Minimum Distance of Cyclic Codes

Dr. M. Mary Jansi Rani[1]

Head and Assistant Professor,
Department of Mathematics,
Thanthai Hans Roever College, Perambalur.

ABSTRACT In this paper Introduce the nature of a minimal prime ideal in R_n and observe that as $n \in \mathbb{Z}$ has only a finite number of prime divisors, the ideal (n) in $\mathbb{Z}$ has only a finite number of minimal prime ideals.

Keywords Minimal prime ideal in R_n , Prime divisors , Reduced modulo , Cyclic complement , Primitive element , Linear factor , BCH code.

1. Introduction

Let C be a cyclic order in R_n , then there exists a unique idempotent $e(x) \in C$ such that

$C = \langle e(x) \rangle$. Further if e(x) is an idempotent in C , then $C = \langle e(x) \rangle$ if and only if e(x) is a unity element of C was introduced in [1]. Let C be a cyclic code over $\mathbb{F}_q$ with generating idempotent e(x). Then the generating polynomial of C is $g(x) = \gcd(e(x), x^2-1)$ computed in $\mathbb{F}_q[x]$ and also discussed property of minimal ideals of R_n .

In [4] produced some properties of commutative ring R with unity , every maximal ideal is a prime ideal and also every proper ideal of the ring R possesses at least one proper ideal . In this chapter introduce the nature of a minimal prime ideal in R_n and observe that finite number of minimal prime ideals.

2. Preliminaries

Definition 2.1 Let R_n be acommutative ring with unity. An ideal P of R is called a prime ideal if for all $a,b \in R$, $ab \in P$ implies that either $a \in P$ [or] $b \in P$.
Example2.1.1 Let $\mathbb{Z}$ be a ring of integer, we consider the ideal [P] generated by a prime . If for $a,b \in \mathbb{Z}$, $ab \in [P]$, then $a \in [P]$ or $b \in [P]$.

As R_n is principal ideal domain and finitely generated each ideal of R_n is contained in a minimal ideal . So every proper code C of R_n is contained in a minimal code say C_m . In [9] the authors give property of minimal ideal of R_n.
Fact 2.1 In a commutative ring R with unity,every minimal ideal is a prime ideal in [4].
Fact 2.2 Let I be a proper ideal of a commutative ring with unity then I is a minimal ideal if and only if R\ I is a field in [4] .
Definition 2.5 Let R be a commutative ring with unity, let I be a proper ideal of R. A prime ideal P of R is said to be a minimal prime ideal of I if $I \subseteq P$ and there exists no prime ideal P' of R such that $I \subseteq P' \subseteq P$.

The minimal prime ideals of the zero ideal . (0) are called minimal prime ideals of R.
Definition 2.6 A prime ideals P of R is called a minimal prime ideal(R) if it does not contain any other prime ideal $\neq (0)$.

We observe that as $n \in \mathbb{Z}$ has only a finite number of prime divisors, the ideal (n) in $\mathbb{Z}$ has only a finite number of minimal prime ideals.

Fact 2.3 (Correspondence theorem) Let f be a homomorphism from a ring R into a ring R′. Then there is a one-one correspondence between , those ideals I of R Such that Kerf ⊆ I and the set of all ideals I′ of R′ and I is given by I′ = f(I) . For proof see in [4].

Corollary Fact 2.3 Given an ideal I of a ring R, there is a canonical homomorphism of R onto R/I ,that is V: R→ R/I is such that Ker V= I.There is a one-one correspondence between the ideals of R containing J and the ideals of R/J. That is every ideal in R/I is of the form J/I where J is an ideal of R containing I.

In otherwords we describe if it Fact 2.3 Let I be an ideal of a ring R then there is aone-to-one correspondence between the set of all ideals of R which contain IU and the set of ideals of R/I given by J→J/I. That is every ideal in R/I is of the form J/I where J is an ideal of R which contains I.

Next, we consider R_n, the ideals of R_n are of the form $\alpha f(x)+(x^n-1)$ as $R_n= \pi_q[x] / (x^n-1)$ is a P.I.D. Further deg $f(x) \leq (n-1)$. We consider the irreduclibe divisors of x^n-1 .Let p(x) is an irreducible divisors of x^n-1, I = (x^n-1) is contained in (p(x)) further (p(x)) is a maximal ideal of $F_q[x]$. Therefore, the ideal J =(p(x)) is a prime ideal of $F_q[x]$. If a(x) b(x) ∈ J, then either a(x) ∈ J (or) b(x) ∈ J.

