



Multi-dimensional constacyclic codes of arbitrary length over finite fields

Swati Bhardwaj · Madhu Raka

Received: 7 March 2023 / Accepted: 19 June 2023 / Published online: 1 July 2023
© The Indian National Science Academy 2023

Abstract Multi-dimensional cyclic code is a natural generalization of cyclic code. In an earlier paper we explored two-dimensional constacyclic codes over finite fields. Following the same technique, here we characterize the algebraic structure of multi-dimensional constacyclic codes, in particular three-dimensional (α, β, γ) -constacyclic codes of arbitrary length $s\ell k$ and their duals over a finite field $\mathbb{F}_q$, where α, β, γ are non zero elements of $\mathbb{F}_q$. We give necessary and sufficient conditions for a three-dimensional (α, β, γ) -constacyclic code to be self-dual.

Keywords Cyclic codes · Self-dual · Central primitive idempotents

Mathematics Subject Classification 94B15 · 94B05 · 11T71

1 Introduction

A multi-dimensional cyclic code or more precisely an n -D cyclic code of length $s_1 s_2 \cdots s_n$ over $\mathbb{F}_q$ is an ideal in the polynomial ring $\mathbb{F}_q[x_1, x_2, \dots, x_n]/\langle x_1^{s_1} - 1, x_2^{s_2} - 1, \dots, x_n^{s_n} - 1 \rangle$. Because of their rich mathematical structure, involving Algebraic Geometry or ideals in a polynomial quotient ring, multi-dimensional cyclic codes are of great importance. Two-dimensional (2-D) cyclic codes are used in daily technical applications such as video encoding. The characterization for 2-D cyclic codes, for the first time was presented by Ikai et al. [9] in 1975. Since the method was pure, it did not help decode these codes. After that Imai [10] introduced basic theories for binary 2-D cyclic codes using the concept of ‘common zero’.

One of the main concerns about n -D cyclic codes is to find the related generator polynomials. In 2016, Sepasdar and Khashyarmansh [15] obtained generator polynomials of two-dimensional cyclic codes of length $s \cdot 2^k$ ($s_1 = s, s_2 = 2^k$) over $\mathbb{F}_{p^m}$ iteratively, where p is an odd prime. The authors state in the concluding remarks of their paper [15] that their method does not work for arbitrary 2-D cyclic codes, not even when $s_1 = 3, s_2 = 3$. In 2017, Sepasdar [16](unpublished) gave a method for obtaining generator matrix of 2-D cyclic codes of arbitrary length $s_1 s_2$, but this method is not very practical.

Constacyclic codes over finite fields have a very significant role in the theory of error-correcting codes. A lot of work on constacyclic codes has been done in recent years, see for example [2, 4, 6, 14]. Given nonzero elements α and β of $\mathbb{F}_q$, a two-dimensional (α, β) -constacyclic code of length $s\ell$ is an ideal of the polynomial

Communicated by Bakshi Gurmeet Kaur.

S. Bhardwaj · M. Raka (✉)
Centre for Advanced Study in Mathematics, Panjab University, Chandigarh 160014, India
E-mail: mraka@pu.ac.in

S. Bhardwaj
E-mail: swatibhardwaj2296@gmail.com

ring $\mathbb{F}_q[x, y]/\langle x^s - \alpha, y^\ell - \beta \rangle$. In 2018, Rajabi and Khashyarmansh [13] investigated some repeated-root two-dimensional (α, β) -constacyclic codes of length $2p^s \cdot 2^k$ over $\mathbb{F}_{p^m}$, where p is an odd prime, using the structure of 2-D cyclic codes given in [15].

The authors [3] gave a novel method to characterize the algebraic structure of 2-D (α, β) -constacyclic codes of arbitrary length $s\ell$ and their duals over a finite field $\mathbb{F}_q$, using central primitive idempotents of the ring $\mathbb{F}_q[y]/\langle y^\ell - \beta \rangle$. This method is quite different from that of [13, 15, 16] and it does not require s to be a multiple of p , the characteristic of $\mathbb{F}_q$ as in [13].

There are much less results about general n -D cyclic codes. Güneri et al. [7] obtained a trace representation for multidimensional cyclic codes via Delsarte's theorem. This relates the weights of the codewords to the number of affine rational points of Artin Schreier type hypersurfaces over finite fields. In 2018, Lalasoa et al. [11] generalized the method of Sepasdar [16] and constructed a basis of a 3-D cyclic code. Andriamifidisoa et al. [1] and Lalasoa et al. [11], [12] applied the method of Sepasdar [16] to construct a basis of a 3-D cyclic code of arbitrary length. As is for 2-D codes, this construction is not practical.

Generalizing our method of [3], in this paper, we study multi-dimensional constacyclic codes and their duals. Due to the ease in visualization of the idea, we give the construction of generator polynomials of 3-D constacyclic codes and their duals. Generator matrices of a general n -D constacyclic code can be computed in a similar way. A 3-D (α, β, γ) -constacyclic code $\mathcal{C}$ of length $s\ell k$ is an ideal of the ring $\mathbb{F}_q[x, y, z]/\langle x^s - \alpha, y^\ell - \beta, z^k - \gamma \rangle$. In Section 2.1, we study primitive central idempotents of the rings $\mathbb{F}_q[z]/\langle z^k - \gamma \rangle$ and $\mathbb{F}_q[y]/\langle y^\ell - \beta \rangle$ and discuss some of their properties. Generator polynomials and generator matrices of 3-D (α, β, γ) -constacyclic code $\mathcal{C}$ and its dual are obtained in Sections 2.2 and 2.3 respectively. In Section 2.4, we give necessary and sufficient conditions for a 3-D constacyclic code to be self-dual for $\alpha, \beta, \gamma \in \{1, -1\}$.

2 Three dimensional (α, β, γ) -constacyclic codes of length $s\ell k$

Firstly we recall the definition of a λ -quasi-twisted code over $\mathbb{F}_q$.

Definition 1 Let

$$\begin{aligned} a &= (a_{0,0}, a_{1,0}, \dots, a_{m-1,0} | a_{0,1}, \dots, a_{m-1,1} | \dots | a_{0,n-1}, \dots, a_{m-1,n-1}) \\ &= (a^{(0)} | a^{(1)} | \dots | a^{(n-1)}) \end{aligned}$$

where $a^{(i)} = (a_{0,i}, a_{1,i}, \dots, a_{m-1,i})$, be a vector in $\mathbb{F}_q^{mn}$ divided into n equal parts each of length m . A linear code C of length mn over $\mathbb{F}_q$ is called a λ -quasi-twisted code of index n if $\tau_\lambda(a) = (\lambda a^{(n-1)} | a^{(0)} | \dots | a^{(n-2)}) \in C$ whenever $a \in C$. When $\lambda = 1$, C is called quasi-cyclic code of index n .

Throughout the paper $\mathcal{R}$ denotes the polynomial ring $\mathbb{F}_q[x, y, z]/\langle x^s - \alpha, y^\ell - \beta, z^k - \gamma \rangle$. Let $\mathcal{C}$ be a three dimensional (α, β, γ) -constacyclic code over $\mathbb{F}_q$, i.e. $\mathcal{C}$ is an ideal of the ring $\mathcal{R}$. Each codeword c in $\mathcal{C}$ has a unique polynomial representation

$$c(x, y, z) = \sum_{i=0}^{s-1} \sum_{j=0}^{\ell-1} \sum_{t=0}^{k-1} c_{i,j,t} x^i y^j z^t. \quad (1)$$

For fixed $j, t, 0 \leq j \leq \ell - 1, 0 \leq t \leq k - 1$, let

$$c_x^{(y^j, z^t)} = (c_{0,j,t}, c_{1,j,t}, \dots, c_{s-1,j,t})$$

denote the s -tuple whose co-ordinates are coefficients of $x^i y^j z^t, 0 \leq i \leq s - 1$ in $c(x, y, z)$ given by (1). The subscript x in $c_x^{(y^j, z^t)}$ denotes that in this tuple the power i of x^i is varying. Define,

$$c^{(z^t)} = (c_x^{(y^0, z^t)} | c_x^{(y^1, z^t)} | \dots | c_x^{(y^{\ell-1}, z^t)})$$

then, $c^{(z^t)}$ is a $s\ell$ -tuple whose co-ordinates are all the coefficients of z^t in $c(x, y, z)$.

Similarly, define $c_y^{(x^i, z^t)} = (c_{i,0,t}, c_{i,1,t}, \dots, c_{i,\ell-1,t}), c_z^{(x^i, y^j)} = (c_{i,j,0}, c_{i,j,1}, \dots, c_{i,j,k-1}),$

$$c^{(x^i)} = (c_y^{(x^i, z^0)} | c_y^{(x^i, z^1)} | \dots | c_y^{(x^i, z^{k-1})}) \text{ and } c^{(y^j)} = (c_z^{(x^0, y^j)} | c_z^{(x^1, y^j)} | \dots | c_z^{(x^{s-1}, y^j)}).$$



The co-ordinates of the ℓk -tuple $c^{(x^i)}$ and the co-ordinates of sk -tuple $c^{(y^j)}$ are the coefficients of x^i and y^j respectively in $c(x, y, z)$.

