P- ISSN 1991-8941 E-ISSN 2706-6703
2007,(1), (3) :117-121
Journal of University of Anbar for Pure Science (JUAPS)
Open Access

LINEAR CODE THROUGH POLYNOMIAL MODULO Z^n

MAKARIM ABDULWAHIDE

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

ARTICLE INFO

Received: 5 / 5 /2007
Accepted: 25 / 11 /2007
Available online: 14/6/2012
DOI: 10.37652/juaps.2007.15603

Keywords:
Linear code ,
polynomial ,
modulo z^n .

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 $(Z^n , + , \bullet)$.

It is known that mutually orthogonal Latin of order n,where n is the element in Z^n generate A $[\frac{1}{2}]$ – 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.

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 $L= L^{ij}$ is a Latin square that generate

a linear code modulo n iff L is of the form $L^{ij} = (i\beta + j\alpha) \bmod n$ for some integer α , β 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 $m= 2^{w-1} = n/2$. Then p(x) is permutation polynomial modulo m .

proof :Clearly,p(x +m)=p(x)(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 $p(x) = p(x') = y \pmod m$, for some y .

* Corresponding author at: DEPT. OF INFORMATION SYSTEMS -COLLEGE OF COMPUTERS -UNIVESITY OF AL-ANBAR, Iraq.E-mail address: mak_alturky@yahoo.com

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 Z^{n} congruent to y modulo m .

Lemma* :

Let p(x)= a^{0} + a^{1} x + …+ 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 $\in$ 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} w > 1 :

- x(a+ bx) where a is odd and b is even .
- x + x^{2} + x^{4} .
- 1+ x + x^{2} + …+ 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 polynomial p(x,0) , p(x,1) , p(0,y) and p1,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}, … , L^{t} , the code is the set of all code words of the form (i,j , l^{1}, l^{2}, … 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-entry of L^{k} 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 :

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

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

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^{ij} , α_{1} , β_{1}) and B=(b^{ij} , α_{2} , β_{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^{i1j1} , b^{i1j1}) = (a^{i2j2}, b^{i2j2})

Then , by (let A = (a^{ij} , α , β) 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 $a^{i,g\alpha^{-1}-i\beta\alpha^{-1}}$) ….(*) , we have

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

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

subtracting (1) from (2) yields

$i_1\beta_1\alpha_1^{-1} - i_2\beta_1\alpha_1^{-1} =$

$i_1\beta_2\alpha_2^{-1} - i_2\beta_2\alpha_2^{-1}$

$\Rightarrow i_1\beta_1\alpha_1^{-1} - i_2\beta_1\alpha_1^{-1} - i_1\beta_2\alpha_2^{-1} + i_2\beta_2\alpha_2^{-1} = 0$

$\Rightarrow i_1(\beta_1\alpha_1^{-1} - \beta_2\alpha_2^{-1}) - i_2(\beta_1\alpha_1^{-1} - \beta_2\alpha_2^{-1}) = 0$

$\Rightarrow (i_1 - i_2)(\beta_1\alpha_1^{-1} - \beta_2\alpha_2^{-1}) = 0$

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 (*) , 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 $A = (a_{ij}, \alpha_1, \beta_1)$ 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 $\alpha_1 = \beta_1 \neq \beta_2$ 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 cods 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 $p_1 \leq p_2 \leq \ldots \leq p_h$ 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 cods 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

$A = (a_{ij}, \alpha_1, \beta_1)$

consider the set of difference :

$D = \{ (\beta_1\alpha_1^{-1} - \beta_m\alpha_m^{-1}) :$

$(l^m_{ij}, \alpha_m, \beta_m) \in (S - \{A\}) \} (\bmod\ p_1)$

Suppose that there exist two Latin square $B = (b_{ij}, \alpha_2, \beta_2)$ 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 (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 $\beta_1\alpha_1^{-1} \bmod p_1 \in D$. 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 (if $n \times n$

Latin square $L = l^{ij}$ generate a linear code modulo n then $l^{00} = 0$)

