A SYNDROME-DISTRIBUTION DECODING OF MOLS $\mathcal{L}_p$ CODES

D. G. KIM[1], S. HAHN[2] AND Y.S. KIM[2]

[1] Chungwoon University, Hongsung-Eup,Chungnam 350-800, South Korea
[2] Department of Mathematics, KAIST, Taejon 305-701, South Korea

Abstract. Let p be an odd prime number. We introduce simple and useful decoding algorithm for orthogonal Latin square codes of order p. Let H be the parity check matrix of orthogonal Latin square code. For any $x \in \mathrm{GF}(p)^n$, we call xH^t the syndrome of x. This method is based on the syndrome-distribution decoding for linear codes. In $\mathcal{L}_p$, we need to find the first and the second coordinates of codeword in order to correct the errored received vector.

1. Introduction

The organization of this paper is as follows: In Section 1, we will recall the well-known definitions concerning Latin squares and maximum set of orthogonal Latin squares. And we will summarize a construction of $p-1$ mutually orthogonal Latin squares when p is a prime number [6].

In Section 2, for an odd prime p, we will review a p-ary codes of specified minimum distance corresponding to $p-1$ mutually orthogonal Latin squares [4].

In 1970, D. C. Bossen, R. T. Chien and M. Y. Hsiao [2] have constructed a class of decodable multiple error-correcting codes which is based on one-step majority decoding method. In Section 3, we will prove the theorems which provide a new algorithm for orthogonal Latin square codes in Section 4. Finally, we will give a syndrome-distribution dedcoding algorithm and examples corresponding to each steps of this algorithm.

Definition. A Latin square of order n is $n \times n$ square array of numbers from an n-symbol alphabet (say $0, 1, \ldots, n-1$) in which each row and each column contains each symbol exactly once. A pair of Latin squares of order n is (pairwise-) orthogonal if, when one square is superimposed on the other, every ordered pair of elements are distinct. In particular, a set of Latin squares of order n, any pair of which are orthogonal, is called a set of mutually (pairwise-) orthogonal Latin squares (MOLS).

Notice that we can permute rows and columns of the array without destroying the Latin square property. This implies that we can always permute the rows and columns of the array so that the elements in the first row and first column are ordered. The orthogonality of two Latin square is not destroyed by relabeling the symbols in the rows (or columns).

To obtain a code corresponding to a set of mutually orthogonal Latin squares, it is important to determine the maximum possible number of mutually orthogonal Latin squares of given order n. Since [3], it is well known that $n-1$ is an upper bound. In particular if n is a prime number, there exist exactly $n-1$ mutually orthogonal Latin squares.

Theorem 1 ([3]). *For any n, there are at most $n-1$ mutually orthogonal Latin squares of order n.*

Let p be an odd prime. Then there exists a finite field GF(p) with p elements. Take an $p \times p$ array

$$L_t = [u_t(i,j)], \qquad 0 \le i,j \le p-1, \quad 1 \le t \le p-1$$

and in the cell (i,j) of this array put the integer $u_t = u_t(i,j)$ given by

$$u_t = t \cdot i + j$$

where t is a fixed nonzero element of $GF(p)$. We write down the following Latin square L_t of order p, $1 \le t \le p-1$,

$$\begin{array}{cccc}
0 & 1 & \cdots & p-1 \\
t & t+1 & \cdots & t+p-1 \\
2t & 2t+1 & \cdots & 2t+p-1 \\
\vdots & \vdots & \vdots & \vdots \\
(p-1)t & (p-1)t+1 & \cdots & (p-1)t+p-1
\end{array}$$

where all expressions are to be taken mod p. In [1] and [6], we have seen that $\{L_1, \ldots, L_{p-1}\}$ is a set of $p-1$ orthogonal Latin squares.

As an example, we can write down a set of four orthogonal Latin squares of order 5,

		L_1						L_2		
0	1	2	3	4		0	1	2	3	4
1	2	3	4	0		2	3	4	0	1
2	3	4	0	1		4	0	1	2	3
3	4	0	1	2		1	2	3	4	0
4	0	1	2	3		3	4	0	1	2

		L_3						L_4		
0	1	2	3	4		0	1	2	3	4
3	4	0	1	2		4	0	1	2	3
1	2	3	4	0		3	4	0	1	2
4	0	1	2	3		2	3	4	0	1
2	3	4	0	1		1	2	3	4	0 .

