

Received February 22, 2020, accepted March 13, 2020, date of publication March 24, 2020, date of current version April 7, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2982909

Some Results on Images of a Class of λ -Constacyclic Codes Over Finite Fields

JIAN GAO^{1,2,3}, JUAN LI⁴, AND YONGKANG WANG¹ 

¹School of Mathematics and Statistics, Shandong University of Technology, Zibo 255000, China

²Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China

³Hunan Provincial Key Laboratory of Mathematical Modeling and Analysis in Engineering, Changsha University of Science and Technology, Changsha 410114, China

⁴Chern Institute of Mathematics and LPNC, Nankai University, Tianjin 300071, China

Corresponding author: Jian Gao (dezhougaojian@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 11701336, Grant 11626144, and Grant 11671235, in part by the Scientific Research Fund of Hubei Key Laboratory of Applied Mathematics, Hubei University, under Grant HBAM201804, and in part by the Scientific Research Fund of Hunan Provincial Key Laboratory of Mathematical Modeling and Analysis in Engineering, Changsha University of Science and Technology, under Grant 2018MMAEZD09.


ABSTRACT In this paper, we show that any λ -constacyclic code over \mathbb{F}_{q^m} is a λ -constacyclic code over \mathbb{F}_q under some special maps. Moreover, we show that the images of these λ -constacyclic codes can be put into the concatenated form.

INDEX TERMS λ -constacyclic codes, images of maps, concatenated codes.

I. INTRODUCTION

Cyclic codes are one of the most interesting families of codes because of their good algebraic structures. λ -Constacyclic codes were introduced as an extension of the class of cyclic codes and form an important class of linear codes in coding theory [2], [4]. These codes have practical applications such as mathematics and engineering. They can be encoded by shift registers. Recently, many coding scholars have done further research on constructing quantum codes [5], [8], [9].

One interesting research problem of cyclic codes in coding theory is that the q -image of this class of linear codes over finite fields. The q -image of cyclic codes over finite fields can be used to construct good linear codes with long length. Moreover, q -image of cyclic codes in concatenated form is relative to the sequences structure, codes coverage radius and depth distribution, which can be used into the data compression and transmission [10]. This research issue was first addressed by Hanan–Palermo [11] and then by MacWilliams [12]. These papers restricted themselves to the case $q = 2$. However, they are hard to be generalized to \mathbb{F}_{q^m} with q a prime power. In [14], Séguin gave a simple characterization of all q -image of cyclic codes over \mathbb{F}_{q^m} .

The associate editor coordinating the review of this manuscript and approving it for publication was Congduan Li .

As a generalization of cyclic codes, constacyclic codes were introduced in [1]. Since then, the problem of studying the algebraic structure of constacyclic codes is of great interest. In the last two decades, there has been much work on simple-root and repeated-root constacyclic codes of various length over finite fields [2], [4], [17]. Recently, constacyclic codes over finite chain rings are extensively studied including the algebraic structure, cardinality and minimum distance [3], [7], [13], [18].

Similar to the problem for cyclic codes over the finite field \mathbb{F}_{q^m} , in this paper, we discuss the q -images of λ -constacyclic codes over \mathbb{F}_{q^m} . Further, we give the description on q -images of λ -constacyclic codes in a concatenated form.

This paper is organized as follows. In Section 2, we mainly give some basic results on linear codes and λ -constacyclic codes over finite fields. In Sections 3 and 4, we give some results on the primary components of λ -constacyclic codes. In Section 5, we present a concatenated description of q -images of λ -constacyclic codes over \mathbb{F}_{q^m} .

II. PRELIMINARIES

Let \mathbb{F}_q be a finite field and $\lambda \in \mathbb{F}_q^*$, where q is a prime power and \mathbb{F}_q^* is the unit group of \mathbb{F}_q . Let $C \subseteq \mathbb{F}_q^n$ be a linear code, i.e. a non zero vector subspace of \mathbb{F}_q^n . The linear code C is said to be a λ -constacyclic code if and only if for any codeword $(c_0, c_1, \dots, c_{n-1}) \in C$ we have $(\lambda c_{n-1}, c_0, \dots, c_{n-2}) \in C$.

In this paper, we always suppose $\gcd(n, q) = 1$. Define a following \mathbb{F}_q -module isomorphism

$$f : \mathbb{F}_q^n \rightarrow \mathbb{F}_q[x]/\langle x^n - \lambda \rangle$$

$$(c_0, c_1, \dots, c_{n-1}) \mapsto c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}. \quad (1)$$

One can verify that C is a λ -constacyclic code of length n over \mathbb{F}_q if and only if $f(C)$ is an ideal of $\mathbb{F}_q[x]/\langle x^n - \lambda \rangle$. Moreover, $f(C) = \langle g(x) \rangle$, where $g(x)$ is a monic factor of $x^n - \lambda$. In this paper, we identify C with $f(C)$, i.e. the λ -constacyclic code C of length n over \mathbb{F}_q is an ideal of $\mathbb{F}_q[x]/\langle x^n - \lambda \rangle$.

Since $\gcd(n, q) = 1$, then the polynomial $x^n - \lambda$ has roots $\beta, \beta\xi, \dots, \beta\xi^{n-1}$ in some Galois extension field of \mathbb{F}_q , where β is an n th root of λ and ξ is a primitive n th root of unity. Therefore

$$x^n - \lambda = \prod_{t=0}^{n-1} (x - \beta\xi^t).$$

Let \mathbb{F}_{q^m} be a finite field, where q is a prime power and $m \geq 2$. Define a map as follows

$$F : \mathbb{F}_{q^m}[x]/\langle x^n - \lambda \rangle \rightarrow \bigoplus_{t=0}^{n-1} \mathbb{F}_{q^m}[x]/\langle x - \beta\xi^t \rangle$$

$$c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} \mapsto$$

$$F(c(x)) = (c(\beta), c(\beta\xi), \dots, c(\beta\xi^{n-1})). \quad (2)$$

Then F is a well-defined ring isomorphism.

Let $\rho_t = c(\beta\xi^t) = \sum_{k=0}^{n-1} c_k(\beta\xi^t)^k$. Clearly,

$$(\rho_0, \rho_1, \dots, \rho_{n-1})$$

$$= (c_0, c_1, \dots, c_{n-1})$$

$$\times \begin{pmatrix} 1 & 1 & \dots & 1 \\ \beta & \beta\xi & \dots & \beta\xi^{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ \beta^{n-1} & (\beta\xi)^{n-1} & \dots & (\beta\xi^{n-1})^{n-1} \end{pmatrix}, \quad (3)$$

which implies that

$$c_t = \frac{1}{n} \sum_{k=0}^{n-1} \rho_k (\beta\xi^k)^{-t}, \quad t = 0, 1, \dots, n-1.$$

Note that β is an n th root of λ and ξ is a primitive n th root of unity, then $\beta^{q-1} = \xi^\varepsilon$, $0 \leq \varepsilon \leq n-1$, which implies that $\beta^{kq} = \beta^k \xi^{k\varepsilon}$. Let $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} \in \mathbb{F}_q[x]/\langle x^n - \lambda \rangle$. Then

$$\rho_t^q = (c(\beta\xi^t))^q = \sum_{k=0}^{n-1} c_k^q (\beta\xi^t)^{kq}$$

$$= \sum_{k=0}^{n-1} c_k \beta^k \xi^{k(tq+\varepsilon)} = \rho_{tq+\varepsilon}, \quad (4)$$

where $t = 0, 1, \dots, n-1$. Similarly, we have $\rho_t^{q^2} = \rho_{\varepsilon+q\varepsilon+tq^2}$.

Let $x^n - \lambda = h_1(x)h_2(x)\dots h_r(x)$, where $h_i(x)$ is a monic irreducible polynomial with degree d_i over \mathbb{F}_q , for $i = 1, 2, \dots, r$. Denote by U_i , $i = 1, 2, \dots, r$, the q -cyclotomic coset corresponding to $h_i(x)$. Let $\mathbb{F}_{q^{d_i}}$ be the d_i th Galois extension field of \mathbb{F}_q , i.e., $\mathbb{F}_{q^{d_i}} \cong \mathbb{F}_q[x]/\langle h_i(x) \rangle$, where $\deg(h_i(x)) = d_i$, for $i = 1, 2, \dots, r$. Suppose that μ is the order of λ in the unit group \mathbb{F}_q^* and $\beta\xi^{u_i} = \beta^{1+u_i\mu}$, where $1 + u_i\mu$ is a complete set of representatives of cyclotomic cosets of q modulo n . Then for a fixed $1 + u_i\mu \in U_i$, $u_i \in \{0, 1, \dots, n-1\}$, the elements of the set $U_i = \{1 + u_i\mu, (1 + u_i\mu)q, \dots, (1 + u_i\mu)q^{k_i-1}\}$ are the roots of $h_i(x)$. It is well known that the finite field $\mathbb{F}_q[x]/\langle h_i(x) \rangle$ is isomorphic to a minimal constacyclic code of length n over \mathbb{F}_q with the parity check polynomial $h_i(x)$. If we denote by θ_i the generating primitive idempotent for the minimal constacyclic code, then the isomorphism is given by the map

$$\chi : \langle \theta_i \rangle \rightarrow \mathbb{F}_q[x]/\langle h_i(x) \rangle$$

$$c(x) \mapsto c(\beta^{1+u_i\mu}). \quad (5)$$

Therefore, for any $c(x) \in \langle \theta_i \rangle$, we have $c(\beta^k) \neq 0$, $k \in U_i$, for $i = 1, 2, \dots, r$.

Definition 1: Let n be a positive integer and \mathbb{F}_{q^n} be an n th Galois extension field of \mathbb{F}_q . Let r be an element of \mathbb{F}_{q^n} . Its trace relative to \mathbb{F}_q is defined by

$$Tr_1^n(r) = r + r^q + r^{q^2} + \dots + r^{q^{n-1}}.$$

From the above description, we have the following trace representation of λ -constacyclic codes directly.

Theorem 1: Let C be a λ -constacyclic code of length n over \mathbb{F}_{q^m} with parity check polynomial $h(x) = h_1(x)h_2(x)\dots h_s(x)$. Suppose $c = (c_0, c_1, \dots, c_{n-1}) \in C$, then

$$c_t = \frac{1}{n} \sum_{i=1}^s Tr_1^{d_i}(\rho_i(\beta\xi^{u_i})^{-t}),$$

where $t = 0, 1, \dots, n-1$, $d_i = \deg(h_i(x))$, $i = 1, 2, \dots, s$.

Let $\underline{\alpha} = \{\alpha_0, \alpha_1, \dots, \alpha_{m-1}\}$ be a basis for \mathbb{F}_{q^m} over \mathbb{F}_q . Define the map $d_{\underline{\alpha}}$ from $\mathbb{F}_{q^m}[z]/\langle z^n - \lambda \rangle$ into $\mathbb{F}_q[z]/\langle z^{nm} - \lambda \rangle$ by

$$d_{\underline{\alpha}} : \mathbb{F}_{q^m}[z]/\langle z^n - \lambda \rangle \rightarrow \mathbb{F}_q[z]/\langle z^{nm} - \lambda \rangle$$

$$a(z) = \sum_{j=0}^{n-1} a_j z^j \mapsto \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j} z^{mj+i}, \quad (6)$$

where $a_j = \sum_{i=0}^{m-1} a_{i,j} \alpha_i$ and $a_{i,j} \in \mathbb{F}_q$.

Proposition 1: Let $a(z) \in \mathbb{F}_{q^m}[z]/\langle z^n - \lambda \rangle$. From the definition of $d_{\underline{\alpha}}$, we have $d_{\underline{\alpha}}(za(z)) = z^m d_{\underline{\alpha}}(a(z))$.

Proof: Let $a(z) = \sum_{j=0}^{n-1} a_j z^j \in \mathbb{F}_{q^m}[z]/\langle z^n - \lambda \rangle$. Then $za(z) \bmod (z^n - \lambda) = \lambda a_{n-1} + \sum_{j=0}^{n-2} a_j z^{j+1}$. Thus, we have $d_{\underline{\alpha}}(za(z)) = \sum_{i=0}^{m-1} \lambda a_{i,n-1} z^{m(n-1)+i} + \sum_{i=0}^{m-1} \sum_{j=0}^{n-2} a_{i,j} z^{m(j+1)+i}$. By the equation (6), we can get $d_{\underline{\alpha}}(a(z)) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j} z^{mj+i} = a_{0,0} z^0 + a_{1,0} z + \dots + a_{m-1,0} z^{m-1} + \dots + \lambda a_{0,n-1} z^{-m} + \lambda a_{1,n-1} z^{-m+1} + \dots + \lambda a_{m-1,n-1} z^{-1}$, which implies that $d_{\underline{\alpha}}(za(z)) = z^m d_{\underline{\alpha}}(a(z))$. \square

Now we suppose that C is a λ -constacyclic code of length n with dimension k over \mathbb{F}_{q^m} . Then by the definition of $d_{\underline{\alpha}}$ and Proposition 1, we deduce that $d_{\underline{\alpha}}(C)$ is a linear code of length nm with dimension km over \mathbb{F}_q . Moreover, $d_{\underline{\alpha}}(C)$ is a λ -quasi-twisted code over \mathbb{F}_q .

