Journal of Computer and Mathematical Sciences, *Vol.10(1),20-32 January 2019* *ISSN 0976-5727 (Print)*
(An International Research Journal), *www.compmath-journal.org* *ISSN 2319-8133 (Online)*

Codes over Muffin Ideals of Quaternion Integer Ring-$\left(\frac{-1,-1}{\mathbb{Z}_p}\right)$

Shaikh Javed Shafee[1]* and Arunkumar R. Patil[2]

[1]Department of Mathematics,
Government Polytechnic, Hingoli-431513 (M.S.), INDIA.
[2]Department of Mathematics,
Shri Guru Gobind Singhji Institute of Engineering & Technology,
Nanded-431606 (M.S.), INDIA.
email:shaikhjaved2080@gmail.com, arun.iitb@gmail.com

(Received on: December 20, 2018)

ABSTRACT

In this paper dual of cyclic codes and BCH-codes constructed associated with Muffin ideals over quaternion integer rings-$\left(\frac{-1,-1}{\mathbb{Z}_p}\right)$ where $\mathbb{Z}_p$-set of integers modulo an odd prime number p. Later, a generator matrix in standard form, the generator polynomial, length, dimension for these BCH code find outs explicitly. Also, the decoding method for BCH codes over-$\left(\frac{-1,-1}{\mathbb{Z}_p}\right)$ has given.

Keywords: Cyclic codes, Dual codes, BCH codes, Quaternion algebra, Muffin Ideal**,** Mannheim distance.

1. INTRODUCTION

Cyclic codes and their duals over different rings are of considerable interests to both the mathematicians and engineers due to their algebraic structure and enormous engineering applications. Therefore, Cyclic codes and their duals with respect to different metrics (distance) such as Hamming distance, Lee distance, Hurwitz distance has become a popular area of research to many researchers belonging to these communities. Recently, cyclic codes with Mannheim distance over rings of Gaussian integers are introduced by K. Huber[3] in 2004 and further studied by M. Ozen and M. Guzeltepe in 2009[5,6]. For the knowledge of Quaternion

rings over integers one can refer to the work of Hamilton[7]. The quaternion rings of integers and Muffin ideals over ring of quaternion integers were introduced by Werner in 2010[2,4]. The cyclic codes associated to muffin ideals over quaternion integer ring discussed in[1]. BCH codes are a well known class of linear codes and every text book on coding theory with the method of decoding discussed in[13]. The detailed about muffin ideals of quatenion integer rings has given by Werner in[2].

The main goal of this paper is to compute generating sets for dual of cyclic codes and the decoding method of BCH associated with the muffin ideals of a quaternion integer ring not necessarily commutative. We determine the generator matrix in standard form of these codes. Also, the decoding algorithm for BCH codes has given here. The content of this paper is organized as follows. In section 2, we define rings of quaternion integers and the basic notions associated with these rings. In section 3, we obtain the set of all generating polynomials and the generator matrix in standard form for dual of cyclic codes associated to muffin ideals. In section 4, the generator polynomial for BCH codes and their decoding method with algorithm over quotient ring of quaternion integer ring modulo a odd quaternion π has given.

2. PRELIMINARIES

An algebra $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)$ over Galois field $\mathbb{Z}_p$ where p-odd prime is a Hamilton quaternion algebra if there is a basis $\{1, e_1, e_2, e_3\}$ such that ${e_1}^2 = {e_2}^2 = -1, e_3 = e_1e_2 = -e_2e_1$ with any quaternion element $\alpha \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)$ is of the form $\alpha = a + be_1 + ce_2 + de_3$, where $a, b, c, d \in \mathbb{Z}_p$ and p is odd prime integer. For all quaternions α, β in $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)$ the addition $\alpha + \beta$ and multiplication $\alpha\beta$ are again in $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)$, hence this quaternion ring is the associative division ring with unity(not necessarily commutative). The bar conjugate $\overline{\alpha}$ is defined as $\overline{\alpha} = a - be_1 - ce_2 - de_3$. We can associate two measures for any $\alpha \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)$ called norm and trace. For an $\alpha = a + be_1 + ce_2 + de_3$ its norm is denoted and defined by $\eta(\alpha) = \alpha\overline{\alpha} = \overline{\alpha}\alpha = |\alpha|^2 = \mathrm{a}^2 + b^2 + c^2 + d^2$, so for all $\alpha \neq 0$ quaternions, the inverse of α is also a quaternions which obtains as $\alpha^{-1} = \frac{\overline{\alpha}}{\eta(\alpha)}$. Another obvious property of norm is $\eta(\alpha\beta) = \eta(\alpha)\eta(\beta)$. Similarly, the trace measure is denoted by $\tau(\alpha) = \alpha + \overline{\alpha}$. It follows that $\tau(\alpha) = 2a$. Since, $\alpha^2 = \alpha^2 + \alpha\overline{\alpha} - \alpha\overline{\alpha} = \alpha(\alpha + \bar{\alpha}) - \alpha\overline{\alpha}$ so any quaternion $\alpha \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)$ is the root of quadratic equation $x^2 - \tau(\alpha)x + \eta(\alpha) = 0$. Also center of $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)$ is field, hence for any quaternion the minimal polynomial is,

$$min_\alpha(x) = \begin{cases} x^2 - \tau(\alpha)x + \eta(\alpha), & \alpha \notin \mathbb{Z}_p \\ x - \alpha, & \alpha \in \mathbb{Z}_p. \end{cases}$$

For α, β in $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)$ it is obvious that $min_\alpha(x) = min_\beta(x)$ if and only if $\eta(\alpha) = \eta(\beta)$ and $\tau(\alpha) = \tau(\beta)$.

