Computers, Materials & Continua
DOI: 10.32604/cmc.2022.025245
Article

Tech Science Press

Quaternion Integers Based Higher Length Cyclic Codes and Their Decoding Algorithm

Muhammad Sajjad[1], Tariq Shah[1,*], Mohammad Mazyad Hazzazi[2], Adel R. Alharbi[3] and Iqtadar Hussain[4]

[1]Department of Mathematics, Quaid-I-Azam University, Islamabad, 45320, Pakistan
[2]Department of Mathematics, College of Science, King Khalid University, Abha, 61413, Saudi Arabia
[3]College of Computing and Information Technology, University of Tabuk, Tabuk, 71491, Saudi Arabia
[4]Department of Mathematics, Statistics and Physics, Qatar University, Doha, 2713, Qatar
*Corresponding Author: Tariq Shah. Email: stariqshah@gmail.com
Received: 17 November 2021; Accepted: 15 February 2022

Abstract: The decoding algorithm for the correction of errors of arbitrary Mannheim weight has discussed for Lattice constellations and codes from quadratic number fields. Following these lines, the decoding algorithms for the correction of errors of $n = \frac{p-1}{2}$ length cyclic codes (C) over quaternion integers of Quaternion Mannheim (QM) weight one up to two coordinates have considered. In continuation, the case of cyclic codes of lengths $n = \frac{p-1}{2}$ and $2n - 1 = p - 2$ has studied to improve the error correction efficiency. In this study, we present the decoding of cyclic codes of length $n = \varphi(p) = p - 1$ and length $2n - 1 = 2\varphi(p) - 1 = 2p - 3$ (where p is prime integer and φ is Euler phi function) over Hamilton Quaternion integers of Quaternion Mannheim weight for the correction of errors. Furthermore, the error correction capability and code rate tradeoff of these codes are also discussed. Thus, an increase in the length of the cyclic code is achieved along with its better code rate and an adequate error correction capability.

Keywords: Mannheim distance; monoid ring; cyclic codes; parity check matrix extension; syndromes decoding; code rate and error correction capability

1 Introduction

The study of the features of codes and their suitability for various applications is known as coding theory. Data compression, error detection and correction, security, data storage, and data transmission are all performed by codes. Code words are used in some digital communication systems for error correction or detection. Because of this, all code words in a message may have the same pattern of digits. As a result, the message becomes more redundant. As part of the message identification, each code word (without the first) in the message would have a code syndrome. The cyclic code does not utilize these syndromes for error correction. When a message's code words have been switched in specific sections of the system, simple decoding methods may reveal this. To decide which syndromes are appropriate, random and burst error correction codes are analyzed and compared to one another.

A perfect code is defined as one that achieves a bound (the sphere-packing bound) in a given metric. Perfect codes have long piqued the interest of coding theorists and mathematicians, since they play an essential theoretical and practical role in coding theory. Over finite fields, several perfect codes with regard to the Hamming metric are known, [1–5]. In the perspective of Hamming distance, the single error correction of cyclic codes (C) over the ring $\mathbb{Z}_m$ of integers modulo m are defined by Han et al. [6]. Then, Tamm et al. [7] established that integer's cyclic codes for general construction are perfect, and these codes are used for single error correction.

Though, in [8] Huber investigated that cyclic codes over Gaussian integers for two-dimensional signal space are perfect for one Mannheim error, and he further shaded light on the difference in Hamming and Mannheim distances. On the other hand, in [9] Huber substantiated the Mac William's theorem for the codes having symbols from a finite field with a two-dimensional modulo metric. Neto et al. [10] spoke the cyclic codes over Gaussian integers $\mathbb{Z}[i]$ for Mannheim weight one and two, besides he has given a comparison of these cyclic codes with the cyclic codes having symbols from the ring $\mathbb{Z}[w]$ of algebraic integers. Nevertheless, Kostadinov [11] derived the bit error probability of the transmitted code word of an integer cyclic code using quadrature amplitude modulation (QAM). For two-dimensional signal patterns like QAM, Severe coding difficulties arise from the algebraic theory of block-cyclic codes over finite fields.

The cyclic, Bose Chaudhuri Hocquenghem (BCH), Srivastava, alternant, and Goppa codes having symbols from a unitary finite commutative ring R, are described by Andrade et al. in [12]. Accordingly, for this purpose, they used the factor ring of polynomial ring $R[x]$ in one indeterminate x. Özen et al. [13] has introduced Quaternion Mannheim (QM) distance as a metric and give a decoding procedure of Cyclic codes of length $n = \frac{p-1}{2}$ over Quaternion integers. Andrade et al. [14,15] has given the modified Berlekamp-Massey decoding algorithm for cyclic, BCH, Goppa, alternan and Srivastava codes designed by the monoid ring $R[x, \frac{1}{2}\mathbb{Z}_0]$ analogue to the codes obtained by polynomial ring $R[x]$. In continuation, Shah et al. [16,17] in the place of a polynomial ring, the construction of cyclic, BCH, Goppa, alternan and Srivastava codes over a finite ring are realized by the monoid ring.

Özen et al. in [18] further contributed some results on the construction of cyclic codes over some finite Quaternion integer rings with respect to the QM distance. However, Güzeltepe et al. [19] has discussed Gaussian, Lipschitz, and Hurwitz weight codes for error correction and revealed that these codes are perfect. A comparison of the code rate, bandwidth, and average energy is also part of the study of [19]. Following the cyclic code's design through monoid ring as described in [14–19] have introduced the decoding of C over Quaternion integers of length $n = \frac{p-1}{2}$ for QM weight two. Moreover, they also discussed the corresponding $2n - 1 = p - 2$ length cyclic codes of the $n = \frac{p-1}{2}$ length cyclic codes for QM weight one and two.

The goal of this work is to demonstrate a decoding procedure for cyclic codes of length $n = \varphi(p) = p-1$ with QM weight one and two by following the lines drawn in [13,20]. In addition, followed monoid ring technique given in [20] for the designing of cyclic codes, the decoding procedure of the cyclic codes of length $2n - 1 = 2\varphi(p) - 1 = 2p - 3$ with QM weight one and two is obtained. Thus, a gain in the increase code rate of cyclic codes due to prime p, is achieved.

The rest of the paper is laid out as follows: Related work is discussed in Section 2. In Section 3, single and double error-correcting cyclic codes of length $n = \varphi(p) = p - 1$ for QM weight one and two by following techniques in [10,20]. In Section 4, the parity check matrix (H) of the cyclic code of length $n = \varphi(p) = p - 1$ is extended to parity check matrix (H) of the cyclic code of length $2n - 1 = 2\varphi(p) - 1 = 2p - 3$. Consequently, single and double error-correcting cyclic codes of length $2n - 1 = 2\varphi(p) - 1$ for QM weight one and two through monoid rings by following techniques in [20]

is obtained. In Section 5, code length and code rates comparison of the cyclic codes for different odd primes. Finally, Section 6, concluded the findings of the study and future directions respectively.

2 Preliminaries

This section provides the key concepts and basic findings that will be used in the study of upcoming sections. First of all, we recall definition of Quaternion integers, QM weight, QM distance and some related results.

2.1 Hamilton Quaternion Integers

By following [21], the Hamilton Quaternion algebra over the set of the real number $\mathbb{R}$, indicate by $H(\mathbb{R})$, is the associative unital algebra by the following conditions.

1. $H(\mathbb{R}) = \{b_0 + b_1 i + b_2 j + b_3 k : b_0, b_1, b_2, b_3 \in \mathbb{R}\}$ is free $\mathbb{R}$ module.
2. Multiplicative identity is 1.
3. $i^2 = j^2 = k^2 = -1$ *and* $jk = -kj = i, ki = -ik = j, ij = -ji = k$.

The Quaternion integer ring $H(\mathbb{Z}) = \{b_0 + b_1 i + b_2 j + b_3 k : b_0, b_1, b_2, b_3 \in \mathbb{Z}\}$ is contain in $H(\mathbb{R})$, where $\mathbb{Z}$ is the ring of integers. If $q = b_0 + b_1 i + b_2 j + b_3 k$ is a Quaternion integer, then $\overline{q} = b_0 - b_1 i - b_2 j - b_3 k$ is the Quaternion conjugate of q. $N(q) = q\overline{q} = b_0^2 + b_1^2 + b_2^2 + b_3^2$ is the norm of q. A Quaternion integer q having only two parts one is scalar part b_0 and other is vector part $b_1 i + b_2 j + b_3 k$. In Quaternion integer's commutative property of multiplication is not hold. It is possible only in case of two vector part of quaternion integers are parallel.

Define $H(K)$ as: $H(K) = \{c + dV : c, d \in \mathbb{Z}\}$, Where V indicates $(i + j + k)$. $H(K)$ is a subring of the Quaternion integer ring $H(\mathbb{Z})$, then the commutative property of multiplication holds over $H(K)$.

Theorem: In [21], the set of natural numbers for each odd rational prime p, there is a prime $\pi \in H(\mathbb{Z})$, such that $N(\pi) = p = \pi\overline{\pi}$. In particular, p is not prime in $H(\mathbb{Z})$.

Corollary: In [18], $\pi \in H(\mathbb{Z})$ is prime in $H(\mathbb{Z})$ if and only if $N(\pi)$ is prime in $\mathbb{Z}$.

Definition: In [18], let residue class of $H(K)_\pi$ is $H(K)$ modulo π, $\pi = a + bV$. Then, the modulo function

$\omega : H(K) = \{c + dV : c, d \in \mathbb{Z}\} \to H(K)_\pi$

define as $\omega(q) = z \; mod \; \pi = q - \left[\frac{q\overline{\pi}}{\pi\overline{\pi}}\right]\pi\overline{\pi}.$

where $z \in H(K)_\pi$. In the above expression, the number of [.] is rounding to the nearest integer. Quaternion integer rounding should be possible by rounding the coefficients of vector part and scalar part independently to the nearest integer.

