{(12)}(Q)$ be such that $G \leq B$. The Latin trade $T_{\tau,G}$ is a block under the action of B if and only if $B_eG = GB_e$.*

Proof Suppose firstly that $B_eG = GB_e$. Let $\Theta' \in B$ be such that $\Theta'(e) \in T_{\tau,G}$. Then, there exists an autoparatopism $\Theta'' \in G$ such that $\Theta'(e) = \Theta''(e)$. Thus, $\Theta''^{-1}\Theta' \in B_e$. Letting $\Theta''^{-1}\Theta' = \Theta_1$, we have $\Theta' = \Theta''\Theta_1$.

Next, let $\Theta_2 \in G$. Since $B_eG = GB_e$, $\Theta_2^{-1}\Theta_1^{-1}\Theta_2 \in B_e$. Thus,

$$\begin{aligned} & \Theta_2^{-1}\Theta_1^{-1}\Theta_2(e) = e \\ \Leftrightarrow\ & \Theta'\Theta_2(\Theta_2^{-1}\Theta_1^{-1}\Theta_2(e)) = \Theta'\Theta_2(e) \\ \Leftrightarrow\ & \Theta''\Theta_1\Theta_2(\Theta_2^{-1}\Theta_1^{-1}\Theta_2(e)) = \Theta'\Theta_2(e) \\ \Leftrightarrow\ & \Theta''\Theta_2(e) = \Theta'\Theta_2(e). \end{aligned}$$

Hence, since $\Theta''\Theta_2 \in G$, we have that $\Theta'\Theta_2(e) \in T_{\tau,G}$.

In summary, whenever $\Theta' \in B$ satisfies $\Theta'(e) \in T_{\tau,G}$, we have that $\Theta'\Theta_2(e) \in T_{\tau,G}$, for each $\Theta_2 \in G$. Thus, the Latin trade $T_{\tau,G}$ is a block under the action of B.

Conversely, suppose that the Latin trade $T_{\tau,G}$ is a block under the action of B. Let $\Theta_1 \in B_e$ and $\Theta_2 \in G$. By the definition of a block, since $\Theta_1(e) = e$, we have that $\Theta_1(\Theta_2(e)) \in T_{\tau,G}$ and thus $\Theta_1(\Theta_2(e)) = \Theta_3(e)$ for some $\Theta_3 \in G$. In turn, $\Theta_3^{-1}\Theta_1\Theta_2 \in B_e$. Thus $\Theta_1\Theta_2 = \Theta_3\Theta_4$ for some $\Theta_4 \in B_e$. It follows that $B_eG \subseteq GB_e$. By elementary group theory, $|B_eG| = |GB_e|$, so we have that $B_eG = GB_e$. □

We have already indicated that our approach is identified under certain conditions with the constructive method described in Theorem 1.1. More precisely, it happens when the subgroup $G \leq \mathrm{Apar}_{(12)}(Q)$ constitutes indeed a subgroup in the automorphism group $\mathrm{Aut}(Q)$. The following result shows how both constructions can be identified.

Theorem 3.7 *Let $G \leq \mathrm{Aut}(Q)$ and $\tau := (e, \alpha, \overline{\alpha}) \in \mathrm{Ent}(L(Q)) \times G \times G$ be such that*

(C1′) $\alpha \in G_e^{\mathrm{row}} \setminus G_e^{\mathrm{col}}$;
(C2′) $\overline{\alpha} \in G_e^{\mathrm{col}}$; *and*
(C3′) $\overline{\alpha}^{-1}\alpha \in G_e^{\mathrm{sym}}$.

Suppose in turn that

(B1) $G_e^{\mathrm{row}} = \langle\alpha\rangle$;
(B2) $G_e^{\mathrm{col}} = \langle\overline{\alpha}\rangle$;
(B3) $G_e^{\mathrm{sym}} = \langle\overline{\alpha}^{-1}\alpha\rangle$;
(B4) $|\langle\alpha\rangle \cap \langle\overline{\alpha}\rangle| = 1$.

Let $a := \alpha^{-1}$, $b := \overline{\alpha}$, $c := \overline{\alpha}^{-1}\alpha$, $A := \langle a\rangle$, $B := \langle b\rangle$ and $C := \langle c\rangle$. Then, the Latin bitrade $(T_{\tau,G}, T'_{\tau,G})$ described as in Theorem 3.2 is isotopic to the Latin

bitrade (T°, T^*) *described as in Theorem 1.1 via the pair of isotopisms* (Θ, Θ') *that is defined as follows.*

$$\Theta g(e) := (gA, gB, gC)$$

and

$$\Theta' g(e) := (gA, gB, ga^{-1}C),$$

for all automorphism $g \in G$.

Proof First, suppose that $\Theta g_1(e) = \Theta g_2(e)$, for some $g_1, g_2 \in G$. Then $g_2^{-1}g_1 \in G_e$. From (B4), $g_1 = g_2$. Thus, Θ is an injection. Since $|T_{\tau,G}| = |T^\circ| = |G|$ by Theorem 1.1 and Theorem 3.2, Θ is in turn a bijection.

