LINEAR CODE THROUGH POLYNOMIAL MODULO Z_n

MAKARIM ABDULWAHIDE
DEPT. OF INFORMATION SYSTEMS -COLLEGE OF COMPUTERS -UNIVESITY OF AL-ANBAR

Abstract :-
A polynomial \( p(x) = a_0 + a_1 x + \ldots + a_d x^d \) is said to be a permutation polynomial over a finite ring \( R \) if \( P \) permute the elements of \( R \). where \( R \) is the ring \( (Z_n, +, \cdot) \).
It is known that mutually orthogonal Latin of order \( n \), where \( n \) is the element in \( Z_n \) generate \( A, [2] \) - error correcting code with \( n^2 \) code words. And we found no a pair of polynomial defining a pair of orthogonal Latin square modulo \( Z_n \) where \( n = 2^w \) generate a linear code.

Keywords: Linear code, polynomial, modulo \( Z_n \)

Introduction :-
A polynomial \( p(x) = a_0 + a_1 x + \ldots + a_d x^d \) with integral coefficient is a permutation polynomial modulo \( n \) if and only if \( a_1 \) is odd and \((a_2 + a_4 + a_6 + \ldots)\) is even and \((a_3 + a_5 + a_7 + \ldots)\) is even, and this condition satisfies where \( n = 2^w \), \( w \geq 2 \) and this condition depend only on the parity of the coefficient. It is easy to state necessary and sufficient condition for polynomial to represent a Latin square of order \( n = 2^w \).
Latin square are dealt with extensively in Denes and Keed well [1974]. Two \( n \times n \) Latin squares \( A = a_{ij} \) and \( B = b_{ij} \) are orthogonal if Latin square:
\[
\{(a_{ij}, b_{ij}) : i, j \in \{0, 1, 2, \ldots, n-1\}\} = n^2
\]
As set of \( t > 0 \) Latin squares are pairwise mutually orthogonal if every pair of Latin squares in the set are orthogonal. A code \( C \) is Linear if the addition of any two code words is another codeword. A \( n \times n \) matrix \( L = L^\perp \) is a Latin square that generate a linear code modulo \( n \) iff \( L \) is of the form \( L^\perp = (i^{\beta} + j^{\alpha}) \mod n \) for some integer \( \alpha, \beta \) satisfying:
\[
1- 0 < \alpha, \beta < n
\]
\[
2- \gcd (\alpha, n) = \gcd (\beta, n) = 1
\]
This condition characterize every Latin square that generate a linear code modulo \( n \), and if \( n \) is even or a power of 2 are not very useful in terms of generating linear codes modulo \( n \). characterizing permutation polynomial:

Theorem (1) : Let \( p(x) = a_0 + a_1 x + \ldots + a_d x^d \) be a polynomial with integral coefficient and its a permutation polynomial modulo \( Z_n \) where \( n = 2^w \) where \( w > 0 \), and
Let \( m = 2^{w-1} = \frac{n}{2} \). Then \( p(x) \) is permutation polynomial modulo \( m \).

Proof: Clearly, \( p(x+m) = p(x)(\text{mod } m) \) for any \( x \).

Assume that \( p(x) \) is permutation polynomial modulo \( n \) if \( p \) is not a permutation polynomial modulo \( m \), such that \( p(x) = p(x') = y \) (mod \( m \)), for some \( y \).

This collision means there are four values \( \{ x, x + m, x', x' + m \} \) modulo \( n \) that \( p \) maps to a value congruent to \( y \) modulo \( m \).

But there can only be two such values if \( p \) is a permutation polynomial, since there are only two values in \( \mathbb{Z}_n \) congruent to \( y \) modulo \( m \).

Lemma: Let \( p(x) = a_0 + a_1 x + \ldots + a_d x^d \) be polynomial with integral coefficient, and let \( n = 2m \), if \( p(x) \) is a permutation polynomial modulo \( n \), then \( p(x + m) = p(x) + m \) (mod \( n \)) for all \( x \in \mathbb{Z}_n \).