Definition: Let $\beta, \rho \in H(K)_\pi$ and $\alpha = \beta - \rho = (b_0 + b_1 i + b_2 j + b_3 k)\,(mod\ \pi)$. The QM weight of γ be characterized as $W_{QM}(\alpha) = |b_0| + |b_1| + |b_2| + |b_3|$

and Quaternion Mannheim distance $d_{QM}(\alpha)$ between β and ρ is defined as $W_{QM}(\alpha) = d_{QM}(\rho, \beta)$

Remark: Indeed, Quaternion Mannheim weight W_{QM} is a metric.

2.2 Construction of Cyclic Codes

Construction of cyclic codes of length $n = \varphi(p) = p - 1$ by following the techniques of [10]. Let ξ is the primitive element of $H(K)_\pi$, p be a prime in $\mathbb{Z}$, where $\pi = b_0 + b_1 i + b_2 j + b_3 k$, $p = \pi\overline{\pi}$ and $\xi^{p-1} = 1$. Then cyclic code (C) defined by H as follows;

$$H = \begin{pmatrix} \xi^0 & \xi^1 \cdots & \xi^{\varphi(p)-1} \\ \vdots & \ddots & \vdots \\ \xi^0 & \xi^{t+1} \cdots & \xi^{(t+1)(\varphi(p)-1)} \end{pmatrix} \tag{1}$$

where t is nonnegative integer less than n. A vector $c = (c_0, c_1, \ldots;, c_{\varphi(p)-1}) \in H(K)_\pi^n$ is a codeword of C if and only if $Hc^{tr} = 0$. If $c(z) = \sum_{j=0}^{n-1} c_j z^j$ is a codeword polynomial, then $c(\xi^{i+1}) = 0, for\ i = 0, 1, 2, \cdots, t$. The polynomial $f(z) = (z - \xi)(z - \xi^2) \cdots (z - \xi^{t+1})$ is the generator polynomial of cyclic code C, and $C = \langle f(z) \rangle$ is a principle ideal of $H(K)_\pi[z]/\langle z^n - 1 \rangle$. If we multiple $c(z)$ by $z(mod(z^n - 1))$, then $zc(z) = c_0 z + c_1 z^2 + \cdots + c_{n-1} z^n$. But we know that $z^n = 1$. Therefore, if $c(z) \in C$, then $zc(z) \in C$. Thus, multiply $c(z)$ by $z(mod(z^n + 1))$ means the following:

1. For Cyclic Shift $c(z)$ shift one place to the right.
2. Locating the initial symbol of the new codeword by rotating the coefficient c_{n-1} by π radians.

3 Error Correction of Cyclic Codes of Length $n = \varphi(p)$ for QM Weights One and Two

This section consists of decoding method for C of length $n = \varphi(p)$ that uses the techniques in [[13], Section 3, and Section 4] and [[17], Section 3, Theorem 2, Lemma 1 and Theorem 3] to rectify single and double errors of QM weight one and two.

3.1 Single Error Correcting Cyclic Codes of QM Weight One

Let ξ is the primitive element of $H(K)_\pi$, $\pi = b_0 + b_1 i + b_2 j + b_3 k$, $p = \pi\overline{\pi}$ and $\xi^{p-1} = 1$ Then,

$$H = \begin{pmatrix} \xi^0 & \xi^1 & \xi^2 & \cdots & \xi^{\varphi(p)-1} \end{pmatrix} \tag{2}$$

$$G = \begin{pmatrix} -\xi^1 & 1 & 0 \cdots & 0 \\ \vdots & & \ddots & \vdots \\ -\xi^{\varphi(p)-1} & 0 & 0 \cdots & 1 \end{pmatrix} \tag{3}$$

The one QM error-correcting codes of length $n = \varphi(p)$ can be constructed by H. Then C defined by H in Eq. (2) is able to correct any QM error of weight one. The possible error values are 1 or -1. For the decoding procedure first step is to find the syndrome $S(r) = Hr^{tr}$ with the help of H and the received vector r. Then the error value is computed by $S\xi^{-l}$, where $l(mod\ n = \varphi(p))$ is a non-negative integer which is helpful for error location. Hence, $c = r - e$ is the corrected codeword.

Illustration: Let $\pi = 4 + i + j + k$, $p = 19$, $n = \varphi(p) = 18$ and $\xi = 2$. Then, H and G by using Eqs. (2) and (3) and ξ be the primitive element of $H(K)_\pi$, see Tab. 1 respectively;

$$H = \begin{pmatrix} \xi^0 & \xi^1 & \xi^2 & \cdots & \xi^{17} \end{pmatrix}; G = \begin{pmatrix} -\xi^1 & 1 & 0 \cdots & 0 \\ \vdots & & \ddots & \vdots \\ -\xi^{17} & 0 & 0 \cdots & 1 \end{pmatrix};$$

$$r = (1 - i - j - k, 1, -1 + i + j + k, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1)_{1\times 18}$$

$$S(r) = Hr^{tr} = i + j + k \equiv \xi^{11}(mod\pi)$$

Table 1: $\xi = 2$ is the root of $z^9 + 1$

ξ^l	*Value*	ξ^l	*Value*	ξ^l	*Value*
ξ^0	1	ξ^6	$3i + 3j + 3k$	ξ^{12}	$2i + 2j + 2k$
ξ^1	2	ξ^7	$-1 + i + j + k$	ξ^{13}	3
ξ^2	$-i - j - k$	ξ^8	$-2 + 2i + 2j + 2k$	ξ^{14}	$2 - i - j - k$
ξ^3	$-2i - 2j - 2k$	ξ^9	-1	ξ^{15}	$-3i - 3j - 3k$
ξ^4	-3	ξ^{10}	-2	ξ^{16}	$1 - i - j - k$
ξ^5	$-2 + i + j + k$	ξ^{11}	$i + j + k$	ξ^{17}	$2 - 2i - 2j - 2k$

$11 \equiv 11(mod\ 18)$, it means error occur in received vector at location 12. Hence error value is $S\xi^{-11} = 1(mod\ \pi)$. $c = (1 - i - j - k, 1, -1 + i + j + k, 0, 0, 0, 0, 0, 0, 0, 0, -1, 0, 0, 0, 0, 0, -1)$.

$Hc^{tr} = O(mod\ \pi)$. Hence, c is a codeword of C.

Perfect codes of Length $n = \varphi(p)$ for QM Weight One:

The cyclic codes defined by H of length $n = \varphi(p) = p - 1$ in Eq. (2), can be generalized as

$$H = \begin{pmatrix} \xi^0 & \xi^1 & \xi^2 & \cdots & \xi^{\varphi(p^r)-1} \end{pmatrix} \tag{4}$$

The cyclic codes defined by the generalized H are perfect in Eq. (4), by the sphere packing bound, since we have $p^{n-r}(n+2) = p^{n-r}p^r = p^n$.

3.2 Double Error Correcting Cyclic Codes of QM Weight One

Theorem: Let cyclic code (C) defined by H in Eq. (1). Then cyclic code (C) can be correct error as the form $e(x) = e_j x^j + e_i x^i$, where $0 \le W_{QM}(e_j), W_{QM}(e_i) \le 1$.

Proof: Consider two errors occur at two different places l_1, l_2 in received r and two error vectors e_1, e_2 of QM weight $0 \le w_{QM}(e_1), W_{QM}(e_2) \le 1$. First, find syndromes with the help of H and the transpose of received vector r as;

$$H = \begin{pmatrix} \xi^0 & \xi^1 & \xi^2 & \cdots & \xi^{\varphi(p)-1} \\ \xi^0 & \xi^2 & \xi^4 & \cdots & \xi^{2\varphi(p)-2} \end{pmatrix} \tag{5}$$

$$S(r) = Hr^{tr} = \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} (mod\pi) \tag{6}$$

Now we find a polynomial $h(x)$ for the location and correction of errors as follows:

$$h(x) = (x - \xi^{l_1})(x - \xi^{l_2}) = x^2 - (\xi^{l_1} + \xi^{l_2})x + \xi^{l_1}.\xi^{l_2} = x^2 - s_1 x + \eta \tag{7}$$

Where we can get η by syndromes. From $s_1 = \xi^{l_1} + \xi^{l_2}, s_2 = \xi^{2l_1} + \xi^{2l_2}$ and $\eta = \xi^{l_1}\xi^{l_2}$. we get

$$s_1^2 - s_2 = (\xi_2^{l_1} + \xi^{l_2})^2 - (\xi^{2l_1} + \xi^{2l_2}) = 2\xi^{l_1}\xi^{l_2} = 2\eta \tag{8}$$

$$\frac{s_1^2 - s_2}{2} = \frac{2\eta}{2} = \eta\,(mod\pi) \tag{9}$$

Thus, $h(x)$ helps for the locations and error values. If $\xi_1^{l_1}$ and $\xi_2^{l_2}$ are roots of $h(x)$, then $l_1(modn) = m_1$, $l_2(modn) = m_2$ are locations of error and error values are $e_1 = \frac{\xi^{l_1}}{m_1}$, $e_2 = \frac{\xi^{l_2}}{m_2}$ which having three possibilities. If both two syndrome s_1 and s_2 are zeros then no error occurs. If $s_1^2 = s_2 \neq 0$, then one error occurs. If $s_1^2 \neq s_2$ and $s_1 \neq 0$, then two error occurs.

Illustration: Let $\pi = 4 + i + j + k$, $p = 19$, $n = \varphi(p) = 18$ and $\xi = 2$. Then, H by using Eq. (5) and elements see Tab. 1 respectively; $H = \begin{pmatrix} \xi^0 & \xi^1 & \xi^2 & \cdots & \xi^{17} \\ \xi^0 & \xi^2 & \xi^4 & \cdots & \xi^{34} \end{pmatrix}$,

$r = (1 - i - j - k, 1, -1 + i + j + k, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1)_{1\times 18}$

$S(r) = Hr^{tr} = \begin{pmatrix} i+j+k \\ 2 - 2i - 2j - 2k \end{pmatrix} = \begin{pmatrix} \xi^{11} \\ \xi^{17} \end{pmatrix} (mod\ \pi) = \begin{pmatrix} s_1 \\ s_2 \end{pmatrix}$, Both syndromes s_1, s_2 are non-zeros and $s_1^2 \neq s_2 \neq 0$. Hence two error occurs. By Eq. (9), $\eta = \frac{s_1^2 - s_2}{2} = \xi^{13}(mod\ \pi)$. Hence error polynomial by Eq. (7) is $h(x) = x^2 - \xi^{11}x + \xi^{13}$. Error locator polynomial roots $h(x)$ are $\xi^{l_1} = \xi^4$ and $\xi^{l_2} = \xi^9$, so, error locations are 4 and 9 in received vector r. Hence, error values are $e^{l_1} = 1$ and $e^{l_2} = 1$. $c = (1 - i - j - k, 1, -1 + i + j + k, 0, -1, 0, 0, 0, 0, -1, 0, 0, 0, 0, 0, 0, 0, -1)_{1\times 18}$.