III. THE PRIMARY COMPONENTS OF λ -CONSTACYCLIC CODES

Let $A = \mathbb{F}_q[x]/\langle x^n - \lambda \rangle$ and A^m be the direct product of A . Clearly, A^m is an A -module. The element $(a_0(x), a_1(x), \dots, a_{m-1}(x))$ of A^m can also be written as $\sum_{i=0}^{m-1} a_i(x)y^i = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j}x^jy^i$, where $a_i(x) = \sum_{j=0}^{n-1} a_{i,j}x^j$, for $i = 0, 1, \dots, m-1$.

Firstly, we introduce a map π from $\mathbb{F}_q[z]/\langle z^{nm} - \lambda \rangle$ into A^m given by

$$\pi : \mathbb{F}_q[z]/\langle z^{nm} - \lambda \rangle \rightarrow A^m$$

$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j}z^{mj+i} \mapsto \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j}x^jy^i.$$

It is easy to see that π is an A -module isomorphism.

Let $a(x) \in A$ and $b(z) \in \mathbb{F}_q[z]/\langle z^{nm} - \lambda \rangle$. Suppose $a(x)b(z) = a(z^m)b(z)$, then we have the following proposition.

Proposition 2: (i) $\pi(xb(z)) = \pi(z^m b(z)) = x\pi(b(z))$;

(ii) Suppose $\pi(a(z)) = (a_0(x), a_1(x), \dots, a_{m-1}(x)) = \underline{a}(x)$, then $\pi(za(z)) = \tau(\underline{a}(x))$, where $\tau(\underline{a}(x)) = (xa_{m-1}(x), a_0(x), \dots, a_{m-2}(x))$;

(iii) $d_{\underline{\alpha}}(C)$ is a λ -constacyclic code if and only if $\pi(d_{\underline{\alpha}}(C))$ is invariant under the action of τ .

Proof: (i) By the definition of π , we can get $\pi(z^m b(z)) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{ij}x^{j+1}y^i = x \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{ij}x^jy^i = x\pi(b(z))$.

(ii) Since

$$za(z) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{ij}z^{mj+i+1}$$

$$= \lambda a_{m-1,n-1} + a_{0,0}z + \dots + a_{m-2,0}z^{m-1} + \dots$$

$$+ a_{m-1,n-2}z^{mn-m} + a_{0,n-1}z^{mn-m+1} + \dots$$

$$+ a_{m-1,n-1}z^{mn-1},$$

$$\pi(za(z)) = (\lambda a_{m-1,n-1} + a_{m-1,0}x + \dots + a_{m-1,n-2}x^{n-1},$$

$$\dots, a_{m-2,0} + a_{m-2,1}x + \dots + a_{m-2,n-1}x^{n-1}),$$

and

$$(xa_{m-1}(x), a_0(x), \dots, a_{m-2}(x))$$

$$= (\lambda a_{m-1,n-1} + a_{m-1,0}x + \dots + a_{m-1,n-2}x^{n-1}$$

$$, \dots, a_{m-2,0} + a_{m-2,1}x + \dots + a_{m-2,n-1}x^{n-1}),$$

which implies that

$$\pi(za(z)) = (xa_{m-1}(x), a_0(x), \dots, a_{m-2}(x)) = \tau(\underline{a}(x)).$$

(iii) Let $\underline{a}(x) = (a_0(x), a_1(x), \dots, a_{m-1}(x)) \in \pi(d_{\underline{\alpha}}(C))$. Then

$$\tau(\underline{a}(x)) = \pi(za(z)) = (xa_{m-1}(x), a_0(x), \dots, a_{m-2}(x)).$$

Assume that $a(z) \in d_{\underline{\alpha}}(C)$, then $za(z) \in d_{\underline{\alpha}}(C)$ since $d_{\underline{\alpha}}(C)$ is λ -constacyclic. So $\pi(za(z)) \in \pi(d_{\underline{\alpha}}(C))$. Therefore $\tau(\underline{a}(x)) \in d_{\underline{\alpha}}(C)$. On the other hand, since $\underline{a}(x) \in \pi(d_{\underline{\alpha}}(C))$, which implies that $\tau(\underline{a}(x)) = \pi(za(z)) \in \pi(d_{\underline{\alpha}}(C))$. Since π is an A -module isomorphism, then we have that $za(z) \in d_{\underline{\alpha}}(C)$. \square

In the following, we define a map $D_{\underline{\alpha}}$ from $\mathbb{F}_{q^m}[z]/\langle z^n - \lambda \rangle$ into A^m as $D_{\underline{\alpha}} = \pi \circ d_{\underline{\alpha}}$ so that

$$D_{\underline{\alpha}} : \mathbb{F}_{q^m}[z]/\langle z^n - \lambda \rangle \rightarrow A^m$$

$$\sum_{i=0}^{n-1} a_j z^j \mapsto \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} a_{i,j} x^j y^i,$$

where a_j is defined by (6).

Our work is to determine the pairs $(\underline{\alpha}, C)$ for which $D_{\underline{\alpha}}(C)$ is τ -invariant. If C is a λ -constacyclic code over \mathbb{F}_{q^m} , then $D_{\underline{\alpha}}(C)$ is a submodule of A^m . We now introduce a few notions.

For any $\underline{a}(x) = (a_0(x), a_1(x), \dots, a_{m-1}(x)) \in A^m$, the order of $\underline{a}(x)$ denoted by $ord(\underline{a}(x))$ is defined to be a nonzero monic polynomial $f(x)$ of least degree such that $f(x)\underline{a}(x) = \underline{0}$. Set $ord(\underline{0}) = 1$. Clearly, if $a(x) \in A$, then $ord(a(x)) = \frac{x^n - \lambda}{gcd(a(x), x^n - \lambda)}$. Moreover, $ord(\underline{a}(x)) = lcm_{0 \leq i \leq m-1} ord(a_i(x))$. Similarly, if M is a submodule of A^m , then $ord(M)$ is the nonzero monic polynomial $f(x)$ of least degree such that $f(x)\underline{a}(x) = \underline{0}$, where $\underline{a}(x) \in M$. If

$$M = \bigoplus_{i=1}^t M_i,$$

then $ord(M) = lcm_{1 \leq i \leq t} ord(M_i)$.

Lemma 1: Let $gcd(n, q) = 1$, $h(x) = ord(M)$ and $h(x) = h_1(x)h_2(x) \dots h_t(x)$, where $h_i(x)$ are different irreducible polynomials. Then

$$M = \bigoplus_{i=1}^t \frac{h(x)}{h_i(x)} M_i.$$

Proof: Since $gcd(n, q) = 1$, then $\frac{h(x)}{h_1(x)}, \frac{h(x)}{h_2(x)}, \dots, \frac{h(x)}{h_t(x)}$ are pairwise coprime. Thus, there exist $a_1(x), a_2(x), \dots, a_t(x) \in \mathbb{F}_q[x]$ such that

$$\frac{h(x)}{h_1(x)} a_1(x) + \frac{h(x)}{h_2(x)} a_2(x) + \dots + \frac{h(x)}{h_t(x)} a_t(x) = 1.$$

Multipled by M , we have

$$\frac{h(x)}{h_1(x)} M + \frac{h(x)}{h_2(x)} M + \dots + \frac{h(x)}{h_t(x)} M = M.$$

If $i \neq j$, we have $h_i(x) | \frac{h(x)}{h_j(x)}$. Moreover

$$gcd\left(\frac{h(x)}{h_j(x)} \mid j \neq i, j = 1, 2, \dots, t\right)$$

$$= h_i(x) gcd\left(\frac{h(x)}{h_j(x)h_i(x)} \mid j \neq i, j = 1, 2, \dots, t\right)$$

$$= h_i(x)$$

and $h_i(x)M = \sum \frac{h(x)}{h_j(x)}M$. Thus $\frac{h(x)}{h_i(x)}M \cap \sum_{j \neq i} \frac{h(x)}{h_j(x)}M = 0$.

Let $M_i = \frac{h(x)}{h_j(x)}M, 1 \leq i \leq t$. Then $M = M_1 \oplus M_2 \oplus \dots \oplus M_t$ and M_i 's are called the primary components of M . Clearly, $ord(M_i) = h_i(x)$. If $ord(M)$ is an irreducible polynomial, then M is called a primary submodule.

Lemma 2: Let $M \subset A^m$ be a submodule. Then M is τ -invariant if and only if its primary components are τ -invariant.

Proof: Assume that $M_i = \frac{h(x)}{h_j(x)}M, 1 \leq i \leq t$. For any $\alpha(x) \in M$, let

$$\alpha(x) = \{\alpha_1(x) + \alpha_2(x) + \dots + \alpha_t(x) \mid \alpha_i(x) \in M_i, 1 \leq i \leq t\}.$$

Since M_i is τ -invariant, then $\tau(\alpha_i(x)) \in M_i$. Thus

$$\tau(\alpha(x)) = \tau(\alpha_1(x)) + \tau(\alpha_2(x)) + \dots + \tau(\alpha_t(x)) \in M.$$

Conversely, let $\underline{a}(x) \in M_i$. Then $ord(\underline{a}(x)) = h_i(x)$ or $ord(\underline{a}(x)) = 0$. Since

$$\tau(\underline{a}(x)) = (xa_{m-1}(x), a_0(x), \dots, a_{m-2}(x)),$$

it follows that $ord(\tau(\underline{a}(x))) = ord(\underline{a}(x)) = h_i(x)$. Since $\underline{a}(x) \in M_i$ and M is τ -invariant, then $\tau(\underline{a}(x)) \in M_i$. \square

Let $x^n - \lambda = h_1(x)h_2(x) \dots h_r(x)$. Then, for any $i = 1, 2, \dots, r, P_i = \frac{x^n - \lambda}{h_i(x)}A^m$ is a primary component of A^m . Hence if $M \subset A^m$ is a primary submodule of order $h_i(x)$, then $M \subset P_i$.

Let $h(x)$ be an irreducible factor of $x^n - \lambda$ of degree k , and P be the primary component of A^m of order $h(x)$. Let $\beta\xi^t$ be a root of $h(x)$ and $\mathbb{F}_{q^k} = \mathbb{F}_q(\beta\xi^t)$. Now we define the following maps

$$\begin{aligned} \phi : \mathbb{F}_{q^k}[\omega]/\langle \omega^m - \beta\xi^t \rangle &\rightarrow P \\ a(\omega) = \sum_{i=0}^{m-1} a_i\omega^i &\mapsto \frac{1}{n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} Tr_1^k(a_i(\beta\xi^t)^{-j})x^jy^i \end{aligned} \quad (7)$$

and

$$\begin{aligned} \psi : P &\rightarrow \mathbb{F}_{q^k}[\omega]/\langle \omega^m - \beta\xi^t \rangle \\ \underline{a}(x) = (a_0(x), a_1(x), \dots, a_{m-1}(x)) &\mapsto \sum_{i=0}^{m-1} a_i(\beta\xi^t)\omega^i. \end{aligned} \quad (8)$$

It is easy to see that ϕ is well defined. In other words, $\phi(a(\omega)) \in P$. Further, it is easy to verify that ϕ and ψ are inverses of each other.

Finally, we make $\mathbb{F}_{q^k}[\omega]/\langle \omega^m - \beta\xi^t \rangle$ into an A -module by setting

$$a(x) \sum_{i=0}^{m-1} b_i\omega^i = \sum_{i=0}^{m-1} a(\beta\xi^t)b_i\omega^i,$$

where $a(x) \in A$ and $\sum_{i=0}^{m-1} b_i\omega^i \in \mathbb{F}_{q^k}[\omega]/\langle \omega^m - \beta\xi^t \rangle$. For any $a(x) \in A$ and $\underline{a}(x) = (a_0(x), a_1(x), \dots, a_{m-1}(x)), \underline{b}(x) = (b_0(x), b_1(x), \dots, b_{m-1}(x)) \in P$, we have

$$\psi(\underline{a}(x) + \underline{b}(x)) = \psi(\underline{a}(x)) + \psi(\underline{b}(x))$$

and $\psi(a(x)\underline{a}(x)) = \sum_{i=0}^{m-1} a(\beta\xi^t)a_i(\beta\xi^t)\omega^i = a(x)\sum_{i=0}^{m-1} a_i(\beta\xi^t)\omega^i = a(x)\psi(\underline{a}(x))$, which implies that ψ is an A -module isomorphism.

Theorem 2: Let $\gcd(n, q) = 1, h(x)$ be a q -ary irreducible factor of $x^n - \lambda$ of degree k and $\beta\xi^t \in \mathbb{F}_{q^k}$ be a root of $h(x)$. Let M be a primary submodule of A^m of order $h(x)$ and $U = \psi(M)$ the corresponding q^k -ary submodule of $\mathbb{F}_{q^k}[\omega]/\langle \omega^m - \beta\xi^t \rangle$. Then M is τ -invariant if and only if U is an ideal of $\mathbb{F}_{q^k}[\omega]/\langle \omega^m - \beta\xi^t \rangle$.

