Comment.Math.Univ.Carolin. 45,2 (2004)191–212

Embedding 3-homogeneous latin trades into abelian 2-groups

Nicholas J. Cavenagh

Abstract. Let T be a partial latin square and L be a latin square with $T \subseteq L$. We say that T is a latin trade if there exists a partial latin square T' with $T' \cap T = \emptyset$ such that $(L \setminus T) \cup T'$ is a latin square. A k-homogeneous latin trade is one which intersects each row, each column and each entry either 0 or k times. In this paper, we show the existence of 3-homogeneous latin trades in abelian 2-groups.

Keywords: latin square, latin trade, abelian 2-group

Classification: 05B15, 20N05

1. Introduction

Given a particular latin square L, what is the smallest size of a partial latin square P such that P is contained in L, P is contained in no other latin square, and is minimal with respect to this property? (Equivalently, given a latin square L, what is the size of the smallest critical set in L?)

In general the solution to this problem is difficult, but there is possibility of progress when the latin square L is the multiplication table for a group.

Consider the following latin square L, which is (isotopic to) the multiplication table for the group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

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

L

0	1		
		3	
			1
	2		

P

The partial latin square P is a critical set for $(\mathbb{Z}_2)^2$. It is well known that $|P| = 5$ is the smallest possible size for a critical set in $(\mathbb{Z}_2)^2$, and that P is in fact the unique partial latin square with this property (up to isotopism).

Supported by Ministry of Education of the Czech Republic as project LN00A056.

If we delete any entry in P, the resultant partial latin square P' will have two completions (fitting the definition of critical set). If we consider the difference between L and an alternative completion for P', we obtain a latin trade.

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

L'

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

$L \setminus L'$

For example, if we delete the entry 1 from the first row and second column of P, the resultant partial latin square P' has completion to latin square L' on the left. On the right we give the corresponding latin trade $L \setminus L' \subseteq L$.

Similarly, for each entry in the critical set P shown above we can obtain a latin trade T in L that intersects P in exactly one entry. So there is a connection between the latin trades in a latin square L and the critical sets in L. (Indeed they occupy the same chapter in the *CRC Handbook of Combinatorial Designs* [25]).

There are three interesting points to note about the above example of the latin trade $L \setminus L'$. Namely, it is

1. large with respect to the size of the latin square L;
2. necessary to establish the critical set of smallest size in $(\mathbb{Z}_2)^2$;
3. 3-homogeneous — that is, each row, column and entry occurs 3 times.

In this paper, we take a construction of 3-homogeneous latin trades from [8], and some linearly independent vectors from $(\mathbb{Z}_2)^n$ and cook up a general way of finding 3-homogeneous latin trades in $(\mathbb{Z}_2)^n$. We conjecture that some of these latin trades, and in general k-homogeneous latin trades can be used to determine critical sets in $(\mathbb{Z}_2)^n$ of small sizes.

2. Definitions

We start with basic definitions which allow us to state and prove our main results.

Let $N = N(n)$ be some finite set of size n. Let $R(N) = \{r_i \mid i \in N\}$, $C(N) = \{c_i \mid i \in N\}$ and $E(N) = \{e_i \mid i \in N\}$.

A *partial latin square* P of order n is a set of ordered triples of the form (r_i, c_j, e_k), where $r_i \in R(N)$, $c_j \in C(N)$ and $e_k \in E(N)$ with the following properties:

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

We may also represent a partial latin square P as an $n \times n$ array with entries chosen from the set $E(N)$ such that if $(r_i, c_j, e_k) \in P$, the *entry* e_k occurs in cell (r_i, c_j).

A partial latin square has the property that each entry occurs at most once in each row and at most once in each column. If all the cells of the array are filled then the partial latin square is termed a latin square. That is, a *latin square* L of order n is an $n \times n$ array with entries chosen from the set $E(N)$ in such a way that each element of $E(N)$ occurs precisely once in each row and precisely once in each column of the array.

For a given partial latin square P the set of cells

$$\mathcal{S}_P = \{(r_i, c_j) \mid (r_i, c_j, e_k) \in P, \quad \text{for some} \quad e_k \in E(N)\}$$

is said to determine the *shape* of P and $|\mathcal{S}_P|$ is said to be the *size* of the partial latin square. That is, the size of P is the number of non-empty cells in the array. For each $i \in N$, let $\mathcal{R}_P^i$ denote the set of entries occurring in row r_i of P. Formally, $\mathcal{R}_P^i = \{e_k \mid (r_i, c_j, e_k) \in P\}$. For each $j \in N$, we define $\mathcal{C}_P^j = \{e_k \mid (r_i, c_j, e_k) \in P\}$. Finally, for each $k \in N$, we define $\mathcal{E}_P^k = \{(r_i, c_j) \mid (r_i, c_j, e_k) \in P\}$.

A partial latin square T of order n is said to be a *latin trade* (or *latin interchange*) if $T \neq \emptyset$ and there exists a partial latin square T' (called a *disjoint mate* of T) of order n, such that

- $\mathcal{S}_T = \mathcal{S}_{T'}$,
- if $(r_i, c_j, e_k) \in T$ and $(r_i, c_j, e_{k'}) \in T'$ then $k \neq k'$,
- for each $i \in N(n)$, $\mathcal{R}_T^i = \mathcal{R}_{T'}^i$,
- for each $j \in N(n)$, $\mathcal{C}_T^j = \mathcal{C}_{T'}^j$.

Important facts on latin trades may be found in [11], [12], [13], [16] and of course in the "latin square bible" [10]. In [14] it is shown how to embed a minimal latin trade onto an orientable surface. We thus may associate with a minimal latin trade a genus.

A latin trade T of order n is said to be *k-homogeneous* if

- for each $i \in N(n)$, $|\mathcal{R}_T^i| = 0$ or k, and
- for each $j \in N(n)$, $|\mathcal{C}_T^j| = 0$ or k, and
- for each $k \in N(n)$, $|\mathcal{E}_T^k| = 0$ or k.

Clearly if T is k-homogeneous, its size is equal to km for some integer m, where $m \geq k$. A minimal 2-homogeneous latin trade is uniquely a 2×2 latin subsquare.

A *critical set* in a latin square L (of order n) is a partial latin square $P \subseteq L$, such that

(1) L is the only latin square of order n which has element e_k in cell (r_i, c_j) for each $(r_i, c_j, e_k) \in P$; and
(2) no proper subset of P satisfies (1).

Let T be a partial latin square that is a subset of a latin square L. Observe (as in the example in the Introduction) that T is a latin trade if and only if there exists a disjoint mate T', with $T' \cap T = \emptyset$, such that $(L \setminus T) \cup T'$ is a latin square. It follows that a critical set P in a latin square L must intersect every latin trade in L; and is minimal with respect to this property.

Because k-homogeneous latin trades often have the property of being large in size (with respect to the size of the latin square) yet primary, they often are related to critical sets of small size. It is known that using only 2-homogeneous and 3-homogeneous latin trades, we can determine minimum critical sets in the latin squares for both $((\mathbb{Z}_2)^2, +)$ (size 5) and $((\mathbb{Z}_2)^3, +)$ (size 25) ([23]). (The size of the smallest critical set in $((\mathbb{Z}_2)^4, +)$ is not known, but is no greater than 124 [23].) We conjecture that k-homogeneous latin trades with $k > 3$ can be used to locate small critical sets in $((\mathbb{Z}_2)^n, +)$ for larger values of n. (See also Section 7.)

The best known lower bound for the size of a critical set in an arbitrary latin square of order n is $\lfloor (4n-8)/3 \rfloor$ [20]. This bound can be improved under certain restrictions; such as if the critical set has an empty row ($2n-4$, [5]), the critical set has a strongly forced completion ($\lfloor n^2/4 \rfloor$, [3]), or if the latin square is the addition table for the integers modulo n ($n^{4/3}/2$, [6]). It is conjectured in [4] that in fact $\lfloor n^2/4 \rfloor$ is the actual lower bound. This is known to be true for $n \leq 7$ ([1], [2]).

3. Hexagonal constructions

The constructions in this section are given in detail in [8], complete with proofs. Here we give just enough detail for the embeddings into $(\mathbb{Z}_2)^n$ later in the paper.

