



About on the obtaining of some quantum code parameters from $(-2v^{m-1} + 1)$ -constacyclic codes over the ring $R = \mathbb{F}_q + v\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$

Gökhan GÖKGÖZ and Figen ÖKE

Abstract

In this study, the hull dimensions of $(-2v^{m-1} + 1)$ -constacyclic codes over the ring $R = \mathbb{F}_q + v\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$ with $v^m = v$ are determined. In addition, by using a special Gray map, a necessary condition is given under which the generator polynomial of a $(-2v^{m-1} + 1)$ -constacyclic code over R yields, through the polynomial representation of the Gray map, the generator polynomial of the corresponding cyclic code over $\mathbb{F}_q$. Later, an example is presented showing that the parameters of a quantum error-correcting code over $\mathbb{F}_q$ can be obtained from a $(-2v^{m-1} + 1)$ -constacyclic code over R by means of the X-construction method. Furthermore, the case in which the number of $(-2v^{m-1} + 1)$ -constacyclic codes of length n over R equals the number of cyclic codes of length $2n$ over $\mathbb{F}_q$ is examined, and an example is provided in which the parameters of the quantum error-correcting codes arising from those cyclic codes—which are Gray images of $(-2v^{m-1} + 1)$ -constacyclic codes over R —are presented.

1 Introduction

In this study, some results from Tian et al. [2] are extended to $(-2v^{m-1} + 1)$ -constacyclic codes over the ring $R = \mathbb{F}_q + v\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$ ($v^m = v$). By using the orthogonal idempotent elements $e_0, e_1, \dots, e_{m-1}$ of R , we establish

Key Words: Hulls; Quantum Construction X Method; Constacyclic Codes; Gray Map.
2010 Mathematics Subject Classification: Primary 11T71, 68P30 ; Secondary 81P70.
Received: 21.11.2025
Accepted: 31.01.2026

the necessary and sufficient condition for a linear code of length n over R to be a $(-2v^{m-1} + 1)$ -constacyclic code. We also provide a theorem to determine the hull dimension of such $(-2v^{m-1} + 1)$ -constacyclic codes over R . We examine the general form over $R = \mathbb{F}_q + v\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$ ($v^m = v$) of the Gray map, which was previously defined by Tian et al. [2] over $\mathbb{F}_q + u\mathbb{F}_q$ ($u^2 = u$), by Raka et al. [1] over $R = \mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p + u^3\mathbb{F}_p$ ($u^4 = u$), and by Zhang et al. [8] over R_1 . When $m > 2$, the Gray map is not a vector space isomorphism, unlike the $m = 2$ case; thus, the results from [2] are not directly applicable. For $m > 2$, we provide an example showing that, under specific conditions, data from the generator polynomials of $(-2v^{m-1} + 1)$ -constacyclic codes over $R = \mathbb{F}_q + v\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$ ($v^m = v$) can be used to construct new quantum error-correcting code parameters through the Gray images of these codes and the X-quantum construction method. Moreover, even though a one-to-one correspondence has not been established, we present an example related to the parameters of quantum error-correcting codes obtained via the X-quantum construction from those cyclic codes that are Gray images of $(-2v^{m-1} + 1)$ -constacyclic codes over R , in the scenario where the number of these constacyclic codes equals the number of cyclic codes of length $2n$ over $\mathbb{F}_q$.

The study of Tian et al. [2] examined hull dimensions of constacyclic codes of length n over $\mathbb{F}_q + v\mathbb{F}_q$ with $v^2 = v$, under both Euclidean and Hermitian inner products. Using a suitable Gray map from $\mathbb{F}_q + v\mathbb{F}_q$ to $\mathbb{F}_q^2$, they determined the hulls of the Gray images of $(-2v + 1)$ -constacyclic codes and, via the X-quantum construction, obtained new QECC parameters.

Hull dimensions play a central role in X-quantum constructions, for which Tian et al. [2] relied on [4, 7]. One classical approach for deriving quantum code parameters is the CSS construction. Cengellenmis and Dertli [3] obtained new quantum codes over $\mathbb{F}_q$ using a self-duality-preserving Gray map defined on $R = \mathbb{F}_q + v\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$ with $v^m = v$, $(m-1) \mid (p-1)$, p odd prime, $q = p^s$.

Shi et al. [15] studied the algebraic structure of the same ring R and described skew cyclic codes together with a general Gray map. Raka et al. [1] investigated $(-2u^3 + 1)$ -constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p + u^3\mathbb{F}_p$ with $u^4 = u$ and analyzed their Gray images. Moreover, Shi et al. [6] showed that the Gray images of u -constacyclic codes over $R = \mathbb{F}_{q^2} + u\mathbb{F}_{q^2} + \cdots + u^{r-1}\mathbb{F}_{q^2}$ (with $u^r = 1$, $r \mid (q+1)$) become cyclic codes over $\mathbb{F}_{q^2}$ under the Fourier transform, and they derived new quantum parameters via Hermitian construction.

Zhang et al. [8] produced parameters for maximal-entanglement EAQECs from Gray images of cyclic codes over $R_{s-1} = \mathbb{F}_q + v_1\mathbb{F}_q + \cdots + v_{s-1}\mathbb{F}_q$, where $v_i^2 = v_i$ and $v_i v_j = 0$ for $i \neq j$. They further obtained ME-MDS EAQECs from Gray images of $(-2v_1 + 1)$ -constacyclic codes over $R_1 = \mathbb{F}_q + v_1\mathbb{F}_q$.

2 Preliminaries

For the fundamental definitions and concepts of algebraic coding theory, the reader is referred to [12] and [11].

The 'hull' concept was first defined by Assmus and Key [9] in their 1990 paper "Affine and projective planes." The hull of a linear code C is $C \cap C^\perp$. The dual is typically defined using the Euclidean inner product, but other inner products, like the Hermitian, may also be used. Massey (1992) [10], in "Linear Codes With Complementary Duals," first explored the properties of linear codes C where $C \cap C^\perp = \{0\}$. He named such codes "LCD" (Linear Complementary Dual) codes.

3 $(-2v^{m-1} + 1)$ -Constacyclic Codes over the Ring $R = \mathbb{F}_q[v]/\langle v^m - v \rangle$

Unless specified otherwise, R will refer to $R = \mathbb{F}_q + v\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$ with $q = p^s$, $(m-1) \mid (p-1)$, p an odd prime, and $v^m = v$. The algebraic structure of R was given by Shi et al. in [5]. In this work, the notation in [5] will be used.

Dinh [13] gave the definition of a constacyclic code over an arbitrary finite ring, and the relationship between a λ -constacyclic code and its dual.

Proposition 1. *The element $(-2v^{m-1} + 1_R)$ is a unit in the ring R .*

Proof. Since $v^m = v$, we have $v^{m-1} = 1$. Thus, $(-2v^{m-1} + 1_R) \cdot (-2v^{m-1} + 1_R) = 4(v^{m-1})^2 - 4v^{m-1} + 1_R = 4 \cdot 1_R - 4 \cdot 1_R + 1_R = 1_R$. Hence, $(-2v^{m-1} + 1_R)$ is a unit. $\square$

Definition 1. *Let C be a linear code of length n over the ring R . Let $(-2v^{m-1} + 1) \in R$ be a unit element and let τ be a $(-2v^{m-1} + 1)$ -constacyclic shift transformation. For every $c = (c_0, c_1, \dots, c_{n-1}) \in C$, if $\tau(c) = ((-2v^{m-1} + 1)c_{n-1}, c_0, \dots, c_{n-2}) \in C$, then the code C is called a $(-2v^{m-1} + 1)$ -constacyclic code over R .*

Proposition 2. *For $i = 0, 1, \dots, m-1$, let C_i be codes of length n over $\mathbb{F}_q$. The code $C = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_{m-1}C_{m-1}$ is a $(-2v^{m-1} + 1)$ -constacyclic code of length n over R if and only if C_0 is a cyclic code and, for $i = 1, 2, \dots, m-1$, each C_i is a negacyclic code.*

Proof. In the factorization $v^m - v = v \cdot (v - v_1) \cdot (v - v_2) \cdots (v - v_{m-1})$, since $f_0 = v - 0 = v$, we have $\hat{f}_0 = (v^{m-1} - 1)$. It is easily seen that the values of a_0 and b_0 satisfying the equality $a_0f_0 + b_0\hat{f}_0 = 1$ are v^{m-2} and -1 , respectively. Indeed, $v^{m-2} \cdot v + (-1) \cdot (v^{m-1} - 1) = 1$. In this case, we obtain $e_0 = -v^{m-1} - 1$.

Let any element of $C_i \subseteq \mathbb{F}_q^n$ ($i = 0, 1, \dots, m-1$) be of the form $(a_0^i, a_1^i, \dots, a_{n-1}^i)$. Since $C \subseteq R^n$ and $R = e_0\mathbb{F}_q \oplus e_1\mathbb{F}_q \oplus \cdots \oplus e_{m-1}\mathbb{F}_q$, for $j = 0, 1, \dots, n-1$, each element $m_j \in R$ can be uniquely written as $m_j = e_0a_j^0 + e_1a_j^1 + \cdots + e_{m-1}a_j^{m-1}$. Therefore, any element of a code C of length n over R can be written as $(m_0, m_1, \dots, m_{n-1})$.

Under these representations: for each $(a_0^i, a_1^i, \dots, a_{n-1}^i) \in C_i$ ($i = 0, 1, \dots, m-1$), we have $m = (m_0, m_1, \dots, m_{n-1}) \in C$, where $m_j = e_0a_j^0 + e_1a_j^1 + \cdots + e_{m-1}a_j^{m-1}$ ($j = 0, 1, \dots, n-1$).

Above, it was shown that $e_0 = -v^{m-1} - 1$. Now observe that $-2v^{m-1} + 1 = 2(-v^{m-1} + 1) - 1 = 2e_0 - 1$. Thus, a $(-2v^{m-1} + 1)$ -constacyclic code and a $(2e_0 - 1)$ -constacyclic code are the same. In the remainder of the proof, the expression “ $(-2v^{m-1} + 1)$ -constacyclic code” will be replaced by “ $(2e_0 - 1)$ -constacyclic code.”

Let $C = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_{m-1}C_{m-1} \subseteq R^n$ be a $(-2v^{m-1} + 1)$ -constacyclic code. Then, for each $m = (m_0, m_1, \dots, m_{n-1}) \in C$, we have $((2e_0 - 1)m_{n-1}, m_0, \dots, m_{n-2}) \in C$.

On the other hand, $((2e_0 - 1)m_{n-1}, m_0, \dots, m_{n-2}) = e_0(a_{n-1}^0, a_0^0, a_1^0, \dots, a_{n-2}^0) + e_1(-a_{n-1}^1, a_0^1, a_1^1, \dots, a_{n-2}^1) + e_2(-a_{n-1}^2, a_0^2, a_1^2, \dots, a_{n-2}^2) + \cdots + e_{m-1}(-a_{n-1}^{m-1}, a_0^{m-1}, a_1^{m-1}, \dots, a_{n-2}^{m-1}) \in C$.

Indeed, $(2e_0 - 1)m_{n-1} = (2e_0 - 1) \cdot (e_0a_{n-1}^0 + e_1a_{n-1}^1 + \cdots + e_{m-1}a_{n-1}^{m-1}) = e_0a_{n-1}^0 - e_1a_{n-1}^1 - \cdots - e_{m-1}a_{n-1}^{m-1}$. Thus, the first components of the two n -tuples are equal. $((2e_0 - 1) \cdot e_0 = 2e_0^2 - e_0 = 2e_0 - e_0 = e_0)$ and $(2e_0 - 1) \cdot e_k a_{n-1}^k = 2e_0 e_k a_{n-1}^k - e_k a_{n-1}^k = 0 - e_k a_{n-1}^k$ ($k = 1, 2, \dots, m-1$).

It is easily seen from $m_j = e_0a_j^0 + e_1a_j^1 + \cdots + e_{m-1}a_j^{m-1}$ for $j = 0, 1, \dots, n-2$ that the other components of the tuples are also equal.

Therefore, considering $C = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_{m-1}C_{m-1} \subseteq R^n$, we obtain $(a_{n-1}^0, a_0^0, a_1^0, \dots, a_{n-2}^0) \in C_0$, $(-a_{n-1}^1, a_0^1, a_1^1, \dots, a_{n-2}^1) \in C_1$, $(-a_{n-1}^2, a_0^2, a_1^2, \dots, a_{n-2}^2) \in C_2$, $\dots$, $(-a_{n-1}^{m-1}, a_0^{m-1}, a_1^{m-1}, \dots, a_{n-2}^{m-1}) \in C_{m-1}$. This means that C_0 is a cyclic code, and $C_1, C_2, \dots, C_{m-1}$ are negacyclic codes.

Conversely, let $C = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_{m-1}C_{m-1} \subseteq R^n$ be a linear code of length n over R . For any codeword $m = (m_0, m_1, \dots, m_{n-1}) \in C$, its components are written as $m_j = e_0a_j^0 + e_1a_j^1 + \cdots + e_{m-1}a_j^{m-1}$ ($j = 0, 1, \dots, n-1$), with $(a_0^i, a_1^i, \dots, a_{n-1}^i) \in C_i$.

Since C_0 is cyclic and $C_1, C_2, \dots, C_{m-1}$ are negacyclic codes over $\mathbb{F}_q$, we have $(a_{n-1}^0, a_0^0, a_1^0, \dots, a_{n-2}^0) \in C_0$, $(-a_{n-1}^1, a_0^1, a_1^1, \dots, a_{n-2}^1) \in C_1$, $\dots$, $(-a_{n-1}^{m-1}, a_0^{m-1}, a_1^{m-1}, \dots, a_{n-2}^{m-1}) \in C_{m-1}$. Therefore, $e_0(a_{n-1}^0, a_0^0, a_1^0, \dots, a_{n-2}^0) + e_1(-a_{n-1}^1, a_0^1, a_1^1, \dots, a_{n-2}^1) + e_2(-a_{n-1}^2, a_0^2, a_1^2, \dots, a_{n-2}^2) + \cdots + e_{m-1}(-a_{n-1}^{m-1}, a_0^{m-1}, a_1^{m-1}, \dots, a_{n-2}^{m-1}) \in C$, which implies $((2e_0 - 1)m_{n-1}, m_0, \dots, m_{n-2}) \in C$.

Hence, C is a $(2e_0 - 1)$ -constacyclic code of length n over R . Therefore, C

is a $(-2v^{m-1} + 1)$ -constacyclic code of length n over R . $\square$

Proposition 3. *Let $C = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_{m-1}C_{m-1}$ be a $(-2v^{m-1} + 1)$ -constacyclic code of length n over R . Let $g_0(x)$ be the generator polynomial of the cyclic code C_0 , and let $g_1(x), g_2(x), \dots, g_{m-1}(x)$ be the generator polynomials of the negacyclic codes $C_1, C_2, \dots, C_{m-1}$, respectively. Then $C = \langle e_0g_0(x), e_1g_1(x), \dots, e_{m-1}g_{m-1}(x) \rangle$.*

Proof. As a consequence of Proposition 2.2. in [13], we obtain the following: $\pi : R^n \rightarrow R[x]/\langle x^n - (-2v^{m-1} + 1) \rangle$, $c = (c_0, c_1, \dots, c_{n-1}) \mapsto \pi(c) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + \langle x^n - (-2v^{m-1} + 1) \rangle$ is an R -module isomorphism.