Proof: Let $b(\omega) = b_0 + b_1\omega + \dots + b_{m-1}\omega^{m-1} \in \mathbb{F}_{q^k}[\omega]/\langle \omega^m - \beta\xi^t \rangle$. Then

$$\begin{aligned} \phi(\omega b(\omega)) &= \phi(\beta\xi^t b_{m-1} + b_0\omega + \dots + b_{m-2}\omega^{m-1}) \\ &= \frac{1}{n} \sum_{j=0}^{n-1} Tr_1^k((\beta\xi^t)^{-j} b_{m-1} \beta\xi^t) x^j \\ &\quad + \frac{1}{n} \sum_{i=1}^{m-1} \sum_{j=0}^{n-1} Tr_1^k(b_{i-1}(\beta\xi^t)^{-j}) x^j y^i. \end{aligned}$$

Let $\underline{b}(x) = \phi(b(\omega))$. Then we have that

$$\begin{aligned} \tau(\underline{b}(x)) &= \tau(\phi(b(\omega))) \\ &= \tau\left(\frac{1}{n} \sum_{j=0}^{n-1} Tr_1^k(b_0(\beta\xi^t)^{-j})x^j, \dots, \frac{1}{n} \sum_{j=0}^{n-1} Tr_1^k(b_{m-1}(\beta\xi^t)^{-j})x^j\right) \\ &= \frac{1}{n} \sum_{j=0}^{n-1} Tr_1^k(b_{m-1}(\beta\xi^t)^{-j})x^{j+1} \\ &\quad + \frac{1}{n} \sum_{i=1}^{m-1} \sum_{j=0}^{n-1} Tr_1^k(b_{i-1}(\beta\xi^t)^{-j})x^j y^i. \end{aligned}$$

Clearly, $\frac{1}{n} \sum_{j=0}^{n-1} Tr_1^k(b_{m-1}(\beta\xi^t)^{-j+1})x^j = \frac{1}{n} \sum_{j=0}^{n-1} Tr_1^k(b_{m-1}(\beta\xi^t)^{-j})x^{j+1}$ implying $\tau(\underline{b}(x)) = \tau(\phi(b(\omega))) = \phi(\omega b(\omega))$. Therefore, M is τ -invariant if and only if $\phi(\omega b(\omega)) \in M$, and $\tau(\phi(b(\omega))) \in M$ if and only if $\psi\tau(\phi(b(\omega))) \in \psi(M) = U$, i.e., $\psi\phi(\omega b(\omega)) = \omega b(\omega) \in \psi(M) = U$. In other words, $d_{\underline{\alpha}}(C)$ is λ -constacyclic if and only if $\pi(d_{\underline{\alpha}}(C))$ is τ -invariant if and only if the submodule of A^m is τ -invariant if and only if U is an ideal. \square

In the following, we determine when $D_{\underline{\alpha}}(C)$ is a primary submodule of A^m first.

Let C be an irreducible q^m -ary λ -constacyclic code of length n with the parity check polynomial $h(x)$ of degree k . Let $\beta\xi^t \in \mathbb{F}_{q^{mk}}$ be a root of $h(x)$. Then, by Theorem 1, we have

$$C = \left\{ \frac{1}{n} \sum_{j=0}^{n-1} Tr_m^{mk}(\rho(\beta\xi^t)^{-j})z^j \mid \rho \in \mathbb{F}_{q^{mk}} \right\}.$$

Let $\underline{\alpha} = \{\alpha_0, \alpha_1, \dots, \alpha_{m-1}\}$ be a basis of \mathbb{F}_{q^m} over \mathbb{F}_q and $\underline{\gamma} = \{\gamma_0, \gamma_1, \dots, \gamma_{m-1}\}$ be the trace-dual basis of $\underline{\alpha}$.

Then $Tr_m^{mk}(\rho(\beta\xi^t)^{-j}) = \sum_{i=0}^{m-1} Tr_1^m(\gamma_i)Tr_m^{mk}(\rho(\beta\xi^t)^{-j}\alpha_i) = \sum_{i=0}^{m-1} Tr_1^{mk}(\rho\gamma_i(\beta\xi^t)^{-j})\alpha_i$. Applying the map $D_{\underline{\alpha}}$ to C , we get

$$\begin{aligned} D_{\underline{\alpha}}(C) &= D_{\underline{\alpha}}\left(\frac{1}{n}\sum_{j=0}^{n-1} Tr_m^{mk}(\rho(\beta\xi^t)^{-j}z^j)\right) \\ &= D_{\underline{\alpha}}\left(\frac{1}{n}\sum_{j=0}^{n-1}\sum_{i=0}^{m-1} Tr_1^{mk}(\rho\gamma_i(\beta\xi^t)^{-j}\alpha_i z^j)\right) \\ &= \left\{\frac{1}{n}\sum_{j=0}^{n-1}\sum_{i=0}^{m-1} Tr_1^{mk}(\rho\gamma_i(\beta\xi^t)^{-j})x^j y^i \mid \rho \in \mathbb{F}_{q^{mk}}\right\}. \end{aligned}$$

Therefore the q -ary code $D_{\underline{\alpha}}(C)$ is given by

$$D_{\underline{\alpha}}(C) = \left\{\frac{1}{n}\sum_{j=0}^{n-1}\sum_{i=0}^{m-1} Tr_1^{mk}(\rho\gamma_i(\beta\xi^t)^{-j})x^j y^i \mid \rho \in \mathbb{F}_{q^{mk}}\right\}. \tag{9}$$

Let $h_0(x) = irr(\beta\xi^t, \mathbb{F}_q)$ be an irreducible polynomial in $\mathbb{F}_q[x]$ and $\beta\xi^t$ be one of its roots. Let $deg(h_0(x)) = k_0$. Then $\mathbb{F}_{q^{k_0}} = \mathbb{F}_q(\beta\xi^t)$. In addition, $\mathbb{F}_{q^{k_0}} = \mathbb{F}_q(\beta\xi^t) \subseteq \mathbb{F}_{q^m}(\beta\xi^t) = \mathbb{F}_{q^{mk}}$, thus $k_0 \mid mk$. Decomposing Tr_1^{mk} as $Tr_1^{k_0} Tr_{k_0}^{mk}$, the set (9) becomes

$$D_{\underline{\alpha}}(C) = \left\{\frac{1}{n}\sum_{j=0}^{n-1}\sum_{i=0}^{m-1} Tr_1^{k_0}((\beta\xi^t)^{-j})Tr_{k_0}^{mk}(\rho\gamma_i)x^j y^i \mid \rho \in \mathbb{F}_{q^{mk}}\right\}. \tag{10}$$

Comparing (9) with (7) for ϕ , we have $U = \psi(D_{\underline{\alpha}}(C)) = \left\{\sum_{i=0}^{m-1} Tr_{k_0}^{mk}(\rho\gamma_i)\omega^i \mid \rho \in \mathbb{F}_{q^{mk}}\right\} \subseteq \mathbb{F}_{q^{k_0}}[\omega]/\langle\omega^m - \beta\xi^t\rangle$ and $ord(D_{\underline{\alpha}}(C)) = h_0(x)$.

In the more general case, we can decompose C as the direct sum of minimal λ -constacyclic codes, i.e.,

$$C = C_1 \oplus C_2 \oplus \dots \oplus C_r,$$

where

$$C_i = \left\langle \frac{x^n - \lambda}{h_i(x)} \right\rangle,$$

$i = 1, 2, \dots, r$ and $h_i(x)$ is an irreducible factor of $x^n - \lambda$ having $\beta\xi^{ti}$ as a root in some Galois extension field of \mathbb{F}_{q^m} . Then

$$D_{\underline{\alpha}}(C) = \bigoplus_{i=1}^r D_{\underline{\alpha}}(C_i)$$

and $D_{\underline{\alpha}}(C_i)$ is a primary submodule with the order $h_{i,0}(x) = irr(\beta\xi^{ti}, \mathbb{F}_q)$.

From the above discussion, we give some results on $D_{\underline{\alpha}}(C)$. The proof process is easy to be verified and we omit it here.

Proposition 3: (i) $D_{\underline{\alpha}}(C)$ is primary if and only if $irr(\beta\xi^{ti}, \mathbb{F}_q) = irr(\beta\xi^{t1}, \mathbb{F}_q)$, where $1 \leq i \leq r$;

(ii) Let $\beta\xi^t = \beta\xi^{t1}$. Suppose $D_{\underline{\alpha}}(C)$ is primary, then there exist integers $u_i, 1 \leq i \leq r$, such that $\beta\xi^{ti} = (\beta\xi^{t1})^{q^{u_i}}$, where $u_i \in \mathbb{Z}_{k_0}, \mathbb{Z}_{k_0} = \{0, 1, \dots, k_0 - 1\}, i = 1, 2, \dots, r$;

(iii) Let $gcd(n, q) = 1$. Then u_i belongs to distinct coests of $m\mathbb{Z}_{k_0}$. In other words, $|u_i| \leq gcd(m, k_0)$;

(iv) Suppose that $r = gcd(m, k_0)$, then the parity check polynomial of C is $h(x) = irr(\beta\xi^t, \mathbb{F}_q)$;

(v) If there exists a subspace U of $\mathbb{F}_{q^{mk}}$ such that $D_{\underline{\alpha}}(C) = \phi(U)$, then the dimension of U is er , where $e = \frac{mk}{k_0}$;

(vi) Let $\beta\xi^t \in \mathbb{F}_{q^{mk}} = \mathbb{F}_{q^m}(\beta\xi^t)$, $h_0(x) = irr(\beta\xi^t, \mathbb{F}_q)$ and $k_0 = deg(h_0(x))$. If $ord(\beta\xi^t) = N$, then $k = \frac{k_0}{gcd(m, k_0)}$.

In summary, if C is a λ -constacyclic code of length n over \mathbb{F}_{q^m} , we can decompose $C = \bigoplus_{i=1}^r C_i$, where $C_i \subseteq C$ is a λ -constacyclic code and $D_{\underline{\alpha}}(C_i), 1 \leq i \leq r$, are the primary submodules of A^m with distinct orders. From the above discussion, we see that the decomposition does not depend on the basis $\underline{\alpha}$ and we call C_i is the primary components of C . If the parity check polynomial of C_i is over \mathbb{F}_q , then we call C_i a trivial primary component and nontrivial otherwise. We can group the trivial primary components by obtaining

$$C = C_0 \oplus \left(\bigoplus_{i=1}^r C_i\right),$$

where C_0 is the sum of the trivial primary components of C and $C_i, 1 \leq i \leq r$, are the different nontrivial components of C . The following example illustrates it.

Example 1: Consider the polynomial $x^7 - 3$ over \mathbb{F}_5 . The order of 3 in \mathbb{F}_5^* is 4. We have $x^7 - 3 = \prod_{i=0}^6 (x - \beta^{1+4i}) = (x - \beta)(x - \beta^5)(x - \beta^9)(x - \beta^{13})(x - \beta^{17})(x - \beta^{21})(x - \beta^{25})$ where β is a primitive 28th root of unity. The powers of β that appear in this factorization are 1, 5, 9, 13, 17, 21, 25, and these are union of two 5-cyclotomic cosets modulo 28. They are $C_5(1) = \{1, 5, 9, 13, 17, 25\}$ and $C_5(25) = \{21\}$. In fact,

$$x^7 - 3 = (x^6 + 2x^5 + 4x^4 + 3x^3 + 2x + 4)(x + 3).$$

Let C be a 625-ary 3-constacyclic code of length 7 with the parity check polynomial $h(x) = (x - \beta)(x - \beta^5)(x - \beta^9)(x - \beta^{21})$. Then $C = C_0 \oplus C_1$, where C_0 has the parity check polynomial $x + 3$ and C_1 has the parity check polynomial $(x - \beta)(x - \beta^5)(x - \beta^9)$.

From Proposition 3, we can deduce that $r \leq gcd(m, k_0)$. In the following result, we will see that if $r = gcd(m, k_0)$, then $d_{\underline{\alpha}}(C)$ is trivial and C_0 plays no role in determining whether $d_{\underline{\alpha}}(C)$ is λ -constacyclic or not, and if $d_{\underline{\alpha}}(C)$ is a λ -constacyclic code for some basis, then the nontrivial components of C are of a special type.

Theorem 3: Let $\mathbb{F}_{q^{mk}} = \mathbb{F}_{q^m}((\beta\xi^t)^{-1}), \mathbb{F}_{q^{k_0}} = \mathbb{F}_q((\beta\xi^t)^{-1})$ and C be a primary λ -constacyclic code of length n over \mathbb{F}_{q^m} with the parity check polynomial

$$h(x) = \prod_{\mu \in S} irr((\beta\xi^t)^{q^\mu}, \mathbb{F}_{q^m}),$$

where S is a set of $r \leq \gcd(m, k_0)$ integers modulo k_0 . Then

(i) Suppose $r = \gcd(m, k_0)$, then $d_{\underline{\alpha}}(C)$ is λ -constacyclic for every basis $\underline{\alpha}$ of \mathbb{F}_{q^m} over \mathbb{F}_q and $d_{\underline{\alpha}}(C) = \left\langle \frac{z^{nm} - \lambda}{h_0(z^m)} \right\rangle$, where $h_0(z) = \text{irr}(\beta\xi^t, \mathbb{F}_q)$.

(ii) Suppose $r < \gcd(m, k_0)$ for some basis $\underline{\alpha}$, then $k = 1$.

Proof: (i) Let $r = \gcd(m, k_0)$. Then $\dim(U) = er = m$ which implies that $U = \mathbb{F}_{q^{k_0}}[\omega]/\langle \omega^m - \beta\xi^t \rangle$. Therefore, by Theorem 2, $d_{\underline{\alpha}}(C)$ is λ -constacyclic. For any $a(z) \in d_{\underline{\alpha}}(C)$, since $\pi(xb(z)) = \pi(z^m b(z)) = x\pi(b(z))$ and $\pi(a(z)) \in D_{\underline{\alpha}}(C)$, $\text{ord}(D_{\underline{\alpha}}(C)) = h_0(z)$, then $\pi(h_0(z^m)a(z)) = h_0(z)\pi(a(z)) = 0$. Further, by π an A -module isomorphism, we also have $h_0(z^m)a(z) = 0$. Since $\text{deg}h_0(z^m) = mk_0 = mrk = \dim(U)$, so we have $h_0(z^m)$ is the parity check polynomial of $d_{\underline{\alpha}}(C)$ and $d_{\underline{\alpha}}(C) = \left\langle \frac{z^{nm} - \lambda}{h_0(z^m)} \right\rangle$.

