Constacyclic and Quasi-Twisted Hermitian Self-Dual Codes over Finite Fields*

Ekkasit Sangwisut[a], Somphong Jitman[b,†] and Patanee Udomkavanich[c]

[a]Department of Mathematics and Statistics, Faculty of Science, Thaksin University, Phatthalung Campus, Phatthalung 93110, Thailand

[b]Department of Mathematics, Faculty of Science, Silpakorn University, Nakhon Pathom 73000, Thailand

[c]Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Bangkok 10330, Thailand

Abstract

Constacyclic and quasi-twisted Hermitian self-dual codes over finite fields are studied. An algorithm for factorizing $x^n - \lambda$ over $\mathbb{F}_{q^2}$ is given, where λ is a unit in $\mathbb{F}_{q^2}$. Based on this factorization, the dimensions of the Hermitian hulls of λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$ are determined. The characterization and enumeration of constacyclic Hermitian self-dual (resp., complementary dual) codes of length n over $\mathbb{F}_{q^2}$ are given through their Hermitian hulls. Subsequently, a new family of MDS constacyclic Hermitian self-dual codes over $\mathbb{F}_{q^2}$ is introduced.

As a generalization of constacyclic codes, quasi-twisted Hermitian self-dual codes are studied. Using the factorization of $x^n - \lambda$ and the Chinese Remainder Theorem, quasi-twisted codes can be viewed as a product of linear codes of shorter length some over extension fields of $\mathbb{F}_{q^2}$. Necessary and sufficient conditions for quasi-twisted codes to be Hermitian self-dual are given. The enumeration of such self-dual codes is determined as well.

1 Introduction

Quasi-twisted (QT) codes, introduced in [4], play an important role in coding theory since they contain remarkable classes of codes such as quasi-cyclic (QC) codes, constacyclic codes, and cyclic codes. In [8], [15] and [20], it has been shown that QT and QC codes meet a modified version of the Gilbert-Vashamov bound. Various codes with good parameters and some optimal codes over finite fields have been obtained from the classes of QT and QC codes (see [9], [1], [5] and [2]). Moreover, there is a link between QC codes and convolution codes in [11] and [28].

Constacyclic codes are an important subclass of QT codes due to their nice algebraic structures and various applications in engineering [3], [10] and [6]. Such codes are optimal in some cases (see, [29], [7], [17], [10] and [14]). These motivate the study of constacyclic codes in [13], [3], [29], [6], [24] and [18].

Self-dual codes are another interesting class of codes due to their fascinating links to other objects and their wide applications [23] and [25]. Both Euclidean and Hermitian self-dual codes are also closely related to quantum stabilizer codes [16]. In [19], [21], [22] and [12], QT and QC codes have been decomposed into a product of linear codes of shorter length and the Euclidean duals of such codes have been determined via this decomposition. Consequently, the characterization of QT and QC Euclidean self-dual codes have been given. In some cases, the enumeration of such codes has been established as well.

To the best of our knowledge, only few works have been done on Hermitian duals of constacyclic and QT codes. In [29], a characterization of Hermitian duals of constacyclic Hermitian self-dual

*This research is supported by the Thailand Research Fund under Research Grant TRG5780065.
†Corresponding author.

codes has been established but not an enumeration. It is therefore of natural interest to characterize and enumerate constacyclic and QT codes with Hermitian self-duality.

Our goal is to study constacyclic and QT codes and their duals with respect to the Hermitian inner product which are defined over a finite field whose cardinality is square. Throughout the paper, we are therefore assume that the cardinality of a field is square and the notation $\mathbb{F}_{q^2}$ will be used.

For a nonzero $\lambda \in \mathbb{F}_{q^2}$, let $o_{q^2}(\lambda)$ denote the order of λ in the multiplicative group $\mathbb{F}_{q^2}^{\times} := \mathbb{F}_{q^2} \setminus \{0\}$. In [29, Proposition 2.3], it has been shown that the Hermitian dual of a λ-constacyclic code is also λ-constacyclic if and only if $o_{q^2}(\lambda)|(q+1)$. Later, in Proposition 6.2, we show that the Hermitian dual of a (λ, ℓ)-QT code over $\mathbb{F}_{q^2}$ is again (λ, ℓ)-QT if and only if $o_{q^2}(\lambda)|(q+1)$. To study constacyclic and QT Hermitian self-dual codes, it suffices to restrict the study to the case where $o_{q^2}(\lambda)|(q+1)$. For $\lambda \in \{1, -1\}$ (or equivalently, $o_{q^2}(\lambda) \in \{1, 2\}$), λ-constacyclic Hermitian self-dual codes have been studied in [26]. In this paper, we give the characterization and enumeration of λ-constacyclic Hermitian self-dual codes of any length n and over $\mathbb{F}_{q^2}$ for every nonzero $\lambda \in \mathbb{F}_{q^2}$ such that $o_{q^2}(\lambda)|(q + 1)$. Subsequently, the characterization and enumeration of QT Hermitian self-dual codes of length $n\ell$ over $\mathbb{F}_{q^2}$ are given in the case where $\gcd(q, n) = 1$.

The paper is organized as follows. In Section 2, some preliminary concepts and proofs of some basic results are discussed. An algorithm for explicit factorization of $x^n - \lambda$ over $\mathbb{F}_{q^2}$ which is key to study constacyclic and QT codes is given in Section 3. In Section 4, the characterization of the Hermitian hulls of constacyclic codes of any length n over $\mathbb{F}_{q^2}$ is given. Subsequently, necessary and sufficient conditions for constacyclic codes of length n over $\mathbb{F}_{q^2}$ to be Hermitian self-dual (resp., Hermitian complementary dual) are determined together with the number of such codes. A new family of MDS constacyclic Hermitian self-dual codes over $\mathbb{F}_{q^2}$ is introduced in Section 5. The decomposition for quasi-cyclic codes is generalized to the case of quasi-twisted codes in Section 6. The number of (λ, ℓ)-QT Hermitian self-dual codes of length $n\ell$ over $\mathbb{F}_{q^2}$ is also determined

2 Preliminaries

In this section, we recall some basic properties of codes and polynomials over finite fields.

Let $\mathbb{F}_{q^2}$ denote a finite field of order q^2. For a positive integer n, denote by $\mathbb{F}_{q^2}^n$ the vector space of all vectors of length n over $\mathbb{F}_{q^2}$. A *linear code* C of length n and dimension k over $\mathbb{F}_{q^2}$ is a k-dimensional subspace of $\mathbb{F}_{q^2}^n$. A linear code C over $\mathbb{F}_{q^2}$ is said to have parameters $[n, k, d]$ if C is of length n, dimension k, and minimum Hamming distance $d = \min\{\omega(\mathbf{c}) \mid \mathbf{0} \neq \mathbf{c} \in C\}$, where $\omega(\mathbf{c})$ denotes the Hamming weight of $\mathbf{c}$. The parameters of every $[n, k, d]$ linear code satisfy the Singleton bound

$$k \leq n - d + 1.$$

An $[n, k, d]$ linear code over $\mathbb{F}_{q^2}$ is said to be a *maximum distance separable (MDS) code* if $k = n - d + 1$.

For a linear code C over $\mathbb{F}_{q^2}$, the Euclidean dual $C^{\perp_E}$ of C is defined under the *Euclidean inner product*

$$\langle \mathbf{a}, \mathbf{b} \rangle_E := \sum_{i=0}^{n-1} a_i b_i,$$

where $\mathbf{a} = (a_0, \ldots, a_{n-1}), \mathbf{b} = (b_0, \ldots, b_{n-1}) \in \mathbb{F}_{q^2}^n$. A code C is said to be *Euclidean self-dual* if $C = C^{\perp_E}$.

The *Hermitian dual* $C^{\perp_H}$ of C is defined under the *Hermitian inner product*

$$\langle \mathbf{a}, \mathbf{b} \rangle_H := \sum_{i=0}^{n-1} a_i b_i^q,$$

where $\mathbf{a} = (a_0, \ldots, a_{n-1})$, $\mathbf{b} = (b_0, \ldots, b_{n-1}) \in \mathbb{F}_{q^2}^n$. The *Hermitian hull* of C is defined to be $Hull_H(C) = C \cap C^{\perp_H}$. A linear code C is said to be *Hermitian self-dual* (resp., *Hermitian complementary dual*) if $C = Hull_H(C) = C^{\perp_H}$ (resp., $Hull_H(C) = \{0\}$). The Euclidean hull of a linear code C is defined in the same fasion and studied in [26].

2.1 Constacyclic Codes

Given a nonzero $\lambda \in \mathbb{F}_{q^2}$, a linear code C of length n over $\mathbb{F}_{q^2}$ is said to be *constacyclic*, or specifically, *λ-constacyclic* if for each $(c_0, c_1, \ldots, c_{n-1}) \in C$, the vector $(\lambda c_{n-1}, c_0, \ldots, c_{n-2})$ is again a codeword in C. A λ-constacyclic code is called *cyclic* and *negacyclic* if $\lambda = 1$ and $\lambda = -1$, respectively. It is well known (see, for example, [29]) that every λ-constacyclic code C of length n over $\mathbb{F}_{q^2}$ can be identified with an ideal in $\mathbb{F}_{q^2}[x]/\langle x^n - \lambda\rangle$ generated by a unique monic divisor of $x^n - \lambda$. Such a polynomial is called the *generator polynomial* of C.

Given a polynomial $f(x) = a_0 + a_1x + \ldots + a_kx^k \in \mathbb{F}_{q^2}[x]$ with nonzeros a_0 and a_k, denote by $f^\dagger(x) := a_0^{-q} \sum_{i=0}^{k} a_i^q x^{k-i}$ the *conjugate-reciprocal polynomial* of $f(x)$. The polynomial $f(x)$ is said to be *self-conjugate-reciprocal* if $f(x) = f^\dagger(x)$. Otherwise, $f(x)$ and $f^\dagger(x)$ are called a *conjugate-reciprocal polynomial pair*.