In addition, when p is a prime power, we can get a similar result [6]. So we will not discuss them here.

2. Orthogonal Latin square codes

S. W. Golomb and E. C. Posner [4] established an important connection between the existence of sets of mutually orthogonal Latin squares and the existence of p-ary codes.

The following two concepts are equivalent:

(1) A set of $p-1$ mutually orthogonal Latin squares of order p,

(2) A linear code with length $p+1$, minimum distance p, p^2 codeword.

The [p+1,2,p] code derived from $p-1$ mutually orthogonal Latin squares of order p is orthogonal Latin square codes of order p. From Section 1 and the above two concepts, we have the codewords as the form $(i,\ j,\ i+j,\dots,(p-1)\cdot i+j)$, $0 \le i,j \le p-1$.

This construction has been generalized to multi-orthogonal higher dimensional Latin hypercubes by Silverman [7]. In this terms, an orthogonal Latin square code is equivalent to a set of $d-1$ mutually $(n-d+1)$-wise orthogonal $(n-d+1)$-dimensional Latin hypercubes where n, d, is the length and minimum distance respectively.

A $[p+1,\ 2,\ p]$ orthogonal Latin square code is linear code with generator matrix G

$$\begin{bmatrix} 1 & 0 & 1 & 2 & 3 & \dots & (p-1) \\ 0 & 1 & 1 & 1 & 1 & \dots & 1 \end{bmatrix} = [I_2\ \ \mathrm{P}],$$

where I_2 is 2×2 identity matrix and

$$\mathrm{P} = \begin{bmatrix} 1 & 2 & 3 & \dots & (p-1) \\ 1 & 1 & 1 & \dots & 1 \end{bmatrix}.$$

Hence the parity check matrix H of orthogonal Latin square code $\mathcal{L}_p$ is :

$$\mathrm{H} = [-\mathrm{P}^t \; I_{p-1}] = \begin{bmatrix} p-1 & p-1 & 1 & 0 & \dots & 0 \\ p-2 & p-1 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & & & \dots & \\ 1 & p-1 & 0 & 0 & \dots & 1 \end{bmatrix},$$

where I_{p-1} is $(p-1) \times (p-1)$ identity matrix and P^t is transpose of P.

3. Main Theorem

In this section, all the arithmetic operations (i.e. addition and multiplication) are based on GF(p).

For convenience, we first define the following notation:

$$\mathbf{c} = (c_1, \dots, c_{p+1}) : \text{codeword in } \mathcal{L}_p.$$
$$\mathbf{r} = (r_1, \dots, r_{p+1}) : \text{received word.}$$
$$\mathbf{e} = (e_1, \dots, e_{p+1}) : \text{error vector.}$$

i.e. $\mathbf{r} = \mathbf{c} + \mathbf{e}$.

H : parity check matrix (see previous Section).

$\mathbf{s} = (s_1, \dots, s_{p-1})$: syndrome vector.

$\mathbf{s}(l) = \mathbf{s} - l \cdot (p-1,\ p-2,\ \dots, 2,\ 1) = (\hat{s}_1,\ \hat{s}_2, \dots, \hat{s}_{p-1})$: dual syndrome with variable l for $1 \le l \le p-1$.

$M_b(\mathbf{s}) = \#\{i \mid s_i = b,\ 1 \le i \le p-1\}$: distribution for some syndrome $\mathbf{s} = (s_1, \dots, s_{p-1})$ and some $b \in \mathrm{GF}(p)$.

$M_b(\mathbf{s}(l)) = \#\{i \mid \hat{s}_i = b,\ 1 \le i \le p-1\}$: dual distribution for some dual syndrome $\mathbf{s}(l)$ and some $b \in \mathrm{GF}(p)$.

