Chapter 6

EAQECCs from Constacyclic Codes over a Class of Non-chain Rings

In 2006, Brun et al. [21] proposed entanglement-assisted quantum error-correcting codes (EAQECCs). These codes can be constructed from any classical linear codes and do not require the dual-containing condition if shared entangled ebits are available. Lu et al. [64] proposed a decomposition of the defining set of constacyclic codes and constructed four classes of MDS EAQECCs with less pre-shared maximally entangled states. Afterward, many researchers have constructed some classes of MDS EAQECCs [38, 44, 59, 65, 82]. In this chapter, we explore the construction of EAQECCs from constacyclic codes over a class of non-chain rings $\mathcal{T}$ as described in Chapter 4. We define a polynomial Gray map and prove that the Gray image of an α-contacyclic code is cyclic for a particular type of α. Further, we propose the construction of EAQECCs from the Gray images of α-constacyclic codes over $\mathcal{T}$ and consequently, construct some new MDS EAQECCs.

6.1 Constacyclic Codes over $\mathcal{T}$

In this section, we revisit a few important results on constacyclic codes over $\mathcal{T}$ from [14]. Further, we define a polynomial Gray map and consequently prove that the Gray image of an α-constacyclic code over $\mathcal{T}$ (for a specific choice of α) is a cyclic code over $\mathbb{F}_q$ under this Gray map. We justify this result with an illustrative example. Then, we recall the factorization $y^n - \gamma$ and a result on BCH (Bose–Chaudhuri–Hocquenghem) type bound for constacyclic codes.

Definition 6.1.1. For a unit α in $\mathcal{T}$, $\mathcal{C} \subseteq \mathcal{T}^n$ is called an α-constacyclic code of length n over $\mathcal{T}$ if it is linear and $\sigma_\alpha(\mathbf{v}) \in \mathcal{C}$ whenever $\mathbf{v} \in \mathcal{C}$, where the α-constacyclic shift $\sigma_\alpha(\mathbf{v})$ of $\mathbf{v} = (\mathsf{v}_0, \mathsf{v}_1, \ldots, \mathsf{v}_{n-1}) \in \mathcal{T}^n$ is defined as:

$$\sigma_\alpha(\mathbf{v}) = (\alpha\mathsf{v}_{n-1}, \mathsf{v}_0, \ldots, \mathsf{v}_{n-2}).$$

Moreover, for a vector $\mathbf{v} = (\mathsf{v}_0, \mathsf{v}_1, \ldots, \mathsf{v}_{n-1}) \in \mathcal{T}^n$, $\mathbf{v} \mapsto \sum_{i=0}^{n-1} \mathsf{v}_i y^i$ is an isomorphism between $\mathcal{T}^n$ and $\mathcal{T}[y]/\langle y^n - \alpha\rangle$. Under this isomorphism, a linear code $\mathcal{C}$ is an α-constacyclic code of length n if and only if it (its image) is a left submodule of $A_n = \mathcal{T}[y]/\langle y^n - \alpha\rangle$.

Lemma 6.1.2. (Theorem 2, [14]) Let $\alpha = \sum_{i_1,i_2,\ldots,i_r} \eta_{i_1 i_2 \ldots i_r} \alpha_{i_1 i_2 \ldots i_r} \in \mathcal{U}(\mathcal{T})$. A linear code $\mathcal{C} = \bigoplus_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ of length n over $\mathcal{T}$ is an α-constacyclic code over $\mathcal{T}$ if and only if $\mathcal{C}_{i_1 i_2 \ldots i_r}$ is an $\alpha_{i_1 i_2 \ldots i_r}$-constacyclic code over $\mathbb{F}_q$, for all $i_j \in \{1, 2, \ldots l_j\}, j = 1, 2, \ldots r$.

Theorem 6.1.3. (Theorem 4, [14]) Let $\alpha = \sum_{i_1,i_2,\ldots,i_r} \eta_{i_1 i_2 \ldots i_r} \alpha_{i_1 i_2 \ldots i_r} \in \mathcal{U}(\mathcal{T})$. Furthermore, let $\mathcal{C} = \bigoplus_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ be an α-constacyclic code of length n over $\mathcal{T}$, where $\mathcal{C}_{i_1 i_2 \ldots i_r} = \langle f_{i_1 i_2 \ldots i_r}(y)\rangle$ is an $\alpha_{i_1 i_2 \ldots i_r}$-constacyclic code of length n over $\mathbb{F}_q$ generated by $f_{i_1 i_2 \ldots i_r}(y)$ and $y^n - \alpha_{i_1 i_2 \ldots i_r} = f_{i_1 i_2 \ldots i_r}(y) g_{i_1 i_2 \ldots i_r}(y)$, for all

$i_j \in \{1, 2, \dots l_j\},\ j = 1, 2, \dots r$. Then there exists a polynomial $f(y)$ in $\mathcal{T}[y]$ such that

(i) $\mathcal{C} = \langle f(y) \rangle$;

(ii) $f(y)$ is a divisor of $y^n - \alpha$;

(iii) $|\mathcal{C}| = q^{l_1 l_2 \dots l_r n - \sum_{i_1, i_2, \dots, i_r} deg(f_{i_1 i_2 \dots i_r}(y))}$.