$Hc^{tr} = O(\bmod \pi)$. Hence, c is a codeword of C.

Theorem: The cyclic code C defined by H in Eq. (1) has the minimum QM distance $d_{QM} \geq 4$. If p be a prime in $\mathbb{Z}$ then π be a prime in $H(\mathbb{Z})$, where $p = \pi\overline{\pi} \geq 19$ and $t = 1$.

Proof: The decoder's ability to distinguish between single and double errors is all that is required in this proof. Assume QM weight error is one. Then, $s_1^2 = s_2 \neq 0(mod\pi)$. From Eq. (7),

$$x_{1,2} = \frac{s_1 \pm \sqrt{\frac{s_2}{s_1}}}{2} = \frac{s_1 \pm s_1}{2} \tag{10}$$

Hence, the decoder can differentiate in single and double errors.

3.3 Single Error Correcting Cyclic Codes of QM Weight Two

Theorem: Let ξ is the primitive element of $H(K)_\pi$, $\pi = b_0 + b_1 i + b_2 j + b_3 k$ and $p = \pi\overline{\pi}$. Let a cyclic code C of length $n = \varphi(p) = p - 1$ define by H.

$$H = \begin{pmatrix} \xi^0 & \xi^1 & \xi^2 & \cdots & \xi^{\varphi(p)-1} \\ \xi^0 & \xi^2 & \xi^4 & \cdots & \xi^{2\varphi(p)-2} \end{pmatrix} \tag{11}$$

then the error of code C can be correct as of the form $e(x) = e_l x^l$, where $1 \leq w_{QM}(e_l) \leq 2$.

Proof: *Let ξ^i is error which occurred in location j, where $0 \leq i \leq n-1$ and $0 \leq j \leq n-1$. Let $e(x) = \xi^i x^j$ be the error structure. Then, $s_1 = \xi^{j+i}$ and $s_2 = \xi^{2j+i}$ are syndromes. Let $s_1 = \xi^{l_1}$ and $s_2 = \xi^{l_2}$ are the basis of $s_j; j = 1, 2$.*

$$\begin{cases} s_1 & = \xi^{j+i}, \Longrightarrow j + i \equiv l_1(modp - 1) \\ s_2 & = \xi^{2j+i}, \Longrightarrow 2j + i \equiv l_2(modp - 1) \end{cases} \tag{12}$$

Eq. (11) having unique solution at $j = l_2 - l_1 \pmod{p-1}$, $i = l_1 - j \pmod{p-1}$. Hence we conclude that error is occurred in location $(l_2 - l_1)(\bmod n)$ with magnitude ξ^i.

Illustration: Let $\pi = 4 + i + j + k$, $p = 19$, $n = \varphi(p) = 18$ and $\xi = 2$. Then, we have H by using Eq. (11) and elements of Tab. 1 respectively; $H = \begin{pmatrix} \xi^0 & \xi^1 & \xi^2 & \cdots & \xi^{17} \\ \xi^0 & \xi^2 & \xi^4 & \cdots & \xi^{34} \end{pmatrix}_{(2\times 18)}$,

$r = (1, -1, -1 + i + j + k, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1)_{1\times 18}$

$S(r) = Hr^{tr} = \begin{pmatrix} 3i + 3j + 3k \\ 3i + 3j + 3k \end{pmatrix} = \begin{pmatrix} \xi^6 \\ \xi^6 \end{pmatrix} (mod\ \pi) = \begin{pmatrix} s_1 \\ s_2 \end{pmatrix}$, Both syndromes s_1, s_2 are non-zeros. By using Eq. (12), $\begin{cases} s_1 & = \xi^6, \Longrightarrow j + i \equiv 6(mod 18) \\ s_2 & = \xi^6, \Longrightarrow 2j + i \equiv 6(mod 18) \end{cases}$, Solve the above system, we get error location $j = 0$ and error magnitude $\xi^6 = 3i + 3j + 3k$.

$e = (3i + 3j + 3k, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)_{1\times 18}$.

$c = (-2 + i + j + k, -1, -1 + i + j + k, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1)_{1\times 18}$

$Hc^{tr} = O\ (\text{mod}\ \pi)$. Hence, c is a codeword of C.

3.4 Double Error Correcting Cyclic Codes of QM Weight Two

Theorem: Let a cyclic code C of length $n = \varphi(p)$ define by H as:

$$H = \begin{pmatrix} \xi^0 & \xi^1 & \xi^2 & \cdots & \xi^{\varphi(p)-1} \\ \xi^0 & \xi^2 & \xi^4 & \cdots & \xi^{2\varphi(p)-2} \\ \xi^0 & \xi^3 & \xi^6 & \cdots & \xi^{3\varphi(p)-3} \\ \xi^0 & \xi^4 & \xi^8 & \cdots & \xi^{4\varphi(p)-4} \end{pmatrix} \tag{13}$$

Then,

1. $\xi^{l_2} - \xi^{l_1} \neq 0$, where $l_1, l_2 \in \mathbb{Z}, 0 \leq l_1 < l_2 \leq n - 1$;
2. $S_1S_3 - S_2^2 \neq 0$, otherwise, in received vector only one coordinate is in error.

Proof: *1. Suppose* $\xi^{l_2} - \xi^{l_1} = 0$. *Then,* $\xi^{l_2} = \xi^{l_1}$ *this implies that* $\xi^{l_1 - l_2} = 1$. *So,* $n|(l_1 - l_2)$. *But* $n > n - 1 \geq l_1 - l_2$, *a contradiction that the order of* ξ *is* n.

2. $S_1.S_3 - S_2^2 = 0$. *Then,* $S_1.S_3 = S_2^2$. *If and only if* $\xi^{2l_1}S_1x + \xi^{2l_2}S_1^2 - \xi^{2l_2}S_1x = (\xi^{l_2} - \xi^{l_1})^2x^2 + \xi^{2l_2}S_1^2 + 2\xi^{l_2}(\xi^{l_1} - \xi^{l_2})S_1x$. *If and only if* $(\xi^{l_1} - \xi^{l_2})^2x^2 + 2\xi^{l_1+l_2}S_1x - \xi^{2l_1}S_1x - \xi^{2l_2}S_1x = 0$. *Therefore, either* $x = 0$ *or* $(\xi^{l_1} - \xi^{l_2})^2x + 2\xi^{l_1+l_2}S_1 - \xi^{2l_1}S_1 - \xi^{2l_2}S_1 = 0$. *if* $x = 0$ *then it is not possible because* $\rho^{l+s} \neq 0$. *If* $(\xi^{l_1} - \xi^{l_2})^2x + 2\xi^{l_1+l_2}S_1 - \xi^{2l_1}S_1 - \xi^{2l_2}S_1 = 0$, *then* $x = \frac{(\xi^{l_1} - \xi^{l_2})^2.S_1}{(\xi^{l_1} - \xi^{l_2})^2} = S_1$. *If and only if* $y = 0$. *That's also correct, if and only if* $\xi^{l_2+s} = 0$. *This is a contradiction that until in a received vector only one coordinate is in error. Hence,* $S_1.S_3 - S_2^2 \neq 0$ *whenever two errors occurs.*

Theorem: Let a cyclic code C of length $n = \varphi(p)$ define by H as:

$H = \begin{pmatrix} \xi^0 & \xi^1 & \xi^2 & \cdots & \xi^{\varphi(p)-1} \\ \xi^0 & \xi^2 & \xi^4 & \cdots & \xi^{2\varphi(p)-2} \\ \xi^0 & \xi^3 & \xi^6 & \cdots & \xi^{3\varphi(p)-3} \\ \xi^0 & \xi^4 & \xi^8 & \cdots & \xi^{4\varphi(p)-4} \end{pmatrix}$; then the error of C can be corrected as the form $e(x) = e_{l_1}x^{l_1} + e_{l_2}x^{l_2}$, where $0 \leq l_1 < l_2 \leq n - 1$ with, $0 \leq W_{QM}(e_{l_1}), W_{QM}(e_{l_2}) \leq 2$.

