

# Linear Codes Through Latin Squares Modulo $n$

Dinesh G. Sarvate and Alexander L. Strehl  
Department of Mathematics  
Department of Computer Science  
College of Charleston, SC  
email: sarvated@cofc.edu, alstrehl@edisto.cofc.edu

## Abstract

It is known that  $t$  mutually orthogonal latin squares of order  $n$  generate a  $\lfloor \frac{t}{2} \rfloor$ -error correcting code with  $n^2$  codewords. In this paper we consider latin squares of order  $n$  made up of elements taken from  $Z_n$ . In this situation we consider when this code is linear. We present necessary and sufficient conditions on the latin squares and obtain a method of constructing a maximal family of mutually orthogonal latin squares that form linear codes. In particular, we have shown that no pair of mutually orthogonal latin squares of even order generate a linear code.

## 1. Introduction

**Definition 1.1.** A matrix  $M$  is a **latin square of order  $n$**  (or an  $n \times n$  **latin square**) if its columns and rows are permutations of  $n$  fixed elements.

**Notation.** In the following discussion the rows and columns of an  $n \times n$  matrix are indexed by  $0, 1, 2, \dots, n - 1$ . All elements in the latin squares in this paper are from  $Z_n$ , where addition and multiplication are defined modulo  $n$ . Therefore, all operations performed on these elements, in this paper, are assumed to be performed modulo  $n$ , however we often state this explicitly for emphasis. Finally, for all latin squares of order  $n$  we assume  $n > 1$ .

**Definition 1.2.** Two  $n \times n$  latin squares  $A = \|a_{ij}\|$  and  $B = \|b_{ij}\|$  are

**orthogonal** if  $|\{ (a_{ij}, b_{ij}) \mid i, j \in \{0, 1, 2, \dots, n-1\}\}| = n^2$ . A set of  $t > 0$  latin squares are **pairwise mutually orthogonal** (or just **mutually orthogonal**) if every pair of latin squares in the set are orthogonal.

**Definition 1.3.** A code  $C$  is **linear** if the addition of any two codewords is another codeword.

Latin squares are dealt with extensively in Denes and Keedwell [1974]. In particular, they showed a method of constructing an error-correcting code of distance  $t + 1$  with  $n^2$  codewords of length  $t + 2$  when given  $t$  mutually orthogonal latin squares. Their method is as follows:

*Given  $t$  mutually orthogonal latin squares  $L_1, L_2, \dots, L_t$ , the code is the set of all codewords of the form  $(i, j, l_1, l_2, \dots, l_t)$  where  $l_1$  is the  $i, j$ -th entry of  $L_1$ ,  $l_2$  is the  $i, j$ -th entry of  $L_2$ , and  $l_k$  is the  $i, j$ -th entry of  $L_k$  where  $1 \leq k \leq t$ .*

This method of construction was also rediscovered by Kadowaki, Kageyama, Kimura, and Yanagida [2000]. In particular, they gave the following example of a perfect code (every vector is correctable) using two orthogonal latin squares of order 3.

With our notation the two latin squares are:

$$\begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}$$

The code constructed using these two is

$$\{(0, 0, 0, 0), (0, 1, 1, 1), (0, 2, 2, 2), (1, 0, 1, 2), (1, 1, 2, 0), (1, 2, 0, 1), (2, 0, 2, 1), (2, 1, 0, 2), (2, 2, 1, 0)\}$$

A noteworthy feature of this code is that it is also a linear code when addition and multiplication are defined modulo  $n$ . The question that arises naturally is when, if ever, do other linear codes result from this construction? When a code  $C$  results from applying the above method to some set of mutually orthogonal latin squares we say that these latin squares **generate**  $C$ . If  $C$  is a linear code we say that these latin squares **generate a linear code modulo  $n$** , where  $n$  is the order of the latin squares.