Proof: This follows directly from theorem (1), since the only two values modulo \( n \) that are congruent modulo \( m \) to \( p(x) \) are \( x \) and \( p(x) + m \).

Example: The following are permutation polynomial modulo \( z^n \) where \( n = 2^w \) where \( w > 1 \):

- \( x(a + bx) \) where \( a \) is odd and \( b \) is even.
- \( x + x^2 + x^4 \).

1+ \( x + x^2 + \ldots + x^d \), where \( d = 1 \) (mod 4)

Theorem (2): A polynomial

\[
p(x, y) = \sum_{i,j} a_{ij} x^i y^j
\]

represents a Latin square modulo \( n = 2^w \) where \( w \geq 2 \), iff

the four polynomials \( p(x,0), p(x,1), p(0,y) \) and \( p(1,y) \), and are all permutation polynomial modulo \( n \).

Example: Second-degree polynomial representing a Latin square modulo \( n = 2^w \)

\( 2xy + x + y = x \). (2y+1)+y = y. (2x + 1) + x.

A method of constructing an error-correcting code of distance \( t+1 \) with \( n^2 \) code words of length \( t+2 \) when given \( t \) mutually orthogonal Latin square:

Given \( t \) mutually orthogonal Latin square

\( L_1, L_2, \ldots, L_t \), the code is the set of all code words of the form \( (i,j, l_1, l_2, \ldots, l_t) \) where \( l_i \) is the I-\( j \)-th entry of \( L_i \), \( l_2 \) is the I-\( j \)-th entry of \( L_2 \) and \( l_t \) is the I-\( j \)-entry of \( L_t \) where \( 1 \leq k \leq t \).

The following example using two orthogonal Latin square of order 3, with our notation the two Latin square are:

\[
\begin{bmatrix}
0 & 1 & 2 \\
1 & 2 & 0 \\
2 & 0 & 1
\end{bmatrix},
\begin{bmatrix}
0 & 1 & 2 \\
1 & 2 & 0 \\
2 & 0 & 1
\end{bmatrix}
\]

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

A noteworthy feature of this code is that it is also a linear code when addition and multiplication are defined modulo \( n \).

If \( C \) is a linear code we say that these Latin square generate a linear code modulo \( n \), where \( n \) is the order of Latin squares.

The following theorem provides necessary and sufficient conditions for two Latin square that generate linear codes modulo \( n \) by themselves to be orthogonal. Two such orthogonal Latin square when taken together generate another linear code modulo \( n \).

Theorem (3):

let \( A = (a_0, a_1, \alpha_1, \beta_1) \) and

\( B = (b_0, b_1, \alpha_2, \beta_2) \). then \( A \) and \( B \) are orthogonal iff

\[\gcd (\beta_1 \alpha_1, \beta_2 \alpha_2, n) = 1\]

Proof: Assume that \( A \) and \( B \) are orthogonal.

corresponding entries of \( A \) and \( B \) are equal : \( (g,h) = (a_0, a_1, b_0, b_1) = (a_0, a_1, b_0, b_1) \)
Then, by ( let $A = (\alpha, \gamma, \beta)$ 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 $a_{i,g^2g^{-1}}$ (**) , we have
\begin{align*}
    j_1 &= g \beta_1 \alpha_1 ^{-1} - i_1 \beta_1 \alpha_1 ^{-1} = h \alpha_2 ^{-1} -  \\
    i_1 \beta_2 \alpha_2 ^{-1} &= j_i \quad \ldots \ldots \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 \ldots \ldots \quad (2)
\end{align*}
subtracting (1) from (2) yields
\begin{align*}
    i_1 \beta_1 \alpha_1 ^{-1} - i_2 \beta_1 \alpha_1 ^{-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 & (\beta_1 \alpha_1 ^{-1} - \beta_2 \alpha_2 ^{-1}) = 0
\end{align*}
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)
\[
    \text{We see that } j_1 = j_2.
\]
Now, assume
\[
    \gcd (\beta_1 \alpha_1 ^{-1} - \beta_2 \alpha_2 ^{-1}, n) > 1,\text{ then}
\]
for some integer $k$, $0 < k < n$
We have that $k(\beta_1 \alpha_1 ^{-1} - \beta_2 \alpha_2 ^{-1}) = 0$
, from (**) , $0$ 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 $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}
\]
This means that the pair $(0,0)$ occurs twice among corresponding entries from $A$ and $B$ are not orthogonal .