A linear code $C \subseteq R^n$ is a $(-2v^{m-1} + 1)$ -constacyclic code if and only if $\pi(C)$ is an ideal of the ring $R[x]/\langle x^n - (-2v^{m-1} + 1) \rangle$.

For $C = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_{m-1}C_{m-1} \subseteq R^n$, we have $\pi(C) = \pi(e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_{m-1}C_{m-1}) = \pi(e_0C_0) \oplus \pi(e_1C_1) \oplus \cdots \oplus \pi(e_{m-1}C_{m-1}) = e_0\pi(C_0) \oplus e_1\pi(C_1) \oplus \cdots \oplus e_{m-1}\pi(C_{m-1}) = \langle e_0g_0(x), e_1g_1(x), \dots, e_{m-1}g_{m-1}(x) \rangle$. Therefore, $C = \langle e_0g_0(x), e_1g_1(x), \dots, e_{m-1}g_{m-1}(x) \rangle$. $\square$

Proposition 4. *If $C = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_{m-1}C_{m-1}$ is a $(-2v^{m-1} + 1)$ -constacyclic code of length n over R , then $C^\perp = e_0C_0^\perp \oplus e_1C_1^\perp \oplus \cdots \oplus e_{m-1}C_{m-1}^\perp$ is also a $(-2v^{m-1} + 1)$ -constacyclic code of length n over R .*

Proof. For $i = 0, 1, \dots, n-1$, let $x_i = e_0x_{i,0} + e_1x_{i,1} + \cdots + e_{m-1}x_{i,m-1} \in R = e_0\mathbb{F}_q \oplus e_1\mathbb{F}_q \oplus \cdots \oplus e_{m-1}\mathbb{F}_q$ and $y_i = e_0y_{i,0} + e_1y_{i,1} + \cdots + e_{m-1}y_{i,m-1} \in R = e_0\mathbb{F}_q \oplus e_1\mathbb{F}_q \oplus \cdots \oplus e_{m-1}\mathbb{F}_q$. Thus, for each $x = (x_0, x_1, \dots, x_{n-1})$, $y = (y_0, y_1, \dots, y_{n-1}) \in R^n$, the Euclidean inner product is $x \cdot y = \sum_{i=0}^{n-1} x_i \cdot y_i = \sum_{i=0}^{n-1} [(e_0x_{i,0} + e_1x_{i,1} + \cdots + e_{m-1}x_{i,m-1}) \cdot (e_0y_{i,0} + e_1y_{i,1} + \cdots + e_{m-1}y_{i,m-1})] = e_0 \cdot \sum_{i=0}^{n-1} (x_{i,0} \cdot y_{i,0}) + e_1 \cdot \sum_{i=0}^{n-1} (x_{i,1} \cdot y_{i,1}) + \cdots + e_{m-1} \cdot \sum_{i=0}^{n-1} (x_{i,m-1} \cdot y_{i,m-1})$, where $e_i^2 = e_i$ and $i \neq j \Rightarrow e_i \cdot e_j = 0$.

In the continuation of the proof, the same index notation will be used for the elements x and y of R^n .

For each $x \in C^\perp \subseteq R^n \Rightarrow$ for each $y \in C \subseteq R^n$, $x \cdot y = 0_{\mathbb{F}_q} \Rightarrow e_0 \sum_{i=0}^{n-1} (x_{i,0} \cdot y_{i,0}) + e_1 \sum_{i=0}^{n-1} (x_{i,1} \cdot y_{i,1}) + \cdots + e_{m-1} \sum_{i=0}^{n-1} (x_{i,m-1} \cdot y_{i,m-1}) = 0_{\mathbb{F}_q} \Rightarrow \sum_{i=0}^{n-1} (x_{i,0} y_{i,0}) = 0_{\mathbb{F}_q}, \sum_{i=0}^{n-1} (x_{i,1} y_{i,1}) = 0_{\mathbb{F}_q}, \dots, \sum_{i=0}^{n-1} (x_{i,m-1} y_{i,m-1}) = 0_{\mathbb{F}_q}$.

Since R is an $\mathbb{F}_q$ -module and $R = e_0\mathbb{F}_q \oplus e_1\mathbb{F}_q \oplus \cdots \oplus e_{m-1}\mathbb{F}_q$, the set $\{e_0, e_1, \dots, e_{m-1}\} \subset R$ is a basis of the ring R , hence linearly independent. Therefore, for $j = 0, 1, \dots, m-1$, $(x_{0,j}, x_{1,j}, \dots, x_{n-1,j}) \in C_j^\perp$.

Thus, $x = (x_0, x_1, \dots, x_{n-1}) = (e_0x_{0,0} + e_1x_{0,1} + \cdots + e_{m-1}x_{0,m-1}, e_0x_{1,0} + e_1x_{1,1} + \cdots + e_{m-1}x_{1,m-1}, \dots, e_0x_{n-1,0} + e_1x_{n-1,1} + \cdots + e_{m-1}x_{n-1,m-1})$

$$= e_0(x_{0,0}, x_{1,0}, \dots, x_{n-1,0}) + e_1(x_{0,1}, x_{1,1}, \dots, x_{n-1,1}) \\ + \dots + e_{m-1}(x_{0,m-1}, x_{1,m-1}, \dots, x_{n-1,m-1}) \in e_0C_0^\perp \oplus e_1C_1^\perp \oplus \dots \oplus e_{m-1}C_{m-1}^\perp.$$

Indeed, since for each $x \in C^\perp \subseteq R^n$ and for each $y \in C$, $\sum_{i=0}^{n-1} (x_{i,0} \cdot y_{i,0}) = 0_{\mathbb{F}_q}$, for all $(y_{0,0}, y_{1,0}, \dots, y_{n-1,0}) \in C_0$, $(x_{0,0}, x_{1,0}, \dots, x_{n-1,0}) \cdot (y_{0,0}, y_{1,0}, \dots, y_{n-1,0}) = 0_{\mathbb{F}_q}$, therefore $(x_{0,0}, x_{1,0}, \dots, x_{n-1,0}) \in C_0^\perp$. Applying similar reasoning,

$$(x_{0,j}, x_{1,j}, \dots, x_{n-1,j}) \in C_j^\perp \text{ for } j = 1, 2, \dots, m-1.$$

Conversely, for $i = 0, 1, \dots, m-1$, let $x^{(i)} \in C_i^\perp \subseteq \mathbb{F}_q^n$. Then for each $x = e_0x^{(0)} + e_1x^{(1)} + \dots + e_{m-1}x^{(m-1)} \in e_0C_0^\perp \oplus e_1C_1^\perp \oplus \dots \oplus e_{m-1}C_{m-1}^\perp \subseteq R^n$ and for each $y = e_0y^{(0)} + e_1y^{(1)} + \dots + e_{m-1}y^{(m-1)} \in C = e_0C_0 \oplus e_1C_1 \oplus \dots \oplus e_{m-1}C_{m-1}$, we have $x \cdot y = e_0(x^{(0)} \cdot y^{(0)}) + e_1(x^{(1)} \cdot y^{(1)}) + \dots + e_{m-1}(x^{(m-1)} \cdot y^{(m-1)}) = 0_{\mathbb{F}_q}$, hence $x \in C^\perp$, and therefore $C^\perp = e_0C_0^\perp \oplus e_1C_1^\perp \oplus \dots \oplus e_{m-1}C_{m-1}^\perp$.

Moreover, from Proposition 2.4. in [13] and Proposition 1., since the code $C \subseteq R^n$ is a $(-2v^{m-1} + 1)$ -constacyclic code, the code $C^\perp \subseteq R^n$ is also a $(-2v^{m-1} + 1)$ -constacyclic code. $\square$

Definition 2. Let $f(x) = \sum_{i=0}^k f_i x^i \in \mathbb{F}_q[x]$, $f_0 \neq 0$, be a polynomial. The polynomial defined by $f^*(x) = f_0^{-1} x^{\deg f(x)} f(\frac{1}{x})$ is called the reciprocal polynomial of $f(x)$. It holds that $\deg f(x) = \deg f^*(x) = k$ and $(f^*)^*(x) = f(x)$. If $f(x) = f^*(x)$, then $f(x)$ is called a self-reciprocal polynomial; otherwise, the pair of polynomials $f(x)$ and $f^*(x)$ is called a reciprocal polynomial pair [2].

Proposition 5. Let $g(x)$ be the generator polynomial of a λ -constacyclic code C , and let $h(x) = \frac{x^n - \lambda}{g(x)}$. Then the polynomial $h^*(x)$ is the generator polynomial of the Euclidean dual code $C^\perp$ [2].

Proposition 6. If $\lambda = \mp 1$ and $C \subseteq R^n$ is a λ -constacyclic code, then the code $C^\perp \subseteq R^n$ is also a λ -constacyclic code [2].

Proof. This follows easily from Proposition 2. $\square$

Corollary 1. Let $C = e_0C_0 \oplus e_1C_1 \oplus \dots \oplus e_{m-1}C_{m-1}$ be a $(-2v^{m-1} + 1)$ -constacyclic code of length n over R . Let the polynomial $g_0(x)$ be the generator polynomial of the cyclic code C_0 , and let the polynomials $g_1(x), g_2(x), \dots, g_{m-1}(x)$ be the generator polynomials of the negacyclic codes $C_1, C_2, \dots, C_{m-1}$, respectively. In this case, for the code $C^\perp = e_0C_0^\perp \oplus e_1C_1^\perp \oplus \dots \oplus e_{m-1}C_{m-1}^\perp \subseteq R^n$, the code $C_0^\perp$ is cyclic, while the codes $C_1^\perp, C_2^\perp, \dots, C_{m-1}^\perp$ are negacyclic. Moreover, let $h_0^*(x)$ be the reciprocal polynomial of $\frac{x^n - 1}{g_0(x)}$, and let the polynomials $h_1^*(x), h_2^*(x), \dots, h_{m-1}^*(x)$ be the reciprocal polynomials of $\frac{x^n + 1}{g_1(x)}, \frac{x^n + 1}{g_2(x)}, \dots, \frac{x^n + 1}{g_{m-1}(x)}$, respectively. Then we have:

$$C^\perp = \langle e_0 h_0^*(x), e_1 h_1^*(x), \dots, e_{m-1} h_{m-1}^*(x) \rangle.$$

Proof. By using Proposition 2., Proposition 3., Proposition 4., and Proposition 5. the desired results are therefore obtained. $\square$

Lemma 1. *If $C = e_0 C_0 \oplus e_1 C_1 \oplus \cdots \oplus e_{m-1} C_{m-1}$ and $D = e_0 D_0 \oplus e_1 D_1 \oplus \cdots \oplus e_{m-1} D_{m-1}$ are linear codes of length n over R , then $C \cap D = e_0(C_0 \cap D_0) \oplus e_1(C_1 \cap D_1) \oplus \cdots \oplus e_{m-1}(C_{m-1} \cap D_{m-1})$.*

Proof. Let for each $x = e_0 x_0 + e_1 x_1 + \cdots + e_{m-1} x_{m-1} \in C \cap D$. $\Leftrightarrow e_0 x_0 + e_1 x_1 + \cdots + e_{m-1} x_{m-1} \in C = e_0 C_0 \oplus e_1 C_1 \oplus \cdots \oplus e_{m-1} C_{m-1}$, and $e_0 x_0 + e_1 x_1 + \cdots + e_{m-1} x_{m-1} \in D = e_0 D_0 \oplus e_1 D_1 \oplus \cdots \oplus e_{m-1} D_{m-1}$. $\Leftrightarrow x_0 \in C_0, x_1 \in C_1, \dots, x_{m-1} \in C_{m-1}$, and $x_0 \in D_0, x_1 \in D_1, \dots, x_{m-1} \in D_{m-1}$. $\Leftrightarrow x_0 \in (C_0 \cap D_0), x_1 \in (C_1 \cap D_1), \dots, x_{m-1} \in (C_{m-1} \cap D_{m-1})$. $\Leftrightarrow x = e_0 x_0 + e_1 x_1 + \cdots + e_{m-1} x_{m-1} \in e_0(C_0 \cap D_0) + e_1(C_1 \cap D_1) + \cdots + e_{m-1}(C_{m-1} \cap D_{m-1})$. Since for $i, j = 0, 1, \dots, m-1$ with $i \neq j$, $C_i \cap C_j = \{0_{\mathbb{F}_q^n}\}$ and $D_i \cap D_j = \{0_{\mathbb{F}_q^n}\}$, it follows that $(C_i \cap D_i) \cap (C_j \cap D_j) = \{0_{\mathbb{F}_q^n}\}$. In this case, $e_0(C_0 \cap D_0) + e_1(C_1 \cap D_1) + \cdots + e_{m-1}(C_{m-1} \cap D_{m-1}) = e_0(C_0 \cap D_0) \oplus e_1(C_1 \cap D_1) \oplus \cdots \oplus e_{m-1}(C_{m-1} \cap D_{m-1})$. Therefore, $C \cap D = e_0(C_0 \cap D_0) \oplus e_1(C_1 \cap D_1) \oplus \cdots \oplus e_{m-1}(C_{m-1} \cap D_{m-1})$. $\square$

Lemma 2. *If $C \subseteq R^n$ is a cyclic code, then $\text{Hull}(C) \subseteq R^n$ is also a cyclic code. Moreover, if $C \subseteq R^n$ is a negacyclic code, then $\text{Hull}(C) \subseteq R^n$ is also a negacyclic code.*

Proof. Since C is a cyclic code, its dual $C^\perp$ is also cyclic; and since C is a negacyclic code, its dual $C^\perp$ is also negacyclic, the proof follows easily. $\square$

Corollary 2. *If C is a $(-2v^{m-1} + 1)$ -constacyclic code of length n over R , then $\text{Hull}(C)$ is also a $(-2v^{m-1} + 1)$ -constacyclic code of length n over R .*

Proof. Since we take $D = C^\perp$ in Lemma 1. and use Proposition 2., Proposition 4., and Lemma 2., the desired result is easily obtained. $\square$

Notation. Unless otherwise stated, the least common multiple of polynomials $P(x)$ and $Q(x)$ will be denoted by $\text{lcm}(P(x), Q(x)) = [P(x), Q(x)]$, and their greatest common divisor will be denoted by $\text{gcd}(P(x), Q(x)) = (P(x), Q(x))$.

Lemma 3. *Let $p(x)$ and $q(x)$ be the generator polynomials of the λ -constacyclic codes C and D of length n over $\mathbb{F}_q$, respectively. Then $C \cap D$ is a λ -constacyclic code whose generator polynomial is $[p(x), q(x)]$ [14].*

Lemma 4. *The ring $R = e_0 \mathbb{F}_q \oplus e_1 \mathbb{F}_q \oplus \cdots \oplus e_{m-1} \mathbb{F}_q$ is an $\mathbb{F}_q$ -vector space.*

Proof. It is easily shown. $\square$

Lemma 5. $R = e_0\mathbb{F}_q \oplus e_1\mathbb{F}_q \oplus \cdots \oplus e_{m-1}\mathbb{F}_q$ is an $\mathbb{F}_q$ -vector space that is isomorphic to the $\mathbb{F}_q$ -vector space $\mathbb{F}_q^m$.