But, if codeword $\mathbf{c}$ is changed into received word $\mathbf{r}$ with error $\mathbf{e}$. Then $\mathbf{s} = \mathrm{H}\,\mathbf{r}^t = \mathrm{H}(\mathbf{c}+\mathbf{e})^t = \mathrm{H}\,\mathbf{c}^t + \mathrm{H}\,\mathbf{e}^t = \mathrm{H}\,\mathbf{e}^t$. So the i-th coordinate s_i of syndrome $\mathbf{s}$ is $s_i = -i \cdot e_1 - e_2 + e_{i+2}$. Since $\mathcal{L}_p$ has minimum distance p, we always assume that the Hamming weight of $\mathbf{e}$ is less than or equal to $\dfrac{p-1}{2}$.

Theorem 2 ([5]). *Let* $\mathbf{r} = (r_1, \ldots, r_{p+1})$ *be a received word and* $\mathbf{s} = (s_1, \ldots, s_{p-1})$ *syndrome of* $\mathbf{r}$.

(1) Both r_1 *and* r_2 *are correct if and only if* $M_0(\mathrm{s}) \geq \frac{p-1}{2}$.

(2) r_1 *is correct and* r_2 *is not correct if and only if* $M_b(\mathrm{s}) \geq \frac{p+1}{2}$ *for some* $b \in \mathrm{GF}(p) - \{0\}$.

Proof of (1) : By previous paragraph, $s_i = -i \cdot e_1 - e_2 + e_{i+2}$, $1 \leq i \leq p-1$. ($\Rightarrow$) If both r_1 and r_2 are correct, $e_1 = e_2 = 0$. So, $s_i \neq 0$ if and only if $e_{i+2} \neq 0$. But since Hamming weight of $\mathbf{e}$ is less than or equal to $\frac{p-1}{2}$, $M_0(\mathrm{s}) \geq \frac{p-1}{2}$.

($\Leftarrow$) Suppose that r_1 is correct and r_2 is not correct (i.e. $e_1 = 0$ and $e_2 \neq 0$). Then $s_i = 0$ if and only if $e_2 = e_{i+2} \neq 0$. But at most $\frac{p-3}{2}$ elements of $e_3, e_4, \ldots, e_{p+1}$ are nonzero. i.e. $M_0(\mathrm{s}) \leq \frac{p-3}{2}$, which contradicts the hypothesis.

Suppose that r_1 is not correct and r_2 is correct(i.e. $e_1 \neq 0$ and $e_2 = 0$). Then, for $i = 1, \ldots, p-1$, $s_i = 0$ if and only if $i \cdot e_1 = e_{i+2}$. But at most $\frac{p-3}{2}$ elements of $e_3, e_4, \ldots, e_{p+1}$ are nonzero. i.e. $M_0(\mathrm{s}) \leq \frac{p-3}{2}$, which contradicts the hypothesis.

Suppose that both r_1 and r_2 are not correct(i.e. $e_1 = e_2 \neq 0$). Then, for $i = 1, \ldots, p-1$, $s_i = 0$ if and only if $i \cdot e_1 + e_2 = e_{i+2}$. But, for $i = -\frac{e_2}{e_1}$, $e_{i+2} = 0$ and for $i \neq -\frac{e_2}{e_1}$, $e_{i+2} \neq 0$. But at most $\frac{p-5}{2}$ elements of $e_3, \ldots, e_{p+1}$ are nonzero. i.e. $M_0(\mathrm{s}) \leq 1 + \frac{p-5}{2} = \frac{p-3}{2}$. This contradicts the hypothesis.

Proof of (2) : ($\Rightarrow$) By assumption, $e_1 = 0$ and $e_2 \neq 0$. But since $e_2 \neq 0$, at least $\frac{p+1}{2}$ elements of $e_3, \ldots, e_{p+1}$ are zero. So, for $b = -e_2$, $M_b(\mathrm{s}) \geq \frac{p+1}{2}$.

($\Leftarrow$) Suppose that r_1 is not correct and r_2 is correct (i.e. $e_1 \neq 0$ and $e_2 = 0$). But since $e_1 \neq 0$, at most $\frac{p-3}{2}$ of $e_3, \ldots, e_{p+1}$ are nonzero. Hence, for $b \neq 0$, $\{i \mid s_i = -i \cdot e_1 + e_{i+2} = b\} \subset \{i \mid e_{i+2} = 0,\ i = -\frac{b}{e_1}\} \cup \{i \mid e_{i+2} \neq 0\}$. Thus $M_b(\mathrm{s}) \leq 1 + \frac{p-3}{2} = \frac{p-1}{2}$. This contradicts the hypothesis.