Definition 1. Let S be the following set of co-ordinates in $\mathbb{R} \times \mathbb{R}$:

$$S = \{(2\sqrt{3}i, 2j), ((2i+1)\sqrt{3}, 2j+1) \mid i, j \in \mathbb{Z}\}.$$

Let C be the set of unit circles in $\mathbb{R} \times \mathbb{R}$ whose centres are the elements of S. (This is the well-known hexagonal lattice in the plane. See Chapter 1 of [9] for more details on lattices and spherical packings.)

If $d \in C$ is a circle with centre (α, β), then let:

- $u_1(d)$ be the circle with centre $(\alpha, \beta+2)$,
- $u_2(d)$ be the circle with centre $(\alpha+\sqrt{3}, \beta+1)$,
- $u_3(d)$ be the circle with centre $(\alpha+\sqrt{3}, \beta-1)$,
- $u_4(d)$ be the circle with centre $(\alpha, \beta-2)$,
- $u_5(d)$ be the circle with centre $(\alpha-\sqrt{3}, \beta-1)$,
- $u_6(d)$ be the circle with centre $(\alpha-\sqrt{3}, \beta+1)$.

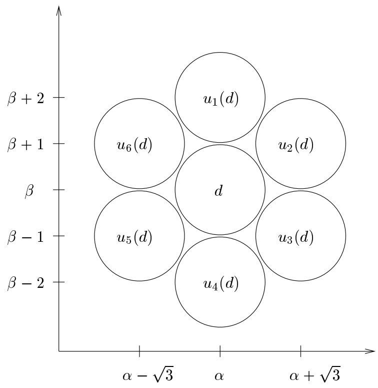

Figure 1: The neighbours of $d \in C$

Lemma 2. *For each i, $1 \le i \le 6$, each circle $d \in C$ intersects $u_i(d)$ at vertex $v_i(d)$.*

Definition 3. Let $d \in C$ with centre (α, β). We define x_d, y_d and z_d to be arcs on the circumference of d given by:

- $x_d = \{(\alpha + \cos\theta, \beta + \sin\theta) \mid 7\pi/6 \le \theta \le 11\pi/6\}$,
- $y_d = \{(\alpha + \cos\theta, \beta + \sin\theta) \mid -\pi/6 \le \theta \le \pi/2\}$,
- $z_d = \{(\alpha + \cos\theta, \beta + \sin\theta) \mid \pi/2 \le \theta \le 7\pi/6\}$.

(See Figure 2.)

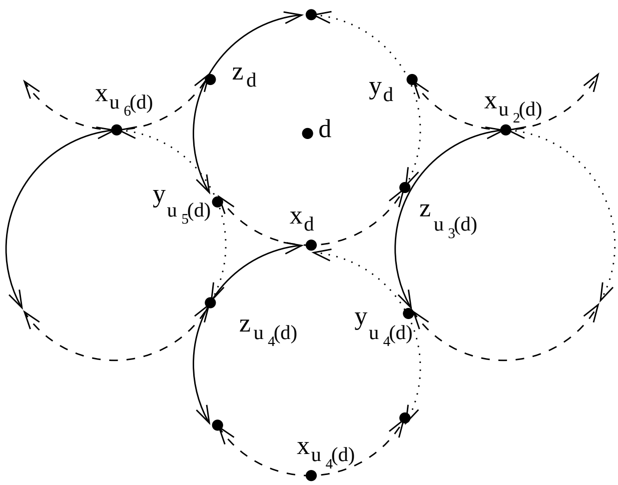

Figure 2

Definition 4. Let $f : C \to N(= N(m))$ where $m \geq 3$. We say that f is *coherent* if for each i, $1 \leq i \leq 6$, $f(d) = f(d')$ implies $f(u_i(d)) = f(u_i(d'))$, for each $d, d' \in C$. (In other words, if two circles d and d' have the same labelling, then $u_i(d)$ and $u_i(d')$ have the same labelling, for each $1 \leq i \leq 6$.)

Definition 5. Let $f : C \to N = (N(m))$, where $m \geq 3$. We say that f is *proper* if for each i, $1 \leq i \leq 6$, $f(d) \neq f(u_i(d))$. (In other words, a coherent labelling is proper if we do not apply the same label to any pair of adjacent circles.)

Definition 6. Let f be a coherent, proper, onto labelling $f : C \to N(= N(m))$. Let $\star$ be a binary operation $R(N) \times C(N) \to E(N)$ defined as follows: $r_i \star c_j = e_k$ if there exist circles $d, d', d'' \in C$ such that $f(d) = i$, $f(d') = j$, $f(d'') = k$, $x_d \cap y_{d'} \cap z_{d''} = \emptyset$, but $x_d \cap y_{d'} = \{(w_1, w_1')\}$, $x_d \cap z_{d''} = \{(w_2, w_2')\}$, and $y_{d'} \cap z_{d''} = \{(w_3, w_3')\}$, where $(w_1, w_1'), (w_2, w_2'), (w_3, w_3') \in \mathbb{R} \times \mathbb{R}$. Otherwise, $r_i \star c_j$ is undefined.

The following lemma is verified on inspection of Figure 2.

Lemma 7. *Let f be a coherent, proper, onto labelling $f : C \to N$ and let $\star$ be defined as in Definition 6. Then $r_i \star c_j = e_k$ if and only if there exist circles d, d' and d'' such that $f(d) = i$, $f(d') = j$, $f(d'') = k$ and either:*
Case 1. *$d = d' = d''$, or*
Case 2. *$d' = u_4(d)$ and $d'' = u_3(d)$, or*
Case 3. *$d' = u_5(d)$ and $d'' = u_4(d)$.*

Proof of the following theorem may be found in [8].

Theorem 8. *Let $\star$ be the operation given in Definitions 6. The set of triples $T = \{(r_i, c_j, r_i \star e_j) \mid r_i \star c_j \text{ is defined } \}$ is a latin trade of size $3m$. Moreover, this latin trade is 3-homogeneous.*

4. Some onto, coherent, proper maps and the corresponding latin trades

Next we give a general form of an onto, coherent and proper mapping $f : C \to N(m_2) \times N(m_1)$. (Henceforth we assume that, in general, $N(m) = \{0, 1, 2 \ldots, m-1\}$.) Furthermore we give, algebraically, the exact elements of the 3-homogeneous latin trades that arise from this mapping.

Definition 9. Let m_1, m_2 and k be integers such that $m_1 \geq 2$, $0 \leq k < m_1$, $m_2 \geq 1$ and if $m_2 = 1$, $m_1 \geq 3$ and $2 \leq k$. Then we define a mapping $f : C \to N(m_2) \times N(m_1)$ such that if $d \in C$ has centre (α, β), then $f(d) = (\eta(d), \omega(d))$, where

$$\delta(d) = \alpha/\sqrt{3} \ (\text{div } m_2),$$
$$\omega(d) = \delta(d)k - (\beta + \alpha/\sqrt{3})/2 \ (\text{mod}\, m_1) \text{ and}$$
$$\eta(d) = \alpha/\sqrt{3} \ (\text{mod}\, m_2).$$

Proof of the following lemma may be found in [8]. (In [8], f is mapped onto $N(m_2m_1)$ rather than $N(m_2) \times N(m_1)$. However this change is cosmetic, and has been made to simplify what follows.)

Lemma 10. *The function $f : C \to N(m_2) \times N(m_1)$, as given in Definition 9, is an onto, proper, coherent labelling.*

Lemma 11. *Let $f : C \to N(m_2) \times N(m_1)$ be an onto, proper, coherent labelling, as given in Definition 9. Then for each circle $d \in C$,*

1. $f(u_4(d)) = (\eta(d), \omega(d) + 1 \pmod{m_1})$;
2. $f(u_3(d)) = (\eta(d) + 1, \omega(d))$ *if* $0 \leq \eta(d) < m_2 - 1$;
3. $f(u_3(d)) = (0, \omega(d) + k \pmod{m_1})$ *if* $\eta(d) = m_2 - 1$;
4. $f(u_5(d)) = (m_2 - 1, \omega(d) - k + 1 \pmod{m_1})$ *if* $\eta(d) = 0$;
5. $f(u_5(d)) = (\eta(d) - 1, \omega(d) + 1 \pmod{m_1})$ *if* $\eta(d) > 0$.