(ii) If $r < \gcd(m, k_0)$ and $d_{\underline{\alpha}}(C)$ is λ -constacyclic, then by Theorem 2 we have that U is an ideal of $\mathbb{F}_{q^{k_0}}[\omega]/\langle \omega^m - \beta\xi^t \rangle$ and $\dim(U) = er < m$. Now, let $a(\omega) = \omega^t - a_1\omega^{t-1} - \dots - a_t \mid (\omega^m - \beta\xi^t)$, where $t = m - er$. Note that $U = \psi(D_{\underline{\alpha}}(C)) = \left\{ \text{Tr}_{k_0}^{mk}(\rho\gamma_i)\omega^i \mid \rho \in \mathbb{F}_{q^{mk}} \right\}$, then we can obtain that U is invariant under the map

$$\begin{aligned} \varphi : \sum_{i=0}^{m-1} a_i \omega^i &\rightarrow \sum_{i=0}^{m-1} a_i^{q^m} \omega^i \\ \sum_{i=0}^{m-1} \text{Tr}(\rho\gamma_i)\omega^i &\mapsto \sum_{i=0}^{m-1} \text{Tr}(\rho\gamma_i)^{q^m} \omega^i, \end{aligned} \quad (11)$$

where

$$\sum_{i=0}^{m-1} \text{Tr}(\rho\gamma_i)^{q^m} \omega^i = \sum_{i=0}^{m-1} \text{Tr}(\rho^{q^m} \gamma_i^{q^m}) \omega^i.$$

Let $\gamma_i \in \mathbb{F}_{q^m}$, then $\gamma_i^{q^m} = \gamma_i$. It follows that U is invariant under the map. We know that $\varphi(a(\omega)) = \omega^t - a_1^{q^m} \omega^{t-1} - \dots - a_t^{q^m} \in U$ and $a(\omega) = \omega^t - a_1 \omega^{t-1} - \dots - a_t \in U$, then $\varphi(a(\omega)) - a(\omega) \in U$, i.e.,

$$\varphi(a(\omega)) - a(\omega) = (a_1^{q^m} - a_1)\omega^{t-1} + \dots + (a_t^{q^m} - a_t) \in U.$$

Further, since $a(\omega)$ is the generator polynomial of U and $\text{deg}(a(\omega)) = t$, then $a_i^{q^m} = a_i, i = 1, 2, \dots, t$. If ρ is a root of $a(\omega)$, then ρ^{q^m} is also a root of $a(\omega)$. Since $a(\omega) \mid (\omega^m - \beta\xi^t)$, it follows that $\rho^m - \beta\xi^t = 0$ and $(\rho^m)^{q^m} = (\beta\xi^t)^{q^m}$. Thus, $\rho^{q^m} - \beta\xi^t = 0$ implying $\beta\xi^t \in \mathbb{F}_{q^m}$. Therefore $k = 1$. \square

Similar to the proof process of Theorems 5 and 8 in [14], if $d_{\underline{\alpha}}(C)$ is λ -constacyclic for some $\underline{\alpha}$, then $r = |S| = 1$ or $k - 1$, where $S \subsetneq \mathbb{Z}_k$. Moreover, C has one nontrivial primary component and the nontrivial primary component C_1 must be one of the following forms

$$\left\langle \frac{x^n - \lambda}{x - (\beta\xi^t)^{q^\mu}} \right\rangle; \left\langle \frac{x^n - \lambda}{\prod_{\mu \in S} (x - (\beta\xi^t)^{q^\mu})} \right\rangle.$$

IV. THE NONTRIVIAL PRIMARY COMPONENT OF A CONSTACYCLIC CODE

In this section, we characterize the nontrivial primary component of constacyclic codes.

Theorem 4: Let $\mathbb{F}_{q^k} \neq \mathbb{F}_{q^m} = \mathbb{F}_q((\beta\xi^t)^{-1}) \subseteq \mathbb{F}_{q^m}$ and C be a λ -constacyclic code of length n over \mathbb{F}_{q^m} with the parity check polynomial $h(x) = \prod_{\mu \in S} (x - (\beta\xi^t)^{q^\mu})$. Let $\underline{\alpha}$ be a basis of \mathbb{F}_{q^m} over \mathbb{F}_q with the trace-dual basis $\underline{\gamma}$. Then $d_{\underline{\alpha}}(C)$ is λ -constacyclic over \mathbb{F}_q if and only if

$$\begin{aligned} I(S) &= \left\{ \sum_{i=0}^{m-1} b_i \omega^i \in \mathbb{F}_{q^k}[\omega]/\langle \omega^m - \beta\xi^t \rangle \mid \sum_{i=0}^{m-1} b_i \gamma_i^{q^{m-\mu}} = 0 \right\} \end{aligned} \quad (12)$$

is an ideal of $\mathbb{F}_{q^k}[\omega]/\langle \omega^m - (\beta\xi^t)^{-1} \rangle$.

Proof: The proof process is similar to that of Theorem 9 in [14]. \square

Denote the dual code of constacyclic code C by C^\perp , we can obtain the following result directly.

Lemma 3: Let C be a λ -constacyclic code of length n over \mathbb{F}_{q^m} and $C = \bigoplus_{i=1}^r C_i, i = 1, 2, \dots, r$, where $\lambda \in \mathbb{F}_q^*$ and $C_i = \left\langle \frac{x^n - \lambda}{f_i(x)} \right\rangle$. Then $C^\perp = C_1^\perp \cap C_2^\perp \cap \dots \cap C_r^\perp$.

Lemma 4: For the same conditions as in Theorem 4, we have

(i) $I(S)$ is an ideal of $\mathbb{F}_{q^k}[\omega]/\langle \omega^m - (\beta\xi^t)^{-1} \rangle$ if and only if $I^n(S)$ is an ideal of $\mathbb{F}_{q^k}[\omega]/\langle \omega^{mn} - 1 \rangle$, where $I^n(S) = \left\{ \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{j,i} \omega^{jm+i} \in \mathbb{F}_{q^k}[\omega] \mid \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{j,i} (\beta\xi^t)^{-j} \gamma_i^{q^{m-\mu}} = 0 \right\}$.

(ii) $I^n(S) \cap \mathbb{F}_q^{mn}$ is the dual code of $d_{\underline{\alpha}}(C)$.

Proof:

(i) The proof process is similar to that of Lemma 2 in [14].

(ii) Since $d_{\underline{\alpha}}$ is an \mathbb{F}_q -module isomorphism and $C = \bigoplus_{\mu \in S} C_\mu$, then $d_{\underline{\alpha}}(C) = d_{\underline{\alpha}}\left(\bigoplus_{\mu \in S} C_\mu\right)$. From Lemma 3, $d_{\underline{\alpha}}(C)^\perp = \bigcap_{\mu \in S} d_{\underline{\alpha}}(C_\mu)^\perp$. From Theorem 4, we have

$$\begin{aligned} D_{\underline{\alpha}}(C_\mu) &= \left\{ \frac{1}{n} \sum_{j=0}^{n-1} \sum_{i=0}^{m-1} \text{Tr}_1^m(\rho \gamma_i^{q^{m-\mu}} (\beta\xi^t)^{-j}) x^j y^i \mid \rho \in \mathbb{F}_{q^m} \right\}. \end{aligned}$$

Therefore

$$\begin{aligned} d_{\underline{\alpha}}(C_\mu) &= \pi^{-1}(D_{\underline{\alpha}}(C_\mu)) \\ &= \left\{ \frac{1}{n} \sum_{j=0}^{n-1} \sum_{i=0}^{m-1} \text{Tr}_1^m(\rho \gamma_i^{q^{m-\mu}} (\beta\xi^t)^{-j}) \omega^{jm+i} \mid \rho \in \mathbb{F}_{q^m} \right\}. \end{aligned}$$

Assume that $d_{\underline{\alpha}}(C_\mu)^\perp = \sum_{j=0}^{n-1} \sum_{i=0}^{m-1} a_{ji} \omega^{jm+i}$, then $a_{ji} \text{Tr}_1^m(\rho \gamma_i^{q^{m-\mu}} (\beta\xi^t)^{-j}) = \text{Tr}_1^m(a_{ji} \rho \gamma_i^{q^{m-\mu}} (\beta\xi^t)^{-j}) = 0$. Thus, $\sum_{j=0}^{n-1} \sum_{i=0}^{m-1} a_{ji} \gamma_i^{q^{m-\mu}} (\beta\xi^t)^{-j} = 0$ implying $d_{\underline{\alpha}}(C)^\perp = I^n(S) \cap \mathbb{F}_q^{mn}$. \square

Let $\mathbb{F}_{q^k} = \mathbb{F}_q((\beta\xi^t)^{-1}) \subseteq \mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^t}$, where \mathbb{F}_{q^t} is some Galois extension field of \mathbb{F}_{q^m} such that $\omega^m - (\beta\xi^t)^{-1}$ can be

factored into the product of distinct irreducible polynomials in $\mathbb{F}_{q^m}[\omega]$. Let $a(\omega) \mid (\omega^m - (\beta\xi^t)^{-1})$ and $\rho \in \mathbb{F}_{q^t}$ be a root of $a(\omega)$. Let $a(\omega) = \text{irr}(\rho, \mathbb{F}_{q^k})$ and $\bar{a}(\omega) = \text{irr}(\rho, \mathbb{F}_q)$. More generally, if $a(\omega) = \prod_{i=1}^s a_i(\omega)^{\varepsilon_i}$ then $\bar{a}(\omega) = \text{lcm}\{\bar{a}_i(\omega)^{\varepsilon_i}\}$.

Lemma 5: Let $\mathbb{F}_{q^k} = \mathbb{F}_q((\beta\xi^t)^{-1})$ and $a(\omega) = \prod_{i=1}^s a_i(\omega)^{\varepsilon_i} \mid (\omega^m - (\beta\xi^t)^{-1})$, where $a_i(\omega)$ are the distinct irreducible factors of $a(\omega)$ in $\mathbb{F}_{q^k}[\omega]$. Then

- (i) $\bar{a}(\omega) = \prod_{i=1}^s \bar{a}_i(\omega)^{\varepsilon_i}$;
- (ii) if $a(\omega) \mid b(\omega)$, then $\bar{a}(\omega) \mid b(\omega)$, where $b(\omega) \in \mathbb{F}_q[\omega]$;
- (iii) $\text{deg}(\bar{a}(\omega)) = k \text{deg}(a(\omega))$;
- (iv) $\frac{\omega^m - (\beta\xi^t)^{-1}}{\bar{a}(\omega)} = f(\omega^m)$, where $f(\omega) = \text{irr}((\beta\xi^t)^{-1}, \mathbb{F}_q)$.

Now, we introduce the main result of this section.

Theorem 5: Let $\mathbb{F}_q \neq \mathbb{F}_{q^k} = \mathbb{F}_q((\beta\xi^t)^{-1}) \subseteq \mathbb{F}_{q^m}$ and

$$C = \left\langle \frac{x^n - \lambda}{x - (\beta\xi^t)^{q^\mu}} \right\rangle$$

be a λ -constacyclic code of length n over \mathbb{F}_{q^m} . Then

(i) There exists a basis $\underline{\alpha} = \{\alpha_0, \alpha_1, \dots, \alpha_{m-1}\}$ of \mathbb{F}_{q^m} over \mathbb{F}_q , for which $d_{\underline{\alpha}}(C)$ is λ -constacyclic if and only if $\omega^m - (\beta\xi^t)^{-1}$ has a monic divisor in $\mathbb{F}_{q^k}[\omega]$ of degree $e = \frac{m}{k}$;

(ii) If $\omega^m - (\beta\xi^t)^{-1}$ has a monic divisor in $\mathbb{F}_{q^k}[\omega]$ of degree e , then $d_{\underline{\alpha}}(C)$ is λ -constacyclic if and only if $\underline{\alpha}$ is the trace-dual basis of $\underline{\gamma} = \{\gamma_0, \gamma_1, \dots, \gamma_{m-1}\}$, where $\gamma_0, \gamma_1, \dots, \gamma_{e-1}$ is a basis of \mathbb{F}_{q^m} over \mathbb{F}_{q^k} and

$$\gamma_j = \sum_{i=1}^e a_i^{q^\mu} \gamma_{j-i}, \quad e \leq j < m, \quad (13)$$

where $a(\omega) = \omega^e - a_1\omega^{e-1} - \dots - a_e \in \mathbb{F}_{q^k}[\omega]$ and $a(\omega) \mid (\omega^m - (\beta\xi^t)^{-1})$. Moreover,

$$d_{\underline{\alpha}}(C) = \left\langle \frac{z^{mn} - \lambda}{\bar{a}(z)^*} \right\rangle,$$

where $\bar{a}(z)^*$ is the reciprocal polynomial of $\bar{a}(z)$.