We next show that Θ preserves rows, columns and entries. To this end, suppose that both entries $g_1(e)$ and $g_2(e)$ share the same row in $T_{\tau,G}$, for some $g_1, g_2 \in G$. Then, $g_2^{-1}g_1 \in G_e^{\text{row}} = A$, and thus, $g_1A = g_2A$. Hence, $\Theta g_1(e)$ and $\Theta g_2(e)$ lie in the same row of T°. Similarly, if two entries in $T_{\tau,G}$ share the same column (or entry), then this property is preserved under the map Θ. Finally, since $\alpha = a^{-1}$, it follows similarly that $\Theta'(T'_{\tau,G}) = T^*$. □

Let us finish this section with some illustrative examples.

Example 3.8 Let Q be the additive group $((\mathbb{Z}_2)^2, +)$, whose Cayley table is

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

The autotopism group $\text{Atop}(Q)$ has size 96. It is generated, for example, by the automorphism (123) and the autotopism $((01), (0213), (0312))$.

Now, we consider the subgroup $G \leq \text{Atop}(Q)$ of size 12 that is generated by the autotopisms

$$\Theta := ((123), (013), (013)) \qquad \text{and} \qquad \overline{\Theta} := ((012), (132), (012)).$$

Conditions (C1)–(C3) in Theorem 3.2 hold and hence, we can construct the Latin bitrade $(T_{\tau,G}, T'_{\tau,G})$, with $e := (0, 0, 0) \in \text{Ent}(L(Q))$ and $\tau := (e, \Theta, \overline{\Theta})$. Since $G_e = \{\text{Id}\}$, we have that $|T_{\tau,G}| = |G| = 12$. Even more, since $|G_e^{\text{row}}| = |G_e^{\text{col}}| = |G_e^{\text{sym}}| = 3$, Lemma 3.4 ensures that both Latin trades $T_{\tau,G}$ and $T'_{\tau,G}$ are 3-homogeneous. Their respective 12 entries are highlighted in bold type within $L(Q)$ as follows.

$\mathbf{0_1}$	$\mathbf{1_3}$	2	$\mathbf{3_0}$
$\mathbf{1_2}$	0	$\mathbf{3_1}$	$\mathbf{2_3}$
$\mathbf{2_0}$	$\mathbf{3_2}$	$\mathbf{0_3}$	1
3	$\mathbf{2_1}$	$\mathbf{1_0}$	$\mathbf{0_2}$

It is orthogonal from Lemma 3.5, because $G_e^{\mathrm{sym}} \cap G_{((0,0,1))}^{\mathrm{sym}} = G_e = \{\mathrm{Id}\}$. ◁

Example 3.9 Let Q be the totally symmetric group $((\mathbb{Z}_2)^3, +)$, whose Cayley table is the Latin square

$$L(Q) \equiv \begin{array}{|c|c|c|c|c|c|c|c|}\hline 0&1&2&3&4&5&6&7\\\hline 1&0&3&2&5&4&7&6\\\hline 2&3&0&1&6&7&4&5\\\hline 3&2&1&0&7&6&5&4\\\hline 4&5&6&7&0&1&2&3\\\hline 5&4&7&6&1&0&3&2\\\hline 6&7&4&5&2&3&0&1\\\hline 7&6&5&4&3&2&1&0\\\hline\end{array}.$$

The automorphism group $\mathrm{Aut}(Q)$ has size 168. It is generated, for example, by the automorphisms (1735)(46) and (1736452). Furthermore, the autotopism group $\mathrm{Atop}(Q)$ has size 10752. It is generated, for example, by the autotopisms

$$((0265)(1374),\ (0573)(1462),\ (0716)(23)) \quad \text{and}$$
$$((0526713),\ (0361542),\ (0647251))\,.$$

Now, let us consider the subgroup $G \leq \mathrm{Atop}(Q)$ of size 32 that is generated by the autotopisms

$$\Theta := ((1643)(27), (0621)(3745), (0621)(3745))$$

and

$$\overline{\Theta} := ((0674)(1532), (1346)(27), (0674)(1532))\,.$$

Conditions (C1)–(C3) in Theorem 3.2 hold and hence, we can construct the Latin bitrade $(T_{\tau,G},\ T'_{\tau,G})$, with $e := (0,0,0)$ and $\tau := (e, \Theta, \overline{\Theta})$. Since $G_e = \{\mathrm{Id}\}$, we have that $|T_{\tau,G}| = |G| = 32$.

Even more, since $|G_e^{\mathrm{row}}| = |G_e^{\mathrm{col}}| = |G_e^{\mathrm{sym}}| = 4$, Lemma 3.4 ensures that both Latin trades $T_{\tau,G}$ and $T'_{\tau,G}$ are 4-homogeneous. Their respective 32 entries are highlighted in bold type within $L(Q)$ as follows.

