MATEMATIČKI VESNIK
МАТЕМАТИЧКИ ВЕСНИК
Corrected proof
Available online 18.01.2023

research paper
оригинални научни рад
DOI: 10.57016/MV-etK5277r

CONSTACYCLIC CODES OVER LIPSCHITZ INTEGERS

Murat Güzeltepe, Gökçen Çetinel and Nükhet Sazak

Abstract. In this paper, the goal is to obtain constacyclic codes over Lipschitz integers in terms of Lipschitz metric. A decoding procedure is proposed for these codes, some of which have been shown to be perfect codes. Performance of constacyclic codes over Lipschitz integers is investigated over Additive White Gaussian Channel (AWGN) by means of symbol error rates and coding gain. According to the achieved results, these codes can be used in coded modulation schemes based on Quadrature Amplitude Modulation (QAM)-type constellations. Furthermore, it is shown that the Lipschitz metric is more suitable than Hamming metric and Lee metric for QAM type two dimensional constellations.

1. Introduction

Huber defined the Mannheim distance and the Mannheim weight over Gaussian integers in 1992 [11]. In this study, the author proposed block codes over Gaussian integers constructed for the Mannheim distance which are convenient for QAM signals. The results of the study showed that the Mannheim distance was much better suited for coding over two dimensional signal space than the Hamming distance. Fan and Gao obtained one error-correcting linear codes over algebraic integer rings [7]. In [9], perfect Mannheim, Lipschitz, and Hurtwitz codes are analyzed. The performance of Lipschitz integer constellations for transmission over the AWGN channel by means of the constellation figure of merit and a construction of sets of Lipschitz integers that leads to a better constellation figure of merit compared to ordinary Lipschitz integer constellations were examined in [8]. A partition of the ring into multiplicative cosets of a subgroup of a group of units was used to construct check matrices for 1-perfect codes over Lipschitz integers in [9]. Unlike this study, in [12] the ring has zero divisors was considered. The ring is similar to the ring $\mathbb{Z}_4$, which is the basic ring for the 1-perfect additive codes studied in [4].

This paper is organized as follows. In Section 2, some fundamental algebraic concepts, and the definitions of Lipschitz integers and Lipschitz distance are given.

2020 Mathematics Subject Classification: 94B05, 94B60
Keywords and phrases: Block code; QAM signal constellations; Lipschitz metric.

In Section 3, the construction of codes which are able to correct errors of Lipschitz weight one is discussed. Also, double error correcting codes which have minimum distance four or more are proposed and decoding procedure for these codes is given. In Section 4, constacyclic codes over Lipschitz integers are presented. Finally, Section 5 compares the constacylic codes over Lipschitz integers and codes from Gaussian integers.

2. Lipschitz integers and Lipschitz distance

DEFINITION 2.1 ([5]). The Hamilton Quaternion Algebra over the set of the real numbers ($\mathbb{R}$), denoted by $H(\mathbb{R})$, is the associative unital algebra given by the following representation:
(i) $H(\mathbb{R})$ is the free $\mathbb{R}$ module over the symbols $1, i, j, k$, that is, $H(\mathbb{R}) = \{a_0 + a_1 i + a_2 j + a_3 k : \ a_0, a_1, a_2, a_3 \in \mathbb{R}\}$;

(ii) 1 is the multiplicative identity;

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

(iv) $ij = -ji = k$, $ki = -ik = j$, $jk = -kj = i$.

Let $\mathbb{Z}$ denote the set of all integers. Then, the set Lipschitz integers is defined by $H(\mathbb{Z}) = \{a_0 + a_1 i + a_2 j + a_3 k : \ a_0, a_1, a_2, a_3 \in \mathbb{Z}\}$. The set $H(\mathbb{Z})$ is of the form a subring of real quaternions $H(\mathbb{R})$ under the addition and multiplication. The conjugate of a Lipschitz integer $q = a_0 + a_1 i + a_2 j + a_3 k$ is $q^\star = a_0 - a_1 i - a_2 j - a_3 k$. The norm of q is $N(q) = qq^\star = a_0^2 + a_1^2 + a_2^2 + a_3^2$. The elements $\pm 1, \pm i, \pm j, \pm k$ are units of $H(\mathbb{Z})$. The product of two Lipschitz integers is not commutative in general. If the vector parts of two Lipschitz integers are parallel to each other, then their product is commutative. The vector part of the Lipschitz integer $q = a_0 + a_1 i + a_2 j + a_3 k$ is $a_1 i + a_2 j + a_3 k$.

