https://dergipark.org.tr/pub/jum

Journal of Universal Mathematics

Vol.8 No.2 pp. 93-103 (2025)
DOI:10.33773/jum.1654134
ISSN-2618-5660

On the Cyclic and λ-Constacyclic Codes over the Quaternion Rings and Their Applications

Abdullah Dertli
abdullah.dertli@omu.edu.tr
Department of Mathematics, Ondokuz Mayis University, Samsun, Turkey

Yasemin Cengellenmis
ycengellenmis@gmail.com
Department of Mathematics, Trakya University, Edirne, Turkey

Article Information

Keywords
Quaternion ring
Quantum codes
Cyclic codes
Constacyclic codes

Dates
Received: 09.03.2025
Accepted: 29.09.2025

AMS Classification
94B05, 94B15, 81P70, 11R52

Abstract

In this paper, the structures of linear codes over the quaternion rings with coefficient from Z_p, $H_p = Z_p + Z_p i + Z_p j + Z_p k$ are given, where p is an odd prime, $i^2 = j^2 = k^2 = p - 1$ and $ij = (p-1)ji = k$. The quaternion rings over Z_p decompose into two parts form $Z_p + iZ_p$(or $Z_p + jZ_p$ or $Z_p + kZ_p$) with idempotent coefficients, depending on selecting a central orthogonal idempotent pair. The structures of cyclic and λ-constacyclic codes over H_p are determined, where $p \equiv 3(mod\ 4)$, p is an odd prime, λ is a unit in H_p and some examples are given. The duals of linear codes over H_p are investigated. The parameters of quantum codes are obtained from cyclic codes and λ-constacyclic over H_p.

1 Introduction

W. R. Hamilton invented quaternions in 1843. Firstly, W. B. V. Kandasamy introduced quaternion rings over Z_p in (Kandasamy, 2000). In (Aristidou & Demetre, 2012), (Miguel & Serodio, 2011), (Tan & Sison, 2021) some properties of these rings were investigated by many authors. In (Akbiyik & Ersoy 2017), cyclic codes over H_3 were determined. Their generator polynomials were given, and their parameters were obtained. Motivated by this work (Akbiyik & Ersoy 2017), we decided to study cyclic and $\lambda-$constacyclic codes over H_p and to obtain their applications to quantum codes.

The paper is organized as follows. In section 2, the structures of quaternion rings over Z_p and some properties are given. In section 3, the structure of a linear code over H_p is determined. In sections 4 and 5, the structures of cyclic and λ-constacyclic codes over H_p are obtained, respectively. Some examples are given. In section 6, dual codes over H_p are investigated. In section 7, the parameters of quantum codes from cyclic codes and λ-constacyclic over H_p are obtained. Some examples are given.

2 Preliminaries

In (Kandasamy, 2000), the non-commutative ring with p^4 elements $H_p = \{a + bi + cj + dk | a, b, c, d \in Z_p, i^2 = j^2 = k^2 = p - 1, ij = (p-1)ji = k\}$ were introduced by Kandasamy, where p is a prime and $Z_p = \{0, 1, ..., p-1\}$.

The sum and left(right) product operations were defined in (Akbiyik & Ersoy 2017) for H_3. Similarly, they can be defined for H_p as follows:

$$\begin{aligned} + \quad &: \quad H_p \times H_p \longrightarrow H_p \\ (z,m) \quad &\mapsto \quad z+m=(a_1+a_2)+(b_1+b_2)i+(c_1+c_2)j+(d_1+d_1)k \end{aligned}$$

$$\begin{aligned} *_L \quad &: \quad H_p \times H_p \longrightarrow H_p \\ (z,m) \quad &\mapsto \quad z*_L m=(a_1a_2+(p-1)b_1b_2+(p-1)c_1c_2+(p-1)d_1d_2)+ \\ &\qquad (a_1b_2+b_1a_2+c_1d_2+(p-1)d_1c_2)i+ \\ &\qquad (a_1c_2+c_1a_2+d_1b_2+(p-1)b_1d_2)j+ \\ &\qquad (a_1d_2+d_1a_2+b_1c_2+(p-1)c_1b_2)k \end{aligned}$$

$$\begin{aligned} *_R \quad &: \quad H_p \times H_p \longrightarrow H_p \\ (z,m) \quad &\mapsto \quad z*_R m=(a_1a_2+(p-1)b_1b_2+(p-1)c_1c_2+(p-1)d_1d_2)+ \\ &\qquad (a_1b_2+b_1a_2+(p-1)c_1d_2+d_1c_2)i+ \\ &\qquad (a_1c_2+c_1a_2+(p-1)d_1b_2+b_1d_2)j+ \\ &\qquad (a_1d_2+d_1a_2+(p-1)b_1c_2+c_1b_2)k \end{aligned}$$

where $z=a_1+b_1i+c_1j+d_1k, m=a_2+b_2i+c_2j+d_2k \in H_p$.
In this paper, we use the left product as an operation for the non commutative ring with unity and denote $*$ instead of $*_L$.
In (Miguel & Serodio, 2011), the structure of the quaternion ring over Z_p was determined, where p is an odd prime. It was constructed as an isomorphism between the ring H_p and the ring of square matrices of order two over the finite field Z_p. Thanks to the relationship between the ring H_p and the ring $M_2(Z_p)$ and by using the Theorem 3.1. in (Cheraghpour & Ghosseiri, 2019), it can be given the number of units, zero divisors, idempotent elements of the ring H_p as follows:

Theorem 2.1. *(Cheraghpour & Ghosseiri, 2019) The number of units in H_p is*

$$U=p(p-1)(p^2-1)$$

Theorem 2.2. *(Cheraghpour & Ghosseiri, 2019) Let p be an odd prime number. Then, the number of zero divisors in H_p is*

$$Z=p^3+p^2-p-1$$

Theorem 2.3. *(Cheraghpour & Ghosseiri, 2019) Let p be an odd prime number. The number of idempotent elements in H_p is*

$$I=p^2+p+2$$

Theorem 2.4. *(Aristidou & Demetre, 2012) If $h=a+bi+cj+dk \in H_p$ is idempotent, then $a=(p+1)/2, b^2+c^2+d^2 \equiv (p^2-1)/4(mod\ p)$.*

Example 2.5. For the idempotent element $h=a+bi+cj+dk \in H_3, a=2, b^2+c^2+d^2 \equiv 2(\ \mathrm{mod}\ 3)$. For $h \in H_5, a=3, b^2+c^2+d^2 \equiv 1(\ \mathrm{mod}\ 5)$. For $h \in H_7, a=4, b^2+c^2+d^2 \equiv 5(\ \mathrm{mod}\ 7)$.