$\mathbf{0_6}$	$\mathbf{1_0}$	$\mathbf{2_1}$	3	4	5	$\mathbf{6_2}$	7
1	$\mathbf{0_3}$	$\mathbf{3_2}$	$\mathbf{2_4}$	5	$\mathbf{4_0}$	7	6
2	$\mathbf{3_7}$	0	1	6	$\mathbf{7_4}$	$\mathbf{4_5}$	$\mathbf{5_3}$
3	2	$\mathbf{1_5}$	0	$\mathbf{7_1}$	$\mathbf{6_7}$	$\mathbf{5_6}$	4
$\mathbf{4_0}$	5	6	7	$\mathbf{0_3}$	1	$\mathbf{2_4}$	$\mathbf{3_2}$
5	4	7	$\mathbf{6_2}$	$\mathbf{1_0}$	$\mathbf{0_6}$	3	$\mathbf{2_1}$
$\mathbf{6_7}$	$\mathbf{7_1}$	4	$\mathbf{5_6}$	2	3	0	$\mathbf{1_5}$
$\mathbf{7_4}$	6	$\mathbf{5_3}$	$\mathbf{4_5}$	$\mathbf{3_7}$	2	1	0

Lemma 3.5 implies that this Latin bitrade is not orthogonal, because $|G_e| = 1$ and $G_e^{\mathrm{sym}} \cap G_{((0,0,6))}^{\mathrm{sym}} = \{(((05)(14)(27)(36),\ (05)(14)(27)(36),\ \mathrm{Id})\,,\ \mathrm{Id}\}$. ◁

The 4-homogeneous Latin trade described in Example 3.9 was first observed in [7], as a singular example not part of a general construction. Therein, it was noted that this Latin trade gives the minimum Hamming distance, 32, from $((\mathbb{Z}_2)^3, +)$ to a Latin square containing no 2×2 subsquares. It is also a minimal Latin trade. Adding any new entry to the Latin trade yields a minimal defining set of the Latin square $((\mathbb{Z}_2)^3, +)$.

Example 3.10 Since the group Q described in Example 3.9 is totally symmetric, we have that $|\mathrm{Apar}(Q)| = 6 \cdot |\mathrm{Atop}(Q)| = 64512$. Moreover, the autoparatopism group $\mathrm{Apar}(Q)$ is generated by the autoparatopisms

$$((123);\ ((0265)(1374),\ (0573)(1462),\ (0716)(23)))$$

and

$$((12);\ ((0526713),\ (0361542),\ (0647251)))\,.$$

Let us consider again the entry $e = (0, 0, 0) \in \mathrm{Ent}(L(Q))$, as in Example 3.9, and let $G' \leq \mathrm{Apar}(Q)$ be the subgroup of size 32 that is generated by the autoparatopisms

$$\Theta' := ((12);\ ((0642)(1753),\ (26)(37),\ (0642)(1753)))$$

and

$$\overline{\Theta}' := ((12);\ ((27)(36),\ (0653)(2174),\ (0653)(2174)))\,.$$

Conditions (C1)–(C3) in Theorem 3.2 hold and hence, we can construct the Latin bitrade $(T_{\tau',G'},\ T'_{\tau',G'})$, with $\tau' := (e, \Theta', \overline{\Theta}')$. Since $\left|G'_e\right| = 1$ and $|G'^{\mathrm{row}}_e| = |G'^{\mathrm{col}}_e| = |G'^{\mathrm{sym}}_e| = 4$, then Lemma 3.4 implies that both Latin trades $T_{\tau',G'}$ and $T'_{\tau',G'}$ are 4-homogeneous. Their respective 32 entries are highlighted in bold type within $L(Q)$ as follows.

$\mathbf{0_6}$	1	2	$\mathbf{3_0}$	$\mathbf{4_3}$	5	$\mathbf{6_4}$	7
1	$\mathbf{0_6}$	$\mathbf{3_0}$	2	5	$\mathbf{4_3}$	7	$\mathbf{6_4}$
$\mathbf{2_0}$	3	$\mathbf{0_7}$	1	6	$\mathbf{7_4}$	$\mathbf{4_2}$	5
3	$\mathbf{2_0}$	1	$\mathbf{0_7}$	$\mathbf{7_4}$	6	5	$\mathbf{4_2}$
4	$\mathbf{5_2}$	6	$\mathbf{7_5}$	0	$\mathbf{1_7}$	$\mathbf{2_1}$	3
$\mathbf{5_2}$	4	$\mathbf{7_5}$	6	$\mathbf{1_7}$	0	3	$\mathbf{2_1}$
$\mathbf{6_5}$	7	4	$\mathbf{5_3}$	2	$\mathbf{3_1}$	0	$\mathbf{1_6}$
7	$\mathbf{6_5}$	$\mathbf{5_3}$	4	$\mathbf{3_1}$	2	$\mathbf{1_6}$	0

◁

4 Further examples

We finish our study by illustrating our constructive proposal with a pair of more comprehensive examples. They refer to the construction of Latin bitrades arising from Mersenne primes and from quadratic orthomorphisms.