DEFINITION 2.2 ([5]). (i) A Lipschitz integer q is odd (respectively, even) if $N(q)$ is an odd (respectively, even) rational integer.

(ii) A Lipschitz integer q is prime if q is not a unit in $H(\mathbb{Z})$, and if, whenever $q = q_1 q_2$ in $H(\mathbb{Z})$, then either q_1 or q_2 is a unit.

(iii) Two Lipschitz integers q_1, q_2 are associative if there exist two unit Lipschitz integers θ, θ', such that $q_1 = \theta q_2 \theta'$.

(iv) $\delta \in H(\mathbb{Z})$ is a right-hand divisor of $q_1 \in H(\mathbb{Z})$ if there exists $q_2 \in H(\mathbb{Z})$ such that $q_1 = q_2 \delta$.

LEMMA 2.3 ([5]). *If q is a Lipschitz integer and π is an odd, then, there exist q_1, $\delta \in H(\mathbb{Z})$, such that $q = q_1 \pi + \delta$, $N(\delta) < N(\pi)$.*

DEFINITION 2.4. Let π be an odd. If there exists $\delta \in H(\mathbb{Z})$ such that $q_1 - q_2 = \beta\pi$ then q_1 is right congruent to q_2 modulo π. It is denoted as $q_1 \equiv_r q_2$.

This equivalence relation is well-defined. We can consider the constellations of the Lipschitz integers modulo this equivalence relation, which we denote as $H(\mathbb{Z})_\pi = \{\, q \pmod{\pi} |\ q \in H(\mathbb{Z})\}$ [4].

THEOREM 2.5 ([13]). *Let π be an odd. Then $H(\mathbb{Z})_\pi$ has $N(\pi)^2$ elements.*

DEFINITION 2.6 ([13]). Let $\pi \neq 0$ be a Lipschitz integer. Given $\alpha, \beta \in H(\mathbb{Z})_\pi$, then the distance between α and β is denoted by $d_\pi(\alpha, \beta)$ and defined as $d_\pi(\alpha, \beta) = |a_0| + |a_1| + |a_2| + |a_3|$, where $\alpha - \beta \equiv_r a_0 + a_1 i + a_2 j + a_3 k \pmod{\pi}$, with $|a_0| + |a_1| + |a_2| + |a_3|$ minimum.

LEMMA 2.7 ([13]). *The distance given in above definition is a metric over $H(\mathbb{Z})_\pi$. This distance is called the Lipschitz distance or Lipschitz metric.*

The Lipschitz weight of the element $\gamma = a_0 + a_1 i + a_2 j + a_3 k$ is defined as $|a_0| + |a_1| + |a_2| + |a_3|$ and is denoted by $w_L(\gamma)$, where $\gamma = \alpha - \beta$ with $|a_0| + |a_1| + |a_2| + |a_3|$ minimum.

More information which are related with the arithmetic properties of $H(\mathbb{Z})$ can be found in [5, pp. 57-71].

3. Cyclic codes over Lipschitz integers

In this section, we give one error correcting Lipschitz weight codes, shortly OLEC. The OLEC codes are not perfect.

3.1 One Lipschitz error correcting codes (OLEC)

Let α be an element of $H(\mathbb{Z})_\pi$ such that $\alpha^{p^2-1} = 1$ and let p be a prime in $\mathbb{Z}$, where $\pi = a_0 + a_1 i + a_2 j + a_3 k$ is a prime and in $\mathbb{Z}$, $p = \pi\pi^\star$. By using the element α, the parity check matrix H and the generator matrix G are obtained as follows, respectively:

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

Hence, the one error correcting codes of length $n = \frac{p^2-1}{2}$ 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 error of the Lipschitz weight one. A Lipschitz error of weight one takes on one of the eight values $\pm 1, \pm i, \pm j, \pm k$. We now give a decoding procedure for these codes. Let the received vector $r = c + e$, where the Lipschitz 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 as $S(r) = Hr^{tr}$, where r^{tr} denotes the transpose of the received vector r. The value of the error is computed as $S\alpha^{-l}$, where $l \pmod{n}$ leads

how to find the location of the error. Notice that we first compute the syndrome of the received vector to be decoded. If the syndrome disappears in the powers of the element α, then the associates of the syndrome are to be checked.

We now consider a simple example with regard to the one Lipschitz error correcting codes.