In this article we give the general structure of all latin squares that generate linear codes modulo  $n$ . Furthermore, we provide necessary and sufficient conditions for two such latin squares to be orthogonal. This completely characterizes all sets of mutually orthogonal latin squares of order

$n$  that generate linear codes modulo  $n$ . We also provide an upper bound on the number of mutually orthogonal latin squares that generate linear codes modulo  $n$ . Lastly, we show by construction that this upper bound is attainable.

## 2. Results

**Theorem 2.1.** *If an  $n \times n$  latin square  $L = \| l_{ij} \|$  generates a linear code modulo  $n$  then  $l_{00} = 0$ .*

**Proof.** Since  $L$  generates a linear code modulo  $n$  the addition of any two codewords is another codeword. Thus  $2(0, 0, l_{00}) = (0, 0, 2l_{00})$  is a codeword. However, this implies that  $l_{00} = 2l_{00}$ , which gives  $l_{00} = 0$ .  $\square$

**Lemma 2.1.** *An  $n \times n$  matrix  $L = \| l_{ij} \|$  of the form  $l_{ij} = (i\beta + j\alpha) \bmod n$  for some integers  $\alpha, \beta$  in the range  $0 < \alpha, \beta < n$  is a latin square iff  $\gcd(\alpha, n) = \gcd(\beta, n) = 1$ .*

**Proof.** First we show that if  $\{\gcd(\alpha, n), \gcd(\beta, n)\} \neq \{1\}$  then  $L = \| l_{ij} \|$  where  $l_{ij} = (i\beta + j\alpha) \bmod n$  is not a latin square. Assume  $\gcd(\alpha, n) > 1$ , then for some integer  $k$ ,  $0 < k < n$  we have that  $k\alpha \bmod n = 0$ . This is true because the elements of  $L$ ,  $\{0, 1, \dots, n-1\}$  form a cyclic group  $G$  with addition modulo  $n$ . One generator of this group is 1. From Fraleigh [1997], we have that the cyclic subgroup of  $G$  generated by  $\alpha$  has order  $\frac{n}{\gcd(\alpha, n)}$ . Thus, if  $\gcd(\alpha, n) > 1$ ,  $\alpha$  generates a cyclic subgroup that doesn't contain all  $n$  elements of  $G$  and hence for some integer  $k$ ,  $0 < k < n$ ,  $k\alpha \bmod n = 0$ . But this means that  $l_{00} = l_{0k} = 0$  and  $L$  has two zeros in its first row. Hence  $L$  cannot be a latin square. Similarly, if  $\gcd(\beta, n) > 1$ , there exists some integer  $k$ ,  $0 < k < n$ , such that  $k\beta \bmod n = 0$ , but then  $l_{00} = l_{k0} = 0$  and  $L$  has two zeros in its first column and therefore cannot be a latin square. We have shown by contrapositive that if  $L = \| l_{ij} \|$  is a latin square of the form  $l_{ij} = (i\beta + j\alpha) \bmod n$  for some integers  $\alpha, \beta$  in the range  $0 < \alpha, \beta < n$ , then  $\gcd(\alpha, n) = \gcd(\beta, n) = 1$ . Next, assume that  $\gcd(\alpha, n) = \gcd(\beta, n) = 1$ , and suppose  $l_{ij_1} = l_{ij_2}$  for some integers  $i, j_1, j_2$  in the range  $0 < i, j_1, j_2 < n$ . This implies that  $i\beta + j_1\alpha \equiv i\beta + j_2\alpha \pmod{n}$  which gives  $(j_1 - j_2)\alpha \equiv 0 \pmod{n}$ . However, since  $\gcd(\alpha, n) = 1$ ,  $j_1 = j_2$ . Similarly if  $l_{i_1j} = l_{i_2j}$  for some  $0 < i_1, i_2, j < n$  we have that  $i_1 = i_2$  since  $\gcd(\beta, n) = 1$ . This means that  $L$  has no row or column with repeated elements, and thus  $L$  is a latin square.  $\square$

**Lemma 2.2.** An  $n \times n$  latin square  $L = \| l_{ij} \|$  of the form  $l_{ij} = (i\beta + j\alpha) \bmod n$  for some integers  $\alpha, \beta$  in the range  $0 < \alpha, \beta < n$  generates a linear code modulo  $n$ .