Proof:

(i) It is straightforward from Theorem 5 that $d_{\underline{\alpha}}(C)$ is λ -constacyclic if and only if

$$I(S) = \left\{ \sum_{i=0}^{m-1} a_i \omega^i \in \mathbb{F}_{q^k}[\omega] / \langle \omega^m - (\beta\xi^t)^{-1} \rangle \mid \sum_{i=0}^{m-1} a_i \gamma_i^{q^{m-\mu}} = 0 \right\}$$

is an ideal of $\mathbb{F}_{q^k}[\omega] / \langle \omega^m - (\beta\xi^t)^{-1} \rangle$. Let $a(\omega) = \omega^e - a_1\omega^{e-1} - \dots - a_e \in \mathbb{F}_{q^k}[\omega]$ be the generator polynomial of I . Since $\dim(I) = \dim(U^\perp) = m - \dim(U) = m - e$, then $a(\omega) \mid (\omega^m - (\beta\xi^t)^{-1})$ and $\text{deg} a(\omega) = e$.

(ii) If $d_{\underline{\alpha}}(C)$ is λ -constacyclic, by (i), we have $I(S) = \langle a(\omega) \rangle = \{b(\omega)a(\omega) \mid b(\omega) \in \mathbb{F}_{q^k}[\omega] / \langle \omega^m - (\beta\xi^t)^{-1} \rangle\}$, which implies that $\{\gamma_0^{q^{m-\mu}}, \gamma_1^{q^{m-\mu}}, \dots, \gamma_{e-1}^{q^{m-\mu}}\}$ are independent over \mathbb{F}_{q^k} . Otherwise, we can get a set of numbers that not all zeros $\{c_0, c_1, \dots, c_{e-1}\}$ satisfying $c_0\gamma_0^{q^{m-\mu}} + c_1\gamma_1^{q^{m-\mu}} + \dots + c_{e-1}\gamma_{e-1}^{q^{m-\mu}} = 0$. Clearly, $\sum_{i=0}^{m-1} c_i \omega^i \in I$. But, any nonzero polynomial in $I(S)$ has degree $\geq e$.

Since $\omega^j a(\omega) \in I, 0 \leq j < m$, then $\gamma_j^{q^{m-\mu}} = \sum_{i=1}^e a_i \gamma_{j-i}^{q^{m-\mu}}, e \leq j < m$. Thus, $\gamma_j^{q^m} = \sum_{i=1}^e a_i^{q^\mu} \gamma_{j-i}^{q^m}$. Since $\gamma_j \in \mathbb{F}_{q^m}$, then

$$\gamma_j = \sum_{i=1}^e a_i^{q^\mu} \gamma_{j-i}, \quad e \leq j < m.$$

Let $a(\omega) = \omega^e - a_1\omega^{e-1} - \dots - a_e \in \mathbb{F}_{q^k}[\omega]$ be a factor of $\omega^m - (\beta\xi^t)^{-1}$ and $\{\gamma_0, \gamma_1, \dots, \gamma_{m-1}\}$ a basis of \mathbb{F}_{q^m} over \mathbb{F}_q . To prove $d_{\underline{\alpha}}(C)$ is λ -constacyclic, we only need to show that I given by (12) is an ideal of $\mathbb{F}_{q^k}[\omega] / \langle \omega^m - (\beta\xi^t)^{-1} \rangle$. Let $\{\gamma_0, \gamma_1, \dots, \gamma_{e-1}\}$ be a basis of \mathbb{F}_{q^m} over \mathbb{F}_{q^k} and $\gamma_j = \sum_{i=1}^e a_i^{q^\mu} \gamma_{j-i}$, where $e \leq j < m$. Clearly, I is a vector space over \mathbb{F}_{q^k} of dimension $m - e$. In the following, we prove that I is an ideal with generator $a(\omega)$. In other words, for any polynomial $b(\omega) \in I$, we have $a(\omega) \mid b(\omega)$. Let $b(\omega) = \sum_{i=0}^e b_i \omega^i$. Then

$$\begin{aligned} 0 &= \sum_{i=0}^e b_i \gamma_i^{q^{m-\mu}} \\ &= \sum_{i=0}^{e-1} b_i \gamma_i^{q^{m-\mu}} + b_e \left(\sum_{i=1}^e a_i^{q^\mu} \gamma_{e-i} \right)^{q^{m-\mu}} \\ &= \sum_{i=0}^{e-1} (b_i + b_e a_{e-i}) \gamma_i^{q^{m-\mu}}. \end{aligned}$$

By the independence of $\gamma_i^{q^{m-\mu}}, 0 \leq i \leq e$, we conclude that $b_i = -b_e a_{e-i}$. Thus, $b(\omega) = \sum_{i=0}^e -b_e a_{e-i} \omega^i = b_e a(\omega)$. Assume that every polynomial in I of degree $\leq s$, where $e < s < m - 1$. Let $b(\omega) = \sum_{i=0}^s b_i \omega^i$ and $a_i = 0$, where $e < i \leq s$. Then

$$\begin{aligned} 0 &= \sum_{i=0}^{s+1} b_i \gamma_i^{q^{m-\mu}} \\ &= \sum_{i=0}^s b_i \gamma_i^{q^{m-\mu}} + b_{s+1} \sum_{i=1}^s a_i \gamma_{s+1-i}^{q^{m-\mu}} \\ &= \sum_{i=0}^s b_i \gamma_i^{q^{m-\mu}} + b_{s+1} \sum_{i=s+1-e}^s a_{s+1-i} \gamma_i^{q^{m-\mu}} \\ &= \sum_{i=0}^s (b_i + b_{s+1} a_{s+1-i}) \gamma_i^{q^{m-\mu}}. \end{aligned}$$

Hence

$$\sum_{i=0}^s (b_i + b_{s+1} a_{s+1-i}) \omega^i \in I.$$

By induction hypothesis, $a(\omega) \mid \sum_{i=0}^s (b_i + b_{s+1} a_{s+1-i}) \omega^i$. Let $a(\omega)c(\omega) = \sum_{i=0}^s (b_i + b_{s+1} a_{s+1-i}) \omega^i$. Then

$$\sum_{i=0}^{s+1} b_i \omega^i = a(\omega)c(\omega) - b_{s+1} \sum_{i=0}^s a_{s+1-i} \omega_i + b_{s+1} \omega^{s+1}$$

$$\begin{aligned}
 &= a(\omega)c(\omega) - b_{s+1} \sum_{i=1}^e a_i \omega_{s+1-i} + b_{s+1} \omega^{s+1} \\
 &= a(\omega)c(\omega) + b_{s+1} \omega^{s+1-e}.
 \end{aligned}$$

Therefore $a(\omega) \mid \sum_{i=0}^{s+1} b_i \omega^i$

Finally, we will prove $d_{\underline{\alpha}}(C) = \left\langle \frac{z^{mn} - \lambda}{\bar{a}(z)^*} \right\rangle$.

Let $I = \langle a(\omega) \rangle$. According to Lemma 4, we have $I \subseteq I^n$. Thus, $\langle a(\omega) \rangle \cap \mathbb{F}_q^{mn} \subseteq I^n \cap \mathbb{F}_q^{mn}$. Let $b(\omega) \in \langle a(\omega) \rangle \cap \mathbb{F}_q^{mn}$. Then $a(\omega) \mid b(\omega)$. From Lemma 5 (ii), we have $\bar{a}(\omega) \mid b(\omega)$, which implies that $b(\omega) \in \langle \bar{a}(\omega) \rangle$. Therefore

$$\langle a(\omega) \rangle \cap \mathbb{F}_q^{mn} \subseteq \langle \bar{a}(\omega) \rangle.$$

Let $c(\omega) \in \mathbb{F}_q[\omega]$ and $c(\omega) \in \langle \bar{a}(\omega) \rangle$, where $a(\omega) = \prod_{i=1}^s a_i(\omega)^{e_i}$. Since $a_i(\omega) \mid \bar{a}_i(\omega)$ in $\mathbb{F}_{q^k}[\omega]$ and $\bar{a}_i(\omega)^{e_i} \mid c(\omega)$, then $a_i(\omega)^{e_i} \mid c(\omega)$ implying $a(\omega) \mid c(\omega)$. Consequently,

$$\bar{a}(\omega) \subseteq \langle a(\omega) \rangle \cap \mathbb{F}_q^{mn}.$$

Thus $\bar{a}(\omega) = \langle a(\omega) \rangle \cap \mathbb{F}_q^{mn}$. From Lemma 4(ii), we have $d_{\underline{\alpha}}(C)^\perp = I^n(S) \cap \mathbb{F}_q^{mn}$. To prove $d_{\underline{\alpha}}(C) = \left\langle \frac{z^{mn} - \lambda}{\bar{a}(z)^*} \right\rangle$, we only need to show that $d_{\underline{\alpha}}(C)^\perp = \langle \bar{a}(\omega) \rangle$. Now, we have known that $\langle \bar{a}(\omega) \rangle \subseteq I^n \cap \mathbb{F}_q^{mn} = d_{\underline{\alpha}}(C)^\perp$ and $|d_{\underline{\alpha}}(C)^\perp| = q^{mn-m} = |\langle \bar{a}(\omega) \rangle|$. Therefore $d_{\underline{\alpha}}(C)^\perp = \langle \bar{a}(\omega) \rangle$. Thus,

$$d_{\underline{\alpha}}(C) = \left\langle \frac{z^{mn} - \lambda}{\bar{a}(z)^*} \right\rangle.$$

□

Example 2: Consider the polynomial $x^6 - 4$ over \mathbb{F}_5 . The order of 4 in \mathbb{F}_5^* is 2. We have $x^6 - 4 = \prod_{t=0}^5 (x - \beta^{1+2t}) = (x - \beta)(x - \beta^3)(x - \beta^5)(x - \beta^7)(x - \beta^9)(x - \beta^{11})$, where β is a primitive 12th root of unity. And

$$\begin{aligned}
 (x - \beta) \cdot (x - \beta^5) &= x^2 + 2x + 4, & x - \beta^3 &= x + 3, \\
 (x - \beta^7) \cdot (x - \beta^{11}) &= x^2 + 3x + 4, & x - \beta^9 &= x + 2.
 \end{aligned}$$

Let $q = 5, m = k = 2$ and $\mathbb{F}_{25} = \mathbb{F}_5(\beta)$. Let C be an $[6, 1]$ irreducible 25-ary 4-constacyclic code with the parity check polynomial $x - \beta^{-1}$. Then $e = \frac{m}{k} = 1$. We use the recursion $\rho^2 = \rho + 3$ generate \mathbb{F}_{25} , where ρ is a root of $x^2 + 4x + 2$. Then we have

$$\begin{aligned}
 \mathbb{F}_{25} &= \{0, 1, \rho, \rho^2 = \rho + 3, \rho^3 = 4\rho + 3, \rho^4 = 2\rho + 2, \\
 &\rho^5 = 4\rho + 1, \rho^6 = 2, \rho^7 = 2\rho, \rho^8 = 2\rho + 1, \rho^9 = 3\rho + 1, \\
 &\rho^{10} = 4\rho + 4, \rho^{11} = 3\rho + 2, \rho^{12} = 4, \rho^{13} = 4\rho, \rho^{14} = 4\rho + 2, \\
 &\rho^{15} = \rho + 2, \rho^{16} = 3\rho + 3, \rho^{17} = \rho + 4, \rho^{18} = 3, \rho^{19} = 3\rho, \\
 &\rho^{20} = 3\rho + 4, \rho^{21} = 2\rho + 4, \rho^{22} = \rho + 1, \rho^{23} = 2\rho + 3\}.
 \end{aligned}$$

Let $\beta = \rho^2$. Then $\omega^2 - \beta = \omega^2 - \rho^2 = (\omega - \beta)(\omega + \beta)$. Thus, $a(\omega) = (\omega - \rho) \in \mathbb{F}_{25}[\omega]$ is a divisor of $\omega^2 - \rho^2$. Let $\gamma_0 = 1, \gamma_1 = a_1 \gamma_0 = \rho$. Then we have

$$B = Tr_5^{25}(\gamma_i \gamma_j) = \begin{pmatrix} Tr_5^{25}(1) & Tr_5^{25}(\rho) \\ Tr_5^{25}(\rho) & Tr_5^{25}(\rho^2) \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

and

$$B^{-1} = \begin{pmatrix} \frac{2}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix} = \begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix}.$$

Therefore

$$(\alpha_0, \alpha_1) = (\gamma_0, \gamma_1)B^{-1} = (\rho^{20}, \rho^3)$$

is the trace-dual basis of $\gamma = (\gamma_0, \gamma_1)$ and it is a basis of \mathbb{F}_{25} over \mathbb{F}_5 for which $d_{\underline{\alpha}}(C)$ is also a 4-constacyclic code. Further, we can get $\bar{a}(\omega) = (\omega - \rho)(\omega - \rho^5) = \omega^2 + 4\omega + 2$ implying $\bar{a}(\omega)^* = 2\omega^2 + 4\omega + 1$. Therefore, by Theorem 5, we have

$$\begin{aligned}
 d_{\underline{\alpha}}(C) &= \left\langle \frac{x^{12} - 4}{2x^2 + 4x + 1} \right\rangle \\
 &= \langle x^{10} + x^8 + 3x^9 + 4x^7 + 4x^6 + 3x^4 + 4x^3 + 3x^2 + 2x + 2 \rangle.
 \end{aligned}$$

Lemma 6: Let C be a λ -constacyclic code over \mathbb{F}_q^m with the dual code C^\perp . Let $\underline{\alpha}$ be a basis of \mathbb{F}_q^m over \mathbb{F}_q with trace-dual basis $\underline{\alpha}^\perp$. Then $d_{\underline{\alpha}}(C)^\perp = d_{\underline{\alpha}^\perp}(C^\perp)$.