Proof: Let $d \in C$ have centre (α, β).

Then $u_4(d)$ has centre $(\alpha, \beta - 2)$. Thus $\eta(u_4(d)) = \eta(d)$, and $\omega(u_4(d)) = \omega(d) + 1 \pmod{m_1}$.

Next, the circle $u_3(d)$ has centre $(\alpha + \sqrt{3}, \beta - 1)$. Then $\eta(u_3(d)) = \eta(d) + 1 \pmod{m_2}$. If $\eta(d) < m_2 - 1$, then $\alpha/\sqrt{3} \pmod{m_2} < m_2 - 1$, which implies that $\delta(d) = \delta(u_3(d))$. Thus $\omega(d) = \omega(u_3(d))$ in this case. Otherwise $\eta(d) = m_2 - 1$, $\alpha/\sqrt{3} \equiv m_2 - 1 \pmod{m_2}$, $\delta(u_3(d)) = \delta(d) + 1$, $\eta(u_3(d)) = 0$ and $\omega(u_3(d)) \equiv \omega(d) + k \pmod{m_1}$.

Next, the circle $u_5(d)$ has centre $(\alpha - \sqrt{3}, \beta - 1)$. If $\eta(d) = 0$, then $\alpha/\sqrt{3} \equiv 0 \pmod{m_2}$, $\eta(u_5(d)) = m_2 - 1$, $\delta(u_5(d)) = \delta(d) - 1$ and $\omega(u_5(d)) \equiv \omega(d) - k + 1 \pmod{m_1}$. Otherwise $\eta(d) \geq 1$, $\alpha/\sqrt{3} \pmod{m_2} \geq 1$, $\eta(u_5(d)) = \eta(d) - 1$, $\delta(u_5(d)) = \delta(d)$ and $\omega(u_5(d)) = \omega(d) + 1 \pmod{m_1}$. □

The next lemma gives us an exact expression of the elements of a 3-homogeneous latin trade constructed from the proper, onto, coherent map in Definition 9.

Lemma 12. *Let $f : C \to N(m_2) \times N(m_1)$ be an onto, proper, coherent labelling, as given in Definition 9. Then the corresponding operation $\star$, as given in Definition 6, is defined exactly in the following five cases:*

1. $r_{(i,j)} \star c_{(i,j)} = e_{(i,j)}$ $((i,j) \in N(m_2) \times N(m_1))$;
2. $r_{(i,j)} \star c_{(i,j+1 (\mathrm{mod}\, m_1))} = e_{(i+1,j)}$ $(0 \leq i < m_2 - 1, j \in N(m_1))$;
3. $r_{(i,j)} \star c_{(i,j+1 (\mathrm{mod}\, m_1))} = e_{(0,j+k (\mathrm{mod}\, m_1))}$ $(i = m_2 - 1, j \in N(m_1))$;
4. $r_{(i,j)} \star c_{(m_2-1,j-k+1 (\mathrm{mod}\, m_1))} = e_{(i,j+1 (\mathrm{mod}\, m_1))}$ $(i = 0; j \in N(m_1))$;
5. $r_{(i,j)} \star c_{(i-1,j+1 (\mathrm{mod}\, m_1))} = e_{(i,j+1 (\mathrm{mod}\, m_1))}$ $(0 < i \leq m_2 - 1; j \in N(m_1))$.

Proof: The proof is obtained by combining Lemma 7 and the previous lemma. □

5. Examples

Example 13. Here we construct a 3-homogeneous latin trade of size 9. Let $m_1 = 7$, $m_2 = 1$ and $k = 3$ as in Definition 9. So Lemma 10 tells us that f is a coherent, proper mapping onto $N(1) \times N(7)$. So from Lemma 12, we have that the following is a 3-homogeneous latin trade of size 21. (We omit the first subscript since this is always equal to 0).

$$\{(r_0, c_0, e_0), (r_1, c_1, e_1), (r_2, c_2, e_2), (r_3, c_3, e_3), (r_4, c_4, e_4), (r_5, c_5, e_5), (r_6, c_6, e_6),$$
$$(r_0, c_1, e_3), (r_1, c_2, e_4), (r_2, c_3, e_5), (r_3, c_4, e_6), (r_4, c_5, e_0), (r_5, c_6, e_1), (r_6, c_0, e_2),$$
$$(r_0, c_5, e_1), (r_1, c_6, e_2), (r_2, c_0, e_3), (r_3, c_1, e_4), (r_4, c_2, e_5), (r_5, c_3, e_6), (r_6, c_4, e_0).\}$$

In fact, the 3-homogeneous latin trade may be embedded into $(\mathbb{Z}_2)^3$, if we let:

$$r_0 = (0,0,0), c_0 = (0,0,0), e_0 = (0,0,0), r_1 = (1,1,0), c_1 = (1,0,0), e_1 = (0,1,0),$$
$$r_2 = (1,0,0), c_2 = (1,0,1), e_2 = (0,0,1), r_3 = (1,1,1), c_3 = (0,1,1), e_3 = (1,0,0),$$
$$r_4 = (0,1,0), c_4 = (0,0,1), e_4 = (0,1,1), r_5 = (1,0,1), c_5 = (0,1,0), e_5 = (1,1,1),$$
$$r_6 = (0,0,1), c_6 = (1,1,1), e_6 = (1,1,0).$$

Example 14. By now we have encountered two 3-homogeneous latin trades that occur in the multiplication tables for $(\mathbb{Z}_2)^n$ for some integer n: one in the previous example and one in the introduction. Now, we give an example of how we can construct a general 3-homogeneous latin trade in $(\mathbb{Z}_2)^n$ (the value of n is determined by our construction). This technique will be generalised in the following section.

Let us return to the packing of circles C from the previous section for a moment. We will give a proper, coherent, onto function $f : C :\to N(m_2) \times N(m_1)$ as in Definition 9 for some values of m_1, m_2 and k. For now we just assume that $m_1 = 2$ and $m_2 > 1$. We assign to $c_{(0,0)}$, $e_{(0,0)}$, $c_{(0,1)}$ and $e_{(0,1)}$ the vectors $(0,0)$, $(0,0)$, $(0,1)$ and $(1,0)$, respectively, from $(\mathbb{Z}_2)^2$. (See the left-hand-side of Figure 3.)

We henceforth assume that the $\star$ operation is equivalent to addition of vectors modulo 2. Lemma 12 tells us that $r_{(0,0)} \star c_{(0,0)} = e_{(0,0)}$ and $r_{(0,1)} \star c_{(0,1)} = e_{(0,1)}$. Thus $r_{(0,0)} = (0,0)$ and $r_{(0,1)} = (1,1)$.

Since $m_2 \geq 1$, the value $e_{(1,0)}$ must be defined. Case 2 of Lemma 12 tells us that $r_{(0,0)} \star c_{(0,1)} = e_{(1,0)}$, so $e_{(1,0)} = r_{(0,0)} + c_{(0,1)} = (0,1)$. Similarly, $e_{(1,1)} = r_{(0,1)} + c_{(0,0)} = (1,1)$. Next, Case 5 of Lemma 12 tells us that $r_{(1,0)} \star c_{(0,1)} = e_{(1,1)}$ and $r_{(1,1)} \star c_{(0,0)} = e_{(1,0)}$, so $r_{(1,0)} = (1,0)$ and $r_{(1,1)} = (0,1)$. From Case 1 of Lemma 12, $c_{(1,0)} = r_{(1,0)} + e_{(1,0)} = (1,1)$ and $c_{(1,1)} = r_{(1,1)} + e_{(1,1)} = (1,0)$.