Proof. Lemma 4 states that R is an $\mathbb{F}_q$ -vector space. It is clear that $\mathbb{F}_q^m$ is also an $\mathbb{F}_q$ -vector space. Considering the map $f : R = e_0\mathbb{F}_q \oplus e_1\mathbb{F}_q \oplus \cdots \oplus e_{m-1}\mathbb{F}_q \rightarrow \mathbb{F}_q^m$ defined by $e_0\beta_0 + e_1\beta_1 + \cdots + e_{m-1}\beta_{m-1} \mapsto f(\beta) = (\beta_0, \beta_1, \dots, \beta_{m-1})$, the proof follows easily. $\square$

Corollary 3. Let C be a linear code of length n over $R = e_0\mathbb{F}_q \oplus e_1\mathbb{F}_q \oplus \cdots \oplus e_{m-1}\mathbb{F}_q$. Then, for $i = 0, 1, \dots, m-1$, define $C_i = \{x_i \in \mathbb{F}_q^n \mid \exists x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_{m-1} \in \mathbb{F}_q^n \text{ such that } e_0x_0 + e_1x_1 + \cdots + e_{m-1}x_{m-1} \in C\}$. Then $\dim(C) = \dim(C_0) + \dim(C_1) + \cdots + \dim(C_{m-1})$.

Proof. Since $C \subseteq R^n$ is an R -submodule and $\mathbb{F}_q \subseteq R$, we have that C is also an $\mathbb{F}_q$ -vector space. Moreover, for $i = 0, 1, \dots, m-1$, each $C_i \subseteq \mathbb{F}_q^n$ is a linear code, since it is closed under $\mathbb{F}_q$ -scalar multiplication and addition. Therefore, $C_0 \oplus C_1 \oplus \cdots \oplus C_{m-1} \subseteq \mathbb{F}_q^n$ is an $\mathbb{F}_q$ -vector space. Define $\xi : C = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_{m-1}C_{m-1} \subseteq R^n \rightarrow C_0 \oplus C_1 \oplus \cdots \oplus C_{m-1} \subseteq \mathbb{F}_q^n$ by $\sum_{i=0}^{m-1} e_i c_i \mapsto \xi(\sum_{i=0}^{m-1} e_i c_i) = c_0 + c_1 + \cdots + c_{m-1}$. Since every element of the direct sum $C_0 \oplus C_1 \oplus \cdots \oplus C_{m-1}$ has a unique representation, we have that ξ is injective; since ξ preserves addition and scalar multiplication and is surjective, we have that ξ is an $\mathbb{F}_q$ -vector space isomorphism. Therefore, $C = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_{m-1}C_{m-1} \cong C_0 \oplus C_1 \oplus \cdots \oplus C_{m-1}$. We have $\dim(C) = \dim(C_0 \oplus C_1 \oplus \cdots \oplus C_{m-1}) = \dim(C_0) + \dim(C_1) + \cdots + \dim(C_{m-1})$. Therefore, the result follows. $\square$

Proposition 7. Let $C = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_{m-1}C_{m-1}$ be a $(-2v^{m-1} + 1)$ -constacyclic code of length n over R , and let $g_i(x)$ be the generator polynomials of the codes C_i for $i = 0, 1, \dots, m-1$. Then there exists a unique polynomial $g(x) = e_0g_0(x) + e_1g_1(x) + \cdots + e_{m-1}g_{m-1}(x)$ such that $g(x) \mid (x^n - (-2v^{m-1} + 1))$ and $C = \langle g(x) \rangle$.

Proof. From Proposition 3., $C = \langle e_0g_0(x), e_1g_1(x), \dots, e_{m-1}g_{m-1}(x) \rangle$. Since $g(x) = e_0g_0(x) + e_1g_1(x) + \cdots + e_{m-1}g_{m-1}(x)$, it is clear that $\langle g(x) \rangle \subseteq C$. On the other hand, since e_i are orthogonal idempotents for $i = 0, 1, \dots, m-1$, we have $e_0g_0(x) = e_0g(x)$, $e_1g_1(x) = e_1g(x)$, $\dots$, $e_{m-1}g_{m-1}(x) = e_{m-1}g(x)$. Therefore $C \subseteq \langle g(x) \rangle$, hence $g(x)$ is a generator polynomial of C .

Moreover, since C_0 is cyclic and $C_1, C_2, \dots, C_{m-1}$ are negacyclic codes, it follows that $g_0(x) \mid (x^n - 1)$, $g_1(x) \mid (x^n + 1)$, $g_2(x) \mid (x^n + 1)$, $\dots$, $g_{m-1}(x) \mid (x^n + 1)$. Hence there exist polynomials $r_i(x) \in \mathbb{F}_q[x]$ for $i = 0, 1, \dots, m-1$ such that $x^n - 1 = g_0(x)r_0(x)$, $x^n + 1 = g_1(x)r_1(x)$, $x^n + 1 = g_2(x)r_2(x)$, $\dots$, $x^n + 1 = g_{m-1}(x)r_{m-1}(x)$.

On the other hand, $(e_0g_0(x) + e_1g_1(x) + \cdots + e_{m-1}g_{m-1}(x))(e_0r_0(x) + e_1r_1(x) + \cdots + e_{m-1}r_{m-1}(x)) = e_0g_0(x)r_0(x) + e_1g_1(x)r_1(x) + \cdots + e_{m-1}g_{m-1}(x)r_{m-1}(x) = e_0(x^n - 1) + e_1(x^n + 1) + \cdots + e_{m-1}(x^n + 1) = (e_0 + e_1 + \cdots + e_{m-1})x^n + (-e_0 + (e_1 + \cdots + e_{m-1})) = x^n - (2e_0 - 1) = x^n - (-2v^{m-1} + 1)$. Thus $g(x) \mid (x^n - (-2v^{m-1} + 1))$.

Since R is an $\mathbb{F}_q$ -vector space and $\{e_0, e_1, \dots, e_{m-1}\} \subset R$ forms a basis, the expression $g(x) = e_0g_0(x) + e_1g_1(x) + \cdots + e_{m-1}g_{m-1}(x)$ is unique. $\square$

4 Hulls of $(-2v^{m-1} + 1)$ -Constacyclic Codes over the Ring R

In Section 2.3 of [2], the authors provide a factorization method for the polynomials $x^n - 1$ and $x^n + 1$ in the polynomial ring $\mathbb{F}_q[x]$. In this work, we shall use the same notation.

Theorem 1. *Let $C = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_{m-1}C_{m-1}$ be a $(-2v^{m-1} + 1)$ -constacyclic code of length n over R . Let $g_0(x)$ be the generator polynomial of the cyclic code C_0 , and let $g_1(x), g_2(x), \dots, g_{m-1}(x)$ be the generator polynomials of the negacyclic codes $C_1, C_2, \dots, C_{m-1}$, respectively. Let $h_0^*(x)$ denote the reciprocal polynomial of $\frac{x^n-1}{g_0(x)}$, and let $h_1^*(x), h_2^*(x), \dots, h_{m-1}^*(x)$ denote the reciprocal polynomials of $\frac{x^n+1}{g_1(x)}, \frac{x^n+1}{g_2(x)}, \dots, \frac{x^n+1}{g_{m-1}(x)}$, respectively. Then $\text{Hull}(C) = C \cap C^\perp = \langle e_0[g_0(x), h_0^*(x)], e_1[g_1(x), h_1^*(x)], \dots, e_{m-1}[g_{m-1}(x), h_{m-1}^*(x)] \rangle$.*

Proof. If $C = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_{m-1}C_{m-1}$ is a $(-2v^{m-1} + 1)$ -constacyclic code of length n over R , then, since Proposition 2. implies that C_0 is a cyclic code and that for $i = 1, 2, \dots, m-1$ the codes C_i are negacyclic codes, we have, by Proposition 3., that if $g_0(x)$ is the generator polynomial of the cyclic code C_0 and $g_1(x), g_2(x), \dots, g_{m-1}(x)$ are the generator polynomials of the negacyclic codes $C_1, C_2, \dots, C_{m-1}$, then $C = \langle e_0g_0(x), e_1g_1(x), \dots, e_{m-1}g_{m-1}(x) \rangle$. Moreover, if $h_0^*(x)$ is the reciprocal polynomial of $\frac{x^n-1}{g_0(x)}$ and $h_1^*(x), h_2^*(x), \dots, h_{m-1}^*(x)$ are the reciprocal polynomials of $\frac{x^n+1}{g_1(x)}, \frac{x^n+1}{g_2(x)}, \dots, \frac{x^n+1}{g_{m-1}(x)}$, then, since Proposition 4. and Corollary 1. describe the duals, we have $C^\perp = e_0C_0^\perp \oplus e_1C_1^\perp \oplus \cdots \oplus e_{m-1}C_{m-1}^\perp = \langle e_0h_0^*(x), e_1h_1^*(x), \dots, e_{m-1}h_{m-1}^*(x) \rangle$. Since, by Lemma 4., for $i = 0, 1, \dots, m-1$ the generator polynomials of $\text{Hull}(C_i) = C_i \cap C_i^\perp$ are $[g_i(x), h_i^*(x)]$, and since Lemma 1., Lemma 2. and Proposition 3. describe how direct-sum decompositions and generator polynomials combine, we have $\text{Hull}(C) = C \cap C^\perp = \langle e_0[g_0(x), h_0^*(x)], e_1[g_1(x), h_1^*(x)], \dots, e_{m-1}[g_{m-1}(x), h_{m-1}^*(x)] \rangle$. $\square$

Lemma 6. *For all $P(x), Q(x) \in \mathbb{F}_q[x]$, we have $[P(x) \cdot Q(x)]^* = P^*(x) \cdot Q^*(x)$.*

Proof. Let $P(x), Q(x) \in \mathbb{F}_q[x]$ with leading coefficients P_0 and Q_0 , respectively. Then $(P(x)Q(x))^* = (P_0Q_0)^{-1}x^{\deg P + \deg Q}P(1/x)Q(1/x)$
 $= (P_0^{-1}x^{\deg P}P(1/x))(Q_0^{-1}x^{\deg Q}Q(1/x)) = P^*(x)Q^*(x).$ $\square$

Corollary 4. *For all reciprocal polynomial pairs $f(x), f^*(x) \in \mathbb{F}_q[x]$, the product polynomial $f(x)f^*(x) \in \mathbb{F}_q[x]$ is also self-reciprocal.*

Proof. Let $f(x), f^*(x) \in \mathbb{F}_q[x]$ be a reciprocal polynomial pair. Since Lemma 6. implies $(f(x)f^*(x))^* = f^*(x)(f^*(x))^* = f^*(x)f(x)$, therefore $f(x)f^*(x)$ is a self-reciprocal polynomial. $\square$

Theorem 2. *Let $n \in \mathbb{Z}_+$, p be a prime, ε a nonnegative integer, and $(p, \bar{n}) = 1$ so that $n = \bar{n}p^\varepsilon$. Let q be a power of p , and define $N_q = \{\ell \geq 1 \mid \exists k \geq 0 \text{ such that } \ell \mid (q^k + 1)\}$. Let Φ be Euler's totient function, and set $\gamma_0(i, q) = \Phi(i)/\text{ord}_i(q)$ for $i \mid \bar{n}$, $i \in N_q$, $\beta_0(i, q) = \Phi(i)/(2\text{ord}_i(q))$ for $i \mid \bar{n}$, $i \notin N_q$. For $\omega = 1, 2, \dots, m-1$, set $\gamma_\omega(j, q) = \Phi(j)/\text{ord}_j(q)$ for $j \mid 2\bar{n}$, $j \nmid \bar{n}$, $j \in N_q$, $\beta_\omega(j, q) = \Phi(j)/(2\text{ord}_j(q))$ for $j \mid 2\bar{n}$, $j \nmid \bar{n}$, $j \notin N_q$.*

Let $R = \mathbb{F}_q + v\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$ with $q = p^s$, $m-1 \mid (p-1)$, $v^m = v$. Then the hull dimensions of $(-2v^{m-1} + 1)$ -constacyclic codes satisfy $0 \leq a_i \leq \gamma_0(i, q)\lfloor p^\varepsilon/2 \rfloor$, $0 \leq b_i \leq \beta_0(i, q)p^\varepsilon$, $0 \leq c_{\omega, j} \leq \gamma_\omega(j, q)\lfloor p^\varepsilon/2 \rfloor$, $0 \leq d_{\omega, j} \leq \beta_\omega(j, q)p^\varepsilon$. Since

$$\text{Hull}(C) = \sum_{\substack{i \mid \bar{n} \\ i \in N_q}} \text{ord}_i(q) a_i + \sum_{\substack{i \mid \bar{n} \\ i \notin N_q}} \text{ord}_i(q) b_i + \sum_{\substack{j \mid 2\bar{n}, j \nmid \bar{n} \\ j \in N_q \\ \omega=1, \dots, m-1}} \text{ord}_j(q) c_{\omega, j} + \sum_{\substack{j \mid 2\bar{n}, j \nmid \bar{n} \\ j \notin N_q \\ \omega=1, \dots, m-1}} \text{ord}_j(q) d_{\omega, j}$$

Proof. From Section 2.3 of [2]: let i and j be coprime positive integers, $\text{ord}_j(i)$ the order of i modulo j , q a power of a prime number p , and for $n \in \mathbb{Z}_+$ we have $n = \bar{n}p^\varepsilon$ with $(p, \bar{n}) = 1$ and $\varepsilon \in \mathbb{Z}_+ \cup \{0\}$. Define $N_q = \{\ell \geq 1 \mid \exists k \geq 0 \text{ such that } \ell \mid (q^k + 1)\}$, Φ the Euler totient function, $\gamma_0(i, q) = \Phi(i)/\text{ord}_i(q)$, $\beta_0(i, q) = \Phi(i)/(2\text{ord}_i(q))$, where $g_{ki}(x)$ is a monic irreducible self-reciprocal polynomial of degree $\text{ord}_i(q)$, and $f_{ki}(x)$, $f_{ki}^*(x)$ are irreducible reciprocal polynomial pairs of degree $\text{ord}_i(q)$. Then from Section 2.3 of [2] we know that

$$x^n - 1 = (x^{\bar{n}} - 1)^{p^\varepsilon} = \left[\prod_{\substack{i \mid \bar{n} \\ i \in N_q}} \left(\prod_{k=1}^{\gamma_0(i, q)} g_{ki}(x) \right) \cdot \prod_{\substack{i \mid \bar{n} \\ i \notin N_q}} \left(\prod_{k=1}^{\beta_0(i, q)} f_{ki}(x) f_{ki}^*(x) \right) \right]^{p^\varepsilon} \quad (1)$$

That is, for each $i \mid \bar{n}$ with $i \in N_q$, there are $\gamma_0(i, q)$ monic irreducible self-reciprocal factors of degree $\text{ord}_i(q)$, and for each $i \mid \bar{n}$ with $i \notin N_q$, there are $\beta_0(i, q)$ reciprocal polynomial pairs $(f_{ki}(x), f_{ki}^*(x))$ of the same degree.

