Quantum Information Processing (2020) 19:212
https://doi.org/10.1007/s11128-020-02708-3

The images of constacyclic codes and new quantum codes

Xiaoshan Kai[1] · Shixin Zhu[1] · Zhonghua Sun[1]

Received: 25 August 2019 / Accepted: 21 May 2020 / Published online: 11 June 2020

Abstract
Let q be a prime power and $m \geq 2$ be a positive integer. A sufficient condition for the q^2-ary images of constacyclic codes over $\mathbb{F}_{q^{2m}}$ to be Hermitian self-orthogonal is presented. Hermitian self-orthogonal codes over $\mathbb{F}_{q^2}$ are obtained as the images of constacyclic codes over $\mathbb{F}_{q^{2m}}$. Two classes of quantum codes are derived by employing the Hermitian construction. The construction produces quantum codes with better parameters than the previously known ones.

Keywords Constacyclic codes · Hermitian self-orthogonal codes · Quantum codes

1 Introduction

Quantum computation and communication attracted much attention due to efficient quantum algorithms in the late 1990s. It is well known that quantum computation and communication rely on undisturbed evolution of quantum coherence. Unfortunately, the decoherence caused by interaction with the environment destroys the information in a superposition of states. At the same time, because of the no-cloning theorem [42], the technique that duplicates information could not be applied to quantum information. To overcome these difficulties, Shor [33] and Steane [34] showed that quantum error-correcting codes do exist and constructed the first example of quantum codes. This signs the birth of quantum error-correcting codes. Quantum error-correcting codes introduce some auxiliary qubits and make them entangle with the transmitted qubits. The redundancy is stored in the new entangled state. The original state can be recovered by making use of the auxiliary qubits (see [29,31]). Soon afterwards, Calderbank

✉ Xiaoshan Kai
kxs6@sina.com

Shixin Zhu
zhushixin@hfut.edu.cn

Zhonghua Sun
sunzhonghuas@163.com

[1] School of Mathematics, Hefei University of Technology, Hefei 230601, China

et al. [5] presented a mathematical scheme to obtain quantum codes from classical error-correcting codes over $\mathbb{F}_2$ or $\mathbb{F}_4$ with certain orthogonal properties. Finding good quantum error-correcting codes has become another subject of quantum error-correction besides fault-tolerant quantum hardware design. A number of good binary quantum codes were constructed from classical self-orthogonal codes over $\mathbb{F}_2$ or $\mathbb{F}_4$ (see [5,7,10,24]). Later, non-binary quantum codes have received increasing attention because they can be used in the realization of fault-tolerant quantum computation [4,25]. Several construction methods were presented based on self-orthogonal codes over finite fields [2,20].

Due to good algebraic structure, classical cyclic codes were used to construct quantum codes. This yields quantum cyclic codes including quantum BCH codes and quantum Reed-Solomon codes. In [35], Steane discovered efficient binary quantum codes via BCH codes. Non-binary quantum cyclic codes were constructed from Euclidean or Hermitian self-orthogonal codes (see [1,22,27]). Since then, various techniques are applied to construct new and good quantum cyclic codes. At the application level, the theory of quantum shift registers has been discussed in [15,41] and their realization was performed by the ion traps or nuclear magnetic resonance (NMR) in the experiments [9,23]. Meanwhile, designing arithmetic and logic unit based on quantum technologies was proposed in [13,30,32].

As a generalization of cyclic codes, constacyclic codes have been naturally considered to construct quantum codes. Many quantum maximal distance separable (MDS) codes were derived from constacyclic codes (see [6,18,39]). In contrast with quantum cyclic codes, numerous quantum constacyclic codes have better parameters on the same length [17,19]. Liu et al. [26] explored quantum constacyclic codes of length $q^{2m}+1$ and found a lot of good quantum codes. Wang and Gao [40] constructed new quantum codes from constacyclic codes over the finite non-chain ring $\mathbb{F}_q+v\mathbb{F}_q$ with $v^2=v$. Chen et al. [8] constructed new optimal asymmetric quantum codes and quantum convolutional codes from constacyclic codes. The research above indicates that constacyclic codes have advantages in constructing quantum error-correcting codes. Based on concatenated method, Grassl et al. [16] constructed quantum codes from the binary images of Reed-Solomon codes over $\mathbb{F}_{2^k}$. Tangataj and McLaughlin [37] derived good quantum codes from Hermitian self-orthogonal codes over $\mathbb{F}_4$ as the images of cyclic codes over $\mathbb{F}_{4^m}$. Sundeep and Tangataj [36] studied the self-orthogonality of q-ary images of q^m-ary codes and constructed new quantum codes from the images of cyclic codes over $\mathbb{F}_{4^m}$. In the above literature, Hermitian self-orthogonal cyclic codes over large fields or rings were used to construct quantum codes.