So far, the sets

$$\{r_{(0,0)}, r_{(0,1)}, r_{(1,0)}, r_{(1,1)}\}, \{c_{(0,0)}, c_{(0,1)}, c_{(1,0)}, c_{(1,1)}\} \text{ and } \{e_{(0,0)}, e_{(0,1)}, e_{(1,0)}, e_{(1,1)}\}$$

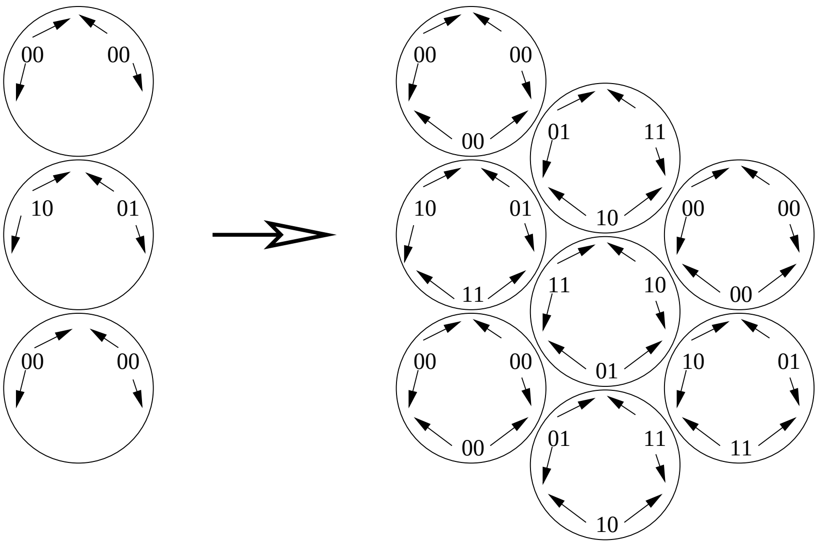

Figure 3: Our example, as seen in the circle packing

are each of size 4 (i.e. they each contain distinct elements).

Let d be a circle such that $f(d) = (1,0)$. Presently the value of $f(u_3(d))$ is undefined; however if we continue to assume that the $\star$ operation is addition modulo 2, we can infer what $f(u_3(d))$ *should* be. From Lemma 7, $r_{f(d)} + c_{f(u_4(d))} = e_{f(u_3(d))}$. Thus $e_{f(u_3(d))} = r_{(1,0)} + c_{(1,1)} = (1,0) + (1,0) = (0,0) = e_{(0,0)}$. So, if we want all elements distinct in our resultant latin trade, we must set $f(u_3(d)) = (0,0)$. In fact, continuing in this fashion induces a labelling of the circles that is as in Definition 9, with $k = 0$ and $m_2 = 2$. (Figure 3 shows this process in terms of the circle packing, with arcs x_d, y_d and z_d replaced by $r_{f(d)}$, $c_{f(d)}$ and $e_{f(d)}$, respectively, for each circle d.) Because the above sets of vectors are distinct, we have a latin trade that occurs in $(\mathbb{Z}_2)^n$ as follows.

$$\{((0,0),(0,0),(0,0)),((1,1),(0,1),(1,0)),((1,0),(1,1),(0,1)),((0,1),(1,0),(1,1)),$$
$$((0,0),(0,1),(0,1)),((1,1),(0,0),(1,1)),((1,0),(1,0),(0,0)),((0,1),(1,1),(1,0)),$$
$$((0,0),(1,0),(1,0)),((1,1),(1,1),(0,0)),((1,0),(0,1),(1,1)),((0,1),(0,0),(0,1))\}.$$

In fact, this latin trade is isotopic to the one given in the introduction.

In Sections 6 and 7 we generalise this idea. It turns out if we start off with a set of linearly independent vectors $\{e_{(0,j)}, c_{(0,j)} \mid 0 \leq j \leq m_1 - 1\}$ we can always "generate" a latin trade in $(\mathbb{Z}_2)^n$ (for some n), in a manner similar to this example.

6. Polynomial matrices

The idea of the next two sections is to obtain a coherent, proper labelling of the hexagonal lattice in the plane (and thus a 3-homogeneous latin trade) by taking a set of linearly independent vectors in $(\mathbb{Z}_2)^{2n}$ and letting the $\star$ operation from Section 3 be the equivalent of the addition of vectors modulo 2. We will thus generalise the example given in the previous section.

First we give a matrix that will act as a kind of "transition matrix" from the set of vectors corresponding to one column of circles in the plane to the set of vectors corresponding to the next column of circles in the plane. In the next section, the transition matrix will be a $2n \times 2n$ matrix over $\mathbb{Z}_2$. However we need to verify various properties of this matrix before being able to define an embedding of certain 3-homogeneous trades into abelian 2-groups. Thus in this section we will initially work with an isomorphic, 2×2 matrix whose entries are polynomials with coefficients in $\mathbb{Z}_2$, calculated modulo $x^n + 1$. The motivation for this alternative representation is to make the initial proofs nicer to read.

The elementary properties of matrices in this section may be found in Lütkepohl's very useful "Handbook of Matrices" ([24]).

Definition 15. Let $P_n(x)$ be the set of polynomials with coefficients from $\mathbb{Z}_2$, maximum degree $n-1$, with addition and multiplication calculated modulo $(x^n + 1)$.

Unless otherwise stated, all polynomials in this section lie in $P_n(x)$.

Definition 16. Let Q be the set of polynomial matrices of dimension 2×2 with elements from $P_n(x)$.

The following lemma is trivial to verify.

Lemma 17. *The set Q, with operations $+$ and $\times$ as matrix multiplication, is a commutative ring with a multiplicative identity.*

In fact Q is almost a field, except that some elements lack multiplicative inverses. We denote the multiplicative identity by I.

Definition 18. For each a, $0 \le a \le n-1$, define $I_n(a)$ to be the $n \times n$ matrix with the entry in position (i, j) equal to 1 if $j - i = a$, and 0 otherwise. (We denote the first row/column of a matrix by zero.) So for example $I_n(0) = I$ is the identity matrix.

The following lemma is easy to verify, with the observation that $I_n(a)I_n(b) = I_n(c)$, where $c \equiv a + b \pmod{n}$.

Lemma 19. *The set of matrices $H = \sum_{a=0}^{n-1} \delta_a I_n(a)$, where each $\delta_a \in \{0, 1\}$, forms a commutative ring with multiplicative identity under normal matrix addition and multiplication, where each entry of the matrix is calculated modulo 2. In fact there is an isomorphism $h : P_n(x) \to H$, given by $h(\sum \delta_i x^i) = \sum \delta_i I_n(i)$.*

Ultimately we will be working over C rather than $P_n(x)$, but the preliminary results are tidier to verify in $P_n(x)$, hence our choice of this representation.

Definition 20. Let $A \in Q$ be the following matrix:

$$A = \begin{bmatrix} 1 & x+1 \\ x+1 & x^2+x+1 \end{bmatrix}.$$

Lemma 21. *Let A be as in the previous definition. Then A has an inverse, which is given by*

$$A^{-1} = \begin{bmatrix} x^{n-1}+1+x & x^{n-1}+1 \\ x^{n-1}+1 & x^{n-1} \end{bmatrix}.$$

PROOF: Observe that $A \times A^{-1} = I$. □

Lemma 22. *The matrix A^m has the following form:*

$$A^m = \begin{bmatrix} q_m(x) & p_m(x) \\ p_m(x) & q_m(x)+xp_m(x) \end{bmatrix},$$

for some $p_m(x), q_m(x) \in P_n(x)$, such that $q_m(x)^2+xp_m(x)q_m(x)+p_m(x)^2 = x^m$.

PROOF: We use a proof by induction. It is easy to check the result is true for $x = 1$. So assume the result is true for $x = k$, for some integer $k \geq 1$. Then, (writing p_k instead of $p_k(x)$ and q_k instead of $q_k(x)$),

$$\begin{aligned} A^{k+1} &= \begin{bmatrix} q_k & p_k \\ p_k & q_k+xp_k \end{bmatrix} \times \begin{bmatrix} 1 & x+1 \\ x+1 & x^2+x+1 \end{bmatrix}, \\ &= \begin{bmatrix} q_k+p_k+xp_k & q_k+xq_k+p_k+xp_k+x^2p_k \\ q_k+xq_k+p_k+xp_k+x^2p_k & p_k+x^2p_k+x^3p_k+q_k+xq_k+x^2q_k \end{bmatrix}. \end{aligned}$$

So let $q_{k+1} = q_k+p_k+xp_k$ and let $p_{k+1} = q_k+xq_k+p_k+xp_k+x^2p_k$, and we have:

$$A^{k+1} = \begin{bmatrix} q_{k+1}(x) & p_{k+1}(x) \\ p_{k+1}(x) & q_{k+1}(x)+xp_{k+1}(x) \end{bmatrix}.$$

The fact that $q_m(x)^2+xp_m(x)q_m(x)+p_m(x)^2 = x^m$, for each integer m, is most easily verified by the fact that $\det(A^m) = (\det(A))^m = x^m$. □

Lemma 23. *There exists a least integer k such that A^k is equal to the identity matrix.*

PROOF: This follows from the fact that A has an inverse (Lemma 21). □

Corollary 24. *There exists an integer k such that $p_k(x) \equiv 0$ (modulo $x^n + 1$) and $q_k(x) \equiv x^l$ (modulo $x^n + 1$) for some integer l.*

Definition 25. Let $\mathrm{ord}(n)$ be the least integer k such that A^k is the identity. Let $\gamma(n)$ be the least integer k such that $p_k(x) \equiv 0$ (modulo x^n+1) and $q_k(x) = x^{r(n)}$ for some integer $r(n)$.

