Self-Dual Codes On Muffin Ideals

Over the Ring of Quaternion Integers

[1]Shaikh Javed Shafee, [2]Ekrarkhan E. Tadvipathan, [3]Arunkumar R. Patil

[1]Lecturer, Department of Mathematics, Government Polytechnic, Hingoli, India
[2]Lecturer, Department of Electronics and Telecommunication, Government Polytechnic, Hingoli, India
[3]Associate Professor, Department of Mathematics, Shri Guru Gobind Singhji Institute of Engg. & Tech., Nanded, India

Abstract : To provide efficient and reliable transmission of data in signal and image process cyclic and dual of cyclic codes on muffin ideals of quaternion integer rings over finite field $\mathbb{z}_{p^e}$, where p is odd prime integer, $e > 0$ is integer with respect to Mannheim distance. The set of generators for cyclic and their dual codes has given. Also, self-dual codes on quaternion integer ring over the finite field $\mathbb{z}_{p^e}$, for integer $e > 0$ corresponding to Mannheim distance has been studied.

***Index Terms*- Cyclic Codes, Dual Codes, Self-Dual Codes, Quaternion Algebra, Muffin Ideals, Mannheim Distance.**

I. INTRODUCTION

In communication channels, codes are used to design the efficient and reliable data transmission methods. Algebraic codes playing important role for redundancy of noise and for detection-correction of errors occurs in data transmission. There are different types of codes such as Reed-Solomon codes, Reed-Muller codes, BCH codes, MDS codes, Turbo codes, etc that used in transmission methods by engineers and mathematicians. The Mathematical structure is the key for all these codes. From last two decade the research scholars in algebraic coding theory have generated a great deal of attention on codes over rings. Linear codes are the most fascinating objects in coding theory because of their algebraic structure and effective decoding algorithms. The cyclic codes associated with Hamming distance and Lee distance over different rings have studied by authors of ([15],[16],[18],[19],[20]). They found generating set, rank and minimum distance. Also cyclic codes associated to Mannheim distance over some finite quaternion integer rings studied in [4], where author finds out generating set. Cyclic codes associated to Mannheim distance over ring of Gaussian Integer where studied by K. Huber[1] in 1994. Later, cyclic codes over ring of quaternion integers where studied by M. Ozen and M. Guzeltepe in 2009([4], [6]). In [4] a method to obtain cyclic codes over commutative quaternion integer rings with respect to quaternion Mannheim distance is discussed. In [6] perfect codes with respect to Mannheim metric and Lipschitz metric over Gaussian integers, Lipschitz integers and Hurwitz integers have been studied. Moreover, an upper bound on the codes with respect to Hurwitz metric over Hurwitz integers is given. Theory of quaternions was invented by Hamilton as a generalization of complex numbers. The muffin ideals over ring of quaternion integers were introduced by Werner in 2010([2], [9]). The structure of cyclic codes and its duals associated to muffin ideal of quaternion integer ring over the finite field $\mathbb{Z}_{p^e}$ with p is an odd prime integer have been studied by authors in series of papers ([24], [25]).
In this paper, structures of cyclic codes and their duals associated to muffin ideals on the ring of quaternion integer(not necessarily commutative) over the finite field $\mathbb{Z}_{p^e}$, where $e > 0$ be a integer have been studied. Also, self-dual codes over muffin ideals under consideration. This paper is organized as follows, in section 2 we define ring of quaternion integers and the basic notions associated with these rings. In section 3 we obtain the set of all generating polynomials of cyclic codes and their duals associated to muffin ideals of the ring . In section 4 the results on self-dual codes on muffin ideals of quaternion integer ring over the finite field $\mathbb{Z}_{p^e}$, where $e > 0$ be a integer have been studied. generator matrix and the Mannheim distance of these codes are given. Finally section 5 is the acknowledgement.