Suppose that both r_1 and r_2 are not correct (i.e. $e_1 \neq 0$, $e_2 \neq 0$). Then at most $\frac{p-5}{2}$ elements of $e_3, \ldots, e_{p+1}$ are nonzero. So, for $b \neq 0$, $\{i \mid s_i = -i \cdot e_1 - e_2 + e_{i+2} = b\} \subset \{i \mid e_{i+2} = 0\} \cup \{i \mid e_{i+2} \neq 0, i = -\frac{b + e_2 - e_{i+2}}{e_1}\}$. Hence $M_b(\mathrm{s}) \leq 1 + \frac{p-5}{2} = \frac{p-3}{2}$. This contradicts the hypothesis.

Theorem 3. *Suppose that r_1 is not correct (i.e. In Theorem 2, the conditions of (1) and (2) are not satisfied).*

(1) r_2 is correct if and only if $M_0(\mathrm{s}(e_1)) \geq \frac{p+1}{2}$.

(2) r_2 is not correct if and only if for some $b \neq 0$, $M_b(\mathrm{s}(e_1)) \geq \frac{p+3}{2}$.

Proof of (1) : ($\Rightarrow$) By definition, the i-th coordinate of dual syndrome $\mathrm{s}(l)$ is $\hat{s}_i = -i \cdot (e_1 - l) - e_2 + e_{i+2}$. Hence by assumption $e_2 = 0$ and at least for $1 \leq i \leq p-1$ the number of e_{i+2} which is zero is greater than or equal to $\frac{p+1}{2}$. So $M_0(\mathrm{s}(e_1)) \geq \frac{p+1}{2}$.

($\Leftarrow$) Suppose that r_2 is not correct. Then for $1 \leq i \leq p-1$, the number of e_{i+2} which is not zero is less than or equal to $\frac{p-5}{2}$. So $M_0(\mathrm{s}(e_1)) \leq \frac{p-5}{2}$. This contradicts the hypothesis.

Proof of (2) : ($\Rightarrow$) By assumption , for $1 \leq i \leq p-1$, the number of e_{i+2} which is zero is greater than or equal to $\frac{p+3}{2}$. So $b = -e_2$, $M_b(\mathrm{s}(e_1)) \geq \frac{p+3}{2}$.

($\Leftarrow$) Suppose that r_2 is correct. Then for $1 \leq i \leq p-1$, the number of e_{i+2} which is not zero is less than or equal to $\frac{p-3}{2}$. So $b \neq 0$, $M_b(\mathrm{s}(e_1)) \leq \frac{p-3}{2}$. This contradicts the hypothesis.

Note: By Theorem 3, $M_b(\mathrm{s}(e_1)) \geq \frac{p+1}{2}$ either for $b = 0$, or for some b such that $b \neq 0$. Therefore, $M_b(\mathrm{s}(e_1)) = \max_{a \in \mathrm{GF}(p)} M_a(\mathrm{s}(l))$ for some l, $1 \leq l \leq p-1$.

4. The syndrome-distribution method of $\mathcal{L}_p$ and examples

Let A (B) be the first (second) coordinate of codeword **c** which is changed into **r** respectively.

Algorithm

Step 1 : If $M_0(\mathrm{s}) \geq \frac{p-1}{2}$, then by Theorem 2-(1), $\mathbf{r}$ is decoded into $\mathbf{c} = (r_1,\ r_2,\ r_1 + r_2, \ldots, (p-1)r_1 + r_2)$.

Step 2 : If $M_0(\mathrm{s}) < \frac{p-1}{2}$ and $M_b(\mathrm{s}) \geq \frac{p+1}{2}$ for $b \neq 0$, then by Theorem 2-(2), $\mathbf{r}$ is decoded into $\mathbf{c} = (r_1, B, r_1 + B, \ldots, (p-1)r_1 + B)$ where $B = r_2 + b$.