For a 3-D constacyclic code $\mathcal{C}$, let

$$\mathcal{C}_1 = \left\{ (c^{(x^0)} | c^{(x^1)} | \dots | c^{(x^{s-1})}) : c(x, y, z) \in \mathcal{C} \right\}, \quad (2)$$

$$\mathcal{C}_2 = \left\{ (c^{(y^0)} | c^{(y^1)} | \dots | c^{(y^{\ell-1})}) : c(x, y, z) \in \mathcal{C} \right\}, \quad (3)$$

$$\mathcal{C}_3 = \left\{ (c^{(z^0)} | c^{(z^1)} | \dots | c^{(z^{k-1})}) : c(x, y, z) \in \mathcal{C} \right\}. \quad (4)$$

Clearly $\mathcal{C}_1, \mathcal{C}_2$ and $\mathcal{C}_3$ are linear codes in $\mathbb{F}_q^{s\ell k}$ and are permutation equivalent.

Note that $xc(x, y, z)$ corresponds to the codeword $(\alpha c^{(x^{s-1})} | c^{(x^0)} | c^{(x^1)} | \dots | c^{(x^{s-2})})$, $yc(x, y, z)$ corresponds to the codeword $(\beta c^{(y^{\ell-1})} | c^{(y^0)} | c^{(y^1)} | \dots | c^{(y^{\ell-2})})$ and $zc(x, y, z)$ corresponds to the codeword $(\gamma c^{(z^{k-1})} | c^{(z^0)} | c^{(z^1)} | \dots | c^{(z^{k-2})})$.

By definitions of a 3-D code and of a λ -quasi-twisted code we immediately have

Proposition 1 $\mathcal{C}$ is a 3-D (α, β, γ) -constacyclic code if and only if $\mathcal{C}_1$ is an α -quasi-twisted code of index s , $\mathcal{C}_2$ is a β -quasi-twisted code of index ℓ and $\mathcal{C}_3$ is a γ -quasi-twisted code of index k .

Rajabi and Khashyarmansh [13] showed that the dual of a two-dimensional (α, β) -constacyclic code is a two-dimensional $(\alpha^{-1}, \beta^{-1})$ -constacyclic code. A similar result holds for a 3-dimensional (α, β, γ) -constacyclic code.

Proposition 2 The dual of a three-dimensional (α, β, γ) -constacyclic code is a three-dimensional $(\alpha^{-1}, \beta^{-1}, \gamma^{-1})$ -constacyclic code.

Proof Let $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ be the corresponding linear codes in $\mathbb{F}_q^{s\ell k}$ as defined in (2), (3), and (4) respectively. Let $\mathcal{C}_1^\perp, \mathcal{C}_2^\perp, \mathcal{C}_3^\perp$ be the duals of $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ in $\mathbb{F}_q^{s\ell k}$.

To prove that $\mathcal{C}^\perp$ is 3-dimensional $(\alpha^{-1}, \beta^{-1}, \gamma^{-1})$ -constacyclic code, it is enough to prove that $\mathcal{C}_1^\perp$ is α^{-1} -quasi twisted code, $\mathcal{C}_2^\perp$ is β^{-1} -quasi twisted code and $\mathcal{C}_3^\perp$ is γ^{-1} -quasi twisted code.

Let $a = (a^{(x^0)} | a^{(x^1)} | \dots | a^{(x^{s-1})}) \in \mathcal{C}_1^\perp$, where $a(x, y, z) \in \mathcal{C}^\perp$ and $b = (b^{(x^0)} | b^{(x^1)} | \dots | b^{(x^{s-1})})$ be an arbitrary element of $\mathcal{C}_1$. Then

$$\tau_\alpha^{s-1}(b) = (\alpha b^{(x^1)} | \alpha b^{(x^2)} | \dots | \alpha b^{(x^{s-1})} | b^{(x^0)}).$$

As $\mathcal{C}_1$ is α -quasi twisted code, $\tau_\alpha^{s-1}(b) \in \mathcal{C}_1$. Therefore, by definition of duality $a \cdot \tau_\alpha^{s-1}(b) = 0$. This gives

$$\begin{aligned} & a^{(x^0)} \cdot \alpha b^{(x^1)} + a^{(x^1)} \cdot \alpha b^{(x^2)} + \dots + a^{(x^{s-2})} \cdot \alpha b^{(x^{s-1})} + a^{(x^{s-1})} \cdot b^{(x^0)} = 0 \\ \Rightarrow & \alpha^{-1} a^{(x^{s-1})} \cdot b^{(x^0)} + a^{(x^0)} \cdot b^{(x^1)} + \dots + a^{(x^{s-2})} \cdot b^{(x^{s-1})} = 0 \\ \text{i. e. } & (\alpha^{-1} a^{(x^{s-1})} | a^{(x^0)} | \dots | a^{(x^{s-2})}) \cdot (b^{(x^0)} | b^{(x^1)} | \dots | b^{(x^{s-1})}) = 0 \\ \text{i. e. } & \tau_{\alpha^{-1}}(a) \cdot b = 0 \text{ for all } b \in \mathcal{C}_1. \end{aligned}$$

This gives $\tau_{\alpha^{-1}}(a) \in \mathcal{C}_1^\perp$ whenever $a \in \mathcal{C}_1^\perp$. Therefore, $\mathcal{C}_1^\perp$ is α^{-1} -quasi twisted code. Similarly, one gets that $\mathcal{C}_2^\perp$ is β^{-1} -quasi twisted code and $\mathcal{C}_3^\perp$ is γ^{-1} -quasi twisted code. $\square$

Definition 2 Let

$$\begin{aligned} c &= (c^{(z^0)} | c^{(z^1)} | \dots | c^{(z^{k-1})}) \\ &= (c_x^{(y^0 z^0)} | c_x^{(y^1 z^0)} | \dots | c_x^{(y^{\ell-1} z^0)} | \dots | c_x^{(y^0 z^{k-1})} | c_x^{(y^1 z^{k-1})} | \dots | c_x^{(y^{\ell-1} z^{k-1})}) \\ &= (c_{0,0,0}, c_{1,0,0}, \dots, c_{s-1,0,0} | c_{0,1,0}, c_{1,1,0}, \dots, c_{s-1,1,0} | \dots | c_{0,\ell-1,0}, c_{1,\ell-1,0}, \dots, c_{s-1,\ell-1,0} | \\ &\quad \dots | c_{0,0,k-1}, c_{1,0,k-1}, \dots, c_{s-1,0,k-1} | c_{0,1,k-1}, c_{1,1,k-1}, \dots, c_{s-1,1,k-1} | \\ &\quad \dots | c_{0,\ell-1,k-1}, c_{1,\ell-1,k-1}, \dots, c_{s-1,\ell-1,k-1}) \in \mathcal{C}. \end{aligned}$$



For $\alpha, \beta, \gamma \in \mathbb{F}_q^*$, define

$$\begin{aligned}\tau_{\alpha,\beta,\gamma}^{1,0,0}(c) &= (\alpha c_{s-1,0,0}, c_{0,0,0}, \dots, c_{s-2,0,0} \mid \dots \mid \alpha c_{s-1,\ell-1,0}, c_{0,\ell-1,0}, \dots, c_{s-2,\ell-1,0} \mid \\ &\quad \dots \mid \alpha c_{s-1,0,k-1}, c_{0,0,k-1}, \dots, c_{s-2,0,k-1} \mid \dots \\ &\quad \mid \alpha c_{s-1,\ell-1,k-1}, c_{0,\ell-1,k-1}, \dots, c_{s-2,\ell-1,k-1}) \\ \tau_{\alpha,\beta,\gamma}^{0,1,0}(c) &= (\beta c_x^{(y^{\ell-1}z^0)} \mid c_x^{(y^0z^0)} \mid \dots \mid c_x^{(y^{\ell-2}z^0)} \mid \dots \mid \beta c_x^{(y^{\ell-1}z^{k-1})} \mid c_x^{(y^0z^{k-1})} \mid \dots \mid c_x^{(y^{\ell-2}z^{k-1})}) \\ \tau_{\alpha,\beta,\gamma}^{0,0,1}(c) &= (\gamma c^{(z^{k-1})} \mid c^{(z^0)} \mid \dots \mid c^{(z^{k-2})}).\end{aligned}$$

Proposition 3 Let $f(x, y, z), g(x, y, z) \in \mathcal{R}$ and let codewords corresponding to $f(x, y, z)$ and $g(x, y, z)$ be

$$\begin{aligned}\underline{a} &= (a^{(z^0)} \mid a^{(z^1)} \mid \dots \mid a^{(z^{k-1})}) \\ &= (a_x^{(y^0z^0)} \mid a_x^{(y^1z^0)} \mid \dots \mid a_x^{(y^{\ell-1}z^0)} \mid \dots \mid a_x^{(y^0z^{k-1})} \mid a_x^{(y^1z^{k-1})} \mid \dots \mid a_x^{(y^{\ell-1}z^{k-1})})\end{aligned}$$

and

$$\begin{aligned}\underline{b} &= (b^{(z^0)} \mid b^{(z^1)} \mid \dots \mid b^{(z^{k-1})}) \\ &= (b_x^{(y^0z^0)} \mid b_x^{(y^1z^0)} \mid \dots \mid b_x^{(y^{\ell-1}z^0)} \mid \dots \mid b_x^{(y^0z^{k-1})} \mid b_x^{(y^1z^{k-1})} \mid \dots \mid b_x^{(y^{\ell-1}z^{k-1})})\end{aligned}$$

respectively. Then, $f(x, y, z)g(x, y, z) = 0$ in $\mathcal{R}$ if and only if $\underline{a}$ is orthogonal to $\underline{b}^* = (b_x^{*(y^{\ell-1}z^{k-1})} \mid \dots \mid b_x^{*(y^0z^{k-1})} \mid \dots \mid b_x^{*(y^1z^0)} \mid b_x^{*(y^0z^0)})$ and all its $(\alpha^{-1}, \beta^{-1}, \gamma^{-1})$ -constacyclic shifts, where $b_x^{*(y^jz^t)} = (b_{s-1,j,t}, b_{s-2,j,t}, \dots, b_{0,j,t})$.