II. QUATERNION ALGEBRA

A generalized quaternion algebra $\mathcal{B}$ over commutative ring with unity R is a 4-dimensional R-algebra(free R -module of rank 4) with a basis $\{1, i, j, k\}$ where elements i, j are the standard generators such that, for some $a, b \in R - \{0\}$, $i^2 = a, j^2 = b, k = ij = -ji$ and so, $k^2 = ij(-ji) = -ab$. It is symbolically denoted as $(a, b/R)$ and represented as $R + iR + jR + kR$. So $\alpha \in \mathcal{B}$ defined as $\alpha = a_1 + a_2 i + a_3 j + a_4 k$ where $a_1, a_2, a_3, a_4 \in R$ and it's conjugate $\bar{\alpha} = a_1 - a_2 i - a_3 j - a_4 k$. Let's $N(\alpha) = \alpha\bar{\alpha} = a_1^2 + a_2^2 + a_3^2 + a_4^2$ - norm and $T(\alpha) = \alpha + \bar{\alpha} = 2a_1$- trace of α. Obviously from the quaternion multiplication, $\mathcal{B}$ is division ring (not necessarily commutative) and if R be a field then, is 4-dimensonal vector space ([21]). The inverse of α is also a quaternion taken as $\alpha^{-1} = \frac{\bar{\alpha}}{N(\alpha)}$. In particular if $a = b = -1$ and R-real field then $\mathcal{B}$ is called Hamilton's quaternion. Hurwitz unit is defined as the quaternion $\mu = \frac{1+i+j+k}{2}$, and it's inverse $\bar{\mu} = \frac{1-i-j-k}{2}$ so that $N(\mu) = \mu\bar{\mu} = 1$ and quaternion algebra $\mathcal{H} = \mathcal{B}[\mu]$ be the Hurwitz quaternion. Any $\alpha \in \mathcal{H}$ can represents as $\alpha = \alpha^{\circ} + e\mu$ where $\alpha^{\circ} \in \mathcal{B}$ and e is either 1 or 0. Moreover $\alpha \in \mathcal{H}$, then $\alpha = a_1 + a_2 i + a_3 j + a_4 k$ where $a_1, a_2, a_3, a_4 \in \mathbb{Z}$ or $a_1, a_2, a_3, a_4 \in \mathbb{Z} + \frac{1}{2}$. In this paper except as noted otherwise, we will use $a = b = -1$ and $R = \mathbb{z}_{p^e}$, for integer $e > 0$ -the ring of integer modulo odd prime p i.e. $\mathcal{B} = \left(-1, -1/\mathbb{z}_{p^e}\right)$. Since the definition of norm and trace one can easily see that, $\alpha^2 - (\alpha + \bar{\alpha})\alpha + \alpha\bar{\alpha} = 0$ hence, every $\alpha \in \mathcal{B}$ is the root of quadratic polynomial $x^2 - T(\alpha)x + N(\alpha) \in R[x]$ and hence we conclude from [21] the following theorem.

Theorem 2.1. Let $\mathcal{B}$ be a division $\mathbb{z}_{p^e}$-algebra of degree 2 over a field $\mathbb{z}_{p^e}$ with char $R \neq 2$. Then either $\mathcal{B} = K$ is a quadratic field extension of $\mathbb{z}_{p^e}$ or $\mathcal{B}$ is a division quaternion algebra over $\mathbb{z}_{p^e}$.

Also for any $\alpha \in \mathcal{B}$, we define the minimal polynomial of α to be $\min_{\alpha}(x) = \begin{cases} x^2 - T(\alpha)x + N(\alpha), & \alpha \notin \mathbb{z}_{p^e}, \\ x - \alpha, & \alpha \in \mathbb{z}_{p^e}. \end{cases}$

For each $\alpha \in \mathcal{B}$ the minimal polynomial is unique i.e. $f(\alpha) = 0$ if and only if $f(x) = \min_{\alpha}(x)$. Also for α, β in $\mathcal{B}$ it is obvious that $\min_{\alpha}(x) = \min_{\beta}(x)$ if and only if $N(\alpha) = N(\beta)$ and $T(\alpha) = T(\beta)$. From [2], there is an isomorphism between quaternion - $\mathcal{B}$ and $M_2(\mathbb{Z}_{p^e})$-the ring of 2x2 matrices over $\mathbb{Z}_{p^e}$ has been given in following result,

Theorem 2.2. [2] Let for odd prime p the commutative ring $\mathbb{Z}_{p^e}$ with $x^2 + y^2 = -1$ for all $x, y \in \mathbb{Z}_{p^e}$, then $\mathcal{B}$ is isomorphic to $M_2(\mathbb{Z}_{p^e})$-the ring of 2 x 2 matrices over $\mathbb{Z}_{p^e}$.