In this paper, we utilize a class of constacyclic codes over $\mathbb{F}_{q^{2m}}$ to construct quantum codes. Let $\mathbb{F}_{q^{2m}}$ be the extension field of $\mathbb{F}_{q^2}$ with degree m. Let η be a nonzero element of $\mathbb{F}_{q^2}$. We provide an explicit criterion for judging the q^2-ary images of η-constacyclic codes over $\mathbb{F}_{q^{2m}}$ to be Hermitian self-orthogonal. Based on Hermitian self-orthogonal images of constacyclic codes over $\mathbb{F}_{q^{2m}}$, we construct some quantum codes with parameters better than the ones available in the literature. It is worth noting that constacyclic codes over $\mathbb{F}_{q^{2m}}$ are not necessarily Hermitian self-orthogonal. The paper is organized as follows. In Sect. 2, basic notations and results about constacyclic codes and quantum codes are recalled. In Sect. 3, a sufficient condition for q^2-ary images of q^{2m}-ary constacyclic codes is given. In Sect. 4, some quantum codes are constructed. Section 5 gives a conclusion.

2 Preliminaries

Let $\mathbb{F}_{q^2}$ be the finite field with q^2 elements, where q is a power of a prime p. The Hamming weight of a vector $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_{q^2}^n$ is the number of nonzero x_i and is denoted by $\mathrm{wt}(\mathbf{x})$. Let $\mathbb{F}_{q^2}^*$ be the multiplicative group of $\mathbb{F}_{q^2}$. Assume that η is an element of $\mathbb{F}_{q^2}^*$. An η-constacyclic code $\mathcal{C}$ over $\mathbb{F}_{q^2}$ of length n is a linear code with the property that if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ then $(\eta c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. An η-constacyclic code $\mathcal{C}$ over $\mathbb{F}_{q^2}$ of length n can be viewed as an ideal in the principal ideal ring $\mathbb{F}_{q^2}[x]/\langle x^n - \eta\rangle$. Hence, $\mathcal{C} = \langle g(x)\rangle$, where $g(x)$ is a monic divisor of $x^n - \eta$. The polynomial $g(x)$ is called the generator polynomial of $\mathcal{C}$, and $h(x) = (x^n - \eta)/g(x)$ is referred to as the parity-check polynomial of $\mathcal{C}$. The roots of $g(x)$ and $h(x)$ are called the zeros and nonzeros of $\mathcal{C}$, respectively. Assume that $\gcd(n, q) = 1$ and η has order r in $\mathbb{F}_{q^2}^*$. Let ξ be a primitive nr-th root of unity such that $\eta = \xi^n$. Then, the roots of $x^n - \eta$ are ξ^{1+rj} for $0 \le j \le n-1$. Denote $\Omega = \{1 + rj \mid 0 \le j \le n-1\}$. For each $s \in \Omega$, denote by $C_{q^2}[s, nr]$ the q^2-cyclotomic coset modulo nr containing s. Then $g(x) = \prod_s \prod_{i \in C_{q^2}[s,nr]} (x - \xi^i)$, where s runs through some subset of representatives of the q^2-cyclomotic cosets modulo nr. Let $Z = \bigcup_s C_{q^2}[s, nr]$ be the union of these q^2-cyclotomic cosets. The set Z is called the zero set of $\mathcal{C}$, and the set $T = \Omega \backslash Z$ is called the nonzero set of $\mathcal{C}$. The following is the BCH-type bound for constacyclic codes (see [3,21]).

