Survey of Primitive Idempotents in FC_{p^n}

[1]Prateek Mor, [2]Monika
[1] Research Scholar , [2]Research Scholar
[1] Department of Mathematics
[1]Maharshi Dayanand University , Rohtak, India

Abstract : This paper gives a brief survey of primitive idempotents in FC_{p^n} for different cases. The expressions for these idempotents are listed. Initially the generating polynomial for cyclic codes is given.

***IndexTerms* - Cyclic Cosets, Idempotents**

I. INTRODUCTION

The theory of detecting and correcting the error was first introduced by Claude Shannon in 1948 in his paper “Mathematical Theory of Communication”. In his paper Shannon said that we can easily transmit any information by coding. There are number of special codes such as cyclic codes, Linear codes, Group codes, polynomial codes etc. Our interest in this paper is to study a very important class of codes called “Cyclic Codes”.

II. Generating Polynomial

Besides the generating polynomial, there are many other polynomials that can be used to generate a cyclic code. One such polynomial called an idempotent generator, can also be used to generate a cyclic code. As the ring R_n is semi-simple therefore each ideal in R_n contains a unique idempotent which also generates the ideal. This idempotent is called the generating idempotent of the corresponding cyclic code. The idempotent generating the minimal ideal (minimal code) in R_n is called a **Primitive idempotent.**

It is well known that the generating polynomial g(x) of the ideal in R_n is a factor of x^n-1. Thus the study of ideal through the generating polynomial depends on the factorization of x^n-1 over the field F. But the factorization of x^n-1 into its irreducible factors in itself is a very difficult problem. To overcome the problem of factorization, we deal with the idempotents that generates the ideals. These idempotents then help us to describe the cyclic codes completely.

Let F=GF(l) be a finite field of order l and n be any integer such that char (F) does not divide n.

Consider the set

$$S = \{0, 1, 2,\ldots,n-1\}.$$

For a, b $\in$ S, say that a ~b if a $\equiv$ bl^i (mod n) for some integer i $\geq$ 0. This is an equivalence relation on set S. The equivalence classes of this relation are called l - cyclotomic class modulo n. The l -cyclotomic coset modulo n containing s $\in$ S is

$$C_s = \{s, sl, sl^2, \ldots, sl^{t_s-1}\},$$

where t_s is the least positive integer with $sl^{t_s-1} \equiv s$ (mod n). Each cyclotomic coset is associated with an irreducible polynomial in the semi simple ring $R_n = \frac{F[x]}{<x^n-1>}$ and hence is also associated with a primitive idempotent in R_n that generates a minimal ideal in R_n equivalently a minimal cyclic code over F. The number of l - cyclotomic class modulo n depends on t, the multiplicative order of l modulo n, where $1 \le t \le \varphi(n)$. Throughout the whole discussion we will assume that F is the field of order q, the group is cyclic and is generated by g.

III. Primitive Idempotents in FC_{p^n}

Let $C_{p^n} =< g >$ be the Cyclic Group. Berman[2] described an explicit expressions for the (n+1) primitive idempotents in FC_{p^n} (without proof), where q is the order of the field, is a prime number such that (q,p)=1 and is primitive root modulo p^i for all $i \ge 1$. Blake and Mullin[3] declared that it is tedious to verify that these expressions are idempotents in FC_{p^n}. Arora and Pruthi[1] gave

an explicit expressions for the (n+1) primitive idempotents in FG(the group algebra of the cyclic group G of order p^n,p is an odd prime,n>1) over the finite field F of prime power order q with (q,p) = 1 and q is primitive root modulo p^n.
In 1997, Arora-Pruthi[1] descried the (n+1) primitive idempotents of FC_{p^n} given by:

$$e_0 = \frac{1}{p^n}\left(1+\sum_{i=1}^{n}\bar{C}_i\right)$$

and for $1 \le i \le n$,

$$e_i = \frac{1}{p^n}\left((p-1)\left(1+\bar{C}_{i+1}+\bar{C}_{i+2}+\ldots+\bar{C}_n\right)-\bar{C}_i\right)$$

where

$$\bar{C}_i = \sum_{s\in C_i} g^s$$

In 2002, Arora, Batra, Cohen and Pruthi[11] described (2n+1) primitive idempotents given by:

$$e_0 = \frac{1}{p^n}\left(1+\sum_{j=1}^{n}\bar{C}_j\right)$$

and

$$e_i = \frac{1}{2}\left(Y_i+\theta G_i\right)$$

$$e_i^* = \frac{1}{2}\left(Y_i-\theta G_i\right)$$

where $Y_i = \dfrac{1}{2p^{n-i+1}}\left((p-1)\left(1+\bar{C}_{i+1}+\bar{C}_{i+2}+\ldots+\bar{C}_n\right)-\bar{C}_i\right)$

and $G_i = \dfrac{1}{p^{n-i+1}}\left(\bar{C}_i-\bar{C}_i^*\right)$

for $1 \le i \le n$, where if $\theta^2 = p$ if p = 4k+1 and $\theta^2 = -p$ if p = 4k-1

where $\bar{C}_i = \sum_{s\in C_i} g^s$

and $\bar{C}_i^* = \sum_{s\in C_i^*} g^s$

Sharma, Bakshi, Dumir and Raka[16] described the primitive idempotents in FC_{p^n} where q is an odd prime power, may not be a primitive root mod p^n, p is an odd prime with (q,p) = 1 and order of q modulo p is f, $\left(\dfrac{p-1}{f},q\right)=1$ and $q^f = 1+p\lambda$. Also p does not divide λ (n$\ge$ 2) and (e,q) = 1, where $p = 1+ef$.
If q is primitive root modulo p then $f = p-1$.
The (en+1) primitive idempotents in FC_{p^n} are given by

$$e_0 = \frac{1}{p^n}\left(1+g+g^2+\ldots+g^{p^n-1}\right),$$

$$e_{p^j} = \frac{f}{p^{j+1}}\sum_{\substack{i=0\\ p^{n-j}|i}}^{p^n-1} g^i + \frac{1}{p^{j+1}}\left\{\rho_0\sum_{i\in C_{p^{n-j-1}}} g^j + \rho_1\sum_{i\in C_{p^{n-j-1}}} g^{aj} + \rho_2\sum_{i\in C_{p^{n-j-1}}} g^{a^2 j} + \ldots + \rho_{e-1}\sum_{i\in C_{p^{n-j-1}}} g^{a^{e-1} j}\right\},$$

$$e_{ap^j} = \frac{f}{p^{j+1}}\sum_{\substack{i=0\\ p^{n-j}|i}}^{p^n-1} g^i + \frac{1}{p^{j+1}}\left\{\rho_1\sum_{i\in C_{p^{n-j-1}}} g^j + \rho_2\sum_{i\in C_{p^{n-j-1}}} g^{aj} + \rho_3\sum_{i\in C_{p^{n-j-1}}} g^{a^2 j} + \ldots + \rho_0\sum_{i\in C_{p^{n-j-1}}} g^{a^{e-1} j}\right\},$$

...

$$e_{a^{e-1}p^j} = \frac{f}{p^{j+1}}\sum_{\substack{i=0\\ p^{n-j}|i}}^{p^n-1} g^i + \frac{1}{p^{j+1}}\left\{\rho_{e-1}\sum_{i\in C_{p^{n-j-1}}} g^j + \rho_0\sum_{i\in C_{p^{n-j-1}}} g^{aj} + \rho_2\sum_{i\in C_{p^{n-j-1}}} g^{a^2 j} + \ldots + \rho_{e-2}\sum_{i\in C_{p^{n-j-1}}} g^{a^{e-1} j}\right\}$$