4.1 Construction of Latin trades via Mersenne primes

Let p be a Mersenne prime; that is, $p = 2^q - 1$, where both p and q are primes. Assume also that $q \geq 3$. If $\mathbb{F}$ denotes the finite field of order 2^q, then let a be a primitive element in $\mathbb{F}$; let i be the unique solution modulo p to $a^{2i} + a^2 + a + 1 = 0$; and let Q be the additive group in $\mathbb{F}$. Suppose furthermore the existence of a positive integer j such that $2^j + i - 1$ is divisible by p.

Let $\omega, \alpha \in \mathrm{Aut}(Q)$ be defined by $\omega(x) = ax$ and $\alpha(x) = x^{(p+1)/2}$. (Note here that $\alpha^{-1}(x) = x^2$ and hence, α^{-1} (and thus α) is an automorphism of Q, because $(x + y)^2 = x^2 + y^2$ over $\mathbb{F}$.) In addition, observe that ω has order p; α^{-1} (and hence α) has order q, and $\alpha\omega^2 = \omega\alpha$, composing from right to left. From Cavenagh et al. [9], for example, we have that ω and α generate a group $G \leq \mathrm{Aut}\,(((\mathbb{Z}_2)^q, +))$ of size pq.

Next, let $e := (1, a, a + 1) \in \mathrm{Ent}(L)$. Then, $G_e = \{\mathrm{Id}\}$ and $|G_e^{\mathrm{row}}| = |G_e^{\mathrm{col}}| = |G_e^{\mathrm{sym}}| = q$. In addition, $\alpha \in G_e^{\mathrm{row}} \backslash G_e^{\mathrm{col}}$. Further, let $\overline{\alpha} = \omega^j \alpha^{-j}$. Since $2^j + i - 1$ is divisible by p, we have that

$$\overline{\alpha}(a) = \omega^i \alpha^{-j}(a) = \omega^i (a^{2^j}) = a^{2^j + i} = a.$$

So, $\overline{\alpha} \in G_e^{\mathrm{col}}$. Moreover,

$$\begin{aligned} \alpha^{-1}\overline{\alpha}(a + 1) = \alpha^{-1}(\omega^i \alpha^{-j}(a + 1)) = \alpha^{-1}(\omega^i (a^{2^j} + 1)) = \alpha^{-1}(a^{2^j + i} + a^i) = \\ = \alpha^{-1}(a + a^i) = a^2 + a^{2i}. \end{aligned}$$

From the above assumption on a, we have that $\overline{\alpha}^{-1}\alpha \in G_e^{\mathrm{sym}}$. As a consequence, the next result follows readily from Theorem 3.2 and Lemma 3.4, for the subgroup G and the tuple $(e, \alpha, \overline{\alpha})$.

Theorem 4.1 *Let $p = 2^q - 1$ be a Mersenne prime such that $a^{2i} + a^2 + a + 1 = 0$, for some positive integer i and some primitive element a, over the field of order 2^q. Suppose furthermore that there exists a positive integer j such that $2^j + i - 1$ is divisible by p. Then, there exists a q-homogeneous minimal Latin trade in $((\mathbb{Z}_2)^q, +)$ of size pq.*

Example 4.2 The hypothesis of Theorem 4.1 holds for $q = 3$, $i = 6$, $j = 1$ and $a^3 = a + 1$. Let Q be the additive group in the finite field of order 8. It is isomorphic to the totally symmetric group $((\mathbb{Z}_2)^3, +)$, whose Cayley table is the Latin square $L(Q)$ described in Example 3.9. Particularly, the elements a, a^2, $a^3 = a + 1$, $a^4 = a^2 + a$, $a^5 = a^2 + a + 1$ and $a^6 = a^2 + 1$ are, respectively, represented by 2, 6, 3, 4, 5 and 7.

From Theorem 4.1, we can construct a 3-homogeneous minimal Latin trade in Q of size 21. To this end, we consider the automorphisms $\omega(x) = ax$ and $\alpha(x) = x^4$ in $\mathrm{Aut}(Q)$, which are, respectively, represented by the permutations (1263457) and (246)(357). In addition, we define the automorphism $\overline{\alpha}(x) = \omega^6\alpha^{-1}(x)$ in $\mathrm{Aut}(Q)$, which is represented by the permutation (174)(356). Finally, we consider the entry $e := (1, 2, 3) \in \mathrm{Ent}(L(Q))$. Our construction yields the following Latin bitrade $\left(T_{\tau,G},\ T'_{\tau,G}\right)$, where $G := \langle\, \omega,\ \alpha \,\rangle$ and $\tau := (e, \alpha, \overline{\alpha})$.