Theorem 2.1 *Assume that* $\gcd(n, q) = 1$. *Let* $\mathcal{C}$ *be an* η*-constacyclic code of length* n *over* $\mathbb{F}_{q^2}$. *If the generator polynomial* $g(x)$ *of* $\mathcal{C}$ *has the elements* $\{\xi^{1+ri} | \, b \le i \le b + d - 1\}$ *as the zeros for some integer* b, *then the minimum Hamming distance of* $\mathcal{C}$ *is at least* $d + 1$.

The Euclidean dual code of a linear code $\mathcal{C}$ of length n over $\mathbb{F}_{q^2}$ is defined as

$$\mathcal{C}^{\perp_E} = \{\mathbf{c} \in \mathbb{F}_{q^2}^n \mid \mathbf{c} \cdot \mathbf{x} = 0 \text{ for all } \mathbf{x} \in \mathcal{C}\},$$

where $\mathbf{c} \cdot \mathbf{x} = \sum_{i=0}^{n-1} c_i x_i$ denotes the Euclidean product inner of $\mathbf{c}$ and $\mathbf{x}$. The Hermitian dual code of $\mathcal{C}$ is defined as

$$\mathcal{C}^{\perp_H} = \{\mathbf{c} \in \mathbb{F}_{q^2}^n \mid \langle \mathbf{c}, \mathbf{x}\rangle_H = 0 \text{ for all } \mathbf{x} \in \mathcal{C}\},$$

where $\langle \mathbf{c}, \mathbf{x}\rangle_H = \sum_{i=0}^{n-1} c_i x_i^q$ denotes the Hermitian product inner of $\mathbf{c}$ and $\mathbf{x}$. For any $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_{q^2}^n$, let $\mathbf{x}^q = (x_0^q, x_1^q, \ldots, x_{n-1}^q)$. Set $\mathcal{C}^q = \{\mathbf{c}^q \mid \mathbf{c} \in \mathcal{C}\}$. It can be directly checked that $\mathcal{C}^{\perp_H} = (\mathcal{C}^q)^{\perp_E} = (\mathcal{C}^{\perp_E})^q$. Hence, $\mathcal{C}^{\perp_E}$ and $\mathcal{C}^{\perp_H}$ have the same minimum Hamming distance. If $\mathcal{C} \subseteq \mathcal{C}^{\perp_H}$ (resp. $\mathcal{C} \subseteq \mathcal{C}^{\perp_E}$), then $\mathcal{C}$ is called a

Hermitian self-orthogonal code (resp. an Euclidean self-orthogonal code). Define the symplectic weight of a vector $(\mathbf{a}|\mathbf{b}) = (a_0, a_1, \ldots, a_{n-1}|b_0, b_1, \ldots, b_{n-1}) \in \mathbb{F}_q^{2n}$ as

$$\mathrm{wt}_s((\mathbf{a}|\mathbf{b})) = |\{i \mid (a_i, b_i) \neq (0,0), 0 \leq i \leq n-1\}|.$$

For two vectors $(\mathbf{a}|\mathbf{b})$, $(\mathbf{a}'|\mathbf{b}') \in \mathbb{F}_q^{2n}$, define the trace-symplectic inner product as

$$\left\langle (\mathbf{a}|\mathbf{b}), (\mathbf{a}'|\mathbf{b}') \right\rangle_s = \mathrm{Tr}_{q/p}(\mathbf{b} \cdot \mathbf{a}' - \mathbf{b}' \cdot \mathbf{a}),$$

where $\mathrm{Tr}_{q/p}$ denotes the trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$. For a linear code $\mathcal{D} \subseteq \mathbb{F}_q^{2n}$, the trace-symplectic dual code of $\mathcal{D}$ is defined as

$$\mathcal{D}^{\perp_s} = \{\mathbf{c} \in \mathbb{F}_q^{2n} \mid \langle \mathbf{c}, \mathbf{x} \rangle_s = 0 \text{ for all } \mathbf{x} \in \mathcal{C}\}.$$

If $\mathcal{D} \subseteq \mathcal{D}^{\perp_s}$, then $\mathcal{D}$ is called a symplectic self-orthogonal code. For any nonempty subset $A \subseteq \mathbb{F}_q^{2n}$, define the weight of A as $\mathrm{wt}_s(A) = \min\{\mathrm{wt}_s(\mathbf{a}) \mid \mathbf{0} \neq \mathbf{a} \in A\}$.