There are $(p^2+p)/2$ idempotent pairs such that they are orthogonal and their sum is 1. They are called

central orthogonal idempotent pairs. If the idempotent element is $h = a + bi + cj + dk \in H_p$, where $a = (p+1)/2, b^2 + c^2 + d^2 \equiv (p^2-1)/4 (\text{mod } p)$, then its pair is $a + (p-b)i + (p-c)j + (p-d)k$.

Example 2.6. In H_5, there are 15 central orthogonal idempotent pairs. These are $\{3+2i+j+4k, 3+3i+4j+k\}, \{3+i, 3+4i\}, \{3+j, 3+4j\}, \{3+k, 3+4k\}, \{3+i+4j+2k, 3+4i+j+3k\}, \{3+4i+2j+k, 3+i+3j+4k\}, \{3+4i+j+2k, 3+i+4j+3k\}, \{3+2i+4j+k, 3+3i+j+4k\}, \{3+i+2j+4k, 3+4i+3j+k\}, \{3+i+j+2k, 3+4i+4j+3k\}, \{3+i+2j+k, 3+4i+3j+4k\}, \{3+2i+j+k, 3+3i+4j+4k\}, \{3+i+j+3k, 3+4i+4j+2k\}, \{3+3i+j+k, 3+2i+4j+4k\}, \{3+i+3j+k, 3+4i+2j+4k\}$.

Theorem 2.7. *(Tan & Sison, 2021) Let H_q be the ring of the quaternions over the finite field F_q, where $q = p^r (\text{odd } p)$. Then H_q is a semisimple ring with $q+1$ proper left(resp. right) ideals and each proper left(resp. right) ideal is principal, minimal and maximal and has q^2 elements.*

Result 2.8. *The quaternion ring over Z_p is a principal ideal ring. Moreover, it is not a finite chain ring.*

Proposition 2.1. Let $h_1 = (p+1)/2 + b_1 i + c_1 j + d_1 k$ be an idempotent element in H_p and $h_2 = (p+1)/2 - b_1 i - c_1 j - d_1 k$ be idempotent pair of h_1, where p is an odd prime. Then every element $h \in H_p$ is uniquely written as $h = h_1 * z_1 + h_2 * z_2$ where $z_1, z_2 \in Z_p + iZ_p$ (or $Z_p + jZ_p$ or $Z_p + kZ_p$) depending on the choice of central orthogonal idempotent pair $\{h_1, h_2\}$.

Proof. Let $h = a + bi + cj + dk$ be an element in H_p. Suppose that $h = h_1 * z_1 + h_2 * z_2$, where $z_1 = e_1 + if_1, z_2 = e_2 + if_2 \in Z_p + iZ_p$ depending on the choice of central orthogonal idempotent pairs $\{h_1, h_2\}$. As $\{h_1, h_2\}$ is the central orthogonal idempotent pair, then $h_s * h_s = h_s$, $h_s * h_t = 0$, where $s, t = 1, 2$, $s \neq t$. By using them, we have $h_1 * h = h_1 * z_1$ and $h_2 * h = h_2 * z_2$. From them, we can obtain $e_1, e_2, f_1, f_2 \in Z_p$, by solving these equations. For the uniqueness; For $h \in H_p$, assume that the element h is written in two different ways as $h = h_1 * z_1 + h_2 * z_2 = h_1 * m_1 + h_2 * m_2$. From this, we have $h_1 * (z_1 + (p-1)m_1) = h_2 * ((p-1)z_2 + m_2)$. By multiplying h_1, we have $z_1 = m_1$, as $h_1 * h_1 = h_1, h_1 * h_2 = 0$. By multiplying h_2, we have $z_2 = m_2$, as $h_2 * h_2 = h_2, h_2 * h_1 = 0$.
The proof is similar to the others depending on the choice of central orthogonal idempotent pairs. □

For the different central orthogonal idempotent pairs, different elements z_1, z_2 are obtained.

Example 2.9. In H_5, $3 + 2i + 3j + 4k \in H_5$ is uniquely written as $3 + 2i + 3j + 4k = (3 + 2i + j + 4k) * 2 + (3 + 3i + 4j + k) * i$ according to the pair$\{3 + 2i + j + 4k, 3 + 3i + 4j + k\}$. But $3 + 2i + 3j + 4k \in H_5$ is uniquely written as $3 + 2i + 3j + 4k = (3 + 3i + j + k) * 2 + (3 + 2i + 4j + 4k) * (1 + 3i)$ according to the pair $\{3 + 3i + j + k, 3 + 2i + 4j + 4k\}$.

Proposition 2.2. Let $h_1 = (p+1)/2 + b_1 i + c_1 j + d_1 k$ be an idempotent element and h_2 be its pair. If $b_1 \neq 0, c_1 = 0, d_1 = 0$, then H_p can be decomposed into $(Z_p + jZ_p) \oplus (Z_p + jZ_p)$ (or $(Z_p + kZ_p) \oplus (Z_p + kZ_p)$). If $b_1 = 0, c_1 \neq 0, d_1 = 0$, then H_p can be decomposed into $(Z_p + iZ_p) \oplus (Z_p + iZ_p)$ (or $(Z_p + kZ_p) \oplus (Z_p + kZ_p)$). If $b_1 = 0, c_1 = 0, d_1 \neq 0$, then H_p can be decomposed into $(Z_p + iZ_p) \oplus (Z_p + iZ_p)$ (or $(Z_p + jZ_p) \oplus (Z_p + jZ_p)$). In the other case, H_p can be decomposed into any of them. Moreover, H_p is a $Z_p + iZ_p$ (or $Z_p + jZ_p$ or $Z_p + kZ_p$)-right module depending on the choice of central orthogonal idempotent pairs $\{h_1, h_2\}$.

