Journal of Advances and Scholarly Researches in Allied Education

Vol. VII, Issue No. XIV, April-2014, ISSN 2230-7540

REVIEW ARTICLE

A STUDY ON MINIMAL CYCLIC CODES OF LENGTH 2_P^N

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

A Study on Minimal Cyclic Codes of Length 2_p^n

Manjeet Singh[1]* Dr. Pradeep Goel[2]

[1] Research Scholar, Department of Mathematics, Sai Nath University, Ranchi, Jharkhand

[2] Professor, M. M. College, Fatehabad, Haryana

Abstract – For all 2(nd+1) primitive idempotences in the ring, explicit terminology $R_{2p^n} = GF(l)[x] < x^{2p^n} - 1 >$, where p and l are so different, peculiar primes $o(l)_{2p^n} = \phi(2p^n)/d, d \geq 1$ A whole, obtained. An integer. Often discussed are the minimum width, polynomials and size generated by these primitive idempotents of the minimal cyclic codes. For eg, the minimum cyclic codes duration 22 parameters are discussed.

Key Words: Cyclotomic Cosets, Primitive Idempotents, Minimal Cyclic Codes, Generating Polynomials, Minimum Distance and Dimension

---------------------------------x---------------------------------

INTRODUCATION

Let F be a region of strange primary order, l and k ≥1 be an integer, $\gcd(l, k)=1$. Let $R_k = \frac{GF(l)[x]}{< x^k - 1 >}$. So R_k half fast. Each R_k ideal is also the exact sum of its least ideals. Therefore, it is enough to find the full collection of primitive idempotents to define the entire set of ideals (codes over F) in R_k. Let $o(l)_k$ Refers to l modulo k order. For $k = 2, 4, p^n, 2p^n, p$ It's odd prime and $o(l)_k = \phi(k)$, Arora and Pruthi are obtained for the full set of primitive idempotents in R_k[4,9]. $k=p^n, 2p^n\ (n \geq 1)$, p odd prime and $o(l)_k = \frac{\phi(k)}{2}$, Batra, Arora[8] are obtained for the entire set of primitive idempotents in R_k. For $k = p^n q\ (n \geq 1)$, p and q different odd primes of which l is the primitive modulo pn root and q $\gcd(\phi(2p^n), \phi(q)) = 2$, Bakshi and Raka are derived from primitive idempotents in R_k[3]. For $k = p^n\ (n \geq 1)$, p odd prime, $o(l)_k = \frac{\phi(k)}{e}$, e is a positive integer, Sharma, Raka, and Dumir are the primitive idempotents in Rk[5]. The primitive idempotents of quadratic residue codes was obtained by Ranjeet Singh and Manju Pruthi [6] $p^n q^m$, p, q Are different odd benefits and $o(l)_{p^n} = \frac{\phi(p^n)}{2}, o(l)_{q^m} = \frac{\phi(q^m)}{2}, \gcd(\frac{\phi(p^n)}{2}, \frac{\phi(q^m)}{2}) = 1$. Amita and P.T. Amita Sahni Sehgal [1] defines the simple idempotents of the minimum cyclical codes of p^n q, p, q as separate primes and, $o(l)_{p^n} = \phi(p^n), o(l)_q = \phi(q), \gcd(\phi(p^n), \phi(q)) = d$, q-1 is not divided by p. The findings of Batra, Arora [8], have been generalised in this article. We take note of when $k=2p^n$, where p and l are strange primes, $o(l)_{2p^n} = \phi(2p^n)/d, d \geq 1$ An integer. - An integer. For the 2(nd+1) primitive idempotents in Rk we get explicit expressions. Often discussed are the minimum width, polynomials and size generated by these primitive idempotents of the minimal cyclic codes. The cyclotomical cosets are mentioned in Section (Lemmas 1- 9 and Theorem 1). $2p^n$ and some primary findings for the Rk primitive idempotents definition. The expressions of primitive idempotents were specifically collected in section (Theorem 3). We address the dimension of section (Theorem 4-6), producing a minimum polynomial distance and a minimum cycle length codes $2p^n$. The different parameters of minimum cyclical codes of 22 are mentioned in section.