Theorem 2.1 Let $\lambda > 2$, if λ is the number of irreducible factors of x^n-1 , then there are λ minimal ideals of R_n.

Proof Let p(x) be an irreducible divisors of x^n-1.(p(x)) is a prime ideal of $\pi_q[x]$.There is an ideal corresponding to (p(x)) in R_n. The corresponding ideal is $(p(x)) / (x^n-1)$ in R_n, as (p(x)) contains (x^n-1) = I for since p(x) divides x^n-1, I = (x^n-1) is contained in the ideal generated by p(x).

Claim Let $(p(x))/ (x^n-1)$ is a minimal prime ideal of k_n, for if a(x)b(x) ∈ p(x) either a(x)∈ b(x) or b(x) ∈ p(x). We assume that a(x)b(x)≠p(x), in the ideal $(p(x/(x^n))-1)$ the element corresponding to a(x)b(x) is $a(x)b(x)+ (x^n-1)$, when a(x)b(x) is reduced modulo (x^n-1),

when $\lambda > 2$, (a(x)b(x)) is less than x, further we note that since (p(x)) is a prime ideal, either $a(x)+(x^n-1)$ or $b(x)+ (x^n-1)$ is an element of $(p(x))/ (x^n-1)$. So, the ideal $(p(x)) / (x^n-1)$ corresponds to a prime ideal of $F_q[x]$. As there is no proper ideal between a maximal ideal of a ring R and the ring R_1 there is ideal Q such that $p(x) / (x^n-1)$ in R_n. That is $(p(x)) / (x^n-1)$ is a minimal prime ideal of R_n Whenever (p(x)) is a maximal ideal of $F_q[x]$.

2. Cyclic Complement of a Cyclic Code

Given two codes C_1 ,C_2 over $\mathbb{F}_2$, we define the sum $C_1 + C_2$ of two codes to be
$C_1 + C_2 = \{ c_1+ c_2 ; c_1 \in C_1, c_1 \in C_2\}$

Definition 3.1 If C is a linear code of length n over $\mathbb{F}_q$ then a complement C^c of C is defined by the relations a . $C+ C^c = \mathbb{F}_q^n$, b . $C \cap C^c = \{0\}$, ingeneral the complement C^c is not unique.

Fact 3.1 In [9] Let C be a cyclic code of length n over $\mathbb{F}_q$ with generator polynomial g(x) generating idempotent e(x) and defining the set T. Let C^c be the cyclic complement of C. Then

i) $h(x) = \frac{X^n-1}{g(x)}$ is the generator polynomial of C^c and 1- e(x) is its generating idempotent.

ii) If S = { 0 , 1 , 2 …….(n-1)} , then show that is the defining set of C^c .

By recall the defining set of C, We have seen that

$$g(x) = \prod_s M_\propto s(x) = \prod \prod_{i \in c_s}(x - \alpha^i)$$

where α is a primitive n^{th} root of unity contained in $\mathbb{F}_q$t , a splitting field of (x^n-1) . Let

$(x^n-1) = \prod_{i=0}^{n-1}(x - \alpha^i)$ is the function of (x^n-1) into linear factor over $\mathbb{F}_q$.

Next we look at the linear code of length n over $\mathbb{F}_q$ as the subspace of $\mathbb{F}_q$.

Fact 3.2 Let V be a finite dimensional vector space over a field F. we take dim V = X . Let W be finite dimensional vector space of dimension m over F. If T : V→ W is a linear transformation then the rank-nullity theorem says that dim (ker T) + dim(T) = dimV = n. Further if W is a subspace of V then W is finite dimensional dimW ≤ dim V and dim(V/M) = dim V – dim W where V/W denotes the quotient space of V by W meaning that we consider the quotient space of the abelian group V by the subgroup W. Therefore a canonical transformation r from V onto V/W defined by r (V) = V + W where V belongs

to the coset of V ker r = W. we apply this fact to $\mathbb{F}_q^n$. $\mathbb{F}_q^n$ is a vector space of dimension n over $\mathbb{F}_q$. Let C be the linear code of dimension k over $\mathbb{F}_q$. The canonical linear transformation r : $\mathbb{F}_q^n \rightarrow \mathbb{F}_q^n /C$ yields that dim ($\mathbb{F}_q^n$ / C) = dim $\mathbb{F}_q^n$ – dim C = x – k.