In this paper, we will consider that H_p is decomposed into $(Z_p + iZ_p) \oplus (Z_p + iZ_p)$. Similar things can be done for the others.

Remark. If $p \equiv 3 (\text{mod } 4)$, then $x^2 \equiv -1 \pmod{p}$ has no solution. So $x^2 + 1 \in Z_p[x]$ is irreducible. Hence, $Z_p + iZ_p$ is a field.

Proposition 2.3. The field F_{p^2} is isomorphic to $Z_p + iZ_p \cong Z_p[x]/ < x^2 + 1 >$, for $p \equiv 3 (\text{mod } 4)$.

Proof. Let $f(x)$ be second degree primitive polynomial over F_p and w be primitive element of F_{p^2}, that is $f(w) = 0$. For every second degree primitive polynomials $f(x)$, by determining $s, t \in F_p$ which satisfy $(sw + t)^2 \equiv -1$ (mod p), it is easily seen that the map ψ from $Z_p + iZ_p$ to F_{p^2} with $\psi(i) = sw + t$, or $\psi(s^{-1}i - s^{-1}t) = w$, is an isomorphism. □

Example 2.10. For $p = 7$, there are $\phi(7^2 - 1)/2 = 8$ second degree primitive polynomials, where ϕ is Euler function. They are $w^2 + 6w + 3, w^2 + 2w + 5, w^2 + 3w + 5, w^2 + 5w + 3, w^2 + w + 3, w^2 + 2w + 3, w^2 + 4w + 5, w^2 + 5w + 5$. The isomorphisms are $\psi(i-3) = w, \psi(5i-1) = w, \psi(i-5) = w, \psi(3i+1) = w, \psi(i+3) = w, \psi(3i-1) = w, \psi(i-2) = w, \psi(2i+1) = w$,respectively.

3 Linear codes over H_p

We know that $(H_p)^n$ is left (right) H_p-module, where p is odd.

Definition 3.1. A left (right) linear code C of length n over H_p is a left (right)H_p-submodule.

Every codeword c in such a left (right)code C is just an n-tuple of the form $c = (c_0, ..., c_{n-1}) \in {H_p}^n$ and can be represented by a polynomial in $H_p[x]$-as follows

$$c = (c_0, ..., c_{n-1}) \longleftrightarrow c(x) = c_0 + c_1 x + ...c_{n-1}x^{n-1} \in H_p[x]$$

In Akbiyik and Ersoy (2017), the Gray map was defined in H_3. Similarly, it can be given in H_p, where $p \equiv 3 \pmod 4$ as follows,

$$\begin{aligned} \Omega_1 \quad &: \quad H_p \longrightarrow (Z_p + iZ_p) \oplus (Z_p + iZ_p) \\ \alpha \quad &\mapsto \quad \Omega_1(\alpha) = (z_1, z_2) \end{aligned}$$

where $\alpha = h_1 * z_1 + h_2 * z_2$. The map is linear. It is also generalized to ${H_p}^n$.
The Gray weight of an element α is defined as

$$w_G(\alpha) = w_H(\psi(z_1), \psi(z_2))$$

where w_H is Hamming weight. The Gray weight of codeword u is $w_G(u) = \sum_{i=1}^{n} w_G(u_i)$. The minimum Gray distance of a code C is

$$d_G(C) = min\{w_G(u) | u \in C\}.$$

Proposition 3.1. The map Ω_1 is an isometry from (${H_p}^n$, Gray distance) to ($(Z_p + iZ_p)^{2n}$, Hamming distance).

Theorem 3.2. *Let C be an (n, A, d_G) linear code over H_p, where n, A and d_G are the code length, the number of codewords and the minimum Gray distance of C, respectively. Then $\Omega_1(C)$ is a $(2n, A, d_G = d_H)$ linear code over F_{p^2}.*

Otherwise, the Gray map is defined in H_p, as follows;

$$\begin{aligned} \Omega_2 \quad &: \quad H_p \longrightarrow (Z_p)^4 \\ \alpha \quad &\mapsto \quad \Omega_2(\alpha) = (\pi(z_1), \pi(z_2)) \end{aligned}$$

where $\alpha = h_1 * z_1 + h_2 * z_2$. The map is linear. It is also generalized to ${H_p}^n$. The weight of an element α is defined as

$$w_G(\alpha) = w_H(\pi(z_1), \pi(z_2))$$

where w_H is Hamming weight and the map π is from the ring $Z_p + iZ_p$ to ${Z_p}^2$ by $a_1 + ib_1 \mapsto (a_1, b_1)$. The Gray weight of codeword u is $w_G(u) = \sum_{i=1}^{n} w_G(u_i)$. The minimum Gray distance of a code C is

$$d_G(C) = min\{w_G(u) | u \in C\}.$$

Proposition 3.2. The map Ω_2 is an isometry from $({H_p}^n$, Gray distance) to $((Z_p)^{4n}$, Hamming distance).

Theorem 3.3. *Let C be an (n, A, d_G) linear code over H_p, where n, A and d_G are the code length, the number of codewords and the minimum Gray distance of C, respectively. Then $\Omega_2(C)$ is a $(4n, A, d_G = d_H)$ linear code over Z_p.*

The left linear code over H_p with length n is represented by

$$C = h_1 * C_1 \oplus h_2 * C_2$$

where C_1, C_2 are linear codes over F_{p^2} with length n.
The right linear code over H_p with length n is represented by

$$C = C_1 * h_1 \oplus C_2 * h_2$$

where C_1, C_2 are linear codes over F_{p^2} with length n.
The following considers that the linear code C is left. Similarly, all can made as the right linear code.