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 $p^1 \le p^2 \le \ldots . \le p^h$ 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 α be an integer in the range $0 < \alpha < n$ that is relatively prime to n .

then the p^1 - 1 Latin square of the of the form rm L $L^k = (l^{ij^k} : , \alpha , \beta)$ as k ranges from 1 to p^1 - 1 mutually orthogonal by

(Lemma ** above part 3) .

so by (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 generate from 4 mutually orthogonal Latin square of order 5 . we use the method described in the proof of theorem (5) with $\alpha = 4$:

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

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

The code C generate 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),
(3,2,1,4,2,0),(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) .

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

(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 .

We can easily develop for computing pairs of orthogonal Latin square that generate a linear code modulo n , for any odd n using (lemma **) above

$L^1 = l^{ij}$ defined by $l^{ij} = (2^k \, i + j) \bmod n$

And $L^2 = l^{ij}$ 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(lemma ** part (3)) these are orthogonal because ,

$\gcd (2^k - 2^{k-1}, n) = \gcd (2^{k-1}, n) = 1$, 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 $w \ge 1$ that form a pair of orthogonal Latin squares .

proof: (Lemma *) implies that $P(x +m, y +m) = P(x) + m \pmod m$ for any permutation polynomial modulo n = 2m .

thus $P_i(x +m , y +m)=P_i(x +m, y) +m \pmod n$ = $P_i(x , y) + 2m \pmod n$

$= P_i(x , y) \pmod n$

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 $l^{00} = 0$) , $2(0, k, a^{0k} , b^{0k})$

$= (0 , 2k , 2 a^{0k} , 2 b^{0k})$

$= (0,0, 2 a^{0k} , 2 b^{0k}) = (0,0,0,0)$.

This means that 2 a^{0k} = 0 and 2 b^{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 , 2 a^{k0} , 2 b^{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

[1] Marshall Hall, Jr. Combinatorial Theory. Blaisdell publishing company , 1967 .

[2] G.H. Hardy and E. M. Wright. An Introduction to the theory of Numbers,Oxford Clarendon Press , fourth edition , 1983 .

[3] Rudolf Lidl and Gary L. Mullen. When dose a polynomial over a finite field permute the elements of the field ? The American Math. Monthly, 95 (3) : 243- 246 , Mar 1988 .

[4] Rex Matthews. Permutation properties of the polynomial 1+ x + … + x^k over a finite field . Proc. Amer. Math. Soc., 120(1):47-51. Jan 1994 .

[5] G. Mullen and H. S tevens . Polynomial function (mod m) . Acta Mathematica Hungaria, 44(3-4):237-241 , 1984 .

[6] Joachim von Gathen. Tests for permutation polynomials . SIAM J. Computing, 20(3) : 591-602, June 1991 .

[7] J.Denes and A.D. Keedwell , Latin square and their applications , A cademic Press , New York and London , (1974) .

[8] John B. Fraleigh , A First Course in Abstract Algebra , Addison – Wwsley , Massachusetts , (1997) .

الرمز الخطي لمتعددة حدود مقياس n

مكارم عبد الواحد عبد الجبار

قسم نظم المعلومات– كلية الحاسوب–جامعة الانبار

Email: mak_alturky@yahoo.com

الخلاصة:

متعددة الحدود $p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_d x^d$ تسمى متعددة حدود تبادلية على الحقل النهائي R إذا كان P تبادل عناصر الحقل R . حيث R هي $(Z^n, +, \cdot)$. والمربعات اللاتينية المتبادلة المتعامدة من المرتبة n حيث انه n هي من عناصر الإعداد الصحيحة Z^n تولد 2/1 من الرمز الخاطئ المصحح ل n^2 من الكلمات المرمزة . وكذلك لا يوجد زوج من متعددة الحدود يعرف لنا زوج من المربعات اللاتينية المتعامدة مقياس Z^n عندما تكون قيمة $n = 2^w$ التي تولد الرمز الخطي .