EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 3, No. 4, 2010, 670-677
ISSN 1307-5543 – www.ejpam.com

Codes over Quaternion Integers

Mehmet Özen*, Murat Güzeltepe

Department of Mathematics, Sakarya University, TR54187 Sakarya, Turkey

Abstract. In this paper, we study codes over some finite fields by using quaternion integers. Also, we obtain the decoding procedure of these codes.

2000 Mathematics Subject Classifications: 94B05, 94B15, 94B35, 94B60

Key Words and Phrases: Block codes, Mannheim distance, Cyclic codes, Syndrome decoding

1. Introduction

In this study, we consider codes over finite fields equipped with a quaternion Mannheim metric. Mannheim distance and codes over Gaussian integers with respect to the Mannheim metric which are suitable for quadrature amplitude modulation (QAM)-type were introduced by Huber in [1, 2]. A Mannheim metric is a Manhattan metric modulo a two-dimensional (2-D) grid. Two classes of codes over Gaussian integers $\mathscr{Z}[i]$ were considered in [1], namely, the one Mannheim error-correcting (OMEC) codes, and codes having minimum Mannheim distance greater than 3. In [2], most of the proposed codes were shown to be $i-$cyclic in the sense of constacyclic codes, as defined by Berlekamp. In a similar technique, in [3], codes over Eisenstein-Jacobi integers $\mathscr{Z}[w]$ were presented together with a decoding algorithm for a proper Mannheim metric.

In Section 2, quaternion integers and quaternion Mannheim distance have been considered. Also, we present some fundamental algebraic concepts. In Section 3, we are interested in constructing perfect codes which are able to correct errors of quaternion Mannheim weight one. In Section 4, double error correcting codes which have minimum distance four or more are constructed and decoding procedure for these codes is given.

*Corresponding author.

Email addresses: ozen@sakarya.edu.tr (M. Özen), mguzeltepe@sakarya.edu.tr (M.Güzeltepe)

2. Quaternion Integers and Quaternion Mannheim Distance

Definition 1. *The Hamilton Quaternion Algebra over the set of the real numbers ($\mathscr{R}$), denoted by $H(\mathscr{R})$, is the associative unital algebra given by the following representation:*

i) $H(\mathscr{R})$ *is the free* $\mathscr{R}$ *module over the symbols* $1,i,j,k$, *that is,* $H(\mathscr{R}) = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in \mathscr{R}\}$;

ii) *1 is the multiplicative identity;*

iii) $i^2 = j^2 = k^2 = -1$;

iv) $ij = -ji = k$, $ik = -ki = j$, $jk = -kj = i$ *[4].*

The set $H(\mathscr{Z})$, which is defined by $H(\mathscr{Z}) = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in \mathscr{Z}\}$ is a subset of $H(\mathscr{R})$, where $\mathscr{Z}$ is the set of all integers. More information which is related to the arithmetic properties of $H(\mathscr{Z})$ can be found in [4, pp. 57-71,]. If $q = a_0 + a_1 i + a_2 j + a_3 k$ is a quaternion integer, its conjugate quaternion is $\overline{q} = a_0 - (a_1 i + a_2 j + a_3 k)$. The norm of q is $N(q) = q\overline{q} = a_0^2 + a_1^2 + a_2^2 + a_3^2$. A quaternion integer consists of two parts which are the real part and the imaginary part. Let $q = a_0 + a_1 i + a_2 j + a_3 k$ be a quaternion integer. Then its real part is a_0 and its imaginary part is $a_1 i + a_2 j + a_3 k$. In the rest of this paper V denotes the imaginary part of a quaternion integer. The commutative property of multiplication does not hold for quaternion integers. However, if the imaginary parts of quaternion integers are parallel to each other, then their product is commutative. Define R as follows:

$$R = \{a + bV : a, b \in \mathscr{Z}\}$$

which is a subring of the quaternion integer ring. The commutative property of multiplication holds over R. Note that the structure of the ring $R = \{a + bV : a, b \in \mathscr{Z}\}$ is related to the prime $\pi = m + nV$, where $m, n \in \mathscr{Z}$.