PRIMITIVE IDEMPOTENTS IN $R_{2p^n} = \frac{GF(l)[x]}{< x^{2p^n} - 1 >}$ AND MINIMAL CYCLIC CODES OF LENGTH $2p^n$ over F(=GF(l))

The minimum cyclical length codes are defined in this section $2p^n$ over F, where p and l are different peculiar primes and $o(l)_{2p^n} = \phi(2p^n)/d, d \geq 1$ An integer. A number of ϕ(n) íntegers of the penalty $a_1, a_2, \ldots, a_{\phi(n)}$, where $\gcd(a_i, n) = 1$ and $a_i \neq a_j$ (mod n) for all $i, j, 1 \leq i, j \leq \phi(n), i \neq j$ Forms the modulo n decreased residue method. Let l be a desirable integer ϕ(n), The primitive root modulo n is then referred to as l. We are conscious that primitive root modulo n only occurs if $n = 2, 4, p^e, 2p^e$ Where p is an odd premium.

Lemma 1: Let P and l be distinctly unusual primes and n ≥ 1.

If $o(l)_{2p^n} = \phi(2p^n)/d$ then $o(l)_{2p^{j+1}} = \frac{\phi(2p^{j+1})}{d}$ for all $0 \leq j \leq n-1$.

Proof: Trivial.

Lemma 2: A positive integer is available $g, 1 < g < 2p$, It is how it is. $\gcd(g, 2pl) = 1$, and $o(g)_{2p} = \phi(p)$, where $g, g^2, \ldots, g^{d-1} \in \{1, l, l^2, \ldots, l^{\frac{\phi(2p)}{d}-1}\}$.

Proof: See [1, Lemma4].

Lemma 3: A positive integer is available $g, 1 < g < 2p$, It is how it is. $\gcd(g, 2pl) = 1$ and $g^i \neq l^k$ (mod 2p) for any $i, k;\ 1 \le i \le d-1$ and $0 \le k \le \frac{\phi(n)}{d}$. In addition, for every $n, 1 \le j < n$, the set $\{1, l, l^2, \ldots, l^{\frac{\phi(p^{n-1})}{d}-1}, g, gl, gl^2, \ldots, gl^{\frac{\phi(p^{n-1})}{d}-1}, \ldots, g^{d-1}, g^{d-1}l, g^{d-1}l^2, \ldots, g^{d-1}l^{\frac{\phi(p^{n-1})}{d}-1}\}$ Type modulo a decreased residue method $2p^{n-j}$.

Proof: Trivial.

Let $S = \{0, 1, 2, \ldots, 2p^n - 1\}$. For a, b ∈ S, say that $a \sim b$ iff $a \equiv b l^i \pmod{2p^n}$ This establishes an equivalence relation on the set S for any integer l ≥ 0. The groups of equivalence attributable to this interaction are referred to as *l*-cyclostomic cosets modulo $2p^n$. The *l* -cyclotomic coset containing

s ∈ S Denoted by is

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

Where ts are the least desirable integer, $sl^{t_s} \equiv s \pmod{2p^n}$ in addition to $|C_s|$ Denotes the order of Cs, containing s, l-cyclotomic coset.

Theorem 1: If p is a strange premium $o(l)_{2p^n} = \phi(2p^n)/d,\ d \ge 1$ An integer, so 2(nd+1) cyclotomic cosets are present for integer n ≥ 1, $\pmod{2p^n}$ Data by

(i) $C_0 = \{0\}$
(ii) $C_{p^n} = \{p^n\}$

For $0 \le j \le n-1,\ 0 \le k \le d-1$

(iii) $C_{g^k p^j} = \{g^k p^j, g^k p^j l, \ldots, g^k p^j l^{\frac{\phi(p^{n-j})}{d}-1}\}$

(iv) $C_{2g^k p^j} = \{2g^k p^j, 2g^k p^j l, \ldots, 2g^k p^j l^{\frac{\phi(p^{n-j})}{d}-1}\}$,

Where g is known as the fixed integer in Lemma 2.

Proof: Trivial.

Note 1: (i) $g^u \in C_1$, If and only if for every integer u $u \equiv 0$ (mod d).

(ii) $-1 \in C_1$ or $-1 \in C_{g^{d/2}}$, if $-1 \in C_1$ then $-C_1 = C_1$ otherwise $-C_1 = C_{g^{d/2}}$.

(iii) If $-C_1 = C_1$ then $-C_{g^k p^j} = C_{g^k p^j}$, otherwise $-C_{g^k p^j} = C_{g^{k+d/2} p^j}$ for all i, k; $0 \le i \le$ n-1 and $0 \le k \le$ d-1.