Proof: Let $\underline{\alpha}^\perp = \underline{\gamma} = (\gamma_0, \gamma_1, \dots, \gamma_{m-1})$. For any $a(z) \in d_{\underline{\alpha}^\perp}(C^\perp)$, we need to show $a(z) \in d_{\underline{\alpha}}(C)^\perp$. Let $a(z) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j} z^{mj+i} \in d_{\underline{\alpha}^\perp}(C^\perp)$. Then $a(z) \in d_{\underline{\gamma}}(C^\perp)$. Thus $d_{\underline{\gamma}}^{-1}(a(z)) = \sum_{j=0}^{n-1} (\sum_{i=0}^{m-1} a_{i,j} \gamma_i) z^j \in C^\perp$. Then for any $b(z) = \sum_{j=0}^{n-1} b_j z^j \in C$, where $b_j = \sum_{i=0}^{m-1} b_{i,j} \gamma_i$ and $b_{i,j} = Tr_1^m(b_j \gamma_i)$, from the above description we have $\sum_{j=0}^{n-1} b_j \sum_{i=0}^{m-1} a_{i,j} \gamma_i = 0$. Since $d_{\underline{\alpha}}(b(z)) = \sum_{j=0}^{n-1} \sum_{i=0}^{m-1} b_{i,j} z^{mj+i} = \sum_{j=0}^{n-1} \sum_{i=0}^{m-1} Tr_1^m(b_j \gamma_i) z^{mj+i} \in d_{\underline{\alpha}}(C)$, then we get $Tr_1^m(\sum_{j=0}^{n-1} \sum_{i=0}^{m-1} b_j a_{i,j} \gamma_i) = \sum_{j=0}^{n-1} \sum_{i=0}^{m-1} a_{i,j} Tr_1^m(b_j \gamma_i) = 0$. Thus, $\sum_{j=0}^{n-1} \sum_{i=0}^{m-1} a_{i,j} z^{mj+i} \in d_{\underline{\alpha}}(C)^\perp$. Therefore, $d_{\underline{\alpha}^\perp}(C^\perp) \subseteq d_{\underline{\alpha}}(C)^\perp$.

On the other hand, $d_{\underline{\alpha}}(C)^\perp \subseteq (d_{\underline{\alpha}^\perp}(C^\perp)^\perp)^\perp = d_{\underline{\alpha}^\perp}(C^\perp)$. Consequently, $d_{\underline{\alpha}}(C)^\perp = d_{\underline{\alpha}^\perp}(C^\perp)$. □

From Theorem 3, Lemmas 5 and 6, we can get the following result.

Theorem 6: Let $\mathbb{F}_q \neq \mathbb{F}_{q^k} = \mathbb{F}_q((\beta \xi^t)^{-1}) \subseteq \mathbb{F}_q^m$ and

$$C = \left\langle \frac{x^n - \lambda}{\prod_{\mu \in S} (x - (\beta \xi^t)^{q^\mu})} \right\rangle$$

be a λ -constacyclic code of length n over \mathbb{F}_q^m , where $S \subseteq \mathbb{Z}_k$ and $|S| = k - 1$. Then

(i) there exists a basis $\underline{\alpha}$ of \mathbb{F}_q^m over \mathbb{F}_q for which $d_{\underline{\alpha}}(C)$ is λ -constacyclic if and only if $\omega^m - (\beta \xi^t)^{-1}$ has a monic divisor in $\mathbb{F}_{q^k}[\omega]$ of degree $e = \frac{m}{k}$.

(ii) if $\omega^m - (\beta \xi^t)^{-1}$ has a monic divisor over \mathbb{F}_{q^k} of degree e , then $d_{\underline{\alpha}}(C)$ is λ -constacyclic if and only if $\alpha_{m-1}, \alpha_{m-2}, \dots, \alpha_{m-e}$ are independent and

$$\alpha_j = \sum_{i=1}^e a_i^{q^i} \alpha_{j+i}, 0 \leq j < m - e \tag{14}$$

where $a(\omega) = \omega^e - a_1 \omega^{e-1} - \dots - a_e \in \mathbb{F}_{q^k}[\omega]$ and $a(\omega) \mid (\omega^m - (\beta \xi^t)^{-1})$, and $v \in \mathbb{Z}_k, v \notin S$. Moreover

$$d_{\underline{\alpha}}(C) = \left\langle \frac{z^{mn} - \lambda}{\bar{b}(z)^*} \right\rangle,$$

TABLE 1. All the elements of $\mathbb{F}_{3^4}^*$.

i	ρ^i	i	ρ^i	i	ρ^i
1	ρ	28	$\rho + 1$	55	$\rho^3 + 2\rho^2 + \rho + 2$
2	ρ^2	29	$\rho^2 + \rho$	56	$\rho^2 + 2\rho + 1$
3	ρ^3	30	$\rho^3 + \rho^2$	57	$\rho^3 + 2\rho^2 + \rho$
4	$\rho^3 + 1$	31	$2\rho^3 + 1$	58	$3\rho^3 + \rho^2 + 1$
5	$\rho^3 + \rho + 1$	32	$2\rho^3 + \rho + 2$	59	$2\rho^2 + 1$
6	$\rho^3 + \rho^2 + \rho + 1$	33	$2\rho^3 + \rho^2 + 2\rho + 2$	60	$\rho^3 + \rho^2 + 1$
7	$2\rho^3 + \rho^2 + \rho + 1$	34	$2\rho^2 + 2\rho + 2$	61	$2\rho^3 + \rho + 1$
8	$\rho^2 + \rho + 2$	35	$2\rho^3 + 2\rho^2 + 2\rho$	62	$2\rho^3 + \rho^2 + \rho + 2$
9	$\rho^3 + \rho^2 + 2\rho$	36	$2\rho^3 + 2\rho^2 + 2$	63	$\rho^2 + 2\rho + 2$
10	$2\rho^3 + 2\rho^2 + 1$	37	$\rho + 1$	64	$\rho^3 + 2\rho^2 + 2\rho$
11	$\rho^3 + \rho + 2$	38	$2\rho^2 + \rho$	65	$2\rho^2 + 1$
12	$\rho^3 + \rho^2 + 2\rho + 1$	39	$2\rho^3 + \rho^2$	66	$2\rho^3 + \rho$
13	$2\rho^3 + 2\rho^2 + \rho + 1$	40	2	67	$2\rho^3 + \rho^2 + 2$
14	$\rho^3 + \rho^2 + \rho + 2$	41	2ρ	68	$2\rho + 2$
15	$2\rho^3 + \rho^2 + 2\rho + 1$	42	$2\rho^2$	69	$2\rho^2 + 2\rho$
16	$2\rho^2 + \rho + 2$	43	$2\rho^3$	70	$2\rho^3 + 2\rho^2$
17	$2\rho^3 + \rho^2 + 2\rho$	44	$2\rho^3 + 2$	71	$\rho^3 + 2$
18	$2\rho^2 + 2$	45	$2\rho^3 + 2\rho + 2$	72	$\rho^3 + 2\rho + 1$
19	$2\rho^3 + 2\rho$	46	$2\rho^3 + 2\rho^2 + 2\rho + 2$	73	$\rho^3 + 2\rho^2 + \rho + 1$
20	$2\rho^3 + 2\rho^2 + 2$	47	$\rho^3 + 2\rho^2 + 2\rho + 2$	74	$\rho^2 + \rho + 1$
21	$\rho^3 + 2\rho + 2$	48	$2\rho^2 + 2\rho + 1$	75	$\rho^3 + \rho^2 + \rho$
22	$\rho^3 + 2\rho^2 + 2\rho + 1$	49	$2\rho^3 + 2\rho^2 + \rho$	76	$2\rho^3 + \rho^2 + 1$
23	$\rho^2 + \rho + 1$	50	$\rho^3 + \rho^2 + 2$	77	$\rho + 2$
24	$2\rho^3 + \rho^2 + \rho$	51	$2\rho^3 + 2\rho + 1$	78	$\rho^2 + 2\rho$
25	$\rho^2 + 2$	52	$2\rho^3 + 2\rho^2 + \rho + 2$	79	$\rho^3 + 2\rho^2$
26	$\rho^3 + 2\rho$	53	$\rho^3 + \rho^2 + 2\rho + 2$	80	1
27	$\rho^3 + 2\rho^2 + 1$	54	$2\rho^3 + 2\rho^2 + 2\rho + 1$		

where $\bar{b}(z)^*$ is the reciprocal polynomial of $\bar{b}(z)$ and $b(\omega) = \frac{\omega^m - (\beta\xi^t)^{-1}}{a(\omega)}$.

Proof: This proof process is similar to that of Theorem 5. \square

Example 3: Consider the polynomial $x^5 - 2$ over \mathbb{F}_3 . The order of 2 in \mathbb{F}_3^* is 2. We have $x^5 - 2 = \prod_{t=0}^4 (x - \beta^{1+2t}) = (x - \beta)(x - \beta^3)(x - \beta^5)(x - \beta^7)(x - \beta^9)$, where β is a primitive 10th root of unity. Let $q = 3, k = m = 4, \mathbb{F}_{3^4} = \mathbb{F}_3(\beta)$ and C be a 81-ary 2-constacyclic code of length 5 with the parity check polynomial $h(x) = (x - \beta^{-1})(x - \beta^{-3})(x - \beta^{-9})$. We generate \mathbb{F}_{3^4} by means of recursion $\rho^4 = \rho^3 + 1$, where ρ is a root of $x^4 + 2x^3 + 2$.

Let $\beta = \rho^8$. Then $\omega^4 - \beta = \omega^4 - \rho^8 = (\omega - \rho^2)(\omega - \rho^{22})(\omega - \rho^{42})(\omega - \rho^{62})$. Now, we choose $a(\omega) = (\omega - \rho^2) \in \mathbb{F}_{81}[\omega]$ as a divisor of $\omega^4 - \beta$ of degree 1. Setting $\alpha_3 = 1$, then we have that $\alpha_j = a_1\alpha_{j+1}$. Thus, $\alpha_2 = \rho^2, \alpha_1 = \rho^4, \alpha_0 = \rho^6$. Hence $\underline{\alpha} = \{\rho^6, \rho^4, \rho^2, 1\}$ is a basis of \mathbb{F}_{81} over \mathbb{F}_3 for which $d_{\underline{\alpha}}(C)$ is a 2-constacyclic code. Since $b(\omega) = \frac{\omega^4 - \beta}{\omega - \rho^2} = (\omega - \rho^{22})(\omega - \rho^{42})(\omega - \rho^{62})$, then $\bar{b}(\omega) = \text{irr}(\rho^{22}, \mathbb{F}_3)\text{irr}(\rho^{42}, \mathbb{F}_3)\text{irr}(\rho^{62}, \mathbb{F}_3) = \omega^{12} + \omega^{11} + 2\omega^9 + \omega^5 + 2\omega^4 + \omega^3 + 2\omega^2 + 1$. Further $\bar{b}(\omega)^* = \omega^{12} + 2\omega^{10} + \omega^9 + 2\omega^8 + \omega^7 + 2\omega^3 + \omega + 1$. Consequently, we have

$$d_{\underline{\alpha}}(C) = \left\langle \frac{x^{20} - 2}{x^{12} + 2x^{10} + x^9 + 2x^8 + x^7 + 2x^3 + x + 1} \right\rangle = \langle x^8 + x^6 + 2x^5 + 2x^4 + x^2 + 2x + 1 \rangle. \quad (15)$$

Now, we make a conclusion on the Theorems 3, 5 and 6.