Lemma 26. *The set of matrices of the form A^k, where $p_k(x) \equiv 0$ (modulo x^n+1) and $q_k(x) = x^c$ for some integer c form a group under multiplication. Moreover, this group is cyclic, with generator $A^{\gamma(n)}$.*

PROOF: Any such matrix A^k has an inverse, given by:

$$\begin{bmatrix} x^{n-c} & 0 \\ 0 & x^{n-c} \end{bmatrix}.$$

The result follows. □

Corollary 27. *If k is any integer such that $p_k(x) = 0$, then $\gamma(n)|k$.*

Open problem 28. Determine explicitly the form of A^m for any integer m. Or, more specifically for our purposes, determine $\gamma(n)$ for each integer n.

We next solve this problem when n is an even power. The following lemma is easily verified.

Lemma 29. *For any integer k,*

$$A^{2k} = (A^k)^2 = \begin{bmatrix} q_k(x)^2 + p_k(x)^2 & x(p_k(x)^2) \\ x(p_k(x))^2 & q_k(x)^2 + p_k(x)^2 + (xp_k(x))^2 \end{bmatrix}.$$

In fact, we can give explicitly the form of A^k, where k is any power of two, as shown in the next lemma.

Lemma 30. *Let $k = 2^a$, for some integer $a \geq 0$. Then,*

$$p_k(x) = x^{2^a-1}(x^{2^a}+1) \quad \textit{and}$$
$$q_k(x) = x^{2^{a+1}-2} + \sum_{b=1}^{a-1}(x^{(2^{a-b})(2^b-1)} + x^{(2^{a+1-b})(2^b-1)}).$$

PROOF: First we show that $p_k(x) = x^{2^a-1}(x^{2^a}+1)$ by induction. This is clearly true for $a = 0$. Assume it is true for some $a \geq 0$. From the previous lemma, $p_{2k}(x) = x(x^{2^a-1}(x^{2^a}+1))^2 = x^{2^{a+1}-1}(x^{2^{a+1}}+1)$. This completes the induction.

Next we verify that $q_k(x) = x^{2^{a+1}-2} + \sum_{b=1}^{a-1}(x^{(2^{a-b})(2^b-1)} + x^{(2^{a+1-b})(2^b-1)})$ by induction. If $a = 0$, $q_k(x) = 1$, which is true. So assume it is true for some $a \geq 0$. Then from the previous lemma

$$\begin{aligned}
q_{2k}(x) &= p_k(x)^2 + q_k(x)^2 \\
&= (x^{2(2^a-1)} + x^{2^{a+2}-2}) + x^{4(2^a-1)} + \sum_{b=1}^{a-1}(x^{(2^{a-b+1})(2^b-1)} + x^{(2^{a+2-b})(2^b-1)}) \\
&= x^{2^{a+2}-2} + \sum_{b=1}^{a}(x^{(2^{a+1-b})(2^b-1)} + x^{(2^{a+2-b})(2^b-1)}),
\end{aligned}$$

completing the induction. □

Corollary 31. *If n is an even power, $\gamma(n) = n$ and $r(n) = 0$.*

Proof: Let $n = 2^a$ for some integer $a \geq 1$. From the previous lemma, $p_n(x) = 0$, and

$$\begin{aligned}
q_n(x) &= x^{2^{a+1}-2} + \sum_{b=1}^{a-1}(x^{(2^{a-b})(2^b-1)} + x^{(2^{a+1-b})(2^b-1)}) \\
&= x^{2^{a+1}-2} + x^{2^a} + x^{2^a-2} + \sum_{b=1}^{a-2}(x^{(2^{a-b})(2^b-1)} + x^{(2^{a-b})(2^{b+1}-1)}).
\end{aligned}$$

But $x^{(2^{a-b})(2^{b+1}-1)} = x^{(2^{a-b})(2^b+2^b-1)} = x^{2^a}x^{2^{a-b}(2^b-1)} = x^{2^{a-b}(2^b-1)}$ since we are working modulo $x^{2^a}+1$. Thus the terms in the sum all cancel, and $q_n(x) = x^{2^{a+1}-2} + x^{2^a} + x^{2^a-2} = x^{2^a}x^{2^a-2} + x^{2^a} + x^{2^a-2} = 1 = x^0$.

From Corollary 27, $\gamma(n)|n$. But for all b such that $b < a$, $p_{2^b}(x) = x^{2^{b+1}-1} + x^{2^b-1}$, which is not equivalent to 0 (modulo x^n). Thus $m(2^a) = 2^a$ and $r(n) = 0$. □

7. Embeddings in the abelian 2-group

Now we are ready to demonstrate precisely some embeddings of 3-homogeneous latin trades into abelian 2-groups. First we give some definitions and lemmas that allow us to make use of the polynomial matrix theory from the previous section.

Definition 32. If $p(x) \in P_n(x)$ and $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$, we can associate with $p(x)$ a vector $v(p(x)) = (a_0, a_1, \ldots, a_{n-1})$, where $a_i \in \mathbb{Z}_2$, for each i, $1 \leq i \leq n$. We also define an operation $\oplus$ that concatenates two vectors; that is, if $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_n)$, then $a \oplus b = (a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n)$.

Definition 33. Let $C \in Q$, with

$$C = \begin{bmatrix} a(x) & b(x) \\ c(x) & d(x) \end{bmatrix}.$$

We define a matrix $\omega(C) = M_{2n\times 2n}(\mathbb{Z}_2)$ as follows. Row i of this matrix is equal to $v(x^i a(x)) \oplus v(x^i b(x))$ for $0 \leq i \leq n-1$ and row i is equal to $v(x^i c(x)) \oplus v(x^i d(x))$ for $n \leq i \leq 2n-1$. (We take the convention of labelling the first row of a matrix as row 0.) So,

$$\omega(C) = \begin{bmatrix} v(a(x)) \oplus v(b(x)) \\ v(xa(x)) \oplus v(xb(x)) \\ \vdots \quad \vdots \\ v(x^{n-1}a(x)) \oplus v(x^{n-1}b(x)) \\ v(c(x)) \oplus v(d(x)) \\ v(xc(x)) \oplus v(xd(x)) \\ \vdots \quad \vdots \\ v(x^{n-1}c(x)) \oplus v(x^{n-1}d(x)) \end{bmatrix}.$$

Example 34. For $n = 3$,

$$\omega(A) = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Lemma 35. *The mapping ω is an isomorphism from the group $(\{A^k \mid k \in \mathbb{Z}\}, \times)$ to the group $(\{(\omega(A))^k \mid k \in \mathbb{Z}\}, \times)$.*

PROOF: Observe that to construct $w(C)$ from C, we replace each element $\sum \delta_i x^i \in P_n(x)$ of C by the matrix $\sum \delta_i I_n(i) \in H$. The result then follows from the isomorphism given in Lemma 19. □

Lemma 36. *Let $B \in M_{2n\times 2n}(\mathbb{Z}_2)$ be a matrix whose rows are linearly independent. Then the rows of $(\omega(A))^m B$ are linearly independent, for any integer m.*

PROOF: First we show that if the rows of B are linearly independent, then the rows of $(\omega(A))B$ are linearly independent. The general result then follows recursively.