Proposition 1 Let p be an odd prime and $x, y \in \mathbb{Z}_p$ such that for any $x^2 + y^2 = -1$, then $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)$ is isomorphic to $\mathcal{M}_2(\mathbb{Z}_p)$ ring of the matrices of order 2×2 over $\mathbb{Z}_p$ [2].

Regarding quaternion elements α in $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)$ following are the straightforward consequences. α is odd (resp. even) quaternion if $\eta(\alpha)$ is an odd (resp. even) positive integer. α is an unit quaternion if $\eta(\alpha) = 1$. α is a prime quaternion if it is not a unit and for every $\beta, \gamma \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)$, with $\alpha = \beta\gamma$ then either β or γ is a unit. α is a product of prime quaternions if it is not a prime and $\eta(\alpha) > 1$. Also for integer $n > 0$, there exist $\alpha_1, \alpha_2 \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right) \cap \mathbb{Q}$ such that $\alpha^n = \alpha_1\alpha + \alpha_2 \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)$, where $\mathbb{Q}$ - set of rational numbers[2].

Definition 1 Let $\pi \neq 0$ be an odd quaternion integer. If there exist $\delta \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)$ such that $\alpha_1 - \alpha_2 = \delta\pi$ then $\alpha_1, \alpha_2 \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)$ 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 $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi = \left\{\alpha \,(mod\, \pi) \mid \alpha \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)\right\}$. According to the modulo function the mapping $\mu : \mathbb{Z}_p \longrightarrow \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ defined by $\mu(t) = \left[\frac{t\overline{\pi}}{p}\right]\pi(mod\, \pi),\ t \in \mathbb{Z}_{\boldsymbol{p}}$ is isomorphism and hence $\left(\frac{-1,-1}{\mathbb{Z}_{\boldsymbol{p}}}\right)_\pi$ is isomorphic to $\mathbb{Z}_{\boldsymbol{p}}$,
where $\boldsymbol{p = \pi\overline{\pi}}$ is an odd prime[6].

Definition 2 For quaternion integer ring $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)$, the set $\left\{f(x) \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi[x] \mid f(\alpha) = 0 \text{ for all } \alpha \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi\right\}$ is called the Muffin of $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ and denoted as $Muff\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$.

Proposition 2 If $\left(\frac{-1,-1}{\mathbb{Z}_{\boldsymbol{p}}}\right)_{\boldsymbol{\pi}}$ is finite nonzero quotient ring of $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)$ then $Muff\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ is an ideal of $\left(\frac{-1,-1}{\mathbb{Z}_{\boldsymbol{p}}}\right)_{\boldsymbol{\pi}}[x]$.

Proposition 3 Let $\left(\frac{-1,-1}{\mathbb{Z}_{\boldsymbol{p}}}\right)_{\boldsymbol{\pi}}$ is a finite nonzero quotient ring of $\left(\frac{-1,-1}{\mathbb{Z}_{\boldsymbol{p}}}\right)$ and $n = char\left(\frac{-1,-1}{\mathbb{Z}_{\boldsymbol{p}}}\right)_{\boldsymbol{\pi}}$, then $Muff\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ contains a monic polynomials with coefficients in $\mathbb{Z}_p$.

From the above propositions it is clears that $Muff\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ is a nonzero ideal containing a monic polynomials with coefficients in $\mathbb{Z}_p$, hence there exist such a polynomial with least degree. Now since quaternion integer ring $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ need not be commutative, throughout this paper the product of any polynomials $f(x), g(x) \in Muff\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi[x]$ has taken as, $(f * g)(x) = \sum_i \alpha_i\, g(x)x^i$. So that for any $\alpha \in Muff\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ the product taken as $(f * g)(\alpha) = \sum_i \alpha_i\, g(\alpha)\alpha^i$ such that if $g(\alpha) = 0$ then $(f * g)(\alpha) = 0$.

3. CYCLIC AND IT'S DUAL CODES OVER $Muff\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$

3.1 Cyclic Codes

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

Proposition 4 Let $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ is quotient of quaternion ring where π is odd prime in $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)$ with $p = \pi\overline{\pi}$, then $Muff\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ contains a monic polynomial with coefficients in $\mathbb{Z}_p$.

Proposition 5 Let $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ is quotient of quaternion ring where π is odd prime in $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)$ with $p = \pi\overline{\pi}$ then, every monic quadratic polynomial in $\mathbb{Z}_p[x]$ is the minimal polynomial of some $\alpha \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi - \mathbb{Z}_p$.

Theorem 6 Let $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ is quotient of quaternion ring where π is odd prime in $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)$ with $p = \pi\overline{\pi}$ then, $g_p(x) = (x^{p^2} - x)(x^p - x)$ is generating polynomial for the quaternion cyclic code C over $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$.