Let $g(x)$ be the generator polynomial of a λ-constacyclic code C of length n over $\mathbb{F}_{q^2}$ and let $h(x) = \frac{x^n-\lambda}{g(x)}$. Then $h^\dagger(x)$ is a monic divisor of $x^n - \lambda$ and it is the generator polynomial of $C^{\perp_H}$ (see [29, Lemma 2.1]). Therefore, C is Hermitian self-dual if and only if $g(x) = h^\dagger(x)$. By [26, Theorem 1], $Hull_H(C)$ is generated by $\mathrm{lcm}(g(x), h^\dagger(x))$.

2.2 Quasi-Twisted Codes

View a codeword in a linear code C of length $n\ell$ over $\mathbb{F}_{q^2}$ as an $n\times\ell$ matrix over $\mathbb{F}_{q^2}$. Given a nonzero $\lambda \in \mathbb{F}_{q^2}$, a linear code C of length $n\ell$ over $\mathbb{F}_{q^2}$ is said to be *(λ,ℓ)-quasi-twisted ((λ,ℓ)-QT) of length $n\ell$ over $\mathbb{F}_{q^2}$* if for each

$$\mathbf{c} = \begin{bmatrix} c_{00} & c_{01} & \cdots & c_{0,\ell-1} \\ c_{10} & c_{11} & \cdots & c_{1,\ell-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n-1,0} & c_{n-1,1} & \cdots & c_{n-1,\ell-1} \end{bmatrix} \in C,$$

the vector

$$\mathbf{c}' = \begin{bmatrix} \lambda c_{n-1,0} & \lambda c_{n-1,1} & \cdots & \lambda c_{n-1,\ell-1} \\ c_{00} & c_{01} & \cdots & c_{0,\ell-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n-2,0} & c_{n-2,1} & \cdots & c_{n-2,\ell-1} \end{bmatrix}$$

is again a codeword in C. We define an action $T_{\lambda,\ell}$ on the codewords as $T_{\lambda,\ell}(\mathbf{c}) = \mathbf{c}'$. Then every (λ,ℓ)-QT code is invariant as a subspace under the action $T_{\lambda,\ell}$.

Let $R := \mathbb{F}_{q^2}[x]/\langle x^n - \lambda\rangle$. Define a map $\psi : \mathbb{F}_{q^2}^{n\ell} \to R^\ell$ by

$$\psi(\mathbf{c}) = \begin{bmatrix} c_0(x) \\ c_1(x) \\ \vdots \\ c_{\ell-1}(x) \end{bmatrix} = \begin{bmatrix} c_{00} + c_{10}x + \ldots + c_{n-1,0}x^{n-1} \\ c_{01} + c_{11}x + \ldots + c_{n-1,1}x^{n-1} \\ \vdots \\ c_{0,\ell-1} + c_{1,\ell-1}x + \ldots + c_{n-1,\ell-1}x^{n-1} \end{bmatrix}. \tag{2.1}$$

Then the next lemma follows.

Lemma 2.1. The map ψ induces a one-to-one correspondence between the QT-codes of length $n\ell$ over $\mathbb{F}_{q^2}$ and the R-submodules of R^ℓ.

3 The Factorization of $x^n - \lambda$ in $\mathbb{F}_{q^2}[x]$

In this section, we give an algorithm for the factorization of $x^n - \lambda$ in $\mathbb{F}_{q^2}[x]$ which is key to study both the structures of λ-constacyclic and (λ,ℓ)-QT codes.

Let λ be a nonzero element in $\mathbb{F}_{q^2}$ such that $o_{q^2}(\lambda) = r$ and let n be a positive integer written in the form of $n = n'p^\nu$, where $p = \mathrm{char}(\mathbb{F}_{q^2})$, $p \nmid n'$ and $\nu \geq 0$.

Since the map $a \mapsto a^{p^\nu}$ on $\mathbb{F}_{q^2}$ is a power of the Frobenious automorphism of $\mathbb{F}_{q^2}$ over $\mathbb{F}_p$, there is a unique $\Lambda \in \mathbb{F}_{q^2}$ such that $\Lambda^{p^\nu} = \lambda$. Then

$$x^n - \lambda = \left(x^{n'} - \Lambda\right)^{p^\nu}. \tag{3.1}$$

Since an automorphism is order preserving, we have $o_{q^2}(\Lambda) = o_{q^2}(\lambda) = r$. Therefore, it is sufficient to focus on the factorization of $x^{n'} - \Lambda$.

Let k be the smallest integer such that $(n'r)|(q^{2k} - 1)$. Then, there exists a primitive $n'r$th root of ξ in $\mathbb{F}_{q^{2k}}$ such that $\xi^{n'} = \Lambda$, and hence,

$$x^{n'} - \Lambda = x^{n'} - \xi^{n'}. \tag{3.2}$$

It is not dificult to see that $x^{n'} - \xi^{n'}$ divides $x^{n'r} - 1$. Since $x^{n'r} - 1 = \prod_{j|n'r} Q_j(x)$, where

$$Q_j(x) := \prod_{z \in \mathbb{Z}_j^\times} \left(x - \xi^{\left(\frac{n'r}{j}\right)z}\right)$$

is the *jth cyclotomic polynomial* over $\mathbb{F}_{q^2}$ (see [13]) , we have

$$x^{n'} - \xi^{n'} = \gcd\left(\prod_{j|n'r} Q_j(x), x^{n'} - \xi^{n'}\right) = \prod_{j|n'r} \gcd\left(Q_j(x), x^{n'} - \xi^{n'}\right). \tag{3.3}$$

Hence, for each divisor j of $n'r$, $\xi^{\left(\frac{n'r}{j}\right)z}$ is a root of $x^{n'} - \xi^{n'}$ if and only if $\xi^{n'\left(\frac{n'r}{j}\right)z} = \xi^{n'}$, or equivalently, $\left(\frac{n'r}{j}\right)z \equiv 1 \bmod r$. The set of elements in $\mathbb{Z}_{n'r}$ satisfying the preceeding conditions is denoted by

$$S_j := \left\{ \left(\frac{n'r}{j}\right)z \in \mathbb{Z}_{n'r} \;\middle|\; z \in \mathbb{Z}_j^\times, \left(\frac{n'r}{j}\right)z \equiv 1 \bmod r \right\}.$$

In other words, S_j is the set of all s's such that ξ^s is a root of

$$\gcd(Q_j(x), x^{n'} - \xi^{n'}) = \prod_{s \in S_j} (x - \xi^s).$$

It follows that

$$\deg \gcd(Q_j(x), x^{n'} - \xi^{n'}) = |S_j|.$$

For each $j \mid n'r$, necessary and sufficient conditions for S_j to be nonempty are given in the following proposition.

Proposition 3.1. Let j be a positive divisor of $n'r$. Then $S_j \neq \emptyset$ if and only if

$$\gcd\left(\frac{n'r}{j}, r\right) = 1.$$

Proof. Assume that $S_j \neq \emptyset$. Then there exists $\left(\frac{n'r}{j}\right)z \in S_j$. Then $\left(\frac{n'r}{j}\right)z - rm = 1$ for some $m \in \mathbb{N}$. It follows that $\gcd\left(\frac{n'r}{j}, r\right) = 1$.

Conversely, assume that $\gcd\left(\frac{n'r}{j}, r\right) = 1$. Then there exists $w_1 \in \mathbb{Z}_r^\times$ such that $\frac{n'r}{j}w_1 \equiv 1 \bmod r$. Observe that $(rm + w_1)\left(\frac{n'r}{j}\right) \equiv 1 \bmod r$ for all $m \in \mathbb{Z}^+$. By Dirichlet's theorem on arithmetic progressions (see [27]), there exist infinitely many primes of the form $rm + w_1$. Let $m_1 \in \mathbb{Z}^+$ be such that $rm_1 + w_1$ is prime and $rm_1 + w_1 > j$. Hence, we obtain $w = (rm_1 + w_1) \bmod j$ such that $w \in \mathbb{Z}_j^\times$ and $w\left(\frac{n'r}{j}\right) \equiv 1 \bmod r$. Therefore, $S_j \neq \emptyset$ as desired. □

From now on, we focus only on the positive divisors j of $n'r$ such that $S_j \neq \emptyset$, or equivalently, $\gcd\left(\frac{n'r}{j}, r\right) = 1$. The cardinality of S_j is determined in the following lemma.

Lemma 3.2. Let j be a positive divisor of $n'r$ such that $\gcd\left(\frac{n'r}{j}, r\right) = 1$. Then $|S_j| = \frac{\phi(j)}{\phi(r)}$, where ϕ is the Euler's totient function.

Proof. Let H_j be defined by $H_j := \left\{h \in \mathbb{Z}_j^{\times} \mid h \equiv 1 \bmod r\right\}$. We divide the proof into two steps. First, we show that $|S_j| = |H_j|$. Then we determine $|H_j|$.

By Proposition 3.1, we have $S_j \neq \emptyset$. Let $\left(\frac{n'r}{j}\right)w \in S_j$, where $w \in \mathbb{Z}_j^{\times}$. Then there exists $w' \in \mathbb{Z}_j^{\times}$ such that $ww' \equiv 1 \bmod j$.

Let $\Phi : S_j \to H_j$ be defined by $\Phi\left(\left(\frac{n'r}{j}\right)z\right) = w'z$. Since $w'z \equiv w'w\left(\frac{n'r}{j}\right)z \equiv \left(\frac{n'r}{j}\right)z \equiv 1 \bmod r$, we have $w'z \in H_j$. Let $\left(\frac{n'r}{j}\right)z_1 = \left(\frac{n'r}{j}\right)z_2$ in S_j. Then $\left(\frac{n'r}{j}\right)(z_1 - z_2) \equiv 0 \bmod n'r$. Since $j = \frac{n'r}{n'r/j}$, we have $z_1 \equiv z_2 \bmod j$, and hence, $w'z_1 \equiv w'z_2 \bmod j$. Therefore, Φ is well-defined.