**Proof.** Let  $C$  be the code generated from  $L$ . Consider the two codewords  $c_1 = (i_1, j_1, i_1\beta + j_1\alpha)$  and  $c_2 = (i_2, j_2, i_2\beta + j_2\alpha)$ . Then

$$c_1 + c_2 = (z_1, z_2, (z_1\beta + z_2\alpha) \bmod n)$$

where  $z_1 = (i_1 + i_2) \bmod n$  and  $z_2 = (j_1 + j_2) \bmod n$ . Thus, from the structure of  $L$  we have that  $c_1 + c_2 \in C$ .  $\square$

**Lemma 2.3.** If  $L = \| l_{ij} \|$  is an  $n \times n$  latin square that generates a linear code modulo  $n$ , then  $L$  is of the form  $l_{ij} = (i\beta + j\alpha) \bmod n$  for some integers  $\alpha, \beta$  in the range  $0 < \alpha, \beta < n$  and  $\gcd(\alpha, n) = \gcd(\beta, n) = 1$ .

**Proof.** From Theorem 2.1,  $l_{00} = 0$ . Let  $l_{01} = \alpha$  and  $l_{10} = \beta$  for some integers  $\alpha, \beta$  in the range  $0 < \alpha, \beta < n$ . Now let  $C$  be the code generated from  $L$ . Assume  $C$  is a linear code modulo  $n$ . Then any multiple of a codeword is a codeword. Thus, for any integer  $k$ ,  $0 \leq k < n$ ,  $k(0, 1, \alpha) = (0, k, k\alpha)$  and we have that  $l_{0k} = k\alpha$ . Also  $k(1, 0, \beta) = (k, 0, k\beta)$  and we have that  $l_{k0} = k\beta$ . Furthermore, for any  $0 < i, j < n$ , we have that

$$i(1, 0, \beta) + j(0, 1, \alpha) = (i, 0, i\beta) + (0, j, j\alpha) = (i, j, i\beta + j\alpha)$$

Hence,  $l_{ij} = i\beta + j\alpha$ . From Lemma 2.1, for  $L$  to be a latin square,  $\gcd(\alpha, n) = \gcd(\beta, n) = 1$ .  $\square$

**Theorem 2.2.** An  $n \times n$  matrix  $L = \| l_{ij} \|$  is a latin square that generates a linear code modulo  $n$  iff  $L$  is of the form  $l_{ij} = (i\beta + j\alpha) \bmod n$  for some integers  $\alpha, \beta$  satisfying 1)  $0 < \alpha, \beta < n$  and 2)  $\gcd(\alpha, n) = \gcd(\beta, n) = 1$ .

**Proof.** Follows immediately from Lemmas 2.1, 2.2, and 2.3.  $\square$

The above theorem characterizes every latin square that is a possible member of a set of mutually orthogonal latin squares that generate a linear code modulo  $n$ . Latin squares of even order are not very useful in terms of generating linear codes modulo  $n$  as the following result shows.

**Theorem 2.3.** If  $n$  is an even positive integer, then there is no pair of  $n \times n$  mutually orthogonal latin squares that generate a linear code modulo  $n$ .

**Proof.** Let  $A = \| a_{ij} \|$  and  $B = \| b_{ij} \|$  be two  $n \times n$  mutually orthogonal latin squares that generate a linear code with  $n = 2k$  for some positive integer  $k$ . Then, by Theorem 2.1,  $2(0, k, a_{0k}, b_{0k}) = (0, 2k, 2a_{0k}, 2b_{0k}) = (0, 0, 2a_{0k}, 2b_{0k}) = (0, 0, 0, 0)$ . This means that  $2a_{0k} = 0$  and  $2b_{0k} = 0$ . We have that  $a_{0k} \neq 0$  and  $b_{0k} \neq 0$  because 0 already occurs in the first rows of  $A$  and  $B$ . Thus, we clearly have that  $a_{0k} = b_{0k} = k$ . However, we also have  $2(k, 0, a_{k0}, b_{k0}) = (0, 0, 2a_{k0}, 2b_{k0})$ , hence  $a_{k0} = b_{k0} = k$ . Therefore