Remarks: 1) $\alpha \in \mathcal{B}$ is odd (resp. even) if $N(\alpha)$ is an odd (resp. even) positive integer. 2) $\alpha \in \mathcal{B}$ is said to be unit if $N(\alpha) = 1$. 3) $\alpha \in \mathcal{B}$ is a prime quaternions if it is not a unit, and for every $\beta, \gamma \in \mathcal{B}$, where $\alpha = \beta\gamma$ where , either β or γ is a unit. 4) Any quaternion $\alpha \in \mathcal{B}$ is a prime if $N(\alpha)$ is prime in $\mathbb{N}$-set of natural numbers. 5) Every quaternion $\alpha \in \mathcal{B}$ with $N(\alpha) > 1$ is a product of prime quaternions.

Lemma 2.3 [2] For every $\alpha \in \mathcal{B}(\text{or } \mathcal{H})$ & $n \geq 0$,there exist $\alpha_1, \alpha_2 \in \mathcal{B} \cap \mathbb{Q}(\text{or } \mathcal{H} \cap \mathbb{Q})$ such that $\alpha^n = \alpha_1\alpha + \alpha_2 \in \mathcal{B}(\text{or } \mathcal{H})$, where $\mathbb{Q}$- set of rational number.

Definition 2.4 The center of $\mathcal{B}$ is $Z(\mathcal{B}) = \{\alpha \in \mathcal{B} \mid \alpha\beta = \beta\alpha, \text{for all } \beta \in \mathcal{B}\}$. We say $\mathcal{B}$ is central if $Z(\mathcal{B}) = \mathbb{Z}_{p^e}$ and $\mathcal{B}$ is simple if the only two-sided ideals of $\mathcal{B}$ are (0) and $\mathcal{B}$ (or equivalently that any $\mathbb{Z}_{p^e}$-algebra homomorphism with domain $\mathcal{B}$ is either the zero map or injective).

Definition 2.5 Let $\pi \neq 0$ be an odd quaternion integer. If there exist $\delta \in \mathcal{B}$ such that $\alpha_1 - \alpha_2 = \delta\pi$ then $\alpha_1, \alpha_2 \in \mathcal{B}$ are said to be right congruent modulo π and it is denoted as $\alpha_1 \equiv_r \alpha_2$.

Since equivalence relation is well-defined, consider here the ring of the quaternion integers modulo this equivalence relation and denotes as $\mathcal{B}_\pi = \{\alpha \pmod{\pi} \mid \alpha \in \mathcal{B}\}$. According to the modulo function the mapping $\mu : \mathbb{Z}_{p^e} \longrightarrow \mathcal{B}_\pi$ defined by $\mu(t) = \left\lfloor \frac{t\overline{\pi}}{p^e} \right\rfloor \pi \pmod{\pi}$, $t \in \mathbb{Z}_{p^e}$ is isomorphism and hence $\mathcal{B}_\pi$ is isomorphic to$\mathbb{Z}_{p^e}$, where $p^e = \pi\overline{\pi}$ is an odd prime [6].

Definition 2.6 For quaternion integer ring $\mathcal{B}$, the set $\{f(x) \in \mathcal{B}_\pi[x] \mid f(\alpha) = 0 \text{ for all } \alpha \in \mathcal{B}_\pi\}$ is called the Muffin of $\mathcal{B}_\pi$ and denoted as Muff $\mathcal{B}_\pi$.

Lemma 2.7 If $\mathcal{B}_\pi$ is finite nonzero quotient ring of $\mathcal{B}$, then Muff $\mathcal{B}_\pi$ is an ideal of $\mathcal{B}_\pi[x]$.

Lemma 2.8 Let $\mathcal{B}_\pi$ is a finite nonzero quotient ring of $\mathcal{B}$, then Muff $\mathcal{B}_\pi$ contains a monic polynomials with coefficients in $\mathbb{Z}_{p^e}$.