where ρ_0 is an eigenvalue of the matrix Δ and ($\rho_0,\rho_1,\rho_2,\ldots,\rho_{e-1}$) is the eigen vector corresponding to ρ_0. The matrix Δ is given by

$$\Delta = \begin{pmatrix} A_{00}-f & A_{01}-f & A_{02}-f & \cdots & A_{0(e-1)}-f \\ A_{10} & A_{11} & A_{12} & \cdots & A_{1(e-1)} \\ A_{20} & A_{21} & A_{22} & \cdots & A_{2(e-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_{(e-1)0} & A_{(e-1)1} & A_{(e-1)2} & \cdots & A_{(e-1)(e-1)} \end{pmatrix}$$

if f is even, and is given by

$$\Delta = \begin{pmatrix} A_{00} & A_{01} & A_{02} & \cdots & A_{0(e-1)} \\ A_{10} & A_{11} & A_{12} & \cdots & A_{1(e-1)} \\ A_{20} & A_{21} & A_{22} & \cdots & A_{2(e-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_{\left(\frac{e}{2}\right)0}-f & A_{\left(\frac{e}{2}\right)1}-f & A_{\left(\frac{e}{2}\right)2}-f & \cdots & A_{\left(\frac{e}{2}\right)(e-1)}-f \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_{(e-1)0} & A_{(e-1)1} & A_{(e-1)2} & \cdots & A_{(e-1)(e-1)} \end{pmatrix}$$

if f is odd, where A_{ij} is the number of ordered pairs (s,t), such that

$g^{es+i} + 1 = g^{et+j}$, $0 \le s,t \le f-1$.

In 2010 S.K.Arora and Kulvir Singh [18] described an explicit expression for 4(n-1) primitive idempotents in FG , the semisimple group algebra of the cyclic group G of order 2^n (n≥3) over the finite field F of prime power order q, where q is quadratic residue modulo 2^n.

Then the primitive idempotents FC_{2^n} are given by

$$e_0 = Y_0 \ ,$$

$$e_{(1),n} = Y_1$$

$$e_{(1),n-1} = \frac{1}{2}\left[Y_2 - 2\theta^2(G_{(1,2),1} + G_{(3,4),1})\right],$$

$$e_{(2),n-1} = \frac{1}{2}\left[Y_2 + 2\theta^2(G_{(1,2),1} + G_{(3,4),1})\right],$$

for $1 \le i \le n-2$

$$e_{(1),i} = \frac{1}{4}\left[Y_{i+2} - 2\theta^2(G_{(1,2),i+1} + G_{(3,4),i+1}) - 4\theta(G_{(2,4),i} + \theta^2 G_{(1,3),i})\right],$$

$$e_{(2),i} = \frac{1}{4}\left[Y_{i+2} + 2\theta^2(G_{(1,2),i+1} + G_{(3,4),i+1}) - 4\theta(\theta^2 G_{(2,4),i} + G_{(1,3),i})\right],$$

$$e_{(3),i} = \frac{1}{4}\left[Y_{i+2} - 2\theta^2(G_{(1,2),i+1} + G_{(3,4),i+1}) + 4\theta(G_{(2,4),i} + \theta^2 G_{(1,3),i})\right],$$

$$e_{(4),i} = \frac{1}{4}\left[Y_{i+2} + 2\theta^2(G_{(1,2),i+1} + G_{(3,4),i+1}) + 4\theta(\theta^2 G_{(2,4),i} + G_{(1,3),i})\right],$$

where $\theta^2 = \sqrt{-1}$ and $\theta \in GF(l)$, l being the characteristic of F and

for $1 \le i \le n$ and $1 \le \beta \le 4$, $S_{(\beta),i} = \sum_{s \in C_{(\beta),i}} g^s$