EXAMPLE 3.1. Let $\pi = 2+i+j+k$ and $\alpha = 1-i+j$. Then, we obtain the parity check matrix H by using the primitive element α of $H(\mathbb{Z})_\pi$ as $H = \begin{bmatrix} 1, & \alpha, & \alpha^2, & \dots & \alpha^{23} \end{bmatrix}$.

Let the received vector r be $\begin{pmatrix} -1-j, & 1, & 0 & , \dots, & 0 \end{pmatrix}$. Then the syndrome S of r is $S(r) = Hr^{tr} = -i = -i\alpha^0$. This shows that the location of the error is found $0 \equiv 0 \pmod{24}$ and the value of the error is $S\alpha^0 = -i$. So, the received vector r is corrected as $c = r - e = \begin{pmatrix} -1+i-j, & 1, & 0, & \dots & ,0 \end{pmatrix}$. This code is not a perfect code since it does not satisfy the sphere packing bound given in [10, p. 48].

4. Constacyclic codes over Lipschitz integers

The purpose of this section is to define constacyclic codes over $H(\mathbb{Z})_\pi$ obtained from Lipschitz integers. The definitions of these codes depend on the cardinality of the group of units in $H(\mathbb{Z})$. Berlekamp's definition [2] can be used to define the constacyclic codes over algebraic numbers.

DEFINITION 4.1. A linear code C over $H(\mathbb{Z})_\pi$ is said to be a constacyclic code or a θ-cyclic code if, whenever a codeword $c_0, c_1, \dots, c_{n-1}$ is in C, then so is $(\theta c_{n-1}, c_0, \dots, c_{n-2})$, where θ is some element of the set $\{\pm i, \pm j, \pm k\}$.

4.1 One Lipschitz error correcting constacyclic codes (OLECC)

Let α be an element of $H(\mathbb{Z})$ such that $\alpha^{(p^2-1)/8} = \pm i, \pm j, \pm k$, where p is a prime in $\mathbb{Z}$, $\pi = a_0 + a_1 i + a_2 j + a_3 k$ is a Lipschitz prime, and $p = \pi\pi^\star$. The null-space C of the parity-check matrix $H = \begin{pmatrix} 1, & \alpha, & \alpha^2, & \cdots, & \alpha^{(p^2-1)/8-1} \end{pmatrix}$ is a one Lipschitz error correcting constacyclic code (OLECC).

An OLECC code C of length $n = \frac{p^2-1}{8}$ is able to correct any error of Lipschitz weight one. A code that attains the sphere packing bound is said to be a perfect code. Let $[n, k, 3]$ denote a linear code C of length n and minimum distance 3 over a ring or field with p^2 elements, then, the sphere packing bound is calculated as $p^{2n} \geq p^{2k} + p^{2k} tn$, where k denotes the dimension of the code C and t denotes the number of errors which Lipschitz weight is one. The dimension of an OLECC code is $n-1$. In Lipschitz metric, $t = 8$. It is important that an OLECC code is perfect since it satisfies the sphere packing bound. Take an OLECC code with parameters $[n, k, 3]$, then we have $p^{2k} + p^{2k} tn = p^{2(n-1)} + p^{2(n-1)} 8\frac{p^2-1}{8} = p^{2n}$.

EXAMPLE 4.2. Let $\pi = 2 + i + j + k$ and $\alpha = 1 + i$. Then, we obtain the parity check matrix H as $H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \end{pmatrix}$. Let the received vector r be

$\big(1+i-k,\ \ 1,\ \ 1,\ \ j,\ \ 0,\ \ 0\big)$. Then, the syndrome S of r computes as $S(r) = rH^{tr} = 3+i-j+k \equiv -i+k \pmod{\pi} = j\alpha^3$. Hence, we obtain the corrected vector as $c = r - e = (1+i-k,\ 1,\ 1,\ 0,\ 0,\ 0)$. The powers of α are given in Table 1. This $[6,5,3]$ code is able to correct any error of the Lipschitz weight one. The number of all words is $(7^2)^6 = 7^{12}$, the number of all codewords is $(7^2)^5 = 7^{10}$ and the number of words having one Lipschitz error is equal to the product of 48 and 7^{10}. It is clear that the $[6,5,3]$ code is perfect.