4 Cyclic codes over H_p

In this section, the structure of cyclic codes over H_p is given, where p is an odd prime.
A cyclic shift σ acts on ${H_p}^n$ as

$$\sigma(c_0, ..., c_{n-1}) = (c_{n-1}, c_0, ..., c_{n-2})$$

A left (right) linear code C over H_p of length n is said to be left(right) cyclic code if it is invariant under the cyclic shift. i.e.$\sigma(C) = C$.
Using the polynomial representation of codewords in ${H_p}^n$ in $H_p[x]$, we see that for a codeword $c \in {H_p}^n, \sigma(c)$ corresponds to $xc(x)$ in $H_p[x]/ < x^n - 1 >$. A subset C of ${H_p}^n$ is a left (right) cyclic code of length n over H_p if and only if its polynomial representation is a left(right) ideal of the ring $H_p[x]/ < x^n - 1 >$.
As H_p is a principal ideal ring, so is $H_p[x]/ < x^n - 1 >$.

Theorem 4.1. *Let $C = h_1 * C_1 \oplus h_2 * C_2$ be a code over H_p, where $p \equiv 3 (mod\ 4)$. Then C is a cyclic code over H_p of length n if and only if C_1, C_2 are cyclic codes of length n over F_{p^2}.*

Proof. Let C be a cyclic code and $x = (x_0, ..., x_{n-1}) \in C_1, y = (y_0, ..., y_{n-1}) \in C_2$ such that $c_s = h_1 * x_s + h_2 * y_s$, for $s = 0, ..., n-1$. $\sigma(c) = h_1 * \sigma(x) + h_2 * \sigma(y) = h_1 * (x_{n-1}, x_0, ..., x_{n-2}) + h_2 * (y_{n-1}, y_0, ..., y_{n-2}) \in C$ for $c = (c_0, ..., c_{n-1}) \in C$. So C_1, C_2 are cyclic codes over F_{p^2}.
Conversely, let $c = (c_0, ..., c_{n-1}) \in C$, where $c_s = h_1 * x_s + h_2 * y_s$, for $s = 0, 1, ..., n-1$. Since C_1, C_2 are cyclic codes over F_{p^2}, for $x = (x_0, , , ., x_{n-1}), y = (y_0, ..., y_{n-1}) \in {F_{p^2}}^n$, we have $\sigma(x) = (x_{n-1}, x_0, ..., x_{n-2}) \in C_1$, $\sigma(y) = (y_{n-1}, y_0,$
$..., y_{n-2}) \in C_2$. Hence $\sigma(c) = (h_1 * x_{n-1} + h_2 * y_{n-1}, h_1 * x_0 + h_2 * y_0, ..., h_1 * x_{n-2} + h_2 * y_{n-2}) = h_1 * (x_{n-1}, x_0, ..., x_{n-2}) + h_2 * (y_{n-1}, y_0, ..., y_{n-2}) \in C$. Hence, C is a cyclic code of length n over H_p. □

Theorem 4.2. *Let $C_i =< g_i(x) >$ be a cyclic code of length n over F_{p^2} with parameters (n, M_i, d_i), where $g_i(x) | x^n - 1$ for $i = 1, 2$ and $p \equiv 3 (mod\ 4)$. Then $C =< g(x) >$ is a cyclic code over H_p with parameters (n, M, d), where $|C| = M = M_1 M_2, d = d_L(C) = min\{d_1, d_2\}, g(x) = h_1 * g_1(x) + h_2 * g_2(x)$ and $g(x) | x^n - 1$.*

If not $p \equiv 3 (\mathrm{mod}\ 4)$, we can say:

Theorem 4.3. *Let $C = h_1 * C_1 \oplus h_2 * C_2$ be a code over H_p. Then C is a cyclic code over H_p of length n if and only if C_1, C_2 are cyclic codes of length n over the ring $Z_p + iZ_p \cong Z_p[x]/ < x^2 + 1 >$.*

Example 4.4. Let $p=3, \psi(1+i)=w$ and $w^2=w+1$. Let

$$C_1=\left\langle x^4+2x^3+2x^2+(1+w)x+1\right\rangle=\left\langle x^4+2x^3+2x^2+2ix+1\right\rangle$$

$$C_2=\left\langle x^3+w^5x^2+(1+w)x+1\right\rangle=\left\langle x^3+(2+2i)x^2+2ix+1\right\rangle$$

be cyclic codes over Z_3+iZ_3 with length 20. Then, C_1 is a cyclic code with parameters $[20,16,3]$ and C_2 is a cyclic code over Z_3+iZ_3 with parameters $[20,17,3]$. If we choose $\{2+j+2k, 2+2j+k\}$ as a central orthogonal idempotent pair, then

$$\begin{aligned} C &= \left\langle \begin{array}{c} (2+j+2k)*\left(x^4+2x^3+2x^2+2ix+1\right)+ \\ (2+2j+k)*\left(x^3+(2+2i)x^2+2ix+1\right) \end{array} \right\rangle \\ &= \left\langle (2+j+2k)x^4+(j+2k)x^3+(2+i+2j+2k)x^2+2ix+j+2k\right\rangle \end{aligned}$$

is a $\left(20,9^{33},3\right)$ cyclic code over H_3.

Example 4.5. Let $p=7, \psi(i-3)=w$ and $w^2=w+4$. Let $C_1=C_2=\langle g_1(x)\rangle$, where $g_1(x)=x^8+(4+4i)x^7+2ix^6+(5+i)x^5+(4+3i)x^4+(6-i)x^3+(4+3i)x^2+(i-3)x+i$ be cyclic codes over Z_7+iZ_7 with length 16. Then, C_1 is a cyclic code over Z_7+iZ_7 with parameters $[16,8,9]$. Also, it is an MDS code. If we choose $\{4+3i+4j+k, 4+4i+3j+6k\}$ as a central orthogonal idempotent pair, then $C=\langle(4+3i+4j+k)*g_1(x)+(4+4i+3j-k)*g_2(x)\rangle$is a $\left(16,49^{16},9\right)$ cyclic code over H_7.