for $1 \le i \le n-2$, $1 \le l,m \le 4$ and $l \ne m$, $G_{(l,m),i} = \frac{1}{2^{n-i+1}}\left(S_{(l),i} - S_{(m),i}\right)$

for $1 \le i \le n$,

$$Y_i = \frac{1}{2^{n-i+1}}\left[\left\{1 + \left(\sum_{j=i+1}^{n-2}\sum_{\beta=1}^{4} S_{(\beta),j}\right) + \left(S_{(1),n-1} - S_{(2),n-1}\right) + S_{(1),n}\right\} - \sum_{\beta=1}^{4} S_{(\beta),i}\right]$$

$$Y_0 = \frac{1}{2^n}\sum_{t=0}^{2^n-1} g^t$$

Again S.K.Arora and Kulvir Singh describe the 8(n-2) primitive idempotents in the semisimple group algebra of the cyclic group G of order 2^n (n≥4) over the finite field F of prime power order q, where q=8k+1 is a quadratic residue modulo 2^n.

FC_{2^n} has 8(n-2) primitive idempotents given by

$$e_0^* = Y_0 \ , \quad e_{(1),n}^* = Y_1$$

$$e_{(1),n-1}^* = \frac{1}{2}\left[Y_2 - 2\theta^2(G_{(1,2),1} + G_{(3,4),1})\right],\ e_{(2),n-1}^* = \frac{1}{2}\left[Y_2 + 2\theta^2(G_{(1,2),1} + G_{(3,4),1})\right],$$

$$e_{(1),n-2}^* = \frac{1}{4}\left[Y_3 - 2\theta^2(G_{(1,2),2} + G_{(3,4),2}) - 4\theta(G_{(2,4),1} + \theta^2 G_{(1,3),1})\right],$$

$$e_{(2),n-2}^* = \frac{1}{4}\left[Y_3 + 2\theta^2(G_{(1,2),2} + G_{(3,4),2}) - 4\theta(\theta^2 G_{(2,4),1} + G_{(1,3),1})\right],$$

$$e_{(3),n-2}^* = \frac{1}{4}\left[Y_3 - 2\theta^2(G_{(1,2),2} + G_{(3,4),2}) + 4\theta(G_{(2,4),1} + \theta^2 G_{(1,3),1})\right],$$

$$e_{(4),n-2}^* = \frac{1}{4}\left[Y_3 + 2\theta^2(G_{(1,2),2} + G_{(3,4),2}) + 4\theta(\theta^2 G_{(2,4),1} + G_{(1,3),1})\right],$$

for $1 \le i \le n-3$

$$e_{(1),i}^* = \frac{1}{8}\left[Y_{i+3} - 2\theta^2(G_{(1,2),i+2} + G_{(3,4),i+2}) - 4\theta(G_{(2,4),i+1} + \theta^2 G_{(1,3),i+1}) - 8\sqrt{\theta}(G_{(4,8),i}^* + \theta G_{(3,7),i}^* + \theta^2 G_{(2,6),i}^* + \theta^3 G_{(1,5),i}^*)\right],$$

$$e_{(2),i}^* = \frac{1}{8}\left[Y_{i+3} + 2\theta^2(G_{(1,2),i+2} + G_{(3,4),i+2}) - 4\theta(\theta^2 G_{(2,4),i+1} + G_{(1,3),i+1}) + 8\sqrt{\theta}(G_{(2,6),i}^* - \theta G_{(1,5),i}^* - \theta^2 G_{(4,8),i}^* + \theta^3 G_{(3,7),i}^*)\right],$$

$$e_{(3),i}^* = \frac{1}{8}\left[Y_{i+3} - 2\theta^2(G_{(1,2),i+2} + G_{(3,4),i+2}) - 4\theta(G_{(2,4),i+1} + \theta^2 G_{(1,3),i+1}) + 8\sqrt{\theta}(G_{(3,7),i}^* - \theta G_{(4,8),i}^* - \theta^2 G_{(1,5),i}^* + \theta^3 G_{(2,6),i}^*)\right],$$