Proof For convenience, we give a proof for $s = \ell = k = 2$. Also we skip commas in subscripts of $c_{i,j,t}$. For, $c = (c^{(z^0)} \mid c^{(z^1)}) = (c_x^{(y^0z^0)} \mid c_x^{(y^1z^0)} \mid c_x^{(y^0z^1)} \mid c_x^{(y^1z^1)}) = (c_{000}, c_{100} \mid c_{010}, c_{110} \mid c_{001}, c_{101} \mid c_{011}, c_{111})$ we have

$$\begin{aligned}\tau_{\alpha^{-1}\beta^{-1}\gamma^{-1}}^{001}(c) &= (\gamma^{-1}c^{(z^1)} \mid c^{(z^0)}) \\ &= (\gamma^{-1}c_{001}, \gamma^{-1}c_{101} \mid \gamma^{-1}c_{011}, \gamma^{-1}c_{111} \mid c_{000}, c_{100} \mid c_{010}, c_{110}), \\ \tau_{\alpha^{-1}\beta^{-1}\gamma^{-1}}^{010}(c) &= (\beta^{-1}c_{010}, \beta^{-1}c_{110} \mid c_{000}, c_{100} \mid \beta^{-1}c_{011}, \beta^{-1}c_{111} \mid c_{001}, c_{101}), \\ \tau_{\alpha^{-1}\beta^{-1}\gamma^{-1}}^{100}(c) &= (\alpha^{-1}c_{100}, c_{000} \mid \alpha^{-1}c_{110}, c_{010} \mid \alpha^{-1}c_{101}, c_{001} \mid \alpha^{-1}c_{111}, c_{011}).\end{aligned}$$

Let

$$\begin{aligned}h(x, y, z) &= f(x, y, z)g(x, y, z) \\ &= (a_{000}x^0y^0z^0 + a_{100}x^1y^0z^0 + a_{010}x^0y^1z^0 + a_{110}x^1y^1z^0 + a_{001}x^0y^0z^1 \\ &\quad + a_{101}x^1y^0z^1 + a_{011}x^0y^1z^1 + a_{111}x^1y^1z^1) \\ &\quad (b_{000}x^0y^0z^0 + b_{100}x^1y^0z^0 + b_{010}x^0y^1z^0 + b_{110}x^1y^1z^0 + b_{001}x^0y^0z^1 \\ &\quad + b_{101}x^1y^0z^1 + b_{011}x^0y^1z^1 + b_{111}x^1y^1z^1).\end{aligned}$$

Then for $k_1, k_2, k_3 \in \{0, 1\} \pmod{2}$, coefficient of $x^{k_1}y^{k_2}z^{k_3}$ is

$$\begin{aligned}h_{k_1k_2k_3} &= \sum_{\substack{i+i'=k_1 \\ j+j'=k_2 \\ t+t'=k_3}} a_{ij t} b_{i'j't'} + \sum_{\substack{i+i'=s+k_1 \\ j+j'=k_2 \\ t+t'=k_3}} \alpha a_{ij t} b_{i'j't'} + \sum_{\substack{i+i'=k_1 \\ j+j'=\ell+k_2 \\ t+t'=k_3}} \beta a_{ij t} b_{i'j't'} \\ &\quad + \sum_{\substack{i+i'=k_1 \\ j+j'=k_2 \\ t+t'=k+k_3}} \gamma a_{ij t} b_{i'j't'} + \sum_{\substack{i+i'=s+k_1 \\ j+j'=\ell+k_2 \\ t+t'=k_3}} \alpha \beta a_{ij t} b_{i'j't'} + \sum_{\substack{i+i'=s+k_1 \\ j+j'=\ell+k_2 \\ t+t'=k+k_3}} \alpha \gamma a_{ij t} b_{i'j't'} \\ &\quad + \sum_{\substack{i+i'=k_1 \\ j+j'=\ell+k_2 \\ t+t'=k+k_3}} \beta \gamma a_{ij t} b_{i'j't'} + \sum_{\substack{i+i'=s+k_1 \\ j+j'=\ell+k_2 \\ t+t'=k+k_3}} \alpha \beta \gamma a_{ij t} b_{i'j't'}.\end{aligned}$$



For $k_1, k_2, k_3 \in \{0, 1\} \pmod{2}$, one finds that

$$h_{k_1 k_2 k_3} = \alpha^{k_1+1} \beta^{k_2+1} \gamma^{k_3+1} \underline{a} \cdot \tau_{\alpha^{-1} \beta^{-1} \gamma^{-1}}^{k_1+1, k_2+1, k_3+1} (b_{111}, b_{011}, b_{101}, b_{001}, b_{110}, b_{010}, b_{100}, b_{000}).$$

Therefore, $h_{k_1 k_2 k_3} = 0$ if and only if

$$\underline{a} \cdot \tau_{\alpha^{-1} \beta^{-1} \gamma^{-1}}^{k_1+1, k_2+1, k_3+1} (\underline{b}^*) = 0,$$

if and only if $\underline{a}$ is orthogonal to $\underline{b}^*$ and all its $(\alpha^{-1}, \beta^{-1}, \gamma^{-1})$ -constacyclic shifts. $\square$

For a non-empty subset S of a commutative ring R , the annihilator of S is the set $\text{ann}(S) = \{f \in R : fg = 0 \text{ for all } g \in S\}$. Then $\text{ann}(S)$ is an ideal of R . For a polynomial $f(x)$ with $\deg(f(x)) = k$, its reciprocal is defined as $f^*(x) = x^k f(1/x)$. For any set S of polynomials, we use the notation $S^* = \{f^* : f \in S\}$. The above proposition immediately gives the following result.

Proposition 4 Suppose that $\alpha, \beta, \gamma \in \{1, -1\}$. Let C be a three-dimensional (α, β, γ) -constacyclic code, then the dual code $C^\perp$ is $(\text{ann}(C))^*$, also denoted as $\text{ann}^*(C)$.

2.1 Primitive central idempotents and their properties

In this section we study primitive central idempotents of the rings $\mathbb{F}_q[z]/\langle z^k - \gamma \rangle$ and $\mathbb{F}_q[y]/\langle y^\ell - \beta \rangle$ and discuss some of their properties.

Let r be the order of γ in $\mathbb{F}_q$ so that $\gamma^r = 1$ and $r|(q-1)$. Let ω be a rk^{th} root of unity such that $\omega^k = \gamma$. Assume that $q \equiv 1 \pmod{rk}$ so that $\omega \in \mathbb{F}_q$, since for some integer k' , $\omega^{q-1} = \omega^{rk k'} = \gamma^{rk k'} = 1$. Then,

$$z^{rk} - 1 = (z-1)(z-\omega)(z-\omega^2) \cdots (z-\omega^{rk-1}).$$

For $0 \leq t \leq rk-1$, define

$$\xi_t(z) = \frac{(z-1)(z-\omega) \cdots (z-\omega^{t-1})(z-\omega^{t+1}) \cdots (z-\omega^{rk-1})}{(\omega^t-1)(\omega^t-\omega) \cdots (\omega^t-\omega^{t-1})(\omega^t-\omega^{t+1}) \cdots (\omega^t-\omega^{rk-1})}. \quad (5)$$

Then $\xi_0(z), \xi_1(z), \dots, \xi_{rk-1}(z)$ are primitive central idempotents in $\mathbb{F}_q[z]/\langle z^{rk} - 1 \rangle$, i.e. $\xi_0(z) + \xi_1(z) + \cdots + \xi_{rk-1}(z) = 1$ and $\xi_t(z)\xi_{t'}(z) = \delta_{t,t'}\xi_t(z)$ for $t, t' \in \{0, 1, 2, \dots, rk-1\}$, where $\delta_{t,t'}$ is the Kronecker delta function. For a proof of it see [5]. Also, $\xi_t(\omega^t) = 1$ and $\xi_t(\omega^{t'}) = 0$ for $t \neq t'$. The following Lemmas 1-5 are similar to [3], therefore proofs are skipped.

Lemma 1 For $t = 0, 1, 2, \dots, rk-1$, we have

$$\xi_t(z) = \frac{1}{rk} \left(1 + \omega^{rk-t}z + (\omega^{rk-t}z)^2 + \cdots + (\omega^{rk-t}z)^{rk-1} \right).$$

Lemma 2 $\xi_{1+tr}(z)z^{t'} = (\omega^{1+tr})^{t'} \xi_{1+tr}(z)$, for $t, t' \in \{0, 1, 2, \dots, k-1\}$.