**Lemma** : Let $A= (\alpha, \gamma, \beta)$ and $B= (\beta, \gamma, \beta)$ then
\begin{enumerate}
    (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 $\gcd (\alpha_2 - \beta_2, n) = 1$.
\end{enumerate}
(3) if $\alpha_1 = \alpha_2$ then $A$ and $B$ are
orthogonal iff $\gcd (\beta_2 - \beta_1, n) = 1$ .

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

It is of interest to know how many mutually orthogonal Latin square of some $n$
exist that together generate a linear code modulo $n$.

The following theorem gives an upper bound for this number .

Theorem (4) : suppose that the prime
factorization of $n$ is $n = p_1 \ p_2 \ldots p^h$, such
that $p_1 \leq p_2 \ldots \leq p^h$ and $p_1 \ p^2 \ldots p^h$
are prime . then there are at most $p_1 - 1$
mutually orthogonal Latin square of order $n$ that generate a linear code modulo $n$ .

proof : suppose that there exist a set of
more than $p_1 - 1$ mutually orthogonal
Latin square of order $n$ that generate a linear code modulo $n$ .

Fix one of the Latin square in $S$ , say
$A = (\alpha, \gamma, \beta)$ .
We have
\[
    \text{consider the set of difference}:
\]
\[
    D = \{(\beta_1 \alpha_1 ^{-1} - \beta_2 \alpha_2 ^{-1}, n) \} \\
    (1^m, \alpha m, \beta m) \in (S - \{A\})(\mod p^1)
\]
Suppose that there exist two Latin square
$B=(\beta, \gamma, \beta_2)$ and $C= (\gamma, \alpha_3, \beta_3)$
In $S - \{A\}$ such that $\beta_1 \alpha_1 ^{-1} \beta_2 \alpha_2 ^{-1}$
$\equiv \beta_1 \alpha_1 ^{-1} \beta_2 \alpha_2 ^{-1} \equiv 0 \ (\mod p^1)$
This implies that $\beta_2 \alpha_2 ^{-1} \beta_3 \alpha_3 ^{-1}$
$\equiv 0 \ (\mod p^1)$ . however by theorem (3)
We have $B$ 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 $S - \{A\}$ contribute a distinct element to $D$.

This means that there are exactly $p_1 - 1$
elements in $S - \{A\}$ and that $D=\{1,2, p_1 - 1\}$
There for $\beta_1 \alpha_1 ^{-1} \mod p_1 \in D$ . So for some Latin square $K=(1,\gamma, \alpha_3, \beta)$ 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 \(( n \times n)\) Latin square \( L = l_{ij} \) generate a linear code modulo \( n \) then \( l_{100} = 0 \)

\( K \) is not a Latin square.

Theorem (5) : suppose that the prime factorization of \( n \) is \( n = p^1 p^2 \ldots p^h \), such that \( p^1 \leq p^2 \leq \ldots \leq p^h \) and \( p^1 p^2 \ldots p^h \) are prime. Then there exists such that \( p^1 - 1 \) mutually orthogonal Latin square 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 square of the form \( \text{rm} \) \( L = (l_{ij}^k : \alpha, \beta) \) as \( k \) ranges from 1 to \( p^1 - 1 \) mutually orthogonal by \((\text{Lemma}^* \text{ above part 3})\).

So by \((\text{theorem} 4)\) this is a maximal set of mutually orthogonal Latin square of order \( n \) that generate a linear code modulo \( n \).