Lemma 4: If β is primitive, for every odd prime p and positive integer k. $2p^k$ th Unity root in any GF(*l*) extension area and $o(l)_{2p^k} = \phi(2p^k) \pmod{2p^k}$, after that

$$\sum_{s=0}^{\phi(2p^k)-1} \beta^{l^s} = \begin{cases} 1 & \text{if } k = 1 \\ 0 & \text{if } k > 1. \end{cases}$$

Proof: Including Lemma 4..

Let α be primitive $2p^n$th Unity root in any GF (*l*)extension area. For $0 \le i \le n-1$ and $0 \le k \le d-1$, define $A_i^{(k)} = \sum_{s \in C_{g^k p^i}} \alpha^{2s}$ and $B_i^{(k)} = \sum_{s \in C_{g^k p^i}} \alpha^{s}$ .Since $C_{g^k l} = C_{g^k}$, therefore $(A_i^{(k)})^l = A_i^{(k)}$, so that each , $A_i^{(k)}, B_i^{(k)} \in GF(l)$.

Lemma 6: Each *l* For,

$$0 \le i \le n-1,\ \sum_{k=0}^{d-1} A_i^{(k)} = \begin{cases} 0 & \text{if } i \le n-2 \\ -p^{n-1} & \text{if } i = n-1. \end{cases}$$

Proof. See [1, Lemma 10].

Lemma 7: Each *l* For,

$$0 \le i \le n-1,\ \sum_{k=0}^{d-1} B_i^{(k)} = \begin{cases} 0 & \text{if } i \le n-2 \\ p^{n-1} & \text{if } i = n-1. \end{cases}$$

Proof: Much as above.

Lemma 8: Every h, $k,\ 0 \le h, k \le d-1,\ 0 \le i, j \le n,$

$$\sum_{s \in C_{g^h p^i}} \alpha^{2g^k p^j s} = \begin{cases} 1 & \text{if } i+j \ge n, j = n, \\ \frac{\phi(p^{n-j})}{d} & \text{if } i+j \ge n, j \le n-1, \\ \frac{1}{p^j} A_{i+j}^{(h+k)} & \text{if } i+j \le n-1. \end{cases}$$

Proof: Case (i) For $j = n,\ i+j \ge n,\ C_{g^h p^i} = C_{g^h p^n} = C_{p^n}$, So, $\sum_{s \in C_{p^n}} \alpha^{2g^k p^j s} = 1.$

Case (ii) Let $i + j \ge n$ and $j \le n-1$ The above number then sums to $\frac{\phi(p^{n-j})}{d}$

Case (iii) If $i + j \le n - 1$ then $\sum_{s \in C_{g^h p^i}} \alpha^{2g^k p^j s} = \sum_{s=0}^{\frac{\phi(2p^{n-i})}{d}-1} \beta^{l^s}$, where $\beta = \alpha^{2g^{(h+k)} p^{i+j}}$, then β is primitive p^{n-i-j} th Unity's source. That's why, $\beta^{l^r} = \beta^{l^s}$ whether and if only $l^r \equiv l^s \pmod{p^{n-i-j}}$ whether and if only $r \equiv s \pmod{\frac{\phi(p^{n-i-j})}{d}}$.

Then

$$\sum_{s=0}^{\frac{\phi(2p^{n-i})}{d}-1} \beta^{l^s} = p^j \sum_{s=0}^{\frac{\phi(p^{n-i-j})}{d}-1} \beta^{l^s}$$

Also,

$$A_{i+j}^{(h+k)} = \sum_{s \in C_{g^h p^{i+j}}} \alpha^{2l^s} = \sum_{s=0}^{\frac{\phi(2p^n)}{d}-1} \beta^{l^s} = \frac{\phi(2p^n)}{d} \cdot \frac{d}{\phi(p^{n-j})} \sum_{s=0}^{\frac{\phi(p^{n-j})}{d}-1} \beta^{l^s} = \frac{1}{p^{i+j}} A_{i+j}^{(h+k)}$$

Then we get the appropriate number from the above discussion.

Lemma 9: Everyone $h, k,\ 0 \le h, k \le d-1,\ 0 \le i, j \le n,$

$$\sum_{s\in C_{g^k p^j}} \alpha^{g^k p^j s} = \begin{cases} -1 & \text{if } i+j \ge n,\ j=n, \\ -\dfrac{\phi(p^{n-j})}{d} & \text{if } i+j\ge n,\ j\le n-1, \\ \dfrac{1}{p^j} B_{i+j}^{(h+k)} & \text{if } i+j\le n-1. \end{cases}$$

Proof: Like Lemma 8..