From the above lemmas it is clears that Muff $\mathcal{B}_\pi$ is a nonzero ideal containing a monic polynomials with coefficients in $\mathbb{Z}_{p^e}$, hence there exist such a polynomial with least degree. Now since quaternion integer ring $\mathcal{B}_\pi$ need not be commutative, throughout this paper the product of any polynomials $f(x), g(x) \in \text{Muff}\mathcal{B}_\pi[x]$ has taken as, $(f * g)(x) = \sum_i \alpha_i\, g(x)x^i$. So that for $\alpha \in \mathcal{B}_\pi$ the product taken as $(f * g)(\alpha) = \sum_i \alpha_i\, g(\alpha)\alpha^i$ such that if $g(\alpha) = 0$ then $(f * g)(\alpha) = 0$.

For quadrature amplitude modulation (QAM) the Mannheim distance as minimum distance is more suitable to detect and correct single, double error over quaternions rather than hamming distance[12]. In this paper Mannheim distance as minimum distance over $\mathcal{B}_\pi$ is under consideration.

Definition 2.9 For any $\alpha, \beta \in \mathcal{B}_\pi$ and $\gamma = \alpha - \beta = \gamma_1 + \gamma_2 i + \gamma_3 j + \gamma_4 k \in \mathcal{B}_\pi$ the quaternion Mannheim weight of γ is denoted and defined as, $\omega_M(\gamma) = |\gamma_1| + |\gamma_2| + |\gamma_3| + |\gamma_4|$ is minimum. Also, the quaternion Mannheim distance δ_M between quaternions α and β in $\mathcal{B}_\pi$ is defined as $\delta_M(\alpha, \beta) = \omega_M(\gamma)$, here $\delta_M : \mathcal{B}_\pi \times \mathcal{B}_\pi \longrightarrow \mathcal{B}_\pi$. Obviously the quternion Mannheim distance δ_M is metric over $\mathcal{B}_\pi$([4], [6], [12], [23]).

III. CYCLIC AND IT'S DUAL CODES OVER *Muff* $\mathcal{B}_\pi$

3.1. Cyclic Codes

Let $C = \{(q_0, q_1, q_2, \ldots, q_{n-1}) \in \mathcal{B}_\pi{}^n \mid f(q_i) = 0\ \forall\ q_i \in \mathcal{B}_\pi, 0 \leq i \leq n-1\ \&\ f(x) \in \mathcal{B}_\pi[x]\}$, so by definition C is the Muff $\mathcal{B}_\pi = \{f(x) \mid f(q_i) = 0\ \forall\ q_i \in \mathcal{B}_\pi, 0 \leq i \leq n-1\}$. Now the map $\mathcal{B}_\pi{}^n \longrightarrow \mathcal{B}_\pi[x]/(x^2 - 1)$ given by $(q_0, q_1, q_2, \ldots, q_{n-1}) \longrightarrow q_0 + q_1x + q_2x^2 + \cdots + q_{n-1}x^{n-1}$ is bijective and implies that for any $(q_0, q_1, q_2, \ldots, q_{n-1}) \in C$ the cyclic shift $(q_{n-1}, q_0, q_1, \ldots, q_{n-2})$ is in C . This correspondence defines $C \in \mathcal{B}_\pi{}^n$ is a $\mathcal{B}_\pi$-quaternion cyclic codes of length n. We have following well established results related to these codes ([1], [4]).

Lemma 3.1.1 Let $\mathcal{B}_\pi$ is quotient of quaternion ring where π is odd prime in $\mathcal{B}$ with $p^e = \pi\overline{\pi}$, then Muff $\mathcal{B}_\pi$ contains a monic polynomial with coefficients in $\mathbb{Z}_{p^e}$.

Lemma 3.1.2 Let $\mathcal{B}_\pi$ is quotient of quaternion ring where π is odd prime in $\mathcal{B}$ with $p^e = \pi\overline{\pi}$ then, every monic quadratic polynomial in $\mathbb{Z}_{p^e}[x]$ is the minimal polynomial of some $\alpha \in \mathcal{B}_\pi - \mathbb{Z}_{p^e}$.

Lemma 3.1.3 Let $\mathcal{B}_\pi$ is quotient of quaternion ring where π is odd prime in $\mathcal{B}$ with $p^e = \pi\overline{\pi}$ then, $g_{p^e}(x) = (x^{p^2} - x)(x^p - x)$ is generating polynomial for the quaternion cyclic code C over $\mathcal{B}_\pi$.