6.1.1 Polynomial Gray map

Let ω be a primitive element of the finite field $\mathbb{F}_{q^2}$. For a divisor $L = l_1 l_2 \cdots l_r$ of $q^2 - 1$, define $\gamma = \omega^{\frac{q^2-1}{L}}$, which is a primitive Lth root of unity.

Further, let

$$\alpha = \sum_{i_1, i_2, \dots, i_r} \eta_{i_1 i_2 \dots i_r} \alpha_{i_1 i_2 \dots i_r},$$

where $\alpha_{i_1 i_2 \dots i_r} = \gamma^{k_{i_1 i_2 \cdots i_r}}$ and

$$k_{i_1 i_2 \dots i_r} = \sum_{j=1}^{r} (i_j - 1) l_{j+1} l_{j+2} \dots l_r.$$

Throughout this chapter, α will be chosen in this way, and the ring $\mathcal{T}$ will be defined as

$$\mathcal{T} = \mathbb{F}_{q^2}[u_1, u_2, \dots, u_r] / \langle f_j(u_j), u_i u_j - u_j u_i \rangle,$$

where $f_j(u_j)$ are monic polynomials that split into distinct linear factors.

We define a polynomial Gray map as follows:

$$\varphi : \mathcal{T}[y] / \langle y^n - \alpha \rangle \to \mathbb{F}_{q^2}[y] / \langle y^{l_1 l_2 \dots l_r n} - 1 \rangle$$

$$\mathbf{c}(y) = \sum_{i_1,i_2,\ldots,i_r} \eta_{i_1 i_2 \ldots i_r} c_{i_1 i_2 \ldots i_r}(y) \mapsto \varphi(\mathbf{c}(y)),$$

where

$$\varphi(\mathbf{c}(y)) = (c_{i_1 i_2 \ldots i_r}(y))_{i_1 i_2 \ldots i_r} \mathbf{M} \begin{bmatrix} 1 \\ y \\ y^n \\ \vdots \\ y^{(L-1)n} \end{bmatrix}, \ c_{i_1 i_2 \ldots i_r}(y) \in \mathbb{F}_{q^2}[y],$$

$$\mathbf{M} = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \gamma^{-1} & \gamma^{-2} & \ldots & \gamma^{-(L-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \gamma^{-(L-1)} & \gamma^{-2(L-1)} & \ldots & \gamma^{-(L-1)(L-1)} \end{bmatrix}.$$

One can readily verify that $\varphi(\mathbf{c}(y))$ is well defined. Note that $\varphi(\mathbf{c}(y))$ is the polynomial representation of $\Phi(\mathbf{c})$ (defined in Chapter 4).

Theorem 6.1.4. Let $\mathcal{C} = \bigoplus_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ be an α-constacyclic code of length n over $\mathcal{T}$ such that $\mathcal{C}_{i_1 i_2 \ldots i_r} = f_{i_1 i_2 \ldots i_r}(y)$ for $i_j \in \{1, 2, \ldots, l_j\}$, $j = 1, 2, \ldots, r$. Then $\varphi(\mathcal{C})$ is a cyclic code of length $l_1 l_2 \ldots l_r n$ over $\mathbb{F}_{q^2}$ generated by $\prod_{i_1 i_2 \ldots i_r} f_{i_1 i_2 \ldots i_r}(y)$.

Proof. Note that $\alpha = \sum_{i_1,i_2,\ldots,i_r} \eta_{i_1 i_2 \ldots i_r} \alpha_{i_1 i_2 \ldots i_r}$, where $\alpha_{i_1 i_2 \ldots i_r} = \gamma^{k_{i_1 i_2 \ldots i_r}}$ and $k_{i_1 i_2 \ldots i_r} = \sum_{j=1}^{r} (i_j - 1) l_{j+1} l_{j+2} l_r$. By Lemma 6.1.2, the linear code $\mathcal{C}$ is an α-constacyclic code if and only if $\mathcal{C}_{i_1 i_2 \ldots i_r}$ is an $\alpha_{i_1 i_2 \ldots i_r}$-constacyclic code over $\mathbb{F}_{q^2}$ for all $i_j \in \{1, 2, \ldots, l_j\}$, $j = 1, 2, \ldots, r$. Since $f_{i_1 i_2 \ldots i_r}(y) | y^n - \alpha_{i_1 i_2 \ldots i_r}$, there exists $g_{i_1 i_2 \ldots i_r}(y) \in \mathbb{F}_{q^2}[y]$ such that $f_{i_1 i_2 \ldots i_r}(y) g_{i_1 i_2 \ldots i_r}(y) = y^n - \alpha_{i_1 i_2 \ldots i_r}$ for $i_j \in \{1, 2, \ldots, l_j\}$, $j = 1, 2, \ldots, r$. Thus

$$\prod_{i_1,i_2,\ldots,i_r} f_{i_1 i_2 \ldots i_r}(y) g_{i_1 i_2 \ldots i_r}(y) = \prod_{i_1,i_2,\ldots,i_r} (y^n - \alpha_{i_1 i_2 \ldots i_r})$$