So let the rows of B be $b_0, b_1, \ldots, b_{2n-1}$ and let the rows of $(\omega(A))(B)$ be $c_0, c_1, \ldots, c_{2n-1}$. Then,

$$c_i = \begin{cases} b_i + b_{n+i} + b_{(i+1)(\mathrm{mod}\, n)+n} (\text{ if } 0 \leq i \leq n-1); \\ b_{i-n} + b_{(i+1)(\mathrm{mod}\, n)} + b_i + b_{(i+1)(\mathrm{mod}\, n)+n} + b_{(i+2)(\mathrm{mod}\, n)+n} \\ \qquad (\text{if } n \leq i \leq 2n-1). \end{cases}$$

Now suppose that the rows of $(\omega(A))(B)$ are not linearly independent.

That is, $\sum_{i=0}^{2n-1} \epsilon_i c_i = 0$ for some $\epsilon_i \in \mathbb{Z}_2$. Or, equivalently,

$$\sum_{i=0}^{n-1} \epsilon_i (b_i + b_{n+i} + b_{((i+1)(\mathrm{mod}\, n)+n)}) +$$
$$\sum_{i=n-1}^{2n-1} \epsilon_i (b_{i-n} + b_{(i+1)(\mathrm{mod}\, n)} + b_i + b_{((i+1)(\mathrm{mod}\, n)+n)} + b_{((i+2)(\mathrm{mod}\, n)+n)}) = 0.$$

But since

$$\sum_{i=0}^{n-1} \epsilon_i b_{n+i} = \sum_{i=0}^{n-1} \epsilon_i b_{(i+1)(\mathrm{mod}\, n)+n},$$
$$\sum_{i=n}^{2n-1} \epsilon_i b_{i-n} = \sum_{i=n}^{2n-1} \epsilon_i b_{(i+1)(\mathrm{mod}\, n)}$$

and

$$\sum_{i=n}^{2n-1} \epsilon_i b_{(i+1)(\mathrm{mod}\, n)+n} = \sum_{i=n}^{2n-1} \epsilon_i b_{(i+2)(\mathrm{mod}\, n)+n},$$

and because we are working over $\mathbb{Z}_2$, we can cancel terms to obtain $\sum_{i=0}^{2n-1} \epsilon_i b_i = 0$, contradicting the linear independence of the rows of B. □

The following lemma facilitates the reader in comprehending the connection between a matrix $C \in Q$ and the matrix $w(C)$ in the proofs that follow.

Lemma 37. *Let B be a $2n \times 2n$ matrix with rows $r_0, r_1, \dots r_{2n-1}$. Let $\delta_i \in \{0,1\}$, for $0 \le i \le 2n-1$. Then*

$$(v(\sum_{i=0}^{n-1} \delta_i x^i) \oplus v(\sum_{j=0}^{n-1} \delta_j x^j))B$$

is equal to the following sum of rows in B:

$$\sum_{i=0}^{n-1} \delta_i r_i + \sum_{j=0}^{n-1} \delta_{n+j} r_j.$$

Definition 38. Let $B \in M_{2n\times 2n}(\mathbb{Z}_2)$ be a matrix whose rows are linearly independent. Let $a_{(i,j)}$, $b_{(i,j)} \in (\mathbb{Z}_2)^{2n}$ be row j, $n+j$ (respectively) of the matrix $(\omega(A))^i B$, where $0 \le i \le \gamma(n) - 1$ and $0 \le j \le n-1$. (Here we count the first row of a matrix as row zero.)

Lemma 39. *The set of vectors* $\{a_{(i,j)} \mid (i,j) \in N(\gamma(n)) \times N(n)\}$ *are distinct. The set of vectors* $\{b_{(i,j)} \mid (i,j) \in N(\gamma(n)) \times N(n)\}$ *are distinct. The set of vectors* $\{a_{(i,j)} + b_{(i,j)} \mid (i,j) \in N(\gamma(n)) \times N(n)\}$ *are distinct.*

PROOF: First we show that the set of vectors $\{a_{(i,j)} \mid (i,j) \in N(\gamma(n)) \times N(n)\}$ are distinct. Suppose that $a_{(i,j)} = a_{(i',j')}$. The rows of B are linearly independent, so from the previous lemma, if $i = i'$ then $j = j'$.

Next suppose, without loss of generality that $i' > i$. Then row j of the matrix $(\omega(A))^i B$ is equal to row j' of the matrix $(\omega(A))^{i'} B$. Equivalently, since $\omega(A)$ has an inverse, row j' of $(\omega(A))^{i-i'} B$ is equal to row j of B.

Let $k = i - i'$, and observe that k is strictly less than $\gamma(n)$. So from Lemma 22 and Lemma 37, we have $(v(x^{j'} q_k(x)) \oplus v(x^{j'} p_k(x)))B$ is equal to row j of B. But also from Lemma 37, row j of B is equal to $(v(x^j) \oplus v(0))B$. Since the rows of B are linearly independent, we have $x^{j'} q_k(x) = x^j$ and $x^{j'} p_k(x) = 0$. Thus $p_k(x) = 0$, and $q_k(x) = x^{j-j'}$, contradicting the minimality of $\gamma(n)$.

Next we show that the set of vectors $\{b_{(i,j)} \mid (i,j) \in N(\gamma(n)) \times N(n)\}$ are distinct. Suppose that $b_{(i,j)} = b_{(i',j')}$. As above, if $i = i'$ then $j = j'$, because of the previous lemma. Assume $i' > i$.

Also, by similar reasoning as above, we obtain row $j' + n$ of $(\omega(A))^k B$ is equal to row $j + n$ of B, for some $k < \gamma(n)$. So from Lemma 22 and Lemma 37 we have $v(x^{j'} p_k(x)) \oplus v(x^{j'}(x p_k(x) + q_k(x)))B$ is equal to $(v(0) \oplus v(x^j))B$. Since the rows of B are linearly independent, we have $x^{j'}(x p_k(x) + q_k(x)) = x^j$ and $x^{j'} p_k(x) = 0$. Thus $p_k(x) = 0$, and $q_k(x) = x^{j-j'}$, again contradicting the minimality of $\gamma(n)$.

Finally, we show that the set of vectors $\{a_{(i,j)} + b_{(i,j)} \mid (i,j) \in N(\gamma(n)) \times N(n)\}$ are distinct. Suppose that $a_{(i,j)} + b_{(i,j)} = a_{(i',j')} + b_{(i',j')}$. As above, if $i = i'$ then the previous lemma implies $j = j'$.

Also, by similar reasoning to above, we obtain row $j' + n$ plus row j' of $(\omega(A))^k B$ is equal to row $j + n$ plus row j of B, for some $k < \gamma(n)$. So we have $v(x^{j'}(q_k(x) + p_k(x))) \oplus v(x^{j'}((x+1)p_k(x) + q_k(x)))B$ is equal to row $j+n$ plus row j of B, which is in turn equal to $(v(x^j) \oplus v(x^j))B$. Since the rows of B are linearly independent, we have $x^{j'}(p_k(x) + q_k(x)) = x^j$ and $x^{j'}((x+1)p_k(x) + q_k(x)) = x^j$. Thus $p_k(x) = (x+1)p_k(x)$, which in turn implies that $p_k(x) = 0$. Also $q_k(x) = x^{j-j'}$, contradicting the minimality of $\gamma(n)$. □

The following four lemmata do the dirty work for the main theorem that follows.