$$e_{(4),i}^* = \frac{1}{8}\left[Y_{i+3} + 2\theta^2(G_{(1,2),i+2} + G_{(3,4),i+2}) + 4\theta(\theta^2 G_{(2,4),i+1} + G_{(1,3),i+1}) - 8\sqrt{\theta}(G_{(1,5),i}^* + \theta G_{(2,6),i}^* + \theta^2 G_{(3,7),i}^* + \theta^3 G_{(4,8),i}^*)\right],$$

$$e_{(5),i}^* = \frac{1}{8}\left[Y_{i+3} - 2\theta^2(G_{(1,2),i+2} + G_{(3,4),i+2}) - 4\theta(G_{(2,4),i+1} + \theta^2 G_{(1,3),i+1}) + 8\sqrt{\theta}(G_{(4,8),i}^* + \theta G_{(3,7),i}^* + \theta^2 G_{(2,6),i}^* + \theta^3 G_{(1,5),i}^*)\right],$$

$$e_{(6),i}^* = \frac{1}{8}\left[Y_{i+3} + 2\theta^2(G_{(1,2),i+2} + G_{(3,4),i+2}) - 4\theta(\theta^2 G_{(2,4),i+1} + G_{(1,3),i+1}) - 8\sqrt{\theta}(G_{(2,6),i}^* + \theta G_{(1,5),i}^* + \theta^2 G_{(4,8),i}^* + \theta^3 G_{(3,7),i}^*)\right],$$

$$e_{(7),i}^* = \frac{1}{8}\left[Y_{i+3} - 2\theta^2(G_{(1,2),i+2} + G_{(3,4),i+2}) + 4\theta(G_{(2,4),i+1} + \theta^2 G_{(1,3),i+1}) - 8\sqrt{\theta}(G_{(3,7),i}^* - \theta G_{(4,8),i}^* + \theta^2 G_{(1,5),i}^* + \theta^3 G_{(2,6),i}^*)\right],$$

$$e_{(8),i}^* = \frac{1}{8}\left[Y_{i+3} + 2\theta^2(G_{(1,2),i+2} + G_{(3,4),i+2}) + 4\theta(\theta^2 G_{(2,4),i+1} + G_{(1,3),i+1}) + 8\sqrt{\theta}(G_{(1,5),i}^* + \theta G_{(2,6),i}^* + \theta^2 G_{(3,7),i}^* + \theta^3 G_{(4,8),i}^*)\right],$$

Where $\theta^2 = \sqrt{-1}$ and $\theta \in GF(l)$, l being the characteristic of F and

for $1 \le i \le n$ and $1 \le \beta \le 8$, $S_{(\beta),i}^* = \sum_{s \in C_{(\beta),i}^*} g^s$

for $1 \le i \le n-3$, $1 \le l, m \le 8$ and $l \ne m$, $G_{(l,m),i}^* = \frac{1}{2^{n-i+1}}\left(S_{(l),i}^* - S_{(m),i}^*\right)$

for $1 \le i \le n-3$,

$$G_{(1,2),i} = G_{(1,2),i}^* + G_{(5,6),i}^*,$$

$$G_{(1,3),i} = G_{(1,3),i}^* + G_{(5,7),i}^*,$$

$$G_{(2,4),i} = G_{(2,4),i}^* + G_{(6,8),i}^*,$$

$$G_{(3,4),i} = G_{(3,4),i}^* + G_{(7,8),i}^*$$

for $1 \le i \le n$,

$$Y_i = \frac{1}{2^{n-i+1}}\left[\left\{1 + \left(\sum_{j=i+1}^{n-3}\sum_{\beta=1}^{8} S_{(\beta),j}^*\right) + \left(S_{(1),n-2}^* + \ldots + S_{(4),n-2}^*\right) + \left(S_{(1),n-1}^* - S_{(2),n-1}^*\right) + S_{(1),n}^*\right\} - \sum_{\beta=1}^{8} S_{(\beta),i}^*\right]$$