Theorem 3.1.4 Let $C \neq \{0\}$ of $\mathcal{B}_\pi{}^n$ is a cyclic code of length n over of $\mathcal{B}_\pi$. Let $g_{p^e}(x)$ be a monic code polynomial of minimal degree in C. Then $g_{p^e}(x)$ is uniquely determined in C with $C = \{q(x)g_{p^e}(x) \mid q(x) \in \mathcal{B}_\pi[x], \deg(q(x)) = n - r\}$ where $r = \deg(g_{p^e}(x)) = ap^2 + bp$. In particular, C has dimension $k = n - r = n - (ap^2 + bp)$ with odd prime $p^e = \pi\overline{\pi} \in \mathbb{Z}_{p^e}$ and $a, b \in \{0,1\}$ depends on whether the roots of $g_{p^e}(x)$ are in $\mathbb{Z}_{p^e}$ or not. The polynomial $g_{p^e}(x)$ divides $(x^n - 1)$ in Muff $\mathcal{B}_\pi$.

Definition 3.1.5 Let $f(x)$ be the polynomial in $\mathcal{B}_\pi[x]$. The content of $f(x)$ is the ideal of $\mathcal{B}_\pi$ generated by the coefficients of $f(x)$. That is, if $f(x) = \sum_{r=0}^{m} \alpha_r x^r \in \mathcal{B}_\pi[x]$ the content of $f(x)$ to be an ideal $(\alpha_0, \alpha_1, \ldots, \alpha_m)$ and it is denoted as $\text{con}(f)$.

Definition 3.1.6 Let $\pi \in \mathcal{B}$ be odd quaternion. The annihilator of an Ideal $\mathbb{I} = \pi\mathcal{B}$ in a ring $\mathcal{B}$ to be define as a set $A(\alpha) = \{\alpha \in \mathcal{B} \mid \alpha\,\mathbb{I} = \mathbb{I}\alpha = (0) = (x^n - 1)\}$.

Definition 3.1.7 Let $\pi\mathcal{B}$ be an ideal in a ring $\mathcal{B}$ and let $\varphi: \mathcal{B} \to \frac{\mathcal{B}}{\pi\mathcal{B}} = \mathcal{B}_\pi$ be the quotient map. We define inverse image of Muff $\mathcal{B}_\pi$ in $\mathcal{B}_\pi[x]$ as $\widetilde{\text{Muff}}(\mathcal{B}_\pi) = \varphi^{-1}\text{Muff}\,\mathcal{B}_\pi = \{f(x) \in \mathcal{B}_\pi[x] \mid f(\alpha) \in \pi\mathcal{B} \text{ for all } \alpha \in \mathcal{B}\}$.

Theorem 3.1.8 Let $\mathcal{B}_\pi$ is quotient of quaternion ring where π is odd in $\mathcal{B}$ with $p^e = \pi\overline{\pi}$, $e > 0$. Assume that $p_1, p_2, \ldots, p_t$ are all primes dividing the norm of π, then generating set for cyclic code over Muff $\mathcal{B}_\pi$ obtains as

$$\text{Muff}\,\mathcal{B}_\pi = \left(g_{p^e},\ p_1\widetilde{\text{Muff}}(\mathcal{B}_\pi/A(p_1)), \ldots,\ p_t\widetilde{\text{Muff}}(\mathcal{B}_\pi/A(p_t))\right).$$