0	1	2	3	4	5	6	7
1	0	$\mathbf{3_5}$	2	$\mathbf{5_7}$	4	$\mathbf{7_3}$	6
2	3	0	$\mathbf{1_4}$	6	$\mathbf{7_1}$	$\mathbf{4_7}$	5
3	$\mathbf{2_6}$	1	0	$\mathbf{7_2}$	$\mathbf{6_7}$	5	4
4	5	$\mathbf{6_3}$	7	0	$\mathbf{1_6}$	2	$\mathbf{3_1}$
5	$\mathbf{4_2}$	7	6	1	0	$\mathbf{3_4}$	$\mathbf{2_3}$
6	7	4	$\mathbf{5_1}$	$\mathbf{2_5}$	3	0	$\mathbf{1_2}$
7	$\mathbf{6_4}$	$\mathbf{5_6}$	$\mathbf{4_5}$	3	2	1	0

Lemma 3.5 implies that this Latin bitrade is orthogonal, because

$$G_e^{\mathrm{sym}} \cap G_{((1,2,5))}^{\mathrm{sym}} = \{\mathrm{Id}\} = G_e.$$

Furthermore, the subgroup $\mathrm{Aut}(Q)_e \leq \mathrm{Aut}(Q)$ has size four. It is generated by the automorphisms (46)(57) and (45)(67). Then,

$$\left(|\mathrm{Aut}(Q)| \,/\, |\mathrm{Aut}(Q)_e|\right) \,/\, |T_{\tau,G}| = 2.$$

Indeed, under the action of the subgroup G, there are two disjoint and isomorphic copies of the Latin trade $T_{\tau,G}$. These turn out to be the original $T_{\tau,G}$ and its transpose, which arises, for instance, by replacing the entry e in the tuple τ by the entry $(1, 3, 2)$. (Note here that $\mathrm{Aut}(Q)_{((1,3,2))} = \mathrm{Aut}(Q)_e$.) Alternatively, if we add the generator $(12)(56) \in \mathrm{Aut}(Q)$ to the group G to create a group G' of order 42, then the latter induces two orbits on the set

$$\mathrm{Ent}(L(T_{\tau,G})) = \{(i, j, i + j) \in \mathrm{Ent}(L(Q)) \mid 0 \notin \{i, j, i + j\}\} \subset \mathrm{Ent}(L(Q)).$$

One is the above Latin trade $T_{\tau,G}$. The other one is its transpose, which is obviously also a Latin trade. Note that the subgroup $\mathrm{Aut}(Q)_e \leq \mathrm{Aut}(Q)$ does not stabilize the Latin trade $T_{\tau,G}$ as a set, because ω maps, for instance, the entry $(2, 6, 4) \in \mathrm{Ent}(T_{\tau,G})$ to the entry $(0, 4, 6) \notin \mathrm{Ent}(T_{\tau,G})$. Since the group G is the stabilizer in $\mathrm{Aut}(Q)$ of the Latin trade $T_{\tau,G}$, the latter is not a block in the action of $\mathrm{Aut}(Q)$ on $L(Q)$. For instance, the automorphism $(1746325) \in \mathrm{Aut}(Q)$ maps the entry e to the entry $(7, 5, 2) \notin \mathrm{Ent}(T_{\tau,G})$. ◁

4.2 Construction of Latin trades via quadratic orthomorphisms

Theorem 3.2 can be implemented to construct Latin bitrades from quadratic orthomorphisms over finite fields. An *orthomorphism* over a finite field $\mathbb{F}_q$, with q an odd prime power, is a permutation $\theta : \mathbb{F}_q \to \mathbb{F}_q$ such that the map $x \to \theta(x) - x$ is also a permutation of $\mathbb{F}_q$. It is *canonical* if $\theta(0) = 0$, while it is *quadratic* if there are two constants $a, b \in \mathbb{F}_q \backslash \{0\}$ such that $\theta(x) = ax$, whenever x is a perfect square, and $\theta(x) = bx$, otherwise. Observe that every quadratic orthomorphism is canonical.

Theorem 4.3 [15, 20] *Two constants a and b define a quadratic orthomorphism as above if and only if ab and $(a-1)(b-1)$ are non-zero squares in $\mathbb{F}_q$.*

For any given orthomorphism θ over $\mathbb{F}_q$, let $L(\theta)$ denote the Latin square of order q such that

$$\mathrm{Ent}(L(\theta)) := \left\{(i,\ j,\ \theta(j-i)+i) \mid i, j \in \mathbb{F}_q\right\}. \tag{6}$$

The automorphism group $\mathrm{Aut}(L(\theta))$ has been characterized in [14] whenever θ is quadratic and q is odd. We consider the subgroup $B(q)$ (or B when the context is clear) of $\mathrm{Aut}(L(\theta))$ given by all automorphisms of the form $f(x) = gx + h$, where $h \in \mathbb{F}_q$ and g is a perfect square in $\mathbb{F}_q$. Observe that the order of $B(q)$ is $q(q-1)/2$.