Let $\mathcal{C}$ be an η-constacyclic code over $\mathbb{F}_{q^2}$ of length n. Assume that the order r of η in $\mathbb{F}_{q^2}^*$ is a divisor of $q+1$. Then $\mathcal{C}^{\perp_H}$ is still η-constacyclic [18]. Suppose that $\mathcal{C}$ has nonzero set $T \subseteq \Omega$. Then $\mathcal{C}^{\perp_H}$ has zero set $-qT = \{-qz (\mathrm{mod}\ nr) \mid z \in T\}$. Moreover, $\mathcal{C} \subseteq \mathcal{C}^{\perp_H}$ if and only if $-qT \bigcap T = \emptyset$. In the next section, we will derive Hermitian self-orthogonal codes over $\mathbb{F}_{q^2}$ from constacyclic codes over $\mathbb{F}_{q^{2m}}$, where $m \geq 2$ is a positive integer. Let $\mathbb{F}_{q^{2m}}$ be an extension field of $\mathbb{F}_{q^2}$ with degree m. Then $\mathbb{F}_{q^{2m}}$ can be viewed as an m-dimensional vector space over $\mathbb{F}_{q^2}$. The trace map $\mathrm{Tr}_{q^{2m}/q^2} : \mathbb{F}_{q^{2m}} \rightarrow \mathbb{F}_{q^2}$ is defined as

$$\mathrm{Tr}_{q^{2m}/q^2}(a) = a + a^{q^2} + \cdots + a^{q^{2(m-1)}}.$$

Let $\mathcal{A} = \{\alpha_0, \alpha_1, \ldots, \alpha_{m-1}\}$ and $\mathcal{B} = \{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ be two bases of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$. If

$$\mathrm{Tr}_{q^{2m}/q^2}(\alpha_i \beta_j^{q^m}) = \begin{cases} 1, & i = j, \\ 0, & i \neq j \end{cases}$$

for $0 \leq i, j \leq m-1$, then the bases $\mathcal{A}$ and $\mathcal{B}$ are said to be Hermitian dual to each other. Similar to the Euclidean dual bases, it can be verified that any basis of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$ has a unique Hermitian dual basis (see [38]).

Now, we review some basic concepts on quantum error-correct codes. Quantum bits or qubits are the basic unit for quantum systems used to store quantum information. The state of a qubit is a nonzero vector in the complex vector space $\mathbb{C}^q$. Denote by $\{|x\rangle \mid x \in \mathbb{F}_q\}$ an orthonormal basis of $\mathbb{C}^q$ with respect to the Hermitian inner product. Let $\mathcal{H} = (\mathbb{C}^q)^{\otimes n} = \mathbb{C}^{q^n}$ be the n-th tensor product of $\mathbb{C}^q$. A quantum system of n qubits has basis states of the form

$$|x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle = |x_1 x_2 \cdots x_n\rangle.$$

So a quantum state of such a system can be represented as a superposition of these basis states and is specified by q^n amplitudes. A quantum state having the property that it cannot be written as a product of states of its component systems is said to be an entangled state. Entangled states play a crucial role in quantum computation and quantum information. In an entangled state, the component systems are correlated. A quantum error-correcting scheme is proposed by entangling the transmitted qubits of a quantum codeword with some ancilla qubits (see [29,31]).