Following the notations of [6], let $P_{k,\gamma} = 1 + r\mathbb{Z}_{kr} = \{1 + rt : t = 0, 1, \dots, k-1\}$. Then $\omega^i, i \in P_{k,\gamma}$ are all the roots of $z^k - \gamma$, i.e.

$$z^k - \gamma = (z-\omega)(z-\omega^{1+r})(z-\omega^{1+2r}) \cdots (z-\omega^{1+(k-1)r}). \quad (6)$$

Let $z^{rk} - 1 = (z^k - \gamma)Q(z)$, where $Q(z) = \prod_{i \notin P_{k,\gamma}} (z - \omega^i)$. For $0 \leq t \leq k-1$, define

$$\zeta_t(z) = \frac{(z-\omega) \cdots (z-\omega^{1+(t-1)r})(z-\omega^{1+(t+1)r}) \cdots (z-\omega^{1+(k-1)r})}{(\omega^{1+tr}-\omega) \cdots (\omega^{1+tr}-\omega^{1+(t-1)r})(\omega^{1+tr}-\omega^{1+(t+1)r}) \cdots (\omega^{1+tr}-\omega^{1+(k-1)r})}. \quad (7)$$

Then $\zeta_0(z), \zeta_1(z), \dots, \zeta_{k-1}(z)$ are primitive central idempotents in $\mathbb{F}_q[z]/\langle z^k - \gamma \rangle$.

Note that

$$\text{If } r = 1, \zeta_t(z) = \xi_{t+1}(z) \text{ and } \zeta_{k-1}(z) = \xi_0(z) \text{ and} \quad (8)$$

$$\zeta_t(\omega^{1+tr}) = 1 \text{ and } \zeta_t(\omega^{1+t'r}) = 0 \text{ for } t \neq t'. \quad (9)$$



Lemma 3 For $t = 0, 1, 2, \dots, k-1$ we have $\xi_{1+tr}(z) = \zeta_t(z) \left(\frac{Q(z)}{c_t} \right)$ for some constant c_t in $\mathbb{F}_q^*$.

Lemma 4 $\zeta_t(z)z^{t'} = (\omega^{1+tr})^{t'} \zeta_t(z)$ for $t, t' \in \{0, 1, 2, \dots, k-1\}$.

Lemma 5 The reciprocal polynomials of $\zeta_t(z)$, for $t = 0, 1, \dots, k-1$, are given by

$$\zeta_t^*(z) = \begin{cases} b_t \zeta_{k-2-t}(z) & \text{if } \gamma = 1 \\ b_t \zeta_{k-1-t}(z) & \text{if } \gamma = -1 \end{cases} \quad (10)$$

for some constant $b_t \in \mathbb{F}_q^*$ with the understanding that for $\gamma = 1$ and $t = k-1$, $\zeta_{k-2-t}(z) = \zeta_{-1}(z) = \xi_0(z) = \zeta_{k-1}(z)$.

Similarly, let r' be the order of β in $\mathbb{F}_q$ so that $\beta^{r'} = 1$ and $r' \mid (q-1)$. Let θ be the $r'\ell^{th}$ root of unity such that $\theta^\ell = \beta$. Assume that $q \equiv 1 \pmod{r'\ell}$ so that $\theta \in \mathbb{F}_q$. We define $\chi_j(y)$, the primitive central idempotents in $\mathbb{F}_q[y]/\langle y^{r'\ell} - 1 \rangle$ similar to $\xi_t(z)$ as defined in (5) and then define, as in (7), primitive central idempotents $\eta_j(y)$, $0 \leq j \leq \ell-1$, in $\mathbb{F}_q[y]/\langle y^\ell - \beta \rangle$ given by

$$\eta_j(y) = \frac{(y - \theta)(y - \theta^{1+r'}) \dots (y - \theta^{1+(j-1)r'})(y - \theta^{1+(j+1)r'}) \dots (y - \theta^{1+(\ell-1)r'})}{(\theta^{1+jr'} - \theta) \dots (\theta^{1+jr'} - \theta^{1+(j-1)r'}) (\theta^{1+jr'} - \theta^{1+(j+1)r'}) \dots (\theta^{1+jr'} - \theta^{1+(\ell-1)r'})}.$$

We have similar results for $\chi_j(y)$ and $\eta_j(y)$ as obtained in Lemmas 1, 2, $\dots$, 5. In particular

Lemma 6 The reciprocal polynomials of $\eta_j(y)$, for $j = 0, 1, \dots, \ell-1$, are given by

$$\eta_j^*(y) = \begin{cases} c_j \eta_{\ell-2-j}(y) & \text{if } \beta = 1 \\ c_j \eta_{\ell-1-j}(y) & \text{if } \beta = -1 \end{cases} \quad (11)$$

for some constant $c_j \in \mathbb{F}_q^*$ with the understanding that for $\beta = 1$ and $j = \ell-1$, $\eta_{\ell-2-j}(y) = \eta_{-1}(y) = \chi_0(y) = \eta_{\ell-1}(y)$.

Similar to (9), we have

$$\eta_j(\theta^{1+jr'}) = 1 \text{ and } \eta_j(\theta^{1+j'r'}) = 0 \text{ for } j \neq j'. \quad (12)$$

2.2 Generator matrix

In this section we obtain generators of a three-dimensional (α, β, γ) -constacyclic code of arbitrary length $s\ell k$. Let $\mathcal{C}$ be a three dimensional (α, β, γ) -constacyclic code, i.e. $\mathcal{C}$ is an ideal of the ring $\mathcal{R} = \mathbb{F}_q[x, y, z]/\langle x^s - \alpha, y^\ell - \beta, z^k - \gamma \rangle$. Define, for $0 \leq t \leq k-1$,

$$I_t = \{f(x, y) \in \mathbb{F}_q[x, y]/\langle x^s - \alpha, y^\ell - \beta \rangle : \zeta_t(z)f(x, y) \in \mathcal{C}\} \quad (13)$$

Then I_t , $0 \leq t \leq k-1$, are ideals in the ring $\mathbb{F}_q[x, y]/\langle x^s - \alpha, y^\ell - \beta \rangle$, i.e. I_t are two dimensional (α, β) -constacyclic codes.

For each t , $0 \leq t \leq k-1$, there exist polynomials $p_j^{(t)}(x)$, $0 \leq j \leq \ell-1$, such that $p_j^{(t)}(x)|x^s - \alpha$ and the ideals I_t are generated by (see Theorem 1 of [3])

$$I_t = \langle \eta_0(y)p_0^{(t)}(x), \eta_1(y)p_1^{(t)}(x), \dots, \eta_{\ell-1}(y)p_{\ell-1}^{(t)}(x) \rangle, \quad (14)$$

where $\eta_0(y), \eta_1(y), \dots, \eta_{\ell-1}(y)$ are primitive central idempotents in $\mathbb{F}_q[y]/\langle y^\ell - \beta \rangle$.

Theorem 1 Let $\mathcal{C}$ be an ideal in the ring $\mathcal{R} = \mathbb{F}_q[x, y, z]/\langle x^s - \alpha, y^\ell - \beta, z^k - \gamma \rangle$, then

$$\mathcal{C} = \langle p_j^{(t)}(x)\eta_j(y)\zeta_t(z) : 0 \leq t \leq k-1, 0 \leq j \leq \ell-1 \rangle; \quad (15)$$

and a generator matrix of $\mathcal{C}$ is given by



$$G = \begin{pmatrix} p_0^{(0)}(x)\eta_0(y)\zeta_0(z) \\ xp_0^{(0)}(x)\eta_0(y)\zeta_0(z) \\ \vdots \\ x^{s-a_{0,0}-1}p_0^{(0)}(x)\eta_0(y)\zeta_0(z) \\ \vdots \\ p_{\ell-1}^{(0)}(x)\eta_{\ell-1}(y)\zeta_0(z) \\ xp_{\ell-1}^{(0)}(x)\eta_{\ell-1}(y)\zeta_0(z) \\ \vdots \\ x^{s-a_{0,\ell-1}-1}p_{\ell-1}^{(0)}(x)\eta_{\ell-1}(y)\zeta_0(z) \\ \vdots \\ \vdots \\ p_{\ell-1}^{(k-1)}(x)\eta_{\ell-1}(y)\zeta_{k-1}(z) \\ xp_{\ell-1}^{(k-1)}(x)\eta_{\ell-1}(y)\zeta_{k-1}(z) \\ \vdots \\ x^{s-a_{k-1,\ell-1}-1}p_{\ell-1}^{(k-1)}(x)\eta_{\ell-1}(y)\zeta_{k-1}(z) \end{pmatrix},$$

where $a_{t,j} = \deg p_j^{(t)}(x)$ for $t = 0, 1, \dots, k-1$ and $j = 0, 1, \dots, \ell-1$.