4.2 Double error correcting constacyclic codes

Let $p = 4n+1 \geq 17$ be a prime in $\mathbb{Z}$ which is factored as $\pi\overline{\pi}$, where π is a prime in $H(\mathbb{Z})$. Let γ denote an element of $H(\mathbb{Z})_\pi$ of order $4n$. We consider the code C defined by the following parity check matrix H:

$$H = \begin{pmatrix} \gamma^0 & \gamma^1 & \cdots & \gamma^{n-1} \\ \gamma^0 & \gamma^5 & \cdots & \gamma^{5(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma^0 & \gamma^{4t+1} & \cdots & \gamma^{(4t+1)(n-1)} \end{pmatrix},$$

where $t < n$ is a nonnegative integer. A word $c = (c_0, c_1, \ldots, c_{n-1}) \in H(\mathbb{Z})_\pi^n$ is a codeword of C if and only if $cH^{tr} = 0$. If $c(x) = \sum_{r=0}^{n-1} c_r x^r$ is a code polynomial, we get $c(\gamma^{4s+1}) = 0$, for $s = 0, 1, \ldots, t$. The polynomial $g(x) = (x-\gamma)(x-\gamma^5)\ldots(x-\gamma^{4t+1})$ is the generator polynomial of C, and $C = \langle g(x)\rangle$ is a (left or right) ideal of $H(\mathbb{Z})_\pi[x]/\langle x^n+1\rangle$. If multiplying the code polynomial $c(x)$ by $x (\text{mod } (x^n+1))$, we get $xc(x) = c_0x + c_1x^2 + \ldots + c_{n-1}x^{n-1}$. But we known that $x^n = \pm i, \pm j, \pm k$. It is shown that these codes belong to the class of constacyclic codes. If $c(x) \in C$, then $xc(x) \in C$. Thus, multiplying $c(x)$ by x (mod (x^n+1)) means the shifting of $c(x)$ cyclically one position to the right.

THEOREM 4.3. *Let C be the code defined by above parity check matrix H. Then, C is able to correct some error pattern of the form $e(x) = e_s x^s + e_t x^t$, where $0 \leq w_L(e_s), w_L(e_s) \leq 1$.*

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 $0 \leq w_L(e_1), w_L(e_2) \leq 1$. We compute the syndrome S of r as $S(r) = rH^{tr} = (s_1,\ s_5)$. Since the product of the powers of γ must be commutative, we change from the syndromes $s_1,\ s_2$ to the syndromes $\theta_1 s_1', \theta_1 s_5'$, respectively, where $\theta_1 \in \{1, i, j, k\}$. The polynomial $\sigma(z)$, which helps us to find the locations of the errors and the values of the errors, is computed as follows: $\sigma(z) = (z-\gamma^{l_1})(z-\gamma^{l_2}) = z^2 - s_1'z + \varepsilon$, where ε is determined from the syndromes. From $s_1' = \gamma^{l_1} + \gamma^{l_2}$, $s_5' = \gamma^{5l_1} + \gamma^{5l_2}$ and $\varepsilon = \gamma^{l_1+l_2}$, we get

$$\varepsilon^2 - (s_1')^2\varepsilon + \frac{(s_1')^5 - s_5'}{5s_1'} = 0.$$

Thus, the roots of the polynomial $\sigma(z)$ lead us to find the locations of the errors and their values. If γ^{l_1}, γ^{l_2} are the roots of the polynomial $\sigma(z)$, then the locations of the

errors are $l_1 \pmod n$ with the value $\theta_1\beta^{l_1}/\beta^{l_1(\bmod n)}$ and $l_2 \pmod n$ with the value $\theta_1\beta^{l_2}/\beta^{l_2(\bmod n)}$. Hence, we can distinguish three situations:

(i) No error: $s_1' = s_5' \bmod \pi$.

(ii) One error: $(s_1')^5 = s_5' \neq 0$.

(iii) Two errors: $(s_1')^5 \neq s_5'$ and $s_1' \neq 0$. □

EXAMPLE 4.4. Let $\pi = 4 + k$ and let $\gamma = 1 + k$. Let C be the code defined by the parity check matrix

$$H = \begin{pmatrix} \gamma^0 & \gamma^1 & \gamma^2 & \gamma^3 \\ \gamma^0 & \gamma^5 & \gamma^{10} & \gamma^{15} \end{pmatrix}.$$

The powers of γ are shown in Table 2. Let the received vector r be $(-2,\ -2k,\ 1-i,\ i)$. We now apply the decoding procedure for the code in Theorem 4.3.