A q-ary quantum code is a K-dimensional subspace of the Hilbert space $\mathbb{C}^{q^n}$. Let a and b be any two elements of $\mathbb{F}_q$. Define the unitary operators $X(a)$ and $Z(b)$ on $\mathbb{C}^q$ as $X(a)|x\rangle = |x + a\rangle$ and $Z(b)|x\rangle = \omega^{\mathrm{Tr}_{q/p}(bx)}|x\rangle$, where $\omega = \exp(2\pi i/p)$ is a primitive p-th root of unity. For any vector $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_q^n$, let $X(\mathbf{a}) = X(a_1) \otimes \cdots \otimes X(a_n)$. The set $\mathcal{E}_n = \{X(\mathbf{a})X(\mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n\}$ forms an error basis on $\mathbb{C}^{q^n}$. The basis $\mathcal{E}_n$ can generate a finite error group $G_n = \{\omega^i X(\mathbf{a})X(\mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n, 0 \le i \le p-1\}$. For a quantum error $\mathbf{e} = \omega^\lambda X(\mathbf{a})X(\mathbf{b}) \in G_n$ with $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_q^n$ and $\mathbf{b} = (b_0, b_1, \dots, b_{n-1}) \in \mathbb{F}_q^n$, the quantum weight is defined as $\mathrm{wt}_Q(\mathbf{e}) = \mathrm{wt}_s((\mathbf{a}|\mathbf{b}))$. A quantum code has minimum distance d if and only if it can detect all errors in G_n of weight less than d, but cannot detect some error of weight d. A quantum stabilizer code $\mathcal{Q}$ is a nonzero subspace of $\mathbb{C}^{q^n}$ that satisfies $\mathcal{Q} = \bigcap_{E\in S}\{v \in \mathbb{C}^{q^n} \mid Ev = v\}$, where S is a subgroup of G_n. Denoted by $((n, K, d))_q$ or $[[n, k, d]]_q$ a quantum stabilizer code $\mathcal{Q}$ with dimension K and minimum distance d, where $k = \log_q K$. An $[[n, k, d]]_q$ quantum code can encode k logical qubits of information into n physical qubits and has q^k basis codewords. For a subgroup S of G_n, let $C_{G_n}(S)$ be the centralizer of S in G_n and $SZ(G_n)$ be the subgroup generated by S and the center $Z(G_n)$. Regard a quantum error $\omega^\lambda X(\mathbf{a})X(\mathbf{b})$ in G_n as an element $(\mathbf{a}|\mathbf{b})$ in $\mathbb{F}_q^{2n}$, then $C_{G_n}(S)$ and $SZ(G_n)$ are, respectively, mapped into an additive code and its dual code with respect to the symplectic inner product. Moreover, $SZ(G_n)$ is a subgroup of $C_{G_n}(S)$. Based on this, the connection between quantum stabilizer codes and classical additive codes was established in [2,20]

Theorem 2.2 [2,20] *An $((n, K, d))_q$ quantum stabilizer code exists if and only if there exists an additive code $\mathcal{C} \subseteq \mathbb{F}_q^{2n}$ of size q^n/K such that $\mathcal{C} \subseteq \mathcal{C}^{\perp_s}$ and $\mathrm{wt}_s(\mathcal{C}^{\perp_s} \backslash \mathcal{C}) = d$ if $K > 1$ (and $\mathrm{wt}_s(\mathcal{C}^{\perp_s}) = d$ if $K = 1$).*

We briefly recall the connection between Hermitian codes and quantum stabilizer codes (see [2,5]). Let γ_0 be a nonzero element in $\mathbb{F}_q$. Take $\gamma \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$ so that $\gamma^q = -\gamma + \gamma_0$. It is easy to verify that $\mathcal{B} = \{1, \gamma\}$ is a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Let $\mathcal{D}$ be a Hermitian self-orthogonal code over $\mathbb{F}_{q^2}$ of length n, then the image $\mathcal{L}_\mathcal{B}(\mathcal{D})$ of $\mathcal{D}$ under the basis $\mathcal{B}$ is a linear code over $\mathbb{F}_q$ of length $2n$. Let $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \in \mathcal{D}$ and $\mathbf{b} = (b_0, b_1, \dots, b_{n-1}) \in \mathcal{D}^{\perp_H}$. Let $a_i = a_i^{(1)} + \gamma a_i^{(2)}$ and $b_i = b_i^{(1)} + \gamma b_i^{(2)}$. Then