EVALUATION OF PRIMITIVE IDEMPOTENTS

When α is a primitive unity mth root in a GF(l) extension area, then the polynomial $M^{(s)}(x)=\prod_{i\in C_s}(x-\alpha^i)$ is the lowest GF polynomial (l). Let Ωs the ideal in Rm be the minimum provided by $\frac{x^m-1}{M^s(x)}$ To be and defines Ωs the primitive idempotent of $\theta_s(x)=\sum_{i\in C_s} x^i$.

Theorem 2: $\theta_s(x)=\sum_{i=0}^{m-1} \varepsilon_i x^i$, where $\varepsilon_i=\sum_{j\in C_s}\alpha^{-ij}$ for all $i\ge 0$.

Proof: See [1, Theorem 1].

Theorem 3: The primitive idempotents in 2 (nd+1) R_{2p^n} are known by

(i) $\theta_0(x)=\dfrac{1}{2p^n}(1+x+x^2+\ldots+x^{2p^n-1})$

(ii) $\theta_{p^n}(x)=\dfrac{1}{2p^n}\{1-\sigma_{p^n}(x)\}+\dfrac{1}{2p^n}\left\{\sum_{k=0}^{d-1}\sum_{i=0}^{n-1}(\sigma_{2g^k p^i}(x)-\sigma_{g^k p^i}(x))\right\}$

(iii) For $0\le j\le n-1,\ 0\le k\le d-1$,

$$\theta_{g^k p^j}(x)=\frac{p-1}{2p^{j+1}d}\left\{1-\sigma_{p^n}(x)+\sum_{h=0}^{d-1}\sum_{i=n-j}^{n-1}(\sigma_{2g^h p^i}(x)-\sigma_{g^h p^i}(x))\right\}+\frac{1}{2p^{n+j}}\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}(B_{i+j}^{(\gamma+h)}\sigma_{g^h p^i}(x)+A_{i+j}^{(\gamma+h)}\sigma_{2g^h p^i}(x))$$

(iv) For $0\le j\le n-1,\ 0\le k\le d-1$,

$$\theta_{2g^k p^j}(x)=\frac{p-1}{2p^{j+1}d}\left\{1+\sigma_{p^n}(x)+\sum_{h=0}^{d-1}\sum_{i=n-j}^{n-1}(\sigma_{g^h p^i}(x)+\sigma_{2g^h p^i}(x))\right\}+$$

$$\frac{1}{2p^{n+j}}\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}A_{i+j}^{(\gamma+h)}(\sigma_{g^h p^i}(x)+\sigma_{2g^h p^i}(x)).$$

Proof:

(i) By Theorem $2,\ \theta_0(x)=\sum_{r=0}^{2p^n-1}\varepsilon_r x^r$, where $\varepsilon_r=\frac{1}{2p^n}\sum_{s\in C_0}\alpha^{-rs}=\frac{1}{2p^n}$ for all r. Therefore, $\theta_0(x)=\dfrac{1}{2p^n}(1+x+x^2+\ldots+x^{2p^n-1})$.

(ii) By Theorem $2,\ \theta_{p^n}(x)=\sum_{r=0}^{2p^n-1}\varepsilon_r x^r$, where $\varepsilon_r=\frac{1}{2p^n}\sum_{s\in C_{p^n}}\alpha^{-rs}$. Since by Note 1, $-C_{p^n}=C_{p^n}$, therefore, $\varepsilon_r=\frac{1}{2p^n}\sum_{s\in C_{p^n}}\alpha^{rs}$. Now, $\varepsilon_0=\frac{1}{2p^n},\ \varepsilon_{p^n}=-\frac{1}{2p^n}$.

For $0\le i\le n-1,\ 0\le k\le d-1$, We've got Lemma 8 and Lemma 9

$$\varepsilon_{g^k p^i}=\frac{1}{2p^n}\sum_{s\in C_{p^n}}\alpha^{g^k p^i s}=-\frac{1}{2p^n},\ \varepsilon_{2g^k p^i}=\frac{1}{2p^n}\sum_{s\in C_{p^n}}\alpha^{2g^k p^i s}=\frac{1}{2p^n q}.$$

Thus,

$$\theta_{p^n}(x)=\frac{1}{2p^n}\{1-\sigma_{p^n}(x)\}+\frac{1}{2p^n}\left\{\sum_{k=0}^{d-1}\sum_{i=0}^{n-1}(\sigma_{2g^k p^i}(x)-\sigma_{g^k p^i}(x))\right\}$$