$$(a_{0k}, b_{0k}) = (a_{k0}, b_{k0}) = (k, k)$$

and we have that  $A$  and  $B$  are not orthogonal, a contradiction.  $\square$

**Notation.** If  $A = \| a_{ij} \|$  is a latin square that generates a linear code and is of the form  $a_{ij} = (i\beta + j\alpha) \bmod n$  for some integers  $\alpha, \beta$  in the range  $0 < \alpha, \beta < n$ , then we denote  $A$  by  $A = (\| a_{ij} \|, \alpha, \beta)$ .

This notation emphasizes the fact that any  $n \times n$  latin square used to generate a linear code is completely described by its  $\alpha$  and  $\beta$ .

**Lemma 2.4.** Let  $A = (\| a_{ij} \|, \alpha, \beta)$  and let  $g$  be some integer in the range  $0 \leq g < n$ . Then,  $g$  occurs in the  $i$ -th row of  $A$  at the position  $a_{i, g\alpha^{-1} - i\beta\alpha^{-1}}$ .

**Proof.** We know that  $g$  occurs in the  $i$ -th row of  $A$  because  $A$  is a latin square. Thus, for some integer  $k_i, 0 \leq k_i < n$ , we have that  $i\beta + k_i\alpha = g$  which implies that  $k_i = (g - i\beta)\alpha^{-1} = g\alpha^{-1} - i\beta\alpha^{-1}$   $\square$

The following theorem provides necessary and sufficient conditions for two latin squares that generate linear codes modulo  $n$  by themselves to be orthogonal. Two such orthogonal latin squares when taken together generate another linear code modulo  $n$ .

**Theorem 2.4.** Let  $A = (\| a_{ij} \|, \alpha_1, \beta_1)$  and  $B = (\| b_{ij} \|, \alpha_2, \beta_2)$ . Then,  $A$  and  $B$  are orthogonal iff  $\gcd((\beta_1\alpha_1^{-1} - \beta_2\alpha_2^{-1}), n) = 1$ .

**Proof.** Assume that  $\gcd((\beta_1\alpha_1^{-1} - \beta_2\alpha_2^{-1}), n) = 1$ . Now assume that two corresponding entries of  $A$  and  $B$  are equal:  $(g, h) = (a_{i_1j_1}, b_{i_1j_1}) = (a_{i_2j_2}, b_{i_2j_2})$ . Then, from Lemma 2.4, we have

$$j_1 = g\alpha_1^{-1} - i_1\beta_1\alpha_1^{-1} = h\alpha_2^{-1} - i_1\beta_2\alpha_2^{-1} = j_1 \quad (1)$$

$$j_2 = g\alpha_1^{-1} - i_2\beta_1\alpha_1^{-1} = h\alpha_2^{-1} - i_2\beta_2\alpha_2^{-1} = j_2 \quad (2)$$

Subtracting (1) from (2) yields

$$\begin{aligned} i_1\beta_1\alpha_1^{-1} - i_2\beta_1\alpha_1^{-1} &= i_1\beta_2\alpha_2^{-1} - i_2\beta_2\alpha_2^{-1} \\ \Rightarrow i_1\beta_1\alpha_1^{-1} - i_2\beta_1\alpha_1^{-1} - i_1\beta_2\alpha_2^{-1} + i_2\beta_2\alpha_2^{-1} &= 0 \\ \Rightarrow i_1(\beta_1\alpha_1^{-1} - \beta_2\alpha_2^{-1}) - i_2(\beta_1\alpha_1^{-1} - \beta_2\alpha_2^{-1}) &= 0 \\ \Rightarrow (i_1 - i_2)(\beta_1\alpha_1^{-1} - \beta_2\alpha_2^{-1}) &= 0. \end{aligned}$$

We have that  $i_1 = i_2$  since  $\gcd((\beta_1\alpha_1^{-1} - \beta_2\alpha_2^{-1}), n) = 1$ . Comparing (1) and (2) we see that  $j_1 = j_2$ .