$$
\begin{aligned}
\langle \mathbf{a}, \mathbf{b}\rangle_H &= \sum_{i=0}^{n-1} a_i b_i^q \\
&= \sum_{i=0}^{n-1} \left[a_i^{(1)} + \gamma a_i^{(2)}\right]\left[b_i^{(1)} + (\gamma_0 - \gamma) b_i^{(2)}\right]
\end{aligned}
$$

$$= \sum_{i=0}^{n-1} \left[a_i^{(1)} b_i^{(1)} + \gamma_0 a_i^{(1)} b_i^{(2)} + \gamma \left(a_i^{(2)} b_i^{(1)} - a_i^{(1)} b_i^{(2)} \right) + \gamma^{q+1} a_i^{(2)} b_i^{(2)} \right]$$
$$= 0.$$

Note that γ^{q+1} is in $\mathbb{F}_q$, so it must be $\langle \mathbf{a}, \mathbf{b} \rangle_H = a_i^{(2)} b_i^{(1)} - a_i^{(1)} b_i^{(2)} = 0$, implying that $\mathcal{L}_{\mathcal{B}}(\mathcal{D})$ is a trace-symplectic self-orthogonal code. Applying Theorem 2.2 produces an explicit construction of quantum stabilizer codes from Hermitian self-orthogonal codes.

Theorem 2.3 (Hermitian Construction) [2,5] *Let $\mathcal{C}$ be a Hermitian self-orthogonal $[n, k]$ linear code over $\mathbb{F}_{q^2}$ and let $d = \min\{\mathrm{wt}(\boldsymbol{v}) \mid \boldsymbol{v} \in \mathcal{C}^{\perp_H} \backslash \mathcal{C}\}$. Then a q-ary $[[n, n-2k, d]]$ quantum stabilizer code can be obtained from $\mathcal{C}$.*

3 Images of constacyclic codes

Let $\mathcal{A} = \{\alpha_0, \alpha_1, \ldots, \alpha_{m-1}\}$ be a basis of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$. For any $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_{q^{2m}}^n$, each entry of $\mathbf{x}$ can be expressed as $x_i = \sum_{j=0}^{m-1} x_{ij} \alpha_j$, where $x_{ij} \in \mathbb{F}_{q^2}$. We can define a map $\mathcal{L}_{\mathcal{A}}$ from $\mathbb{F}_{q^{2m}}^n$ to $\mathbb{F}_{q^2}^{nm}$ as

$$\mathcal{L}_{\mathcal{A}}((x_0, x_1, \ldots, x_{n-1})) = (x_{00}, \ldots, x_{n-1,0}, x_{01}, \ldots, x_{n-1,1}, x_{0,m-1}, \ldots, x_{n-1,m-1}).$$

It is obvious that $\mathcal{L}_{\mathcal{A}}$ is an isomorphism of the $\mathbb{F}_{q^2}$-vector space. Let $\mathcal{C}$ be a linear $[n, k, d]$ code over $\mathbb{F}_{q^{2m}}$. Define the q^2-ary image of $\mathcal{C}$ with respect to the basis $\mathcal{A}$ to be $\mathcal{L}_{\mathcal{A}}(\mathcal{C}) = \{\mathcal{L}_{\mathcal{A}}(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}\}$. Then $\mathcal{L}_{\mathcal{A}}(\mathcal{C})$ is an $[mn, km, \geq d]$ linear code over $\mathbb{F}_{q^2}$.

Lemma 3.1 *Let $\mathcal{A} = \{\alpha_0, \alpha_1, \ldots, \alpha_{m-1}\}$ be a basis of $\mathbb{F}_{q^{2m}}$ over $\mathbb{F}_{q^2}$ and $\mathcal{B} = \{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ be a Hermitian dual basis of $\mathcal{A}$. Let $\mathcal{C}$ be a linear $[n, k]$ code over $\mathbb{F}_{q^{2m}}$ and $\mathcal{C}^{\perp_H}$ be its Hermitian dual code. If m is odd, then $\mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_H} = \mathcal{L}_{\mathcal{B}}(\mathcal{C}^{\perp_H})$. If m is even, then $\mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_H} = \mathcal{L}_{\mathcal{B}}(\mathcal{C}^{\perp_H})^q$.*