$$
\begin{aligned}
&= \prod_{i_1,i_2,\ldots,i_r} (y^n - \gamma^{k_{i_1 i_2 \ldots i_r}}) \\
&= \prod_{j=0}^{L-1} (y^n - \gamma^j) \\
&= y^{Ln} - 1 = y^{l_1 l_2 \ldots l_r n} - 1
\end{aligned}
$$

and

$$
\prod_{\substack{i_1,i_2,\ldots,i_r \\ (i_1,i_2,\ldots,i_r) \neq (t_1,t_2,\ldots,t_r)}} f_{i_1 i_2 \ldots i_r}(y) \mid \left(\frac{y^{Ln} - 1}{y^n - \alpha_{t_1 t_2 \ldots t_r}} \right) = \left(\frac{y^{l_1 l_2 \ldots l_r n} - 1}{y^n - \alpha_{t_1 t_2 \ldots t_r}} \right), \tag{6.1}
$$

for $t_j \in \{1, 2, \ldots, l_j\}$, $j = 1, 2, \ldots, r$. Let $\mathbf{c}(y) = \sum_{i_1,i_2,\ldots,i_r} \eta_{i_1 i_2 \ldots i_r} f_{i_1 i_2 \ldots i_r}(y) a_{i_1 i_2 \ldots i_r}(y)$ be an element of $\mathcal{C}$, where $a_{i_1 i_2 \ldots i_r}(y) \in \mathbb{F}_{q^2}[y]$. Then

$$
\begin{aligned}
\varphi(\mathbf{c}(y)) = &\sum_{i_1,i_2,\ldots,i_r} f_{i_1 i_2 \ldots i_r} a_{i_1 i_2 \ldots i_r} + \sum_{i_1,i_2,\ldots,i_r} \alpha_{i_1 i_2 \ldots i_r}^{-k_{i_1 i_2 \ldots i_r}} f_{i_1 i_2 \ldots i_r} a_{i_1 i_2 \ldots i_r} \\
&+ \sum_{i_1,i_2,\ldots,i_r} \alpha_{i_1 i_2 \ldots i_r}^{-2k_{i_1 i_2 \ldots i_r}} f_{i_1 i_2 \ldots i_r} a_{i_1 i_2 \ldots i_r} + \cdots \\
&+ \sum_{i_1,i_2,\ldots,i_r} \alpha_{i_1 i_2 \ldots i_r}^{(-l_{i_1 i_2 \ldots i_r})(-k_{i_1 i_2 \ldots i_r})} f_{i_1 i_2 \ldots i_r} a_{i_1 i_2 \ldots i_r} \\
&= \sum_{t_1,t_2,\ldots,t_r} \Big(\sum_{i_1,i_2,\ldots,i_r} \alpha_{t_1 t_2 \ldots t_r}^{-k_{i_1 i_2 \ldots i_r}} f_{i_1 i_2 \ldots i_r} a_{i_1 i_2 \ldots i_r} \Big) y^{k_{t_1 t_2 \ldots t_r}} \\
&= \sum_{i_1,i_2,\ldots,i_r} \left(\sum_{t_1,t_2,\ldots,t_r} \alpha_{t_1 t_2 \ldots t_r}^{-k_{i_1 i_2 \ldots i_r}} y^{k_{t_1 t_2 \ldots t_r}} \right) f_{i_1 i_2 \ldots i_r} a_{i_1 i_2 \ldots i_r} \\
&= \sum_{i_1,i_2,\ldots,i_r} \alpha_{i_1 i_2 \ldots i_r} \left(\frac{y^{l_1 l_2 \ldots l_r n} - 1}{y^n - \alpha_{i_1 i_2 \ldots i_r}} \right) f_{i_1 i_2 \ldots i_r} a_{i_1 i_2 \ldots i_r}.
\end{aligned}
$$

Therefore, by 6.1, there exists $h(y) \in \mathbb{F}_{q^2}[y]$ such that

$$
\left(\prod_{i_1,i_2,\ldots,i_r} f_{i_1 i_2 \ldots i_r} \right) h = \varphi(\mathbf{c}(y)).
$$

This shows that $\varphi(\mathcal{C}) \subseteq \langle \prod_{i_1,i_2,\ldots,i_r} f_{i_1 i_2 \ldots i_r} \rangle$. Also, we have

$|\varphi(\mathcal{C})| = |\mathcal{C}| = q^{2(l_1 l_2 \ldots l_r n - \sum_{i_1,i_2,\ldots,i_r}(deg(f_{i_1 i_2 \ldots i_r}(y)))}$ and