Let $z_1, z_2 \in \mathbb{Z}_j^{\times}$ be such that $\Phi\left(\left(\frac{n'r}{j}\right)z_1\right) = \Phi\left(\left(\frac{n'r}{j}\right)z_2\right)$. Then $w'z_1 = w'z_2$ in $\mathbb{Z}_j^{\times}$, *i.e.*, $w'z_1 \equiv w'z_2 \bmod j$. Hence, we have $z_1 \equiv z_2 \bmod j$. It follows that $\left(\frac{n'r}{j}\right)z_1 \equiv \left(\frac{n'r}{j}\right)z_2 \bmod n'r$, and hence, $\left(\frac{n'r}{j}\right)z_1 = \left(\frac{n'r}{j}\right)z_2$ in S_j. Therefore, Φ is injective.

For each $h \in H_j$, we have $\left(\frac{n'r}{j}\right)wh$ in S_j and $\Phi\left(\left(\frac{n'r}{j}\right)wh\right) = w'wh \equiv h \bmod j$. Then Φ is surjective, and hence, it is a bijection. Therefore, $|S_j| = |H_j|$.

By the Fundamental Theorem of Arithmetic, we have $j = p_1^{a_1} \dots p_t^{a_t}$, where $p_1 < p_2 < \cdots < p_t$ are primes and a_i is a positive integer. Since $\gcd(\frac{n'r}{j}, r) = 1$, we have $r|j$. Hence, we can write $r = p_1^{b_1} \dots p_t^{b_t}$, where b_i is non-negative integer and $b_i \leq a_i$ for all $1 \leq i \leq t$. By the Chinese Remainder Theorem,

$$\mathbb{Z}_j^{\times} \cong \mathbb{Z}_{p_1^{a_1}}^{\times} \times \mathbb{Z}_{p_2^{a_2}}^{\times} \times \cdots \times \mathbb{Z}_{p_t^{a_t}}^{\times}$$

and each element in H_j corresponds to $(z_1, \dots, z_t)$ in $H_{p_1^{a_1}} \times \cdots \times H_{p_t^{a_t}}$. Therefore,

$$|H_j| = |H_{p_1^{a_1}}| \cdot |H_{p_2^{a_2}}| \cdots |H_{p_t^{a_t}}|. \tag{3.4}$$

Note that, for each $1 \leq i \leq t$,

$$H_{p^{a_i}} = \left\{z \in \mathbb{Z}_{p^{a_i}}^{\times} \mid z \equiv 1 \bmod p^{b_i}\right\} = \left\{1, 1 + p^{b_i}, 1 + 2p^{b_i}, \dots, 1 + (p^{a_i - b_i} - 1)p^{b}\right\}.$$

Then $|H_{p^{a_i}}| = p^{a_i - b_i} = \frac{p^{a_i}}{p^{b_i}} = \frac{\phi(p^{a_i})}{\phi(p^{b_i})}$.

From (3.4), we conclude that

$$|H_j| = \frac{\phi(p_1^{a_1})}{\phi(p_1^{b_1})} \cdot \frac{\phi(p_2^{a_2})}{\phi(p_2^{b_2})} \cdots \frac{\phi(p_t^{a_t})}{\phi(p_t^{b_t})} = \frac{\phi(j)}{\phi(r)}$$

as desired. □

Therefore, for each divisor j of $n'r$ with $\gcd\left(\frac{n'r}{j}, r\right) = 1$, we have

$$\deg \gcd(Q_j(x), x^{n'} - \xi^{n'}) = \frac{\phi(j)}{\phi(r)}.$$

Let π be a map defined on the pair (j, q^2), where i is a positive integer, by

$$\pi(j, q^2) := \begin{cases} 0 & \text{if } j|(q^{2k} + q) \text{ for some } k \geq 0, \\ 1 & \text{otherwise.} \end{cases}$$

For each positive integer j such that $\gcd(j, q) = 1$, *the order of* q^2 *in the multiplicative group* $\mathbb{Z}_j^{\times}$ is denoted by $ord_j(q^2)$. The following lemma can be obtained by replacing q with q^2 in the proofs of [26, Lemma 3 and Lemma 19].

Lemma 3.3. Let j be a positive integer and let $\mathbb{F}_{q^2}$ be a finite field with $\gcd(j, q) = 1$. The jth cyclotomic polynomial $Q_j(x)$ factors into $\frac{\phi(j)}{ord_j(q^2)}$ distinct monic irreducible polynomials over $\mathbb{F}_{q^2}$ of the same degree $ord_j(q^2)$, where ϕ is the Euler's totient function.

If $\pi(j, q^2) = 0$, then all the irreducible polynomials in the factorization of $Q_j(x)$ are self-conjugate-reciprocal. Otherwise, they form conjugate-reciprocal polynomial pairs.

By Lemma 3.3, $\gcd(Q_j(x), x^{n'} - \xi^{n'})$ can be factored into $\frac{\phi(j)}{\phi(r)ord_j(q^2)}$ distinct monic irreducible polynomials over $\mathbb{F}_{q^2}$ of the same degree $ord_j(q^2)$. In addition,

$$\gcd(Q_j(x), x^{n'} - \xi^{n'}) = \begin{cases} \prod_{i=1}^{\gamma(j)} g_{ij}(x) & \text{if } \pi(j, q^2) = 0, \\ \prod_{i=1}^{\beta(j)} f_{ij}(x) f_{ij}^{\dagger}(x) & \text{otherwise,} \end{cases} \tag{3.5}$$

where

$$\gamma(j) := \frac{\phi(j)}{\phi(r)ord_j(q^2)}, \tag{3.6}$$

$$\beta(j) := \frac{\phi(j)}{2\phi(r)ord_j(q^2)}, \tag{3.7}$$

$f_{ij}(x)$ and $f_{ij}^{\dagger}(x)$ are a monic irreducible conjugate-reciprocal polynomial pair, and $g_{ij}(x)$ is a monic irreducible self-conjugate-reciprocal polynomial.

By (3.1)-(3.3), and (3.5), it can be concluded that

$$\begin{aligned} x^n - \lambda &= \left(x^{n'} - \Lambda\right)^{p^\nu} = \left(x^{n'} - \xi^{n'}\right)^{p^\nu} \\ &= \left(\prod_{j|n'r,\ \gcd\left(\frac{n'r}{j}, r\right)=1} \gcd(Q_j(x), x^{n'} - \xi^{n'}) \right)^{p^\nu} \\ &= \prod_{\substack{j|n'r,\ \gcd\left(\frac{n'r}{j}, r\right)=1 \\ \pi(j,q^2)=0}} \prod_{i=1}^{\gamma(j)} \left(g_{ij}(x)\right)^{p^\nu} \prod_{\substack{j|n'r,\ \gcd\left(\frac{n'r}{j}, r\right)=1 \\ \pi(j,q^2)=1}} \prod_{i=1}^{\beta(j)} \left(f_{ij}(x)\right)^{p^\nu} \left(f_{ij}^{\dagger}(x)\right)^{p^\nu}. \end{aligned} \tag{3.8}$$

For simplicity, let

$$\Omega = \left\{ j \mid n'r \;\middle|\; \gcd\left(\frac{n'r}{j}, r\right) = 1 \text{ and } \pi(j, q^2) = 0 \right\} \tag{3.9}$$

and

$$\Omega' = \left\{ j \mid n'r \;\middle|\; \gcd\left(\frac{n'r}{j}, r\right) = 1 \text{ and } \pi(j, q^2) = 1 \right\}. \tag{3.10}$$

Then (3.8) becomes

$$x^n - \lambda = \prod_{j\in\Omega} \prod_{i=1}^{\gamma(j)} \left(g_{ij}(x)\right)^{p^\nu} \prod_{j\in\Omega'} \prod_{i=1}^{\beta(j)} \left(f_{ij}(x)\right)^{p^\nu} \left(f_{ij}^{\dagger}(x)\right)^{p^\nu}. \tag{3.11}$$

Let $\mathtt{s}$ and $\mathtt{t}$ denote the number of monic irreducible self-conjugate-reciprocal polynomials and the number of monic irredcible conjugate-reciprocal polynomial pairs in the factorization of $x^{n'} - \Lambda$, respectively. Then

$$\mathtt{s} = \sum_{j\in\Omega} \gamma(j) \tag{3.12}$$

and

$$\mathtt{t} = \sum_{j\in\Omega'} \beta(j), \tag{3.13}$$

where γ and β are defined in (3.6) and (3.7), respectively.

Example 3.4. Consider $\mathbb{F}_4 = \left\{0, 1, \alpha, \alpha^2 = \alpha + 1\right\}$. Let $n = 5$. Then $o_4(\alpha) = 3$ and

$$\left\{ j \mid j \text{ is a divisor of 15 and } \gcd\left(\frac{15}{j}, 3\right) = 1 \right\} = \{3, 15\}.$$

Since $\pi(3, 4) = 0$, $\pi(15, 4) = 1$ and $ord_3(4) = 1$ and $ord_{15}(4) = 2$, we have $\gamma(3) = \frac{\phi(3)}{\phi(3)ord_3(4)} = 1 = \beta(4) = \frac{\phi(15)}{2\phi(3)ord_{15}(4)}$. Therefore, by (3.11)-(3.13), the factors of $x^5 - \alpha$ contains $\gamma(3) = 1$ irreducible self-conjugate-reciprocal polynomial of dergree $ord_3(4) = 1$ and $\gamma(5) = 1$ irreducible conjugate-reciprocal polynomial pair of dergree $ord_{15}(4) = 2$.