Theorem 1. *For every odd, rational prime p in the set of natural numbers $\mathscr{N}$, there exists a prime $\pi \in H(\mathscr{Z})$, such that $N(\pi) = p = \pi\overline{\pi}$. In particular, p is not prime in $H(\mathscr{Z})$ [4, p. 66].*

Corollary 1. *$\pi \in H(\mathscr{Z})$ is prime in $H(\mathscr{Z})$ if and only if $N(\pi)$ is prime in $\mathscr{Z}$ [4, p. 66].*

Definition 2. *Let R_π be the residue class of R modulo π, where $\pi = m+nV$ is a prime quaternion integer. Then the modulo function $\mu : R = \{a + bV : a, b \in \mathscr{Z}\} \to R_\pi$ is defined by*

$$\mu(q) = z \bmod \pi = q - [\frac{q\overline{\pi}}{\pi\overline{\pi}}]\pi, \tag{1}$$

where $z \in R_\pi$. In (1), the symbol of $[\cdot]$ is rounding to the closest integer. The rounding of a quaternion integer can be done by rounding the real part and coefficients of the imaginary part separately to the closest integer.

We can employ the extended Euclidean algorithm for the ring R to compute u and v which satisfy

$$1 = u\pi + v\overline{\pi}.$$

The Table 1 gives π, u, and v for the primes in $\mathscr{Z}$. Let π be a prime quaternion integer and let $p = \pi\overline{\pi}$. Let us define a function $f : \mathscr{Z}_p \to R_\pi$ by

$$z = f(r) = \mu(r + \pi).$$

The function f defines a bijective mapping from $\mathscr{Z}_p$ into R_π. Using the equation $1 = u\pi + v\overline{\pi}$, we get the inverse mapping f^{-1} as

$$r = f^{-1}(z) \equiv z(v\overline{\pi}) + \overline{z}(u\pi) \bmod p.$$

If r is an element of $\mathscr{Z}_p$, then $r = k\pi + z$ and $r = \overline{r} = \overline{k\pi} + \overline{z}$, hence,

$$\begin{aligned} z(v\overline{\pi}) + \overline{z}(u\pi) &= (r - k\pi)(v\overline{\pi}) + (r - \overline{k\pi})(u\pi) \\ &\equiv r(v\overline{\pi} + u\pi) \bmod p \\ &\equiv r \bmod p. \end{aligned}$$

f defines an isomorphism, namely, $f(z_1 + z_2) = f(z_1) + f(z_2)$ and $f(z_1 z_2) = f(z_1)f(z_2)$. Since the remainder from dividing the element q by the element π is $z = \mu(q)$ the norm of the element obtained by the function μ is minimum [4, p. 61].

Let us introduce the quaternion Mannheim distance. Let $\alpha, \beta \in R_\pi$ and $\gamma = \beta - \alpha = a_0 + a_1 i + a_2 j + a_3 k \pmod{\pi}$, where a proper π is a prime quaternion integer. Let the quaternion Mannheim weight of γ be defined as

$$w_{QM}(\gamma) = \left|a_0\right| + \left|a_1\right| + \left|a_2\right| + \left|a_3\right|.$$

The quaternion Mannheim distance d_{QM} between α and β is defined as

$$d_{QM}(\alpha, \beta) = w_{QM}(\gamma).$$

Indeed, d_{QM} is a metric. Let α, β and γ be any three elements of R_π. We have

i) $d_{QM}(\alpha, \beta) = w_{QM}(\delta_1)$, with $\alpha - \beta \equiv \delta_1 \pmod{\pi}, \delta_1 \in R_\pi$ and $N(\delta_1)$ minimum,

ii) $d_{QM}(\alpha, \gamma) = w_{QM}(\delta_2)$, with $\alpha - \gamma \equiv \delta_2 \pmod{\pi}, \delta_2 \in R_\pi$ and $N(\delta_2)$ minimum,

iii) $d_{QM}(\beta, \gamma) = w_{QM}(\delta_3)$, with $\gamma - \beta \equiv \delta_3 \pmod{\pi}, \delta_3 \in R_\pi$ and $N(\delta_3)$ minimum. Thus, $\alpha - \beta \equiv \delta_2 + \delta_3 \pmod{\pi}$. Notwithstanding, $N(\delta_2 + \delta_3) \geq N(\delta_1)$, because $\alpha - \beta \equiv \delta_1 \pmod{\pi}$ and $N(\delta_1)$ is minimum. Therefore, $d_{QM}(\alpha, \beta) \leq d_{QM}(\alpha, \gamma) + d_{QM}(\gamma, \beta)$. Other metric conditions are clear.