Example 4.6. Let $p=11, \psi(3i+2)=w$ and $w^2=4w+9$. Let

$$C_1=\left\langle x^7+3x^5+6x^4+10x^3+4x^2+5x+10\right\rangle$$

$$C_2=\left\langle x^7+7x^6+5x^5+7x^4+6x^3+6x^2+6x+10\right\rangle$$

be cyclic codes over $Z_{11}+iZ_{11}$ with length 43. Then, C_1 and C_2 are cyclic codes over $Z_{11}+iZ_{11}$ with parameters $[43,36,5]$. If we choose $\{6+3i+8j-k, 6+8i+3j+k\}$ as a central orthogonal idempotent pair, then

$$C=\left\langle \begin{array}{c} x^7+(9+i-j+7k)x^6+(4+5i+6j+2k)x^5+(1-3i+3j+k)x^4 \\ +(8+i-j+7k)x^3+(5+5i+6j+2k)x^2+(-3i+3j+k)x-1 \end{array} \right\rangle$$

is a $\left(43,121^{72},5\right)$ cyclic code over H_{11}.

Let $p=11, n=17$. Similarly, for $C_1=C_2=\left\langle \begin{array}{c} x^8+w^{97}x^7+w^{41}x^6+w^3x^5+w^{46}x^4 \\ +w^3x^3+w^{41}x^2+w^{97}x+1 \end{array} \right\rangle$, C is a $\left(17,121^{18},9\right)$ cyclic code over H_{11}.

5 λ- Constacyclic codes over H_p

In this section, the structures of λ-constacyclic codes over H_p are investigated where $p\equiv 3(\text{mod } 4)$ and the unit λ which satisfies $\lambda * h_r = h_r * \lambda$, for all $r=1,2$.
A λ-constacyclic shift γ acts on ${H_p}^n$ as

$$\gamma(c_0,...,c_{n-1})=(\lambda c_{n-1}, c_0, ..., c_{n-2})$$

A left (right) linear code C over H_p of length n is said to be left(right)$\lambda-$consta cyclic code if it is

invariant under the λ-constacyclic shift, where λ is a unit in H_p. i.e.$\gamma(C) = C$. Using the polynomial representation of codewords in ${H_p}^n$ in $H_p[x]$, we see that for a codeword $c \in {H_p}^n, \gamma(c)$ correspond to $xc(x)$ in $H_p[x]/ < x^n - \lambda >$, where λ is a unit in H_p.
A subset C of ${H_p}^n$ is a left (right) λ-constacyclic code of length n over H_p if and only if its polynomial representation is an left(right) ideal of the ring $H_p[x]/ < x^n - \lambda >$.
As H_p is a principal ideal ring, so is $H_p[x]/ < x^n - \lambda >$.

Theorem 5.1. *Let $C = h_1 * C_1 \oplus h_2 * C_2$ be a code over H_p and $\lambda = h_1 * \lambda_1 + h_2 * \lambda_2$ be a unit in H_p. If C is a λ-constacyclic code over H_p of length n ,then C_1, C_2 are λ_1, λ_2-constacyclic codes of length n over $Z_p + iZ_p \cong F_{p^2}$, respectively.*

Proof. Let $x = (x_0, ..., x_{n-1}) \in C_1$ and $y = (y_0, ..., y_{n-1}) \in C_2$. Since C be a $\lambda = h_1 * \lambda_1 + h_2 * \lambda_2$-constacyclic code over H_p of length n, for every $c = (c_0, ..., c_{n-1}) = (h_1 * x_0 + h_2 * y_0, ..., h_1 * x_{n-1} + h_2 * y_{n-1}) \in C$, we have $((h_1 * \lambda_1 + h_2 * \lambda_2) * (h_1 * x_{n-1} + h_2 * y_{n-1}), h_1 * x_0 + h_2 * y_0, ..., h_1 * x_{n-2} + h_2 * y_{n-2}) \in C$. Therefore we get $(h_1 * \lambda x_{n-1} + h_2 * \lambda y_{n-1}, h_1 * x_0 + h_2 * y_0, ..., h_1 * x_{n-2} + h_2 * y_{n-2}) = (h_1 * \lambda_1 x_{n-1} + h_2 * \lambda_2 y_{n-1}, h_1 * x_0 + h_2 * y_0, ..., h_1 * x_{n-2} + h_2 * y_{n-2}) = h_1 * (\lambda_1 x_{n-1}, x_0, ..., x_{n-2}) + h_2 * (\lambda_2 y_{n-1}, y_0, ..., y_{n-2}) \in C = h_1 * C_1 \oplus h_2 * C_2$. From this, we get C_1, C_2 are λ_1, λ_2-constacylic codes over F_{p^2}, respectively. □

Example 5.2. Let $\{h_1, h_2\} = \{3 + i, 3 + 4i\}$,$\lambda = i$ and $p = 5$. Since C is a λ-constacyclic code over H_5, we get C_1, C_2 are $3, 2$-constacyclic codes over F_{25}.

Remark. The converse of the theorem in the above is not true generally. Let $p = 3$. Although $2 + i$ and $1 + 2i$ are units in $Z_3 + iZ_3$ and $i + j + k = (2 + i + 2k) * (1 + 2i) + (2 + 2i + k) * (2)$, and $i + j + k$ is not a unit in H_3.

Depending on λ_1, λ_2 choice, if $\lambda = h_1 * \lambda_1 + h_2 * \lambda_2$ is a unit in H_p, then the converse of theorem is true.

Theorem 5.3. *For λ_1, λ_2, let $\lambda = h_1 * \lambda_1 + h_2 * \lambda_2$ be a unit in H_p. If C_1, C_2 are λ_1, λ_2-constacyclic codes of length n over $Z_p + iZ_p \cong F_{p^2}$ respectively, then C is a $\lambda = h_1 * \lambda_1 + h_2 * \lambda_2$-constacyclic code over H_p of length n.*