Example 4.4 The triple $(q, a, b) = (11, 2, 6)$ satisfies the hypothesis of Theorem 4.3. Thus, the permutation

$$\theta := (12)(36)(48)(5\,10)(79)$$

is a quadratic orthomorphism in $\mathbb{F}_{11}$. Then,

$$L(\theta) \equiv \begin{array}{|c|c|c|c|c|c|c|c|c|c|c|}\hline 0&2&1&6&8&10&3&9&4&7&5\\\hline 6&1&3&2&7&9&0&4&10&5&8\\\hline 9&7&2&4&3&8&10&1&5&0&6\\\hline 7&10&8&3&5&4&9&0&2&6&1\\\hline 2&8&0&9&4&6&5&10&1&3&7\\\hline 8&3&9&1&10&5&7&6&0&2&4\\\hline 5&9&4&10&2&0&6&8&7&1&3\\\hline 4&6&10&5&0&3&1&7&9&8&2\\\hline 3&5&7&0&6&1&4&2&8&10&9\\\hline 10&4&6&8&1&7&2&5&3&9&0\\\hline 1&0&5&7&9&2&8&3&6&4&10\\\hline\end{array}$$

The group B is generated by the automorphisms $\alpha(x) = 3x$ and $\overline{\alpha}(x) = 5x - 4$. Now, let $e := (0, 1, 2) \in \mathrm{Ent}(L(Q))$ and let $G = B$. Conditions (C1)–(C3) in Theorem 3.2 hold and hence, we can construct the Latin bitrade $(T_{\tau,G},\ T'_{\tau,G})$, with $\tau := (e, \alpha, \overline{\alpha})$.

Since $G_e = \{\mathrm{Id}\}$ and $|G_e^{\mathrm{row}}| = |G_e^{\mathrm{col}}| = |G_e^{\mathrm{sym}}| = 5$, then Lemma 3.4 implies that both Latin trades $T_{\tau,G}$ and $T'_{\tau,G}$ are 5-homogeneous. They are highlighted in bold type

within $L(\theta)$ as follows.

0	$\mathbf{2_6}$	1	$\mathbf{6_7}$	$\mathbf{8_2}$	$\mathbf{10_8}$	3	9	4	$\mathbf{7_{10}}$	5
6	1	$\mathbf{3_7}$	2	$\mathbf{7_8}$	$\mathbf{9_3}$	$\mathbf{0_9}$	4	10	5	$\mathbf{8_0}$
$\mathbf{9_1}$	7	2	$\mathbf{4_8}$	3	$\mathbf{8_9}$	$\mathbf{10_4}$	$\mathbf{1_{10}}$	5	0	6
7	$\mathbf{10_2}$	8	3	$\mathbf{5_9}$	4	$\mathbf{9_{10}}$	$\mathbf{0_5}$	$\mathbf{2_0}$	6	1
2	8	$\mathbf{0_3}$	9	4	$\mathbf{6_{10}}$	5	$\mathbf{10_0}$	$\mathbf{1_6}$	$\mathbf{3_1}$	7
8	3	9	$\mathbf{1_4}$	10	5	$\mathbf{7_0}$	6	$\mathbf{0_1}$	$\mathbf{2_7}$	$\mathbf{4_2}$
$\mathbf{5_3}$	9	4	10	$\mathbf{2_5}$	0	6	$\mathbf{8_1}$	7	$\mathbf{1_2}$	$\mathbf{3_8}$
$\mathbf{4_9}$	$\mathbf{6_4}$	10	5	0	$\mathbf{3_6}$	1	7	$\mathbf{9_2}$	8	$\mathbf{2_3}$
$\mathbf{3_4}$	$\mathbf{5_{10}}$	$\mathbf{7_5}$	0	6	1	$\mathbf{4_7}$	2	8	$\mathbf{10_3}$	9
10	$\mathbf{4_5}$	$\mathbf{6_0}$	$\mathbf{8_6}$	1	7	2	$\mathbf{5_8}$	3	9	$\mathbf{0_4}$
$\mathbf{1_5}$	0	$\mathbf{5_6}$	$\mathbf{7_1}$	$\mathbf{9_7}$	2	8	3	$\mathbf{6_9}$	4	10

A second, disjoint 5-homogeneous trade can be found using $e := (0, 10, 5) \in \mathrm{Ent}(L(Q))$, $\alpha(x) = 4x$ and $\overline{\alpha}(x) = 9x - 3$:

0	2	$\mathbf{1_4}$	6	8	10	$\mathbf{3_1}$	$\mathbf{9_3}$	$\mathbf{4_5}$	7	$\mathbf{5_9}$
$\mathbf{6_{10}}$	1	3	$\mathbf{2_5}$	7	9	0	$\mathbf{4_2}$	$\mathbf{10_4}$	$\mathbf{5_6}$	8
9	$\mathbf{7_0}$	2	4	$\mathbf{3_6}$	8	10	1	$\mathbf{5_3}$	$\mathbf{0_5}$	$\mathbf{6_7}$
$\mathbf{7_8}$	10	$\mathbf{8_1}$	3	5	$\mathbf{4_7}$	9	0	2	$\mathbf{6_4}$	$\mathbf{1_6}$
$\mathbf{2_7}$	$\mathbf{8_9}$	0	$\mathbf{9_2}$	4	6	$\mathbf{5_8}$	10	1	3	$\mathbf{7_5}$
$\mathbf{8_6}$	$\mathbf{3_8}$	$\mathbf{9_{10}}$	1	$\mathbf{10_3}$	5	7	$\mathbf{6_9}$	0	2	4
5	$\mathbf{9_7}$	$\mathbf{4_9}$	$\mathbf{10_0}$	2	$\mathbf{0_4}$	6	8	$\mathbf{7_{10}}$	1	3
4	6	$\mathbf{10_8}$	$\mathbf{5_{10}}$	$\mathbf{0_1}$	3	$\mathbf{1_5}$	7	9	$\mathbf{8_0}$	2
3	5	7	$\mathbf{0_9}$	$\mathbf{6_0}$	$\mathbf{1_2}$	4	$\mathbf{2_6}$	8	10	$\mathbf{9_1}$
$\mathbf{10_2}$	4	6	8	$\mathbf{1_{10}}$	$\mathbf{7_1}$	$\mathbf{2_3}$	5	$\mathbf{3_7}$	9	0
1	$\mathbf{0_3}$	5	7	9	$\mathbf{2_0}$	$\mathbf{8_2}$	$\mathbf{3_4}$	6	$\mathbf{4_8}$	10

◁

The previous example can be generalized as follows.

Theorem 4.5 *Let θ be a quadratic orthomorphism in $\mathbb{F}_q$ based on two distinct constants a and b such that ab and $(a-1)(b-1)$ are non-zero squares in $\mathbb{F}_q$. Let m be the order of the group generated by b/a and $(b-1)/(a-1)$ in the multiplicative group of $\mathbb{F}_q$. Then, there is an m-homogeneous Latin trade T in $L(\theta)$ of size mq. In fact, there are $(q-1)/m$ disjoint trades in $L(\theta)$, each one of them m-homogeneous.*

Proof First, let $e := (0, 1, a) \in \mathrm{Ent}(L(\theta))$, $\alpha_1(x) = bx/a$ and $\overline{\alpha_1}(x) = (b-1)(x-1)/(a-1)+1$, both of them in B_q. Conditions (C1)–(C3) in Theorem 3.2 are satisfied, so long as $a \neq b$.

Thus, there is a Latin trade $T_{\tau_1,G}$ in $L(\theta)$ defined as in Theorem 3.7, where $\tau_1 := (e, \alpha, \overline{\alpha})$ and G is the group of automorphisms generated by α_1 and $\overline{\alpha_1}$. Observe that $|G| = mq$, $|G_e^{\mathrm{row}}| = |G_e^{\mathrm{col}}| = |G_e^{\mathrm{sym}}| = m$ and $G_e = \{\mathrm{Id}\}$. By Lemma 3.4, $T_{\tau_1,G}$ is m-homogeneous.

Observe that $G \leq B$, because ab and $(a-1)(b-1)$ are perfect squares in $\mathbb{F}_q$, and hence, b/a and $(b-1)/(a-1)$, which are the respective coefficients of x in the orthomorphisms α_1 and $\overline{\alpha_1}$, are also perfect squares in $\mathbb{F}_q$. Then, based on the fact that $B_e = \{\mathrm{Id}\}$, we have from Lemma 3.6 that our Latin trade $T_{\tau_1,G}$ is a block under the action of B. In turn, there are $q(q-1)/2m$ disjoint and isotopic copies of $T_{\tau_1,G}$ in $L(\theta)$ under action of B.

Next, fix a z which is not a perfect square in F_q. define $e' := (0, z, bz) \in \mathrm{Ent}(L(\theta))$, $\alpha_2(x) = ax/b$ and $\overline{\alpha_2}(x) = (a-1)(x-z)/(b-1)+z$. Observe that the group G defined above is generated by α_2 and $\overline{\alpha_2}$. In turn, as above, there is an m-homogenous Latin trade $T_{\tau_2,G}$ in $L(\theta)$ defined as in Theorem 3.7, where $\tau_2 := (e', \alpha_2, \overline{\alpha_2})$. Moreover, there are $q(q-1)/2m$ disjoint and isotopic copies of $T_{\tau_2,G}$ in $L(\theta)$ under the action of B.