Proof Let $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$ be any codeword in $\mathcal{C}$ with $u_i = \sum_{j=0}^{m-1} u_{ij} \alpha_j$, where $u_{ij} \in \mathbb{F}_{q^2}$. Let $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ be any codeword in $\mathcal{C}^{\perp_H}$ with $v_i = \sum_{\ell=0}^{m-1} v_{i\ell} \beta_\ell$, where $v_{i\ell} \in \mathbb{F}_{q^2}$. Then

$$(\mathbf{u}, \mathbf{v})_H = \sum_{i=0}^{n-1} u_i v_i^{q^m} = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{m-1} u_{ij} \alpha_j \right) \left(\sum_{\ell=0}^{m-1} v_{i\ell}^{q^m} \beta_\ell^{q^m} \right) = 0. \quad (1)$$

Taking the trace on two sides of (1), we can get that

$$\mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}((\mathbf{u}, \mathbf{v})_H) = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \sum_{\ell=0}^{m-1} u_{ij} v_{i\ell}^{q^m} \mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}} \left(\alpha_j \beta_\ell^{q^m} \right) = 0. \quad (2)$$

If m is odd, then $v_{i\ell}^{q^m} = v_{i\ell}^q$ for $0 \le i \le n-1$ and $0 \le \ell \le m-1$. By the orthogonality of bases, (2) becomes $\sum_{i=0}^{n-1}\sum_{j=0}^{m-1} u_{ij}v_{ij}^q = 0$. This shows that $\mathcal{L}_{\mathcal{B}}(\mathcal{C}^{\perp_H}) \subseteq \mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_H}$. If m is even, then $v_{i\ell}^{q^m} = v_{i\ell}$ for $0 \le i \le n-1$ and $0 \le \ell \le m-1$. By the orthogonality of bases, (2) becomes $\sum_{i=0}^{n-1}\sum_{j=0}^{m-1} u_{ij}v_{ij} = 0$. This shows that $\mathcal{L}_{\mathcal{B}}(\mathcal{C}^{\perp_H}) \subseteq \mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_E}$, i.e., $\mathcal{L}_{\mathcal{B}}(\mathcal{C}^{\perp_H})^q \subseteq \mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_H}$. Note that $\mathcal{L}_{\mathcal{B}}(\mathcal{C}^{\perp_H})$ and $\mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_H}$ have the same cardinality. The desired result follows. □

Let η be a fixed nonzero element of $\mathbb{F}_{q^2}$. Assume that η has order r in $\mathbb{F}_{q^2}^*$. Note that $\mathbb{F}_{q^2}^*$ is a subgroup of $\mathbb{F}_{q^{2m}}^*$, so η must be in $\mathbb{F}_{q^{2m}}^*$ and has order r. An η-constacyclic code over $\mathbb{F}_{q^{2m}}$ of length n is an ideal in $\mathbb{F}_{q^{2m}}[x]/\langle x^n - \eta\rangle$. Let ξ be a primitive nr-th root of unity. Let $\mathcal{C} \subseteq \mathbb{F}_{q^{2m}}[x]/\langle x^n - \eta\rangle$ be the η-constacyclic code with zero set $Z_{2m} \subseteq \Omega = \{1 + rj \mid 0 \le j \le n-1\}$. Note that Z_{2m} is a union of some q^{2m}-cyclotomic cosets modulo nr, moreover, $\mathcal{C} = \langle g(x)\rangle$ where $g(x) = \prod_{z\in Z_{2m}}(x - \xi^z)$. To study the q^2-ary image of $\mathcal{C}$, we consider an η-constacyclic code over $\mathbb{F}_{q^2}$ of length n. For any $\lambda \in C_{q^{2m}}[s, nr]$, it is obvious that $\lambda \in C_{q^2}[s, nr]$. Define the set Z_2 to be the union of the q^2-cyclotomic cosets modulo nr contained in Z_{2m}, i.e.,

$$Z_2 = \bigcup_{C_{q^2}[\lambda,nr]\subseteq Z_{2m}} C_{q^2}[\lambda, nr]. \tag{3}$$

Let $\mathcal{D}$ be the η-constacyclic code over $\mathbb{F}_{q^2}$ of length n with zero set $Z_2 \subseteq \Omega$. Then $\mathcal{D}$ has generator polynomial

$$g_{q^2}(x) = \prod_{z\in Z_2}(x - \xi^z).$$

Note that $g_{q^2}(x)$ is a polynomial over $\mathbb{F}_{q^2}$. It is obvious that $g_{q^2}(x)$ is a divisor of $g(x)$ with the highest degree in $\mathbb{F}_{q^2}[x]$.