From the discussion above, we can determine the degrees and the number of self-conjugate-reciprocal polynomials and conjugate-reciprocal polynomial pairs in the factorization of $x^{n'} - \Lambda$ in (3.11). However, we are not yet able to determine the explicit irreducible factors of $x^{n'} - \Lambda$. The following algorithm gives the explicit factors of $x^{n'} - \Lambda$.

A *q^2-cyclotomic coset modulo $n'r$ containing a*, denoted by $S_{q^2}(a)$, is defined to be the set

$$S_{q^2}(a) := \left\{q^{2i} \cdot a \bmod n'r \mid i = 0, 1, \ldots\right\}.$$

Since $\gcd(Q_j(x), x^{n'} - \xi^{n'})$ can be factored as a product of irreducible polynomials in $\mathbb{F}_{q^2}[x]$, S_j is a union of some q^2-cyclotomic cosets modulo $n'r$. Therefore, we conclude the following algorithm.

Algorithm

1. For each $j|n'r$ such that $\gcd\left(\frac{n'r}{j}, r\right) = 1$, find the set S_j.
2. Partition S_j into q^2-cyclotomic cosets modulo $n'r$.
3. Determine $\pi(j, q^2)$.
   (3.1) If $\pi(j, q^2) = 1$, then denote by T_j a set of q^2-cyclotomic cosets of S_j such that $S_{q^2}(a) \in T_j$ if and only if $S_{q^2}(-qa) \notin T_j$. Let $\mathscr{T}_j$ denote a set of representative of q^2-cyclotomic cosets in each q^2-cyclotomic cosets in T_j.
   (3.2) If $\pi(j, q^2) = 0$, let $\mathscr{S}_j$ denote a set of representative of q^2-cyclotomic cosets in S_j.
4. We have
$$x^{n'} - \Lambda = \prod_{a \in \mathscr{S}_j} m_{\xi^a}(x) \prod_{b \in \mathscr{T}_j} m_{\xi^b}(x) m^{\dagger}_{\xi^b}(x).$$

The following example illustrates an application of the algorithm.

Example 3.5. Let $\mathbb{F}_4 = \left\{0, 1, \alpha, \alpha^2 = \alpha + 1\right\}$. Then $o_4(\alpha) = 3$. To factor $x^5 - \alpha$ over $\mathbb{F}_4$, let ξ be a primitive 15th root of unity in $\mathbb{F}_{16}$ such that $\alpha = \xi^5$. Note that all $j|5 \cdot 3$ with $\gcd\left(\frac{15}{j}, 3\right) = 1$ are 3 and 15. Since $\pi(3, 4) = 0$ and $\pi(15, 4) = 1$, we have $S_3 = \left\{5z \,\middle|\, z \in \mathbb{Z}_3^\times, 5z \equiv 1 \bmod 3\right\} = \{10\} = \mathscr{S}_3$ and $S_{15} = \left\{z \,\middle|\, z \in \mathbb{Z}_{15}^\times, z \equiv 1 \bmod 3\right\} = \{1, 4, 7, 13\}$. Partitioning S_{15} into 4-cyclotomic coset modulo 15, we have $S_{15} = \{1, 4\} \cup \{7, 13\}$. Then $T_{15} = \{\{1, 4\}\}$ and $\mathscr{T}_{15} = \{1\}$. Therefore, $x^5 - \alpha$ can be written in term of equation (3.11) as

$$x^5 - \alpha = m_{\xi^{10}}(x)\left(m_\xi(x) m_\xi(x)^\dagger\right) = (x + \alpha^2)(x^2 + x + \alpha)(x^2 + \alpha x + \alpha).$$

4 Hermitian Hull of λ-Constacyclic Codes

In this section, the dimensions of the Hermitian hulls of constacyclic codes of length n over $\mathbb{F}_{q^2}$ are determined via the factorization of $x^n - \lambda$ given in Section 3. The number of constacyclic Hermitian self-dual codes and the number of Hermitian complementary dual constacyclic codes of length n over $\mathbb{F}_{q^2}$ are given as well.

Theorem 4.1. Let $\mathbb{F}_{q^2}$ denote a finite field of order q^2 with characteristic p and let $n = \overline{n}p^\nu$ with $p \nmid \overline{n}$. Then the dimensions of the Hermitian hulls of λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$ are of the form

$$\sum_{j\in\Omega} ord_j(q^2)\cdot \mathsf{a}_j + \sum_{j\in\Omega'} ord_j(q^2)\cdot \mathsf{b}_j, \tag{4.1}$$

where $0 \leq \mathsf{a}_j \leq \gamma(j)\left\lfloor \frac{p^\nu}{2}\right\rfloor$ and $0 \leq \mathsf{b}_j \leq \beta(j)p^\nu$.

Proof. The theorem can be obtained using arguments similar to those in the proof of [26, Theorem 5] by replacing χ with π and q with q^2. □

Next theorem gives a characterization of λ-constacyclic Hermitian self-dual codes in terms of Ω defined in (3.9).

Theorem 4.2. Let $\mathbb{F}_{q^2}$ denote a finite field of order q^2 with characteristic p and let $n = \overline{n}p^\nu$ with $p \nmid \overline{n}$. Let $x^n - \lambda$ be factored as in (3.11). Then there exists a λ-constacyclic Hermitian self-dual code of length n over $\mathbb{F}_{q^2}$ if and only if

1. $\Omega = \emptyset$, or
2. $\Omega \neq \emptyset$ and $p = 2$.

In this case, the generator polynomial of a code is of the form

$$g(x) = \begin{cases} \prod_{j\in\Omega'}\prod_{i=1}^{\beta(j)} \left(f_{ij}(x)\right)^{v_{ij}}\left(f_{ij}^\dagger(x)\right)^{w_{ij}} & \text{if } \Omega = \emptyset,\\ \prod_{j\in\Omega}\prod_{i=1}^{\gamma(j)} \left(g_{ij}(x)\right)^{2^{\nu-1}} \prod_{j\in\Omega'}\prod_{i=1}^{\beta(j)} \left(f_{ij}(x)\right)^{v_{ij}}\left(f_{ij}^\dagger(x)\right)^{w_{ij}} & \text{if } \Omega \neq \emptyset \text{ and } p = 2, \end{cases} \tag{4.2}$$

where $0 \leq v_{ij}, w_{ij} \leq p^\nu$ and $v_{ij} + w_{ij} = p^\nu$.

Proof. Let C be a λ-constacyclic code of length n over $\mathbb{F}_q$ with the generator polynomial $g(x)$. Then, by (3.11), we have

$$g(x) = \prod_{j\in\Omega}\prod_{i=1}^{\gamma(j)} \left(g_{ij}(x)\right)^{u_{ij}} \prod_{j\in\Omega'}\prod_{i=1}^{\beta(j)} \left(f_{ij}(x)\right)^{v_{ij}}\left(f_{ij}^\dagger(x)\right)^{w_{ij}}, \tag{4.3}$$

where $0 \leq u_{ij}, v_{ij}, w_{ij} \leq p^\nu$. It follows that

$$h(x) := \frac{x^n - \lambda}{g(x)} = \prod_{j\in\Omega}\prod_{i=1}^{\gamma(j)} \left(g_{ij}(x)\right)^{p^\nu - u_{ij}} \prod_{j\in\Omega'}\prod_{i=1}^{\beta(j)} \left(f_{ij}(x)\right)^{p^\nu - v_{ij}}\left(f_{ij}^\dagger(x)\right)^{p^\nu - w_{ij}},$$

and hence,

$$h^\dagger(x) = \frac{x^n - \lambda}{g(x)} = \prod_{j\in\Omega}\prod_{i=1}^{\gamma(j)} \left(g_{ij}(x)\right)^{p^\nu - u_{ij}} \prod_{j\in\Omega'}\prod_{i=1}^{\beta(j)} \left(f_{ij}(x)\right)^{p^\nu - w_{ij}}\left(f_{ij}^\dagger(x)\right)^{p^\nu - v_{ij}}.$$

Assume that C is Hermitian self-dual. Then $g(x) = h(x)^\dagger$. By comparing the exponents, we have

$$u_{ij} = p^\nu - u_{ij} \quad \text{and} \quad v_{ij} = p^\nu - w_{ij},$$

and hence, $2u_{ij} = p^\nu$ and $v_{ij} + w_{ij} = p^\nu$. Since $2u_{ij} = p^\nu$, we have $p = 2$ or $\Omega = \emptyset$.

Conversely, assume that $\Omega = \emptyset$, or $\Omega \neq \emptyset$ and $p = 2$. Let $g(x)$ be defined as in (4.2) and $h(x) = \frac{(x^n - \lambda)}{g(x)}$. It is not difficult to see that $g(x) = h^\dagger(x)$, and hence, a constacyclic code generated by $g(x)$ is Hermitian self-dual. □

Corollary 4.3. Let $\mathtt{t}$ be the number of monic irreducible conjugate-reciprocal polynomial pairs as in (3.13). The number of λ-constacyclic Hermitian self-dual codes of length n over $\mathbb{F}_{q^2}$ is

$$\begin{cases} (p^\nu + 1)^{\mathtt{t}} & \text{if } \Omega = \emptyset, \\ (2^\nu + 1)^{\mathtt{t}} & \text{if } \Omega \neq \emptyset \text{ and } p = 2, \\ \quad 0 & \text{if } \Omega \neq \emptyset \text{ and } p \neq 2. \end{cases}$$

In particular, if $\Omega' = \emptyset$ (or equivalently, $\pi(\overline{n}r, q^2) = 0$) and $p = 2$, then there exists a unique λ-constacyclic Hermitian self-dual code. In this case, the generator polynomial is

$$\prod_{j\in\Omega}\prod_{i=1}^{\gamma(j)} \left(g_{ij}(x)\right)^{2^{\nu-1}}.$$

Proof. By Theorem 4.2, the number of generator polynomials of λ-constacyclic Hermitain self-dual codes of length n over $\mathbb{F}_{q^2}$ depends only on v_{ij} and w_{ij} such that $v_{ij}+w_{ij} = p^\nu$ where $0 \le v_{ij}, w_{ij} \le p^\nu$. Then the number of λ-constacyclic Hermitain self-dual codes of length n over $\mathbb{F}_{q^2}$ is $(p^\nu + 1)^t$.