3. One Quaternion Mannheim Error Correcting Codes

Let α be a primitive element of R_π and let p be a prime in $\mathscr{Z}$, where $\pi = a_0+a_1i+a_2j+a_3k$ is a quaternion prime number and $p = \pi\bar{\pi}$. Then, $\alpha^{p-1} = 1$ and the parity check matrix H and the generator matrix G by using the primitive element α are obtained as follows, respectively;

$$H = \begin{pmatrix} \alpha^0 & \alpha^1 & \cdots & \alpha^{(p-1)/2-1} \end{pmatrix}, G = \begin{pmatrix} -\alpha^1 & 1 & 0 & \cdots & 0 \\ -\alpha^2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ -\alpha^{(p-1)/2-1} & 0 & 0 & & 1 \end{pmatrix}.$$

Hence, the one quaternion Mannheim error correcting codes of length $n = (p-1)/2$ can be constructed by the parity check matrix H. Then the code C defined by the above parity check matrix H is able to correct any quaternion Mannheim error of weight one. The value of one quaternion Mannheim error is 1 or -1. The decoding algorithm for these codes is clear. Let the received vector be $r = c+e$, where the weight of the error vector e is 1 and the vector c is a codeword. Then the syndrome of the received vector r is computed by $S(r) = Hr^{tr}$, where r^{tr} denote the transpose of the received vector r. The value of the error is computed by $S\alpha^{-l}$, where $l \pmod n$ helps to find the location of the error, l is a nonnegative integer, and n is equal to $(p-1)/2$.
We now consider a basic example with regard to the one quaternion Mannheim error correcting codes.

Example 1. *Let $\pi = 2+i+j+k$ and $\alpha = 1-i-j-k$. Then, we obtain the parity check matrix H and the generator matrix G by using the primitive element α of R_π as follows, respectively;*

$$H = \begin{pmatrix} \alpha^0, & \alpha^1, & \cdots, & \alpha^{(p-1)/2-1} \end{pmatrix}, G = \begin{pmatrix} -\alpha^1, & 1, & 0, & \cdots, & 0 \\ -\alpha^2, & 0, & 1, & \cdots, & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ -\alpha^{(p-1)/2-1}, & 0, & 0, & & 1 \end{pmatrix}.$$

Let the received vector r be $\begin{pmatrix} 1-i-j-k, & 0, & -1+i+j+k \end{pmatrix}$, then $S(r) = Hr^{tr} = 4 \equiv -1+i+j+k \equiv \alpha^4 (mod\, \pi)$ (See Table 2), and the location of the error is found $4 \equiv 1 (\mathrm{mod} 3)$. The value of the error is computed as $S\alpha^{-l} = -1$. So, the received vector r is corrected as $c = r-e = \begin{pmatrix} 1-i-j-k, & 1, & -1+i+j+k \end{pmatrix}$.

The code, of which the parity check matrix is $H = \begin{pmatrix} \alpha^0, & \alpha^1, & \cdots, & \alpha^{(p-1)/2-1} \end{pmatrix}$ can be generalized as $n = (p^r-1)/2$. In this situation, the parity check matrix would be

$$H = \begin{pmatrix} \alpha^0, & \alpha^1, & \cdots, & \alpha^{(p^r-1)/2-1} \end{pmatrix}. \tag{2}$$

The codes defined by (2) are perfect since we have $p^{n-r}(2n+1) = p^{n-r}p^r = p^n$ by the sphere packing bound.

4. Double Error Correcting Codes

Let p be a prime in $\mathscr{Z}$ which is factored in $H(\mathscr{Z})$ as $\pi\overline{\pi}$, where π is a prime in $H(\mathscr{Z})$. Let β denote an element of R_π of order $2n$. Thus $\beta^n = -1$, and we can write $R_\pi = \langle\beta\rangle \cup \{0\}$ since β is a primitive element of R_π, where $\langle.\rangle$ denotes an ideal. Therefore, we consider the code C defined by the following parity check matrix H:

$$H = \begin{pmatrix} \beta^0, & \beta^1, & \beta^2, & \cdots, & \beta^{n-1} \\ \beta^0, & \beta^3, & \beta^6, & \cdots, & \beta^{3(n-1)} \\ \vdots & & & & \\ \beta^0, & \beta^{2t+1}, & \beta^{2(2t+1)}, & \cdots, & \beta^{(n-1)(2t+1)} \end{pmatrix}, \tag{3}$$