Also the generating matrix $\mathbb{G}$ for quaternion cyclic code one can obtains here as,

$$\mathbb{G} = \begin{bmatrix} g_p(x) \\ xg_p(x) \\ x^2 g_p(x) \\ \vdots \\ x^{n-(ap^2+bp)-1} g_p(x) \end{bmatrix},$$

where the length of cyclic code C is given by $n = k + ap^2 + bp$ with dimension k for all p-odd prime and $a, b \in \{0,1\}$ depends on whether $\boldsymbol{\alpha} \notin \mathbb{z}_{\boldsymbol{p}}$ or $\boldsymbol{\alpha} \in \mathbb{z}_{\boldsymbol{p}}$ **(**i.e. whether minimal polynomials are linear and/or quadratic)

Theorem 7 Let $C \neq \{0\}$ of $\left(\frac{-1,-1}{\mathbb{z}_{\boldsymbol{p}}}\right)_{\boldsymbol{\pi}}^{\boldsymbol{n}}$ is a cyclic code of length n over of $\left(\frac{-1,-1}{\mathbb{z}_{\boldsymbol{p}}}\right)_{\boldsymbol{\pi}}$. Let $g_p(x)$ be a monic code polynomial of minimal degree in C. Then $g_p(x)$ is uniquely determined in C with $C = \{q(x)g_p(x) | \, q(x) \in \left(\frac{-1,-1}{\mathbb{z}_{\boldsymbol{p}}}\right)_{\boldsymbol{\pi}} [x], \, deg(q(x)) = n - r\}$ where $r = deg(g_p(x)) = ap^2 + bp$. In particular, C has dimension $k = n - r = n - (ap^2 + bp)$ with odd prime $p = \pi\overline{\pi} \in z_p$ and $a, b \in \{0,1\}$ depends on whether the roots of $g_p(x)$ are in $\mathbb{z}_{\boldsymbol{p}}$ or not. The polynomial $g_p(x)$ divides $(x^n - 1)$ in $Muff\left(\frac{-1,-1}{\mathbb{z}_p}\right)_{\pi}$.

Proof. As $C \neq \{0\}$, it contains nonzero code polynomials, each of which has a unique monic scalar multiple. Thus there is a monic polynomial $g_p(x)$ in C of minimal degree . Let this degree is $r = ap^2 + bp$ where $a, b \in \{0,1\}$ depends on whether the roots of $g_p(x)$ are in $\mathbb{z}_{\boldsymbol{p}}$ or not and its unique even if $g_p(x)$ is not. Let set of polynomials $C_1 = \{q(x)g_p(x) \mid q(x) \in \left(\frac{-1,-1}{\mathbb{z}_{\boldsymbol{p}}}\right)_{\boldsymbol{\pi}} [x], de\, g(q(x)) = n - r\}$. Obviously C_1 certainly contained in C, since it is composed of those multiples of the code polynomial $g_p(x)$ with the additional property of having degree less than n. Also, under addition and scalar multiplication C_1 is an $\left(\frac{-1,-1}{\mathbb{z}_{\boldsymbol{p}}}\right)_{\pi}$-vector space of dimension $n - r$. Since $g_p(x)$ is generator polynomial the code polynomial $c(x)$ is an $\left(\frac{-1,-1}{\mathbb{z}_{\boldsymbol{p}}}\right)_{\pi}[x]$-multiple of $g_p(x)$ and so is in the set C_1. By the division algorithm we have $c(x) = q(x)g_p(x) + u(x)$ for some $q(x), \, u(x) \in \left(\frac{-1,-1}{\mathbb{z}_{\boldsymbol{p}}}\right)_{\pi} [x]$ with $de\, g(u(x)) < de\, g\left(g_p(x)\right)$. Therefore $u(x) = c(x) - q(x)g_p(x)$. Since, $c(x) \in C$ and $q(x)g_p(x) \in C_1$ (as $c(x)$ has degree less than n). Thus by linearity, the right hand side of this equation is in C, hence the remainder term $u(x) \in C$. If (x) was nonzero, then it would have a monic scalar multiple belonging to C and of smaller degree than r. But this would contradict the original choice of $g_p(x)$. Therefore $p(x) = 0$ and $c(x) = q(x)g_p(x)$, as desired.

Next let $x^n - 1 = h(x)g_p(x) + s(x)$ for some $s(x)$ of degree less than $de\, g\left(g_p(x)\right)$. Then as before, $s(x) = (-h(x))g_p(x) \pmod{(x^n - 1)}$ belongs to C. Again, if $s(x)$ is not zero, then

it has a monic scalar multiple belonging to C and of smaller degree than that of $g_p(x)$, a contradiction. Thus $s(x) = 0$ and $x^n - 1 = h(x)g_p(x)$, that is $g_p(x)$ divides $(x^n - 1)$.

3.2 Dual of Cyclic Codes

Definition 3 Let C be an quaternion cyclic code over $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ with the generator polynomial $g_p(x)$. The polynomial $h(x) \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi [x]$ determined by $x^n - 1 = h(x)g_p(x)$ is said to be check polynomial for C.

Following corollary is an easy consequence of theorem 7.

Corollary 8 There is an one-to-one correspondence between the cyclic codes in $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi^n$ and the monic divisors of $x^n - 1$ in $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi [x]$.

Proposition 9 If C is the cyclic code of length n with check polynomial $h(x)$, then $C = \{c(x) \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi [x] \mid c(x)h(x) = 0(mod(x^n - 1))\}$.