Proof: Let $\mathbb{I} = \left(g_{p^e}, \widetilde{p_1 Muff}(\mathcal{B}_\pi/A(p_1)), \ldots, \widetilde{p_t Muff}(\mathcal{B}_\pi/A(p_t))\right)$. Since the definition of inverse image to Muff $\mathcal{B}_\pi$,for any element γ and any ideal $\mathbb{I}$ of $\mathcal{B}_\pi$ such that $\mathbb{I} \subseteq A(\gamma)$ then, $\widetilde{\gamma Muff}(\mathcal{B}_\pi/\mathbb{I}) \subseteq Muff\,\mathcal{B}_\pi$. So that $\mathbb{I} \subseteq Muff\,\mathcal{B}_\pi$. Now we want to prove $\mathbb{I} \supseteq Muff\,\mathcal{B}_\pi$. Let $f(x) \in Muff\,\mathcal{B}_\pi$, since g_{p^e} is monic there exist $g(x), h(x) \in \mathcal{B}_\pi[x]$ such that $f = gg_{p^e} + h$ where either $h = 0$ or $deg(h) < deg(g_{p^e})$. If $h = 0$, then $f(x) \in \langle g_{p^e}\rangle$ hence, desire. So assume $deg(h) < deg(g_{p^e})$. It is sufficient to show that $h(x) \in \left(\widetilde{p_1 Muff}(\mathcal{B}_\pi/A(p_1)), \ldots, \widetilde{p_t Muff}(\mathcal{B}_\pi/A(p_t))\right)$. Since $deg(h) < deg(g_{p^e})$, then $con(h) \neq 1$. Hence there exist a prime divisor p_l of $N(\pi)$ with $con(h) \subseteq p_l\mathcal{B}_\pi$. Then $h(x) \in \left(\widetilde{p_l Muff}(\mathcal{B}_\pi/A(p_l))\right)$, so that $Muff\,\mathcal{B}_\pi \subseteq \mathbb{I}$. Hence, desire.

3.2. Dual of Cyclic Codes

Definition 3.2.1 Let C be an quaternion cyclic code over $\mathcal{B}_\pi$with the generator polynomial $g_{p^e}(x)$. The polynomial $h(x) \in \mathcal{B}_\pi[x]$ determined by $x^n - 1 = h(x)g_{p^e}(x)$ is said to be check polynomial for C.

Following corollary is an easy consequence of theorem 3.1.4.

Corollary 3.2.2 There is an one-to-one correspondence between the cyclic codes on ${\mathcal{B}_\pi}^n$ and the monic divisors of $x^n - 1$ in $\mathcal{B}_\pi[x]$

Lemma 3.2.3 If C is the cyclic code of length n with check polynomial $h(x)$, then $C = \{c(x) \in \mathcal{B}_\pi[x] \mid c(x)h(x) = 0\ mod\ x^n - 1\}$.

Proof: If $c(x) \in C$, then by above theorem 3.1.4 there is a $q(x)$ with $c(x) = q(x)g_{p^e}(x)$. Then $c(x)h(x) = q(x)g_{p^e}(x)h(x) = q(x)(x^n - 1) = 0(mod(x^n - 1))$. Now consider an arbitrary polynomial $c(x) \in \mathcal{B}_\pi[x]$ with $c(x)h(x) = u(x)(x^n - 1)$ say. Then $c(x)h(x) = u(x)(x^n - 1) = u(x)g_{p^e}(x)h(x)$, hence $[c(x) - u(x)g_{p^e}(x)]h(x) = 0$. As $x^n - 1 = h(x)g_{p^e}(x)$ and $h(x) \neq 0$. There fore $c(x) - u(x)g_{p^e}(x) = 0$ and $c(x) = u(x)g_{p^e}(x)$ as desired.

Definition 3.2.4 Let C be a linear code over $\mathcal{B}_\pi$, the dual code $C^\perp$ of code C is the set of all vectors which are orthogonal to all code words in C.That is $C^\perp = \{\, d(x) \mid c(x)d(x) = 0\ \forall\ c(x) \in C\,\}$.

It is straight forward that if C is a linear code, then $C^\perp$ is also a linear code.

Definition 3.2.5 Let $h(x) = \sum_{i=0}^{k} h_i x^i$ be a polynomial of degree k over $\mathcal{B}_\pi$ then reciprocal polynomial is denoted and defined as $h_R(x) = x^k h(\frac{1}{x})$.

Remarks: The non zero roots of polynomial $h(x)$ are the roots of its reciprocal polynomial $h_R(x)$. If the polynomial $h(x)$ is divisor of $x^n - 1$ over $\mathcal{B}_\pi$ then its reciprocal polynomial $h_R(x)$ also be a divisor of $x^n - 1$ over $\mathcal{B}_\pi$.

In next theorem we conclude the dual $C^\perp$ of a cyclic code C is again a cyclic code and it associated with the check polynomial of C over $\mathcal{B}_\pi$.