Now, assume  $\gcd((\beta_1\alpha_1^{-1} - \beta_2\alpha_2^{-1}), n) > 1$ , then for some integer  $k$ ,  $0 < k < n$  we have that  $k(\beta_1\alpha_1^{-1} - \beta_2\alpha_2^{-1}) = 0$ . From Lemma 2.4, 0 occurs in the  $k$ -th row in  $A$  at  $-k\beta_1\alpha_1^{-1}$  and in  $B$  at  $-k\beta_2\alpha_2^{-1}$  but

$$\begin{aligned} k(\beta_1\alpha_1^{-1} - \beta_2\alpha_2^{-1}) = 0 &\Rightarrow k\beta_2\alpha_2^{-1} = k\beta_1\alpha_1^{-1} \\ &\Rightarrow -k\beta_2\alpha_2^{-1} = -k\beta_1\alpha_1^{-1} \end{aligned}$$

This means that the pair  $(0, 0)$  occurs twice among corresponding entries from  $A$  and  $B$  and thus  $A$  and  $B$  are not orthogonal.  $\square$

**Corollary 2.1.** Let  $A = (\| a_{ij} \|, \alpha_1, \beta_1)$  and  $B = (\| b_{ij} \|, \alpha_2, \beta_2)$ . Then

- (1) If  $\alpha_1 = \beta_1$  then  $A$  and  $B$  are orthogonal only if  $\alpha_2 \neq \beta_2$ .
- (2) If  $\alpha_1 = \beta_1$  then  $A$  and  $B$  are orthogonal iff  $\gcd(\alpha_2 - \beta_2, n) = 1$ .
- (3) If  $\alpha_1 = \alpha_2$  then  $A$  and  $B$  are orthogonal iff  $\gcd(\beta_2 - \beta_1, n) = 1$ .
- (4) If  $\alpha_1 = \beta_1 = \alpha_2 \neq \beta_2$  then  $A$  and  $B$  are orthogonal iff  $\gcd(\beta_2 - \alpha_1, n) = 1$ .

**Proof.** We prove (2), and the rest follow obviously. Assume  $\alpha_1 = \beta_1$ . Applying Theorem 2.4, we have that  $A$  and  $B$  are orthogonal iff

$$\begin{aligned} 1 &= \gcd((\beta_1\alpha_1^{-1} - \beta_2\alpha_2^{-1}), n) = \gcd((\alpha_1\alpha_1^{-1} - \beta_2\alpha_2^{-1}), n) \\ &= \gcd((1 - \beta_2\alpha_2^{-1}), n) = \gcd((\alpha_2 - \beta_2), n) = 1 \end{aligned}$$

Note that we used the fact that  $\gcd(\alpha_2, n) = \gcd(\alpha_2^{-1}, n) = 1$  in the last step above. (1) and (4) follow directly from (2), and (3) follows from Theorem 2.4.  $\square$

It is of interest to know how many mutually orthogonal latin squares of some order  $n$  exist that together generate a linear code modulo  $n$ . The next theorem gives an upper bound for this number. After that we provide a construction that achieves this upper bound for any  $n$ . This construction can be used to generate a linear code modulo  $n$  with maximum error-correction from a set of mutually orthogonal latin squares.