$|\langle \prod_{i_1,i_2,\ldots,i_r} f_{i_1 i_2 \ldots i_r}(y)\rangle| = q^{2(l_1 l_2 \ldots l_r n - \sum_{i_1,i_2,\ldots,i_r}(deg(f_{i_1 i_2 \ldots i_r}(y)))}$. Thus, we have $\varphi(\mathcal{C}) = \langle \prod_{i_1,i_2,\ldots,i_r} f_{i_1 i_2 \ldots i_r}\rangle$. Since, $\varphi(\mathcal{C})$ is an ideal of the ring $\mathbb{F}_{q^2}[y]/\langle y^{l_1 l_2 \ldots l_r n} - 1\rangle$, we have $\varphi(\mathcal{C})$ is a cyclic code of length $l_1 l_2 \ldots l_r n$ over $\mathbb{F}_{q^2}$ with the generator polynomial $\prod_{i_1,i_2,\ldots,i_r} f_{i_1 i_2 \ldots i_r}$. □

Example 6.1.5. For $q = 3^2, r = 2$, let $\mathcal{T} = \mathbb{F}_{3^4}[u_1, u_2]/\langle u_1^2 - 1, u_2^2 - 1, u_1 u_2 - u_2 u_1\rangle$. Then $\eta_{11} = u_1 u_2, \eta_{12} = u_1(1 - u_2), \eta_{21} = (1 - u_1)u_2, \eta_{22} = (1 - u_1)(1 - u_2)$ and every element $\mathbf{v} \in \mathcal{T}$ can be uniquely written as $\mathbf{v} = \eta_{11} v_{11} + \eta_{12} v_{12} + \eta_{21} v_{21} + \eta_{22} v_{22}$. Let ω be a primitive element of $\mathbb{F}_{3^4}$. Let $\gamma = \omega^{20}$ and $\alpha_{11} = \gamma^{k_{11}} = \gamma^0 = 1$, $\alpha_{12} = \gamma^{k_{12}} = \gamma^1 = \gamma = \omega^{20}$, $\alpha_{21} = \gamma^{k_{21}} = \gamma^2 = \omega^{40}$, $\alpha_{22} = \gamma^{k_{22}} = \gamma^3 = \omega^{60}$. For $\alpha = \sum_{i_1=1}^{2} \sum_{i_2=1}^{2} \eta_{i_1 i_2} \alpha_{i_1 i_2}$, let $\mathcal{C} = \eta_{11}\mathcal{C}_{11} \oplus \eta_{12}\mathcal{C}_{12} \oplus \eta_{21}\mathcal{C}_{21} \oplus \eta_{22}\mathcal{C}_{22}$ be an α-constacyclic code length $n = 5$ over $\mathcal{T}$ such $\mathcal{C}_{i_1 i_2} = \langle f_{i_1 i_2}(y)\rangle$. Let

$$M = \begin{bmatrix} \alpha_{11}^{-k_{11}} & \alpha_{12}^{-k_{11}} & \alpha_{21}^{-k_{11}} & \alpha_{22}^{-k_{11}} \\ \alpha_{11}^{-k_{12}} & \alpha_{12}^{-k_{12}} & \alpha_{21}^{-k_{12}} & \alpha_{22}^{-k_{12}} \\ \alpha_{11}^{-k_{21}} & \alpha_{12}^{-k_{21}} & \alpha_{21}^{-k_{21}} & \alpha_{22}^{-k_{21}} \\ \alpha_{11}^{-k_{22}} & \alpha_{12}^{-k_{22}} & \alpha_{21}^{-k_{22}} & \alpha_{22}^{-k_{22}} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \gamma^{-1} & \gamma^{-2} & \gamma^{-3} \\ 1 & \gamma^{-2} & \gamma^{-4} & \gamma^{-6} \\ 1 & \gamma^{-3} & \gamma^{-6} & \gamma^{-9} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \gamma^3 & \gamma^2 & \gamma \\ 1 & \gamma^2 & 1 & \gamma^2 \\ 1 & \gamma & \gamma^2 & \gamma^3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega^{60} & \omega^{40} & \omega^{20} \\ 1 & \omega^{40} & 1 & \omega^{40} \\ 1 & \omega^{20} & \omega^{40} & \gamma^{60} \end{bmatrix}.$$

Then the Gray image of $\mathcal{C}$ under the polynomial Gray may, $\varphi(\mathcal{C})$ is a cyclic code of length 20 over $\mathbb{F}_{3^4}$ generated by $f_{11}(y) f_{12}(y) f_{21}(y) f_{22}(y)$.

Let n be positive integer and $q = p^e$ be a prime power such that $\gcd(n, q) = 1$. Further, let γ be sth root of unity. Then, there exists a primitive snth root of unity

ω in some extension field of $\mathbb{F}_{q^2}$ such that $\omega^n = \gamma$. Therefore,

$$y^n - \gamma = \prod_{k=0}^{n-1}(y - \omega^{1+sj}).$$

Let $\Omega = \{1 + ks | 0 \leq k \leq n-1\}$. For each $i \in \Omega$, let C_i be the q^2-cyclotomic coset modulo sn containing i, i.e.,

$$C_i = \{i, iq^2, iq^4, \ldots, iq^{2(m_i-1)}\},$$

where m_i is the smallest positive integer such that $iq^{2m_i} \equiv i \pmod{sn}$. Let $\mathcal{C}$ be a γ-constacyclic code of length n over $\mathbb{F}_{q^2}$ such $\mathcal{C} = \langle f(y) \rangle$. Define $Z = \{i \in \Omega | g(\omega^i) = 0\}$ to be the defining set of $\mathcal{C}$. Obviously, the defining set of $\mathcal{C}$ must be a union of some q^2-cyclotomic cosets modulo sn and $\dim(\mathcal{C}) = n - |Z|$.