(i) Calculating the syndrome: $S(r) = rH^{tr} = \begin{pmatrix} -2i, & -i+j \end{pmatrix} \pmod \pi$. Take $\theta_1 = i$. One can verify that $(s_1')^5 \neq s_5'$, which shows that two errors have occurred.

(ii) Using the formula

$$\varepsilon^2 - (s_1')^2\varepsilon + \frac{(s_1')^5 - s_5'}{5s_1'} = 0 \ \Rightarrow\ (1+2k)\,\varepsilon^2 + k\,(1+2k)\,\varepsilon + 1 = 0 \pmod \pi$$

we obtain $\varepsilon = 1 - k \pmod \pi$ and the roots of the polynomial $\sigma(z)$ are γ^3, γ^{10} (see Table 4). Therefore, the locations of the errors are $l_1 = 3 \equiv 3 \pmod 4$ with the value $\theta_1\gamma^3/\gamma^3 = i$ and $l_2 = 2 \equiv 10 \pmod 4$ with the value $\theta_1\gamma^{10}/\gamma^2 = -i$. Hence, we obtain the corrected vector $c = r - e = (-2,\ -2k,\ 1,\ 0)$.

THEOREM 4.5. *Let $p = 6n + 1 \geq 31$ be a prime and γ be an element of $H(\mathbb{Z})_\pi$ with order $6n$. The code C having the following parity check matrix:*

$$H = \begin{pmatrix} 1 & \gamma & \gamma^2 & \dots & \gamma^{n-1} \\ 1 & \gamma^7 & \gamma^{14} & \dots & \gamma^{7(n-1)} \\ 1 & \gamma^{13} & \gamma^{26} & \dots & \gamma^{13(n-1)} \\ 1 & \gamma^{19} & \gamma^{38} & \dots & \gamma^{19(n-1)} \end{pmatrix},$$

can correct any error pattern of the form $e(x) = e_s x^s + e_t x^t$, where $0 \leq w_L(e_s), w_L(e_t) \leq d_{max}$. Here, we define d_{max} as $d_{max} = \max\{\, w_L(q) |\ q \in H(\mathbb{Z})\}$.

Proof. Let we receive the vector $r = c + e$. Let two errors occur at different locations l_1, l_2. Then syndrome of r is

$$S(r) = (rH^{tr})^{tr} = \begin{pmatrix} S_1 \\ S_7 \\ S_{13} \\ S_{19} \end{pmatrix} = \begin{pmatrix} \gamma^{L_1} + \gamma^{L_2} \\ \gamma^{7L_1} + \gamma^{7L_2} \\ \gamma^{13L_1} + \gamma^{13L_2} \\ \gamma^{19L_1} + \gamma^{19L_2} \end{pmatrix},$$

where $l_1{=}L_1 \pmod n$ and $l_2{=}L_2 \pmod n$. Let $\theta_t \in \{\pm 1, \pm i, \pm j, \pm k\}$ for $0{\leq}t{\leq}8$. Consider $S'(r)$

$$S'(r) = \begin{pmatrix} S'_1 \\ S'_7 \\ S'_{13} \\ S'_{19} \end{pmatrix} = \begin{pmatrix} \theta_1 S_1 \theta_2 \\ \theta_3 S_7 \theta_4 \\ \theta_5 S_{13} \theta_6 \\ \theta_7 S_{19} \theta_8 \end{pmatrix}$$

Here, the syndromes $S'_1, S'_7, S'_{13}, S'_{19}$ equal to some of the power of γ. From the syndromes and $\epsilon = \gamma^{L_1+L_2}$ we get

$$\begin{aligned} S'_1 S'_{13} - (S'_7)^2 &= \epsilon Z^2 - 4\epsilon^7, \\ S'_1 S'_{19} - S'_7 S'_{13} &= \epsilon Z^3 - 4\epsilon^7 Z, \\ S'_7 S'_{19} - (S'_{13})^2 &= \epsilon^6 (Z^2 - 4\epsilon^7), \end{aligned}$$

where $Z = \gamma^{L_1} + \gamma^{6L_2}$. Using these equations, we have

$$Z = \frac{S_1{}' S_{19}{}' - S_7{}' S_{13}{}'}{S_1{}' S_{13}{}' - (S_7{}')^2}, \quad \epsilon = \frac{S_7{}' S_{19}{}' - (S_{13}{}')^2}{S_1{}' S_{13}{}' - (S_7{}')^2}.$$

The roots of the equation $x^2 - Zx + \epsilon^6 = 0$ give the locations and the values of errors. □

5. Comparison between constacyclic codes from Lipschitz integers and codes from Gaussian integers

In this section, the codes over $H(\mathbb{Z})_\pi$ and codes over Gaussian integers presented in [11] are compared in terms of coding gain and symbol error probability, when the alphabets being considered have the same cardinality. Gaussian integers $\mathbb{Z}[i]$ forms a square lattice. Figure 1 shows the complex plane and square points in Figure 1 are the elements of the set $\mathbb{Z}[i]_{2+i} = \{0, \pm 1, \pm i\}$.

