韓國數學敎育學會誌 시리즈 E
<數學敎育 프로시딩>
1997. 7. 제6집, 371-381.

Journal of the Korea Society of Mathematical Education
Proceedings of Mathematical Education
Series E: July 1997, Vol. 6, 371-381.

A Syndrome-distribution decoding MOLS L_p codes

S. Hahn, D. G. Kim and Y. S. Kim (KAIST)

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 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 [7].

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]. And using the weight enumerator of this code, we will find the minimum distance of its dual code. So we shall show how its dual codes is to Hamming codes of order 2 over $\mathrm{GF}(p)$.

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 an algorithm for orthogonal Latin square codes in Section 4. Finally, we will give a syndrome-decoding algorithm and examples corresponding to each steps of this algorithm.

1991 *Mathematics Subject Classification.* 05E99, 94B35.

Key words and phrases. dual code, Hamming code, maximum distance seperable, orthogonal Latin squares, syndrome.

Definition 1. A Latin square of order p is $p \times p$ square array of numbers from an p-symbol alphabet (say $0,\ 1,\dots,p-1$) in which each row and each column contains each symbol exactly once. Two Latin squares of the same order are (pairwise-) orthogonal if, when one Latin square is superimposed on the other, every ordered pair of elements are distinct. In particular, a set of Latin squares of the same order, 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 preserving the Latin square property. So, we can always permute the rows and columns of the array so that the elements in the initial row and initial column are ordered. Also, if two Latin squares are orthogonal, the relabeling can be done independently for each square without destroying orthogonality.

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 p. Since [3], it is well known that $p-1$ is an upper bound. In particular if p is a prime number, there exist exactly $p-1$ mutually orthogonal Latin squares.

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

Definition 2. A set of $p-1$ mutually (pairwise-)orthogonal Latin squares of order p is said to be a complete of mutually (pairwise-)orthogonal Latin squares.

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, $1 \le t \le p-1$,

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

where all expressions are to be taken mod p. In [1] and [7], we have seen that $\{L_1, \dots, L_{p-1}\}$ 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,

$$\begin{array}{ccccc}
\multicolumn{5}{c}{L_1} \\
0 & 1 & 2 & 3 & 4 \\
1 & 2 & 3 & 4 & 0 \\
2 & 3 & 4 & 0 & 1 \\
3 & 4 & 0 & 1 & 2 \\
4 & 0 & 1 & 2 & 3
\end{array}
\qquad
\begin{array}{ccccc}
\multicolumn{5}{c}{L_2} \\
0 & 1 & 2 & 3 & 4 \\
2 & 3 & 4 & 0 & 1 \\
4 & 0 & 1 & 2 & 3 \\
1 & 2 & 3 & 4 & 0 \\
3 & 4 & 0 & 1 & 2
\end{array}$$

$$\begin{array}{ccccc}
\multicolumn{5}{c}{L_3} \\
0 & 1 & 2 & 3 & 4 \\
3 & 4 & 0 & 1 & 2 \\
1 & 2 & 3 & 4 & 0 \\
4 & 0 & 1 & 2 & 3 \\
2 & 3 & 4 & 0 & 1
\end{array}
\qquad
\begin{array}{ccccc}
\multicolumn{5}{c}{L_4} \\
0 & 1 & 2 & 3 & 4 \\
4 & 0 & 1 & 2 & 3 \\
3 & 4 & 0 & 1 & 2 \\
2 & 3 & 4 & 0 & 1 \\
1 & 2 & 3 & 4 & 0
\end{array}$$

In addition, when p is a prime power, we can get a similar result [7]. So we will not discuss them here.

2. Orthogonal Latin square codes and its dual 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) An existence of 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 [8]. In his 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.

For any given two cells $(i,j),(i',j')$, we have the $(t+2)$-th coordinate $t\cdot i+j, t\cdot i'+j'$ of the codewords corresponding to $(i,j),(i',j')$ respectively. Since $(t\cdot i+j)+(t\cdot i'+j')$ is the $(t+2)$-th coordinate of the codeword corresponding to $(i+i',j+j')$, 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 .

Example 1. *Let $p = 3$. Then there exist 2 mutually orthogonal Latin squares,*

$$\begin{array}{ccc} & L_1 & \\ 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \qquad \begin{array}{ccc} & L_2 & \\ 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{array} .$$

Thus we get a [4, 2, 3] orthogonal Latin square code $\mathcal{L}_3$ of order 3 over GF(3) with 9 codewords

(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)

.