Proof: Consider $e_{l_1} \neq 0$ and $e_{l_2} \neq 0$. In previous Theorem either $e_{l_1} = 0$ or $e_{l_2} = 0$. So by the help of H there are four syndromes

$$\begin{cases} S_1 &= e_{l_1}\xi^{l_1} + e_{l_2}\xi^{l_2} \\ S_2 &= e_{l_1}\xi^{2l_1} + e_{l_2}\xi^{2l_2} \\ S_3 &= e_{l_1}\xi^{3l_1} + e_{l_2}\xi^{3l_2} \\ S_4 &= e_{l_1}\xi^{3l_1} + e_{l_2}\xi^{3l_2} \end{cases} \tag{14}$$

Let $u = e_{l_1}\xi^{l_1}$ and $v = e_{l_2}\xi^{l_2}$, we get the following linear system of equations

$$\begin{cases} S_1 &= u + v \\ S_2 &= u\xi^{l_1} + v\xi^{l_2} \\ S_3 &= u\xi^{2l_1} + v\xi^{2l_2} \\ S_4 &= u\xi^{3l_1} + u\xi^{3l_2} \end{cases} \tag{15}$$

Two errors can be correct in code C if and only if the Eq. (14) has only unique solution. Since $e_{l_1} \neq 0$ and $e_{l_2} \neq 0$, then the system has unique solution. By using $u + v = S_1$ then Eq. (13) becomes,

$$\begin{cases} (\xi^{l_1} - \xi^{l_2})u = S_2 - \xi^{l_2}S_1 \\ (\xi^{2l_1} - \xi^{2l_2})u = S_3 - \xi^{2l_2}S_1 \\ (\xi^{3l_1} - \xi^{3l_2})u = S_4 - \xi^{3l_2}S_1 \end{cases} \tag{16}$$

which implies that

$$(\xi^{l_1} + \xi^{l_2})(S_2 - \xi^{l_2}S_1) = S_3 - \xi^{2l_2}S_1 \tag{17}$$

$$(\xi^{2l_1} + \xi^{l_1}\xi^{l_2} + \xi^{2l_2})(S_2 - \xi^{l_2}S_1) = S_4 - \xi^{3l_2}S_1 \tag{18}$$

Consider $S = \xi^{l_1} + \xi^{l_2}$ and $P = \xi^{l_1}\xi^{l_2}$. Then

$$\begin{cases} S(S_2 - \xi^{l_2}S_1) &= S_3 - \xi^{2l_2}S_1 \\ (S^2 - P)(S_2 - \xi^{l_2}S_1) &= S_4 - \xi^{3l_2}S_1 \end{cases} \tag{19}$$

From Eq. (16), we get $P = \frac{SS_2 - S_3}{S_1}$, Since $S_1 \neq 0$, from Eq. (17), we get

$$S = \frac{S_1S_4 - S_2S_3}{S_1S_3 - S_2^2} \tag{20}$$

$S_1S_3 - S_2^2 \neq 0$, otherwise in a received vector only one coordinate is in error. By Eqs. (17) and (18),

$$P = \frac{S_2S_4 - S_3^2}{S_1S_3 - S_2^2} \tag{21}$$

$$X^2 - SX + P = 0 \tag{22}$$

is the equation of sum and product of roots and the roots of this equation are $x_1 = \xi^{l_1}$ and $x_2 = \xi^{l_2}$, *where* l_1 and l_2 are error locations and error values are

$$\begin{cases} e_{l_1} = \dfrac{S_2 - \xi^{l_2} S_1}{\xi^{l_1}(\xi^{l_1} - \xi^{l_2})} \\ e_{l_2} = \dfrac{S_2 - \xi^{l_1} S_1}{\xi^{l_2}(\xi^{l_2} - \xi^{l_1})} \end{cases} \tag{23}$$

Illustration: Let $\pi = 4 + i + j + k$, $p = 19$, $n = \varphi(p) = 18$ and $\xi = 2$. Then, H is define by using Eq. (13) and elements of Tab. 1 respectively;

$$H = \begin{pmatrix} \xi^0 & \xi^1 & \xi^2 & \cdots & \xi^{17} \\ \xi^0 & \xi^2 & \xi^4 & \cdots & \xi^{34} \\ \xi^0 & \xi^3 & \xi^6 & \cdots & \xi^{51} \\ \xi^0 & \xi^4 & \xi^8 & \cdots & \xi^{68} \end{pmatrix}_{(4\times 18)}, r = (0,1,0,0\cdots 0,-1)_{1\times 35}$$

$$S(r) = Hr^{tr} = \begin{pmatrix} -3i-3j-3k \\ -2+2i+2j+2k \\ 1 \\ 3 \end{pmatrix} = \begin{pmatrix} \xi^{15} \\ \xi^{8} \\ 1 \\ \xi^{13} \end{pmatrix} (mod\pi) = \begin{pmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \end{pmatrix},$$

Here, S_1, S_2, S_3 and S_4 are four syndromes. By using Eqs. (20) and (21), we get, $S = \xi^{15}$ and $P = 1$. $X^2 - \xi^{15}X + 1 = 0$, and roots of this equation are ξ and ξ^{17}. The error occurs at position 1 and 17 in the received vector r. By Eq. (23), the error values are 1 and -1. $e = (0,1,0,0,\cdots 0,-1)_{1\times 18}, c = (0,0,0,0\cdots 0,0)_{1\times 18}$

$Hc^{tr} = O(mod\pi)$. Hence c is a codeword of C.

4 Parity Check Matrix Extensions of $n = \varphi(p)$ Length to $2n-1 = 2\varphi(p) - 1$ Length Cyclic Codes and Error Correction of these Codes for QM Weight One and Two through Monoid Rings

Parity check matrix extension of C of length $n = \varphi(p)$ to $2n - 1 = 2\varphi(p) - 1$ length and this constructed parity check matrix is in blocks of parity check matrices by following techniques in [[20], Section 4] will be discussed in this Section. Furthermore, single and double error correction of these cyclic codes for quaternion mannheim weight one and two through moniod ring using techniques in [[20]; Section 5].

Let an associative ring and semigroup are $(B, +, .)$ and $(Q, *)$. Let a set Y of all finite non zero functions from Q into B. Let a ring Y which defines by binary operation addition and multiplication as: For $h, g \in Y, s' \in Q$, $(h+g)(s') = h(s') + g(s')$, $(h.g)(s')(x+a)^n = \sum_{t'*u'=s'} h(t').g(u')$.

It is clear that the sum is obtained by the pairs (t', u') elements of Q so that $s' = t' * u'$ and for any $t', u' \in S$ if s' is not expressed as the form $t'*u'$, then $(h.g)s' = 0$. Hence Y is called a semigroup ring of Q over B. If Q is monoid, then Y is known as a monoid ring. Hence Y ring is characterized by $B[Q]$, here Q indicates multiplicative semigroup and Y written as $\sum_{s'\in Q} h(s')s'$. Here Y shows $B[X, Q]$, where Q shows additive semi group. Here isomorphism between additive semigroup Q and multiplicative semigroup $\{X^{s'} : s' \in Q\}$, Hence $h' \in B[X, Q]$ shows unique canonical form of non zero elements $\sum_{k=1}^{n} h(s'_k)X^{s'_k} = hX^{s'_k}$, where h_k is non-zero and $s'_k \neq (s')_j$. The idea of order and degree is not commonly used for the semigroup rings if we take ordered semigroup Q, i.e., if $\sum_{k=1}^{n} h(s'_k)X^{s'_k}$, $s'_1 < s'_2 < s'_3 \cdots < s'_n$ is the canonical form of the non-zero element $h \in B[X, Q]$, then $deg(h) = s'_n$ and $ord(h) = s'$. Now, if integral domain is R, then for $g, h \in B[X, Q]$, then $deg(g + h) = deg(g) + deg(h), ord(g.h) = ord(g) + ord(h)$.

If Q is not Z_0 and B would be an associative ring, semigroup $B[X, Q]$ is called polynomial ring $B[X]$. Of course, $B[X] = B[X, Z_0] \subset B[X; \frac{1}{2}Z_0]$. For semigroup ring concepts the Gilmer's book [22] is better. Extension of parity check matrix H of C of length $2n-1 = p-2$ in [[17]; Section 4]; By following these parity check matrices, we describe H of C of length $2n-1 = 2\varphi(p)-1 = 2p-3$ as follows:

$$H = \begin{pmatrix} (\xi^{\frac{1}{2}})^0 & (\xi^{\frac{1}{2}})^1 \cdots & (\xi^{\frac{1}{2}})^{2\varphi(p)-1-1} \\ \vdots & \ddots & \vdots \\ (\xi^{\frac{1}{2}})^0 & (\xi^{\frac{1}{2}})^{(2t+1)} \cdots & (\xi^{\frac{1}{2}})^{(2t+1)(2\varphi(p)-1-1)} \end{pmatrix} \tag{24}$$

1. H can be written in block form H_{11}, H_{12}, H_{21} and H_{22} as: $H = \begin{pmatrix} H_{11} & H_{12} \\ H_{21} & H_{22} \end{pmatrix}$;
$$H_{11} = \begin{pmatrix} (\xi^{\frac{1}{2}})^0 & (\xi^{\frac{1}{2}})^1 \cdots & (\xi^{\frac{1}{2}})^{\varphi(p)-1} \\ \vdots & \ddots & \vdots \\ (\xi^{\frac{1}{2}})^0 & (\xi^{\frac{1}{2}})^{(t+1)} \cdots & (\xi^{\frac{1}{2}})^{(t+1)(\varphi(p)-1)} \end{pmatrix}; H_{21} = \begin{pmatrix} (\xi^{\frac{1}{2}})^0 & (\xi^{\frac{1}{2}})^{2(\frac{t}{2})+1} \cdots & (\xi^{\frac{1}{2}})^{(\varphi(p)-1)2(\frac{t}{2})+1)} \\ \vdots & \ddots & \vdots \\ (\xi^{\frac{1}{2}})^0 & (\xi^{\frac{1}{2}})^{2t+1} \cdots & (\xi^{\frac{1}{2}})^{(\varphi(p)-1)(2t+1)} \end{pmatrix};$$
$$H_{12} = \begin{pmatrix} (\xi^{\frac{1}{2}})^{\varphi(p)} & \cdots & (\xi^{\frac{1}{2}})^{(2\varphi(p)-1)-1} \\ \vdots & \ddots & \vdots \\ (\xi^{\frac{1}{2}})^{(t+1)(\varphi(p))} & \cdots & (\xi^{\frac{1}{2}})^{(t+1)((2\varphi(p)-1)-1)} \end{pmatrix}; H_{22} = \begin{pmatrix} (\xi^{\frac{1}{2}})^{(\varphi(p))(2(\frac{t}{2})+1)} & \cdots & (\xi^{\frac{1}{2}})^{((2\varphi(p)-1)-1)(2(\frac{t}{2})+1)} \\ \vdots & \ddots & \vdots \\ (\xi^{\frac{1}{2}})^{(\varphi(p))(2t+1)} & \cdots & (\xi^{\frac{1}{2}})^{((2\varphi(p)-1)-1)(2t+1)} \end{pmatrix};$$
Here, H_{11} is equal to H of length $n = \varphi(p) = p-1$ as like in Eq. (1).
2. Parity check matrix of $n = \varphi(p) = p-1$ length is extended to $2n-1 = 2(\xi^{\frac{1}{2}})(p)-1 = 2p-3$ length parity check matrix by adding rows and columns.