There is a one-to-one correspondence between λ -constacyclic codes of length n over $\mathbb{F}_q$ and the monic divisors of $x^n - \lambda$ [15]. Hence, cyclic-code enumeration corresponds to the factorization of $x^n - 1$, whereas constacyclic-code enumeration corresponds to the factorization of $x^n + 1$. If we write $x^n - 1 = \prod_{i|\bar{n}} Q_i(x)$, then

$$(x^{\bar{n}} - 1)(x^{\bar{n}} + 1) = x^{2\bar{n}} - 1 = \prod_{j|2\bar{n}} Q_j(x),$$

and the factors satisfying $j \mid 2\bar{n}$ and $j \nmid \bar{n}$ are the ones associated with the factorization of $x^n + 1$.

Let $r_{tj}(x)$ be a self-reciprocal polynomial of degree $\text{ord}_j(q)$, and let $s_{tj}(x)$, $s_{tj}^*(x)$ be a reciprocal irreducible pair of the same degree. For $w = 1, 2, \dots, m-1$, define $\gamma_w(j, q) = \Phi(j)/\text{ord}_j(q)$ and $\beta_w(j, q) = \Phi(j)/(2 \text{ord}_j(q))$. Then

$$x^n + 1 = (x^{\bar{n}} + 1)^{p^\varepsilon} = \left[\prod_{\substack{j|2\bar{n} \\ j \nmid \bar{n} \\ j \in N_q}} \left(\prod_{t=1}^{\gamma_w(j, q)} r_{tj}(x) \right) \cdot \prod_{\substack{j|2\bar{n} \\ j \nmid \bar{n} \\ j \notin N_q}} \left(\prod_{t=1}^{\beta_w(j, q)} s_{tj}(x) s_{tj}^*(x) \right) \right]^{p^\varepsilon} \quad (2)$$

Primarily, in order to find the number of cyclic codes, if we focus on determining the number of factors of the polynomial $x^n - 1$; from equation (1), any monic divisor of the polynomial $x^n - 1$ can be expressed as $g_0(x) = \prod_{i \in N_q} \left(\prod_{k=1}^{\gamma_0(i, q)} (g_{ki}(x))^{u_{ki}} \right) \cdot \prod_{i \notin N_q} \left(\prod_{k=1}^{\beta_0(i, q)} [(f_{ki}(x))^{v_{ki}} (f_{ki}^*(x))^{w_{ki}}] \right)$, where

$0 \leq u_{ki}, v_{ki}, w_{ki} \leq p^\varepsilon$. (It should be noted that in the products appearing in this expression, taking the upper bounds as $\gamma_0(i, q)$ and $\beta_0(i, q)$ does not mean that all factors $g_{ki}(x)$ are chosen; choosing $u_{ki} = 0$, or similarly $v_{ki} = 0$, $w_{ki} = 0$, implies that the corresponding factor is not selected.) The check polynomial $h_0(x)$ of the polynomial $g_0(x)$ is given by $h_0(x) = \frac{x^n - 1}{g_0(x)} = \frac{(x^{\bar{n}} - 1)^{p^\varepsilon}}{g_0(x)} =$

$$\frac{\left[\prod_{i \in N_q} \left(\prod_{k=1}^{\gamma_0(i, q)} g_{ki}(x) \right) \cdot \prod_{i \notin N_q} \left(\prod_{k=1}^{\beta_0(i, q)} f_{ki}(x) f_{ki}^*(x) \right) \right]^{p^\varepsilon}}{\prod_{i \in N_q} \left(\prod_{k=1}^{\gamma_0(i, q)} (g_{ki}(x))^{u_{ki}} \right) \cdot \prod_{i \notin N_q} \left(\prod_{k=1}^{\beta_0(i, q)} [(f_{ki}(x))^{v_{ki}} (f_{ki}^*(x))^{w_{ki}}] \right)}. \text{ When}$$

the fact that the exponent p^ε in the numerator represents the power of each factor is taken into account and the expression is rearranged, we obtain $h_0(x) = \prod_{i \in N_q} \left(\prod_{k=1}^{\gamma_0(i, q)} (g_{ki}(x))^{p^\varepsilon - u_{ki}} \right) \cdot \prod_{i \notin N_q} \left(\prod_{k=1}^{\beta_0(i, q)} [(f_{ki}(x))^{p^\varepsilon - v_{ki}} (f_{ki}^*(x))^{p^\varepsilon - w_{ki}}] \right)$.

Considering from Lemma 8. that the reciprocal of the product of polynomials equals the product of their reciprocals, since $g_{ki}(x)$ is self-reciprocal, so that $g_{ki}^*(x) = g_{ki}(x)$, and since $(f_{ki}^*)^*(x) = f_{ki}(x)$ holds, so that

$(f_{ki}^*(x))^{p^\varepsilon - v_{ki}} (f_{ki}(x))^{p^\varepsilon - w_{ki}}$ appears in the factorization, we have

$$h_0^*(x) = \prod_{\substack{i|\overline{n} \\ i \in N_q}} \left(\prod_{k=1}^{\gamma_0(i,q)} (g_{ki}(x))^{p^\varepsilon - u_{ki}} \right) \cdot \prod_{\substack{i|\overline{n} \\ i \notin N_q}} \left(\prod_{k=1}^{\beta_0(i,q)} (f_{ki}(x))^{p^\varepsilon - w_{ki}} (f_{ki}^*(x))^{p^\varepsilon - v_{ki}} \right)$$

. From Theorem 1., the hull dimensions of $(-2v^{m-1} + 1)$ -constacyclic codes of length n over R can be obtained from the dimensions of the codes $Hull(C_0)$, $Hull(C_1)$, $Hull(C_2)$, $\dots$, $Hull(C_{m-1})$ for the cyclic code C_0 and the negacyclic codes $C_1, C_2, \dots, C_{m-1}$ over $\mathbb{F}_q$. Therefore, it is necessary to compute the degrees of the polynomials $[g_0(x), h_0^*(x)]$, $[g_1(x), h_1^*(x)]$, $[g_2(x), h_2^*(x)]$, $\dots$, $[g_{m-1}(x), h_{m-1}^*(x)]$.

$$\begin{aligned} \text{We have } [g_0(x), h_0^*(x)] &= \prod_{\substack{i|\overline{n} \\ i \in N_q}} \left(\prod_{k=1}^{\gamma_0(i,q)} (g_{ki}(x))^{\max\{u_{ki}, p^\varepsilon - u_{ki}\}} \right) \\ &\cdot \prod_{\substack{i|\overline{n} \\ i \notin N_q}} \left(\prod_{k=1}^{\beta_0(i,q)} [(f_{ki}(x))^{\max\{v_{ki}, p^\varepsilon - w_{ki}\}} (f_{ki}^*(x))^{\max\{w_{ki}, p^\varepsilon - v_{ki}\}}] \right) \quad (3). \end{aligned}$$

If the exponent $\max\{u_{ki}, p^\varepsilon - u_{ki}\}$ is examined, let $x \in \mathbb{N} \cup \{0\}$ be a variable, and let p^ε be a fixed natural number. Define $\max\{x, p^\varepsilon - x\} = y$. If $x \geq p^\varepsilon - x$ (in this case $x = y$), then $2x \geq p^\varepsilon \Rightarrow x \geq p^\varepsilon/2 \Rightarrow y = x \geq p^\varepsilon/2$. If $p^\varepsilon - x \geq x$ (in this case $p^\varepsilon - x = y$), then $p^\varepsilon \geq 2x \Rightarrow p^\varepsilon/2 \geq x$. If $x = p^\varepsilon/2$ is chosen, then $p^\varepsilon - x = p^\varepsilon - p^\varepsilon/2 = p^\varepsilon/2$, which is the minimum value that the expression $p^\varepsilon - x$ can take. For the smallest value of $x \in \mathbb{N} \cup \{0\}$, the expression $p^\varepsilon - x$ takes its maximum value. Therefore, for $x = 0$, we obtain $y = p^\varepsilon$. Thus, $\lfloor p^\varepsilon/2 \rfloor \leq \max\{u_{ki}, p^\varepsilon - u_{ki}\} \leq p^\varepsilon$. (If polynomial exponents must be positive integers, then $\lfloor p^\varepsilon/2 \rfloor$ may be used.) Now, similarly, if we examine the exponent $\max\{v_{ki}, p^\varepsilon - w_{ki}\} + \max\{w_{ki}, p^\varepsilon - v_{ki}\}$, let $x, y \in \mathbb{N} \cup \{0\}$ be variables and let p^ε be a fixed number. Define $z = \max\{x, p^\varepsilon - y\} + \max\{y, p^\varepsilon - x\}$.

Case I. Suppose $x \geq p^\varepsilon - y$. If $x \geq p^\varepsilon - y$, we have $y \geq p^\varepsilon - x$, therefore $z = \max\{x, p^\varepsilon - y\} + \max\{y, p^\varepsilon - x\} = x + y$.

Case II. Suppose $x \leq p^\varepsilon - y$. If $x \leq p^\varepsilon - y$, we have $y \leq p^\varepsilon - x$, therefore $z = \max\{x, p^\varepsilon - y\} + \max\{y, p^\varepsilon - x\} = 2p^\varepsilon - (x + y)$, hence $z = \max\{x + y, 2p^\varepsilon - (x + y)\}$.

In this case, it is observed that the value of z changes depending on $x + y$. For $x + y = 0$, z takes its maximum value $2p^\varepsilon$. Its minimum value is attained if $x = p^\varepsilon - y$, in which case $z = p^\varepsilon$, therefore $p^\varepsilon \leq \max\{v_{ki}, p^\varepsilon - w_{ki}\} + \max\{w_{ki}, p^\varepsilon - v_{ki}\} \leq 2p^\varepsilon$. In light of the information in Section 2.3 of [2], if similar calculations are carried out for the factorization of the polynomial $x^n + 1 \in \mathbb{F}_q[x]$, then for $w = 1, 2, \dots, m-1$ we have $g_w(x) = \prod_{\substack{j|2\overline{n} \\ j \nmid \overline{n} \\ j \in N_q}} \left(\prod_{t=1}^{\gamma_w(j,q)} (r_{tj}(x))^{x_{tj}} \right)$

$$\begin{aligned}
 & \cdot \prod_{\substack{j|2\bar{n} \\ j \nmid \bar{n} \\ j \notin N_q}} \left(\prod_{t=1}^{\beta_w(j,q)} [(s_{tj}(x))^{y_{tj}} (s_{tj}^*(x))^{z_{tj}}] \right), \text{ and } h_w(x) = \frac{x^n + 1}{g_w(x)} \\
 & = \prod_{\substack{j|2\bar{n} \\ j \nmid \bar{n} \\ j \in N_q}} \left(\prod_{t=1}^{\gamma_w(j,q)} (r_{tj}(x))^{p^\varepsilon - x_{tj}} \right) \cdot \prod_{\substack{j|2\bar{n} \\ j \nmid \bar{n} \\ j \notin N_q}} \left(\prod_{t=1}^{\beta_w(j,q)} [(s_{tj}(x))^{p^\varepsilon - y_{tj}} (s_{tj}^*(x))^{p^\varepsilon - z_{tj}}] \right) \\
 & \text{and hence } h_w^*(x) = \prod_{\substack{j|2\bar{n} \\ j \nmid \bar{n} \\ j \in N_q}} \left(\prod_{t=1}^{\gamma_w(j,q)} (r_{tj}(x))^{p^\varepsilon - x_{tj}} \right) \\
 & \cdot \prod_{\substack{j|2\bar{n} \\ j \nmid \bar{n} \\ j \notin N_q}} \left(\prod_{t=1}^{\beta_w(j,q)} [(s_{tj}(x))^{p^\varepsilon - z_{tj}} (s_{tj}^*(x))^{p^\varepsilon - y_{tj}}] \right). \text{ Therefore, } [g_w(x), h_w^*(x)] = \\
 & \prod_{\substack{j|2\bar{n} \\ j \nmid \bar{n} \\ j \in N_q}} \left(\prod_{t=1}^{\gamma_w(j,q)} (r_{tj}(x))^{\max\{x_{tj}, p^\varepsilon - x_{tj}\}} \right) \\
 & \cdot \prod_{\substack{j|2\bar{n} \\ j \nmid \bar{n} \\ j \notin N_q}} \left(\prod_{t=1}^{\beta_w(j,q)} [(s_{tj}(x))^{\max\{y_{tj}, p^\varepsilon - z_{tj}\}} (s_{tj}^*(x))^{\max\{z_{tj}, p^\varepsilon - y_{tj}\}}] \right) \dots (4).
 \end{aligned}$$

$(\lfloor p^\varepsilon/2 \rfloor \leq \max\{x_{tj}, p^\varepsilon - x_{tj}\} \leq p^\varepsilon, \quad p^\varepsilon \leq \max\{v_{ki}, p^\varepsilon - w_{ki}\} + \max\{w_{ki}, p^\varepsilon - v_{ki}\} \leq 2p^\varepsilon)$. Moreover, $g_0(x)$ and $h_0^*(x)$ are monic divisors of the polynomial $x^n - 1$, and for $w = 1, 2, \dots, m-1$, the polynomials $g_w(x)$ and $h_w^*(x)$ are monic divisors of the polynomial $x^n + 1$ [2]. From Corollary 3., it is known that $\text{boy}(C) = \text{boy}(C_1) + \text{boy}(C_2) + \cdots + \text{boy}(C_{m-1})$, and $\text{Hull}(C) = C \cap C^\perp = (e_0 C_0 \oplus e_1 C_1 \oplus \cdots \oplus e_{m-1} C_{m-1}) \cap (e_0 C_0^\perp \oplus e_1 C_1^\perp \oplus \cdots \oplus e_{m-1} C_{m-1}^\perp) = e_0(C_0 \cap C_0^\perp) \oplus e_1(C_1 \cap C_1^\perp) \oplus \cdots \oplus e_{m-1}(C_{m-1} \cap C_{m-1}^\perp) = e_0 \text{Hull}(C_0) \oplus e_1 \text{Hull}(C_1) \oplus \cdots \oplus e_{m-1} \text{Hull}(C_{m-1})$.

Moreover, $g_0(x)$ and $h_0^*(x)$ are monic divisors of the polynomial $x^n - 1$, and for $w = 1, 2, \dots, m-1$, the polynomials $g_w(x)$ and $h_w^*(x)$ are monic divisors of the polynomial $x^n + 1$ [2]. From Corollary 3., it is known that $\text{boy}(C) = \text{boy}(C_1) + \text{boy}(C_2) + \cdots + \text{boy}(C_{m-1})$, and $\text{Hull}(C) = C \cap C^\perp = (e_0 C_0 \oplus e_1 C_1 \oplus \cdots \oplus e_{m-1} C_{m-1}) \cap (e_0 C_0^\perp \oplus e_1 C_1^\perp \oplus \cdots \oplus e_{m-1} C_{m-1}^\perp) = e_0(C_0 \cap C_0^\perp) \oplus e_1(C_1 \cap C_1^\perp) \oplus \cdots \oplus e_{m-1}(C_{m-1} \cap C_{m-1}^\perp) = e_0 \text{Hull}(C_0) \oplus e_1 \text{Hull}(C_1) \oplus \cdots \oplus e_{m-1} \text{Hull}(C_{m-1})$.