Proof Let the ideal on the right hand side of equation (15) be denoted as $\mathcal{D}$. Let $g(x, y, z)$ be an arbitrary element of $\mathcal{C}$. Then there exist polynomials $g_t(x, y) \in \mathbb{F}_q[x, y]/\langle x^s - \alpha, y^\ell - \beta \rangle$ for $t = 0, 1, \dots, k-1$ such that

$$g(x, y, z) = g_0(x, y) + g_1(x, y)z + \dots + g_{k-1}(x, y)z^{k-1}.$$

Using Lemma 4, we have

$$\begin{aligned} g(x, y, z)\zeta_t(z) &= g_0(x, y)\zeta_t(z) + g_1(x, y)\omega^{1+tr}\zeta_t(z) + \dots + g_{k-1}(x, y)(\omega^{1+tr})^{k-1}\zeta_t(z) \\ &= \zeta_t(z)\{g_0(x, y) + g_1(x, y)\omega^{1+tr} + \dots + g_{k-1}(x, y)(\omega^{1+tr})^{k-1}\} \\ &= \zeta_t(z)g(x, y, \omega^{1+tr}). \end{aligned} \quad (16)$$

Now, $g(x, y, z) \in \mathcal{C}$ implies $g(x, y, z)\zeta_t(z) \in \mathcal{C}$ and hence by definition (13) of I_t , $g(x, y, \omega^{1+tr}) \in I_t$. Further from (14), there exist some polynomials $h_j(x, y) \in \mathbb{F}_q[x, y]/\langle x^s - \alpha, y^\ell - \beta \rangle$, $0 \leq j \leq \ell-1$ such that

$$g(x, y, \omega^{1+tr}) = \sum_{j=0}^{\ell-1} h_j(x, y)\eta_j(y)p_j^{(t)}(x).$$

From equation (16), we get that

$$g(x, y, z)\zeta_t(z) = \zeta_t(z)g(x, y, \omega^{1+tr}) = \zeta_t(z) \sum_{j=0}^{\ell-1} h_j(x, y)\eta_j(y)p_j^{(t)}(x).$$

Since $\sum_{t=0}^{k-1} \zeta_t(z) = 1$, we get $g(x, y, z) = \sum_{t=0}^{k-1} g(x, y, z)\zeta_t(z) = \sum_{t=0}^{k-1} \sum_{j=0}^{\ell-1} \zeta_t(z)h_j(x, y)\eta_j(y)p_j^{(t)}(x)$. Therefore,

$g(x, y, z) \in \mathcal{D}$. Hence, $\mathcal{C} \subseteq \mathcal{D}$. Also, as $\eta_j(y)p_j^{(t)}(x) \in I_t$ for every $j = 0, 1, \dots, \ell-1$, we have, by definition (13) of I_t , $\zeta_t(z)\eta_j(y)p_j^{(t)}(x) \in \mathcal{C}$. This being true for every $t, t = 0, 1, \dots, k-1$, we have $\mathcal{D} = \mathcal{C}$.

In order to prove that G is a generator matrix of $\mathcal{C}$, it is enough to prove that rows of G are linearly independent. Suppose, if possible, there exist polynomials $m_{t,j}(x)$ in $\mathbb{F}_q[x]/\langle x^s - \alpha \rangle$, with $\deg m_{t,j}(x) \leq s - a_{t,j} - 1$, for $t = 0, 1, 2, \dots, k-1$ and $j = 0, 1, 2, \dots, \ell-1$, such that

$$\begin{aligned} m_{0,0}(x)\zeta_0(z)\eta_0(y)p_0^{(0)}(x) + \dots + m_{0,\ell-1}(x)\zeta_0(z)\eta_{\ell-1}(y)p_{\ell-1}^{(0)}(x) + \dots \\ m_{k-1,0}(x)\zeta_{k-1}(z)\eta_0(y)p_0^{(k-1)}(x) + \dots + m_{k-1,\ell-1}(x)\zeta_{k-1}(z)\eta_{\ell-1}(y)p_{\ell-1}^{(k-1)}(x) = 0 \end{aligned}$$



in $\mathbb{F}_q[x, y, z]/\langle x^s - \alpha, y^\ell - \beta, z^k - \gamma \rangle$. Therefore, there exist polynomials $a(x, y, z), b(x, y, z), c(x, y, z) \in \mathbb{F}_q[x, y, z]$ such that

$$\sum_{t=0}^{k-1} \sum_{j=0}^{\ell-1} m_{t,j}(x) \zeta_t(z) \eta_j(y) p_j^{(t)}(x) = a(x, y, z)(x^s - \alpha) + b(x, y, z)(y^\ell - \beta) + c(x, y, z)(z^k - \gamma). \quad (17)$$

Substituting $z = \omega^{1+tr}$ and $y = \theta^{1+jr'}$ in equation (17) and using equations (9) and (12), we get

$$m_{t,j}(x) p_j^{(t)}(x) = a(x, \theta^{1+jr'}, \omega^{1+tr})(x^s - \alpha). \quad (18)$$

Since, $\deg(m_{t,j}(x) p_j^{(t)}(x)) \leq s - a_{t,j} - 1 + a_{t,j} < s$, comparing coefficients of $x^s, x^{s+1}, \dots$ on both sides of (18), we find that coefficients of $a(x, \theta^{1+jr'}, \omega^{1+tr})$ are all zero and hence $a(x, \theta^{1+jr'}, \omega^{1+tr}) = 0$, i.e. $m_{t,j}(x) p_j^{(t)}(x) = 0$ in $\mathbb{F}_q[x]$. Therefore, $m_{t,j}(x) = 0$ for all $t = 0, 1, \dots, k-1$ and $j = 0, 1, \dots, \ell-1$. Thus the rows of G form a generator matrix of $\mathcal{C}$. $\square$

Corollary 1 The dimension of a 3-D (α, β, γ) -constacyclic code $\mathcal{C}$ of length $s\ell k$ is given by $s\ell k - \sum_{t=0}^{k-1} \sum_{j=0}^{\ell-1} a_{t,j}$.

2.3 Generator matrix of dual code

We assume here that $\alpha, \beta, \gamma \in \{1, -1\}$ so that the dual code $\mathcal{C}^\perp$ of a 3-D (α, β, γ) -constacyclic code $\mathcal{C}$ is also an ideal in the ring $\mathcal{R}$. As $\dim(\mathcal{C}) + \dim(\mathcal{C}^\perp) = s\ell k$, therefore $\dim(\mathcal{C}^\perp) = a_{0,0} + \dots + a_{0,\ell-1} + \dots + a_{k-1,0} + \dots + a_{k-1,\ell-1}$. As $p_j^{(t)}(x)$ are divisors of $x^s - \alpha$, there exist polynomials $q_j^{(t)}(x) \in \mathbb{F}_q[x]$ such that $p_j^{(t)}(x) q_j^{(t)}(x) = x^s - \alpha$ for $t = 0, 1, \dots, k-1$ and $j = 0, 1, \dots, \ell-1$. The following theorem gives the generators of the dual code $\mathcal{C}^\perp$:

Theorem 2 Suppose that $\alpha, \beta, \gamma \in \{1, -1\}$. Let $\mathcal{C}$ be a 3-D (α, β, γ) -constacyclic code of length $n = s\ell k$ as given in Theorem 1. Then the dual code

$$\mathcal{C}^\perp = \langle q_j^{(t)*}(x) \eta_j^*(y) \zeta_t^*(z) : 0 \leq t \leq k-1, 0 \leq j \leq \ell-1 \rangle; \quad (19)$$

and a generator matrix of $\mathcal{C}^\perp$ is given by

$$H = \begin{pmatrix} \zeta_0^*(z) \eta_0^*(y) q_0^{(0)*}(x) \\ x \zeta_0^*(z) \eta_0^*(y) q_0^{(0)*}(x) \\ \vdots \\ x^{a_{0,0}-1} \zeta_0^*(z) \eta_0^*(y) q_0^{(0)*}(x) \\ \vdots \\ \zeta_0^*(z) \eta_{\ell-1}^*(y) q_{\ell-1}^{(0)*}(x) \\ x \zeta_0^*(z) \eta_{\ell-1}^*(y) q_{\ell-1}^{(0)*}(x) \\ \vdots \\ x^{a_{0,\ell-1}-1} \zeta_0^*(z) \eta_{\ell-1}^*(y) q_{\ell-1}^{(0)*}(x) \\ \vdots \\ \vdots \\ \zeta_{k-1}^*(z) \eta_{\ell-1}^*(y) q_{\ell-1}^{(k-1)*}(x) \\ x \zeta_{k-1}^*(z) \eta_{\ell-1}^*(y) q_{\ell-1}^{(k-1)*}(x) \\ \vdots \\ x^{a_{k-1,\ell-1}-1} \zeta_{k-1}^*(z) \eta_{\ell-1}^*(y) q_{\ell-1}^{(k-1)*}(x) \end{pmatrix},$$

where $\zeta_t^*(z)$, $\eta_j^*(y)$ and $q_j^{(t)*}(x)$ denote the reciprocal polynomials of $\zeta_t(z)$, $\eta_j(y)$ and $q_j^{(t)}(x)$ respectively.



Proof Let the code on the right hand side of equation (19) be denoted by D . To prove that $D \subset \mathcal{C}^\perp$ it is enough to prove, by Proposition 4, that $\zeta_t^*(z)\eta_j^*(y)q_j^{(t)*}(x) \in \text{ann}(\mathcal{C})^*$ i.e. $\zeta_t(z)\eta_j(y)q_j^{(t)}(x) \in \text{ann}(\mathcal{C})$ for each t, j ; $0 \leq t \leq k-1$, $0 \leq j \leq \ell-1$. As $\mathcal{C} = \langle \zeta_u(z)\eta_v(y)p_v^{(u)}(x), 0 \leq u \leq k-1, 0 \leq v \leq \ell-1 \rangle$, it is enough to prove that

$$\zeta_t(z)\eta_j(y)q_j^{(t)}(x)\zeta_u(z)\eta_v(y)p_v^{(u)}(x) = 0 \quad (20)$$

for all u, v ; $0 \leq u \leq k-1$, $0 \leq v \leq \ell-1$. Now if $u \neq t$, we have $\zeta_u(z)\zeta_t(z) = 0$; when $v \neq j$, we have $\eta_v(y)\eta_j(y) = 0$ and when $u = t$, $v = j$ we have $p_j^{(t)}(x)q_j^{(t)}(x) = x^s - \alpha = 0$ in the ring $\mathcal{R}$. Hence the expression (20) holds i.e. $D \subset \mathcal{C}^\perp$.