Theorem 3.2.6 If C is the cyclic code of length n with check polynomial $h(x)$ of degree, $n - r$ then $C^\perp$ is cyclic with generator polynomial $\frac{1}{h_0}h_R(x)$, where h_0 is constant term of $h(x)$.

IV. SELF-DUAL CODES ON *Muff*$\mathcal{B}_\pi$

These part introduces self-dual codes on muffin ideals Muff $\mathcal{B}_\pi$ of quaternion integer ring $\mathcal{B}_\pi$. Let us first define self-dual codes over muffin ideals of quaternion ring as,

Definition 4.1 A code C on muffin ideal of is said to be self-orthogonal if $C \subseteq C^\perp$ and self-dual if $C = C^\perp$.

In [14] C.J. Miguel, R. Serodio has shown that for odd prime p quaternion integer ring $\mathcal{B}$ contains the zero-divisors and idem-potent elements given as, for odd prime p the number of zero- divisors in $\mathcal{B}$ is $p^3 + p^2 - p$, where as the number of idem-potent elements in $\mathcal{B}$ is $p^2 + p + 2$ and for prime quaternion integer $\pi \in \mathcal{B}$, the quotient ring $\mathcal{B}_\pi$ has cardinality $2\,N(\pi)^2 - 1$[6].

Also consider an idempotent in $\mathcal{B}_\pi[x]$ is a polynomial $e(x)$ such that $e(x)^2 = e(x^2) = e(x) mod(x^n - 1)$. In particular $E(x) = \sum_{i=0}^{i=n-1} q_i x^i$ is idempotent if and only $q_i = q_{2i}(mod\ n)$. It is obvious that, a cyclic code or ideal $C = \langle g_{p^e}(x)\rangle$ contains a unique idempotent $E(x)$ such that $C = \langle E(x)\rangle$. Also $E(x) = p(x)\,g_{p^e}(x)$ for some polynomial $p(x)$, and $E(\alpha^i) = 0$ iff $g_{p^e}(\alpha^i) = 0$ where$\alpha^i \in \mathcal{B}_\pi$ for . The code polynomial $c(x) \in C$ if and only if $c(x)E(x) = c(x)$. (C may contain several idempotents, but only one of them generates C.)

Now we have sets up following result regarding the self-dual codes o muffin ideals of quaternion integer ring $\mathcal{B}_\pi$ as,

Theorem 4.2 Let $C = \{(q_0, q_1, q_2, \ldots, q_{n-1}) \in {\mathcal{B}_\pi}^n : f(q_i) = 0\ \forall\ q_i \in \mathcal{B}_\pi, 0 \leq i \leq n - 1\ \&\ f(x) \in \mathcal{B}_\pi[x]\}$ be cyclic code then it is self-dual code if the quaternions $q_0, q_1, q_2, \ldots, q_{n-1}$ are the idem-potent elements of $\mathcal{B}_\pi$.

Proof: Since code polynomial $c(x) \in C$ if and only if $c(x)E(x) = c(x)$. Let $E(x) = \sum_{i=0}^{i=n-1} q_i x^i$ is idempotent polynomial and $q_0, q_1, q_2, \ldots, q_{n-1}$ are the idem-potent elements of $\mathcal{B}_\pi$. Again $E(x)$ is an idempotent if and only if $E(\alpha^i) = 0$ or 1 for $i = 0, 1, \ldots, n - 1$. If $E(\alpha^i) = 0$ implies generating polynomial $g_{p^e}(\alpha^i) = 0$ it means that $C = \langle g_{p^e}(x)\rangle = \langle 0\rangle = C^\perp$. Otherwise, if $E(\alpha^i) = 1$. We have $C = \langle E(x)\rangle = \langle 1\rangle = C^\perp$. Hence quaternion code C is self-dual, as desire.

V. ACKNOWLEDGMENT

Authors are thankful to The Director, Sanmati Engineering College, Washim and The Editor, International Journal of Emerging Technology and Innovative Research for National Conference on Recent Development in Sciences, Engineering and Technology (RDSET)-2019. Also, first two authors great thankful to The Principal, Government Polytechnic, Hingoli for his moral support in research and publication of these article.

REFERENCES

[1] Huber K., 1994, Codes Over Gaussian Integers, IEEE Trans. Inform. Theory, vol. 40: 207-216.