If Corollary 3. is considered for the linear code $\text{Hull}(C) \subseteq R^n$, then $\text{boy}(\text{Hull}(C)) = \text{boy}(\text{Hull}(C_1)) + \text{boy}(\text{Hull}(C_2)) + \cdots + \text{boy}(\text{Hull}(C_{m-1})) = (n - \deg[g_0(x), h_0^*(x)]) + (n - \deg[g_1(x), h_1^*(x)]) + \cdots + (n - \deg[g_{m-1}(x), h_{m-1}^*(x)])$.

Now, in light of the studies carried out above for the factorization of the polynomials $x^n + 1$ and $x^n - 1$, the expressions for n , $\deg[g_0(x), h_0^*(x)]$, $\deg[g_1(x), h_1^*(x)]$, $\dots$, $\deg[g_{m-1}(x), h_{m-1}^*(x)]$ are obtained as follows: For the expression to be substituted in place of n , let us consider the factorization of the polynomial $x^n - 1$:

$$x^n - 1 = (x^{\bar{n}} - 1)^{p^\varepsilon} = \left[\prod_{i \in N_q} \prod_{k=1}^{\gamma_0(i,q)} g_{ki}(x) \cdot \prod_{i \notin N_q} \prod_{k=1}^{\beta_0(i,q)} f_{ki}(x) f_{ki}^*(x) \right]^{p^\varepsilon}.$$

For a fixed value of i satisfying the corresponding conditions in the product, the expression $\prod_{k=1}^{\gamma_0(i,q)} g_{ki}(x)$ is the product of $\gamma_0(i, q)$ polynomials, each of degree $\text{ord}_i(q)$. Hence, this product has degree $\text{ord}_i(q)\gamma_0(i, q)$.

On the other hand, in the expression $\prod_{k=1}^{\beta_0(i,q)} f_{ki}(x) f_{ki}^*(x)$, each polynomial product $f_{ki}(x) f_{ki}^*(x)$ has degree $2\text{ord}_i(q)$. Since there are $\beta_0(i, q)$ such factors, the total degree is $2\text{ord}_i(q)\beta_0(i, q)$. Moreover, since the degree of the product of polynomials equals the sum of the degrees of the multiplied polynomials, we obtain:

$$\begin{aligned} & \left(\sum_{i \in N_q} \text{ord}_i(q)\gamma_0(i, q) + \sum_{i \notin N_q} 2\text{ord}_i(q)\beta_0(i, q) \right) \cdot p^\varepsilon \\ &= \sum_{i \in N_q} \left[\text{ord}_i(q) \sum_{k=1}^{\gamma_0(i,q)} p^\varepsilon \right] + \sum_{i \notin N_q} \left[2\text{ord}_i(q) \sum_{k=1}^{\beta_0(i,q)} p^\varepsilon \right] = n \end{aligned}$$

(written as $\sum_{k=1}^{\gamma_0(i,q)} p^\varepsilon$ for analogy with the factorization).

The degree of $[g_0(x), h_0^*(x)]$ is obtained by an analogous reasoning as follows: $[g_0(x), h_0^*(x)] = \prod_{i \in N_q} \left(\prod_{k=1}^{\gamma_0(i,q)} (g_{ki}(x))^{\max\{u_{ki}, p^\varepsilon - u_{ki}\}} \right) \cdot \prod_{i \notin N_q} \left(\prod_{k=1}^{\beta_0(i,q)} [(f_{ki}(x))^{\max\{v_{ki}, p^\varepsilon - w_{ki}\}} (f_{ki}^*(x))^{\max\{w_{ki}, p^\varepsilon - v_{ki}\}}] \right)$ for a fixed index i satisfying the above conditions.

In the product $\prod_{k=1}^{\gamma_0(i,q)} (g_{ki}(x))^{\max\{u_{ki}, p^\varepsilon - u_{ki}\}}$ there are $\gamma_0(i, q)$ polynomials, each of degree $\text{ord}_i(q) \cdot \max\{u_{ki}, p^\varepsilon - u_{ki}\}$. Hence the degree of this product polynomial is $\text{ord}_i(q) \cdot \gamma_0(i, q) \cdot \max\{u_{ki}, p^\varepsilon - u_{ki}\}$.

$$\begin{aligned} & \text{Consequently, the degree of the polynomial } \prod_{i \in N_q} \left(\prod_{k=1}^{\gamma_0(i,q)} (g_{ki}(x))^{\max\{u_{ki}, p^\varepsilon - u_{ki}\}} \right) \\ & \text{is } \sum_{i \in N_q} \left(\text{ord}_i(q) \cdot \gamma_0(i, q) \cdot \max\{u_{ki}, p^\varepsilon - u_{ki}\} \right) \\ &= \sum_{i \in N_q} \left(\text{ord}_i(q) \cdot \sum_{k=1}^{\gamma_0(i,q)} \max\{u_{ki}, p^\varepsilon - u_{ki}\} \right). \end{aligned}$$

For the product $\prod_{k=1}^{\beta_0(i,q)} [(f_{ki}(x))^{\max\{v_{ki}, p^\varepsilon - w_{ki}\}} (f_{ki}^*(x))^{\max\{w_{ki}, p^\varepsilon - v_{ki}\}}]$ there are $\beta_0(i, q)$ factors (for the fixed index i satisfying the stated conditions), and each factor has degree $\text{ord}_i(q) \max\{v_{ki}, p^\varepsilon - w_{ki}\} + \text{ord}_i(q) \max\{w_{ki}, p^\varepsilon - v_{ki}\}$. Therefore the degree of the entire product equals $\text{ord}_i(q) \beta_0(i, q) (\max\{v_{ki}, p^\varepsilon - w_{ki}\} + \max\{w_{ki}, p^\varepsilon - v_{ki}\})$.

Let $P(x) = \prod_{\substack{i|\bar{n} \\ i \notin N_q}} \left(\prod_{k=1}^{\beta_0(i,q)} (f_{ki}(x))^{\max\{v_{ki}, p^\varepsilon - w_{ki}\}} (f_{ki}^*(x))^{\max\{w_{ki}, p^\varepsilon - v_{ki}\}} \right)$. Then

the degree of $P(x)$ is $\sum_{\substack{i|\bar{n} \\ i \notin N_q}} \left[\text{ord}_i(q) \beta_0(i, q) (\max\{v_{ki}, p^\varepsilon - w_{ki}\} + \max\{w_{ki}, p^\varepsilon - v_{ki}\}) \right]$, which can be written equivalently as $\sum_{\substack{i|\bar{n} \\ i \notin N_q}} \left[\text{ord}_i(q) \sum_{k=1}^{\beta_0(i,q)} (\max\{v_{ki}, p^\varepsilon - w_{ki}\} + \max\{w_{ki}, p^\varepsilon - v_{ki}\}) \right]$. Therefore, $n - \deg[g_0(x), h_0^*(x)]$

$$= \left(\sum_{i \in N_q} i|n \left[\text{ord}_i(q) \sum_{k=1}^{\gamma_0(i,q)} p^\varepsilon \right] + \sum_{i \notin N_q} i|n \left[2 \text{ord}_i(q) \sum_{k=1}^{\beta_0(i,q)} p^\varepsilon \right] \right) - \sum_{i \in N_q} i|\bar{n} \left(\text{ord}_i(q) \cdot \sum_{k=1}^{\gamma_0(i,q)} \max\{u_{ki}, p^\varepsilon - u_{ki}\} \right) - \sum_{i \notin N_q} i|\bar{n} \left(\text{ord}_i(q) \cdot \sum_{k=1}^{\beta_0(i,q)} (\max\{v_{ki}, p^\varepsilon - w_{ki}\} + \max\{w_{ki}, p^\varepsilon - v_{ki}\}) \right).$$

Similarly, carrying out the same computation for $x^n + 1$ and for the polynomials $[g_1(x), h_1^*(x)]$, $[g_2(x), h_2^*(x)]$, $\dots$, $[g_{m-1}(x), h_{m-1}^*(x)]$, we obtain the following expression for $n - \deg[g_1(x), h_1^*(x)]$:

$$n - \deg[g_1(x), h_1^*(x)] = \left(\sum_{\substack{j|2\bar{n} \\ j \notin N_q}} j|2\bar{n} \left[\text{ord}_{d_j}(q) \sum_{t=1}^{\gamma_1(j,q)} p^\varepsilon \right] + \sum_{\substack{j|2\bar{n} \\ j \notin N_q}} j|2\bar{n} \left[\text{ord}_{d_j}(q) \sum_{t=1}^{\beta_1(j,q)} 2p^\varepsilon \right] \right) - \sum_{\substack{j|2\bar{n} \\ j \notin N_q}} j|2\bar{n} \left[\text{ord}_{d_j}(q) \sum_{t=1}^{\gamma_1(j,q)} \max\{x_{tj}, p^\varepsilon - x_{tj}\} \right] - \sum_{\substack{j|2\bar{n} \\ j \notin N_q}} j|2\bar{n} \left[\text{ord}_{d_j}(q) \sum_{t=1}^{\beta_1(j,q)} (\max\{y_{tj}, p^\varepsilon - z_{tj}\} + \max\{z_{tj}, p^\varepsilon - y_{tj}\}) \right].$$

Moreover, it is known from Proposition 2. that the code $C = e_0 C_0 \oplus e_1 C_1 \oplus \cdots \oplus e_{m-1} C_{m-1} \subseteq R^n$ is a $(-2v^{m-1} + 1)$ -constacyclic code of length n over R if and only if the code C_0 is cyclic and, for $i = 1, 2, \dots, m-1$, the codes C_i are negacyclic.

Therefore, in order to compute the values $(n - \deg[g_2(x), h_2^*(x)])$, $(n - \deg[g_3(x), h_3^*(x)])$, $\dots$, $(n - \deg[g_{m-1}(x), h_{m-1}^*(x)])$, the same procedure as for determining $n - \deg[g_1(x), h_1^*(x)]$ will be applied.

$$\begin{aligned}
 & \text{In the light of this information; } \text{boy}(\text{Hull}(C)) = (n - \deg[g_0(x), h_0^*(x)]) + \\
 & (n - \deg[g_1(x), h_1^*(x)]) + \cdots + (n - \deg[g_{m-1}(x), h_{m-1}^*(x)]) \\
 & = \left(\sum_{i \in N_q} i|\bar{n} [\text{ord}_i(q) \sum_{k=1}^{\gamma_0(i,q)} p^\varepsilon] + \sum_{i \notin N_q} i|\bar{n} [\text{ord}_i(q) \sum_{k=1}^{\beta_0(i,q)} 2p^\varepsilon] \right) \\
 & - \sum_{i \in N_q} i|\bar{n} [\text{ord}_i(q) \sum_{k=1}^{\gamma_0(i,q)} \max\{u_{ki}, p^\varepsilon - u_{ki}\}] \\
 & - \sum_{i \notin N_q} i|\bar{n} [\text{ord}_i(q) \sum_{k=1}^{\beta_0(i,q)} (\max\{v_{ki}, p^\varepsilon - w_{ki}\} + \max\{w_{ki}, p^\varepsilon - v_{ki}\})] \\
 & + \left(\sum_{\substack{j|2\bar{n} \\ j \nmid \bar{n} \\ j \in N_q \\ w=1}}^{m-1} [\text{ord}_{d_j}(q) \sum_{t=1}^{\gamma_w(j,q)} p^\varepsilon] + \sum_{\substack{j|2\bar{n} \\ j \nmid \bar{n} \\ j \notin N_q \\ w=1}}^{m-1} [\text{ord}_{d_j}(q) \sum_{t=1}^{\beta_w(j,q)} 2p^\varepsilon] \right) \\
 & - \sum_{\substack{j|2\bar{n} \\ j \nmid \bar{n} \\ j \in N_q \\ w=1}}^{m-1} [\text{ord}_{d_j}(q) \sum_{t=1}^{\gamma_w(j,q)} \max\{x_{tj}, p^\varepsilon - x_{tj}\}] \\
 & - \sum_{\substack{j|2\bar{n} \\ j \nmid \bar{n} \\ j \notin N_q \\ w=1}}^{m-1} [\text{ord}_{d_j}(q) \sum_{t=1}^{\beta_w(j,q)} (\max\{y_{tj}, p^\varepsilon - z_{tj}\} + \max\{z_{tj}, p^\varepsilon - y_{tj}\})] \\
 & = \sum_{i \in N_q} i|\bar{n} [\text{ord}_i(q) \sum_{k=1}^{\gamma_0(i,q)} (p^\varepsilon - \max\{u_{ki}, p^\varepsilon - u_{ki}\})] \\
 & + \sum_{i \notin N_q} i|\bar{n} [\text{ord}_i(q) \sum_{k=1}^{\beta_0(i,q)} (2p^\varepsilon - (\max\{v_{ki}, p^\varepsilon - w_{ki}\} + \max\{w_{ki}, p^\varepsilon - v_{ki}\}))] \\
 & + \sum_{\substack{j|2\bar{n} \\ j \nmid \bar{n} \\ j \in N_q \\ w=1}}^{m-1} [\text{ord}_{d_j}(q) \sum_{t=1}^{\gamma_w(j,q)} (p^\varepsilon - \max\{x_{tj}, p^\varepsilon - x_{tj}\})] \\
 & + \sum_{\substack{j|2\bar{n} \\ j \nmid \bar{n} \\ j \notin N_q \\ w=1}}^{m-1} [\text{ord}_{d_j}(q) \sum_{t=1}^{\beta_w(j,q)} (2p^\varepsilon - (\max\{y_{tj}, p^\varepsilon - z_{tj}\} + \max\{z_{tj}, p^\varepsilon - y_{tj}\}))].
 \end{aligned}$$

Let us reorganize the terms that appear multiplied by $\text{ord}_i(q)$ in the summations as follows. For the first summation, we have $\left\lfloor \frac{p^\varepsilon}{2} \right\rfloor \leq \max\{u_{ki}, p^\varepsilon - u_{ki}\} \leq p^\varepsilon \Rightarrow -p^\varepsilon \leq -\max\{u_{ki}, p^\varepsilon - u_{ki}\} \leq -\left\lfloor \frac{p^\varepsilon}{2} \right\rfloor \Rightarrow 0 \leq p^\varepsilon - \max\{u_{ki}, p^\varepsilon - u_{ki}\} \leq p^\varepsilon - \left\lfloor \frac{p^\varepsilon}{2} \right\rfloor$. Since for $a \in \mathbb{Z}$ and $x \in \mathbb{R}$ we have $\lfloor a+x \rfloor = a + \lfloor x \rfloor$, it follows that $p^\varepsilon - \left\lfloor \frac{p^\varepsilon}{2} \right\rfloor = \left\lfloor p^\varepsilon - \frac{p^\varepsilon}{2} \right\rfloor = \left\lfloor \frac{p^\varepsilon}{2} \right\rfloor$. Hence, $0 \leq p^\varepsilon - \max\{u_{ki}, p^\varepsilon - u_{ki}\} \leq \left\lfloor \frac{p^\varepsilon}{2} \right\rfloor$. Say $a_i = \gamma_0(i, q)(p^\varepsilon - \max\{u_{ki}, p^\varepsilon - u_{ki}\})$, since we have $0 \leq a_i \leq \gamma_0(i, q) \left\lfloor \frac{p^\varepsilon}{2} \right\rfloor$.

