Indian J. pure appl. Math., **28**(9) : 1235-1240, September 1997

A DECODING ALGORITHM FOR ORTHOGONAL LATIN SQUARE CODES

S. HAHN, D. G. KIM AND Y. S. KIM

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

(*Received* 6 *February* 1996; *after final revision* 10 *April* 1997; *accepted* 21 *April* 1997)

Let p be an odd prime number. We introduce simple and useful decoding algorithm for the orthogonal Latin square codes of order p. This is based on the syndrome decoding for linear codes.

Key Words : Decoding Algorithm; Orthogonal; Latin Square Codes; Hamming Weight; Elements of Cardinality; Parity Check Matrix; Syndrome

1. INTRODUCTION

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

Definition — The set $\mathcal{L}_p = \{(i, j, i+j, ..., (p-1)i+j) \mid i, j \in GF(p)\} \subset GF(p)^{p+1}$ is called orthogonal Latin square code of order p.

Clearly $\mathcal{L}_p$ is linear subspace of dimension 2 in $GF(p)^{p+1}$ and has minimum distance p. So $\mathcal{L}_p$ is $[p+1, 2, p]$-linear code (see[1, 2]).

For all $(i, j, i+j, ..., (p-1)i+j) \in \mathcal{L}_p$,

$$(i, j)\begin{bmatrix} 1 & 0 & 1 & 2 & 3 & \dots & (p-1) \\ 0 & 1 & 1 & 1 & 1 & \dots & 1 \end{bmatrix} = (i, j, i+j, ..., (p-1)i+j).$$

So the generator matrix G of orthogonal Latin square code $\mathcal{L}_p$ is :

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

where I_2 is 2×2 identity matrix and

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

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

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

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

If codeword $c \in \mathcal{L}_p$ is changed into r (i.e. $r = c + e$, where e is error vector), the syndrome s of received word r is : $s = Hr^T = Hc^T + He^T$. So, for $i = 1, \dots, p-1$, $s_i = -i \cdot e_1 - e_2 + e_{i+2}$, where $s = (s_1, \dots, s_{p-1})^T$ and $e = (e_1, \dots, e_{p+1})$.

2. The Syndrome Decoding Algorithm of $\mathcal{L}_p$

For convenience, we first define the following notation :

$c = (c_1, \dots, c_{p+1})$: codeword in $\mathcal{L}_p$,

$r = (r_1, \dots, r_{p+1})$: received word

and $e = (e_1, \dots, e_{p+1})$: error vector,

i.e. $r = c + e$.

H : parity check matrix (see previous Section).

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

$M_b(s)$: for some syndrome $s = (s_1, \dots, s_{p-1})^T$ and some $b \in GF(p)$,

$M_b(s) = \#\{i \mid s_i = b,\ 1 \le i \le p-1\}$.

Since $\mathcal{L}_p$ has minimum distance p, we always assume that the Hamming weight of e is less than equal to $\frac{p-1}{2}$.

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

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

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

PROOF OF (1) : By Section 1, $s_i = -i \cdot e_1 - e_2 + e_{i+2}$, $1 \le i \le p-1$.

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

($\Leftarrow$) 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. $M_0(s) \leq \frac{p-3}{2}$, which is contradict to hypothesis.

Suppose that r_1 is not correct and r_2 is correct (i.e. $e_1 \neq 0$ 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. $M_0(s) \leq \frac{p-3}{2}$, 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. $M_0(s) \leq 1 + \frac{p-5}{2} = \frac{p-3}{2}$. 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 $b = -e_2$, $M_b(s) \geq \frac{p+1}{2}$.

($\Leftarrow$) 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 $b \neq 0$, $\{i \mid s_i = -i \cdot e_1 + e_{i+2} = b\} \subset \left\{ i \mid e_{i+2} = 0,\ i = \frac{b}{e_1} \right\} \cup \{i \mid e_{i+2} \neq 0\}$. Thus $M_b(s) \leq 1 + \frac{p-3}{2} = \frac{p-1}{2}$. 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 $b \neq 0$, $\{i \mid s_i = -i \cdot e_1 - e_2 + e_{i+2} = b\} \subset \{i \mid e_{i+2} = 0\} \cup \left\{ i \mid e_{i+2} \neq 0,\ i = \frac{b + e_2 - e_{i+2}}{e_1} \right\}$. Hence $M_b(s) \leq 1 + \frac{p-5}{2} = \frac{p-3}{2}$. This is contradict to hypothesis.

Remark : In the above Theorem, we get the criterion whether or not the first coordinate r_1 of received word r is correct. But if r_1 is not correct, how do we determine the second coordinate r_2 of received word r to be correct or not ?

(1) Let $r = (r_1, ..., r_{p+1})$ be a received word and r_1 not correct. If r_2 is correct, then a set $R = \{r'_{i+2} \mid r'_{i+2} = i^{-1}(r_{i+2} - r_2),\ i = 1, ..., p-1\}$ has element A of its cardinality $\geq \frac{p+1}{2}$, where A is the first coordinate of codeword which is changed into r. Conversely if $R = \{i^{-1}(r_{i+2} - r_2) \mid i = 1, \ldots p-1\}$ has element A' of cardinality $\geq \frac{p+1}{2}$, then $c = (A', r_2, A' + r_2, ..., (p-1)A' + r_2)$ is codeword that is changes into r because the Hamming distance of c and r is less than equal to $\frac{p-1}{2}$. Thus r_2 is correct.