Theorem 3.1 Let C^c be the complement of a cyclic code C. then $C^C \cong \mathbb{F}_q^n / C$.

Proof Let k be a dimension of the cyclic code

$$\dim(\mathbb{F}_q^n/ C) = \dim(\mathbb{F}_q^n) - \dim C$$
$$= x - k$$

Since any two finite dimensional vector space V and W having the same dimension are isomorphic and since dim C^c = x – k , $C^c \cong \mathbb{F}_q^n / C$.

3.Minimum Distance of a Cyclic Code

Given a cyclic code C of length x over $\mathbb{F}_q$, C posses a definite set T . BCH bound says that if T contains δ – 1 consecutive elements for some integer δ, then C has a minimum distance d satisfying d ≥ δ. since defining set T depends on the primitive element α , β = α^a where g.c.d (a,n) = 1 where β is also primitive n^{th} root of unity. If a^{-1} is the multiplicative inverse of a (mod n), the minimal polynomials M_{α^s}(X) and $M_{\beta^{a^{-1}s}}$ (X) are equal . So the code with defining set T is the same as the code with defining set a^{-1}T modulo relative to the primitive element β. While applying the BCH bound a higher lower bound may be obtained , if we apply a multiplier to the definiting set.

The Hartmann Tzeng bound says that if A denotes a set δ – 1 consecutive elements of T and if B = { jb mod n} where 0 ≤ j ≤ s where g.c.d (b, x) < δ the minimum weight d of C satisfies d ≥ δ – s provided A+B ⊆ T.

Theorem 3.1 Let C be a cyclic code of length n over $\mathbb{F}_q$ with defining set T. Let A be a set of δ – 1 consecutive elements of T. Let B = { j ∈ s\T : j(mod n)} If A+B ⊆ T, the minimum weight d of C satisfies d ≥ δ +│ B │ where │ B │denotes the number of elements of B.

Proof This is a particular case of Hartmann-Tzeng bound where B = { jb mod n } with gcd of (b,n) < δ here b = 1. Further S\T is the defining set of C^c. As $|B| \geq 1$, $d \geq \delta +1$ which in the case of S = 1 in Hartmann-Tzeng bound proof follows on lines of proof given in [9].

Example 3.3.1 Let C be a binary cyclic code of length 17 with defining set
T = {1,2,4,8,9,13,15,16} there are two consecutive elements 8, 9 or 15,16 we take
A = {8,9} $|A| = 2 = \delta - 1$ or $\delta = 3$ B = { j ∈ S\T ; j (mod n)}. we look for these values of j for which A+B ⊆ T S\T = B = { 0,3,5,6,7,10,11,12,14 } A = { 8,9 }

j = 0 A+B ⊆ T
j = 3 A+B = {11,12} ⊈ T
j = 5 A+B = {13,14} ⊈ T
j = 6 A+B = {14,15} ⊈ T
j = 7 A+B = Not ok
j = 10 A+B = {1, 2} ⊆ T
j = 11 A+B = {2, 3} Not ok
j = 12 A+B = {3, 4} Not ok
j = 14 A+B = {5, 6} Not ok. The number of values of j satisfying A+B ⊆ T is 2.Therefore $d \geq 3+2 = 5$ it is known that d = 5.

Reference

[1] Apostal Tom.M , Introduction to analytic number theory, VTM ,Springer verlag third edition (2011).
[2] AroraS.K and Manju Pruthi , Minimal Cyclic Codes of Length $2p^n$ Finite fields and their Applications Volume 5(1999) Pg(177-187)
[3] Arrora S.K ,Sudhir Batra, Stephen D Cohen and Manju Pruthi , The Primitive idempotent of a cyclic group algebra. South east Asian Bullatin of Mathematics Volume 26(2002).
[4] Burton David M, A first course in rings and ideals ,Addison– westey(1965).
[5] Dornhoff . Larry L and Foranz.E.Horn Applied Modern Algebra,Macmillan Publications (1978)
[6] Hill .R , A first course in Coding Theory, Oxford University Press(1986)
[7] Conway J.H and Salone NJA, Self- Dual Codes Over the Integer Modulo 4, Journal of Combinatories theory Series A, Volume 62(1993) Pg (30-40)
[8] Sivaramakrishnan. R Certain number – Theoretic episodes in Algebra,Chapiman & Hall CRC Press (2006) Pg (188-193)
[9] Huffmann .C and Vera Pless Fundamentals of error correcting codes, Cambridge univ press First South Asian Edition (2004)