Proof. Let C_1, C_2 be λ_1, λ_2-constacyclic codes of length n over $Z_p + iZ_p \cong F_{p^2}$ respectively. So $(\lambda_1 x_{n-1}, x_0, ..., x_{n-2}) \in C_1$, for every $(x_0, ..., x_{n-1}) \in C_1$ and $(\lambda_1 y_{n-1}, y_0, ..., y_{n-2}) \in C_2$, for every $(y_0, ..., y_{n-1}) \in C_2$. For every $(c_0, ..., c_{n-1}) = (h_1 * x_0 + h_2 * y_0, ..., h_1 * x_{n-1} + h_2 * y_{n-1}) \in C$, we have $(\lambda * (h_1 * x_{n-1} + h_2 * y_{n-1}), h_1 * x_0 + h_2 * y_0, ..., h_1 * x_{n-2} + h_2 * y_{n-2}) = (h_1 * \lambda x_{n-1} + h_2 * \lambda y_{n-1}, h_1 * x_0 + h_2 * y_0, ..., h_1 * x_{n-2} + h_2 * y_{n-2}) = (h_1 * \lambda_1 x_{n-1} + h_2 * \lambda_2 y_{n-1}, h_1 * x_0 + h_2 * y_0, ..., h_1 * x_{n-2} + h_2 * y_{n-2}) = h_1 * (\lambda_1 x_{n-1}, x_0, ..., x_{n-2}) + h_2 * (\lambda_2 y_{n-1}, y_0, ..., y_{n-2}) \in C = h_1 * C_1 \oplus h_2 * C_2$. Therefore C is λ-constacyclic code over H_p. □

Proposition 5.1. Let $C_i =< g_i(x) >$ be λ_i-constacyclic codes over F_{p^2} such that $g_i(x) | x^n - \lambda_i, d_H(C_i) = d_i$ for $i = 1, 2$. So $C =< g(x) >$ is $\lambda = h_1 * \lambda_1 + h_2 * \lambda_2$-constacyclic code over H_p of length n,with $|C| = M = |C_1||C_2|$ and $d_G(C) = min\{d_1, d_2\}$, where $g(x) = h_1 * g_1(x) + h_2 * g_2(x)$ and $g(x) | x^n - \lambda$.

Example 5.4. Let $p = 3$, $\lambda_1 = \lambda_2 = 2$.

$$\begin{aligned} x^7 - 2 &= (x + 1)\left(x^3 + w^5 x^2 + w^7 x + 1\right)\left(x^3 + w^7 x^2 + w^5 x + 1\right) \\ &= g_1(x)\, g_2(x)\, g_3(x) \in F_9[x] \end{aligned}$$

Let $C_1 = \langle g_3(x) \rangle$, $C_2 = \langle g_1(x)\, g_3(x) \rangle$ be a cyclic codes over $Z_3 + iZ_3$ with length 7. Then, C_1 and C_2 are 2-constacyclic codes over $Z_3 + iZ_3$ with parameters $[7, 4, 4]$, $[7, 3, 5]$, respectively. Also, they are MDS codes. If we choose $\{2 + j + k, 2 + 2j + 2k\}$ as a central orthogonal idempotent pair, then C is a 2-constacyclic code over H_3 with parameters $\left(7, 9^7, 4\right)$.

Example 5.5. Let $p = 7$, $\lambda_1 = \lambda_2 = 6$, $\psi(i - 3) = w$ and $w^2 = w + 4$. Let $C_1 = \left\langle x^4 + 3x^2 - 1 \right\rangle$, $C_2 = \left\langle x^4 + (1 - i)\, x^2 + i \right\rangle$ be a cyclic codes over $Z_7 + iZ_7$ with length 16. Then, C_1 and C_2 are 6-constacyclic codes over $Z_7 + iZ_7$ with parameters $[16, 12, 3]$. If we choose $\{4 + j + 2k, 4 - j + 5k\}$ as a central orthogonal idempotent pair, then C is a 6-constacyclic code over H_7 with parameters $\left(16, 49^{24}, 3\right)$.

Let $p = 7$, $\lambda_1 = \lambda_2 = 3, n = 32$. Similarly, C is a $\left(32, 49^{32}, 5\right)$ 3-constacyclic code over H_7.

Example 5.6. Let $p = 11, \psi(3i + 2) = w$ and $w^2 = 4w + 9$. Let
$C_1 = C_2 = \left\langle x^{12} + w^{10}x^{11} + w^{26}x^{10} + ... + w^{56}x + w^6 \right\rangle$ be 4-constacyclic codes over $Z_{11} + iZ_{11}$ with length 28. Then, C_1 is a 4-constacyclic code over $Z_{11} + iZ_{11}$ with parameters $[28, 16, 8]$. If we choose $\{6 + 3i + 8j - k, 6 + 8i + 3j + k\}$ as a central orthogonal idempotent pair, then C is a 4-constacyclic code over H_{11} with parameters $\left(28, 121^{32}, 8\right)$.

6 Dual codes over H_p

For any $v = (v_1, .., v_n), w = (w_1, w_2, .., w_n) \in {H_p}^n$, where $v_s = h_1 * v_{s,0} + h_2 * v_{s,1}, w_s = h_1 * w_{s,0} + h_2 * w_{s,1}, s = 1, 2, ..., n$, the quaternionic Euclidean inner product of v, w is defined as follows,

$$< v, w >= \sum_{s=1}^{n} v_s * w_s.$$

For any $v = (v_1, .., v_n), w = (w_1, w_2, .., w_n) \in {H_p}^n$, the quaternionic Hermitian inner product of v, w is defined as follows,

$$< v, w >_H = \sum_{s=1}^{n} v_s * \overline{w_s}$$

where $\overline{h} = a + (p-1)bi + (p-1)cj + (p-1)dk$ is conjugate of $h = a + bi + cj + dk \in H_p$.
For C in ${H_p}^n$, the dual of C

$$L(C) = \{v \in {H_p}^n | < v, c >= 0, \text{for all } c \in C\}$$

$$R(C) = \{v \in {H_p}^n | < c, v >= 0, \text{for all } c \in C\}$$

Similarly, the dual of C can be defined for quaternionic Hermitian inner product.
For the code C over H_p, $L(C)$ is a left linear code, $R(C)$ is a right linear code.
As Z_p is a Frobenious ring, by using **Theorem 3.1** in (Tan & Sison, 2021), it is easily seen that H_p is a Frobenious ring. Therefore, the following results about the duals of the codes over H_p can be written by using the same results in (Dougherty & Andre, 2016).
A left linear code C is defined to be self-orthogonal if $C \subset L(C)$ and self dual if $C = L(C)$.

Lemma 6.1. *If C is a left linear code over H_p, then $|R(C)||C| = |H_p|^n$. If C is a right linear code, then $|L(C)||C| = |H_p|^n$.*

Since $\overline{xy} = \overline{y}.\overline{x}$, for any $x, y \in H_p$, then $L(C) = R(C) = C^{\perp}$. So we use the notation $C^{\perp}$ as a dual of C.