Since the number of generator polynomials of λ-constacyclic Hermitian self-dual codes of length n over $\mathbb{F}_{q^2}$ depends only on v_{ij} and w_{ij}, a unique λ-constacylic Hermitian self-dual code occurs if $\Omega' = \emptyset$ and $p = 2$. It is not difficult to see that $\Omega' = \emptyset$ is equivalent to $\pi(n'r, q^2) = 0$. Therefore, the generator polynomial of the code is

$$\prod_{j\in\Omega}\prod_{i=1}^{\gamma(j)} g_{ij}(x)^{2^{\nu-1}}.$$

□

Necessary and sufficient conditions for constacyclic Hermitian complementary dual codes are given as follows.

Theorem 4.4. Let $\mathbb{F}_{q^2}$ denote a finite field of order q^2 with characteristic p and let $n = \overline{n}p^\nu$ with $p \nmid \overline{n}$. Let C be a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$. Then C is Hermitian complementary dual if and only if its generator polynomial is of the form

$$\prod_{j\in\Omega}\prod_{i=1}^{\gamma(j)} \left(g_{ij}(x)\right)^{u_{ij}} \prod_{j\in\Omega'}\prod_{i=1}^{\beta(j)} \left(f_{ij}(x)\right)^{v_{ij}} \left(f_{ij}^{\dagger}(x)\right)^{w_{ij}},$$

where $u_{ij} \in \{0, p^\nu\}$, and $(v_{ij}, w_{ij}) \in \{(0,0), (p^\nu, p^\nu)\}$.

Proof. In the proof of Theorem 4.2, we have λ-constacyclic codes C and $C^\perp$ of length n over $\mathbb{F}_{q^2}$ generated by $g(x)$ and $h^\dagger(x)$ respectively. Hence, C is a λ-constacyclic Hermitian complementary dual code if and only if $\operatorname{lcm}(g(x), h^\dagger(x)) = x^n - \lambda$ or, equivalently $\max\{u_{ij}, p^\nu - u_{ij}\} = p^\nu$, $\max\{v_{ij}, p^\nu - w_{ij}\} = p^\nu$ and $\max\{w_{ij}, p^\nu - v_{ij}\} = p^\nu$. Thus, $u_{ij} \in \{0, p^\nu\}$, and $(v_{ij}, w_{ij}) \in \{(0,0), (p^\nu, p^\nu)\}$. □

Corollary 4.5. The number of λ-constacyclic Hermitian complementary dual codes of length n over $\mathbb{F}_{q^2}$ is

$$2^{\mathtt{s}+\mathtt{t}},$$

where $\mathtt{s}$ is the number of monic irreducible self-conjugate-reciprocal polynomials and $\mathtt{t}$ is the number of monic irreducible conjugate-reciprocal polynomial pairs as in (3.13).

Proof. From the proof of Theorem 4.4, the number of generator polynomials of λ-constacyclic Hermitain complementary dual codes of length n over $\mathbb{F}_{q^2}$ depend only on $u_{ij} \in \{0, p^\nu\}$ and $(v_{ij}, w_{ij}) \in \{(0,0), (p^\nu, p^\nu)\}$. Then the number of λ-constacyclic Hermitain complementary dual codes of length n over $\mathbb{F}_{q^2}$ is $2^{\mathtt{s}+\mathtt{t}}$. □

5 MDS Constacyclic Hermitian Self-dual Codes over $\mathbb{F}_{q^2}$

In this section, we construct a class of MDS λ-constacyclic Hermitian self-dual codes over $\mathbb{F}_{q^2}$. Throughout this section, let n be an even positive integer relatively prime to q such that $(nr)|(q^2-1)$ and $r|(q+1)$, where $r = o_{q^2}(\lambda)$. Equivalently, $n = n'$ in the previous section.

In [29], a family of MDS constacyclic Hermitian self-dual code over $\mathbb{F}_{q^2}$ whose length is a divisor of $q-1$ is introduced. We now introduce a new family of MDS constacyclic Hermitian self-dual code over $\mathbb{F}_{q^2}$ whose length is a divisor of $q+1$. Therefore, our family is different to a family in [29] if $n \neq 2$.

Let ξ be a primitive nrth root of unity in an extension field $\mathbb{F}_{q^{2k}}$ of $\mathbb{F}_{q^2}$ such that $\xi^n = \lambda$. Then the set of all roots of $x^n - \lambda$ is $\left\{\xi, \xi^{r+1}, \xi^{2r+1}, \ldots, \xi^{(n-1)r+1}\right\}$. Define

$$O_{r,n} = \{1, r+1, 2r+1, \ldots, (n-1)r+1\} = \{ir+1 \mid 0 \leq i \leq n-1\} \subseteq \mathbb{Z}_{nr}.$$

Let C be a λ-constacyclic code. The *roots* of the code C is defined to be the roots of its generator polynomial. The *defining set of λ-constacyclic code* C is defined as

$$T := \left\{ir+1 \in O_{r,n} \mid \xi^{ir+1} \text{ is a root of } C\right\}.$$

It is not difficult to see that $T \subseteq O_{r,n}$ and $\dim C = n - |T|$. The following theorem can be obtained by slightly modified [29, Corollary 3.3].

Theorem 5.1. Let C_T be a λ-constacyclic code with the defining set T. Then

(i) C_T is a Hermitian self-orthogonal constacyclic code if and only if $O_{r,n} \setminus T \subseteq -qT$.

(ii) C_T is a constacyclic Hermitian self-dual code if and only if $-qT = O_{r,n} \setminus T$, or equivalently, $T \cap -qT = \emptyset$.

Proof. Note that $q^2 \equiv 1 \bmod nr$. Then, by [29, Corollary 3.3], C_T is a Hermitian self-orthogonal constacyclic code if and only if $-q\left(O_{r,n} \setminus T\right) \subseteq T$. Hence,

$$O_{r,n} \setminus T = -q\left(-q\left(O_{r,n} \setminus T\right)\right) \subseteq -qT.$$

The proof of (ii) can be obtained similarly. □

The BCH bound for constacyclic codes is as follows.

Theorem 5.2 ([2, Theorem 2.2])**.** Let C be a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$. Let $r = o_{q^2}(\lambda)$. Let ξ be a primitive nrth root of unity in an extension field of $\mathbb{F}_{q^2}$ such that $\xi^n = \lambda$. Assume the generator polynomial of C has roots that include the set $\left\{\xi^{ri+1} \mid i_1 \leq i \leq i_1 + d - 1\right\}$. Then the minimum distance of C is at least $d+1$.

Example 5.3. Let $q = 3$, $n = 4$ and let $\lambda = -1$ in $\mathbb{F}_9$. Then $o_9(\lambda) = 2$ and $O_{2,4} = \{1, 3, 5, 7\}$. Let $T = \{1, 3\}$. Then $-qT = 5T = \{5, 7\}$. By Theorems 5.1-5.2 and the Singleton bound, C_T is an MDS λ-constacyclic Hermitian self-dual code with parameter $[4, 2, 3]$ over $\mathbb{F}_9$.

Example 5.4. Let $q = 11$, $n = 6$ and let $\lambda = \alpha^{30}$ in $\mathbb{F}_{121}$ where α is a primitive element of $\mathbb{F}_{121}$. Then $o_{121}(\alpha^{30}) = 4$ and $O_{4,6} = \{1, 5, 9, 13, 17, 21\}$. Let $T = \{1, 5, 9\}$. Then $-qT = 13T = \{13, 17, 21\}$. By Theorems 5.1-5.2 and the Singleton bound, C_T is an MDS λ-constacyclic Hermitian self-dual code with parameter $[6, 3, 4]$ over $\mathbb{F}_{121}$.

Examples 5.3 and 5.4 show that there exist MDS constacyclic Hermitian self-dual codes. The following theorem is a generalization of Examples 5.3 and 5.4.

Theorem 5.5. Let $\lambda \in \mathbb{F}_{q^2}$ be such that $r = o_{q^2}(\lambda)$ is even. Let n be an even integer such that $nr|(q^2-1)$ both n and r divide $q+1$. Let

$$T = \left\{1, r+1, \ldots, \left(\frac{n}{2} - 1\right)r + 1\right\} = \left\{ir+1 \mid 0 \leq i \leq \frac{n}{2} - 1\right\}.$$

If $\frac{2(q+1)}{nr}$ is odd, then C_T is an MDS λ-constacyclic Hermitian self-dual code with parameters $\left[n, \frac{n}{2}, \frac{n}{2} + 1\right]$.