4.1 Single Error Correcting Cyclic Codes of Length $2n-1 = 2\varphi(p)-1$ for QM Weight One

Let $\xi^{\frac{1}{2}}$ is the primitive element of $H(K)_\pi$, p be a prime in $\mathbb{Z}$, $\pi = b_0 + b_1 i + b_2 j + b_3 k$, $p = \pi\overline{\pi}$ and $(\xi^{\frac{1}{2}})^{p-1} = 1$. Then, H and G are define as;

$$H = \left((\xi^{\frac{1}{2}})^0 (\xi^{\frac{1}{2}})^1 \cdots (\xi^{\frac{1}{2}})^{2\varphi(p)-2}\right) \tag{25}$$

$$G = \begin{pmatrix} (\xi^{\frac{1}{2}})^0 & 1 & 0 \cdots & 0 \\ \vdots & & \ddots & \vdots \\ (\xi^{\frac{1}{2}})^0 & 0 & 0 \cdots & 1 \end{pmatrix} \tag{26}$$

The one QM error-correcting codes of length $2n-1 = 2\varphi(p)-1$ can be constructed by H. Then C defined by H in Eq. (25) can correct any QM error of weight one. 1 or -1 are the values of one quaternion Mannheim errors. For the decoding procedure first step is to find the syndrome $S(r) = Hr^{tr}$ with the help of H and the received vector r. Then the error value is computed by $S(\xi^{\frac{1}{2}})^{-l}$, where $l(\text{mod } 2\varphi(p)-1)$ is a non-negative integer which helps for error locations. Hence, $c = r - e$ is the corrected codeword.

Illustration: Let $\pi = 4 + i + j + k$, $p = 19$, $2n - 1 = 2\varphi(p) - 1 = 35$ and $\xi^{\frac{1}{2}} = 2$. Then, H, G by Eqs. (25) and (26) and the primitive element of $H(K)_\pi$ from Tab. 2 respectively;

Table 2: $\xi^{\frac{1}{2}} = 2$ is the root of $(z^{\frac{1}{2}})^9 + 1$

$\xi^{\frac{l}{2}}$	*Value*	$\xi^{\frac{l}{2}}$	*Value*	$\xi^{\frac{l}{2}}$	*Value*
$(\xi^{\frac{1}{2}})^0$	1	$(\xi^{\frac{1}{2}})^6$	$3i + 3j + 3k$	$(\xi^{\frac{1}{2}})^{12}$	$2i + 2j + 2k$
$(\xi^{\frac{1}{2}})^1$	2	$(\xi^{\frac{1}{2}})^7$	$-1 + i + j + k$	$(\xi^{\frac{1}{2}})^{13}$	3
$(\xi^{\frac{1}{2}})^2$	$-i - j - k$	$(\xi^{\frac{1}{2}})^8$	$-2 + 2i + 2j + 2k$	$(\xi^{\frac{1}{2}})^{14}$	$2 - i - j - k$
$(\xi^{\frac{1}{2}})^3$	$-2i - 2j - 2k$	$(\xi^{\frac{1}{2}})^9$	-1	$(\xi^{\frac{1}{2}})^{15}$	$-3i - 3j - 3k$
$(\xi^{\frac{1}{2}})^4$	-3	$(\xi^{\frac{1}{2}})^{10}$	-2	$(\xi^{\frac{1}{2}})^{16}$	$1 - i - j - k$
$(\xi^{\frac{1}{2}})^5$	$-2 + i + j + k$	$(\xi^{\frac{1}{2}})^{11}$	$i + j + k$	$(\xi^{\frac{1}{2}})^{17}$	$2 - 2i - 2j - 2k$

$$H = \begin{pmatrix} 1 & 2 & -i-j-k & \cdots & 1-i-j-k \end{pmatrix}; G = \begin{pmatrix} -1 & & & 1 & 0 \cdots & 0 \\ \vdots & & & & \ddots & \vdots \\ -1+i+j+k & & & 0 & 0 \cdots & 1 \end{pmatrix};$$

$r = (1, 0, -1 + i + j + k, 0, 0, \cdots, -1)_{1\times 35}$, $S(r) = Hr^{tr} = -1 + i + j + k \equiv (\xi^{\frac{1}{2}})^7 (mod\pi)$

The error location is $7 \equiv 7(\text{ mod } 35)$ then, we get error value as $S(\xi^{\frac{1}{2}})^{-7} = 1(\text{ mod } \pi)$.

$c = (1, 0, -1 + i + j + k, 0, 0, 0, 0, -1, 0, \cdots, -1)_{1\times 35}$. $Hc^{tr} = O(\text{mod } \pi)$. Hence c is a corrected codeword of C.

4.2 Double Error Correcting Cyclic Codes of Length $2n - 1 = 2\varphi(p) - 1$ for QM Weight One

Theorem: Let a cyclic code C of length $2n - 1 = 2\varphi(p) - 1$ define by H.

$$H = \begin{pmatrix} (\xi^{\frac{1}{2}})^0 & (\xi^{\frac{1}{2}})^1 & (\xi^{\frac{1}{2}})^2 & \cdots & (\xi^{\frac{1}{2}})^{2\varphi(p)-2} \\ (\xi^{\frac{1}{2}})^0 & (\xi^{\frac{1}{2}})^2 & (\xi^{\frac{1}{2}})^4 & \cdots & (\xi^{\frac{1}{2}})^{4\varphi(p)-4} \end{pmatrix} \tag{27}$$

Then C can correct any error in the form $e(x) = e_j(z^{\frac{j}{2}}) + e_i(z^{\frac{i}{2}})$, where $0 \le W_{QM}(e_j), W_{QM}(e_i) \le 1$.

Proof: *Consider double error is occur at two different places l_1, l_2 in received r and two error vectors e_1, e_2 of quaternion mannheim weight as, $0 \le w_{QM}(e_1), W_{QM}(e_2) \le 1$. First find syndromes by help of parity check matrix H in Eq. (27) and transpose of received vector r as;*

$$S(r) = Hr^{tr} = \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} (mod\pi) \tag{28}$$

Now we find a polynomial $h(x)$ for the location of errors as follows:

$$h(x^{\frac{1}{2}}) = (x^{\frac{1}{2}} - \xi^{\frac{l_1}{2}})(x^{\frac{1}{2}} - \xi^{\frac{l_2}{2}}) = x - (\xi^{\frac{l_1}{2}} + \xi^{\frac{l_2}{2}})x^{\frac{1}{2}} + (\xi^{\frac{l_1}{2}}).(\xi^{\frac{l_2}{2}}) = x - s_1 x^{\frac{1}{2}} + \eta \tag{29}$$

we get η by syndromes. From $s_1 = \xi^{\frac{l_1}{2}} + \xi^{\frac{l_2}{2}}, s_2 = \xi^{l_1} + \xi^{l_2}$ and $\eta = \xi^{\frac{l_1}{2}}.\xi^{\frac{l_2}{2}}$. we get

$$s_1^2 - s_2 = (\xi^{\frac{l_1}{2}} + \xi^{\frac{l_2}{2}})^2 - (\xi^{l_1} + \xi^{l_2}) = 2\xi^{\frac{l_1}{2}}.\xi^{\frac{l_2}{2}} = 2s \tag{30}$$

$$\frac{s_1^2 - s_2}{2} = \frac{2\eta}{2} = \eta(mod\pi) \tag{31}$$

Thus, $h(x)$ lead us to find the location and error values. If $\xi^{\frac{l_1}{2}}$ and $\xi^{\frac{l_2}{2}}$ are roots of $h(x)$, then $l_1(\text{mod } 2n-1) = m_1$, $l_2(\text{mod } 2n-1) = m_2$ are locations of error and error values are $e_1 = \frac{\xi^{\frac{l_1}{2}}}{m_1}$, $e_2 = \frac{\xi^{\frac{l_2}{2}}}{m_2}$. Then there are possibilities. If both two syndrome s_1 and s_2 are zeros then no error occurs. If $s_1^2 = s_2 \neq 0$, then one error occurs. If $s_1^2 \neq s_2$ and $s_1 \neq 0$, then two error occurs.

Illustration: Let $\pi = 4+i+j+k$, $p = 19$, $2n-1 = 2\varphi(p)-1 = 35$ and $\xi^{\frac{1}{2}} = 2$. Then, H by using Eq. (27) and Tab. 2 respectively; $H = \begin{pmatrix} 1 & 2 & \cdots & 1-i-j-k \\ 1 & -i-j-k & \cdots & 2-i-j-k \end{pmatrix}_{2\times 35}$,

$r = (1-i-j-k, 1, -1+i+j+k, 0, \cdots, 0, -1)_{1\times 35}$ $S(r) = Hr^{tr} = \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} (\xi^{\frac{1}{2}})^0 \\ (\xi^{\frac{1}{2}})^9 \end{pmatrix} (mod\pi) = \begin{pmatrix} s_1 \\ s_2 \end{pmatrix}$, Both syndromes s_1, s_2 are non-zeros and $s_1^2 \neq s_2 \neq 0$. Hence two error occurs. By Eq. (31), $\eta = \frac{s_1^2 - s_2}{2} = 1(mod\pi)$. Hence error polynomial by Eq. (29) is $h(x^{\frac{1}{2}}) = x - x^{\frac{1}{2}} + 1$. The error locator polynomial $h(x^{\frac{1}{2}})$ has roots $(\xi^{\frac{1}{2}})^{l_1} = (\xi^{\frac{1}{2}})^3$ and $(\xi^{\frac{1}{2}})^{l_2} = (\xi^{\frac{1}{2}})^{15}$, so, error locations are 3 and 15 in received vector r. Hence, error values are $e^{l_1} = 1$ and $e^{l_2} = 1$. $c = (1-i-j-k, 1, -1+i+j+k, -1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, 0, \cdots, 0, -1)_{1\times 35}$.

$Hc^{tr} = O(mod\pi)$. Hence c is a corrected codeword of C.