Lemma 6.1.6. (BCH type bound of constacyclic codes [26]) Assume that $\gcd(n, q) = 1$. Let $\mathcal{C}$ be a γ-constacyclic code code of length n over $\mathbb{F}_{q^2}$ generated by $f(y)$. Furthermore, let $\{\omega^{1+sk} | 0 \leq k \leq d-2\}$ be the set of roots of $f(y)$, where ω is a primitive snth root of unity. Then the minimum Hamming distance of $\mathcal{C}$ is at least d.

6.2 Construction of EAQECCs

This section deals with the construction of MDS EAQECCs from the constacyclic codes over $\mathcal{T}$. First of all, we recall the definition of EAQECCs, MDS EAQECCs and a few important results on them. Then utilizing these results, we prove our main result. Further, we provide a few illustrative examples to justify our construction. Finally, we conclude this section by enlisting some MDS EAQECCs obtained by this method.

Definition 6.2.1. An EAQECC denoted by $[[n, k, d; c]]_q$ encodes k information qubits with the help of c pairs of maximally entangled states and corrects up to $\lfloor \frac{d-1}{2} \rfloor$ errors, where d is the minimum distance of the code. The performance of an EAQECC is measured by its rate $\frac{k}{n}$ and net rate $\frac{k-c}{n}$.

Suppose that H is an $(n-k) \times n$ parity check matrix of $\mathcal{C}$ over $\mathbb{F}_{q^2}$. Then the Hermitian dual $\mathcal{C}^{\perp_H}$ of $\mathcal{C}$ has an $n \times (n-k)$ generator matrix $H^\dagger$, where $H^\dagger$ is the conjugate transpose of H over $\mathbb{F}_{q^2}$.

Lemma 6.2.2. [21, 96] Let $\mathcal{C}$ be an $[n, k, d]_{q^2}$ classical linear code over $\mathbb{F}_{q^2}$ and H be its parity check matrix. An $[[n, 2k-n+c, d; c]]_q$ EAQECC can be obtained, where $c = \text{rank}(HH^\dagger)$ is the required number of maximally entangled states and $H^\dagger$ is the conjugate transpose matrix of H over $\mathbb{F}_{q^2}$.

Lemma 6.2.3. [26] Let $\beta \in \mathbb{F}_{q^2}^*$ be a primitive lth root of unity and $\mathcal{C}$ be a β-constacyclic code of length n with defining set Z. Suppose that $Z_1 = Z \cap (-qZ)$ and $Z_2 = Z \setminus Z_1$, where $-qZ = \{ln - qx | x \in Z\}$, l is a factor of $q+1$. Then, $Z = Z_1 \cup Z_2$ is called a decomposition of the defining set of $\mathcal{C}$.

Lemma 6.2.4. [26] Let $\mathcal{C}$ be a β-constacyclic code of length n over $\mathbb{F}_{q^2}$, where $\gcd(n, q) = 1$. Suppose that Z is the defining set of $\mathcal{C}$ and $Z = Z_1 \cup Z_2$ is called a decomposition of Z. Then, the number of required entangled states is $c = |Z_1|$.

Lemma 6.2.5. [59] Let $\mathcal{C}$ be a β-constacyclic code with defining set Z. If $Z = Z_1 \cup Z_2$, then $-qZ_1 = Z_1$ and $-qZ_2 \cap Z_2 = \emptyset$.

For an $[n, k, d]$ linear code over $\mathbb{F}_q$, the well-known Singleton bound states that $k \leq n - d + 1$. If the equality $k = n - d + 1$ holds, then the code is called a maximum distance separable (MDS) code. Moreover, the singleton bound for EAQECCs is given below.

Lemma 6.2.6. [21] Let $\mathcal{C}$ be an $[[n,k,d;c]]_q$ EAQECC, where $d \leq \frac{n+2}{2}$. Then, $2(d-1) \leq n-k+c$. If $2(d-1) = n-k+c$, then it is called an MDS EAQECC.

Let ω be a primitive element of $\mathbb{F}_{q^2}$. For a divisor $L = l_1 l_2 \dots l_r$ of q^2-1, let $\gamma = \omega^{\frac{q^2-1}{L}}$ is a primitive Lth root of unity. Let $n = \frac{q^2-1}{s}$, where s is a positive integer. Then

$$y^n - \gamma^j = \prod_{k=0}^{n-1} (y - \gamma^{\frac{s}{L}(j+Lk)}),$$

$j = 0, 1, \dots, L-1$. Let

$$f_{i_1 i_2 \dots i_r} = (y - \gamma^{\frac{s}{L}(k_{i_1 i_2 \dots i_r} + La)})(y - \gamma^{\frac{s}{L}(k_{i_1 i_2 \dots i_r} + Lb)}),$$

$0 \leq a \leq b \leq n-1$, and $\mathcal{C}_{i_1 i_2 \dots i_r} = \langle f_{i_1 i_2 \dots i_r}(y) \rangle,\ i_j \in \{1, 2, \dots, l_j\},\ j = 1, 2, \dots, r.$

Now we state and prove our main result.