Proof. If $c(x) \in C$, then by above theorem 7 there is a $q(x)$ with $c(x) = q(x)g_p(x)$. But then $c(x)h(x) = q(x)g_p(x)h(x) = q(x)(x^n - 1) = 0(mod(x^n - 1))$. Now consider an arbitrary polynomial $c(x) \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi [x]$ with $c(x)h(x) = u(x)(x^n - 1)$ say. Then $c(x)h(x) = u(x)(x^n - 1) = u(x)g_p(x)h(x)$, hence $[c(x) - u(x)g_p(x)]h(x) = 0$. As $x^n - 1 = h(x)g_p(x)$ and $h(x) \neq 0$. There fore $c(x) - u(x)g_p(x) = 0$ and $c(x) = u(x)g_p(x)$ as desired.

Definition 4 Let C be a linear code over $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$, 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 $C^\perp = \{d(x) | c(x)d(x) = 0 \; \forall \; c(x) \in C$.

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

Definition 5 Let $h(x) = \sum_{i=0}^{k} h_i x^i$ be a polynomial of degree k over $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ then reciprocal polynomial is denoted and defined as $h_R(x) = x^k h(\frac{1}{x})$

Again as 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 $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ then its reciprocal polynomial $h_R(x)$ also be a divisor of$x^n - 1$ over $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$.

Next theorem concludes the dual $C^\perp$ of a cyclic code C is again a cyclic code and it associated with the check polynomial of C over $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$.

Theorem 10 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 $h(x)$.

Proof. Let the cyclic code C of length n have generator polynomial $g_p(x)$ of degree r and check polynomial $h(x)$ of degree $n-r=dim\ C$. From corollary, as $h(x)$ is a divisor of x^n-1, it is the generator polynomial for a cyclic code say D of length n and dimension $n-(n-r)=r$. We have $C=\{q(x)g_p(x)\mid q(x)\in\left(\frac{-1,-1}{\mathbb{z}_p}\right)_\pi[x],\ de\,g\big(q(x)\big)<n-r\}$ and $D=\{s(x)h(x)\mid s(x)\in\left(\frac{-1,-1}{\mathbb{z}_p}\right)_\pi[x],\ de\,g\big(s(x)\big)<r\}$. Let $c(x)=q(x)g_p(x)\in C$ with $de\,g\big(q(x)\big)\leq n-r-1$ and let $d(x)=s(x)h(x)\in D$ with $de\,g\big(s(x)\big)\leq r-1$. Consider $c(x)d(x)=q(x)g_p(x)s(x)h(x)=q(x)s(x)(x^n-1)=t(x)(x^n-1)=t(x)x^n-t(x)$,where $t(x)=q(x)s(x)$ with $deg\big(t(x)\big)\leq(n-r-1)+(r-1)=n-2<n-1$. Therefore the coefficient of x^{n-1} is 0. If $c(x)=\sum_{i=0}^{n-1}g_ix^i$ and $d(x)=\sum_{j=0}^{n-1}h_jx^j$ where, g_i, h_j are the quaternion integer modulo odd prime $p=\pi\overline{\pi}$, then the coefficient of x^m in $c(x)d(x)$ is $\sum_{i+j=m}g_ih_j$. Now from coefficient of x^{n-1} in $c(x)d(x)$ we obtain as, $0=\sum_{i+j=n-1}g_ih_j=\sum_{i=0}^{n-1}g_ih_{n-1-i}$

$=g_0h_{n-1}+g_1h_{n-2}+g_2h_{n-3}+\cdots\cdots\cdots+g_ih_{n-1-i}+\cdots\cdots\cdots+g_{n-3}h_2+g_{n-2}h_1+g_{n-1}h_0$

That means, dot product of code word $(g_0,g_1,g_2,\ldots\ldots,g_{n-1})\in C$ with $(h_{n-1},h_{n-2},h_{n-3},\ldots\ldots,h_1,h_0)$ is 0. From the definition $(h_{n-1},h_{n-2},h_{n-3},\ldots\ldots,h_1,h_0)$ is the codeword in $C^{\perp}$ and is a vector corresponding to reciprocal polynomial $h_R(x)$. So that $h_R(x)$ and its $k+1$ cyclic shift are the codewords in $C^{\perp}$. Hence dual code $C^{\perp}$ is also cyclic.

As $deg\big(h_R(x)\big)=deg\big(h(x)\big)=n-r$, the set $\{h_R(x),xh_R(x),\cdots\cdots\cdots,\mathrm{x}^{\mathrm{r}-1}h_R(x)\}$ is the basis for $C^{\perp}$. It shows $h_R(x)$ generates $C^{\perp}$. Thus the monic polynomial $\frac{1}{h_0}h_R(x)$, where h_0 is constant term of $h(x)$ is the generator polynomial of $C^{\perp}$.

From above generator matrix $\mathbb{H}$ for the dual code $C^{\perp}$ over quaternion ring $\left(\frac{-1,-1}{\mathbb{z}_p}\right)_\pi$ obtaines as,

$$\mathbb{H}=\begin{bmatrix}h_R(x)\\xh_R(x)\\x^2h_R(x)\\\vdots\\x^{(ap^2+bp)-1}h_R(x)\end{bmatrix}$$

Since center of quaternion integer ring $\left(\frac{-1,-1}{\mathbb{z}_p}\right)_\pi$ is finite field, the zeros α_i of x^n-1 are the nth roots of unity. And these roots forms cyclic subgroup in $\left(\frac{-1,-1}{\mathbb{z}_p}\right)$ such that $x^n-1=\prod_{i=0}^{n-1}(x-\alpha_i)$.

Definition 6 An element $\alpha \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ is said to be primitive nth root of unity if $x^n - 1 = \prod_{i=0}^{n-1}(x - \alpha^i)$. In another words, $\alpha \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ is primitive root if all the roots of $x^n - 1$ are some power of α.