Step 3 : In the case that the conditions of Step 1 and Step 2 are not satisfied, if for $1 \leq l \leq p-1$, $M_0(\mathrm{s}(l)) \geq \frac{p+1}{2}$, then by Theorem 3-(1) codeword $\mathbf{c} = (A,\ r_2,\ A + r_2, \ldots, (p-1)A + r_2)$, where $A = r_1 - l$.

Step 4 : In the case that the conditions of Step 1 and Step 2 are not satisfied, if for $1 \leq l \leq p-1$, $\max_{b\neq 0} M_b(\mathrm{s}(l)) \geq \frac{p+3}{2}$, then $\mathbf{c} = (A,\ B,\ A + B, \ldots, (p-1)A + B)$, where $A = r_1 - l,\ B = r_2 + b$.

Example 1. Let $p = 5$, $\mathbf{r} = (2,3,1,3,4,1)$.

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

is the parity check matrix for $\mathcal{L}_5$ over GF(5). Then the syndrome s of $\mathbf{r}$

$$\mathrm{H}\,\mathbf{r}^t = \begin{bmatrix} 4 & 4 & 1 & 0 & 0 & 0 \\ 3 & 4 & 0 & 1 & 0 & 0 \\ 2 & 4 & 0 & 0 & 1 & 0 \\ 1 & 4 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \\ 1 \\ 3 \\ 4 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}.$$

Since $M_0(\mathrm{s}) \geq \frac{5-1}{2} = 2$, both r_1 and r_2 are correct. By Step 1, $\mathbf{c} = (2,3,2+3,4+3,1+3,3+3) = (2,3,0,2,4,1)$.

Example 2. Let $p = 5$, $\mathbf{r} = (1,3,3,1,0,1)$. Then the syndrome s of $\mathbf{r}$ is $(4,1,4,4)$. Since $M_0(\mathrm{s}) < \frac{5-1}{2} = 2$ and $M_4(\mathrm{s}) \geq \frac{5+1}{2} = 3$, by Theorem 2-(2) r_1 is correct. By Step 2, we have $B = 3+4 = 2$ and $\mathbf{c} = (1,2,3,4,0,1)$.

Example 3. Let $p = 5$, $\mathbf{r} = (3,2,1,0,2,3)$. Then the syndrome s of $\mathbf{r}$ is $(1,2,1,4)$. From $M_0(\mathrm{s}) < 2$, for any $b \neq 0$ $M_b(\mathrm{s}) < 3$ and $\mathrm{s}(4) = (0,\ 0,\ 3,\ 0)$, we get $M_0(\mathrm{s}(4)) \geq 3$ and so by Step 3, $\mathbf{c} = (4,\ 2,\ 1,\ 0,\ 4,\ 3)$.

Example 4. Let $p = 5$, $\mathbf{r} = (2,1,3,4,0,1)$. Then the syndrome $\mathbf{s}$ of $\mathbf{r}$ is $(0,4,3,2)$. From $M_0(\mathbf{s}) < 2$, for any $b \neq 0$ $M_b(\mathbf{s}) < 3$, and $\mathbf{s}(1) = (1, 1, 1, 1)$, we get $M_1(\mathbf{s}(1)) \geq 4$ and so by Step 4, $\mathbf{c} = (1, 2, 3, 4, 0, 1)$.

References

[1] R. C. Bose and B. Manvel, *Introduction to Combinatorial Theory*, John Wiley & Sons, New York, 1984.

[2] D. C. Bossen, R. T. Chien and M. Y. Hsiao, *Orthogonal Latin square codes*, IBM. J. Res. Develop. 14 (1970), 390–394.

[3] A. Cayley, *On Latin squares*, Messeng. Math. **19** (1890), 115–137.

[4] S. W. Golomb and E. C. Posner, *Rook domains, Latin squares, affine planes, and error-distributing codes*, IEEE Trans. Inform. Theory **IT-10** (1964), 196–208.

[5] S. Hahn, D. G. Kim and Y. S. Kim, *A decoding algorithm for orthogonal Latin square codes*, Indian J. pure appl. Math. **28(9)** (1997), 1235–1240.

[6] H. B. Mann, *On the construction of sets of orthogonal Latin squares*, Ann. Math. Statist. **14** (1943), 401–414.

[7] R. Silverman, *A metrization for power sets with applications to combinatorial analysis*, Canad. J. Math. **12** (1960), 158–176.