Proof. Note that

$$O_{r,n} = \{1, r+1, 2r+1, \ldots, (n-1)r+1\} = \{ir+1 \mid 0 \le i \le n-1\} \subseteq \mathbb{Z}_{nr}$$

and

$$O_{r,n} \setminus T = \left\{ \left(\frac{n}{2}\right) r + 1, \left(\frac{n}{2}+1\right) r + 1, \ldots, (n-1)r+1 \right\} = \left\{ \left(\frac{n}{2}+i\right) r + 1 \mid 0 \le i \le \frac{n}{2} \right\}.$$

Claim that $-qT = O_{r,n} \setminus T$ such that $-q(ir+1) = 1 + (\frac{n}{2}+i)r$ for all $0 \le i \le \frac{n}{2}$. Since $\frac{2(q+1)}{nr}$ is odd, $\frac{q+1}{r} + \frac{n}{2} \equiv 0 \bmod n$. Then $\frac{q+1}{r} + (\frac{n}{2} + i + iq) \equiv \frac{q+1}{r} + \frac{n}{2} + i(q+1) \equiv 0 \bmod n$. We obatin $q+1+\left(\frac{n}{2}+i+iq\right) r \equiv \left(\frac{q+1}{r}\right) r + \left(\frac{n}{2} + i(q+1)\right) r \equiv 0 \bmod nr$, or equivalently, $-q(ir+1) \equiv 1 + \left(\frac{n}{2}+i\right) r \bmod nr$. Therefore, the code C_T is a λ-constacyclic Hermitian self-dual code. Clearly, C is an MDS λ-constacyclic code with parameters $\left[n, \frac{n}{2}, \frac{n}{2}+1\right]$.

□

Since the length of the MDS codes given in [29] is a divisor of $q-1$ and the MDS codes condtructed in Theorem 5.5 is a divisor of $q+1$, the later is different from the former whenever $n \neq 2$. Some families of codes derived from Theorem 5.5 are given in the following example.

Example 5.6. Let q be an odd prime and m be the largest positive integer such that $q \equiv -1 \bmod 2^m$. For each $1 \le i \le m-1$, let $r = 2^i$ and $n = \frac{q+1}{2^{m-i}}$. Then $n|(q+1)$ and $\frac{2(q+1)}{nr} = \frac{q+1}{r^m}$ is odd. Therefore, by Theorem 5.5, there exists an MDS $[n = \frac{q+1}{2^{m-i}}, \frac{q+1}{2^{m-i+1}}, \frac{q+1}{2^{m-i+1}} + 1]$ code over $\mathbb{F}_{q^2}$ for all $1 \le i \le m-1$.

Conditions for nonexistence MDS λ-constacyclic Hermitian self-dual codes of length n over $\mathbb{F}_{q^2}$ are given as follows.

Theorem 5.7. Let $\lambda \in \mathbb{F}_{q^2}$ be such that $r = o_{q^2}(\lambda)$ is even. Let n be an even integer such that $nr|(q^2-1)$. If $a\left(\frac{q+1}{r}\right) \equiv 0 \bmod n$ for some a in $O_{r,n}$ then there are no MDS λ-constacyclic Hermitian self-dual codes of length n over $\mathbb{F}_{q^2}$.

Proof. Let a in $O_{r,n}$ be such that $a\left(\frac{q+1}{r}\right) \equiv 0 \bmod n$. Then, $a(q+1) \equiv 0 \bmod nr$, which implies $-qa = a$. Let C_T be an MDS λ-constacyclic Hermitian self-dual code and let $T \subseteq O_{r,n}$ be the defining set of a code C_T. By Theorem 5.1, $T \cap -qT = \emptyset$ and $T \cup -qT = O_{r,n}$.

If $a \in T$, then $a \in T \cap -qT$, a contradiction. If $a \notin T$, then $a \in -qT$. So $a = -qa \in q^2T = T$, a contradiction. □

The following example shows that there are no (-1)-constacyclic Hermitian self-dual code of length 6 over $\mathbb{F}_{49}$.

Example 5.8. Let $q = 7$, $n = 6$ and let $\lambda = -1$ in $\mathbb{F}_{49}$. Thus, $o_{49}(-1) = 2$ and $O_{2,6} = \{1, 3, 5, 7, 9, 11\}$. Since $3 \cdot \frac{8}{2} = 12 \equiv 0 \bmod 6$, by Theorem 5.7, there are no MDS (-1)-constacyclic Hermitian self-dual code of length 6 over $\mathbb{F}_{49}$.

6 Quasi-Twisted Hermitian Self-Dual Codes over $\mathbb{F}_{q^2}$

In this section, we focus on simple root (λ, ℓ)-QT Hermitian self-dual codes of length $n\ell$ over $\mathbb{F}_{q^2}$, or equivalently, $\gcd(n, q) = 1$. The decomposition of (λ, ℓ)-QT codes is given. The characterization and enumeration of (λ, ℓ)-QT Hermitian self-dual codes of length $n\ell$ over $\mathbb{F}_{q^2}$ can be obtained via this decomposition.

In [12], QT codes over finite fields with respect to the Euclidean inner product were studied. QT codes were decomposed and the Euclidean duals of such codes are determined. In particular, the characterization of Euclidean self-dual QT codes were given. As a generalization of [12] and [19], we study QT codes over finite fields with respect to the Hermitian inner product..

From Lemma 2.1, every (λ, ℓ)-QT code of length $n\ell$ over $\mathbb{F}_{q^2}$ can be viewed as an R submodule of R^ℓ, where $R := \mathbb{F}_{q^2}[x]/\langle x^n - \lambda \rangle$.

Define an *involution* $\sim$ on R to be the $\mathbb{F}_{q^2}$-linear map that sends α to α^q for all $\alpha \in \mathbb{F}_{q^2}$ and sends x to $x^{-1} = x^{n-1}$. Let $\langle \cdot, \cdot \rangle_\sim : R^\ell \times R^\ell \to R$ be defined by

$$\langle \mathbf{v}, \mathbf{s} \rangle_\sim := \sum_{j=0}^{\ell-1} v_j(x)\widetilde{s_j(x)},$$

where $\mathbf{v} = (v_0(x), \dots, v_{\ell-1}(x))$ and $\mathbf{s} = (s_0(x), \dots, s_{\ell-1}(x))$ in R^ℓ. The $\sim$*-dual* of $D \subseteq R^\ell$ is defined to be the set

$$D^{\perp_\sim} := \left\{ \mathbf{v} \in R^\ell \mid \langle \mathbf{v}, \mathbf{s} \rangle_\sim = 0 \ \text{ for all } \mathbf{s} \in D \right\}.$$

We say that $D \subseteq R^\ell$ is $\sim$*-self-dual* if $D = D^{\perp_\sim}$.

Proposition 6.1. Let $\mathbf{a}, \mathbf{b} \in \mathbb{F}_{q^2}^{n\ell}$. Then $\left\langle T_{\lambda,\ell}^k(\mathbf{a}), \mathbf{b} \right\rangle_H = 0$ for all $0 \le k \le n-1$ if and only if $\langle \psi(\mathbf{a}), \psi(\mathbf{b}) \rangle_\sim = 0$.

Proof. Let $\psi(\mathbf{a}) = (a_0(x), \dots, a_{\ell-1}(x)) = \left(\sum_{i=0}^{n-1} a_{i0} x^i, \dots, \sum_{i=0}^{n-1} a_{i,\ell-1} x^i \right)$ and $\psi(\mathbf{b}) = (b_0(x), \dots, b_{\ell-1}(x)) = \left(\sum_{i=0}^{n-1} b_{i0} x^i, \dots, \sum_{i=0}^{n-1} b_{i,\ell-1} x^i \right)$. By comparing the coefficients,

$$0 = \sum_{j=0}^{\ell-1} a_j(x)\widetilde{b_j(x)} = \sum_{j=0}^{\ell-1} \left(\sum_{i=0}^{n-1} a_{ij} x^i \right) \left(\sum_{k=0}^{n-1} b_{kj}^q x^{-k} \right) \tag{6.1}$$

is equivalent to

$$\sum_{j=0}^{\ell-1} \sum_{i=0}^{n-1} a_{i+h,j} b_{ij}^q x^h = 0 \tag{6.2}$$

for all $0 \le h \le n-1$, where the subscripts $i+h$ are computed modulo n. The expression in (6.2) is equivalent to $\left\langle T_{\lambda,\ell}^{-h}(\mathbf{a}), \mathbf{b} \right\rangle_H = 0$ for all $0 \le h \le n-1$. Since $T_{\lambda,\ell}^{-h} = T_{\lambda,\ell}^{(n-h)}$, (6.1) is equivalent to $\left\langle T_{\lambda,\ell}^k(\mathbf{a}), \mathbf{b} \right\rangle_H = 0$ for all $0 \le k \le n-1$. □

Next proposition follows from the definition of QT codes and [29, Proposition 2.3].

Proposition 6.2. Let C be a (λ, ℓ)-QT code of length $n\ell$ over $\mathbb{F}_{q^2}$ and let $C^{\perp_H}$ be the Hermitian dual of C. Then $C^{\perp_H}$ is a (λ^{-q}, ℓ)-QT code of length $n\ell$ over $\mathbb{F}_{q^2}$.

Proof. Let $\mathbf{d} \in C^{\perp_H}$ and let $\mathbf{c} \in C$. Then $\left\langle T_{\lambda,\ell}^i(\mathbf{c}), \mathbf{d} \right\rangle_H = 0$ for all $0 \le i \le n-1$. Since

$$\begin{aligned}
\langle \mathbf{c}, T_{\lambda^{-q},\ell}(\mathbf{d}) \rangle_H &= \left\langle \mathbf{c}, T_{\lambda^{-1},\ell}(\mathbf{d}^q) \right\rangle_E \quad \text{where } \mathbf{d}^q \text{ denote } \left(d_{00}^q, \dots, d_{n-1,\ell-1}^q \right) \\
&= \sum_{j=0}^{\ell-1} c_{0j} d_{n-1,j}^q \lambda^{-1} + \sum_{i=1}^{n-1} \sum_{j=0}^{\ell-1} c_{ij} d_{i-1,j}^q \\
&= \lambda^{-1} \left(\sum_{j=0}^{\ell-1} c_{0j} d_{n-1,j}^q + \sum_{i=1}^{n-1} \sum_{j=0}^{\ell-1} \lambda c_{ij} d_{i-1,j}^q \right) \\
&= \lambda^{-1} \left\langle T_{\lambda,\ell}^{n-1}(\mathbf{c}), \mathbf{d} \right\rangle_H \\
&= 0,
\end{aligned}$$

it follows that $T_{\lambda^{-q},\ell}(\mathbf{d}) \in C^{\perp_H}$. Therefore, $C^{\perp_H}$ is a (λ^{-q}, ℓ)-QT code. □

By Proposition 6.2, both C and $C^{\perp_H}$ are (λ, ℓ)-QT codes if and only if $o_{q^2}(\lambda) | (q+1)$. Therefore, it makes sense to focus on only the case where $o_{q^2}(\lambda) | (q+1)$.