where $t < n$ is a nonnegative integer. A word $c = \begin{pmatrix} c_0, & c_1, & \cdots, & c_{n-1} \end{pmatrix} \in R_\pi^n$ is a codeword of C if and only if $Hc^{tr} = 0$. If $c(x) = \sum_{i=0}^{n-1} c_i x^i$ is a codeword polynomial, we get

$$c(\beta^{2j+1}) = 0, \text{ for } j = 0, 1, \cdots, t.$$

The polynomial $g(x) = (x-\beta)(x-\beta^3)\cdots(x-\beta^{2t+1})$ is the generator polynomial of C, and $C = \langle g(x)\rangle$ is a principal ideal of $R_\pi[x]/\langle x^n+1\rangle$. If we multiply the code polynomial $c(x)$ by $x(mod(x^n+1))$, then we get

$$xc(x) = c_0 x + c_1 x^2 + \cdots + c_{n-1}x^n.$$

But we know that $x^n = -1$. Therefore, if $c(x) \in C$, then $xc(x) \in C$. Thus, multiplying $c(x)$ by $x \pmod{(x^n+1)}$ means the following:

i) Shifting $c(x)$ cyclically one position to the right;

ii) Rotating the coefficient c_{n-1} by π radians and locating it for the first symbol of the new codeword.

Theorem 2. *Let C be the code defined by the parity check matrix as in (3). Then C is able to correct any error pattern of the form $e(x) = e_i x^i + e_j x^j$, where $0 \le w_{QM}(e_i), w_{QM}(e_j) \le 1$.*

Proof. Suppose that double error occurs at two different components l_1, l_2 of the received vector r . Let the error vectors be e_1, e_2, where $0 \le w_{QM}(e_1), w_{QM}(e_2) \le 1$, respectively. First we compute the syndrome S of r:

$$S(r) = Hr^{tr} = \begin{pmatrix} s_1 \\ s_3 \end{pmatrix}. \tag{4}$$

The polynomial $\sigma(z)$, which helps us to find the errors location and the value of the errors, is computed as follows.

$$\sigma(z) = (z-\beta^{l_1})(z-\beta^{l_2}) = z^2 - (\beta^{l_1}+\beta^{l_2})z + \beta^{l_1}.\beta^{l_2} = z^2 - (s_1)z + \varepsilon, \tag{5}$$

where ε is determined from the syndromes. From $s_1 = \beta^{l_1} + \beta^{l_2}, s_3 = \beta^{3l_1} + \beta^{3l_2}$ and $\varepsilon = \beta^{l_1+l_2}$ we get

$$s_1^3 - s_3 = 3\varepsilon\beta^{l_1} + 3\varepsilon\beta^{l_2} + \beta^{3l_2} + \beta^{3l_1} - (\beta^{3l_2} + \beta^{3l_1}) = 3\varepsilon(\beta^{l_1} + \beta^{l_2}) \tag{6}$$

from which we obtain

$$\frac{s_1^3 - s_3}{3s_1} = \frac{3\varepsilon(\beta^{l_1} + \beta^{l_2})}{3(\beta^{l_1} + \beta^{l_2})} = \varepsilon \,(\mathrm{mod}\pi). \tag{7}$$

Thus, the roots of the polynomial $\sigma(z)$ lead us to find the locations of the errors and their values. If $\beta_1^{l_1}$ and $\beta_2^{l_2}$ are the roots of the polynomial $\sigma(z)$, then l_1 and l_2 $(mod\ n)$ are locations of the errors. Thus, we can distinguish three situations: no error, single error, and two errors.

i) No error: $s_1 = s_3 = 0$,

18tem[ii)] One error: $s_1^3 = s_3 \neq 0$,

iii) Two errors: $s_1^3 \neq s_3$ and $s_1 \neq 0$.

We illustrate the decoding procedure with the following example.

Example 2. *Let $\pi = 1 + 2i + 2j + 2k$ and let $\beta = 2$. Let C be the code defined by the parity check matrix*

$$H = \begin{pmatrix} 1, & 2, & -2+i+j+k, & 1-i-j-k, & 3, & i+j+k \\ 1, & 1-i-j-k, & -1, & -1+i+j+k, & 1, & 1-i-j-k \end{pmatrix}.$$

Suppose that the received vector is $r = \begin{pmatrix} 3, & 3, & 1, & 0, & -1, & 1 \end{pmatrix}$. We now apply the decoding procedure for the code in Theorem 2.