(2) In (1), we get the criterion that when r_1 is not correct, whether r_2 is correct or not. Now let us see how to recover codeword c from r, when both r_1 and r_2 are not correct.

For $i = 1, ..., p-2$,

$$r_{i+3} - r_{i+2} = \begin{cases} A & \text{if both } r_{i+2} \text{ and } r_{i+3} \text{ are correct} \\ \text{some value} & \text{otherwise,} \end{cases}$$

where A is the first coordinate of codeword c which is changed into r.

If, for $1 \leq i \leq p-1$, r_{i+2} is not correct, it effects on two values $r_{i+3} - r_{i+2}$ and $r_{i+2} - r_{i+1}$. But since errors in $r_3, ..., r_{p+1}$ are at most $\frac{p-5}{2}$ and the number of values $r_{i+3} - r_{i+2}$ ($i = 1, ..., p-2$) are $p-2$, so A appears at least in $r_{i+3} - r_{i+2}$ ($i = 1, ..., p-2$) 3 times. i.e., $(p-2) - 2 \cdot \left(\frac{p-5}{2}\right) = 3$. Hence elements of its cardinalitty ≥ 3 in $\{r_4 - r_3, r_5 - r_4, ..., r_{p+1} - r_p\}$ are candidates for A.

If A' is candidate for A, then for some i ($i = 1, ..., p-2$), $A' = r_{i+3} - r_{i+2}$. So, for $B' = r_{i+2} - i \cdot A'$, $(A', B', A' + B', ..., (p-1)A' + B')$ is candidate for codeword c which is changed into r. Hence at most of $\frac{p-1}{3}$ candidates for codeword c, the candidate which is of Hamming distance from $r \leq \frac{p-1}{2}$ is codeword c.

ALGORITHM

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

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

Step 3 : In the case that the conditions of Step 1 and step 2 are not satisfied, if $\{i^{-1}(r_{i+2} - r_2) \mid i = 1, \ldots p-1\}$ has element A of its cardinality $\geq \frac{p+1}{2}$, then r is decoded into $c = (A, r_2, A + r_2, \ldots, (p-1)A + r_2)$ by Remark-(1).

Step 4 : In the case that the conditions of Step 1 and Step 2 are not satisfied, if $\{i^{-1}(r_{i+2} - r_2) \mid i = 1, \ldots, p-1\}$ has no element of cardinality $\geq \frac{p+1}{2}$ (i.e. both r_1 and r_2 are not correct), we see Remark-(2).

Example 1 — Let $p = 5$, $r = (2, 3, 1, 3, 4, 1)$.

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

is the parity check matrix for $\mathcal{L}_5$. Then the syndrome s of r

$$Hr^T = \begin{bmatrix} 4 & 4 & 1 & 0 & 0 & 0 \\ 3 & 4 & 0 & 1 & 0 & 0 \\ 2 & 4 & 0 & 0 & 1 & 0 \\ 1 & 4 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \\ 1 \\ 3 \\ 4 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}.$$

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

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

Example 3 — Let $p = 5$, $r = (3, 2, 1, 0, 2, 3)$. Then the syndrome s of r is $(1, 2, 1, 4)^T$. We have $M_0(s) < 2$ and $M_b(s) < \frac{5+1}{2} = 3$, for $b = 1, 2, 3, 4$. But $\{r_3 - r_2, 2^{-1}(r_4 - r_2), 3^{-1}(r_5 - r_2), 4^{-1}(r_6 - r_2)\} = \{4, 4, 0, 4\}$ has element 4 of cardinality $\geq \frac{5+1}{2} = 3$. By Step 3, r is decoded into $c = (4, 2, 1, 0, 4, 3)$.

Example 4 — Let $p = 5$, $\boldsymbol{r} = (2, 1, 3, 4, 0, 1)$. Then the syndrome s of $\boldsymbol{r}$ is $(0, 4, 3, 2)^T$. Since $M_0(s) < 2$ and $M_b(s) < 3$, $\{r_3 - r_2, 2^{-1}(r_4 - r_2), 3^{-1}(r_5 - r_2), 4^{-1}(r_6 - r_2)\} = \{2, 4, 3, 0\}$ has no element of cardinality ≥ 3. By Step 4 (Remark-(2)), $\{r_{i+3} - r_{i+2} \mid i = 1, 2, 3\} = \{1, 1, 1\}$ has element 1 of cardinality ≥ 3. Thus 1 is the first coordinate of codeword $\boldsymbol{c}$ and the second coordinate of $\boldsymbol{c}$ is 2. Hence $\boldsymbol{c} = (1, 2, 3, 4, 0, 1)$.

REFERENCES

1. R. C. Bose and B. Manvel, *Introduction to Combinatorial Theory*, John Wiley & Sons, New York, (1984), p. 135-144.
2. 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.