$$Y_0 = \frac{1}{2^n}\sum_{t=0}^{2^n-1} g^t$$

IV. OTHER POSSIBILITIES:

Although, a number of codes have been found yet many problems exists for the primitive idempotents in the cyclic group algebra. One of the main problem is to find out the primitive idempotents for the cyclic group FG, G is cyclic group of order m [m=p^n or p^{n}r^m or n(any natural number)], and F is Field of order q, where order of q modulo m [m=p^n or p^{n}r^m or n(any natural number)] respectively is any number *t*(say) with $1 \le t \le \phi(m)$.

V. ACKNOWLEDGMENT

There is no funding agency.

BIBLIOGRAPHY

[1.] Arora, S.K. and Pruthi, M. 1997. Minimal Codes of Prime-Power Length, Finite Fields Appl., 3, 99-113.

[2.] Berman, S. D. 1967. Semisimple cyclic and abelian code, II, Cybernatics, 3,17-23.

[3.] Blake, I.F, et al. 1975. The Mathematical Theory of Coding, Academic Press, New York.

[4.] Bakshi G. K. and Raka, M. 2003. Minimal Cyclic codes of length $p^n q$, Finite Fields Appl., 9, 432-448.

[5.] Bose, R. C. and Ray- Chaudhari, C. R. 1960. On a class of error correcting binary group codes, Info. and Control, 3, 67-79.

[6.] Elias, P. 1954. Error-free coding, IRE Trans. Inform. Theory., IT-4, 29-37.

[7.] Elias, P. 1955. Coding for noisy channels, IRE Conv. Rec.,3, 37-46.

[8.] Golay, M. J. E. 1949. Notes on Digital Coding, Proc. IRE, 37, 657.

[9.] Hamming, R.W. 1980. Coding and Information Theory, Prentice Hall, Inc.

[10.] Muller, D.E. 1954. Applications of Boolean algebra to Switching Circuit Design and to Error Detection, IRE Trans. Electron. Comput., EC-3, 6-12.

[11.] Pruthi, M. 2001. Cyclic Codes of Length 2^m, Proc. Indian Acad. Sci. Math. Sci., 111, 371-379.

[12.] Prange, E. 1957. Cyclic error-correcting codes in two symbols, AFCRC-TN 57-103, Air Force Cambridge Research Centre, Cambridge, Mass, (1957).

[13.] Prange, E. 1959. The use of coset equivalence in analysis and decoding of group codes, AFCRC-TN 55-164, Air Force Cambridge Research Centre, Cambridge, Mass, .

[14.] Peterson, W. W. 1961. Error correcting codes, The MIT press, Cambridge, Mass, (1961).

[15.] Pless, V. 1981. Introduction of the Theory of Error Correcting Codes, Interscience Publication, New York.

[16.] Sharma, A. et al. 2004. Cyclotomic numbers and primitive idempotents in the ring $GF(q)[x]/(x^{p^n}-1)$, Finite Fields Appl., 10, 653-673.

[17.] Singh, K. and Arora, S.K. 2010. Primitive Idempotents in FC_{2^n} -I, Int. J. Algebra, 4,1231-1241.

[18.] Singh, K. and Arora, S.K. 2010. Primitive Idempotents in FC_{2^n} -II, Int. J. Algebra, 4, 1243-1254.

[19.] Slepian, D. 1956. A class of binary Signalling Alphabets, Bell Syst. Tech. J., 35, 203-204.

[20.] Slepian, D. 1960. Some further theory of group codes, Bell Syst. Tech. J., 39, 1219-1252.

[21.] Shannon, C.E. 1948 A mathematical Theory of Communication, Bell Syst. Tech. J., 27, 379-423, 623-656.