(iii) For $0\le j\le n-1,\ 0\le k\le d-1$,

If $\theta_{g^k p^j}(x)=\sum_{r=0}^{2p^n-1}\varepsilon_r^{(k,j)}x^r$ Theorem 2 and note 1 are then included., $\varepsilon_r^{(k,j)}=\frac{1}{2p^n}\sum_{s\in C_{g^k p^j}}\alpha^{-rs}=\frac{1}{2p^n}\sum_{s\in C_{g^\gamma p^j}}\alpha^{rs}$, u = 0 or u = d/2 according as $-1\in C_1$ or $-1\in C_{g^{d/2}}$, Thus, $\varepsilon_r^{(k,j)}=\frac{1}{2p^n}\sum_{s\in C_{g^\gamma p^j}}\alpha^{rs}$ where $\gamma=k+u \pmod d$ and $0\le\gamma\le d-1$ Now, $\varepsilon_0^{(k,j)}=\frac{1}{2p^n}\sum_{s\in C_{g^\gamma p^j}}\alpha^{s}=\frac{\phi(2p^{n-j})}{2p^n d},\ \varepsilon_{p^n}^{(k,j)}=\frac{1}{2p^n}\sum_{s\in C_{g^\gamma p^j}}\alpha^{p^n s}=-\frac{\phi(p^{n-j})}{2p^n d}$.

For $0\le i\le n-1$, We've got Lemma 8 and Lemma 9

$$\varepsilon_{g^h p^i}^{(k,j)}=\frac{1}{2p^n}\sum_{s\in C_{g^\gamma p^j}}\alpha^{g^h p^i s}=\frac{1}{2p^n}\begin{cases}-\dfrac{\phi(p^{n-j})}{d} & \text{if } i\ge n-j,\ j\le n-1,\\ \dfrac{1}{p^j}B_{i+j}^{(h+k)} & \text{if } i\le n-j-1.\end{cases}$$

$$\varepsilon_{2g^h p^i}^{(k,j)}=\frac{1}{2p^n}\sum_{s\in C_{g^\gamma p^j}}\alpha^{2g^h p^i s}=\frac{1}{2p^n}\begin{cases}\dfrac{\phi(p^{n-j})}{d} & \text{if } i\ge n-j,\ j\le n-1,\\ \dfrac{1}{p^j}A_{i+j}^{(h+k)} & \text{if } i\le n-j-1.\end{cases}$$

We can also evaluate $\theta_{2g^k p^j}(x)$.

REFERENCES

[1] A. Sahni and P. T. Sehgal (2012). "Minimal Cyclic Codes of length pn q," Finite Fields Appl., pp. 1017-1036.

[2] F.J. Mac Williams & N.J.A. Sloane : The Theory of Error Correcting Codes Bell Laboratories Murray Hill NJ 07974 U.S.A.

[3] G. K. Bakshi and Madhu Raka (2003). "Minimal Cyclic Codes of Length pn q," Finite Fields Appl. 9(4), pp. 432-448.

[4] M. Pruthi and S.K. Arora (1997). "Minimal Cyclic Codes of Prime Power Length," Finite Field and their Application, 3, pp. 99-113.

[5] M. Raka; G.K. Bakshi ; A. Sharma, V. C. Dumir (2004). "Cyclotomic numbers and primitive idempotents in the ring (1) ( )[ ] – n p x GF q x ," Finite Field & Their Appl.3 no.2, pp. 653-673.

[6] R. Singh and M. Pruthi (2011). "Primitive idempotents of quadratic residue codes of length pn q m ," Int. J. Algebra 5, pp. 285-294.

[7] S. Batra and S.K. Arora (2001). "Minimal quadratic residue cyclic codes of length pn (p odd prime)," Korean J. Comput & Appl. Math. Vol. 8(3), pp. 531-547.

[8] S. Batra and S.K. Arora (2010). "Some cyclic codes of length 2pn (p odd prime)," Design Codes Cryptography , Vol. 57(3).

[9] B. Chen, H. Liu, and G. Zhang (2014). Some minimal cyclic codes over finite fields, Discrete Math. 331, pp. 142–150.

[10] C. Ding and V. Pless (1999). Cyclotomy and duadic codes of prime lengths, IEEE Trans. Inform. Theory 45, no. 2, pp. 453–466.

Corresponding Author

Manjeet Singh*

Research Scholar, Department of Mathematics, Sai Nath University, Ranchi, Jharkhand