Since, generator polynomial $g_p(x)$ and check polynomial $h(x)$ of cyclic code C are the factors of $x^n - 1$, following proposition sets relation between zeros of generator polynomials for C and $C^\perp$.

Proposition 11 If C is the cyclic code with generator polynomial $g_p(x)$ and check polynomial $h(x)$ over $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ then $g_p(x) = \prod_{i \in K}(x - \alpha^i)$, where $K = \{0,1,2,\ldots\ldots,n-1\}$. In particular some nth roots of unity are zeros of the code and another nth roots of unity which are non zeros of code are the zeros of dual of code. And so, any $c(x) \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi^n$ is a codeword in C if and only if $c(\alpha^i) = 0$.

Above proposition concludes possibility to define the cyclic codes in terms of zeros of code polynomials associated to $Muff\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$. As a consequence of this fact we construct a special type of cyclic code called Bose, Chaudhuri and Hocquenghem(BCH) codes.

4. BCH CODES ASSOCIATED TO $Muff\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$

4.1. BCH Codes over $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$

For quadrature amplitude modulation (QAM) the Mannheim distance as minimum distance is more suitable than hamming distance to detect and correct single, double error over quaternions[6] and hence Mannheim distance as minimum distance here is under consideration over $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$.

Definition 7 For any $\alpha, \beta \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ and $\gamma = \alpha - \beta = \gamma_1 + \gamma_2 e_1 + \gamma_3 e_2 + \gamma_4 e_3 \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$, 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 $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ is defined as $\delta_M(\alpha, \beta) = \omega_M(\gamma)$. Again since mapping $\delta_M : \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi \times \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi \longrightarrow \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ is well-defined, the quternion Mannheim distance δ_M is metric over $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ [1,6].

Definition 8 A cyclic code of length n over $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ is a BCH code of designed Mannheim distance δ_M(say) if for some integer b > 0, the generator polynomial $g_p(x)$ is the lowest degree

monic polynomial over $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_{\pi}$ having $\alpha^{\mathscr{b}}, \alpha^{\mathscr{b}+1}, \alpha^{\mathscr{b}+2}, \ldots\ldots\ldots, \alpha^{\mathscr{b}+\delta_M-2} \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_{\pi}$ as zeros. Further, if $\mathscr{b} = 1$ then corresponding code called as narrow-sense BCH code.

In another words, the cyclic code is a BCH code if generator polynomial $g_p(x) = L.C.M.\{\mathrm{M}^{\mathscr{b}}(\mathrm{x}), \mathrm{M}^{\mathscr{b}+1}(\mathrm{x}), \ldots\ldots \mathrm{M}^{\mathscr{b}+\delta_M-2}(\mathrm{x})\}$ where $\mathrm{M}^{\mathscr{b}}(\mathrm{x}), \mathrm{M}^{\mathscr{b}+1}(\mathrm{x}), \ldots\ldots \mathrm{M}^{\mathscr{b}+\delta_M-2}(\mathrm{x})$ are the unique monic minimal polynomials for the quaternions $\alpha^{\mathscr{b}}, \alpha^{\mathscr{b}+1}, \alpha^{\mathscr{b}+2}, \ldots\ldots\ldots, \alpha^{\mathscr{b}+\delta_M-2}$ respectively in $Muff\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_{\pi} \cap \mathbb{Z}_p[x]$ with minimum Mannheim distance δ_M. Hence, $c(x)$ is a BCH codeword if and only if $c(\alpha^{\mathscr{b}}) = c(\alpha^{\mathscr{b}+1}) = \cdots\ldots\ldots\ldots\ldots = c(\alpha^{\mathscr{b}+\delta_M-2}) = 0$.

Since, $\forall\ \alpha \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_{\pi}$ the minimal polynomial is $min_{\alpha}(x) = \begin{cases} x^2 - \tau(\alpha)x + \eta(\alpha), & \alpha \notin \mathbb{Z}_p \\ x - \alpha, & \alpha \in \mathbb{Z}_p \end{cases}$ with $min_{\alpha}(\alpha) = min_{\alpha}(\bar{\alpha}) = 0$. Let us consider $f(x) = h(x)min_{\alpha}(x) + ax + b$, with $h(x);\ ax + b \in \mathbb{Z}_p[x]$ be any polynomial in ring $Muff\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_{\pi} \cap \mathbb{Z}_p[x]$. From quadrature amplitude modulation $f(x)$ has degree at least $p > 2$ [1]. Now for any solution α of $f(x)$ we have $f(\alpha) = a\alpha + b = 0$ and $f(\alpha) = a\alpha + b = 0$ which gives $a\alpha = a\bar{\alpha}$. It means either $a = 0$ or $\alpha = \bar{\alpha}$. If $\alpha \notin \mathbb{Z}_p$ so $\alpha \neq \bar{\alpha}$ and then $a = 0$, hence $f(\alpha) = b = 0$, which implies $f(x) = h(x)min_{\alpha}(x)$. Thus for any arbitrary $\alpha \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_{\pi} - \mathbb{Z}_p$, the monic polynomials with minimum degree must divides any $f(x)$ over $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_{\pi}$. Further, due to isomorphism this monic polynomials with minimum degree must also divides any $f(x)$ over $\mathbb{Z}_p$. In above context it is straight forward that, for each $q_i \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_{\pi},\ o \leq i \leq n-1$, their is an monic minimal polynomial that divides any polynomial of $Muff\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_{\pi} \cap \mathbb{Z}_p[x]$ over $\mathbb{Z}_p$ and hence, least common multiple of these monic minimal polynomials also divides any polynomial of $Muff\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_{\pi} \cap \mathbb{Z}_p[x]$ over $\mathbb{Z}_p$. Again, from theorem 6, the generator polynomial for these code is $g_p(x) = (x^{p^2} - x)(x^p - x)$. Finally, for any cyclic code C associated to $Muff\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_{\pi}$ generator polynomial is the least common multiple of these monic minimal polynomials, which is the proof of the following proposition.