For the second summation: $p^\varepsilon \leq \max\{v_{ki}, p^\varepsilon - w_{ki}\} + \max\{w_{ki}, p^\varepsilon - v_{ki}\} \leq 2p^\varepsilon \Rightarrow -2p^\varepsilon \leq -(\max\{v_{ki}, p^\varepsilon - w_{ki}\} + \max\{w_{ki}, p^\varepsilon - v_{ki}\}) \leq -p^\varepsilon \Rightarrow 0 \leq 2p^\varepsilon - (\max\{v_{ki}, p^\varepsilon - w_{ki}\} + \max\{w_{ki}, p^\varepsilon - v_{ki}\}) \leq p^\varepsilon$. Say $b_i = 2p^\varepsilon -$

$(\max\{v_{ki}, p^\varepsilon - w_{ki}\} + \max\{w_{ki}, p^\varepsilon - v_{ki}\})$, since we have $0 \leq b_i \leq p^\varepsilon$.

When similar arrangements are made for $w = 1, 2, \dots, m-1$, it follows that $0 \leq a_i \leq \gamma_0(i, q) \cdot \left\lfloor \frac{p^\varepsilon}{2} \right\rfloor$, $0 \leq b_i \leq \beta_0(i, q) \cdot p^\varepsilon$, $0 \leq c_{\omega, j} \leq \gamma_\omega(j, q) \cdot \left\lfloor \frac{p^\varepsilon}{2} \right\rfloor$, $0 \leq d_{\omega, j} \leq \beta_\omega(j, q) \cdot p^\varepsilon$. Therefore, we obtain

$$\dim(\text{Hull}(C)) = \sum_{i \in N_q} \text{ord}_i(q) \cdot a_i + \sum_{\substack{i \in \bar{N}_q \\ i \notin N_q}} \text{ord}_i(q) \cdot b_i + \sum_{\substack{j \in 2\bar{n}, j \nmid \bar{n} \\ j \in N_q \\ \omega=1,2,\dots,m-1}} \text{ord}_j(q) \cdot c_{\omega, j} + \sum_{\substack{j \in 2\bar{n}, j \nmid \bar{n} \\ j \notin N_q \\ \omega=1,2,\dots,m-1}} \text{ord}_j(q) \cdot d_{\omega, j}.$$

□

Example 1. For $p = q = 7$, $n = 4$ and $m = 4$, the hull dimensions of the $(-2v^3 + 1)$ -constacyclic codes C of length 4 over the ring $R = \mathbb{F}_7[v]/\langle v^4 - v \rangle$ are obtained as follows:

Since $(p, \bar{n}) = 1$, we have $\varepsilon = 0$. The divisors of 4 are 1, 2, and 4. Since $1, 2, 4 \in N_7$, there are no $\beta_0(i, 7)$ values in Theorem 2.. We get $\gamma_0(1, 7) = \gamma_0(2, 7) = \gamma_0(4, 7) = 1$.

Similarly, the divisors of 8 are 1, 2, 4, 8. It is easy to see that $8 \in N_7$ for $8 \nmid 7$. In this case, for $\omega = 1, 2, 3$, we obtain $\gamma_\omega(8, 7) = 2$, and there are no $\beta_\omega(8, 7)$ values. Since $\lceil 7^0/2 \rceil = 0$, we have $a_1 = a_2 = a_4 = 0$ and $c_{\omega, 8} = 0$ for $\omega = 1, 2, 3$.

$$\text{Therefore, } \dim(\text{Hull}(C)) = \sum_{i \in N_7} \text{ord}_i(7) \cdot a_i + \sum_{\substack{j \in 8, j \nmid 4 \\ j \in N_7 \\ \omega=1,2,3}} \text{ord}_j(7) \cdot c_{\omega, j} = 0.$$

Example 2. For $p = 5$, $q = 25$ and $m = 5$, the hull dimensions of the $n = 20$ -length $(-2v^4 + 1)$ -constacyclic codes over the ring $R = \mathbb{F}_{25}[v]/\langle v^5 - v \rangle$ are obtained as follows: Since $n = 20 = 4 \cdot 5$, we have $\bar{n} = 4$ and $\varepsilon = 1$. The divisors of 4 are 1, 2 and 4. It is easily seen that $1, 2 \in N_{25}$ and $4 \notin N_{25}$. Since $25^1 \equiv 0 \equiv 1 \pmod{1}$, $\text{ord}_1(25) = 1$. Thus, $\gamma_0(1, 25) = \frac{\Phi(1)}{\text{ord}_1(25)} = 1$, $\gamma_0(2, 25) = \frac{\Phi(2)}{\text{ord}_2(25)} = \frac{1}{1} = 1$, and $\beta_0(4, 25) = \frac{\Phi(4)}{2 \cdot \text{ord}_4(25)} = \frac{2}{2 \cdot 1} = 2$. The divisors of $2 \cdot \bar{n} = 8$ are 1, 2, 4 and 8. It is seen that $8 \notin N_{25}$ for the value $8 \nmid 4$. In this case, γ_ω does not exist for $\omega = 1, 2, 3, 4$, and $\beta_\omega(8, 25) = \frac{\Phi(8)}{2 \cdot \text{ord}_8(25)} = \frac{4}{2 \cdot 1} = 2$. From the inequalities $0 \leq a_1 \leq \gamma_0(1, 25) \cdot \lfloor 5^1/2 \rfloor$, $0 \leq a_2 \leq \gamma_0(2, 25) \cdot \lfloor 5^1/2 \rfloor$, $0 \leq b_4 \leq \beta_0(4, 25) \cdot 5^1$ and $0 \leq d_{\omega, 8} \leq \beta_\omega(8, 25) \cdot 5^1$ for $\omega = 1, 2, 3, 4$, we obtain $0 \leq a_1 \leq 2$, $0 \leq a_2 \leq 2$, $0 \leq b_4 \leq 10$, and $0 \leq d_{\omega, 8} \leq 10$ ($\omega = 1, 2, 3, 4$). In this case, $\dim(\text{Hull}(C)) = \text{ord}_1(25) \cdot a_1 + \text{ord}_2(25) \cdot a_2 + \text{ord}_4(25) \cdot b_4 + \text{ord}_8(25) \cdot d_{1,8} + \text{ord}_8(25) \cdot d_{2,8} + \text{ord}_8(25) \cdot d_{3,8} + \text{ord}_8(25) \cdot d_{4,8}$, which simplifies to $\dim(\text{Hull}(C)) = a_1 + a_2 + b_4 + d_{1,8} + d_{2,8} + d_{3,8} + d_{4,8}$ and we get $\dim(\text{Hull}(C)) = 0, 1, 2, 3, \dots, 49$.

5 The Euclidean Hulls of Gray Images of Some Constacyclic Codes over the Ring R

Theorem 3. For any positive integer n , let $N = 2n$. Let p be a prime, ω a non-negative integer such that $(p, N) = 1$ and $N = \bar{N}p^\omega$. Let q be a power of p , and let the set $N_q = \{\ell \geq 1 \mid \exists k \geq 0 \text{ s.t. } \ell \mid (q^k + 1)\}$ be defined. Let Φ be the Euler totient function, $\bar{\gamma}(l, q) = \frac{\Phi(l)}{\text{ord}_l(q)}$ for $(l \mid \bar{N} \text{ and } l \in N_q)$, and $\bar{\beta}(l, q) = \frac{\Phi(l)}{2 \text{ord}_l(q)}$ for $(l \mid \bar{N} \text{ and } l \notin N_q)$. In this case, the hull dimension of cyclic codes over $\mathbb{F}_q$ is given by $\sum_{l \in N_q, l \mid \bar{N}} \text{ord}_l(q) A_l + \sum_{l \mid \bar{N}, l \notin N_q} \text{ord}_l(q) B_l$, where $0 \leq A_l \leq \bar{\gamma}(l, q) \lfloor p^\omega/2 \rfloor$ and $0 \leq B_l \leq \bar{\beta}(l, q) p^\omega \lfloor 2 \rfloor$.

Example 3. Consider a $(-2v^3 + 1)$ -constacyclic code C of length $n = 24$ over $R = \mathbb{F}_7 + v\mathbb{F}_7 + v^2\mathbb{F}_7 + v^3\mathbb{F}_7$ with $m = 4$, $q = 7$ and $v^4 = v$. Since $N = 2n = 48$ and $(48, 7) = 1$, we have $p^\omega = 7^0 = 1$ and thus $\bar{N} = 48$. The divisors of 48 are 1, 2, 3, 4, 6, 8, 12, 16, 24, 48. It is seen that 1, 2, 4, 8 $\in N_7$ and 3, 6, 12, 16, 24, 48 $\notin N_7$. We compute: $\bar{\gamma}(1, 7) = \frac{\Phi(1)}{\text{ord}_1(7)} = \frac{1}{1} = 1$, $\bar{\gamma}(2, 7) = \frac{\Phi(2)}{\text{ord}_2(7)} = \frac{1}{1} = 1$, $\bar{\gamma}(4, 7) = \frac{\Phi(4)}{\text{ord}_4(7)} = \frac{2}{2} = 1$, $\bar{\gamma}(8, 7) = \frac{\Phi(8)}{\text{ord}_8(7)} = \frac{4}{2} = 2$, $\bar{\beta}(3, 7) = \frac{\Phi(3)}{2 \text{ord}_3(7)} = \frac{2}{2 \cdot 1} = 1$, $\bar{\beta}(6, 7) = \frac{\Phi(6)}{2 \text{ord}_6(7)} = \frac{2}{2 \cdot 1} = 1$, $\bar{\beta}(12, 7) = \frac{\Phi(12)}{2 \text{ord}_{12}(7)} = \frac{4}{2 \cdot 2} = 1$, $\bar{\beta}(16, 7) = \frac{\Phi(16)}{2 \text{ord}_{16}(7)} = \frac{8}{2 \cdot 2} = 2$, $\bar{\beta}(24, 7) = \frac{\Phi(24)}{2 \text{ord}_{24}(7)} = \frac{8}{2 \cdot 2} = 2$, $\bar{\beta}(48, 7) = \frac{\Phi(48)}{2 \text{ord}_{48}(7)} = \frac{16}{2 \cdot 2} = 4$. From $0 \leq A_1 \leq \bar{\gamma}(1, 7) \lfloor 7/2 \rfloor$, $0 \leq A_2 \leq \bar{\gamma}(2, 7) \lfloor 7/2 \rfloor$, $0 \leq A_4 \leq \bar{\gamma}(4, 7) \lfloor 7/2 \rfloor$, $0 \leq A_8 \leq \bar{\gamma}(8, 7) \lfloor 7/2 \rfloor$, $0 \leq B_3 \leq \bar{\beta}(3, 7) \cdot 7$, $0 \leq B_6 \leq \bar{\beta}(6, 7) \cdot 7$, $0 \leq B_{12} \leq \bar{\beta}(12, 7) \cdot 7$, $0 \leq B_{16} \leq \bar{\beta}(16, 7) \cdot 7$, $0 \leq B_{24} \leq \bar{\beta}(24, 7) \cdot 7$, $0 \leq B_{48} \leq \bar{\beta}(48, 7) \cdot 7$, we get $0 \leq A_1, A_2, A_4 \leq 3$, $0 \leq A_8 \leq 6$, $0 \leq B_3, B_6, B_{12} \leq 7$, $0 \leq B_{16}, B_{24} \leq 14$, $0 \leq B_{48} \leq 28$. Since $\dim(\text{Hull}(\eta(C))) = \text{ord}_1(7)A_1 + \text{ord}_2(7)A_2 + \text{ord}_4(7)A_4 + \text{ord}_8(7)A_8 + \text{ord}_3(7)B_3 + \text{ord}_6(7)B_6 + \text{ord}_{12}(7)B_{12} + \text{ord}_{16}(7)B_{16} + \text{ord}_{24}(7)B_{24} + \text{ord}_{48}(7)B_{48} = A_1 + A_2 + 2A_4 + 2A_8 + B_3 + B_6 + 2B_{12} + 2B_{16} + 2B_{24} + 2B_{48}$, we obtain $\dim(\text{Hull}(\eta(C))) \in \{0, 1, 2, \dots, 163, 164\}$.

Example 4. For $m = 2$, $q = 9$, and $n = 4$, the hull dimensions of the cyclic codes $\eta(C)$ (which are the images of the $(-2v + 1)$ -constacyclic codes over the ring $R = \mathbb{F}_9 + v\mathbb{F}_9$ with $v^2 = v$) under the η Gray map are obtained as follows: since $N = 2 \cdot 4 = 8$ and $(8, 3) = 1$, we have $p^\omega = 3^0 = 1$. For the divisors of 8, namely 1, 2, 4, 8, we find that 1, 2 $\in N_9$ and 4, 8 $\notin N_9$. The values are calculated as $\bar{\gamma}(1, 9) = \frac{\Phi(1)}{\text{ord}_1(9)} = \frac{1}{1} = 1$, $\bar{\gamma}(2, 9) = \frac{\Phi(2)}{\text{ord}_2(9)} = \frac{1}{1} = 1$, $\bar{\beta}(4, 9) = \frac{\Phi(4)}{2 \text{ord}_4(9)} = \frac{2}{2 \cdot 1} = 1$, and $\bar{\beta}(8, 9) = \frac{\Phi(8)}{2 \text{ord}_8(9)} = \frac{4}{2 \cdot 1} = 2$. From $0 \leq A_1 \leq \bar{\gamma}(1, 9) \lfloor 3^0/2 \rfloor$, $0 \leq A_2 \leq \bar{\gamma}(2, 9) \lfloor 3^0/2 \rfloor$, $0 \leq B_4 \leq \bar{\beta}(4, 9) \cdot 3^0$, and $0 \leq B_8 \leq \bar{\beta}(8, 9) \cdot 3^0$, we get $A_1 = A_2 = 0$, $0 \leq B_4 \leq 1$, and $0 \leq B_8 \leq 2$.

Hence, since $\dim(\text{Hull}(\eta(C))) = \text{ord}_4(9) B_4 + \text{ord}_8(9) B_8 = B_4 + B_8$, we obtain $\dim(\text{Hull}(\eta(C))) \in \{0, 1, 2, 3\}$.