Corollary 6.3. Let $\lambda \in \mathbb{F}_{q^2} \setminus \{0\}$ be such that $o_{q^2}(\lambda) | (q+1)$. Let C be a (λ, ℓ)-QT code of length $n\ell$ over $\mathbb{F}_{q^2}$ and let $\psi(C)$ be its image in R^ℓ under ψ defined in (2.1). Then $\psi(C)^{\perp_\sim} = \psi(C^{\perp_H})$. In particular, C is Hermitian self-dual if and only if $\psi(C)$ is $\sim$-self-dual.

6.1 Decomposition

Since $\gcd(q, n) = 1$, by (3.11), $x^n - \lambda$ can be factored as follows

$$x^n - \lambda = g_1(x) \dots g_s(x) h_1(x) h_1^\dagger(x) \dots h_t(x) h_t^\dagger(x),$$

where $h_j(x)$ and $h_j^\dagger(x)$ are a monic irreducible conjugate-reciprocal polynomial pair for all $1 \le j \le t$ and $g_i(x)$ is a monic irreducible self-conjugate-reciprocal polynomial for all $1 \le i \le s$.

By the Chinese Remainder Theorem (c.f. [12] and [19]), we write

$$R = \mathbb{F}_{q^2}[x]/\langle x^n - \lambda\rangle \cong \left(\prod_{i=1}^{s} \mathbb{F}_{q^2}[x]/\langle g_i(x)\rangle\right) \times \left(\prod_{j=1}^{t} \left(\mathbb{F}_{q^2}[x]/\left\langle h_j(x)\right\rangle \times \mathbb{F}_{q^2}[x]/\left\langle h_j^\dagger(x)\right\rangle\right)\right).$$

For simplicity, let $G := \mathbb{F}_{q^2}[x]/\langle g_i(x)\rangle_i$, $H_j' := \mathbb{F}_{q^2}[x]/\left\langle h_j(x)\right\rangle$ and $H_j'' := \mathbb{F}_{q^2}[x]/\left\langle h_j^\dagger(x)\right\rangle$. Then we have

$$R = \mathbb{F}_{q^2}[x]/\langle x^n - \lambda\rangle \cong \left(\prod_{i=1}^{s} G_i\right) \times \left(\prod_{j=1}^{t} \left(H_j' \times H_j''\right)\right). \tag{6.3}$$

For an irreducible self-conjugate-reciprocal factor $f(x)$ of $x^n - \lambda$ in $\mathbb{F}_{q^2}[x]$ of degree k, the map $\mathbb{F}_{q^2}[x]/\langle f(x)\rangle$

$$\bar{\ }: \mathbb{F}_{q^2}[x]/\langle f(x)\rangle \longrightarrow \mathbb{F}_{q^2}[x]/\langle f(x)\rangle$$

defined by $c(x) = \sum_{i=0}^{k-1} c_i x^i + \langle f\rangle \mapsto \overline{c(x)} = \sum_{i=0}^{k-1} c_i^q x^{-i} + \langle f\rangle$ is an automorphim.

For irreducible conjugate-reciprocal factors pair $f(x)$ and $f^\dagger(x)$ of $x^n - \lambda$ in $\mathbb{F}_{q^2}[x]$ of degree k, the extension fields $\mathbb{F}_{q^2}[x]/\langle f(x)\rangle$ and $\mathbb{F}_{q^2}[x]/\left\langle f^\dagger(x)\right\rangle$ are isomorphic. The map

$$\hat{\ }: \mathbb{F}_{q^2}[x]/\langle f(x)\rangle \longrightarrow \mathbb{F}_{q^2}[x]/\left\langle f^\dagger(x)\right\rangle$$

defined by $c(x) = \sum_{i=0}^{k-1} c_i x^i + \langle f(x)\rangle \mapsto \widehat{c(x)} = \sum_{i=0}^{k-1} c_i^q x^{-i} + \left\langle f^\dagger(x)\right\rangle$ is an isomorphism.

Using the above isomorphisms, we have

$$R = \mathbb{F}_{q^2}[x]/\langle x^n - \lambda\rangle \cong \left(\prod_{i=1}^{s} G_i\right) \times \left(\prod_{j=1}^{t} \left(H_j' \times H_j'\right)\right). \tag{6.4}$$

Let σ_1, σ_2 denote the isomorphisms in (6.3) and (6.4), respectively. Then an element $\mathbf{r} \in R$ can be written as

$$\sigma_1(\mathbf{r}) = (r_1, \dots, r_s, r_1', r_1'', \dots, r_t', r_t'') \ \text{ in } \ \left(\prod_{i=1}^{s} G_i\right) \times \left(\prod_{j=1}^{t} \left(H_j' \times H_j''\right)\right),$$

where $r_i \in G_i, r_j' \in H_j'$ and $r_j'' \in H_j''$, and

$$\sigma_2(\mathbf{r}) = \left(r_1, \dots, r_s, r_1', \widehat{r_1''}, \dots, r_t', \widehat{r_t''}\right) \ \text{ in } \ \left(\prod_{i=1}^{s} G_i\right) \times \left(\prod_{j=1}^{t} \left(H_j' \times H_j'\right)\right), \tag{6.5}$$

where $r_i \in G_i$ and $r_j', \widehat{r_j''} \in H_j'$. Therefore, an element $\tilde{\mathbf{r}} \in R$ can be expressed as

$$\sigma_1(\tilde{\mathbf{r}}) = \left(\overline{r_1}, \dots, \overline{r_s}, \widehat{r_1''}, \widehat{r_1'}, \dots, \widehat{r_t''}, \widehat{r_t'}\right) \ \text{ in } \ \left(\prod_{i=1}^{s} G_i\right) \times \left(\prod_{j=1}^{t} \left(H_j' \times H_j''\right)\right),$$

where $\overline{r_i} \in G_i, \widehat{r_j''} \in H_j'$ and $\widehat{r_j'} \in H_j''$, and

$$\sigma_2(\tilde{\mathbf{r}}) = \left(\overline{r_1}, \dots, \overline{r_s}, \widehat{r_1''}, r_1', \dots, \widehat{r_t''}, r_t'\right) \ \text{ in } \ \left(\prod_{i=1}^{s} G_i\right) \times \left(\prod_{j=1}^{t} \left(H_j' \times H_j'\right)\right), \tag{6.6}$$

where $\overline{r_i} \in G_i$ and $\widehat{r_j''}, r_j' \in H_j'$.

Remark 6.4. If $f(x)$ is self-conjugate-reciprocal, then $\sim$ induces the field automorphism $\bar{}$ on $\mathbb{F}_{q^2}[x]/\langle f(x)\rangle \cong \mathbb{F}_{q^{2k}}$. The map $r \mapsto \overline{r}$ on $\mathbb{F}_{q^2}[x]/\langle f(x)\rangle$ is actually the map $r \mapsto r^{q^k}$ on $\mathbb{F}_{q^{2k}}$.

Using statements similar to those in the proof of [19, Proposition 4.1], we conclude the next proposition.

Proposition 6.5. Let $\mathbf{a}, \mathbf{b} \in R^\ell$ and write $\mathbf{a} = (\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{\ell-1})$ and $\mathbf{b} = (\mathbf{b}_0, \mathbf{b}_1, \ldots, \mathbf{b}_{\ell-1})$. Decomposing $\sigma_2(\mathbf{a}_i)$ and $\sigma_2(\mathbf{b}_i)$ using (6.4), we have

$$\sigma_2(\mathbf{a}_i) = (a_{i1}, \ldots, a_{is}, a'_{i1}, a''_{i1}, \ldots, a'_{it}, a''_{it}) \quad \text{and} \quad \sigma_2(\mathbf{b}_i) = (b_{i1}, \ldots, b_{is}, b'_{i1}, b''_{i1}, \ldots, b'_{it}, b''_{it}),$$

where $a_{ij}, b_{ij} \in G_i$ and $a'_{ij}, a''_{ij}, b'_{ij}, b''_{ij} \in H'_j$. Then

$$\begin{aligned}\langle \sigma_2(\mathbf{a}), \sigma_2(\mathbf{b})\rangle_\sim &= \sum_{i=1}^{\ell-1} \sigma_2(\mathbf{a}_i)\widetilde{\sigma_2(\mathbf{b}_i)} \\ &= \left(\sum_i a_{i1}\overline{b_{i1}}, \ldots, \sum_i a_{is}\overline{b_{is}}, \sum_i a'_{i1}b''_{i1}, \sum_i a''_{i1}b'_{i1}, \ldots, \sum_i a'_{it}b''_{it}, \sum_i a''_{it}b'_{it} \right).\end{aligned}$$

In particular, $\langle \sigma_2(\mathbf{a}), \sigma_2(\mathbf{b})\rangle_\sim = 0$ if and only if $\sum_i a_{ij}\overline{b_{ij}} = 0$ for all $1 \le j \le s$ and $\sum_i a'_{ik}b''_{ik} = 0 = \sum_i a''_{ik}b'_{ik}$ for all $1 \le k \le t$.