Proposition 12 The cyclic code $C = \left\{(q_0, q_1, q_2, \ldots\ldots, q_{n-1}) \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_{\pi}^{n} \mid f(q_i) = 0\ \forall\ q_i \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_{\pi}, 0 \leq i \leq n-1\ \&\ f(x) \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_{\pi}[x]\right\}$ with generator polynomial $g_p(x) = (x^{p^2} - x)(x^p - x)$ associated to $Muff\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_{\pi}$ is the BCH code.

Also for BCH code C with codeword $c = (q_0, q_1, q_2, \ldots\ldots, q_{n-1})$ associated to muffin ideals, we have $c(\alpha^{\mathscr{b}}) = c(\alpha^{\mathscr{b}+1}) = \cdots\ldots\ldots\ldots\ldots = c(\alpha^{\mathscr{b}+\delta_M-2}) = 0$, then the parity check matrix of this code will be

$$\mathcal{H} = \begin{bmatrix} 1 & \alpha^{\mathscr{b}} & \alpha^{2\mathscr{b}} & & \alpha^{(n-1)\mathscr{b}} \\ 1 & \alpha^{\mathscr{b}+1} & \alpha^{2(\mathscr{b}+1)} & \cdots & \alpha^{(n-1)(\mathscr{b}+1)} \\ 1 & \alpha^{\mathscr{b}+2} & \alpha^{2(\mathscr{b}+2)} & & \alpha^{(n-1)(\mathscr{b}+2)} \\ & \vdots & & \ddots & \vdots \\ 1 & \alpha^{\mathscr{b}+\delta_M-2} & \alpha^{2(\mathscr{b}+\delta_M-2)} & \cdots & \alpha^{(n-1)(\mathscr{b}+\delta_M-2)} \end{bmatrix}$$

and $\mathcal{H}c^T = 0$. Now we would like to find the length and dimensions for these codes.

Definition 9 Let n be co-prime to π (i.e. co-prime to $p = \pi\bar{\pi}$). The cyclotomic coset π modulo n containing i is the partition of elements from $\left(\frac{-1,-1}{\mathbb{z}_p}\right)_\pi$ defined as $C_i = \{(i.p^j \ mod \ n) \in \mathbb{z}_n \mid j = 0,1,2,..,\}$, where $\bigcup_{j=1}^{t} C_{i_j} = \mathbb{z}_n$.

Since cardinality of $\left(\frac{-1,-1}{\mathbb{z}_p}\right)_\pi$ with odd prime $p = \pi\bar{\pi}$ is p^2, for any primitive element $\alpha \in \left(\frac{-1,-1}{\mathbb{z}_p}\right)_\pi$ the roots of minimal polynomial of α are in $\left(\frac{-1,-1}{\mathbb{z}_{p^m}}\right)_\pi$ where smallest integer $m > 2$ called multiplicative order of p modulo n. Here n divides $p^{2m} - 1$. In particular $|C_1| = m$. So that $x^n - 1$ divides $x^{p^{2m}-1} - 1$ [14]. Hence the length of BCH code associated to muffin ideals $Muff\left(\frac{-1,-1}{\mathbb{z}_p}\right)_\pi$ over the quaternion integer ring $\left(\frac{-1,-1}{\mathbb{z}_p}\right)$ modulo π is $p^{2m} - 1$. Further, the dimension for these code obtains by the following proposition.

Proposition 13 A BCH code associated to $Muff\left(\frac{-1,-1}{\mathbb{z}_p}\right)_\pi$ of length $p^{2m} - 1$ with designed Mannheim distance δ_M has dimension at least $p^{2m} - 1 - m(\delta_M - 1)$.

Proof. Let C_i be the cyclotomic coset π modulo $p^{2m} - 1$ containing i and $\bigcup_{i=1}^{a+\delta_M-2} Ci = S$. As C is a BCH code of length $p^{2m} - 1$ and $\alpha \in \left(\frac{-1,-1}{\mathbb{z}_p}\right)_\pi$ is nth primitive root of unity, therefore its generator polynomial becomes as,

$g_p(x) = lcm\left(\prod_{i\epsilon C_{a+1}}(x - \alpha^i), \prod_{i\epsilon C_a}(x - \alpha^i), \ldots\ldots, \prod_{i\epsilon C_{a+\delta_M-2}}(x - \alpha^i)\right) = \prod_{i\epsilon C_a}(x - \alpha^i)$.

And dimension obtains is $k = p^{2m} - 1 - deg\left(g_p(x)\right) = p^{2m} - 1 - |S| = p^{2m} - 1 - \left|\bigcup_{i=1}^{a+\delta_M-2} Ci\right| \geq p^{2m} - 1 - \sum_{i=a}^{a+\delta_M-2}|Ci| \geq p^{2m} - 1 - \sum_{i=a}^{a+\delta_M-2} m = p^{2m} - 1 - m(\delta_M - 1)$ as desire.