It remains to show that the above sets of trades are disjoint. Suppose there is $f \in B$ which maps e to e', where $f(x) = gx + h$. Then $f(0) = h = 0$, $f(1) = g + h = z$ and $f(a) = ga + h = bz$. In turn, $g = z(b-1)/(a-1)$, contradicting the fact that g is a perfect square. Thus, e and e' lie in distinct orbits of B and therefore all the trades constructed above form a pairwise disjoint set of size $q(q-1)/m$. □

Acknowledgements The authors want to express their gratitude to the referees for their valuable comments which have helped improve this work. In addition, they are very grateful to Professor Ian Wanless, for his assistance in the development of this study. Finally, Falcón's work is partially supported by both the Research Project FQM-016 *"Codes, Design, Cryptography and Optimization"*, from Junta de Andalucía, and the Research Project TED2021-130566B-100 *"New graphical authentication schemes in Information Management Systems by means of fractal images based on Latin squares"*, from Ministry of Science and Innovation of the Government of Spain.

Funding Funding for open access publishing: Universidad de Sevilla/CBUA.

Data Availability The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Declarations

Conflict of interest The authors declare no declare that they have conflict of interest.

References

1. Bean, R., Bidkhori, H., Khosravi, M., Mahmoodian, E.S.: k-homogeneous Latin trades. Bayreuth. Math. Schr. **74**, 7–18 (2005)

2. Behrooz Bagheri, Gh., Mahmoodian, E.S.: On the existence of k-homogeneous Latin bitrades. Util. Math. **85**, 333–345 (2011)
3. Blackburn, S., McCourt, T.: Triangulations of the sphere, bitrades and abelian groups. Combinatorica **34**, 527–546 (2014). https://doi.org/10.1007/s00493-014-2924-7
4. Cavenagh, N.J.: The theory and application of Latin bitrades: a survey. Math. Slovaca **58**, 691–718 (2008). https://doi.org/10.2478/s12175-008-0103-2
5. Cavenagh, N.J.: Embedding 3-homogeneous Latin trades into abelian 2-groups. Comment. Math. Univ. Carolin. **45**, 191–212 (2004)
6. Cavenagh, N.J., Donovan, D., Drápal, A.: 3-homogeneous Latin trades. Discrete Math. **300**, 57–70 (2005). https://doi.org/10.1016/j.disc.2005.04.021
7. Cavenagh, N.J., Donovan, D., Drápal, A.: 4-homogeneous Latin trades. Australas. J. Combin. **32**, 285–303 (2005)
8. Cavenagh, N.J., Ramadurai, R.: On the distances between Latin squares and the smallest defining set size. J. Combin. Des. **25**, 147–158 (2017). https://doi.org/10.1002/jcd.21529
9. Cavenagh, N.J., Drápal, A., Hämäläinen, C.: Latin bitrades derived from groups. Discrete Math. **308**, 6189–6202 (2008). https://doi.org/10.1016/j.disc.2007.11.041
10. Cavenagh, N.J., Wanless, I.M.: Latin trades in groups defined on planar triangulations. J. Algebraic Combin. **30**, 323–347 (2009). https://doi.org/10.1007/s10801-008-0165-9
11. Drápal, A.: Hamming distances of groups and quasi-groups. Discrete Math. **235**, 189–197 (2001). https://doi.org/10.1016/S0012-365X(00)00272-7
12. Drápal, A.: How far apart can the group multiplication tables be? Eur. J. Combin. **13**, 335–343 (1992). https://doi.org/10.1016/S0195-6698(05)80012-5
13. Drápal, A., Kepka, T.: Group distances of Latin squares. Comm. Math. Univ. Carolinae **26**, 275–283 (1985)
14. Drápal, A., Wanless, I.: Isomorphisms of quadratic quasigroups. Proc. Edinb. Math. Soc. (2) **66**, 1085–1109 (2023). https://doi.org/10.1017/s0013091523000585
15. Evans, A.B.: Orthogonal Latin squares based on groups, *Developments in Mathematics***57**, Springer, Cham (2018). https://doi.org/10.1007/978-3-319-94430-2
16. Evans, T.: Embedding incomplete Latin squares. Amer. Math. Monthly **67**, 958–961 (1960). https://doi.org/10.2307/2309221
17. Falcón, R.M., Stones, R.J.: Partial Latin rectangle graphs and autoparatopism groups of partial Latin rectangles with trivial autotopism groups. Discrete Math. **340**, 1242–1260 (2017). https://doi.org/10.1016/j.disc.2017.01.002
18. Keedwell, A.D., Dénes, J.: Latin squares and their applications, 2nd edition. Elsevier/North-Holland, Amsterdam (2015)
19. Vojtěchovský, P.: Distances of groups of prime order, In: *Contributions to general algebra*, 11 (Olomouc/Velké Karlovice, 1998), 225–231, Heyn, Klagenfurt (1999)
20. Wanless, I.: Atomic Latin squares based on cyclotomic orthomorphisms, *Electron. J. Combin.***12** (2005), Paper no. R22, 23 pp. https://doi.org/10.37236/1919