Lemma 40. *Let* $0 \le i < \gamma(n)$ *and* $0 \le j \le n-1$. *Then*

$$a_{(i+1,j)} = a_{(i,j)} + b_{(i,j)} + b_{(i,j+1(\mathrm{mod}\, n))}.$$

PROOF: From Definition 38, $a_{(i+1,j)}$ is equal to the jth row in the matrix $(\omega(A))^{i+1} B = \omega(A)(\omega(A))^i B$. From the definition of A, we have that row j

of $(\omega(A))(\omega(A))^i B$ is equal to $(v(x^j) \oplus v(x^j(x+1)))(\omega(A))^i B$. This in turn (using Lemma 37) is equal to the sum of rows j, $n+j$ and $j+1 \pmod n + n$ in the matrix $(\omega(A))^i B$, that is, $a_{(i+1,j)} = a_{(i,j)} + b_{(i,j)} + b_{(i,j+1 (\mathrm{mod}\, n))}$. □

Lemma 41. *Let $0 < i < \gamma(n)$ and $0 \le j \le n-1$. Then*

$$b_{(i-1,j)} = a_{(i,j)} + a_{(i,j-1 (\mathrm{mod}\, n))} + b_{(i,j-1 (\mathrm{mod}\, n))}.$$

Proof: From Definition 38, $b_{(i-1,j)}$ is equal to the $(n+j)$th row in the matrix $(\omega(A))^{i-1}B = (\omega(A^{-1}))(\omega(A))^i B$. Observing the structure of A^{-1}, we have that row $n+j$ of $(\omega(A^{-1}))(\omega(A))^i B$ is equal to $(v(x^{j-1}+x^j) \oplus v(x^{j-1}))(\omega(A))^i B$. This in turn (using Lemma 37) is equal to the sum of rows j, $j-1 \pmod n$ and $j-1 \pmod n + n$ in the matrix $(\omega(A))^i B$, that is, $b_{(i-1,j)} = a_{(i,j)} + a_{(i,j-1 (\mathrm{mod}\, n))} + b_{(i,j-1 (\mathrm{mod}\, n))}$. □

Lemma 42. *Let $i = \gamma(n) - 1$ and $0 \le j \le n-1$. Then*

$$a_{(0,j+r(n) (\mathrm{mod}\, n))} = a_{(i,j)} + b_{(i,j)} + b_{(i,j+1 (\mathrm{mod}\, n))}.$$

Proof: Now, $i+1 = \gamma(n)$, so by the definition of $\gamma(n)$, $p_{i+1}(x) = 0$ and $q_{i+1}(x) = x^{r(n)}$. Thus row j of $(\omega(A))^{i+1}B$ is equal to $(v(x^{j+r(n) (\mathrm{mod}\, n)}) \oplus v(0))B$ which is equal to $a_{(0,j+r(n) (\mathrm{mod}\, n))}$, by Lemma 37. But row j of $(\omega(A)^{i+1})B$ is also equal to $(v(x^j) \oplus v(x^j(x+1)))(\omega(A))^i B$, which in turn is equal to $a_{(i,j)} + b_{(i,j)} + b_{(i,j+1 (\mathrm{mod}\, n))}$ as in Lemma 40. The result follows. □

Lemma 43. *Let $i = \gamma(n) - 1$ and $0 \le j \le n-1$. Then*

$$b_{(i,j-r(n)+1 (\mathrm{mod}\, n))} = a_{(0,j)} + b_{(0,j)} + a_{(0,j+1 (\mathrm{mod}\, n))}.$$

Proof: First, let $l = j - r(n) + 1 \pmod n$. Then, by definition, $b_{(i,l)}$ is equal to row $l+n$ of $(\omega(A))^i B = (\omega(A^{-1}))(\omega(A))^{i+1}B$. By observing the structure of A^{-1}, this is in turn equal to

$$(v(x^{l-1 (\mathrm{mod}\, n)} + x^l) \oplus v(x^{l-1 (\mathrm{mod}\, n)}))(\omega(A))^{i+1}B,$$

or, by Lemma 37, the sum of rows $l-1 \pmod n$, l and $l-1 \pmod n + n$ in $(\omega(A))^{i+1}B$. But $i+1 = \gamma(n)$, so row x of $(\omega(A))^{i+1}B$ will be $a_{(0,r(n)+x (\mathrm{mod}\, n))}$ or $b_{(0,r(n)+x (\mathrm{mod}\, n))}$, for $0 \le x \le n-1$ and $n \le x \le 2n-1$ respectively. Thus,

$$\begin{aligned} b_{(i,l)} &= a_{(0,l-1+r(n) (\mathrm{mod}\, n))} + a_{(0,l+r(n) (\mathrm{mod}\, n))} + b_{(0,l+r(n)-1 (\mathrm{mod}\, n))} \\ &= a_{(0,j)} + a_{(0,j+1 (\mathrm{mod}\, n))} + b_{(0,j)}, \end{aligned}$$

as required. □

Definition 44. Let $n \geq 2$, and $\gamma(n)$, $r(n)$, B, $a_{(i,j)}$, $b_{(i,j)}$ $(0 \leq i \leq \gamma(n)-1$, $0 \leq j \leq n-1)$ be as in previous definitions. Let f be an onto, coherent, proper map defined as in Lemma 9 with $m_1 = n$, $m_2 = \gamma(n)$ and $k = r(n) \pmod n$. (Clearly $\gamma(n) > 1$ for all $n \geq 2$, so these values of m_1, m_2 and k satisfy the conditions of Lemma 9.)

For each $(i,j) \in N(\gamma(n)) \times N(n)$, let $r_{(i,j)} = a_{(i,j)} + b_{(i,j)}$, $c_{(i,j)} = b_{(i,j)}$ and $e_{(i,j)} = a_{(i,j)}$. Let $\star$ be as defined in Definition 6, based on the onto, coherent, proper map $f : C \to N(\gamma(n)) \times N(n)$. Then let T_n be the set of triples $(r_{(i,i')}, c_{(j,j')}, e_{(k,k')})$ such that $r_{(i,i')} \star c_{(j,j')} = e_{(k,k')}$.

Theorem 45. *The set of triples T_n, as given in the previous definition, is a 3-homogeneous latin trade of size $3\gamma(n)n$ in the latin square for $(\mathbb{Z}_2)^{2n}$.*

Proof: Theorem 8 tells us that T_n is a 3-homogeneous latin trade. We need to show also that T_n embeds into $(\mathbb{Z}_2)^{2n}$. Then Lemma 39 tells us $|T_n| = 3\gamma(n)n$ as claimed. So it remains to be shown that $r_{(i,i')} \star c_{(j,j')} = e_{(k,k')}$ implies $r_{(i,i')} + c_{(j,j')} = e_{(k,k')}$ (or, equivalently, $a_{(i,i')} + b_{(i,i')} + b_{(j,j')} + a_{(k,k')} = 0$). This is done by a systematic checking of the cases from Lemma 12.

So take Case 1 from Lemma 12. Here $r_{(i,j)} \star c_{(i,j)} = e_{(i,j)}$, where $(i,j) \in N(\gamma(n)) \times N(n)$. We need $a_{(i,j)} + b_{(i,j)} + b_{(i,j)} + a_{(i,j)} = 0$, which holds trivially. Next Case 2 from Lemma 12: $r_{(i,j)} \star c_{(i,j+1 (\operatorname{mod} n))} = e_{(i+1,j)}$, where $0 \leq i < n-1$. We want to show that $a_{(i,j)} + b_{(i,j)} + b_{(i,j+1(\operatorname{mod} n))} + a_{(i+1,j)} = 0$. But from Lemma 40, $a_{(i+1,j)} = a_{(i,j)} + b_{(i,j)} + b_{(i,j+1(\operatorname{mod} n))}$ as required.

In Case 3 of Lemma 12, we have $r_{(i,j)} \star c_{(i,j+1(\operatorname{mod} n))} = e_{(0,j+r(n)(\operatorname{mod} n))}$, where $i = \gamma(n) - 1$ and $j \in N(n)$. Let $l = j + r(n) \pmod n$. Then from Lemma 42, $a_{(0,l)} = a_{(i,j)} + b_{(i,j)} + b_{(i,j+1(\operatorname{mod} n))}$. This is the desired result for this case.

Now for Case 4. Here $r_{(i,j)} \star c_{(\gamma(n)-1,j-r(n)+1(\operatorname{mod} n))} = e_{(i,j+1(\operatorname{mod} n))}$, where $i = 0$ and $j \in N(n)$. Let $l = j - r(n) + 1 \pmod n$. From Lemma 43, $b_{(\gamma(n)-1,l)} = a_{(0,j)} + b_{(0,j)} + a_{(0,j+1(\operatorname{mod} n))}$ as required.