Theorem 6.2. *The left linear code C is a self-orthogonal over H_p if and only if C_1 and C_2 are all self-orthogonal codes over F_{p^2}.*

Proof. Clearly, C is self-orthogonal over H_p if C_1 and C_2 are all self-orthogonal over F_{p^2}. On the other hand, let C be a self-orthogonal code over H_p and for any element $c \in C$, we have $c = h_1 * c_1 + h_2 * c_2$, where $c_1 \in C_1$ and $c_2 \in C_2$. Since C is a self orthogonal, it follows that $c^2 = h_1 * {c_1}^2 + h_2 * {c_2}^2 = 0$. It means that ${c_1}^2 = {c_2}^2 = 0$. Thus, $c_1 \in C_1^{\perp}$ and $c_2 \in C_2^{\perp}$. Therefore, C_1 and C_2 are all self-orthogonal codes over F_{p^2}. □

Theorem 6.3. *Let C be a left linear code of length n over H_p. If C is a self-orthogonal, so is $\Omega_1(C)$.*

Proof. It is enough tho show that the map Ω_1 preserves the orthogonality, that is $< \Omega_1(c_0), \Omega_1(c_1) >= 0$ when $< c_0, c_1 >= 0$. Let $t = h_1 * x_1 + h_2 * x_2, r = h_1 * y_1 + h_2 * y_2 \in H_p$, where $x_1, x_2, y_1, y_2 \in F_{p^2}$. By the quaternionic Euclidean inner product of t and r, we get

$$< t, r >= h_1 * x_1 y_1 + h_2 * x_2 y_2 = 0$$

since $h_1 + h_2 = 1$, we have $x_1y_1 + x_2y_2 = 0$, for every central idempotent pair. In this case, it follows that $< \Omega_1(t), \Omega_1(r) >= x_1y_1 + x_2y_2 = 0$, which completes the proof. □

Proposition 6.1. Let $C = h_1 * C_1 \oplus h_2 * C_2$ be a left linear code of length n over H_p. Then

$$C^{\perp} = h_1 * C_1^{\perp} \oplus h_2 * C_2^{\perp}.$$

7 Quantum codes obtained from Cyclic and λ-Constacyclic Codes

In this section, the parameters of the quantum codes will first be obtained from the left cyclic code over H_p.

Theorem 7.1. *(CSS Construction) (Calderbank et al., 1998) Let $C_1 = [n, k_1, d_1]_q$ and $C_2 = [n, k_2, d_2]_q$ be linear codes over GF(q) with $C_2 \subseteq C_1$. Then there exists a quantum error-correcting code $C = [[n, k_1 - k_2, min\{d_1, d_2^{\perp}\}]]_q$, where $d_2^{\perp}$ denotes the minimum Hamming distance of the dual code $C_2^{\perp}$ of C_2. Further, if $C_1^{\perp} = C_2$, then there exists a quantum error-correcting code $C = [[n, 2k_1 - n, d_1]]$.*

Lemma 7.2. *((Calderbank et al., 1998), Theorem 13) A cyclic code C over a finite field with generator polynomial $g(x)$ contains its dual code if and only if*

$$x^n - 1 \equiv 0 (mod g(x) g^{'}(x))$$

where $g^{'}(x)$ is the reciprocal polynomial of $g(x)$.

Theorem 7.3. *Let $C = h_1 * C_1 \oplus h_2 * C_2$ be a left cyclic code of length n over H_p and $C =< g(x) >$, where $g(x) = h_1 * g_1(x) + h_2 * g_2(x)$, $C_1 =< g_1(x) >, C_2 = g_2(x)$. Then $L(C) \subseteq C$ iff*

$$x^n - 1 \equiv 0 \left(mod g_s(x) g_s^{'}(x) \right)$$

for $s = 1, 2$.

Proof. Let $x^n - 1 \equiv 0 \left(mod g_s(x) g_s^{'}(x) \right)$ for $s = 1, 2$. From **Lemma 7.2**, we have $C_1^{\perp} \subseteq C_1, C_2^{\perp} \subseteq C_2$. This shows that $h_s C_s^{\perp} \subseteq h_s C_s$, for $s = 1, 2$. We have $L(C) = h_1 * C_1^{\perp} \oplus h_2 * C_2^{\perp} \subseteq h_1 * C_1 \oplus h_2 * C_2 = C$, by using **Proposition 6.1**.
Conversely, if $L(C) \subseteq C$, then we have $h_1 * C_1^{\perp} \oplus h_2 * C_2^{\perp} \subseteq h_1 * C_1 \oplus h_2 * C_2$. So $C_s^{\perp} \subseteq C_s$ for $s = 1, 2$. So from **Lemma 7.2**, we get $x^n - 1 \equiv 0 \left(mod g_s(x) g_s^{'}(x) \right)$, for $s = 1, 2$. □

Theorem 7.4. *Let $C = h_1 * C_1 \oplus h_2 * C_2$ be a cyclic code of length n over H_p and let the parameters of code $\Omega_1(C)$ be $[2n, k, d_G]$, where d_G is the minimum Gray distance of C. If $L(C) \subseteq C$, then there exists a quantum error correcting code with parameter $[[2n, 2k - 2n, d_G]]$ over F_{p^2}.*

We give the following lemma to obtain the parameters of quantum codes from λ-constacyclic codes over H_p, where $\lambda = -1$.

Lemma 7.5. *A negacyclic code C over a finite field with generator polynomial $g(x)$ contains its dual code if and only if*

$$x^n + 1 \equiv 0 (mod g(x) g^{'}(x))$$

where $g^{'}(x)$ is the reciprocal polynomial of $g(x)$.

Theorem 7.6. *Let $C = h_1 * C_1 \oplus h_2 * C_2$ be a left $(p-1)$-constacyclic code (negacyclic) of length n over H_p and $C =< g(x) >$, where $g(x) = h_1 * g_1(x) + h_2 * g_2(x)$, $C_1 =< g_1(x) >, C_2 =< g_2(x) >$. Then $L(C) \subseteq C$ iff*

$$x^n + 1 \equiv 0 \left(mod g_s(x) g_s^{'}(x) \right)$$

for $s = 1, 2$.