Also as $c = (c_0, c_1, .., c_{n-1}) \ \epsilon \ C$ then $c(\alpha^{\mathscr{b}}) = c(\alpha^{\mathscr{b}+1}) = \cdots \ldots = c(\alpha^{\mathscr{b}+\delta_M-2}) = 0$, and $\mathcal{H}c^T = 0$, where $\mathcal{H}$ is parity check matrix of C defined above. If possible consider c has weight $\omega_M \leq \delta_M - 1$, it means $c_i \neq 0$ for $i \epsilon \{a_1, a_2, \ldots, a_{\omega_M}\}$. Now $\mathcal{H}c^T = 0$ implies

$$\begin{bmatrix} \alpha^{a_1\mathscr{b}} & \alpha^{a_2\mathscr{b}} & \cdots & \alpha^{a_{\omega_M}\mathscr{b}} \\ \alpha^{a_1(\mathscr{b}+1)} & \alpha^{a_2(\mathscr{b}+1)} & & \alpha^{a_{\omega_M}(\mathscr{b}+1)} \\ \vdots & & \ddots & \vdots \\ \alpha^{a_1(\mathscr{b}+\omega_M-1)} & \alpha^{a_2(\mathscr{b}+\omega_M-1)} & \cdots & \alpha^{a_{\omega_M}(\mathscr{b}+\omega_M-1)} \end{bmatrix} \begin{bmatrix} c_{a_1} \\ c_{a_2} \\ \vdots \\ c_{a_{\omega_M}} \end{bmatrix} = 0$$

But the determinant of the matrix on the left taken as

$$\alpha^{(a_1+a_2+\cdots\ldots+a_{\omega_M})\mathscr{b}}\begin{vmatrix} 1 & \ldots & 1 \\ \alpha^{a_1} & & \alpha^{a_{\omega_M}} \\ \cdots & \ddots & \cdots \\ \alpha^{a_{1(\omega_M-1)}} & \ldots & \alpha^{a_{\omega_M}(\omega_M-1)} \end{vmatrix}$$

is Vander-monde determinant and so is non-zero, which contradicts to consideration $\omega_M \leq \delta_M - 1$. Hence, in reference to the minimum Mannheim distance for C following proposition given as,

Proposition 14 A BCH code associated to $Muff\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$with designed Mannheim distance δ_M has minimum Mannheim distance $\partial_M > \delta_M$.

4.2 Decoding of BCH code over $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$

Here an algorithm for decoding and t-error correction of the narrow-sense BCH codes has given. Let C is narrow-sense BCH code ($\mathscr{b} = 1$) associated to $Muff\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ of length $p^{2m} - 1$ with designed Mannheim distance $\delta_M = 2t + 1$ and the generating polynomial $g_p(x)$. Here for any $c \in C$, $\mathcal{H}c^T = 0$ where $\mathcal{H}$ is takes as

$$\mathcal{H} = \begin{bmatrix} 1 & \alpha & (\alpha)^2 & & (\alpha)^{(n-1)} \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{(n-1)} \\ 1 & \alpha^3 & (\alpha^3)^2 & & (\alpha^3)^{(n-1)} \\ & \vdots & & \ddots & \vdots \\ 1 & \alpha^{2t} & (\alpha^{2t})^2 & \cdots & (\alpha^{2t})^{(n-1)} \end{bmatrix}$$

Consider $w(x) = w_0 + w_1x + \_\_\_ + w_{n-1}x^{n-1}$ be the received word with syndrome $S(w)$ and error polynomial $e(x)$ respectively with Mannheim distance for error polynomial $\omega_M(e(x)) \leq t$. Also let $c(x)$ is codeword given by $c(x) = w(x) - e(x)$. The syndromes of $w(x)$ are taken as $(s_0, s_1, \ldots, s_{2t-1}) = \mathcal{H}(w_0, w_1, \ldots, w_{n-1})^T$. Since $\alpha^{i+1} \in \left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$ for $i = 0, 1, \ldots, 2t-1$ are the roots of $g_p(x)$, so the syndromes are $s_i = w(\alpha^{i+1}) = e(\alpha^{i+1})$. If possible, suppose errors are take place at positions $i_0, i_1, \ldots, i_{l-1}$ with $l \leq t$, hence $e(x) = x^{i_0} + x^{i_1} + \ldots + x^{i_{l-1}}$. So we obtains the system of linear equations in form of syndromes as,

$$\alpha^{i_0} + \alpha^{i_1} + \cdots \ldots \ldots . + \alpha^{i_{l-1}} = s_0 = w(\alpha)$$
$$\left(\alpha^{i_0}\right)^2 + \left(\alpha^{i_1}\right)^2 + \cdots \ldots \ldots . + \left(\alpha^{i_{l-1}}\right)^2 = s_1 = w(\alpha^2)$$
$$\vdots$$
$$\vdots$$
$$\left(\alpha^{i_0}\right)^{2t} + \left(\alpha^{i_1}\right)^{2t} + \cdots \ldots \ldots . + \left(\alpha^{i_{l-1}}\right)^{2t} = s_{2t-1} = w(\alpha^{2t})$$

The decoder can easily calculate the s_{2t-1} as, dividing $w(x)$ by the minimal polynomial $\mathrm{M}^{i_{l-1}}(x)$ of $\alpha^{i_{l-1}}$ over $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$. That is $w(x) = q(x)\mathrm{M}^{i_{l-1}}(x) + r(x)$, where $deg\left(r(x)\right) \leq deg\left(\mathrm{M}^{i_{l-1}}(x)\right)$ over $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$. Hence $s_{2t-1} = w(\alpha^{2t}) = r(x)$ at $x = \alpha^{2t}$ [9].