To prove that $\dim(D) = a_{0,0} + \dots + a_{0,\ell-1} + \dots + a_{k-1,0} + \dots + a_{k-1,\ell-1} = \dim(\mathcal{C}^\perp)$, we need to show that the rows of H are linearly independent. Suppose, if possible, there exist polynomials $m_{0,0}(x), \dots, m_{0,\ell-1}(x), \dots, m_{k-1,\ell-1}(x)$ in $\mathbb{F}_q[x]/\langle x^s - \alpha \rangle$, with $\deg m_{t,j}(x) \leq a_{t,j} - 1$ for $t = 0, 1, 2, \dots, k-1$ and $j = 0, 1, 2, \dots, \ell-1$ such that

$$m_{0,0}(x)q_0^{(0)*}(x)\eta_0^*(y)\zeta_0^*(z) + \dots + m_{k-1,\ell-1}(x)q_{\ell-1}^{(k-1)*}(x)\eta_{\ell-1}^*(y)\zeta_{k-1}^*(z) = 0$$

in $\mathbb{F}_q[x, y, z]/\langle x^s - \alpha, y^\ell - \beta, z^k - \gamma \rangle$.

Therefore, there exist polynomials $a(x, y, z), b(x, y, z), c(x, y, z) \in \mathbb{F}_q[x, y, z]$ such that

$$\sum_{t=0}^{k-1} \sum_{j=0}^{\ell-1} m_{t,j}(x)q_j^{(t)*}(x)\eta_j^*(y)\zeta_t^*(z) = a(x, y, z)(x^s - \alpha) + b(x, y, z)(y^\ell - \beta) + c(x, y, z)(z^k - \gamma). \quad (21)$$

Let first $r = r' = 1$. Then by Lemma 5, $\zeta_t^*(z) = c_t \zeta_{k-2-t}(z)$ and $\eta_j^*(y) = b_j \eta_{\ell-2-j}(y)$ for some constant c_t and $b_j \in \mathbb{F}_q^*$. Also by equation (9), we have $\zeta_{k-2-t}(\omega^{k-1-t}) = 1$, and $\zeta_{k-2-t'}(\omega^{k-1-t}) = 0$ for $t \neq t'$. Similarly by (12), we have $\eta_{\ell-2-j}(\theta^{\ell-1-j}) = 1$, and $\eta_{\ell-2-j'}(\theta^{\ell-1-j}) = 0$ for $j \neq j'$.

Substituting $y = \theta^{\ell-1-j}$, $z = \omega^{k-1-t}$ in equation (21), we get

$$m_{t,j}(x)c_t b_j q_j^{(t)*}(x) = a(x, \theta^{\ell-1-j}, \omega^{k-1-t})(x^s - \alpha).$$

Since $\deg(m_{t,j}(x)q_j^{(t)*}(x)) \leq a_{t,j} - 1 + s - a_{t,j} < s$, comparing coefficients of $x^s, x^{s+1}, \dots$ on both sides we find that coefficients of $a(x, \theta^{\ell-1-j}, \omega^{k-1-t})$ are all zero and hence $a(x, \theta^{\ell-1-j}, \omega^{k-1-t}) = 0$ in $\mathbb{F}_q[x]$. Therefore, $m_{t,j}(x) = 0$ for all $j = 0, 1, \dots, \ell-1$ and $t = 0, 1, \dots, k-1$.

Let now $r = r' = 2$. Then by Lemma 5, $\zeta_t^*(z) = c_t \zeta_{k-1-t}(z)$ and $\eta_j^*(y) = b_j \eta_{\ell-1-j}(y)$. Also by equation (9), we have $\zeta_{k-1-t}(\omega^{1+2(k-1-t)}) = 1$, and $\zeta_{k-1-t'}(\omega^{1+2(k-1-t)}) = 0$ for $t \neq t'$. Similarly, by (12), we have $\eta_{\ell-1-j}(\theta^{1+2(\ell-1-j)}) = 1$, and $\eta_{\ell-1-j'}(\theta^{1+2(\ell-1-j)}) = 0$ for $j \neq j'$. Substituting $y = \theta^{1+2(\ell-1-j)}$, $z = \omega^{1+2(k-1-t)}$ in equation (18), we get

$$m_{t,j}(x)c_t b_j q_j^{(t)*}(x) = a(x, \theta^{1+2(\ell-1-j)}, \omega^{1+2(k-1-t)})(x^s - \alpha).$$

Working as above we find that $m_{t,j}(x) = 0$ for all $j = 0, 1, \dots, \ell-1$ and $t = 0, 1, \dots, k-1$.

When $r = 2$ and $r' = 1$. By Lemma 5, $\zeta_t^*(z) = c_t \zeta_{k-1-t}(z)$ and $\eta_j^*(y) = b_j \eta_{\ell-2-j}(y)$. Also by equations (9) and (12), we have $\zeta_{k-1-t}(\omega^{1+2(k-1-t)}) = 1$, $\zeta_{k-1-t'}(\omega^{1+2(k-1-t)}) = 0$ for $t \neq t'$; $\eta_{\ell-2-j}(\theta^{\ell-1-j}) = 1$, and $\eta_{\ell-2-j'}(\theta^{\ell-1-j}) = 0$ for $j \neq j'$. We substitute $y = \theta^{\ell-1-j}$, $z = \omega^{1+2(k-1-t)}$ in equation (18) and working as above find that $m_{t,j}(x) = 0$ for all $j = 0, 1, \dots, \ell-1$ and $t = 0, 1, \dots, k-1$.

The case $r = 1$ and $r' = 2$ is similar.

Therefore $D = \mathcal{C}^\perp$ and the rows of H form a generator matrix of $\mathcal{C}^\perp$. $\square$

Remark 1 If $\deg(p_j^{(t)}(x)) = a_{t,j} = 0$ for some t, j ; $0 \leq t \leq k-1$, $0 \leq j \leq \ell-1$, i.e. $p_j^{(t)}(x) = \lambda$, a constant, then the polynomials

$$\zeta_t^*(z)\eta_j^*(y)q_j^{(t)*}(x), x\zeta_t^*(z)\eta_j^*(y)q_j^{(t)*}(x), \dots, x^{a_{t,j}-1}\zeta_t^*(z)\eta_j^*(y)q_j^{(t)*}(x)$$

do not contribute any rows in H .



2.4 Self-dual codes

Theorem 3 Suppose that $\alpha, \beta, \gamma \in \{1, -1\}$. Then a three-dimensional (α, β, γ) -constacyclic code $\mathcal{C}$ of length $n = s\ell k$ is self-dual if and only if

- (i) $s\ell k = 2(a_{00} + \cdots + a_{0,\ell-1} + \cdots + a_{k-1,0} + \cdots + a_{k-1,\ell-1})$
- (ii) for every t, j ; $0 \leq t \leq k-1, 0 \leq j \leq \ell-1$,

$$q_j^{(t)*}(x) = m_{tj}(x)p_{\ell-2-j}^{(k-2-t)}(x), \quad p_j^{(t)}(x) = m'_{tj}(x)q_{\ell-2-j}^{(k-2-t)*}(x) \quad \text{if } \beta = 1, \gamma = 1 \quad (22)$$

$$q_j^{(t)*}(x) = m_{tj}(x)p_{\ell-1-j}^{(k-1-t)}(x), \quad p_j^{(t)}(x) = m'_{tj}(x)q_{\ell-1-j}^{(k-1-t)*}(x) \quad \text{if } \beta = -1, \gamma = -1$$

$$q_j^{(t)*}(x) = m_{tj}(x)p_{\ell-2-j}^{(k-1-t)}(x), \quad p_j^{(t)}(x) = m'_{tj}(x)q_{\ell-2-j}^{(k-1-t)*}(x) \quad \text{if } \beta = 1, \gamma = -1$$

$$q_j^{(t)*}(x) = m_{tj}(x)p_{\ell-1-j}^{(k-2-t)}(x), \quad p_j^{(t)}(x) = m'_{tj}(x)q_{\ell-1-j}^{(k-2-t)*}(x) \quad \text{if } \beta = -1, \gamma = 1$$

for some non-zero polynomials $m_{tj}(x), m'_{tj}(x)$ in $\mathbb{F}_q[x]/\langle x^s - \alpha \rangle$. When $\gamma = 1$ and $t = k-1$, the superscript $k-2-t$ be replaced by $k-1$. Similarly when $\beta = 1$ and $j = \ell-1$, the subscript $\ell-2-j$ be replaced by $\ell-1$.