Proposition 8. *Let the map $\eta : R \rightarrow \mathbb{F}_q^2$ be defined such that $\eta(a_0 + va_1 + v^2a_2 + \cdots + v^{m-1}a_{m-1}) \mapsto (-a_{m-1}, 2a_0 + a_{m-1})$. η is well-defined and an $\mathbb{F}_q$ -linear map. Furthermore, the map $\eta : R^n \rightarrow \mathbb{F}_q^{2n}$ is generalized for all $r = (a_{0,0} + va_{0,1} + v^2a_{0,2} + \cdots + v^{m-1}a_{0,m-1}, a_{1,0} + va_{1,1} + v^2a_{1,2} + \cdots + v^{m-1}a_{1,m-1}, \dots, a_{n-1,0} + va_{n-1,1} + v^2a_{n-1,2} + \cdots + v^{m-1}a_{n-1,m-1}) \in R^n$ as $\eta(r) = (-a_{0,m-1}, -a_{1,m-1}, \dots, -a_{n-1,m-1}, 2a_{0,0} + a_{0,m-1}, 2a_{1,0} + a_{1,m-1}, \dots, 2a_{n-1,0} + a_{n-1,m-1})$. Moreover, the map $\eta : (R^n, d_G) \rightarrow (\mathbb{F}_q^{2n}, d_H)$ defined above is an isometry, where d_G is the Gray distance and d_H is the Hamming distance.*

Proof. It can be easily shown that the map η defined in the theorem is well-defined and an $\mathbb{F}_q$ -linear map. Considering that η is an $\mathbb{F}_q$ -linear map and the definition of the Gray weight defined on R^n , we see that for all $a, b \in R^n$, $d_G(a, b) = w_G(a - b) = w_H(\eta(a - b)) = w_H(\eta(a) - \eta(b)) = d_H(\eta(a), \eta(b))$. This means that the map $\eta : (R^n, d_G) \rightarrow (\mathbb{F}_q^{2n}, d_H)$ is an isometry. $\square$

The Gray map η defined in Proposition 8. is a generalization of the Gray map Φ defined by Raka et al. [1] over the ring $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p + u^3\mathbb{F}_p$ ($u^4 = u$, p is a prime, and $p \equiv 1 \pmod{3}$) to the ring R . Furthermore, the Gray map η in the work of Tian et al. [2] is obtained when $m = 2$.

Theorem 4. *Let v be the $(-2v^{m-1} + 1)$ -constacyclic shift map on R^n , and let σ be the cyclic shift map on $\mathbb{F}_q^{2n}$. Then $\sigma \circ \eta = \eta \circ v$.*

Proof. For all $r = (a_{0,0} + va_{0,1} + v^2a_{0,2} + \cdots + v^{m-1}a_{0,m-1}, a_{1,0} + va_{1,1} + v^2a_{1,2} + \cdots + v^{m-1}a_{1,m-1}, \dots, a_{n-1,0} + va_{n-1,1} + v^2a_{n-1,2} + \cdots + v^{m-1}a_{n-1,m-1}) \in R^n$, we compute the left-hand side: $(\sigma \circ \eta)(r) = \sigma(\eta(r)) = \sigma(-a_{0,m-1}, -a_{1,m-1}, \dots, -a_{n-1,m-1}, 2a_{0,0} + a_{0,m-1}, 2a_{1,0} + a_{1,m-1}, \dots, 2a_{n-1,0} + a_{n-1,m-1})$, and applying σ yields $(2a_{n-1,0} + a_{n-1,m-1}, -a_{0,m-1}, -a_{1,m-1}, \dots, -a_{n-1,m-1}, 2a_{0,0} + a_{0,m-1}, 2a_{1,0} + a_{1,m-1}, \dots, 2a_{n-2,0} + a_{n-2,m-1})$.

On the other hand, $(\eta \circ v)(r) = \eta(v(r)) = \eta((-2v^{m-1} + 1)(a_{n-1,0} + va_{n-1,1} + v^2a_{n-1,2} + \cdots + v^{m-1}a_{n-1,m-1}), a_{0,0} + va_{0,1} + \cdots, a_{1,0} + va_{1,1} + \cdots, \dots, a_{n-2,0} + va_{n-2,1} + \cdots)$. Using $-2v^{m-1}v = -2v^m = -2v$, $-2v^{m-1}v^2 = -2v^mv = -2v^2$, $\dots$, $-2v^{m-1}v^k = v^k$ for $k = 1, 2, \dots, m-1$, the expression becomes $\eta(a_{n-1,0} - va_{n-1,1} - v^2a_{n-1,2} + \cdots + v^{m-1}(-a_{n-1,m-1} - 2a_{n-1,0}), a_{0,0} + va_{0,1} + \cdots, a_{1,0} + va_{1,1} + \cdots, \dots, a_{n-2,0} + va_{n-2,m-1} + \cdots)$. Applying η gives $(a_{n-1,m-1} + 2a_{n-1,0}, -a_{0,m-1}, -a_{1,m-1}, \dots, -a_{n-2,m-1}, -a_{n-1,m-1}, 2a_{0,0} + a_{0,m-1}, 2a_{1,0} + a_{1,m-1}, \dots, 2a_{n-2,0} + a_{n-2,m-1})$. Therefore $\sigma \circ \eta = \eta \circ v$. $\square$

Corollary 5. *Let C be a $(-2v^{m-1} + 1)$ -constacyclic code of length n over R . Then $\eta(C)$ is a cyclic code of length $2n$ over $\mathbb{F}_q$.*

Proof. Let $C \subseteq R^n$ be a $(-2v^{m-1} + 1)$ -constacyclic code of length n over R . From the previous theorem, $(\sigma \circ \eta)(C) = (\eta \circ v)(C)$, which implies $\sigma(\eta(C)) = \eta(v(C))$. Since C is a $(-2v^{m-1} + 1)$ -constacyclic code, it is closed under v , so $v(C) = C$. Therefore $\sigma(\eta(C)) = \eta(C)$, hence $\eta(C)$ is a cyclic code. $\square$

The polynomial representation of the η Gray map defined in Proposition 10. is the map $\eta_P : R[x]/\langle x^n - (-2v^{m-1} + 1) \rangle \rightarrow \mathbb{F}_q[x]/\langle x^{2n} - 1 \rangle$, where $i = 0, 1, \dots, m-1$ and $a_i(x) \in \mathbb{F}_q[x]$. It is defined by $r(x) = e_0a_0(x) + e_1a_1(x) + \cdots + e_{m-1}a_{m-1}(x)$ being mapped to $\eta_P(r(x)) = (a_0(x) - a_{m-1}(x)) + x^n(a_0(x) + a_{m-1}(x))$. The map η_P is well-defined since $\{e_0, e_1, \dots, e_{m-1}\} \subset R$ is a basis of R as an $\mathbb{F}_q$ -vector space. Moreover, $\eta_P(r(x))$ is the polynomial representation of $\eta(r) \in \mathbb{F}_q^{2n}$ for $r \in R^n$.

When $m = 2$, the results in Section 3.2 of Tian et al. [2] are obtained. Is it possible, for $m > 2$, to determine the generator polynomial of the cyclic code $\eta(C)$ of length $2n$ over $\mathbb{F}_q$ (the image of the $(-2v^{m-1} + 1)$ -constacyclic code C of length n over R under η) from the generator polynomial of C ? As stated in Section 2.3 of [2], under what conditions is $\eta_P(g(x))$ a divisor of $x^{2n} - 1 \in \mathbb{F}_q[x]$ for a $(-2v^{m-1} + 1)$ -constacyclic code C with generator polynomial $g(x) = e_0g_0(x) + e_1g_1(x) + \cdots + e_{m-1}g_{m-1}(x)$? There exist $h_0(x)$ and $h_{m-1}(x) \in \mathbb{F}_q[x]$ such that $x^n - 1 = g_0(x)h_0(x)$ and $x^n + 1 = g_{m-1}(x)h_{m-1}(x)$ for the generator polynomials $g_0(x)$ and $g_{m-1}(x)$ of the cyclic code C_0 and the negacyclic code C_{m-1} , respectively. On the other hand, the generator polynomial of a λ -constacyclic code of length n over $\mathbb{F}_q$ is a divisor of $x^n - \lambda \in \mathbb{F}_q[x]$, and its polynomial representation is an ideal of $\mathbb{F}_q[x]/\langle x^n - \lambda \rangle$. An ideal may have multiple generators. Choosing generators such that $h_0(x) + h_{m-1}(x) \in \mathbb{F}_q^*$ for the check polynomials $h_0(x)$ and $h_{m-1}(x)$ of C_0 and C_{m-1} , respectively, yields the desired correspondence.

Proposition 9. *Let $C = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_{m-1}C_{m-1}$ be a $(-2v^{m-1} + 1)$ -constacyclic code of length n over R . Let $g_0(x)$ be the generator polynomial of the cyclic code C_0 , and let $g_1(x), g_2(x), \dots, g_{m-1}(x)$ be the generator polynomials of the negacyclic codes $C_1, C_2, \dots, C_{m-1}$, respectively. Let the unique generator polynomial of C be $g(x) = e_0g_0(x) + e_1g_1(x) + \cdots + e_{m-1}g_{m-1}(x)$. If $h_0(x) + h_{m-1}(x) \in \mathbb{F}_q^*$ for the parity-check polynomials $h_0(x)$ and $h_{m-1}(x)$ of the codes C_0 and C_{m-1} , then $\eta_P(g(x)) \mid (x^{2n} - 1)$.*

Proof. Since $C_0 \subseteq \mathbb{F}_q^n$ is cyclic and $C_{m-1} \subseteq \mathbb{F}_q^n$ is negacyclic, we have $x^n - 1 = g_0(x)h_0(x)$ and $x^n + 1 = g_{m-1}(x)h_{m-1}(x)$ in $\mathbb{F}_q[x]$. Assume that $h_0(x) + h_{m-1}(x) \in \mathbb{F}_q^*$, i.e., $h_0(x) + h_{m-1}(x)$ is a nonzero constant polynomial in $\mathbb{F}_q[x]$, hence invertible. Consider $(h_0(x) + h_{m-1}(x))^{-1}h_0(x)h_{m-1}(x) \in \mathbb{F}_q[x]$.

Then $(h_0 + h_{m-1})^{-1}h_0h_{m-1}\eta_P(g(x))$. Using $\eta_P(g(x)) = g_0(x)(x^n + 1) + g_{m-1}(x)(x^n - 1)$, we get
 $(h_0 + h_{m-1})^{-1}h_0h_{m-1}g_0(x)(x^n + 1) + (h_0 + h_{m-1})^{-1}h_0h_{m-1}g_{m-1}(x)(x^n - 1)$.
 Since $x^n - 1 = g_0(x)h_0(x)$ and $x^n + 1 = g_{m-1}(x)h_{m-1}(x)$, this becomes
 $(h_0 + h_{m-1})^{-1}h_{m-1}(x)(x^n - 1)(x^n + 1) + (h_0 + h_{m-1})^{-1}h_0(x)(x^n + 1)(x^n - 1)$.
 Hence $((h_0 + h_{m-1})^{-1}h_{m-1} + (h_0 + h_{m-1})^{-1}h_0)(x^{2n} - 1)$, where the coefficient is in $\mathbb{F}_q[x]$. Therefore, $\eta_P(g(x)) \mid (x^{2n} - 1)$. $\square$

5.1 Parameters of Quantum Error-Correcting Codes

Definition 3. Let q be a power of a prime and $\mathbb{C}$ be the complex field. A q -ary quantum code of length n is a vector subspace of the Hilbert space $(\mathbb{C}^q)^{\otimes n} \cong \mathbb{C}^{q^n}$ [16].

Theorem 5. (*X Quantum Construction Method*) Let $C \subseteq \mathbb{F}_q^n$ be an $[n, k]$ code, and let $e = n - k - \dim_{\mathbb{F}_q}(C \cap C^\perp)$ under the Euclidean inner product. In this case, there exists a quantum error-correcting code with parameters $[[n + e, 2k - n + e, d]]_q$, where $d \geq \min\{d(C), d(C + C^\perp) + 1\}$ (as cited [2] from [4] and [7]).

5.1.1 Parameters of Quantum Codes over $\mathbb{F}_q$ from Generator Polynomials of $(-2v^{m-1} + 1)$ -Constacyclic Codes over the Ring R

There exists an element $\rho \in \mathbb{F}_q^*$ such that for a $(-2v^{m-1} + 1)$ -constacyclic code $C = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_{m-1}C_{m-1}$ of length n over the ring $R = \mathbb{F}_q + v\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$ ($q = p^s$, $m - 1 \mid p - 1$, p is an odd prime, and $v^m = v$), let $h_0(x)$ be the control polynomial for a monic generator polynomial $g_0(x)$ of the cyclic code C_0 , and let $h_{m-1}(x)$ be the control polynomial for a monic generator polynomial $g_{m-1}(x)$ of the negacyclic code C_{m-1} . In this case, $x^n + 1 = g_{m-1}(x)h_{m-1}(x)$ holds. If there exists $\xi \in \mathbb{F}_q^*$ such that $h_0(x) + \xi^{-1}h_{m-1}(x) = \rho \in \mathbb{F}_q[x]$, then from the equality $x^n + 1 = (\xi g_{m-1}(x))(\xi^{-1}h_{m-1}(x))$ and Proposition 9., it is easy to see that $\eta_P(g(x))$ is the generator polynomial of the cyclic code $\eta(C) \subseteq \mathbb{F}_q^{2n}$ for the code C with generator polynomial $g(x) = e_0g_0(x) + e_1g_1(x) + \cdots + e_{m-1}(\xi g_{m-1}(x))$. Subsequently, the parameters of the quantum code corresponding to this constacyclic code are obtained using Theorem 5..