Example: we give an example of a linear code generated from 4 mutually orthogonal Latin square of order 5. We use the method described in the proof of theorem (5) with \( \alpha = 4 \):

\[
\begin{align*}
0 & \ 4 \ 3 \ 2 \ 1 \\
1 & \ 0 \ 4 \ 3 \ 2 \\
2 & \ 1 \ 0 \ 4 \ 3 \\
3 & \ 2 \ 1 \ 0 \ 4 \\
4 & \ 3 \ 2 \ 1 \ 0
\end{align*}
\]

\[
\begin{align*}
0 & \ 4 \ 3 \ 2 \ 1 \\
1 & \ 0 \ 4 \ 3 \ 2 \\
2 & \ 1 \ 0 \ 4 \ 3 \\
3 & \ 2 \ 1 \ 0 \ 4 \\
4 & \ 3 \ 2 \ 1 \ 0
\end{align*}
\]

The code \( C \) generated by these Latin square is \( C = (0,0,0,0,0,0) \), \( (0,1,4,4,4,4) \), \( (0,2,3,3,3,3),(0,3,2,2,2,2),(0,4,1,1,1,1) \), \( (1,0,1,2,3,4),(1,1,0,1,2,3),(1,2,4,0,1,2),(1,3,3,4,0,1),(1,4,2,3,4,0),(2,0,2,4,1,3) \), \( (2,1,1,3,0,2),(2,2,0,2,4,1),(2,3,4,1,3,0),(2,4,3,0,2,4),(3,0,31,4,2),(3,1,2,0,3,1) \), \( (3,2,1,4,0,2),(3,4,2,0,3),(4,0,4,3,2,1),(4,1,3,2,1,0),(4,2,2,1,0,4),(4,3,1,0,4,3) \).

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

\[
(0,0,0,0,0,0) + (0,1,4,4,4,4) + (0,2,3,3,3,3) + (0,4,1,1,1,1) = (0,0,0,0,0,0)
\]

And \( L_1 = l_{ij}^1 \) defined by \( l_{ij}^1 = (2^k i + j) \) mod \( n \)

\( L_2 = l_{ij}^2 \) defined by \( l_{ij}^2 \equiv (2^{k-1} i + j) \pmod{n} \)

This works whenever \( 2^k < n \) because

\( L_1 = (l_{ij}^1, 1, 2^k) \) and \( L_2 = (l_{ij}^2, 1, 2^{k-1}) \)

However by \((\text{lemma}^* \text{ part (3)})\) these are orthogonal because,

\( \gcd(2^k - 2^{k-1}, n) = \gcd(2, n) = 1 \), since \( n \) is odd.

When \( n = 2^w \), the following theorem show that there are no pair of mutually orthogonal Latin square of even order.

Theorem (6) : there are no two polynomial \( P_1(x, y) \), \( P_2(x, y) \) modulo 2\( ^w \) for \( w \geq 1 \) that form a pair of orthogonal Latin squares.

Proof: \((\text{Lemma}^*)\) implies that \( P(x + m, y + m) = P(x) + m \pmod{m} \) for any permutation polynomial modulo \( n = 2m \).

Thus \( P_1(x + m, y + m) = P_1(x + m, y) + m \pmod{n} \) = \( P_1(x, y) + 2m \pmod{n} \) = \( P_1(x, y) \pmod{n} \)

Therefore \((P_1(x, y), P_2(x, y))\) = \((P_1(x + m, y + m), P_2(x + m, y + m))\) and the pair \((P_1, P_2)\) fails at being a pair of orthogonal Latin squares.
Theorem (7) : 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 (if $n \times n$ Latin square $L = l_{ij}$ generate a linear code modulo $n$ then $l_{00} = 0$),

$2(0,k,a_{0k},b_{0k}) = (0,2k,2a_{0k},2b_{0k})$

$= (0,0,2a_{0k},2b_{0k}) = (0,0,0,0)$.

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.

References