Theorem 7: Let $\gcd(n, q) = 1$ and C be a q^m -ary λ -constacyclic code of length n with the parity check polynomial $h(x)$. Then there exists a basis $\underline{\alpha}$ of \mathbb{F}_{q^m} over \mathbb{F}_q for which $d_{\underline{\alpha}}(C)$ is λ -constacyclic if and only if

(i) Let $h(x) \in \mathbb{F}_q[x]$, then $d_{\underline{\alpha}}(C)$ is λ -constacyclic for every basis $\underline{\alpha}$. Further, the parity check polynomial of $d_{\underline{\alpha}}(C)$ is $h(z^m)$;

(ii) Let $h(x) = h_0(x)(x - (\beta\xi^t)^{q^\mu})$, where $h_0(x) \in \mathbb{F}_q[x]$ and $\mu \in \mathbb{Z}_k$. Let $\mathbb{F}_q \neq \mathbb{F}_{q^k} = \mathbb{F}_q((\beta\xi^t)^{-1}) \subseteq \mathbb{F}_{q^m}$, and $\omega^m - (\beta\xi^t)^{-1}$ have a divisor over \mathbb{F}_{q^k} of degree $e = \frac{m}{k}$. Then, $d_{\underline{\alpha}}(C)$ is λ -constacyclic if and only if $\underline{\alpha}$ is the trace-dual basis of $\gamma = \{\gamma_0, \gamma_1, \dots, \gamma_{m-1}\}$, where $\gamma_0, \gamma_1, \dots, \gamma_{e-1}$ is a basis of \mathbb{F}_{q^m} over \mathbb{F}_{q^k} and

$$\gamma_j = \sum_{i=1}^e a_i^{q^{\mu}} \gamma_{j-i}, e \leq j < m \quad (16)$$

with $a(\omega) = \omega^e - a_1\omega^{e-1} - \dots - a_e \in \mathbb{F}_{q^k}[\omega]$ and $a(\omega) \mid (\omega^m - (\beta\xi^t)^{-1})$. Moreover

$$d_{\underline{\alpha}}(C) = \left\langle \frac{z^{mn} - \lambda}{h_0(z^m)\bar{a}(z)^*} \right\rangle,$$

where $\bar{a}(z)^*$ is the reciprocal polynomial of $\bar{a}(z)$;

(iii) Let $h(x) = h_0(x)\prod_{\mu \in S} (x - (\beta\xi^t)^{q^\mu})$, where $h_0(x) \in \mathbb{F}_q[x]$ and $S \subseteq \mathbb{Z}_k$. Let $\mathbb{F}_q \neq \mathbb{F}_{q^k} = \mathbb{F}_q((\beta\xi^t)^{-1}) \subseteq \mathbb{F}_{q^m}$, and $\omega^m - (\beta\xi^t)^{-1}$ have a monic divisor over \mathbb{F}_{q^k} of degree e . Then, $d_{\underline{\alpha}}(C)$ is λ -constacyclic if and only if $\alpha_{m-1}, \alpha_{m-2}, \dots, \alpha_{m-e}$ are independent and

$$\alpha_j = \sum_{i=1}^e a_i^{q^v} \alpha_{j+i}, 0 \leq j < m - e$$

where $a(\omega) = \omega^e - a_1\omega^{e-1} - \dots - a_e \in \mathbb{F}_{q^k}[\omega]$ is a factor of $\omega^m - (\beta\xi^t)^{-1}$ and $v \in \mathbb{Z}_k, v \notin S$. Moreover,

$$d_{\underline{\alpha}}(C) = \left\langle \frac{z^{mn} - \lambda}{\bar{b}(z)^*} \right\rangle,$$

where $\bar{b}(z)^*$ is the reciprocal polynomial of $\bar{b}(z)$ and $b(\omega) = \frac{\omega^m - (\beta\xi^t)^{-1}}{a(\omega)}$. \square

V. CONCATENATED FORM OF q -ARY IMAGES

We have shown that, under certain conditions, the q -ary images of λ -constacyclic codes are also λ -constacyclic. In this section, we will give a representation of some λ -constacyclic q -ary images in concatenated form. To do this, we will use two related tools in this section. One is an \mathbb{F}_q -ring isomorphism between $\mathbb{F}_q[z]/\langle z^{mm} - \lambda \rangle$ and $\mathbb{F}_q[x, y]/\langle x^n - \lambda, y^m - x \rangle$, the other is the notion of a concatenated code.

We have introduced the map $d_{\underline{\alpha}}$ from $\mathbb{F}_{q^m}[z]/\langle z^n - \lambda \rangle$ into $\mathbb{F}_q[z]/\langle z^{mm} - \lambda \rangle$ by

$$d_{\underline{\alpha}} : \mathbb{F}_{q^m}[z]/\langle z^n - \lambda \rangle \rightarrow \mathbb{F}_q[z]/\langle z^{mm} - \lambda \rangle$$

$$a(z) = \sum_{j=0}^{n-1} a_j z^j \mapsto \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_{i,j} z^{mj+i},$$

where $a_j = \sum_{i=0}^{m-1} a_{i,j}\alpha_i$ and $a_{i,j} \in \mathbb{F}_q$.

From the definition of d_α , we have $a(z) = \sum_{j=0}^{n-1} \sum_{i=0}^{m-1} a_{i,j} \alpha_i z^j$. Now, let $a_i(z) = \sum_{j=0}^{n-1} a_{i,j} z^j$. Then $a_i(z^m) = \sum_{j=0}^{n-1} a_{i,j} z^{mj}$. Thus, $d_\alpha(a(z)) = \sum_{i=0}^{m-1} a_i(z^m) z^i$.

Lemma 7: Let $d_\alpha(c(z)) = \sum_{i=0}^{m-1} c_i(z^m) z^i \in \mathbb{F}_q[z]/\langle z^{mn} - \lambda \rangle$. Then

$$d_\alpha^{-1}(zd_\alpha(c(z))) = \alpha_0 z c_{m-1}(z) + \sum_{i=1}^{m-1} \alpha_i c_{i-1}(z).$$

Proof: Since

$$zd_\alpha(c(z)) = \sum_{i=0}^{m-1} c_i(z^m) z^{i+1} = \sum_{i=1}^m c_{i-1}(z^m) z^i,$$

then $d_\alpha^{-1}(zd_\alpha(c(z))) = d_\alpha^{-1}(\sum_{i=1}^{m-1} c_{i-1}(z^m) z^i + c_{m-1}(z^m) z^m) = \sum_{i=1}^{m-1} \alpha_i c_{i-1}(z) + \alpha_0 z c_{m-1}(z)$. \square

Define a map as follows

$$\begin{aligned} \Pi : \mathbb{F}_q[z]/\langle z^{mn} - \lambda \rangle &\rightarrow \mathbb{F}_q[x, y]/\langle x^n - \lambda, y^m - x \rangle \\ \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j} z^{mj+i} &\mapsto \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j} x^j y^i. \end{aligned}$$

It is easy to verify that Π is a ring isomorphism over \mathbb{F}_q .

Definition 2: [16] Let C be a linear code over \mathbb{F}_{q^m} . Then $Tr_1^m(C) = \{(Tr_1^m(b_1), Tr_1^m(b_2), \dots, Tr_1^m(b_n)) \mid (b_1, b_2, \dots, b_n) \in C\}$ is called the trace code of C . It is a linear code over \mathbb{F}_q .

Let $\alpha = \{\alpha_0, \alpha_1, \dots, \alpha_{m-1}\}$ be a basis of \mathbb{F}_{q^m} over \mathbb{F}_q . For all $0 \leq i \leq m-1$, define a map from $\mathbb{F}_{q^m}^n$ into \mathbb{F}_q^n by

$$\begin{aligned} h_i : \mathbb{F}_{q^m}^n &\rightarrow \mathbb{F}_q^n \\ \sum_{j=0}^{m-1} \alpha_j c_j &\mapsto c_i, \end{aligned} \quad (17)$$

where $c_j \in \mathbb{F}_{q^m}^n, j = 0, 1, \dots, n-1$.

Clearly, for all $0 \leq i \leq m-1, h_i$ is a \mathbb{F}_q -linear map.

Proposition 4: Let C be a λ -constacyclic code of length n over \mathbb{F}_{q^m} . Then, for all $0 \leq i \leq m-1, h_i(C) = Tr_1^m(C)$.

Proof: Let $\alpha = \{\alpha_0, \alpha_1, \dots, \alpha_{m-1}\}$ be a basis of \mathbb{F}_{q^m} over \mathbb{F}_q and $\gamma = \{\gamma_0, \gamma_1, \dots, \gamma_{m-1}\}$ be its dual basis. Then we have $\alpha_i \gamma_j = 1$ where $i = j$, otherwise $\alpha_i \gamma_j = 0$. Now, let $c = \sum_{i=0}^{m-1} h_i(c) \alpha_i \in C$. For any $c \in C$, we have $Tr_1^m(\gamma_j c) = Tr_1^m(\gamma_j \sum_{i=0}^{m-1} h_i(c) \alpha_i) = Tr_1^m(\sum_{i=0}^{m-1} h_i(c) \gamma_j \alpha_i) = Tr_1^m(h_i(c)) = h_i(c)$, where $0 \leq i \leq m-1$.

For any codeword c of C and γ_j of \mathbb{F}_{q^m} , we have that $\gamma_j c$ runs through C . Consequently, $Tr_1^m(C) \subseteq h_i(C)$. Therefore $h_i(C) = Tr_1^m(h_i(C)) = Tr_1^m(\sum_{i=0}^{m-1} h_i(c) \gamma_j \alpha_i) = Tr_1^m(\gamma_j c) \subseteq Tr_1^m(C)$. Thus, we have that $Tr_1^m(C) = h_i(C)$. \square

From the above discussion, we have the following result.

Theorem 8: Let C be a λ -constacyclic code over \mathbb{F}_{q^m} with the minimal generating set $\{g_1, g_2, \dots, g_k\}$. Then, $\{h_i(g_j), 0 \leq i \leq m-1, 1 \leq j \leq k\}$ generates $Tr_1^m(C)$ over \mathbb{F}_q .

Proof: Let $c = \sum_{j=1}^k \lambda_j g_j \in C$, where $\lambda_j \in \mathbb{F}_{q^m}$. Assume that $\alpha = \{\alpha_0, \alpha_1, \dots, \alpha_{m-1}\}$ be a basis of \mathbb{F}_{q^m} over \mathbb{F}_q . Then there exist elements $\lambda_{js} \in \mathbb{F}_q$ and $\rho_{sir} \in \mathbb{F}_q$ such that $\lambda_j = \sum_{s=0}^{m-1} \lambda_{js} \alpha_s$ and $\alpha_s \alpha_i = \sum_{r=0}^{m-1} \rho_{sir} \alpha_r$. According to Definition 2, we have $g_j = \sum_{i=0}^{m-1} h_i(g_j) \alpha_i$, for all $1 \leq j \leq k$. Therefore,

$$\begin{aligned} c &= \sum_{j=1}^k \lambda_j g_j = \sum_{j=1}^k \sum_{s=0}^{m-1} \lambda_{js} \alpha_s g_j \\ &= \sum_{i=0}^{m-1} \sum_{j=1}^k \sum_{s=0}^{m-1} \lambda_{js} \alpha_s h_i(g_j) \alpha_i \\ &= \sum_{r=0}^{m-1} \sum_{j=1}^k \sum_{i=0}^{m-1} \sum_{s=0}^{m-1} \lambda_{js} \rho_{sir} h_i(g_j) \alpha_r. \end{aligned}$$

Consequently, for all $0 \leq r \leq m-1$, we have

$$h_r(c) = \sum_{r=0}^{m-1} \sum_{j=1}^k \sum_{s=0}^{m-1} \lambda_{js} \rho_{sir} h_i(g_j),$$

which implies that $\{h_i(g_j), 0 \leq i \leq m-1, 1 \leq j \leq k\}$ generates $h_r(C)$. \square

Corollary 1: Let $\alpha = \{\alpha_0, \alpha_1, \dots, \alpha_{m-1}\}$ be a basis of \mathbb{F}_{q^m} over \mathbb{F}_q and C be an $[n, k]$ λ -constacyclic code over \mathbb{F}_{q^m} with the generator polynomial $g(x) = \sum_{i=0}^{m-1} \alpha_i g_i(x)$ for some $g_i(x) \in \mathbb{F}_q[x]$. Then $Tr(C)$ is generated by $\gcd(g_0(x), g_1(x), \dots, g_{m-1}(x))$.

Proof: Since C is a λ -constacyclic code over \mathbb{F}_q , then $Tr(C)$ is also a λ -constacyclic code over \mathbb{F}_q . From Theorem 8, we have that $\{h_i(x^j g(x)), 0 \leq j \leq k-1\} = \{x^j g_i(x) \mid g_i(x) \in \mathbb{F}_q[x], 0 \leq i \leq m-1, 0 \leq j \leq k-1\}$. Then $Tr(C) = \langle \gcd(x^j g_i(x) \mid 0 \leq i \leq m-1, 0 \leq j \leq k-1) \rangle = \langle \gcd(g_0(x), g_1(x), \dots, g_{m-1}(x)) \rangle$. \square

From the Eq. (5) in Section 1, the map χ from $\langle \theta_i \rangle$ to $\mathbb{F}_q[x]/\langle h_i(x) \rangle$ defined by $\chi(c(x)) = c(\beta \xi^t)$ is a field isomorphism, where $\beta \xi^t = \beta^{1+u_i}$ is a root of $h_i(x)$. Now, let the inverse χ^{-1} of χ be defined by $\chi^{-1}(e) = \sum_{i=0}^{n-1} c_i x^i$, where $c_i = \frac{1}{n} Tr(e(\beta \xi^t)^{-i}), 0 \leq i \leq n-1$.

Definition 3: Let A be an $[n, k]$ λ -constacyclic minimal code over \mathbb{F}_q and B be an ideal of $\mathbb{F}_{q^k}[y]/\langle y^N - (\beta \xi^t) \rangle$, where $\beta \xi^t$ is a nonzero root of A . Then the linear code $A \square B = \{\sum_{j=0}^{N-1} \chi^{-1}(b_j) y^j \mid \sum_{j=0}^{N-1} b_j y^j \in B\}$ is called a concatenated code with $\beta \xi^t$ -constacyclic outer code B .

Theorem 9: Let A be an $[n, k]$ λ -constacyclic minimal code over \mathbb{F}_q and B be an ideal of $\mathbb{F}_{q^k}[y]/\langle y^N - (\beta \xi^t) \rangle$, where $\beta \xi^t$ is a nonzero root of A . Then the concatenated code $A \square B = \{\sum_{j=0}^{N-1} \chi^{-1}(b_j) y^j \mid \sum_{j=0}^{N-1} b_j y^j \in B\}$ is an ideal of $T_{n,N}$, where $T_{n,N} = \mathbb{F}_q[x, y]/\langle x^n - \lambda, y^N - x \rangle$.