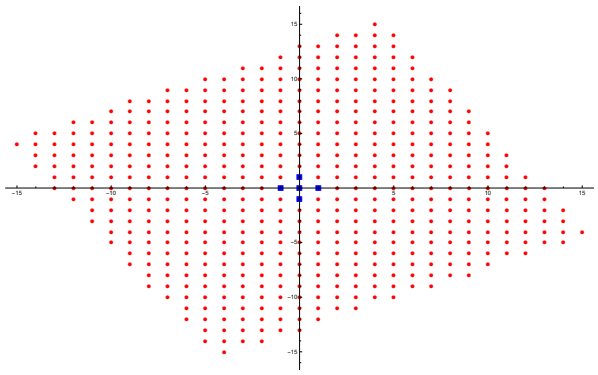

Figure 1: Gaussian integers form a square lattice

Lipschitz integers $H(\mathbb{Z})$ also form a lattice. Each Lipschitz integer is represented in four dimensions. Figure 2 demonstrates some Lipschitz integers. In Figure 2, big points represent the set $H(\mathbb{Z})_{1+i+j} = \{0, \pm 1, \pm i, \pm j, \pm k\}$. To better understand Figure 2, we give only one point $0 = 0 + 0i + 0j + 0k = (0, 0, 0, 0)$ in Figure 3, and two points $0 = 0 + 0i + 0j + 0k = (0, 0, 0, 0)$ and $1 = 1 + 0i + 0j + 0k = (1, 0, 0, 0)$ in Figure 4, respectively. In Figure 4, big points represent Lipschitz integer 0 and small points represent Lipschitz integer 1.

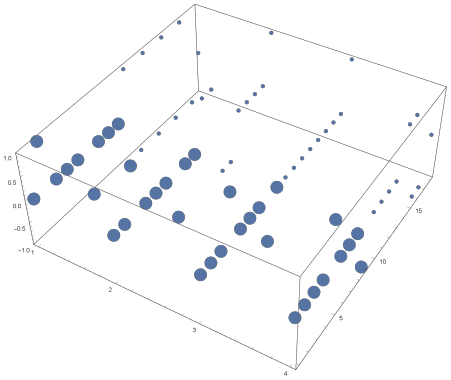

Figure 2: Lipschitz integers form a lattice

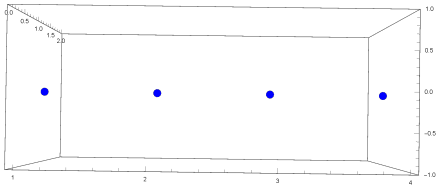

Figure 3: One point $0 = 0 + 0i + 0j + 0k = (0, 0, 0, 0)$

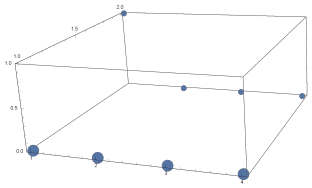

Figure 4: Two points $0 = 0 + 0i + 0j + 0k = (0, 0, 0, 0), 1 = 1 + 0i + 0j + 0k = (1, 0, 0, 0)$

A basic communication system consits of three components: modulator, communication channel, and demodulator. In this paper, Binary Shift Keying (BPSK) and Quadriphase Shift Keying (QPSK) digital modulation schemes are considered to investigate the performance of the proposed codes. BPSK is a digital communication

scheme in which data is transmitted over a communication channel by changing the phase of a carrier. The BPSK waveform contains phase shift of $\pm pi$ radians. In other words, the modulation occurs by varying the sine and cosine inputs at a precise time. The constellation points of BPSK are usually located at uniform angular spacing around a circle. In this way, maximum phase separation between adjacent points are achieved and noise immunity is increased. BPSK is widely used in wireless Local Area Networks (LANs), Radio Frequency Identification (RFID) and Bluetooth communications. QPSK is also a phase modulation scheme in which two information bits are modulated at once, selecting one of four possible carrier phase shift states. QPSK has four constellation points equispaced around the circle and is utilized for satellite transmission of MPEG2 video, cable modems, video conferencing, cellular phone systems and other forms of digital communication over an RF carrier [6, 15].