4.3 *Single Error Correcting Cyclic Codes of Length* $2n-1 = 2\varphi(p)-1$ *for QM Weight Two*

Theorem: Let $\xi^{\frac{1}{2}}$ is the primitive element of $H(K)_\pi$, $\pi = b_0 + b_1 i + b_2 j + b_3 k$ and $p = \pi\overline{\pi}$. Let a cyclic code C of length $2n-1 = 2\varphi(p)-1 = 2p-3$ define by H.

$$H = \begin{pmatrix} (\xi^{\frac{1}{2}})^0 & (\xi^{\frac{1}{2}})^1 & (\xi^{\frac{1}{2}})^2 & \cdots & (\xi^{\frac{1}{2}})^{2\varphi(p)-2} \\ (\xi^{\frac{1}{2}})^0 & (\xi^{\frac{1}{2}})^2 & (\xi^{\frac{1}{2}})^4 & \cdots & (\xi^{\frac{1}{2}})^{4\varphi(p)-4} \end{pmatrix} \tag{32}$$

then C can correct errors as the form of $e(x) = e_l(x^{\frac{l}{2}})$, where $1 \leq w_{QM}(e_l) \leq 2$.

Proof: Suppose that $(\xi^{\frac{1}{2}})^i$ is error magnitude, $0 \leq i \leq 2n-2$ has occurred in location j, where $0 \leq j \leq 2n-2$. Let $e(x) = (\xi^{\frac{1}{2}})^i x^j$ be the error pattern. Then, $s_1 = (\xi^{\frac{1}{2}})^{j+i}$ and $s_2 = (\xi^{\frac{1}{2}})^{2j+i}$ are syndromes. Let $s_1 = (\xi^{\frac{1}{2}})^{l_1}$ and $s_2 = (\xi^{\frac{1}{2}})^{l_2}$ are the basis of $s_j; j = 1, 2$. We have

$$\begin{cases} s_1 = (\xi^{\frac{1}{2}})^{j+i}, \Longrightarrow j+i \equiv l_1(mod\varphi(p)) \\ s_2 = (\xi^{\frac{1}{2}})^{2j+i}, \Longrightarrow 2j+i \equiv l_2(mod\varphi(p)) \end{cases} \tag{33}$$

Eq. (33) having unique solution at $j = l_2 - l_1(\text{ mod } p-1)$, $i = l_1 - j(\text{ mod } p-1)$. Hence, error is occurred in location $(l_2 - l_1)(\text{ mod } 2n-1)$ with magnitude $(\xi^{\frac{1}{2}})^i$.

Illustration: Let $\pi = 4+i+j+k$, $p = 19$, $n = \varphi(p) = 18$ and $(\xi^{\frac{1}{2}}) = 2$. Then, H is defined by using Eq. (32) and Tab. 2 respectively; $H = \begin{pmatrix} 1 & 2 & \cdots & 1-i-j-k \\ 1 & -i-j-k & \cdots & 2-i-j-k \end{pmatrix}_{2\times 35}$,

$r = (1, -1, -1+i+j+k, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, 0 \cdots 0, 0)_{1\times 35}$;

$$S(r) = Hr^{tr} = \begin{pmatrix} 3i+3j+3k \\ 3i+3j+3k \end{pmatrix} = \begin{pmatrix} (\xi^{\frac{1}{2}})^6 \\ (\xi^{\frac{1}{2}})^6 \end{pmatrix} (mod\pi) = \begin{pmatrix} s_1 \\ s_2 \end{pmatrix}, \begin{cases} s_1 & = (\xi^{\frac{1}{2}})^6, \Longrightarrow j+i \equiv 6(mod 18) \\ s_2 & = (\xi^{\frac{1}{2}})^6, \Longrightarrow 2j+i \equiv 6(mod 18) \end{cases}$$

Solve the above system and get error location $j = 0$ and error magnitude $(\xi^{\frac{1}{2}})^6 = 3i + 3j + 3k$.

$$e = \begin{pmatrix} 3i+3j+3k, 0, 0, \cdots 0, 0 & \end{pmatrix}_{1\times 35}$$

$$r = (1, -1, -1+i+j+k, 0, 0, 0, -3i-3j-3k, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, 0 \cdots 0, 0)_{1\times 35}$$

$Hc^{tr} = O(mod\pi)$. Hence c is a codeword of cyclic code C.

4.4 *Double Error Correcting Cyclic Codes of Length* $2n-1 = 2\varphi(p)-1$ *for QM Weight Two*

Lemma: Let C be a cyclic code of length $2n-1 = 2\varphi(p)-1$ define by H as:

$$H = \begin{pmatrix} (\xi^{\frac{1}{2}})^0 & (\xi^{\frac{1}{2}})^1 & (\xi^{\frac{1}{2}})^2 & \cdots & (\xi^{\frac{1}{2}})^{2\varphi(p)-2} \\ (\xi^{\frac{1}{2}})^0 & (\xi^{\frac{1}{2}})^2 & (\xi^{\frac{1}{2}})^4 & \cdots & (\xi^{\frac{1}{2}})^{4\varphi(p)-4} \\ (\xi^{\frac{1}{2}})^0 & (\xi^{\frac{1}{2}})^3 & (\xi^{\frac{1}{2}})^6 & \cdots & (\xi^{\frac{1}{2}})^{6\varphi(p)-6} \\ (\xi^{\frac{1}{2}})^0 & (\xi^{\frac{1}{2}})^4 & (\xi^{\frac{1}{2}})^8 & \cdots & (\xi^{\frac{1}{2}})^{8\varphi(p)-8} \end{pmatrix} \tag{34}$$

then,

1. $(\xi^{\frac{1}{2}})^{l_2} - (\xi^{\frac{1}{2}})^{l_1} \neq 0$, where $l_1, l_2 \in \mathbb{Z}, 0 \leq l_1 < l_2 \leq 2n-2$.
2. $S_1S_3 - S_2^2 \neq 0$, otherwise in received vector only one coordinate is in error.

Proof:

1. Suppose $(\xi^{\frac{1}{2}})^{l_2} - (\xi^{\frac{1}{2}})^{l_1} = 0$. Then, $(\xi^{\frac{1}{2}})^{l_2} = (\xi^{\frac{1}{2}})^{l_1}$ this implies that $(\xi^{\frac{1}{2}})^{l_1-l_2} = 1$.So, $(2n-1)|(l_1-l_2)$. But $2n-1 > n-1 \geq l_1 - l_2$, a contradiction that the order of $(\xi^{\frac{1}{2}})$ is $2n-1$.
2. $S_1.S_3 - S_2^2 = 0$. Then, $S_1.S_3 = S_2^2$ if and only if $(\xi^{\frac{1}{2}})^{2l_1}S_1x + (\xi^{\frac{1}{2}})^{2l_2}S_1^2 - (\xi^{\frac{1}{2}})^{2l_2}S_1x = ((\xi^{\frac{1}{2}})^{l_2} - (\xi^{\frac{1}{2}})^{l_1})^2x^2 + (\xi^{\frac{1}{2}})^{2l_2}S_1^2 + 2(\xi^{\frac{1}{2}})^{l_2}((\xi^{\frac{1}{2}})^{l_1} - (\xi^{\frac{1}{2}})^{l_2})S_1x$ if and only if $((\xi^{\frac{1}{2}})^{l_1} - (\xi^{\frac{1}{2}})^{l_2})^2x^2 + 2(\xi^{\frac{1}{2}})^{l_1+l_2}S_1x - (\xi^{\frac{1}{2}})^{2l_1}S_1x - (\xi^{\frac{1}{2}})^{2l_2}S_1x = 0$. Therefore, either $x = 0$ or $((\xi^{\frac{1}{2}})^{l_1} - (\xi^{\frac{1}{2}})^{l_2})^2x + 2(\xi^{\frac{1}{2}})^{l_1+l_2}S_1 - (\xi^{\frac{1}{2}})^{2l_1}S_1 - (\xi^{\frac{1}{2}})^{2l_2}S_1 = 0$. if $x = 0$ then it is not possible because $\rho^{l+s} \neq 0$. If $((\xi^{\frac{1}{2}})^{l_1} - (\xi^{\frac{1}{2}})^{l_2})^2x + 2(\xi^{\frac{1}{2}})^{l_1+l_2}S_1 - (\xi^{\frac{1}{2}})^{2l_1}S_1 - (\xi^{\frac{1}{2}})^{2l_2}S_1 = 0$, then $x = \frac{((\xi^{\frac{1}{2}})^{l_1} - (\xi^{\frac{1}{2}})^{l_2})^2.S_1}{((\xi^{\frac{1}{2}})^{l_1} - (\xi^{\frac{1}{2}})^{l_2})^2} = S_1$. If and only if $y = 0$. That is, if and only if $(\xi^{\frac{1}{2}})^{l_2+s} = 0$. This is a contradiction unless in a received vector only one coordinate is in error. Thus, $S_1.S_3 - S_2^2 \neq 0$. So, two error occurs.

Theorem: Let C be a cyclic code of length $2n-1 = 2\varphi(p)-1$ defined by H in previous Theorem.

Then error of C can be correct in the form of $e(x) = e_{l_1}x^{l_1} + e_{l_2}x^{l_2}$, where $0 \leq l_1 < l_2 \leq 2n-2$ with, $0 \leq W_{QM}(e_{l_1}), W_{QM}(e_{l_2}) \leq 2$.