By (6.4), we have

$$R^\ell \cong \left(\prod_{i=1}^{s} G_i^\ell \right) \times \left(\prod_{j=1}^{t} \left({H'_j}^\ell \times {H'_j}^\ell \right) \right).$$

In particular, R submodule C of R^ℓ can be decomposed as

$$C \cong \left(\prod_{i=1}^{s} C_i \right) \times \left(\prod_{j=1}^{t} \left(C'_j \times C''_j \right) \right),$$

where C'_j and C''_j are linear codes of length ℓ over H'_j and C_i is a linear code of length ℓ over G_i.

By Proposition 6.5, we have

$$C^{\perp_H} \cong \left(\prod_{i=1}^{s} C_i^{\perp_H} \right) \times \left(\prod_{j=1}^{t} \left({C''_j}^{\perp_E} \times {C'_j}^{\perp_E} \right) \right),$$

and hence, the next corollary follows.

Corollary 6.6. An R submodule C of R^ℓ is $\sim$-self-dual, or equivalently, a (λ, ℓ)-QT code $\psi^{-1}(C)$ of length $n\ell$ over $\mathbb{F}_{q^2}$ is Hermitian self-dual if and only if

$$C \cong \left(\prod_{i=1}^{s} C_i \right) \times \left(\prod_{j=1}^{t} \left(C'_j \times {C'_j}^{\perp_E} \right) \right),$$

where C_i is a Hermitian self-dual code of length ℓ over G_i for $1 \le i \le s$, C'_j is a linear code of length ℓ over H_j, and ${C'_j}^{\perp_E}$ is Euclidean dual of C'_j for $1 \le j \le t$.

Let $N(q, \ell)$ (resp., $N_H(q, \ell)$) denote the number of linear codes (resp., Hermitian self-dual codes) of length ℓ over $\mathbb{F}_q$. It is well known [25] that

$$N(q, \ell) = \sum_{i=0}^{\ell} \prod_{j=0}^{i-1} \frac{q^\ell - q^i}{q^i - q^j} \tag{6.7}$$

and

$$N_H(q, \ell) = \begin{cases} \prod_{i=0}^{\frac{\ell}{2}-1} (q^{i+\frac{1}{2}} + 1) & \text{if } \ell \text{ is even,} \\ 0, & \text{otherwise,} \end{cases} \tag{6.8}$$

where the empty product is regarded as 1.

Proposition 6.7. Let $\mathbb{F}_{q^2}$ be a finite field and let n, ℓ be positive integers such that ℓ is even and $\gcd(n, q) = 1$. Let λ be a nonzero element in $\mathbb{F}_{q^2}$ such that $o_{q^2}(\lambda)|(q + 1)$. Suppose that $x^n - \lambda = g_1(x) \dots g_s(x)h_1(x)h_1^\dagger(x) \dots h_t(x)h_t^\dagger(x)$. Let $d_i \deg g_i(x)$ and $e_j = \deg h_j(x)$. The number of (λ, ℓ)-QT Hermitian self-dual codes of length $n\ell$ over $\mathbb{F}_{q^2}$ is

$$\prod_{i=1}^{s} N_H(q^{2d_i}, \ell) \prod_{j=1}^{t} N(q^{2e_j}, \ell).$$

In the case where $\Omega = \emptyset$ or $\pi(n'r, q^2) = 0$, the formula for the number of Hermitian self-dual (λ, ℓ)-QT codes of length $n\ell$ over $\mathbb{F}_{q^2}$ can be simplified in the following corollaries.

Corollary 6.8. Let $x^n - \lambda = g_1(x) \dots g_s(x)h_1(x)h_1^\dagger(x) \dots h_t(x)h_t^\dagger(x)$. and let $e_j = \deg h_j(x)$. If $\Omega = \emptyset$, then the number of (λ, ℓ)-QT Hermitian self-dual codes of length $n\ell$ over $\mathbb{F}_{q^2}$ is

$$\prod_{j=1}^{t} N(q^{2e_j}, \ell).$$

Corollary 6.9. Let $x^n - \lambda = g_1(x) \dots g_s(x)h_1(x)h_1^\dagger(x) \dots h_t(x)h_t^\dagger(x)$ and let $d_i = \deg g_i(x)$. If $\pi(n'r, q^2) = 0$, then the number of (λ, ℓ)-QT Hermitian self-dual codes of length $n\ell$ over $\mathbb{F}_{q^2}$ is

$$\prod_{i=1}^{s} N_H(q^{2d_i}, \ell).$$

Acknowledgements

The authors thank Borvorn Suntornpoch for useful discussions.

References

[1] N. Aydin, T. Asamov, T. A. Gulliver, *Some open problems on quasi-twisted and related code constructions and good quaternary codes*, in: Proceedings of IEEE ISIT’ 2007, Nice, France (2007), 856–860.

[2] N. Aydin, I. Siap, D. J. Ray-Chaudhuri, *The structure of* 1*-generator quasi-twisted codes and new linear codes*, Des. Codes Cryptogr., **24** (2001), 313–326.

[3] G. K. Bakshi, M. Raka, *A class of constacyclic codes over a finite field*, Finite Fields Appl., **18** (2012), 362–377.

[4] E. R. Berlekamp, “Algebraic Coding Theory,” McGraw-Hill, New York, 1968.

[5] E. Z. Chen, *An explicit construction of* 2*-generator quasi-twisted codes*, IEEE Trans. Inform. Theory, **54** (2008), 5770–5773.

[6] B. Chen, Y. Fan, L. Lin, H. Liu, *Constacyclic codes over finite fields*, Finite Fields Appl., **18** (2012), 1217–1231.

[7] B. Chen, H. Q. Dinh, Y. Fan, S. Ling, *Polyadic constacyclic codes*, EEE Trans. Inform. Theory, **61** (2015) , 4895–4904.

[8] V. Chepyzhov, *A Gilbert-Vashamov bound for quasitwisted codes of rate* $\frac{1}{n}$, Proceedings of the Joint Swedish-Russian International Workshop on Information Theory, Mölle, Sweden (1993), 214–218.

[9] R. Daskalov, P. Hristov, *New quasi-twisted degenerate ternary linear codes*, IEEE Trans. Inform. Theory, **49** (2003), 2259–2263.

[10] T. A. Gulliver, M. Harada, H. Miyabayashi, *Double circulant and quasi-twisted self-dual codes over $\mathbb{F}_5$ and $\mathbb{F}_7$*, Advances in Mathematics of Communications, **1** (2007), 223 – 238.

[11] T. A. Gulliver, N. P. Secord, S. A. Mahmoud, *A link between quasi-cyclic codes and convolution codes*, IEEE Trans. Inform. Theory, **44** (1998), 431–435.

[12] Y. Jia, *On quasi-twisted codes over finite fields*, Finite Fields Appl., **18** (2012), 237–257.

[13] Y. Jia, S. Ling, C. Xing, *On self-dual cyclic codes over finite fields*, IEEE Trans. Inform. Theory, **13** (2011), 2243–2251.

[14] X. Kai, X. Zhu, P. Li, *Constacylic codes and some new quantum MDS codes*, IEEE Trans. Inform. Theory, **60** (2014) , 2080–2086.

[15] T. Kasami, *A Gilbert-Varshamov bound for quasi-cyclic codes of rate $\frac{1}{2}$*, IEEE Trans. Inform. Theory, **20** (1974), 679.

[16] A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli, *Nonbinary stabilizer codes over finite fields*, IEEE Trans. Inform. Theory, **52** (2006), 4892–4914.

[17] G. G. La Guardia *On optimal constacyclic codes*, http://arxiv.org/abs/1311.2505, (2013).

[18] L. Lin, H. Liu, B. Chen, *Existence conditions for self-orthogonal negacyclic codes over finite fields*, Advances in Mathematics of Communications, **9** (2015), 1 – 7.

[19] S. Ling, P. Solé, *On the algebraic structure of quasi-cyclic codes I: Finite fields*, IEEE Trans. Inform. Theory, **47** (2001) , 2751–2760.

[20] S. Ling, P. Solé, *Good self-dual quasi-cyclic codes exist*, IEEE Trans. Inform. Theory, **49** (2003), 1052–1053.

[21] S. Ling, P. Solé, *On the algebraic structure of quasi-cyclic codes III: Generator theory*, IEEE Trans. Inform. Theory, **51** (2005), 2692–2700.

[22] S. Ling, H. Niederreiter, P. Solé, *On the algebraic structure of quasi-cyclic codes IV: Repeated roots*, Des. Codes Crypt., **38** (2006), 337–361.

[23] G. Nebe, E. M. Rains, N. J. A. Sloane, "Self-Dual Codes and Invariant Theory," Algorithms and Computation in Mathematics vol. 17. Springer-Verlag, Berlin, Heidelberg, 2006.

[24] H. Özadamb, F. Özbudak, *A note on negacyclic and cyclic codes of length p^s over a finite field of characteristic p*, Advances in Mathematics of Communications, **3** (2009), 265 –271.

[25] E. M. Rains, N. J. A. Sloane, Self-dual codes. In: Handbook of Coding Theory, 177–294, Elsevier, North-Holland, Amsterdam, 1998.

[26] E. Sangwisut, S. Jitman, S. Ling, P. Udomkavanich, *Hulls of cyclic and negacyclic codes over finite fields*, Finite Fields Appl., **33** (2015), 232–257.

[27] J. P. Serre, "A course in arithmetic," Graduate Texts in Mathematics 7, Springer-Verlag, New York-Heidelberg-Berlin, 1973.

[28] G. Solomon, H. C. A. van Tilborg, *A connection between block and convolutional codes*, SIAM J. Appl. Math., **37** (1979), 358-369.

[29] Y. Yang, W. Cai, *On self-dual constacyclic codes over finite fields*, Des. Codes Cryptogr., **74** (2015), 355-364.