Next we defines error locator polynomial as, $\sigma(z) = \prod_{j=0}^{l-1}(1 - \alpha^{i_j}z) = \sum_{i-0}^{l-1}\sigma_i z^i$, where the coefficients are the elementary symmetric functions given as $\sigma_i = (-1)^{l-1}\alpha^{i_0}\alpha^{i_1} \dots \dots \dots \alpha^{i_{l-1}}$ and so one can find the errors at positions i_{l-1} corresponding to the roots of error locator polynomial over $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$.

Example 15 [Double error-correcting codes over $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)_\pi$] Let two errors occurred at t_1 and t_2 positions with $t_1 + t_2 = \beta_1 \neq 0$ and ${t_1}^3 + {t_2}^3 = \beta_2$. So that syndrome $S = \mathcal{H}w^T = \begin{pmatrix}\beta_1 \\ \beta_2\end{pmatrix}$. Since $\beta_2 = {t_1}^3 + {t_2}^3 = (t_1 + t_2)({t_1}^2 + t_1t_2 + {t_2}^2) = \beta_1({\beta_1}^2 + t_1t_2)$, so that $ij = {\beta_2}/{\beta_1} + {\beta_1}^2$. It's obvious that t_1, t_2 are the roots of quadratic equation $x^2 + \beta_1 x + \left({\beta_2}/{\beta_1} + {\beta_1}^2\right) = 0$ with $\beta_1 \neq 0$. Using this decoding algorithm the following are the easy consequence.

$i)$ *If* $\beta_1 = \beta_2 = 0$, then no error occurred in received word.

$ii)$ *If* $\beta_1 \neq 0$, $\beta_2 = {\beta_1}^3$, then it correct a single error at location $t_1 = \beta_1$.

$iii)$ *If* $\beta_1 \neq 0$, $\beta_2 \neq {\beta_1}^3$ gives quadratic equation with two distinct roots t_1 and t_2 then it corrects errors at these locations.

CONCLUSION

Dual of cyclic codes and BCH codes with parameters length, dimension, minimum Mannheim distance constructed explicitly over the muffin ideals of Hamiltonian quaternion integer ring. This construction over such algebraic structure is purely of theoretical interest. The consequences and applications of this characterization are yet to be explored.

ACKNOWLEDGEMENT

The authors are very grateful to Director, School of Mathematical Sciences, S. R. T. M. University, Nanded and Director, S. G. G. S. I. E. & T., Nanded as they provides platform for research.

REFERENCES

1. J. S. Shaikh, A. R. Patil, Cyclic Codes Associated to Muffin Ideals over Quaternion Integer Ring $\left(\frac{-1,-1}{\mathbb{Z}_p}\right)$, *Asian Journal of Mathematics and Computer Research* 24(2): 67-74, (2018).
2. N. J. Werner, Integer-valued polynomials over quaternion rings, Ph. D. Thesis, The Ohio State University; (2010).
3. K. Huber, Codes over Gaussian integers, *IEEE Trans. Inform. Theory*. 1(40):207-216 (1994).

4. N. J. Werner, Integer-valued polynomials over quaternion rings, *Journal of Algebra.;* 324:1754{1769. (2010).
5. M. Guzeltepe, O. Heden, Perfect Mannheim, Lipchitz and Hurwitz weight codes, *Mathematical Communications*.19:253-276 (2014).
6. M. Ozen , M. Guzeltepe, Cyclic codes over some finite quaternion integer rings, *Selcuk Journal of Applied Mathematics*.;11(2):71-76 (2010).
7. C. J. Miguel, R. Serodio, On the structure of quaternion rings over $\mathbb{z}_{\boldsymbol{m}}$, *International Journal of Algebra*.; 5(27):1313-1325 (2011).
8. Taher Abualrub, Cyclic Codes And Their Duals Over $\mathbb{z}_{\boldsymbol{m}}$, *Ann. Sci. Math. Quebec* 23, no. 2, 109-118 (1999).
9. F. J. MacWilliams and N. J. A. Sloane, The Theory of Error Correcting Codes, North Holland, Amsterdam, (1977).
10. M. Ozen , M. Guzeltepe, Codes over Quaternion Integers *European Journal of Pure and Applied mathematics* Vol. 3, No. 4, 670-677 ISSN 1307-5543 (2010).
11. M. Guzeltepe, Codes over Hurwitz Integers, Elsevier, Article in Press, *Discrete Mathematics.*
12. S. Ling, C. Xing, Coding Theory-A First Course, Cambridge University Press, First Edition, (2004).
13. J. L. Massey, Shift register synthesis and BCH decoding, *IEEE Transactions on Information Theory*, vol. IT-15, pp. 122-127 (1969).
14. C.Martinez, E. Stafford, R.Beivide, E.Gabidulin, Perfect Codes over Lipchitz Integers, in: *Proc. IEEE Int. Symp. Information Theory*, Nice, 1366-1370 January (2007).
15. John Voight Quaternion algebras, jvoight@gmail.com v0.9.2 April 18, (2017).