Proof: Clearly, $A \square B$ is a linear code. Let $c(x, y) \in A \square B$. Then we need to show that $xc(x, y) \bmod (x^n - \lambda), yc(x, y) \bmod (x^n - \lambda, y^N - x)$ are elements of $A \square B$. Let $b(y) = \sum_{j=0}^{N-1} b_j y^j \in B$. Then $c(x, y) = \sum_{j=0}^{N-1} \chi^{-1}(b_j) y^j \in A \square B$. Since B is a $\beta \xi^t$ -constacyclic code, then $b_1(y) = \beta \xi^t b(y) \in B$

and $b_2(y) = yb(y) \in B \text{ mod}(y^N - \beta\xi^t)$. Moreover,

$$\begin{aligned} &\chi^{-1}(\beta\xi^t b_j) \\ &= \frac{1}{n} \sum_{i=0}^{n-1} \text{Tr}(\beta\xi^t b_j(\beta\xi^t)^{-i})x^i \\ &= \frac{1}{n} \sum_{i=0}^{n-1} \text{Tr}(b_j(\beta\xi^t)^{1-i})x^i \\ &= \frac{1}{n} (\text{Tr}(b_j\beta\xi^t + \text{Tr}(b_j)x + \dots + \text{Tr}(b_j(\beta\xi^t)^{-n+2}x^{n-1})) \end{aligned}$$

and

$$\begin{aligned} &\chi^{-1}(b_j) \\ &= x \frac{1}{n} \sum_{i=0}^{n-1} \text{Tr}((\beta\xi^t)^{-i} b_j)x^i = \frac{1}{n} (\text{Tr}(b_j)x \\ &\quad + \text{Tr}((\beta\xi^t)^{-1} b_j)x^2 + \dots + \text{Tr}((\beta\xi^t)^{-n+1} b_j)x^n) \\ &= \frac{1}{n} (\text{Tr}(b_j\beta\xi^t) + \text{Tr}(b_j)x + \dots + \text{Tr}(b_j(\beta\xi^t)^{-n+2}x^{n-1}) \\ &\quad \times (\text{mod } x^n - \lambda)). \end{aligned}$$

Therefore, $\chi^{-1}(\beta\xi^t b_j) = x\chi^{-1}(b_j)(\text{mod } x^n - \lambda)$. Let $c_1(x, y)$ and $c_2(x, y)$ be two elements of the concatenated code corresponding to $b_1(y)$ and $b_2(y)$. Then

$$c_1(x, y) = \sum_{j=0}^{N-1} \chi^{-1}(\beta\xi^t b_j)y^j = xc(x, y)(\text{mod } x^n - \lambda)$$

and

$$\begin{aligned} c_2(x, y) &= \chi^{-1}(b_0)y + \chi^{-1}(b_1)y^2 + \dots + \chi^{-1}(b_{N-1})y^N \\ &= yc(x, y)(\text{mod } x^n - \lambda, y^N - x). \end{aligned}$$

□

The following theorem is a fundamental result in this section.

Theorem 10: Let C be an $[n, k]$ λ -constacyclic code over \mathbb{F}_{q^m} such that $d_{\underline{\alpha}}(C)$ is also a λ -constacyclic code and $\underline{\alpha} = \{\alpha_0, \alpha_1, \dots, \alpha_{m-1}\}$ be a basis of \mathbb{F}_{q^m} over \mathbb{F}_q . Assume that $\text{Tr}(C)$ is a λ -constacyclic minimal code of dimension s over \mathbb{F}_q having a nonzero root η , $\eta \in \mathbb{F}_{q^s}$ such that $\{1, \eta, \dots, \eta^{s-1}\}$ is a basis of \mathbb{F}_{q^s} over \mathbb{F}_q , then

(i) $C_\eta = \{\sum_{i=0}^{m-1} c_i(\eta)y^i \mid \sum_{i=0}^{m-1} \alpha_i c_i(x) \in C\}$ is an ideal of $\mathbb{F}_{q^s}[y]/\langle y^m - \eta \rangle$.

(ii) $\Pi(d_{\underline{\alpha}}(C)) = \text{Tr}(C) \square C_\eta$.

Proof: (i) Suppose that $u \in \mathbb{F}_{q^s}$, then $u = \sum_{t=0}^{s-1} u_t \eta^t$, $u_t \in \mathbb{F}_q$, for all $0 \leq t \leq s-1$. Let $c(x) = \sum_{i=0}^{m-1} \alpha_i c_i(x) \in C$, for some $c_i(x) \in \mathbb{F}_q[x]$, and $c_\eta(y) = \sum_{i=0}^{m-1} c_i(\eta)y^i$. Then $a(y) = uc_\eta(y) = u \sum_{i=0}^{m-1} c_i(\eta)y^i = \sum_{i=0}^{m-1} \sum_{t=0}^{s-1} u_t \eta^t c_i(\eta)y^i$. Now, define a map

$$\begin{aligned} f_\eta : C &\rightarrow \mathbb{F}_{q^s}[y]/\langle y^m - \eta \rangle \\ \sum_{i=0}^{m-1} \alpha_i c_i(x) &\mapsto \sum_{i=0}^{m-1} c_i(\eta)y^i. \end{aligned}$$

Since $u \in \mathbb{F}_{q^s}$ and $c_\eta(y) = \sum_{i=0}^{m-1} c_i(\eta)y^i$, then $a(y) \in \mathbb{F}_{q^s}[y]/\langle y^m - \eta \rangle$. Moreover, $f_\eta^{-1}a(y) = f_\eta^{-1}(\sum_{i=0}^{m-1} \sum_{t=0}^{s-1} u_t \eta^t c_i(\eta)y^i) = \sum_{i=0}^{m-1} \sum_{t=0}^{s-1} u_t x^t c_i(x) \alpha_i \in C$. Therefore, $uc_i(\eta)y^i \in C_\eta$.

From Lemma 7, $\alpha_0 z c_{m-1}(z) + \sum_{i=1}^{m-1} \alpha_i c_{i-1}(z) \in C$, which implies that $\alpha_0 \eta c_{m-1}(\eta) + \sum_{i=1}^{m-1} c_{i-1}(\eta)y^i \in C_\eta$. Thus, we have $\alpha_0 \eta c_{m-1}(\eta) + \sum_{i=1}^{m-1} c_{i-1}(\eta)y^i \equiv y \sum_{i=0}^{m-1} c_i(\eta)y^i = yc_\eta(x) \text{ mod}(y^m - \eta)$. Therefore C_η is an ideal of $\mathbb{F}_{q^s}[y]/\langle y^m - \eta \rangle$.

(ii) Clearly, $\text{Tr}(C) \square C_\eta = \{\sum_{i=0}^{m-1} \chi^{-1}(c_i(\eta))y^i \mid \sum_{i=0}^{m-1} c_i(\eta)y^i \in C_\eta\}$, i.e.,

$$\text{Tr}(C) \square C_\eta = \{\sum_{i=0}^{m-1} \chi^{-1}(c_i(\eta))y^i \mid \sum_{i=0}^{m-1} \alpha_i c_i(x) \in C\}.$$

Since, for all $0 \leq i \leq m-1$, $\chi^{-1}(c_i(\eta)) = \chi^{-1}(\chi c_i(x)) = c_i(x)$, then we have $\text{Tr}(C) \square C_\eta = \{\sum_{i=0}^{m-1} c_i(x)y^i \mid \sum_{i=0}^{m-1} \alpha_i c_i(x) \in C\}$. By the definitions of the maps Π and $d_{\underline{\alpha}}$, we have $\Pi(d_{\underline{\alpha}}(C)) = \text{Tr}(C) \square C_\eta$. □

Example 4: Let $\mathbb{F}_{25} = \mathbb{F}_5(\beta)$ be given in Example 2. Recall that $x^6 - 4 = \prod_{t=0}^5 (x - \beta^{1+2t}) = (x^2 + 3x + 4)(x^2 + 2x + 4)(x + 3)(x + 2)$. Let C be an $[6, 1]$ λ -constacyclic code with parity check polynomial $h(x) = (x - \beta^{-1})$ over \mathbb{F}_{25} , where $\lambda = 4 \in \mathbb{F}_5^*$. Clearly, by Example 2, we have that $d_{\underline{\alpha}}(C)$ is a 4-constacyclic code over \mathbb{F}_5 , for some basis $\underline{\alpha} = \{\alpha_0, \alpha_1\}$ of \mathbb{F}_{25} over \mathbb{F}_5 . Since the parity check polynomial of C is $h(x) = x - \beta^{-1}$, then its generator polynomial is $g(x) = (x - \beta^7)(x^2 + 2x + 4)(x + 3)(x + 2)$. Thus, by Corollary 1, we can get $\text{Tr}_5^{25}(C)$ is a minimal 4-constacyclic code of dimension 2 with generator polynomial $(x^2 + 2x + 4)(x + 3)(x + 2)$ over \mathbb{F}_5 . Further, β^7 is a nonzero root of $\text{Tr}_5^{25}(C)$. Therefore, $\Pi(d_{\underline{\alpha}}(C)) = \text{Tr}(C) \square C_{\beta^7}$, where $\underline{\alpha} = \{\rho^{20}, \rho^3\}$, $\beta^7 = \rho^{14} = 3\rho^{20}$ and $\{1, \rho^{14}\}$ is a basis of \mathbb{F}_{25} over \mathbb{F}_5 .

VI. CONCLUSION

In this paper, we studied some results on the images of a class of constacyclic codes over finite fields. We determined the connection between q^m -constacyclic codes and the images codes under some special mappings. Moreover, we have also shown that the images of these constacyclic codes can be put into the concatenated form. As some applications, constructing LCD codes and quantum codes from constacyclic codes may be interesting open problems in future.

REFERENCES

- [1] E. Berlekamp, *Algebraic Coding Theory*. New York, NY, USA: McGraw-Hill, 1968.
- [2] G. K. Bakshi and M. Raka, "A class of constacyclic codes over a finite field," *Finite Fields Appl.*, vol. 18, no. 2, pp. 362–377, Mar. 2012.
- [3] Y. Cao, "On constacyclic codes over finite chain rings," *Finite Fields Appl.*, vol. 24, pp. 124–135, Nov. 2013.
- [4] B. Chen, Y. Fan, L. Lin, and H. Liu, "Constacyclic codes over finite fields," *Finite Fields Appl.*, vol. 18, no. 6, pp. 1217–1231, Nov. 2012.
- [5] B. Chen, S. Ling, and G. Zhang, "Application of constacyclic codes to quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 3, pp. 1474–1484, Mar. 2015.
- [6] H. Dinh, "Constacyclic codes of length 2^s over Galois extension rings of $F_2 + uF_2$," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1730–1740, May 2009.

- [7] H. Dinh, "Constacyclic codes of length p^s over $F_{p^m} + uF_{p^m}$," *J. Algebra*, vol. 324, no. 5, pp. 940–950, Sep. 2010.
- [8] X. Kai, S. Zhu, and P. Li, "Constacyclic codes and some new quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2080–2086, Apr. 2014.
- [9] Y. Liu, R. Li, L. Lv, and Y. Ma, "A class of constacyclic BCH codes and new quantum codes," *Quantum Inf. Process.*, vol. 16, no. 3, p. 66, Mar. 2017, doi: 10.1007/s11128-017-1533-y.
- [10] C. Mouaha, "On cyclic q -ary images in concatenated form," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2618–2621, Jun. 2009.
- [11] M. Hanan and F. Palermo, "On cyclic codes for multi-phase data transmission systems," *SIAM J. Appl. Math.*, vol. 12, pp. 794–804, Dec. 1964.
- [12] F. MacWilliams, "On binary cyclic codes which are also cyclic codes over $GF(2^s)$," *SIAM J. Appl. Math.*, vol. 19, pp. 75–95, Jul. 1970.
- [13] M. Özen, F. Uzekmek, N. Aydin, and N. Özzaim, "Cyclic and some constacyclic codes over the ring $Z_4[u]/(u^2 - 1)$," *Finite Fields Appl.*, vol. 38, pp. 27–39, Mar. 2016.
- [14] G. Séguin, "The q -ary image of a q^m -ary cyclic code," *IEEE Trans. Inf. Theory*, vol. 41, no. 2, pp. 387–399, Mar. 1995.
- [15] A. Sharma and S. Rani, "On constacyclic codes over finite fields," *Cryptography Commun.*, vol. 8, no. 4, pp. 617–636, Oct. 2016.
- [16] W. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.
- [17] Y. Yang and W. Cai, "On self-dual constacyclic codes over finite fields," *Des., Codes Cryptogr.*, vol. 74, no. 2, pp. 355–364, Jul. 2015.
- [18] S. Zhu and X. Kai, "A class of constacyclic codes over Z_{p^m} ," *Finite Fields Appl.*, vol. 16, no. 4, pp. 243–254, Jul. 2010.



JUAN LI received the master's degree from the Shandong University of Technology, in 2018. She is currently pursuing the Ph.D. degree with the Chern Institute of Mathematics and LPMC, Nankai University. Her research interests include coding theory and cryptography.



JIAN GAO received the Ph.D. degree from the Chern Institute of Mathematics, Nankai University, in 2015. He is currently an Associate Professor with the School of Mathematics and Statistics, Shandong University of Technology. His research interests include coding theory and cryptography.



YONGKANG WANG received the master's degree from the Shandong University of Technology, in 2019. His research interests include coding theory and cryptography.

...