Then this code $\mathcal{L}_3$ is the only self-dual linear orthogonal Latin square code because for a 2-dimensional linear code $\mathcal{L}_p$, the dimension of self-dual code $\mathcal{L}_p^{\perp}$ is $p-1$ and $p-1=2$ only when $p=3$.

From [9], it is easy to see that a $[p+1,\ 2,\ p]$ orthogonal Latin square code $\mathcal{L}_p$ is a maximum distance separable (MDS) code. Thus this code has the maximum possible distance between codewords.

Consider the dual code $\mathcal{L}_p^{\perp}$ of $\mathcal{L}_p$. It is well known that the error correcting capability of a code is determined by the minimum distance between all pairs of distinct codewords. Since $\mathcal{L}_p$ is linear, so is $\mathcal{L}_p^{\perp}$. Thus the minimum distance of $\mathcal{L}_p^{\perp}$ is equal to the minimum weight among all non-zero codewords of $\mathcal{L}_p^{\perp}$. So if we use the weight enumerator of $\mathcal{L}_p^{\perp}$, we can find not only the minimum distance but also the error correcting capability of $\mathcal{L}_p^{\perp}$. Let A_i denote the number of codewords of weight i in $\mathcal{L}_p$. The number of codewords of weight i in $\mathcal{L}_p$ over GF(p) has been completely determined in [5] and [6], i.e.

$$\begin{aligned} A_i &= \binom{p+1}{i} \sum_{j=0}^{i-p} (-1)^j \binom{i}{j} (p^{i-p+1-j} - 1) \\ &= \binom{p+1}{i} (p-1) \sum_{j=0}^{i-p} (-1)^j \binom{i-1}{j} p^{i-p-j}. \end{aligned}$$

Thus

$$\begin{aligned} A_p &= \binom{p+1}{p}(p-1) \\ &= p^2 - 1. \end{aligned}$$

So, the weight enumerator $A(z)$ of $\mathcal{L}_p$ is $A_0 + A_p z^p$ where $A_0 = 1$, $A_p = p^2 - 1$. Let $B(z)$ denote the weight enumerator of the dual code $\mathcal{L}_p^{\perp}$. Then by [5] and [6] we have

$$\begin{aligned} B(z) &= p^{-2}(1+(p-1)z)^{p+1} A\left(\frac{1-z}{1+(p-1)z}\right) \\ &= p^{-2}(1+(p-1)z)\{(1+(p-1)z)^p + (p^2-1)(1-z)^p\} \\ &= 1 + B_3 z^3 + \cdots , \end{aligned}$$

where B_3 is the number of codewords of weight 3. Thus the minimum distance of $\mathcal{L}_p^{\perp}$ is 3, and so $\mathcal{L}_p^{\perp}$ is a single-error-correcting code. By [5], the dual code $\mathcal{L}_p^{\perp}$ is a $[p+1,\ p-1,\ 3]$ MDS linear code over GF(p). Therefore $\mathcal{L}_p^{\perp}$ is perfect code because $(1+(p+1)(p-1)) \cdot p^{p-1} = p^{p+1}$ where $1+(p+1)(p-1)$ is the number of vectors in a sphere of radius 1 about a codeword and p^{p-1} is the number of spheres.

Theorem 2 [9]. *Let C be an $[n,k,d]$ code over* GF(p) *with parity check matrix H. C is MDS if and only if every $n-k$ columns of H are linearly indenpendent.*

From Theorem 2 and concept for the Hamming code of order 2, the dual code $\mathcal{L}_p^{\perp}$ is the Hamming code of order 2 over GF(p).

3. Main Theorems

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:

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

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

H : parity check matrix (see previous Section).

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

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

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

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

But, if codeword $\mathbf{c}$ is changed into received word $\mathbf{r}$ with error $\mathbf{e}$. Then $\mathrm{s} = \mathrm{H}\,\mathbf{r}^T = \mathrm{H}(\mathbf{c}+\mathbf{e})^T = \mathrm{H}\,\mathbf{c}^T + \mathrm{H}\,\mathbf{e}^T = \mathrm{H}\,\mathbf{e}^T$. So the i-th coordinate s_i of syndrome 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 $\frac{p-1}{2}$.

Theorem 3. *Let* $\mathrm{r} = (r_1, \ldots, r_{p+1})$ *be a received word and* $\mathrm{s} = (s_1, \ldots, s_{p-1})$ *syndrome of* $\mathbf{r}$.