[2] Nicholas J. Werner, 2010, Integer-valued polynomials over quaternion rings, Journal of Algebra. 32(4):1754-1769.

[3] Guiliana Davidoff, Peter Sarnak and Alain Velette, Elementary number theory, group theory and Ramanujan graphs

[4] .Mehmet Ozen, Murat Guzeltepe, 2009, Cyclic codes over some finite quaternion integer rings, Department of Mathematics, Sakarya University, TR54187 Sakarya, Turkey

[5] Gross, Benedict H., and Mark W. Lucianovic, 2009. On cubic rings and quaternion rings. Journal of Number Theory 129(6): 1468-1478.

[6] Murat Guzeltepe, 2012, Perfect mannheim, Lipschitz and Hurwitz weight codes, Department of Mathematics, Sakarya University, TR54187 Sakarya, Turkey

[7] Taher Abualrub, 1999, Cyclic Codes And Their Duals Over $\mathbb{z}_m$, Ann. Sci. Math. Quebec 23(2): 109-118.

[8] F. J. MacWilliams and N. J. A. Sloane, 1978, The Theory of Error-Correcting Codes. Amsterdam, The Netherlands: North-Holland.

[9] Nicholas J. Werner, Integer-valued Polynomials over Matrix Rings, Department of Mathematics, The Ohio State University, 231 West 18th Avenue, Columbus, OH 43210

[10] Mehmet Özen, Murat Güzeltepe, Cyclic Codes over Some Finite Rings, Department of Mathematics, Sakarya University, TR54187 Sakarya, Türkiye

[11] Milan Markovic, 2014, Factorization of natural numbers based on quaternion algebra using lipschitz integers, Institute of Mathematics University of Zurich

[12] Murat Guzeltepe, Olof Heden, 2014, Perfect Mannheim, Lipschitz and Hurwitz weight codes Math. Commun. 19: 253–276.

[13] Sophie Frisch, 2013, Integer-valued polynomials on algebras, Appeared in J. Algebra 373: 414-425.

[14] C.J. Miguel, R. Serodio,2011, On the structure of quaternion rings over z_p, International journal on algebra, 27(5):1313-1325

[15] Pramod Kumar Kewat, Bappaditya Ghosh and Sukhamoy Pattanayak, 2015, Cyclic codes over the Ring $\mathbb{z}_p[u,v]/\langle u^2, v^2, uv - vu\rangle$ 34:161-175.

[16] Pramod Kumar Kewat and Sarika Kushwaha, 2017, Cyclic codes over the Ring $F_p[u,v,w] / \langle u^2, v^2, w^2, uv - vu, vw - wv, uw - wu\rangle$, Bulletin of Korean Mathematical Society

[17] T.Y. Lam, 1991, A first course in noncommutative rings, Springer-Verlag,.

[18] Bahattin Yildiz and Suat Karadeniz. 2011, Cyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$, Des.Codes Cryptogr., 58(3):221–234.

[19] Taher Abualrub and Irfan Siap. 2007, Cyclic codes over the rings $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2Z_2$, Des. Codes Cryptogr., 42(3):273-287.

[20] Taher Abualrub and Irfan Siap. 2006, On the construction of cyclic codes over the ring $Z_2 + uZ_2$, In Proceeding the 9th WSEAS international conference on applied mathematics, Istanbul, Turkey, pp 430-435.

[21] John Voight, 2017, Quaternion algebras, jvoight@gmail.com v0.9.2.

[22] Rudolf Lidl and Harald Niederreiter, 1986, Introduction to finite fields and their applications, Cambridge University Press, Cambridge,.

[23] Mehmet Özen, Murat Güzeltepe, 2010, Codes over Quaternion Integers, European Journal of Pure and Applied Mathematics 3(4): 670-677

[24] Shaikh J.S., Patil A.R., 2018, Cyclic codes associated muffin ideals over quaternion integer ring $(-1 - 1/Z_p)$, Asian Journal of Mathematics and Computer Research 24(2): 67-74,

[25] Shaikh J.S., Patil A.R., 2019, Codes over muffin ideals of quaternion integer ring $(-1 - 1/\mathrm{Z_p})$, Journal of Computer and Mathematical Sciences, 10(1): 20-32.