Example 5. Let $C = e_0C_0 \oplus e_1C_1 \oplus e_2C_2 \oplus e_3C_3 \oplus e_4C_4 \subseteq R^2$ be a $(-2v^4 + 1)$ -constacyclic code of length $n = 2$ over the ring $R = \mathbb{F}_5 + v\mathbb{F}_5 + v^2\mathbb{F}_5 + v^3\mathbb{F}_5 + v^4\mathbb{F}_5$ ($v^5 = v$) for $q = p = 5$. In the continuation of the example, considering the field isomorphism $\mathbb{F}_5 \cong \mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$, the element $\bar{a} \in \mathbb{Z}_5$ will be written as a for ease of notation, and arithmetic operations will be performed

modulo 5. The orthogonal idempotent elements of the ring $R = \mathbb{F}_5 + v\mathbb{F}_5 + v^2\mathbb{F}_5 + v^3\mathbb{F}_5 + v^4\mathbb{F}_5$ ($v^5 = v$) are $e_0 = 1 + 4v^4$, $e_1 = 4v + 4v^2 + 4v^3 + 4v^4$, $e_2 = v + 4v^2 + v^3 + 4v^4$, $e_3 = 2v + v^2 + 3v^3 + 4v^4$, and $e_4 = 3v + v^2 + 2v^3 + 4v^4$. It is also known that the code C_0 is a cyclic code, and the codes C_1, C_2, C_3 and C_4 are negacyclic codes over $\mathbb{F}_5$. In this case, the monic factors chosen from the factorizations $x^2 - 1 = (x - 1)(x + 1)$ and $x^2 + 1 = (x - 2)(x + 2)$ in the polynomial ring $\mathbb{F}_5[x]$ will be the generator polynomials of the cyclic and negacyclic codes, respectively. Let the generator polynomial of the cyclic code C_0 be chosen as $g_0(x) = x - 1 \in \mathbb{F}_5[x]$. On the other hand, there are different generators that generate an ideal. Let $\mathbb{F}$ be any field. It is clear that for every $\kappa \in \mathbb{F}^*$ and $P \in \mathbb{F}[x]$, $\kappa \mid P$ ($P = \kappa \cdot ((\kappa^{-1})P)$) holds. Considering the writing $x^2 + 1 = (x + 2)(x - 2) = 1 \cdot (x + 2)(x - 2) = 4 \cdot 4 \cdot (x + 2)(x - 2) = (4(x + 2))(4(x - 2)) = (4x + 3)(4x + 2)$, let the generator polynomial of the negacyclic code C_4 be chosen as $g_4(x) = 4x + 2$. It is easy to see that the ideals generated by the elements $x - 2$ and $4(x - 2) \in \mathbb{F}_5[x]/\langle x^2 - 1 \rangle$ are the same. In this case, let the generator polynomial of the $(-2v^4 + 1)$ -constacyclic code over the ring R be $g(x) = e_0(x - 1) + e_1g_1(x) + e_2g_2(x) + e_3g_3(x) + e_4(4x + 2)$, where $g_1(x)$, $g_2(x)$, and $g_3(x)$ are the generator polynomials of the negacyclic codes C_1 , C_2 , and C_3 , respectively. It is clear that all combinations of the polynomials $g_i(x)$ for $i = 1, 2, 3$ give a class of generator polynomials of $(-2v^4 + 1)$ -constacyclic codes over R whose images under the η_P map are the same. We calculate $\eta_P(g(x)) = g_0(x)(x^2 + 1) + g_4(x)(x^2 - 1) = (x - 1)(x^2 + 1) + (4x + 2)(x^2 - 1) = x^2 + 2x + 2$. The factorization of the polynomial $x^4 - 1$ in $\mathbb{F}_5[x]$ is $x^4 - 1 = (x - 1)(x + 1)(x - 2)(x + 2) = ((x - 1)(x - 2))((x + 1)(x + 2)) = (x^2 + 2x + 2)(x^2 + 3x + 2)$. Since $\eta_P(g(x)) \mid (x^4 - 1)$, the polynomial $\eta_P(g(x)) = x^2 + 2x + 2$ is the generator polynomial of the cyclic code $\eta(C)$ of length 4 over $\mathbb{F}_5$. Let the generator polynomial be denoted by $\tilde{g}(x)$ and the check polynomial by $\tilde{h}(x)$. It is clear that the η Gray map given in Proposition 8. is not an injective map for values $n > 2$. In fact, $\tilde{g}(x)$ is the generator polynomial of the cyclic code $\eta(C)$ for the code C that represents a class of $(-2v^4 + 1)$ -constacyclic codes of length 2 over the ring $R = \mathbb{F}_5 + v\mathbb{F}_5 + v^2\mathbb{F}_5 + v^3\mathbb{F}_5 + v^4\mathbb{F}_5$ ($v^5 = v$) corresponding to the polynomials $g_0(x)$ and $g_4(x)$. For the polynomial $\tilde{h}(x) = x^2 + 3x + 2 \in \mathbb{F}_5[x]$, the polynomial $\tilde{h}^*(x) = 2^{-1}x^2\tilde{h}(1/x) = 3x^2(1/x^2 + 3/x + 2) = x^2 + 4x + 3$ is the generator polynomial of the cyclic code $\eta(C)^\perp \subseteq \mathbb{F}_5^4$. Furthermore, by the factorizations $x^2 + 2x + 2 = (x + 3)(x + 4)$ and $x^2 + 4x + 3 = (x + 3)(x + 1)$ in $\mathbb{F}_5[x]$, it is easily seen that the generator polynomial of the cyclic code $\eta(C) \cap \eta(C)^\perp$ is $\text{lcm}[\tilde{g}(x), \tilde{h}^*(x)] = [x^2 + 2x + 2, x^2 + 4x + 3] = (x + 3)(x + 4)(x + 1) = x^3 + 3x^2 + 2x + 2 \in \mathbb{F}_5[x]$, and the generator polynomial of the cyclic code $\eta(C) + \eta(C)^\perp$ is $\text{gcd}(\tilde{g}(x), \tilde{h}^*(x)) = (x^2 + 2x + 2, x^2 + 4x + 3) = x + 3 \in \mathbb{F}_5[x]$. In this case, $\dim_{\mathbb{F}_5}(\eta(C) \cap \eta(C)^\perp) = \dim_{\mathbb{F}_5}(\text{Hull}(\eta(C))) = 1$. Furthermore, $d_H(\eta(C)) = 3$ and $d_H(\eta(C) + \eta(C)^\perp) = 2$ (calculated using Magma [17]). In

light of the data obtained from these works, when Theorem 5. is considered for the $[4, 2]$ code $\eta(C) \subseteq \mathbb{F}_5^4$, the existence of a quantum code with parameters $[[5, 1, \geq 3]]_5$ is observed. Similar works can yield new quantum code parameters by selecting different generator polynomials $g_1(x)$ and $g_4(x)$.

5.1.2 Parameters of Quantum Codes via the Number of Cyclic Codes over $\mathbb{F}_q$ and $(-2v^{m-1} + 1)$ -Constacyclic Codes over the Ring R

Assume that $(n, q) = 1$ (to avoid multiple roots in the factorization), q is a power of an odd prime, and the polynomials $x^n - 1$ and $x^n + 1$ have c and d monic irreducible factors, respectively, in the polynomial ring $\mathbb{F}_q[x]$. Since the equality $x^{2n} - 1 = (x^n - 1)(x^n + 1)$ and $(2n, q) = 1$ always hold in $\mathbb{F}_q[x]$, the polynomial $x^{2n} - 1$ has $c + d$ monic irreducible factors in the factorization in the polynomial ring $\mathbb{F}_q[x]$. Therefore, there are 2^{c+d} cyclic codes of length $2n$ over $\mathbb{F}_q$.

On the other hand, for a $(-2v^{m-1} + 1)$ -constacyclic code $C = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_{m-1}C_{m-1}$ of length n over the ring $R = \mathbb{F}_q + v\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$ ($q = p^s$, $(m-1) \mid (p-1)$, p is an odd prime and $v^m = v$), $c \cdot d^{m-1}$ distinct generator polynomials $g(x) = e_0g_0(x) + e_1g_1(x) + \cdots + e_{m-1}g_{m-1}(x)$ can be written. Therefore, there are $c \cdot d^{m-1}$ distinct $(-2v^{m-1} + 1)$ -constacyclic codes of length n over the ring R .

Since the images of the $(-2v^{m-1} + 1)$ -constacyclic codes over the ring R under the η Gray map are cyclic codes over $\mathbb{F}_q$, for codes satisfying the equality $2^{c+d} = c \cdot d^{m-1}$, all cyclic codes of length $2n$ over $\mathbb{F}_q$ become images of the $(-2v^{m-1} + 1)$ -constacyclic codes over R under the η Gray map. Consequently, the parameters of the quantum codes obtainable from the cyclic codes of length $2n$ over $\mathbb{F}_q$ using Theorem 5. are obtained from the images of the $(-2v^{m-1} + 1)$ -constacyclic codes over R under the η Gray map.

From Section 2.3 of [2], when $(n, q) = 1$ is chosen, it is easily seen that the total number of irreducible factors in the factorization of the polynomial $x^n - 1$ in $\mathbb{F}_q[x]$ is $\sum_{i \mid n} \frac{\Phi(i)}{\text{ord}_i(q)}$.

Example 6. For $q = 7$, $n = 5$, $\sum_{i \mid 5} \frac{\Phi(i)}{\text{ord}_i(7)} = \frac{\Phi(1)}{\text{ord}_1(7)} + \frac{\Phi(5)}{\text{ord}_5(7)} = 2$, and for $q = 7$, $2n = 10$, $\sum_{i \mid 10} \frac{\Phi(i)}{\text{ord}_i(7)} = \frac{\Phi(1)}{\text{ord}_1(7)} + \frac{\Phi(2)}{\text{ord}_2(7)} + \frac{\Phi(5)}{\text{ord}_5(7)} + \frac{\Phi(10)}{\text{ord}_{10}(7)} = 4$. Thus, $m = 4$ must be chosen (since under the above notation $c = 2$, $d = 2$, we have $2 \cdot 2^{m-1} = 2^{2+2}$). In this case, the number of $(-2v^3 + 1)$ -constacyclic codes of length 5 over the ring $R = \mathbb{F}_7 + v\mathbb{F}_7 + v^2\mathbb{F}_7 + v^3\mathbb{F}_7$ ($v^4 = v$) is equal to the number of cyclic codes of length 10 over $\mathbb{F}_7$. This means the η Gray map is a one-to-one correspondence between the cyclic codes of length 10 over $\mathbb{F}_7$ and the $(-2v^3 + 1)$ -constacyclic codes over R .

In the continuation of the example, the isomorphism $\mathbb{F}_7 \cong \mathbb{Z}_7$ will be considered, and for ease of notation, the element $\bar{a} \in \mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ will be denoted as a , and arithmetic operations will be performed modulo 7.

The factorization of the polynomial $x^{10} - 1$ in the polynomial ring $\mathbb{F}_7[x]$ is in the form $x^{10} - 1 = (x - 1)(x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 + 6x^3 + x^2 + 6x + 1)$. Let these factors be written as $P_1 = x - 1$, $P_2 = x + 1$, $P_3 = x^4 + x^3 + x^2 + x + 1$, and $P_4 = x^4 + 6x^3 + x^2 + 6x + 1$. Considering this data, it is noted that in Theorem 3, $1, 2, 5, 10 \in N_7$ (i.e., for $l \mid 10$, $l \notin N_7$) and $\omega = 0$, it is observed that the hull dimensions of all cyclic codes of length 10 over $\mathbb{F}_7$ are 0 (meaning these codes are LCD codes).

The quantum code parameters corresponding to the generator polynomial of the cyclic code $\eta(C)$ (the Gray image of a C $(-2v^3 + 1)$ -constacyclic code over the ring $R = \mathbb{F}_7 + v\mathbb{F}_7 + v^2\mathbb{F}_7 + v^3\mathbb{F}_7$ ($v^4 = v$)) obtained through the calculations and Theorem 5. are as in the table below:

Table 1: Quantum code parameters from cyclic Gray images of $(-2v^3 + 1)$ -constacyclic codes over $R = \mathbb{F}_7 + v\mathbb{F}_7 + v^2\mathbb{F}_7 + v^3\mathbb{F}_7$.

Generator Polynomial of $\eta(C)$	Quantum Code
1	$[[10, 10, \geq 1]]_7$
P_1	$[[11, 9, \geq 2]]_7$
P_2	$[[11, 9, \geq 2]]_7$
P_3	$[[14, 6, \geq 2]]_7$
P_4	$[[14, 6, \geq 2]]_7$
$P_1 P_2$	$[[12, 8, \geq 2]]_7$
$P_1 P_3$	$[[15, 5, \geq 2]]_7$
$P_1 P_4$	$[[15, 5, \geq 2]]_7$
$P_2 P_3$	$[[15, 5, \geq 2]]_7$
$P_2 P_4$	$[[15, 5, \geq 2]]_7$
$P_3 P_4$	$[[18, 2, \geq 2]]_7$
$P_1 P_2 P_3$	$[[16, 4, \geq 2]]_7$
$P_1 P_2 P_4$	$[[16, 4, \geq 2]]_7$
$P_1 P_3 P_4$	$[[19, 1, \geq 2]]_7$
$P_2 P_3 P_4$	$[[19, 1, \geq 2]]_7$
$P_1 P_2 P_3 P_4$	$[[20, 0, \geq 2]]_7$

Acknowledgements: Gökhan Gökğöz acknowledges the partial support received from The Scientific and Technological Research Council of Turkey (TÜBİTAK) through the 2211 PhD Scholarship Program.

References

- [1] M. Raka, L. Kathuria, M. Goyal, $(1-2u^3)$ -constacyclic codes and quadratic residue codes over $\mathbb{F}_p[u]/\langle u^4 - u \rangle$, *Cryptography and Communications* **9** (4) (2017), 459–473.

- [2] Z. Tian, J. Gao, Y. Gao, Hulls of constacyclic codes over finite non-chain rings and their applications in quantum codes construction, *Quantum Information Processing* **23** (1) (2024).
- [3] Y. Cengellenmiş, A. Dertli, The Quantum Codes over $\mathbb{F}_q$ and Quantum Quasi-cyclic Codes over $\mathbb{F}_p$, *Mathematical Sciences and Applications E-Notes* **7** (1) (2019), 87–93.
- [4] A. Degwekar, K. Guenda, T. A. Gulliver, Extending Construction X for Quantum Error-Correcting Codes, *Proc. ICMCTA*, Springer, (2014), 141–152.
- [5] M. Shi, T. Yao, P. Solé, Skew cyclic codes over a non-chain ring, *Chinese Journal of Electronics* **26** (3) (2017), 544–547.
- [6] X. Shi, X. Huang, Q. Yue, Construction of new quantum codes derived from constacyclic codes over $\mathbb{F}_{q^2} + u\mathbb{F}_{q^2} + \cdots + u^{r-1}\mathbb{F}_{q^2}$, *Applicable Algebra in Engineering, Communication and Computing* **32** (5) (2021), 603–620.
- [7] X. Zhang, Good rate QECCs from the quantum construction X, *Quantum Information Processing* **22** (1) (2023).
- [8] Y. Zhang, Y. Liu, X. Hou, J. Gao, F. Ma, Maximal entanglement EAQECCs from cyclic and constacyclic codes over $\mathbb{F}_q + v_1\mathbb{F}_q + \cdots + v_{s-1}\mathbb{F}_q$, *Quantum Information Processing* **21** (9) (2022).
- [9] E. F. Assmus Jr., J. D. Key, Affine and projective planes, *Discrete Mathematics* **83** (2–3) (1990), 161–187.
- [10] J. L. Massey, Linear codes with complementary duals, *Discrete Mathematics* **106** (1992), 337–342.
- [11] S. Ling, C. Xing, *Coding Theory: A First Course*, Cambridge Univ. Press, 2004.
- [12] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Elsevier, 1977.
- [13] H. Q. Dinh, Constacyclic codes of length ps over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, *Journal of Algebra* **324** (5) (2010), 940–950.
- [14] E. Sangwisut, S. Jitman, S. Ling, P. Udomkavanich, Hulls of cyclic and negacyclic codes over finite fields, *Finite Fields and Their Applications* **33** (2015), 232–257.

- [15] M. Shi, A. Alahmadi, P. Solé, *Codes and Rings: Theory and Practice*, Academic Press, 2017.
- [16] W. Fang, F.-W. Fu, Some new constructions of quantum MDS codes, *IEEE Transactions on Information Theory* **65** (12) (2019), 7840–7847.
- [17] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: The user language, *Journal of Symbolic Computation* **24** (3–4) (1997), 235–265.

Gökhan GÖKGÖZ,
Institute of Natural and Applied Sciences,
Trakya University
22030 Edirne Türkiye
Email: gokhangokgoz3@trakya.edu.tr

Figen ÖKE,
Department of Mathematics,
Trakya University,
22030 Edirne, Türkiye.
Email: figenoke@trakya.edu.tr