Theorem 6.2.7. Let $\mathcal{C} = \bigoplus_{i_1 i_2 \dots i_r} \eta_{i_1 i_2 \dots i_r} \mathcal{C}_{i_1 i_2 \dots i_r}$ be an α-constacyclic code of length n over $\mathcal{T}$ such that $\mathcal{C}_{i_1 i_2 \dots i_r} = \langle f_{i_1 i_2 \dots i_r}(y) \rangle$ is a $\alpha_{i_1 i_2 \dots i_r}$-constacyclic code over $\mathbb{F}_{q^2}$, for $i_j \in \{1, 2, \dots, l_j\},\ j = 1, 2, \dots, r$. Furthermore, let Z be the defining set of $\varphi(\mathcal{C})$ and $Z_{i_1 i_2 \dots i_r} = Z_{i_1 i_2 \dots i_r, 1} \cup Z_{i_1 i_2 \dots i_r, 2}$ be the defining set of $\mathcal{C}_{i_1 i_2 \dots i_r}$, where

$$Z_{i_1 i_2 \dots i_r, 1} = \{C_d | (-qC_d) \equiv C_d \pmod{Ln}, k_{i_1 i_2 \dots i_r} + La \leq d \leq k_{i_1 i_2 \dots i_r} + Lb\},$$
$$Z_{i_1 i_2 \dots i_r, 2} = \{C_e | (-qC_e) \pmod{Ln} \cap C_e = \emptyset, k_{i_1 i_2 \dots i_r} + La \leq d \leq k_{i_1 i_2 \dots i_r} + Lb\},$$

$i_j \in \{1, 2, \dots, l_j\},\ j = 1, 2, \dots, r$. Then, there exists a class of MDS EAQECCs with parameters

$$\left[\left[l_1 l_2 \dots l_r n,\ l_1 l_2 \dots l_r n - 2|Z| + \sum_{i_1, i_2, \dots, i_r} c_{i_1 i_2 \dots i_r},\ |Z|; \sum_{i_1, i_2, \dots, i_r} c_{i_1 i_2 \dots i_r} \right]\right]_q,$$

where $c_{i_1i_2\ldots i_r} = |Z_{i_1i_2\ldots i_r,1}|$ for $i_j \in \{1,2,\ldots,l_j\}$, $j = 1,2,\ldots,r$ and $l_1l_2\ldots l_rn - 2|Z| + \sum_{i_1,i_2,\ldots,i_r} c_{i_1i_2\ldots i_r} \geq 0$.

Proof. Note that $\mathcal{C}_{i_1i_2\ldots i_r} = \langle f_{i_1i_2\ldots i_r}(y)\rangle$, $\Omega_{i_1i_2\ldots i_r} = \{1 + S_{i_1i_2\ldots i_r}k \mid 0 \leq k \leq n-1\}$, $Z_{i_1i_2\ldots i_r} = \{k_{i_1i_2\ldots i_r} \in \Omega_{i_1i_2\ldots i_r} | \gamma^{k_{i_1i_2\ldots i_r}} \text{ is a root of } f_{i_1i_2\ldots i_r(y)}\}$ and $\varphi(\mathcal{C}) = \langle \prod_{i_1i_2\ldots i_r} f_{i_1i_2\ldots i_r}(y)\rangle$. Then

$$\begin{aligned} Z &= \cup_{i_1i_2\ldots i_r} Z_{i_1i_2\ldots i_r} \\ &= \cup_{i_1i_2\ldots i_r}(Z_{i_1i_2\ldots i_r,1} \cup Z_{i_1i_2\ldots i_r,2}) \\ &= (\cup_{i_1i_2\ldots i_r} Z_{i_1i_2\ldots i_r,1}) \cup (\cup_{i_1i_2\ldots i_r} Z_{i_1i_2\ldots i_r,2}) \\ &= \bar{Z}_1 \cup \bar{Z}_2, \end{aligned}$$