1) Calculating the syndrome:

$$S = Hr^{tr} = \begin{pmatrix} s_1 \\ s_3 \end{pmatrix} = \begin{pmatrix} 3 \\ -i-j-k \end{pmatrix} \bmod \pi.$$

One can verify that $s_3 \neq s_1^3$, which shows that two errors have occurred.

2) Calculating the Error Locations and the Value of Errors: Using the formulas (6) and (7), we obtain $\varepsilon \equiv 1-i-j-k \,(\mathrm{mod}\ \pi)$ and the roots of the polynomial $\sigma(z)$ are β^5, β^{10} (See Table 3). Therefore, the locations of the errors are

$l_1 = 5 \equiv 5 \,(\mathrm{mod}\ 6)$ and its value is $(\beta^5 / \beta^5) = 1$ and $l_2 = 10 \equiv 4 \,(\mathrm{mod}\ 6)$ and its value is $(\beta^{10} / \beta^4) = -1$. Thus, one error has occurred in location 6 and its value is 1, and another one in location 5 and its value is -1.

Theorem 3. *The code defined by the parity check matrix (3) has the minimum distance $d_{QM} \geq 4$ if π is a prime in $H(\mathscr{Z})$ and p is a prime in $\mathscr{Z}$, where $p \geq 13$, $p = \pi\overline{\pi}$, and t=1.*

Proof. It is sufficient to show that the decoder can distinguish single and double errors for the proof. Suppose that an error of the quaternion Mannheim weight one did occur. Then $s_1^3 = s_3 \neq 0 \,(\mathrm{mod}\,\pi)$. From Eq. (5), we get

$$z_{1,2} = \frac{s_1 \pm \sqrt{\frac{s_3}{s_1}}}{2} = \frac{s_1 \pm s_1}{2}.$$

In view of Theorem 2, the decoder can distinguish between single and double errors.

5. Conclusion

In this paper, codes over the subring R of the quaternion integer ring $H(\mathscr{Z})$ are constructed and decoding algorithms of these codes are given. Moreover, it is seen that all of the one quaternion Mannheim error correcting codes are perfect. Furthermore, these codes are constructed using a metric which is called quaternion Mannheim metric.

ACKNOWLEDGEMENTS The authors would like to thank the anonymous referees for their helpful comments and suggestions.

References

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

[2] E R Berlekamp. Algebraic Coding Theory, Laguna Hills, CA: Aegan Park, 1984.

[3] K Huber. Codes over Eisenstein-Jacobi integers, AMS. Contemp. Math., vol. 158, pp. 165-179, 1994.

[4] G Davidoff. P Sarnak. and A Valette. Elementary Number Theory, Group Theory, and Ramanujan Graphs, Cambridge University Pres, 2003.

Appendix

Table 1: Table of p, π, a primitive element $\alpha \in R_\pi$, u and v (where $1 = u\pi + v\overline{\pi}$), for $p < 23$.

p	π	α	u	v
7	$2+i+j+k$	$1-i-j-k$	$i+j+k$	2
11	$3+i+j$	$-1-i-j$	$-1+i+j$	2
13	$1+2i+2j+2k$	2	$i+j+k$	$1+i+j+k$
17	$3+2i+2j$	$i+j$	-31	$2+22i+22j$
19	$4+i+j+k$	2	$3i+3j+3k$	$4-2i-2j-2k$

Table 2: Powers of the element $\alpha = 1-i-j-k$ which is a root of x^3+1.

s	α^s	s	α^s
0	1	4	$-1+i+j+k$
1	$1-i-j-k$	5	$i+j+k$
2	$-i-j-k$	6	1
3	-1	7	$1-i-j-k$

Table 3: Powers of the element $\beta = 2$ which is a root of x^6+1.

s	β^s	s	β^s
0	1	8	$2-i-j-k$
1	2	9	$-1+i+j+k$
2	$-2+i+j+k$	10	-3
3	$1-i-j-k$	11	$-i-j-k$
4	3	12	1
5	$i+j+k$	13	2
6	-1	14	$-2+i+j+k$
7	-2	15	$1-i-j-k$