**Theorem 2.5.** *Suppose that the prime factorization of  $n$  is  $n = p_1 p_2 \dots p_h$  such that  $p_1 \leq p_2 \leq \dots \leq p_h$  and  $p_1, p_2, \dots, p_h$  are prime. Then there are at most  $p_1 - 1$  mutually orthogonal latin squares of order  $n$  that generate a linear code modulo  $n$ .*

**Proof.** Suppose that there exists a set  $S$  of more than  $p_1 - 1$  mutually orthogonal latin squares of order  $n$  that generate a linear code modulo  $n$ . Fix one of the latin squares in  $S$ , say  $A = (\| a_{ij} \|, \alpha_1, \beta_1)$ . Consider the set of differences:

$$D = \{(\beta_1 \alpha_1^{-1} - \beta_m \alpha_m^{-1}) \mid (\| l_{ij}^m \|, \alpha_m, \beta_m) \in (S - \{A\})\} \text{ mod } p_1$$

Suppose that there exist two latin squares  $B = (\| b_{ij} \|, \alpha_2, \beta_2)$  and  $C = (\| c_{ij} \|, \alpha_3, \beta_3)$  in  $S - \{A\}$  such that  $\beta_1 \alpha_1^{-1} - \beta_2 \alpha_2^{-1} \equiv \beta_1 \alpha_1^{-1} - \beta_3 \alpha_3^{-1} \pmod{p_1}$ . This implies that  $\beta_2 \alpha_2^{-1} - \beta_3 \alpha_3^{-1} \equiv 0 \pmod{p_1}$ . However, by Theorem 2.4 we have that  $B$  and  $C$  are not orthogonal because  $\gcd(\beta_2 \alpha_2^{-1} - \beta_3 \alpha_3^{-1}, n) \neq 1$ , a contradiction. Thus, we have that each latin square in  $S - \{A\}$  contributes a distinct element to  $D$ . This means that there are exactly  $p_1 - 1$  elements in  $S - \{A\}$  and that  $D = \{1, 2, \dots, p_1 - 1\}$ . Therefore,  $\beta_1 \alpha_1^{-1} \text{ mod } p_1 \in D$ . So for some latin square  $K = (\| l_{ij} \|, \alpha_k, \beta_k)$  we have that  $\beta_1 \alpha_1^{-1} - \beta_k \alpha_k^{-1} \equiv \beta_1 \alpha_1^{-1} \pmod{p_1}$ . However, this implies that  $\beta_k \alpha_k^{-1} \equiv 0 \pmod{p_1}$ , which is a contradiction because by lemma 2.1,  $K$  is not a latin square.  $\square$

**Theorem 2.6.** *Suppose that the prime factorization of  $n$  is  $n = p_1 p_2 \dots p_h$  such that  $p_1 \leq p_2 \leq \dots \leq p_h$  and  $p_1, p_2, \dots, p_h$  are prime. Then there exists a maximal set of  $p_1 - 1$  mutually orthogonal latin squares of order  $n$  that generate a linear code modulo  $n$ .*

**Proof.** Let  $\alpha$  be an integer in the range  $0 < \alpha < n$  that is relatively prime to  $n$ . Then the  $p_1 - 1$  latin squares of the form  $L_k = (\| l_{ij}^k \|, \alpha, k)$  as

$k$  ranges from 1 to  $p_1 - 1$  are, Corollary 2.1(3), mutually orthogonal. By Theorem 2.5, this is a maximal set of mutually orthogonal latin squares of order  $n$  that generate a linear code modulo  $n$ .  $\square$

When  $n$  is a prime number, it is well known that there are exactly  $n - 1$  mutually orthogonal latin squares of order  $n$ . It is worthwhile to note that in such a case, we know, by Theorem 2.6, that there exist  $n - 1$  such mutually orthogonal latin squares of order  $n$  that also generate a linear code modulo  $n$ .