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

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

Proof of (1). By previous paragraph, $s_i = -i \cdot e_1 - e_2 + e_{i+2},\ 1 \le i \le p-1$.

($\Rightarrow$) If both r_1 and r_2 are correct, $e_1 = e_2 = 0$. So, $s_i \ne 0$ if and only if $e_{i+2} \ne 0$. But since Hamming weight of e is less than or equal to $\frac{p-1}{2}$, $M_0(\mathrm{s}) \ge \frac{p-1}{2}$.

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

Suppose that r_1 is not correct and r_2 is correct(i.e. $e_1 \ne 0$ 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. $M_0(\mathrm{s}) \le \frac{p-3}{2}$, which is contradict to 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 is contradict to 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 is contradict to 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 is contradict to hypothesis. □

Theorem 4. *Suppose that r_1 is not correct (i.e. In Theorem 3, 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 is contradict to 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 is contradict to hypothesis. □

Note: since $M_0(\mathrm{s}(e_1))$ and $M_b(\mathrm{s}(e_1))$ (for some $b \neq 0$) is greater than or equal to $\frac{p+1}{2}$ in Theorem 4. $M_0(\mathrm{s}(e_1)) = M_b(\mathrm{s}(e_1)) = \max\limits_{b \in GF(p)} M_b(\mathrm{s}(l))$ for $1 \leq l \leq p-1$. In (2) of Theorem 4, we can take i such that $\hat{s}_i = b$, $\hat{s}_{i+1} = b$, because $M_b(\mathrm{s}(e_1)) \geq \frac{p+1}{2}$. Then $c_1 = r_{i+3} - r_{i+2}$, $c_2 = r_{i+2} - i \cdot c_1$.

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

Algorithm

Step 1 : If $M_0(\mathrm{s}) \geq \frac{p-1}{2}$, then by Theorem 3-(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 3-(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 $\max\limits_{1 \leq l \leq p-1} M_0(\mathrm{s}(l)) \geq \frac{p+1}{2}$, then by Theorem 4-(1) codeword $\mathbf{c} = (A,\ r_2,\ A + r_2, \ldots, (p-1)A + r_2)$, where $A = r_{i+3} - r_{i+2}$ for the i satisfying the condition $\hat{s}_i = 0$, $\hat{s}_{i+1} = 0$ (the i-th coordinate satisfying this statement exists, because $\max\limits_{1 \leq l \leq p-1} M_0(\mathrm{s}(l)) \geq \frac{p+1}{2}$).

Step 4 : In the case that the conditions of Step 1 and Step 2 are not satisfied, if for some $b \neq 0$ $\max\limits_{1 \leq l \leq p-1} M_b(\mathrm{s}(l)) \geq \frac{p+3}{2}$, then $\mathbf{c} = (A,\ B,\ A + B, \ldots, (p-1)A + B)$, where $A = r_{i+3} - r_{i+2}$, $B = r_{i+2} - i \cdot A$ for the i satisfying the condition $\hat{s}_i = b$, $\hat{s}_{i+1} = b$.

Example 2. 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 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 3. 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 3-(2) r_1 is correct. By Step 2, we have $B = 3+4 = 2$ and $\mathbf{c} = (1,2,3,4,0,1)$.

Example 4. 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 5. Let $p = 5$, $\mathbf{r} = (2,1,3,4,0,1)$. Then the syndrome s of $\mathbf{r}$ is $(0,4,3,2)$. From $M_0(\mathrm{s}) < 2$, for any $b \neq 0$ $M_b(\mathrm{s}) < 3$, and $\mathrm{s}(1) = (1,\ 1,\ 1,\ 1)$, we get $M_1(\mathrm{s}(1)) \geq 4$ 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. F. J. MacWilliams, *A theorem on the distribution of weights in a systematic code*, Bell syst. Tech. J. **42** (1963), 79–84.

6. ——— and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North Holland, New York, 1993.
7. H. B. Mann, *On the construction of sets of orthogonal Latin squares*, Ann. Math. Statist. **14** (1943), 401–414.
8. R. Silverman, *A metrization for power sets with applications to combinatorial analysis*, Canad. J. Math. **12** (1960), 158–176.
9. R. C. Singleton, *Maximum distance Q-nary codes*, IEEE Trans. Inform. Theory **IT-10** (1964), 116–118.

Department of Mathematics, Korea Advanced Institute of Science and Technology, Taejon 305-701, South Korea