Proof It is clear that if $\mathcal{C}$ is self-dual, then $s\ell k = 2(a_{00} + \cdots + a_{0,\ell-1} + \cdots + a_{k-1,0} + \cdots + a_{k-1,\ell-1})$. By (19), we find that

$\mathcal{C}^\perp \subset \mathcal{C}$ if each of $q_j^{(t)*}(x)\eta_j^*(y)\zeta_t^*(z)$, $0 \leq t \leq k-1, 0 \leq j \leq \ell-1$ is a linear combination of rows of generator matrix G of $\mathcal{C}$ as given in Theorem 1. This is so if and only if there exist polynomials $h_{uv}(x)$ of $\deg h_{uv} \leq s - a_{u,v} - 1$ in $\mathbb{F}_q[x]/\langle x^s - \alpha \rangle$ such that

$$q_j^{(t)*}(x)\eta_j^*(y)\zeta_t^*(z) = \sum_{u=0}^{k-1} \sum_{v=0}^{\ell-1} h_{uv}(x)p_v^{(u)}(x)\eta_v(y)\zeta_u(z). \quad (23)$$

Again $\mathcal{C} \subset \mathcal{C}^\perp$ if, by (15), each of $p_j^{(t)}(x)\eta_j(y)\zeta_t(z)$, $0 \leq t \leq k-1, 0 \leq j \leq \ell-1$ is a linear combination of rows of generator matrix H of $\mathcal{C}^\perp$ as given in Theorem 2. This is so if and only if there exists polynomials $h'_{uv}(x)$ of $\deg h'_{uv} \leq a_{u,v} - 1$ in $\mathbb{F}_q[x]/\langle x^s - \alpha \rangle$ such that

$$p_j^{(t)}(x)\eta_j(y)\zeta_t(z) = \sum_{u=0}^{k-1} \sum_{v=0}^{\ell-1} h'_{uv}(x)q_v^{(u)*}(x)\eta_v^*(y)\zeta_u^*(z). \quad (24)$$

When $\beta = 1 = \gamma$, we have $r = r' = 1$ and $\zeta_t^*(z) = b_t\zeta_{k-2-t}(z)$, $\eta_j^*(y) = c_j\eta_{\ell-2-j}(y)$ by Lemmas 5 and 6. When $t = k-1$, $\zeta_{k-2-t}(z) = \zeta_{k-1}(z)$ and when $j = \ell-1$, $\eta_{\ell-2-j}(y) = \eta_{\ell-1}(y)$. Multiplying both sides of (23) by $\zeta_{k-2-t}(z)\eta_{\ell-2-j}(y)$ we get

$$q_j^{(t)*}(x)c_j\eta_{\ell-2-j}^2(y)b_t\zeta_{k-2-t}^2(z) = \sum_{u=0}^{k-1} \sum_{v=0}^{\ell-1} h_{uv}(x)p_v^{(u)}(x)\eta_v(y)\eta_{\ell-2-j}(y)\zeta_u(z)\zeta_{k-2-t}(z).$$

As $\zeta_u(z), \eta_v(y)$ are primitive central idempotents, $\mathcal{C}^\perp \subset \mathcal{C}$ if and only if

$$q_j^{(t)*}(x)c_j\eta_{\ell-2-j}(y)b_t\zeta_{k-2-t}(z) = h_{k-2-t,\ell-2-j}(x)p_{\ell-2-j}^{(k-2-t)}(x)\eta_{\ell-2-j}(y)\zeta_{k-2-t}(z)$$

i.e. if and only if

$$q_j^{(t)*}(x) = m_{tj}(x)p_{\ell-2-j}^{(k-2-t)}(x)$$

for some polynomial $m_{tj}(x)$.



Further, (24) can be rewritten as

$$\begin{aligned} p_j^{(t)}(x)\eta_j(y)\zeta_t(z) &= \sum_{u=0}^{k-1} \sum_{v=0}^{\ell-1} b_u c_v h'_{uv}(x) q_v^{(u)*}(x) \eta_{\ell-2-v}(y) \zeta_{k-2-u}(z) \\ &= \sum_{u=-1}^{k-2} \sum_{v=-1}^{\ell-2} b_{k-2-u} c_{\ell-2-v} h'_{k-2-u, \ell-2-v}(x) q_{\ell-2-v}^{(k-2-u)*}(x) \eta_v(y) \zeta_u(z) \end{aligned} \quad (25)$$

with the understanding that $\zeta_{-1}(z) = \xi_0(z) = \zeta_{k-1}(z)$ from equation (8) and similarly $\eta_{-1}(y) = \eta_{\ell-1}(y)$. $\square$

Multiplying both sides of (25) by $\eta_j(y)\zeta_t(z)$, $\mathcal{C} \subset \mathcal{C}^\perp$ if and only if

$$p_j^{(t)}(x)\eta_j(y)\zeta_t(z) = b_{k-2-t} c_{\ell-2-j} h'_{k-2-t, \ell-2-j}(x) q_{\ell-2-j}^{(k-2-t)*}(x) \eta_j(y) \zeta_t(z)$$

i.e., if and only if

$$p_j^{(t)}(x) = m'_{tj}(x) q_{\ell-2-j}^{(k-2-t)*}(x)$$

for some polynomial $m'_{tj}(x)$.

When $\beta = -1 = \gamma$, we have $r = r' = 2$, $\zeta_t^*(z) = b_t \zeta_{k-1-t}(z)$, $\eta_j^*(y) = c_j \eta_{\ell-1-j}(y)$; when $\beta = 1$, $\gamma = -1$, we have $r = 2$, $r' = 1$, $\zeta_t^*(z) = b_t \zeta_{k-1-t}(z)$, $\eta_j^*(y) = c_j \eta_{\ell-2-j}(y)$; and when $\beta = -1$, $\gamma = 1$, we have $r = 1$, $r' = 2$, $\zeta_t^*(z) = b_t \zeta_{k-2-t}(z)$, $\eta_j^*(y) = c_j \eta_{\ell-1-j}(y)$ and the proof is similar.

Theorem 4 If $\beta = 1 = \gamma$ and $\alpha = \pm 1$ then a three-dimensional $(\alpha, 1, 1)$ -constacyclic code $\mathcal{C}$ of length $n = s\ell k$ can not be self-dual if $\gcd(s, q) = 1$, assuming that s is odd if $\alpha = -1$.

Proof Suppose a three-dimensional $(\alpha, 1, 1)$ -constacyclic code is self-dual. On taking $t = k - 1$, $j = \ell - 1$ in equation (22) we get

$$q_{\ell-1}^{(k-1)*}(x) = m_{k-1, \ell-1}(x) p_{\ell-1}^{(k-1)}(x), \quad (26)$$

and

$$p_{\ell-1}^{(k-1)}(x) = m'_{k-1, \ell-1}(x) q_{\ell-1}^{(k-1)*}(x). \quad (27)$$

We have $x^s - \alpha = p_{\ell-1}^{(k-1)}(x) q_{\ell-1}^{(k-1)*}(x)$. If $\gcd(s, q) = 1$, $x - \alpha$ divides exactly one of $p_{\ell-1}^{(k-1)}(x)$ and $q_{\ell-1}^{(k-1)*}(x)$ and not both (If $\alpha = -1$, we assume that s is odd). The reciprocal of $x - \alpha$ is $\pm(x - \alpha)$.

If $x - \alpha | p_{\ell-1}^{(k-1)}(x)$, then from equation (26) we have $x - \alpha | q_{\ell-1}^{(k-1)*}(x)$. This implies $(x - \alpha)^* | (q_{\ell-1}^{(k-1)*}(x))^*$, i.e. $x - \alpha | q_{\ell-1}^{(k-1)}(x)$ as $(f^*)^* = f$. This is not possible, when $\gcd(s, q) = 1$.

If $x - \alpha | q_{\ell-1}^{(k-1)*}(x)$, we have $(x - \alpha)^* | q_{\ell-1}^{(k-1)}(x)$ i.e. $(x - \alpha) | q_{\ell-1}^{(k-1)*}(x)$. This implies, from equation (27), $x - \alpha | p_{\ell-1}^{(k-1)}(x)$, again not possible. $\square$

2.5 Examples

Minimum distances of codes in the following examples have been calculated by software MAGMA.

Example 1 Let $q = 5$, $\alpha = 1$, $\beta = -1$, $\gamma = -1$, $s = 2 = \ell = k$. One finds that $\omega = 2$ is a 4^{th} root of unity in $\mathbb{F}_5^*$ such that $\omega^2 = -1$. Therefore

$$z^2 + 1 = (z - 2)(z - 2^3) = (z - 2)(z - 3).$$

Thus,

$$\zeta_0(z) = -z + 3, \quad \zeta_1(z) = z + 3.$$

Also $\theta = 2$ is a 4^{th} root of unity in $\mathbb{F}_5^*$ such that $\theta^2 = -1$. Therefore,



$$\eta_0(y) = -y + 3, \quad \eta_1(y) = y + 3.$$

We have $x^2 - 1 = (x - 1)(x + 1)$. Suppose, $p_0^{(0)}(x) = p_0^{(1)}(x) = x - 1$, and $p_1^{(0)}(x) = p_1^{(1)}(x) = x + 1$, then by Theorems 1 and 2, generator matrices of two dimensional $(1, -1, -1)$ -constacyclic code $\mathcal{C}$ and $\mathcal{C}^\perp$ are given by

$$G = \begin{pmatrix} (x-1)(-y+3)(-z+3) \\ (x+1)(y+3)(-z+3) \\ (x-1)(-y+3)(z+3) \\ (x+1)(y+3)(z+3) \end{pmatrix} \text{ and } H = \begin{pmatrix} (x+1)(-1+3y)(-1+3z) \\ (-x+1)(1+3y)(-1+3z) \\ (x+1)(-1+3y)(1+3z) \\ (-x+1)(1+3y)(1+3z) \end{pmatrix}$$

respectively. The corresponding code $\mathcal{C}_3$ has a generator matrix

$$G_3 = \begin{pmatrix} 1 & -1 & -2 & 2 & -2 & 2 & -1 & 1 \\ -1 & -1 & -2 & -2 & 2 & 2 & -1 & -1 \\ 1 & -1 & -2 & 2 & 2 & -2 & 1 & -1 \\ -1 & -1 & -2 & -2 & -2 & -2 & 1 & 1 \end{pmatrix}.$$

Then $\mathcal{C}_3$ is a $[8, 4, 2]$ self-dual and (-1) -quasi-twisted code of index 2 over $\mathbb{F}_5[x]$.