Proof: Consider $e_{l_1} \neq 0$ and $e_{l_2} \neq 0$. In Lemma, either $e_{l_1} = 0$ or $e_{l_2} = 0$. So by the help of parity check matrix there are four syndromes

$$\begin{cases} S_1 &= e_{l_1}(\xi^{\frac{1}{2}})^{l_1} + e_{l_2}(\xi^{\frac{1}{2}})^{l_2} \\ S_2 &= e_{l_1}(\xi^{\frac{1}{2}})^{2l_1} + e_{l_2}(\xi^{\frac{1}{2}})^{2l_2} \\ S_3 &= e_{l_1}(\xi^{\frac{1}{2}})^{3l_1} + e_{l_2}(\xi^{\frac{1}{2}})^{3l_2} \\ S_4 &= e_{l_1}(\xi^{\frac{1}{2}})^{3l_1} + e_{l_2}(\xi^{\frac{1}{2}})^{3l_2} \end{cases} \tag{35}$$

Let $u = e_{l_1}(\xi^{\frac{1}{2}})^{l_1}$ and $v = e_{l_2}(\xi^{\frac{1}{2}})^{l_2}$, we get the following linear system of equations

$$\begin{cases} S_1 &= u + v \\ S_2 &= u(\xi^{\frac{1}{2}})^{l_1} + v(\xi^{\frac{1}{2}})^{l_2} \\ S_3 &= u(\xi^{\frac{1}{2}})^{2l_1} + v(\xi^{\frac{1}{2}})^{2l_2} \\ S_4 &= u(\xi^{\frac{1}{2}})^{3l_1} + v(\xi^{\frac{1}{2}})^{3l_2} \end{cases} \tag{36}$$

Two errors can be correct in cyclic code C if and only if the Eq. (35) has only unique solution. Since $e_{l_1} \neq 0$ and $e_{l_2} \neq 0$, then the system has unique solution. By using $u + v = S_1$, then Eq. (34) becomes,

$$\begin{cases} ((\xi^{\frac{1}{2}})^{l_1} - (\xi^{\frac{1}{2}})^{l_2})u = S_2 - (\xi^{\frac{1}{2}})^{l_2}S_1 \\ ((\xi^{\frac{1}{2}})^{2l_1} - (\xi^{\frac{1}{2}})^{2l_2})u = S_3 - (\xi^{\frac{1}{2}})^{2l_2}S_1 \\ ((\xi^{\frac{1}{2}})^{3l_1} - (\xi^{\frac{1}{2}})^{3l_2})u = S_4 - (\xi^{\frac{1}{2}})^{3l_2}S_1 \end{cases} \tag{37}$$

$$((\xi^{\frac{1}{2}})^{l_1} + (\xi^{\frac{1}{2}})^{l_2})(S_2 - (\xi^{\frac{1}{2}})^{l_2}S_1) = S_3 - (\xi^{\frac{1}{2}})^{2l_2}S_1 \tag{38}$$

$$((\xi^{\frac{1}{2}})^{2l_1} + (\xi^{\frac{1}{2}})^{l_1}(\xi^{\frac{1}{2}})^{l_2} + (\xi^{\frac{1}{2}})^{2l_2})(S_2 - (\xi^{\frac{1}{2}})^{l_2}S_1) = S_4 - (\xi^{\frac{1}{2}})^{3l_2}S_1 \tag{39}$$

Consider $S = (\xi^{\frac{1}{2}})^{l_1} + (\xi^{\frac{1}{2}})^{l_2}$ and $P = (\xi^{\frac{1}{2}})^{l_1}(\xi^{\frac{1}{2}})^{l_2}$. Then

$$\begin{cases} S(S_2 - (\xi^{\frac{1}{2}})^{l_2}S_1) &= S_3 - (\xi^{\frac{1}{2}})^{2l_2}S_1 \\ (S^2 - P)(S_2 - (\xi^{\frac{1}{2}})^{l_2}S_1) &= S_4 - (\xi^{\frac{1}{2}})^{3l_2}S_1 \end{cases} \tag{40}$$

From Eq. (37), we get $P = \frac{SS_2 - S_3}{S_1}$, Since $S_1 \neq 0$, from Eq. (38) we get

$$S = \frac{S_1S_4 - S_2S_3}{S_1S_3 - S_2^2} \tag{41}$$

Let $S_1S_3 - S_2^2 \neq 0$, otherwise in a received vector only one coordinate is in error. Put Eq. (38) in Eq. (39) we get

$$P = \frac{S_2S_4 - S_3^2}{S_1S_3 - S_2^2} \tag{42}$$

$$(X^{\frac{1}{2}})^2 - S(X^{\frac{1}{2}}) + P = 0 \tag{43}$$

is the equation of sum and product of roots and the roots of this equation are $x_1 = (\xi^{\frac{1}{2}})^{l_1}$ and $x_2 = (\xi^{\frac{1}{2}})^{l_2}$, *where* l_1 and l_2 are error locations and error values are

$$\begin{cases} e_{l_1} = \dfrac{S_2 - (\xi^{\frac{1}{2}})^{l_2} S_1}{(\xi^{\frac{1}{2}})^{l_1}((\xi^{\frac{1}{2}})^{l_1} - (\xi^{\frac{1}{2}})^{l_2})} \\ e_{l_2} = \dfrac{S_2 - (\xi^{\frac{1}{2}})^{l_1} S_1}{(\xi^{\frac{1}{2}})^{l_2}((\xi^{\frac{1}{2}})^{l_2} - (\xi^{\frac{1}{2}})^{l_1})} \end{cases} \tag{44}$$

Illustration: Let $\pi = 4 + i + j + k$, $p = 19$, $2n - 1 = 2\varphi(19) - 1 = 35$ and $(\xi^{\frac{1}{2}}) = 2$. Then, Parity check matrix H by Eq. (34) and Tab. 2 respectively; $H = \begin{pmatrix} (\xi^{\frac{1}{2}})^0 & (\xi^{\frac{1}{2}})^1 & (\xi^{\frac{1}{2}})^2 & \cdots & (\xi^{\frac{1}{2}})^{34} \\ (\xi^{\frac{1}{2}})^0 & (\xi^{\frac{1}{2}})^2 & (\xi^{\frac{1}{2}})^4 & \cdots & (\xi^{\frac{1}{2}})^{68} \\ (\xi^{\frac{1}{2}})^0 & (\xi^{\frac{1}{2}})^3 & (\xi^{\frac{1}{2}})^6 & \cdots & (\xi^{\frac{1}{2}})^{102} \\ (\xi^{\frac{1}{2}})^0 & (\xi^{\frac{1}{2}})^4 & (\xi^{\frac{1}{2}})^8 & \cdots & (\xi^{\frac{1}{2}})^{136} \end{pmatrix}$,

$r = (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, 0, 0, \cdots 0)_{1\times 35}$

$$S(r) = Hr^{tr} = \begin{pmatrix} -3i - 3j - 3k \\ -2 + 2i + 2j + 2k \\ 1 \\ 3 \end{pmatrix} = \begin{pmatrix} \left(\xi^{\frac{1}{2}}\right)^{15} \\ \left(\xi^{\frac{1}{2}}\right)^{8} \\ 1 \\ \left(\xi^{\frac{1}{2}}\right)^{13} \end{pmatrix} (mod\pi) = \begin{pmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \end{pmatrix},$$

By Eqs. (41) and (42) we get, $S = \xi^{15}$ and $P = 1$. $(X^{\frac{1}{2}})^2 - (\xi^{\frac{1}{2}})^2(X^{\frac{1}{2}}) + P = 0$, and roots of this equation are ξ and ξ^{17}. Error occurs at position 1 and 17 in the received vector. By using Eq. (44), the error values are 1 and -1. $e = (0, 1, 0, 0, \cdots 0, -1)_{1\times 35}$, $c = (0, 0, 0, 0, \cdots 0, 0)_{1\times 35}$. $Hc^{tr} = O(mod\pi)$. Hence, c is a corrected codeword of C.

5 Lengths and Code Rates of Cyclic Codes Comparison

In this section, we will discuss the lengths and the code rates of cyclic codes for every prime p. In [13], Özen et al. have discussed the cyclic codes of length $n = \frac{p-1}{2}$ for every prime p. According to this length $n = \frac{p-1}{2}$, code rate of the cyclic code will be $\frac{n-1}{n} = \frac{p-3}{p-1}$. Similarly, In [17] Shah et al. have discussed the cyclic code of length $2n - 1 = p - 2$ for every prime p. According to this length $2n - 1 = p - 2$, the code rate of C will be $\frac{2n-2}{2n-1} = \frac{p-3}{p-2}$, which shown in the table and pictorial depictions given below:

Tab. 3 shows the previous results of lengths and code rates of paper cited [13] and [17]. Which are given in the last of these papers. And Tab. 4 shows our proposed word according to Tab. 3.

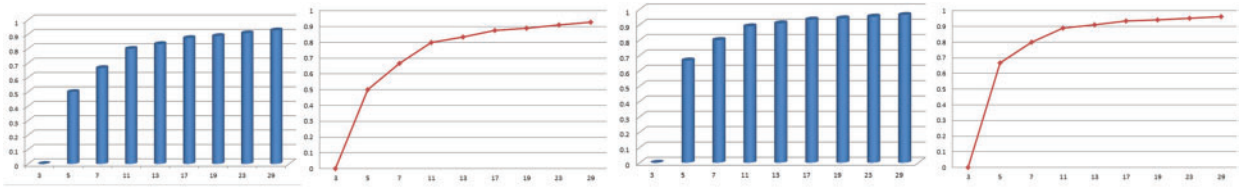
Table 3: Code rate verses different odd primes in [13] and [17]

p	$[n, n-1]$	Code Rate	p	$[2n-1, 2n-2]$	Code Rate
3	[1, 0]	0.0000	3	[1,0]	0.0000
5	[2, 1]	0.5000	5	[3,2]	0.6667

(Continued)

Table 3: Continued

p	$[n, n-1]$	Code Rate	p	$[2n-1, 2n-2]$	Code Rate
7	[3, 2]	0.6667	7	[5, 4]	0.8000
11	[5, 4]	0.8000	11	[9, 8]	0.8889
13	[6, 5]	0.8333	13	[11, 10]	0.9091
17	[8, 7]	0.8750	17	[15, 14]	0.9333
19	[9, 8]	0.8889	19	[17, 16]	0.9412
23	[11, 10]	0.9091	23	[21, 20]	0.9524
29	[14, 13]	0.9286	29	[27, 26]	0.9630