which implies that $\bar{Z}_1 = \cup_{i_1i_2\ldots i_r} Z_{i_1i_2\ldots i_r,1}$, $\bar{Z}_2 = \cup_{i_1i_2\ldots i_r} Z_{i_1i_2\ldots i_r,2}$ and $Z = \bar{Z}_1 \cup \bar{Z}_2$, $c = \sum_{i_1,i_2,\ldots,i_r} c_{i_1i_2\ldots i_r}$, where $c_{i_1i_2\ldots i_r} = |Z_{i_1i_2\ldots i_r,1}|$ for $i_j \in \{1,2,\ldots,l_j\}$, $j = 1,2,\ldots,r$. From Lemma, $\varphi(\mathcal{C})$ is a cyclic code with parameters $[l_1l_2\ldots l_rn, l_1l_2\ldots l_rn-2|Z|, |Z|, |Z|+1]$ and it satisfies $|Z|+1 = l_1l_2\ldots l_rn-(l_1l_2\ldots l_rn-|Z|)+1$. Therefore, $\varphi(\mathcal{C})$ is MDS. Hence, using Lemmas and Theorem, we can construct a class of EAQECCs with parameters $\left[\left[l_1l_2\ldots l_rn, l_1l_2\ldots l_rn - 2|Z| + \sum_{i_1,i_2,\ldots,i_r} c_{i_1i_2\ldots i_r}, |Z|; \sum_{i_1,i_2,\ldots,i_r} c_{i_1i_2\ldots i_r}\right]\right]_q$, where $c_{i_1i_2\ldots i_r} = |Z_{i_1i_2\ldots i_r,1}|$ for $i_j \in \{1,2,\ldots,l_j\}$, $j = 1,2,\ldots,r$ and $l_1l_2\ldots l_rn - 2|Z| + \sum_{i_1,i_2,\ldots,i_r} c_{i_1i_2\ldots i_r} \geq 0$. □

Example 6.2.8. Continuing the Example 6.1.5, consider the factorizations of $y^5 - \gamma$, $y^5 - \gamma^2$, $y^5 - \gamma^3$, $y^5 - \gamma^4 = y^5 - 1$ in $\mathbb{F}_{3^4}[y]$ as:

$$\begin{aligned} y^5 - \gamma &= (y - \omega^{4\times1})(y - \omega^{4\times5})(y - \omega^{4\times9})(y - \omega^{4\times13})(y - \omega^{4\times17}) \\ &= (y - \omega^4)(y - \omega^{20})(y - \omega^{36})(y - \omega^{52})(y - \omega^{68}) \\ y^5 - \gamma^2 &= (y - \omega^{4\times2})(y - \omega^{4\times6})(y - \omega^{4\times10})(y - \omega^{4\times14})(y - \omega^{4\times18}) \\ &= (y - \omega^8)(y - \omega^{24})(y - \omega^{40})(y - \omega^{56})(y - \omega^{72}) \end{aligned}$$

$$\begin{aligned} y^5-\gamma^3 &= (y-\omega^{4\times 3})(y-\omega^{4\times 7})(y-\omega^{4\times 11})(y-\omega^{4\times 15})(y-\omega^{4\times 19}) \\ &= (y-\omega^{12})(y-\omega^{28})(y-\omega^{44})(y-\omega^{60})(y-\omega^{76}) \\ y^5-\gamma^4 = y^5-1 &= (y-\omega^{4\times 4})(y-\omega^{4\times 8})(y-\omega^{4\times 12})(y-\omega^{4\times 16})(y-\omega^{4\times 20}) \\ &= (y-\omega^{16})(y-\omega^{32})(y-\omega^{48})(y-\omega^{64})(y-\omega) \end{aligned}$$

Let

$$\begin{aligned} f_{11}(y) &= y-\omega^{32} \\ f_{12}(y) &= (y-\omega^{4})(y-\omega^{20}) \\ f_{21}(y) &= (y-\omega^{24})(y-\omega^{40}) \\ f_{22}(y) &= (y-\omega^{60})(y-\omega^{76}) \end{aligned}$$

Let $\mathcal{C}_{i_1 i_2} = \langle f_{i_1 i_2}(y) \rangle$ for $i_1 = 1, 2,\ i_2 = 1, 2$. Then,

$$\begin{aligned} &Z_{11,1} = \{8\},\ Z_{11,2} = \emptyset; \\ &Z_{12,1} = \emptyset,\ Z_{12,2} = \{1, 5\}; \\ &Z_{21,1} = \{6\},\ Z_{21,2} = \{9\}; \\ &Z_{22,1} = \emptyset,\ Z_{22,2} = \{15, 19\}. \end{aligned}$$

Therefore,

$$\begin{aligned} c &= c_{11} + c_{12} + c_{21} + c_{22} \\ &= |Z_{11,1}| + |Z_{12,1}| + |Z_{21,1}| + |Z_{22,1}| \\ &= 1 + 0 + 1 + 0 = 2 \end{aligned}$$

and $|Z| = 9$. Hence, by Theorem 6.2.7, there exists an EAQECC with parameters $[[20, 8, 7; 2]]_9$.

Corollary 6.2.9. Let $\mathcal{C} = \bigoplus_{i_1 i_2 \ldots i_r} \eta_{i_1 i_2 \ldots i_r} \mathcal{C}_{i_1 i_2 \ldots i_r}$ be an α-constacyclic code of length n over $\mathcal{T}$ such that $\mathcal{C}_{i_1 i_2 \ldots i_r} = \langle f_{i_1 i_2 \ldots i_r}(y) \rangle$ is a $\alpha_{i_1 i_2 \ldots i_r}$-constacyclic code over $\mathbb{F}_{q^2}$, for $i_j \in \{1, 2, \ldots, l_j\}$, $j = 1, 2, \ldots, r$. If $L = l_1 l_2 \ldots l_r$ is the smallest positive integer such that $-qC_L \equiv C_L \pmod{Ln}$, then there exists a class of MDS EAQECCs with parameters $[[Ln, Ln - c(2L-1), cL+1; c]]_q$, where $1 \leq c \leq n$ and $Ln - c(2L-1) \geq 0$.