Example 2 Let $q = 7, \alpha = 1, \beta = 1, \gamma = -1, s = 2 = \ell$ and $k = 3$. One finds that $\omega = 3$ is a 6^{th} root of unity in $\mathbb{F}_7^*$ such that $\omega^3 = -1$. Therefore

$$z^3 + 1 = (z - 3)(z - 3^3(z - 3^5)) = (z - 3)(z + 1)(z + 2).$$

Thus,

$$\zeta_0(z) = -z^2 - 3z - 2, \quad \zeta_1(z) = -2z^2 + 2z - 2, \quad \zeta_2(z) = 3z^2 + z - 2.$$

Also $y^2 - 1 = (y - 1)(y + 1)$, hence $\eta_0(y) = -3y - 3, \eta_1(y) = 3y - 3$.

We have $x^2 - 1 = (x - 1)(x + 1)$. Suppose, $p_0^{(0)}(x) = p_0^{(1)}(x) = p_0^{(2)}(x) = x - 1$, and $p_1^{(0)}(x) = p_1^{(1)}(x) = p_1^{(2)}(x) = x + 1$, then by Theorems 1 and 2, generator matrices of two dimensional $(1, 1, -1)$ -constacyclic code $\mathcal{C}$ and $\mathcal{C}^\perp$ are given by

$$G = \begin{pmatrix} (x-1)(-3y-3)(-z^2-3z-2) \\ (x+1)(3y-3)(-z^2-3z-2) \\ (x-1)(-3y-3)(-2z^2+2z-2) \\ (x+1)(3y-3)(-2z^2+2z-2) \\ (x-1)(-3y-3)(3z^2+z-2) \\ (x+1)(3y-3)(3z^2+z-2) \end{pmatrix}, H = \begin{pmatrix} (x+1)(-3y-3)(-2z^2-3z-1) \\ (-x+1)(-3y+3)(-2z^2-3z-1) \\ (x+1)(-3y-3)(-2z^2+2z-2) \\ (-x+1)(-3y+3)(-2z^2+2z-2) \\ (x+1)(-3y-3)(-2z^2+z+3) \\ (-x+1)(-3y+3)(-2z^2+z+3) \end{pmatrix}$$

respectively. By Theorem 3, the code $\mathcal{C}$ can not be self-dual as $p_j^{(t)} = p_0^{(0)} = x - 1$ but $q_{\ell-2-j}^{(k-2-t)*} = q_0^{(1)*} = x + 1$. The corresponding code $\mathcal{C}_3$ is a $[12, 6, 2]$ code over $\mathbb{F}_7[x]$. It is a (-1) -quasi-twisted code of index 3.

Example 3 Let $q = 7, \alpha = -1, \beta = 2, \gamma = -1, s = 3, \ell = 2$ and $k = 3$. As computed in Example 2, we have

$$\zeta_0(z) = 6z^2 + 4z + 5, \quad \zeta_1(z) = 5z^2 - 5z + 5, \quad \zeta_2(z) = 3z^2 + z - 2.$$

Also $\theta = 3$ is a 6^{th} root of unity in $\mathbb{F}_7^*$ such that $\theta^2 = 2$. Therefore

$$y^2 - 2 = (y - 3)(y - 3^4) = (y - 3)(y - 4).$$

And hence,

$$\eta_0(y) = 6y + 4, \quad \eta_1(y) = y + 4.$$



We have $x^3 + 1 = (x + 1)(x^2 - x + 1)$. Suppose, $p_0^{(0)}(x) = p_0^{(1)}(x) = x^2 - x + 1$, $p_1^{(0)}(x) = p_0^{(2)}(x) = x + 1$ and $p_1^{(1)}(x) = p_1^{(2)}(x) = 1$, then by Theorem 1, generator matrix of three dimensional $(-1, 2, -1)$ -constacyclic code $\mathcal{C}$ is given by

$$G = \begin{pmatrix} (x^2 - x + 1)(6y + 4)(6z^2 + 4z + 5) \\ (x + 1)(y + 4)(6z^2 + 4z + 5) \\ x(x + 1)(y + 4)(6z^2 + 4z + 5) \\ (x^2 - x + 1)(6y + 4)(5z^2 - 5z + 5) \\ 1(y + 4)(5z^2 - 5z + 5) \\ x(y + 4)(5z^2 - 5z + 5) \\ x^2(y + 4)(5z^2 - 5z + 5) \\ (x + 1)(6y + 4)(3z^2 + z + 5) \\ x(x + 1)(6y + 4)(3z^2 + z + 5) \\ 1(y + 4)(3z^2 + z + 5) \\ x(y + 4)(3z^2 + z + 5) \\ x^2(y + 4)(3z^2 + z + 5) \end{pmatrix}.$$

The corresponding code $\mathcal{C}_3$ is a $[18, 12, 4]$ code over $\mathbb{F}_7[x]$. It is a (-1) -quasi-twisted code of index 3.

3 Conclusion

In this paper we characterize the algebraic structure of three-dimensional (α, β, γ) -constacyclic codes of arbitrary length slk and their duals over a finite field $\mathbb{F}_q$, where α, β, γ are non zero elements of $\mathbb{F}_q$. We give necessary and sufficient conditions for a three-dimensional constacyclic code to be self-dual. The same technique can be applied to characterize the algebraic structure of multi-dimensional constacyclic codes and their duals over a finite field $\mathbb{F}_q$.

References

1. R. Andriamfidisoa, R.M.Lalaso, T.J. Rabehimanana, Finding a Generator Matrix of a Multidimensional Cyclic Code, arXiv:1906.03491v1 [cs.IT] 8 June 2019.
2. Gurmeet K. Bakshi and Madhu Raka, A class of constacyclic codes over a finite field, *Finite Fields Appl.*, **18** (2)(2012), 362-377.
3. Swati Bhargwaj and Madhu Raka, Two dimensional constacyclic codes of arbitrary length over finite fields, *Indian J. Pure Appl. Maths*, **53**(1)(2022), 49-61.
4. B. Chen, H.Q. Dinh and H. Liu, Repeated-root constacyclic codes of length $2l^m pn$, *Finite Fields Appl.*, **33** (2015), 137-159.
5. Mokshi Goyal and Madhu Raka, Duadic and triadic codes over a finite non-chain ring and their Gray images, *Int. J. Information and Coding Theory*, **5**(1)(2018), 36 -54.
6. Mokshi Goyal and Madhu Raka, Polyadic constacyclic codes over the non-chain ring $\mathbb{F}_q[u, v]/\langle f(u), g(v), uv - vu \rangle$, *J. Appl. Math. Comput.*, **62**(1-2)(2020), 425- 447.
7. C. Güneri and F. Özbudak, Multidimensional cyclic codes and Artin-Schreier type hypersurfaces over finite fields, *Finite Fields Appl.*, **14** (2008), 44-58.
8. C. Güneri and F. Özbudak, A relation between quasi-cyclic codes and 2-D cyclic codes, *Finite Fields Appl.*, **18** (2012), 123 -132.
9. T. Ikai, H. Kosako, Y. Kojima, Two-dimensional cyclic codes, *Electron. Commun. Jpn.*, **57**(4) (1974/75), 27-35.
10. H. Imai, A theory of two-dimensional cyclic codes, *Inf. Control*, **34**(1) (1977), 1-21.
11. R.M. Lalaso, R. Andriamfidiso, T.J. Rabehimanana, Basis of a Multicyclic Code as an Ideal in $\mathbb{F}_q[X_1, \dots, X_s]/\langle X_1^{p_1} - 1, \dots, X_s^{p_s} - 1 \rangle$, *J. of Alg. and Related Topics*, **6** (2)(2018), 63-78.
12. R.M. Lalaso, R. Andriamfidiso, T.J. Rabehimanana, Multicyclic Codes and Algebraic Dynamical Systems, *British J. of Math. and Comp. Sci.*, **21** (2)(2017), 1-22.
13. Z. Rajabi and K. Khashyarmansh, Repeated-root two-dimensional constacyclic codes of length $2p^s \cdot 2^k$, *Finite Fields Appl.*, **50** (2018), 122 -137.
14. Madhu Raka, A class of constacyclic codes over a finite field II, *Indian J. Pure Appl. Maths*, **46** (2015), 809-825.
15. Z. Sepasdar, K. Khashyarmansh, Characterizations of some two-dimensional cyclic codes correspond to the ideals of $\mathbb{F}[x, y]/\langle x^s - 1, y^{2^k} - 1 \rangle$, *Finite Fields Appl.*, **41** (2016), 97-112.
16. Z. Sepasdar, Generator Matrix for two-dimensional cyclic codes of arbitrary length, arXiv:1704.08070v1 [math.AC] 26 Apr 2017.



Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