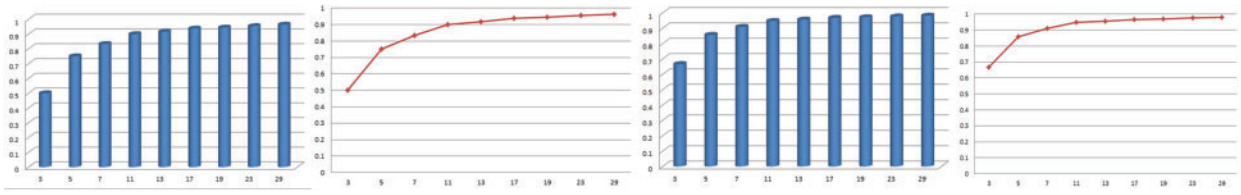


Figures 1, 2, 3 and 4: Code Rate of $\boldsymbol{C}$ of Length $\boldsymbol{n = \frac{p-1}{2}}$ and $\boldsymbol{2n-1 = p-2}$ for Primes in [13] and [17]

However, in proposed study by following [13] and [17], the cyclic codes of length $\boldsymbol{n = \varphi(p) = p-1}$ for every prime $\boldsymbol{p}$. According to this length $\boldsymbol{n = \varphi(p) = p-1}$, code rate of $\boldsymbol{C}$ will be $\frac{n-1}{n} = \frac{\varphi(p)-1}{\varphi(p)} = \frac{p-2}{p-1}$. Also, the cyclic codes of length $\boldsymbol{2n-1 = 2\varphi(p)-1 = 2p-3}$ for every prime $\boldsymbol{p}$. According to this length $\boldsymbol{2n-1 = 2\varphi(p)-1 = 2p-3}$, code rate of $\boldsymbol{C}$ will be $\frac{2n-2}{2n-1} = \frac{2\varphi(p)-2}{2\varphi(p)-1} = \frac{2p-4}{2p-3}$, shown in the table and pictorial depictions given below;

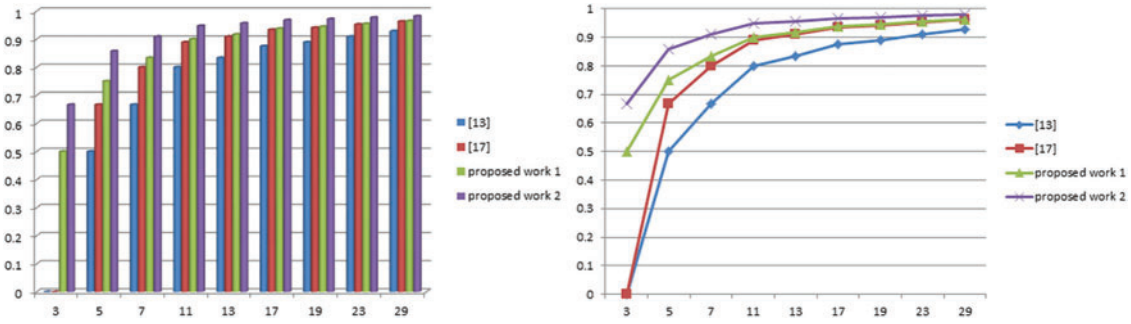
Table 4: Code rate of cyclic code of lengths $\boldsymbol{n = \varphi(p)}$ and $\boldsymbol{2n-1 = 2\varphi\,(p)-1}$ for primes in proposed study

p	$[n, n-1]$	Code Rate	p	$[2n-1, 2n-2]$	Code Rate
3	[2,1]	0.5000	3	[3, 2]	0.6667
5	[4,3]	0.7500	5	[7, 6]	0.8571
7	[6, 5]	0.8333	7	[11, 10]	0.9091
11	[10, 9]	0.9000	11	[19, 18]	0.9474
13	[12, 11]	0.9167	13	[23, 22]	0.9565
17	[16, 15]	0.9375	17	[31, 30]	0.9677
19	[18, 17]	0.9444	19	[35, 34]	0.9714
23	[22, 21]	0.9545	23	[43,42]	0.9767
29	[28, 27]	0.9643	29	[55,54]	0.9818



Figures 5, 6, 7 and 8: Code Rate of Cyclic Code of Lengths $\boldsymbol{n = \varphi(p)}$ and $\boldsymbol{2n - 1 = 2\varphi\,(p) - 1}$ for Primes in Proposed Study

Mutual comparison of Lengths and Code Rates of the Cyclic Codes of lengths $\boldsymbol{n = \frac{p-1}{2}}$, $\boldsymbol{2n - 1 = p - 2}$ with $\boldsymbol{n = \varphi(p) = p - 1}$ and $\boldsymbol{2n - 1 = 2\varphi(p) - 1}$ Lengths and Code Rates of Cyclic Codes as:



Figures 9 and 10: Mutual comparison of proposed work with previous existing works

We observed that if the length of the cyclic codes increases due to prime p, then the code rate and error correction capability of C will be better.

6 Conclusions

The following are the contributions of this study for the efficacy of the cyclic codes over Quaternion integers of QM weight. An effective and consistent modified decoding algorithm for the cyclic codes of lengths $n = \varphi(p)$ and $2n - 1 = 2\varphi(p) - 1$ to obtain the error correction capability has been furnished. The length of cyclic codes increased due to large prime p. For a given prime p, a higher code rates for cyclic codes of lengths $n = \varphi(p) = p - 1$ and $2n - 1 = 2p - 3$ is achieved as compared to the code rates of cyclic codes having lengths $n = \frac{p-1}{2}$ and $2n - 1 = p - 2$. The error correction capability of the cyclic codes of lengths $n = \varphi(p) = p - 1$ and $2n - 1 = 2\varphi(p) - 1 = 2p - 3$ has been improved and it is better than the customary case of the cyclic codes of lengths $n = \frac{p-1}{2}$ and $2n - 1 = p$–2.

Furthermore, the decoding procedure on the base of quaternion integers may be extended to the decoding procedure of octonion integers.

Funding Statement: The authors extend their gratitude to the Deanship of Scientific Research at King Khalid University for funding this work through research groups program under grant number R. G. P. 1/85/42.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. Best, "Perfect codes hardly exist," *IEEE Transactions on Information Theory*, vol. 29, no. 3, pp. 349–351, 1983.

[2] V. Lint and H. Jacobus, "Nonexistence theorems for perfect error correcting codes," *Computers in Algebra and Number Theory (Proceedings, New York NY, USA, March 25-26, 1970), SIAM-AMS Proceedings, American Mathematical Society*, vol. 4, pp. 89–95, 1971.

[3] H. J. Conway and N. J. A. Sloane, "Self-dual codes over the integers modulo 4," *Journal of Combinatorial Theory, Series A*, vol. 62, no. 1, pp. 30–45, 1993.

[4] A. Tietavainen, "On the nonexistence of perfect codes over finite fields," *SIAM Journal on Applied Mathematics*, vol. 24, no. 1, pp. 88–96, 1973.

[5] V. A. Zinoviev and V. K. Leontiev, "The nonexistence of perfect codes over Galois fields," *Probl. Control and Inform. Theory*, vol. 2, no. 2, pp. 123–132, 1973.

[6] A. J. Han and H. Morita, "Codes over the ring of integers modulo m," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 81, no. 10, pp. 2013–2018, 1998.

[7] Tamm and Ulrich, "On perfect integer codes," in *Proc. Int. Symp. on Information Theory IEEE*, vol. 9, no. 1, pp. 117–120, 2005.

[8] K. Huber, "Codes over Gaussian integers," *IEEE Transactions on Information Theory*, vol. 40, no. 1, pp. 207–216, 1994.

[9] K. Huber, "The MacWilliams theorem for two-dimensional modulo metrics," *Applicable Algebra in Engineering, Communication and Computing*, vol. 8, no. 1, pp. 41–48, 1997.

[10] T. P. D. N. Neto, T. Pires, J. C. Interlando, O. M. Favareto, M. Elia *et al.,* "Lattice constellations and codes from quadratic number fields," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1514–1527, 2001.

[11] H. Kostadinov, H. Morita and N. Manev, "Derivation on bit error probability of coded QAM using integer codes," *IEICE TRANSACTIONS on Fundamentals of Electronics Communications and Computer Sciences*, vol. 87, no. 12, pp. 3397–3403, 2004.

[12] D. Andrade, A. Aparecido and R. J. Palazzo, "Linear codes over finite rings," *Trends in Computational and Applied Mathematics*, vol. 6, no. 2, pp. 207–217, 2005.

[13] M. Özen and M. Güzeltepe, "Codes over quaternion integers," *European Journal of Pure and Applied Mathematics*, vol. 3, no. 4, pp. 670–677, 2010.

[14] D. Andrade, A. Aparecido, T. Shah and A. Khan, "Cloud Goppa codes through generalized polynomials and its decoding principle," *International Journal of Applied Mathematics*, vol. 23, no. 3, pp. 517–526, 2010.

[15] D. Andrade, A. Aparecido, T. Shah and A. Khan, "A note on linear codes over semigroup rings," *TEMA (São Carlos)*, vol. 12, no. 2, pp. 79–89, 2011.

[16] T. Shah, A. Khan and A. A. Andrade, "Encoding through generalized polynomial codes," *Computational & Applied Mathematics*, vol. 30, no. 2, pp. 349–366, 2011.

[17] T. Shah, A. Khan and A. A. D. Andrade, "Constructions of codes through the semigroup ring B [X; 122Z0] and encoding," *Computers & Mathematics with Applications*, vol. 62, no. 4, pp. 1645–1654, 2011.

[18] M. Özen and M. Güzeltepe, "Cyclic codes over some finite quaternion integer rings," *Journal of the Franklin Institute*, vol. 348, no. 7, pp. 1312–1317, 2011.

[19] M. Güzeltepe and O. Heden, "Perfect Mannheim, Lipschitz and Hurwitz weight codes," *Mathematical Communications*, vol. 19, no. 2, pp. 253–276, 2014.

[20] T. Shah and S. S. Rasool, "On codes over quaternion integers," *Applicable Algebra in Engineering, Communication and Computing*, vol. 24, no. 6, pp. 477–496, 2013.

[21] G. F. Davidoff, P. Sarnak and A. Valette, "Elementary number theory, and Ramanujan graphs," Cambridge University Press, vol. 55, pp. 45–80, 2003.

[22] R. Gilmer, "Commutative semigroup rings," University of Chicago Press, Chicago, London, vol. 22, no. 1, pp. 63–129, 1984.