The performance of the coding schemes for digital communication systems can be compared with commonly used criteria. Two of these criteria are coding gain and symbol error probability. Coding gain is a significant criterion to evaluate the performance of coding schemes. It can be defined as the difference between Signal-to-Noise Ratio (SNR) levels of the uncoded system and coded system required to the same Bit Error Rate (BER) levels. Coding gain, usually given in decibels, represents the improvement for a coding scheme and is a function of minimum distance and code rate. For a given code, the best code is the code which provides the highest minimum distance [14]. BER is also an important evaluation parameter for digital communication channels that measures the amount of errors will appear in the data at the receiver end of the communication system. It can be expressed as the ratio of the number of errors to the total number of transmitted bits.

$\alpha^0 = 1$	$\alpha^1 = 1 + i$	$\alpha^2 = 1 - j + k$
$\alpha^3 = -i - k$	$\alpha^4 = -i - j$	$\alpha^5 = i + j$
$\alpha^6 = -i$	$\alpha^7 = \alpha\alpha^6$	$\alpha^8 = \alpha^2\alpha^6$

Table 1: Powers of the element $\alpha = 1 + i$ which is root of $x^6 + i$

$\gamma^0 = 1$	$\gamma^1 = 1 + k$	$\gamma^2 = 2k$	$\gamma^3 = -1 - 2k$	$\gamma^4 = k$

Table 2: Powers of the element $\gamma = 1 + k$ which is root of $x^4 - k$

In this section, various tables and figures are prepared to explain the advantages of the proposed codes over AWGN channels. Table 3 provides data about the signal energy per symbol E_s, the energy per bit $E_b = \frac{E_s}{Log_2 p^2}$, and the BPSK/QPSK reference value $10 \log (4E_b)$ [8]. The reference value must be subtracted from the coding gain to see the improvement over BPSK/QPSK as given in Example 5.1. Furthermore, Table 4 demonstrate coding gains achieved by the proposed constacyclic codes over Lipschitz integers for different p values under BPSK/QPSK modulation scenarios. Improvement values given in Table 4 are calculated by substracting the reference

values (Table 3 the last column) from obtained coding gains for different p values. In the following example, we explain the calculation of coding gain that is used to construct Table 4.

p	π	E_s	E_b	$10\log(4E_b)$
7	$2+i+j+k$	2.9388	0.523	3.2056 dB
13	$2+2i+2j+k$	4.4308	0.582	3.670 dB
17	$4+i$	5.6480	0.691	4.414 dB
29	$5+2i$	9.6560	0.994	5.993 dB
37	$6+i$	12.324	1.183	6.75 dB
41	$5+4i$	13.658	1.275	7.075 dB
53	$7+2i$	17.660	1.542	7.9 dB
61	$6+5i$	20.328	1.714	8.36 dB
73	$8+3i$	24.328	1.956	8.955 dB
89	$8+5i$	29.662	2.290	9.62 dB

Table 3: E_s,E_b,$10\log(4E_b)$ table for the proposed codes

p	Coding Gain	Improvement
7	9.834 dB	6.628 dB
13	11.005 dB	7.335 dB
41	14.504 dB	7.429 dB

Table 4: The coding gain and improvement

EXAMPLE 5.1. Consider $[20, 7, d_H = 11]$ Reed-Solomon code with respect to Hamming metric over $GF(7)$ [1] and the $[6, 5, 3]$ OLECC code over $\pi = 2+i+j+k$ that leads to a coding gain of $G = 10\log\left(\frac{7}{20}\,\frac{5}{6}\,33\right) = 9.834$ dB.

Note that, we should subtract $10\log(4E_b)$=3.2056 dB from obtained coding gain to exhibit the improvement. According to the achieved value, we can say that the proposed coding provides about 6.628 dB improvement on coding gain for $p = 7$ (see Table 4, first row). In general, the improvement attained by the proposed coding method is between [6 dB-10 dB].

In addition to the coding gain, bit or symbol error probability can be referred as another criterion to evaluate the performance of digital communication systems. For a fixed bit or symbol error rate, SNR difference between two coding schemes indicates the achievement of the scheme that provides lower error rate [3]. As can be seen from Figure 3, the proposed coding scheme gives lower SNR values in comparison with the coding method investigated in reference [11]. To plot Figure 3, SNR values are varied in [−5 dB,−20 dB] interval and the corresponding P_s values are calculated by using the equations given in reference [14].