**Example 2.1.** We give an example of a linear code generated from 4 mutually orthogonal latin squares of order 5. We use the method described in the proof of Theorem 2.6 with  $\alpha = 4$ :

$$\begin{bmatrix} 0 & 4 & 3 & 2 & 1 \\ 1 & 0 & 4 & 3 & 2 \\ 2 & 1 & 0 & 4 & 3 \\ 3 & 2 & 1 & 0 & 4 \\ 4 & 3 & 2 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 4 & 3 & 2 & 1 \\ 2 & 1 & 0 & 4 & 3 \\ 4 & 3 & 2 & 1 & 0 \\ 1 & 0 & 4 & 3 & 2 \\ 3 & 2 & 1 & 0 & 4 \end{bmatrix}, \begin{bmatrix} 0 & 4 & 3 & 2 & 1 \\ 3 & 2 & 1 & 0 & 4 \\ 1 & 0 & 4 & 3 & 2 \\ 4 & 3 & 2 & 1 & 0 \\ 2 & 1 & 0 & 4 & 3 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 4 & 3 & 2 & 1 \\ 4 & 3 & 2 & 1 & 0 \\ 3 & 2 & 1 & 0 & 4 \\ 2 & 1 & 0 & 4 & 3 \\ 1 & 0 & 4 & 3 & 2 \end{bmatrix}$$

The code  $C$  generated by these latin squares is  $C =$

$$\begin{aligned} & (0, 0, 0, 0, 0, 0), (0, 1, 4, 4, 4, 4), (0, 2, 3, 3, 3, 3), (0, 3, 2, 2, 2, 2), (0, 4, 1, 1, 1, 1), \\ & (1, 0, 1, 2, 3, 4), (1, 1, 0, 1, 2, 3), (1, 2, 4, 0, 1, 2), (1, 3, 3, 4, 0, 1), (1, 4, 2, 3, 4, 0), \\ & (2, 0, 2, 4, 1, 3), (2, 1, 1, 3, 0, 2), (2, 2, 0, 2, 4, 1), (2, 3, 4, 1, 3, 0), (2, 4, 3, 0, 2, 4), \\ & (3, 0, 3, 1, 4, 2), (3, 1, 2, 0, 3, 1), (3, 2, 1, 4, 2, 0), (3, 3, 0, 3, 1, 4), (3, 4, 4, 2, 0, 3), \\ & (4, 0, 4, 3, 2, 1), (4, 1, 3, 2, 1, 0), (4, 2, 2, 1, 0, 4), (4, 3, 1, 0, 4, 3), (4, 4, 0, 4, 3, 2) \end{aligned}$$

This code is linear and one example of this is as follows:

$$\begin{aligned} & (1, 2, 4, 0, 1, 2) + (3, 4, 4, 2, 0, 3) + (2, 1, 1, 3, 0, 2) \\ & + (3, 3, 0, 3, 1, 4) = (4, 0, 4, 3, 2, 1) \in C \end{aligned}$$

**Example 2.2.** We can easily develop a formula for computing pairs of orthogonal latin squares that generate a linear code modulo  $n$ , for any odd  $n$  using Corollary 2.1:

$$L_1 = \| l_{ij} \| \text{ defined by } l_{ij} = (2^k i + j) \bmod n$$

and

$$L_2 = \| l_{ij} \| \text{ defined by } l_{ij} = (2^{k-1} i + j) \bmod n$$

This works whenever  $2^k < n$  because  $L_1 = (\| l_{ij} \|, 1, 2^k)$  and  $L_2 = (\| l_{ij} \|, 1, 2^{k-1})$ . However, by Corollary 2.1(3), these are orthogonal because  $\gcd(2^k - 2^{k-1}, n) = \gcd(2^{k-1}, n) = 1$ , since  $n$  is odd. Note that this degenerates to a well-known method of computing pairs of mutually orthogonal latin squares when  $k$  is set to 1.

## References

- [1] J. Denes and A.D. Keedwell, *Latin Squares and Their Applications*, Academic Press, New York and London, (1974).
- [2] S. Kadowaki, S. Kageyama, M. Kimura, and Y. Yanagida, Error-correcting non-binary codes through Latin squares, *Bulletin of the ICA*, **29** (2000), 67-70.
- [3] John B. Fraleigh, *A First Course in Abstract Algebra*, Addison-Wesley, Massachusetts, (1997).