Finally we have Case 5. Here $r_{(i,j)} \star c_{(i-1,j+1(\operatorname{mod} n))} = e_{(i,j+1(\operatorname{mod} n))}$, where $i > 0, j \in N(n)$. We need to show that $a_{(i,j)} + b_{(i,j)} + b_{(i-1,j+1(\operatorname{mod} n))} + a_{(i,j+1(\operatorname{mod} n))} = 0$. But $b_{(i-1,j+1(\operatorname{mod} n))} = a_{(i,j)} + b_{(i,j)} + a_{(i,j+1(\operatorname{mod} n))} = 0$ (from Lemma 41) as required. This completes the proof. □

Corollary 46. *There exists a 3-homogeneous latin trade of size $3k^2$ in the latin square $(\mathbb{Z}_2)^k$, where k is any even power.*

Proof: This corollary follows from Theorem 45 and Corollary 31. □

The following table gives values of $\gamma(n)$ and $r(n)$ for n up to 8, determined by computer, and lists the sizes and orders of the corresponding 3-homogeneous latin trades T_n.

n	$\gamma(n)$	$r(n)$	$\mathrm{ord}(n)$	$\|T_n\|$	2^{2n}
2	2	0	2	12	16
3	5	1	15	45	64
4	4	0	4	16	256
5	17	1	85	85	1024
6	10	2	30	60	4096
7	21	0	21	147	16384
8	8	0	8	64	65536

Table 1: Values of $\gamma(n)$, $r(n)$, $\mathrm{ord}(n)$, $|T_n|$ and 2^{2n} for $n \leq 8$

8. Open problems

There are many open questions and problems associated with the latin trades T_n. To determine $\gamma(n)$ for each n is one that is connected to the computations done in the paper in the most narrow way. However, there are other ones. For example, we know that T_n embeds into $(\mathbb{Z}_2)^{2n}$ (Theorem 45), but we do not know if $2n$ is the least possible value of m for which there exists an embedding of T_n into $(\mathbb{Z}_2)^m$. In fact, Example 14 shows that the condition that the rows of B are linearly independent is sufficient but not always necessary for our construction to work. The example in Example 13 also shows that our construction does not give all 3-homogeneous latin trades in $(\mathbb{Z}_2)^n$.

We may also think of the size of a latin trade T (with disjoint mate T') in $(\mathbb{Z}_2)^n$ as describing the *Hamming distance*

$$d((\mathbb{Z}_2)^n, L) = |(\mathbb{Z}_2)^n \setminus L|,$$

where $L = ((\mathbb{Z}_2)^n \setminus T) \cup T'$ is a latin square of order 2^n not equal to $(\mathbb{Z}_2)^n$.

The problem of determining the minimum Hamming distance $d((\mathbb{Z}_2)^n, L)$, for any integer n is trivial; $(\mathbb{Z}_2)^n$ contains many latin trades of size 4, which is the minimum size for a latin trade. However, the following problem may not be so trivial:

Open problem 47. What is the minimum value of $d((\mathbb{Z}_2)^n, L)$, where L is a latin square of order 2^n not equal to $(\mathbb{Z}_2)^n$ and L contains no subsquare isotopic to $(\mathbb{Z}_2)^{n-1}$?

We can pose an even stronger question, the answer to which (we believe) would need k-homogeneous trades, where k is in general much larger than 3.

Open problem 48. What is the minimum value of $d((\mathbb{Z}_2)^n, L)$, where L is a latin square of order 2^n not equal to $(\mathbb{Z}_2)^n$ and L contains no subsquare isotopic to $\mathbb{Z}_2$?

For $n = 2$ the answer is infinity, since every latin square of order 4 contains a 2×2 subsquare.

Another interesting problem (mentioned also in [8]) is the determination of k-homogeneous latin trades for $k > 3$. The techniques used in this paper could also be useful in locating 3-homogeneous latin trades in other groups. Of particular interest would be finding 3-homogeneous latin trades in B_n, the latin square based on addition modulo n, for various values of n. We are aware of 3-homogeneous latin trades in B_5 (see below) and B_{21} ([15]), but not of any infinite families of 3-homogeneous latin trades in B_n.

0	1	2		
1	2		4	
2		4	0	
	4	0	1	

Figure 4: A 3-homogeneous latin trade in B_5

The latin square B_n is of particular interest because it is conjectured that B_n yields critical sets of smallest possible size amongst all latin squares of order n, and that this size is $\lfloor n^2/4 \rfloor$ ([4]). In [7] it is shown that the size of a critical set in B_n must be at least $n^{4/3}/2$.

Finally, we note that the 3-homogeneous latin trade from Example 13 has a number of interesting properties. If we delete exactly one row, one column and one entry (such that the row, column and entry intersect in exactly one cell) from the latin square for $(\mathbb{Z}_2)^3$, the remaining elements can be partitioned into exactly two copies of this latin trade. In fact, in Figure 5 we show a critical set in $(\mathbb{Z}_2)^3$ of size 29 formed from one copy of the 3-homogeneous latin trade, plus almost all of the empty row, plus one additional element. (Note the minimum size for a critical set in $(\mathbb{Z}_2)^3$ is 25 [23].) The elements from the latin trade from Example 13 are shown in bold.

000		**010**		**100**			
001	**000**		010				**110**
	011	**000**			**111**		
011	010	001	000	111	110		100
100			**111**		**001**		
		111	**110**				**010**
				010	**011**		**001**
	110		**100**	**011**			

Figure 5: A critical set in $(\mathbb{Z}_2)^3$

Open problem 49. Using 3-homogeneous latin trades, k-homogeneous latin trades or otherwise, construct small (or even minimum) critical sets in $(\mathbb{Z}_2)^n$ and other latin squares.

References

[1] Adams P., Bean R., Khodkar A., *A census of critical sets in the latin squares of order at most six*, Ars Combin. **68** (2003), 203–223.

[2] Adams P., Khodkar A., *Smallest critical sets for the latin squares of order six and seven*, J. Combin. Math. Combin. Computing. **67** (2001), 225–237.

[3] Bates J.A., van Rees G.H.J., *The size of the smallest strong critical set in a latin square*, Ars Combin. **53** (1999), 73–83.

[4] Bate J.A., van Rees G.H.J., *Minimal and near-minimal critical sets in back circulant latin squares*, Australas. J. Combinatorics **27** (2003), 47–62.

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

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

[7] Cavenagh N.J., *The size of the smallest critical set in the back circulant latin square*, submitted.

[8] Cavenagh N.J., Donovan D., Drápal A., 3*-homogeneous latin trades*, submitted.

[9] Conway J.C., Sloane N.J., *Sphere Packings, Lattices and Groups*, New York, Springer-Verlag, 1998.

[10] Dénes J., Keedwell A.D., *Latin Squares and Their Applications*, English Universities Press, London, 1974.

[11] Donovan D., Howse A., Adams P., *A discussion of latin interchanges*, J. Comb. Math. Comb. Comput. **23** (1997), 161–182.

[12] Donovan D., Mahmoodian E.S., *An algorithm for writing any latin interchange as the sum of intercalates*, Bull. Inst. Combin. Appl. **34** (2002), 90–98.

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

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

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

[16] Drápal, Kepka T., *Exchangeable Groupoids I*, Acta Univ. Carolinae - Math. Phys. **24** (1983), 57–72.

[17] Drápal, Kepka T., *Exchangeable Groupoids II*, Acta Univ. Carolinae - Math. Phys. **26** (1985), 3–9.

[18] Drápal, Kepka T., *On a distance of groups and latin squares*, Comment. Math. Univ. Carolinae **30** (1989), 621–626.

[19] Hedayat A.S., *The theory of trade-off for t-designs*, in "Coding theory and design theory, Part II", IMA Vol. Math. Appl. 21, Springer, NY, 1990.

[20] Horak P., Aldred R.E.L., Fleischner H., *Completing Latin squares: critical sets*, J. Combin. Des. **10** (2002), 419–432.

[21] Keedwell A.D., *Critical sets and critical partial latin squares*, in "Proc. Third China-USA International Conf. on Graph Theory, Combinatorics, Algorithms and Applications", World Sci. Publishing, NJ, 1994.

[22] Keedwell A.D., *Critical sets for latin squares, graphs and block designs: A survey*, Congr. Numer. **113** (1996), 231–245.

[23] Khodkar A., *On smallest critical sets for the elementary abelian* 2*-group*, Utilitas Math. **54** (1998), 45–50.
[24] Lütkepohl H., *Handbook of Matrices*, Chichester, John Wiley and Sons, 1996.
[25] Street A.P., *Trades and defining sets*, in: C.J. Colbourn and J.H. Dinitz, Eds., CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL., 1996, pp. 474–478.

Institute for Theoretical Computer Science ITI, Charles University,
Malostranské nám. 25, 118 00 Praha 1, Czech Republic

(*Received* October 10, 2003, *revised* March 29, 2004)