Example 6.2.10. Let $q = 7$, $n = 8$ and $\mathcal{T} = \mathbb{F}_{q^2}[u_1, u_2]/\langle u_1^3 - u_1, u_2^2 - u_2, u_1 u_2 - u_2 u_1 \rangle$. Since $-7C_6 \equiv C_6 \pmod{48}$ and $L = 6$ is the smallest positive integer satisfying this condition, by Corollary 6.2.9, there exists a class of MDS EAQECCs with parameters $[[48, 48 - 11c, 6c + 1; c]]_7$, where $1 \leq c \leq 4$.

TABLE 6.1: MDS EAQECCs constructed from Corollary 6.2.9

Ring	q	n	L	MDS EAQECCs	c
$\mathbb{F}_{q^2}[u_1,u_2,u_3]/\langle u_1^2-u_1, u_2^2-u_2, u_3^2-1, u_iu_j-u_iu_i\rangle$	5	6	8	$[[40, 40-15c, 8c+1; c]]_5$	$1 \leq c \leq 2$
$\mathbb{F}_{q^2}[u_1,u_2]/\langle u_1^3-u_1, u_2^2-u_2, u_1u_2-u_2u_1\rangle$	7	8	6	$[[48, 48-11c, 6c+1; c]]_7$	$1 \leq c \leq 4$
$\mathbb{F}_{q^2}[u_1,u_2]/\langle u_1^3-u_1, u_2^3-u_2, u_1u_2-u_2u_1\rangle$	7	8	9	$[[72, 72-17c, 9c+1; c]]_7$	$1 \leq c \leq 4$
$\mathbb{F}_{q^2}[u_1,u_2,u_3]/\langle u_1^3-1, u_2^2-u_2, u_2^2-1, u_iu_j-u_iu_i\rangle$	7	6	12	$[[72, 72-23c, 12c+1; c]]_7$	$1 \leq c \leq 3$
$\mathbb{F}_{q^2}[u_1,u_2,u_3]/\langle u_1^3-1, u_2^3-u_2, u_2^2-1, u_iu_j-u_iu_i\rangle$	7	8	18	$[[144, 144-35c, 18c+1; c]]_7$	$1 \leq c \leq 4$
$\mathbb{F}_{q^2}[u_1,u_2]/\langle u_1^3-u_1, u_2^2-u_2, u_1u_2-u_2u_1\rangle$	11	12	6	$[[72, 72-11c, 6c+1; c]]_{11}$	$1 \leq c \leq 6$
$\mathbb{F}_{q^2}[u_1,u_2,u_3]/\langle u_1^2-u_1, u_2^2-u_2, u_3^2-1, u_iu_j-u_iu_i\rangle$	13	14	8	$[[112, 112-15c, 8c+1; c]]_{13}$	$1 \leq c \leq 7$
$\mathbb{F}_{q^2}[u_1,u_2]/\langle u_1^3-u_1, u_2^2-u_2, u_1u_2-u_2u_1\rangle$	19	20	6	$[[120, 120-11c, 6c+1; c]]_{19}$	$1 \leq c \leq 10$
$\mathbb{F}_{q^2}[u_1,u_2]/\langle u_1^3-u_1, u_2^3-u_2, u_1u_2-u_2u_1\rangle$	19	10	9	$[[90, 90-17c, 9c+1; c]]_{19}$	$1 \leq c \leq 5$
$\mathbb{F}_{q^2}[u_1,u_2,u_3]/\langle u_1^3-1, u_2^2-u_2, u_2^2-1, u_iu_j-u_iu_i\rangle$	19	20	12	$[[240, 240-23c, 12c+1; c]]_{19}$	$1 \leq c \leq 10$
$\mathbb{F}_{q^2}[u_1,u_2,u_3]/\langle u_1^3-1, u_2^3-u_2, u_2^2-1, u_iu_j-u_iu_i\rangle$	19	20	18	$[[360, 360-35c, 18c+1; c]]_{19}$	$1 \leq c \leq 10$

TABLE 6.2: Comparison with existing MDS EAQECCs

q	n	L	New MDS EAQECCs	Net rate	EAQECCs	Net Rate
7^2	10	4	$[[40, 33, 5; 1]]_{7^2}$	0.80	$[[40, 26, 5; 14]]_{7^2}$ [45]	0.30
7^2	10	4	$[[40, 26, 9; 2]]_{7^2}$	0.60	$[[40, 26, 5; 14]]_{7^2}$ [45]	0.30
13^2	10	5	$[[50, 41, 6; 1]]_{13^2}$	0.80	$[[50, 23, 4; 21]]_{13^2}$ [61]	0.04
13^2	10	5	$[[50, 41, 6; 1]]_{13^2}$	0.80	$[[50, 24, 4; 20]]_{13^2}$ [61]	0.08
13^2	10	5	$[[50, 41, 6; 1]]_{13^2}$	0.80	$[[50, 36, 4; 14]]_{13^2}$ [62]	0.44

****