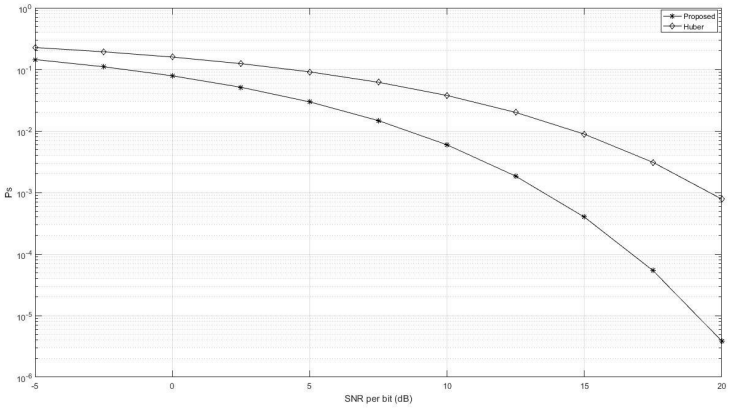

Figure 5: Symbol error rates versus SNR values for transmission over AWGN channel for $p = 61$ in comparison with Reference [11]

Acknowledgement. The work was supported by TÜBİTAK (The Scientific and Technical Research Council of TURKEY) with project number 116F318.

The authors wish to thank the associate editor and two anonymous referees whose comments have greatly improved this paper.

References

[1] N. Aydın, D. Foret, *New linear codes over $GF(3), G(11)$ and $GF(13)$*, J. Algebra Comb. Discrete Struct. Appl., **6(1)** (2018), 13–20.

[2] E. R. Berlekamp, *Algebraic Coding Theory*, Laguna Hills, CA: Aegean park, 1984.

[3] V. K. Bhargava, Q. Yang, D. J. Peterson, *Coding theory and its applications in communication systems*, Def. Sci. J., **43(1)** (1993), 59–69.

[4] J. Borges, J. Rifà, *A characterization of 1-perfect additive codes*, IEEE Trans. Inf. Theory, **45(5)** (1999), 1688–1697.

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

[6] R. P. Devi, H. Nishat, *Performance Evaluation of Digital Modulation Schemes BPSK, QPSK and QAM*, Int. J. Eng. Tech., **3(2)** (2017), 71–74.

[7] Y. Fan, Y. Gao, *Codes Over algebraic integer rings of cyclotomic fields*, IEEE Trans. Inform. Theory, **50(1)** (2004).

[8] J. Freudenberger, S. Shavgulidze, *New four-dimensional signal constellations from Lipschitz integers for transmission over the Gaussian channel*, IEEE IEEE Trans. Comm., **63(7)** (2015).

[9] M. Güzeltepe, O. Heden, *Perfect Mannheim, Lipschitz and Hurwitz weight codes*, Math. Commun., **19(2)** (2014), 253–276.

[10] W. C. Huffman, V. Pless, *Fundamentals of Error Correcting Codes*, Cambridge Unv. Press., 2003.

[11] K. Huber, *Codes over Gaussian integers*, IEEE Trans. Inform.Theory, **40** (1994), 207–216.

[12] D. S. Krotov, *Perfect codes in Doob graphs*, Des. Codes Cryptogr., **80** (2016), 91–102.

[13] C. Martinez, E. Stafford, R. Beivide, E. Gabidulin., *Perfect codes over Lipschitz integers*, IEEE Int. Symposium on Information Theory, ISIT'07, 2007.

[14] J. G. Proakis, M. Salehi, *Communication Systems Engineering*, Prentince Hall, New Jersey, 2002.

[15] J. G. Proakis, M. Salehi, *Digital Communications, McGraw Hill*, International Edition, 2008.

(received 20.08.2021; in revised form 20.03.2022; available online 18.01.2023)

Department of Mathematics, Sakarya University, Turkey

E-mail: mguzeltepe@sakarya.edu.tr

Department of Electirical and Electronics Engineering, Faculty of Engineering, Sakarya University, Turkey

E-mail: gcetinel@sakarya.edu.tr

Department of Electirical and Electronics Engineering, Faculty of Engineering, Sakarya University, Turkey

E-mail: nsazak@sakarya.edu.tr