Proof. It is made as proof of the **Theorem 7.3**. □

Theorem 7.7. *Let $C = h_1 * C_1 \oplus h_2 * C_2$ be a left $(p-1)$-constacyclic code of length n over H_p and let the parameters of the code $\Omega_1(C)$ be $[2n, k, d_G]$, where d_G is the minimum Gray distance of C. If $L(C) \subseteq C$, then there exists a quantum error correcting code with parameter $[[2n, 2k-2n, d_G]]$ over F_{p^2}.*

Example 7.8. Let $p = 7$, $\psi(i-3) = w$ and $w^2 = w+4$. Let $C_1 = C_2 = \langle g(x)\rangle = \left\langle x^3 - x^2 + 4x - 1\right\rangle$ be a cyclic codes over $Z_7 + iZ_7$ with length 6. Obviously $x^6 - 1$ is divisible by $g(x)g^{'}(x)$. Hence, we have $C \subseteq C^{\perp}$. We know that C is a cyclic code of length 6 with minimum Gray distance $d_G = 4$. Thus, we obtain a quantum code with parameters $[[12, 0, 4]]$.

Example 7.9. Let $p = 11, \psi(3i+2) = w$ and $w^2 = 4w + 9$. Let
$C_1 = \langle g_1(x)\rangle = \left\langle x^7 + 5x^6 + 5x^5 + 5x^4 + 4x^3 + 6x^2 + 4x + 10\right\rangle$, $C_2 = \langle g_2(x)\rangle = \left\langle x^7 + 7x^6 + 5x^5 \ + 7x^4 + 6x^3 + 6x^2 + 6x + 10\right.$ be cyclic codes over $Z_{11} + iZ_{11}$ with length 43. Obviously $x^{43} - 1$ is divisible by $g_i(x)g_i^{'}(x)$, for $i = 1, 2$. Hence, we have $C \subseteq C^{\perp}$. We know that C is a cyclic code of length 43 with minimum Gray distance $d_G = 5$.Thus, we obtain a quantum code with parameters $[[86, 58, 5]]$.

Example 7.10. Let $p = 3, \psi(1+i) = w$ and $w^2 = w + 1$. Let
$C_1 = C_2 = \langle g(x)\rangle = \left\langle x^{11} + x^8 + x^6 + 2x^4 + x^3 + x^2 + 2x + 1\right\rangle$ be a negacyclic codes over $Z_3 + iZ_3$ with length 23. Obviously $x^{23} + 1$ is divisible by $g(x)g^{'}(x)$. Hence, we have $C \subseteq C^{\perp}$. We know that C is a negacyclic code of length 23 with minimum Gray distance $d_G = 8$. Thus, we obtain a quantum code with parameters $[[46, 2, 8]]$.

Example 7.11. Let $p = 7, \psi(i-3) = w$ and $w^2 = w + 4$. Let
$C_1 = \langle g_1(x)\rangle = \left\langle x^{11} + w^{27}x^{10} + ... + w^{21}x + 6\right\rangle$ be cyclic code and $C_2 = \langle g_2(x)\rangle = \left\langle x^{11} + w^3x^{10} \ + ... + w^{21}x + 1\right.$ be negacyclic codes over $Z_7 + iZ_7$ with length 23. Obviously $x^{23} - 1$ is divisible by $g_1(x)g_1^{'}(x)$, $x^{23} + 1$ is divisible by $g_2(x)g_2^{'}(x)$. Hence, we have $C \subseteq C^{\perp}$. We know that C is an i-constacyclic code of length 23 with minimum Gray distance $d_G = 11$.Thus, we obtain a quantum code with parameters $[[46, 2, 11]]$.

8 Conclusion

In this paper, the structures of linear codes over a family of the Quaternion rings over Z_p are determined. The structures of cyclic and λ-constacyclic codes over H_p are investigated, where λ is a unit in H_p, for $p \equiv 3 (\text{mod } 4)$. Their applications to quantum codes are obtained.

Funding
The author has not received any financial support for the research, authorship, or publication of this study.

The Declaration of Conflict of Interest/ Common Interest
The authors have no conflicts of interest to declare.

The Declaration of Ethics Committee Approval
This study does not require ethics committee permission or any special permission.

The Declaration of Research and Publication Ethics
The authors declare that they have complied with the scientific, ethical, and citation rules of the Universal Mathematics Journal, that they have not falsified any data, and that this work has not been submitted to any other academic publication. The journal and its editorial board are not responsible for any ethical violations that may occur.

Availability of Data and Materials: Data sharing not applicable to this article as no datasets were

generated or analysed during the current study.

References

Akbiyik, S., & Ersoy, B. A. (2017). Cyclic codes over a non-commutative ring. In *2017 7th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO)*. IEEE.

Aristidou, M., & Demetre, D. (2012). Idempotent elements in quaternion rings over Z_p. *International Journal of Algebra*, *6*, 249–254.

Calderbank, A. R., Rains, E. M., Shor, P. M., & Sloane, N. J. A. (1998). Quantum error correction via codes $GF(4)$. *IEEE Transactions on Information Theory*, *44*, 1369–1387.

Cheraghpour, H., & Ghosseiri, M. N. (2019). On the idempotents, nilpotents, units and zero-divisors of finite rings. *Linear and Multilinear Algebra*, *67*, 327–336.

Dougherty, S. T., & Andre, L. (2016). Euclidean self-dual codes over non-commutative Frobenius rings. *Applicable Algebra in Engineering, Communication and Computing*, *27*, 185–203.

Kandasamy, W. B. V. (2000). On the finite Quaternion rings and skew fields. *Acta Ciencia Indica*, $XXVI(2)$, 133–135.

Miguel, C. J., & Serodio, R. (2011). On the structure of quaternion rings over Z_p. *International Journal of Algebra*, *5*, 1313–1325.

Tan, P. L., & Sison, V. (2021). *Quaternions over Galois rings and their codes. arXiv.* `https://arxiv.org/abs/2109.00735`