Assume that $g(x) = g_{q^2}(x)h(x)$, for some $h(x) \in \mathbb{F}_{q^{2m}}[x]$. Let $c(x) = \sum_{i=0}^{n-1} c_i x^i$ be a codeword in $\mathcal{C}$, where $c_i \in \mathbb{F}_{q^{2m}}$. Under the basis $\mathcal{A} = \{\alpha_0, \alpha_1, \ldots, \alpha_{m-1}\}$, we can write $c_i = \sum_{j=0}^{m-1} c_{ij}\alpha_j$, where $c_{ij} \in \mathbb{F}_{q^2}$. Then

$$c(x) = \sum_{i=0}^{n-1}\left(\sum_{j=0}^{m-1} c_{ij}\alpha_j\right)x^i = \sum_{j=0}^{m-1}\left(\sum_{i=0}^{n-1} c_{ij}x^i\right)\alpha^j.$$

Write $c_j(x) = \sum_{i=0}^{n-1} c_{ij}x^i$, for $0 \le j \le m-1$. Then $c_j(x)$ can be viewed as a word over $\mathbb{F}_{q^2}$ of length n. The following result tells us that the word is from the code $\mathcal{D}$.

Lemma 3.2 *Let $c_j(x)$, $0 \le j \le m-1$, be defined as above. Let $\mathcal{C}$ be the η-constacyclic code in $\mathbb{F}_{q^{2m}}[x]/\langle x^n - \eta\rangle$ with generator polynomial $g(x)$. Let $\mathcal{D}$ be the η-constacyclic code in $\mathbb{F}_{q^2}[x]/\langle x^n - \eta\rangle$ with generator polynomial $g_{q^2}(x)$. Then $c_j(x)$, $0 \le j \le m-1$, are codewords in $\mathcal{D}$.*

Proof Let $\deg(g(x)) = \ell_1$ and $\deg(g_{q^2}(x)) = \ell_2$. Since $c(x)$ belongs to $\mathcal{C}$, we have $c(x) = g(x)s(x)$, for some $s(x) \in \mathbb{F}_{q^{2m}}[x]$ and $\deg(s(x) < n - \ell_1$. Hence, $c(x) = g_{q^2}(x)h(x)s(x)$. Write $t(x) = h(x)s(x)$, then $t(x) \in \mathbb{F}_{q^{2m}}[x]$ and $\deg(t(x) < n - \ell_2$. Under the basis $\mathcal{A} = \{\alpha_0, \alpha_1, \ldots, \alpha_{m-1}\}$, we can write $t(x) = \sum_{j=0}^{m-1} u_j(x)\alpha_j$, where $u_j(x) \in \mathbb{F}_{q^2}[x]$ and $\deg(u_j(x)) < n - \ell_2$. It then follows that $c(x) = \sum_{j=0}^{m-1} g_{q^2}(x)u_j(x)\alpha_j$. Note that $g_{q^2}(x)u_j(x)$ has degree less than n. Thus, $c_j(x) = g_{q^2}(x)u_j(x)$. The desired result follows. □

From Lemma 3.2, we see that each codeword of $\mathcal{L}_{\mathcal{A}}(\mathcal{C})$ is a concatenation of the codewords of an η-constacyclic code in $\mathbb{F}_{q^2}[x]/\langle x^n - \eta\rangle$. This directly yields the following theorem.

Theorem 3.3 *Let $\mathcal{C}$ be the η-constacyclic code in $\mathbb{F}_{q^{2m}}[x]/\langle x^n - \eta\rangle$ with zero set Z_{2m}. Let $\mathcal{D}$ be the η-constacyclic code in $\mathbb{F}_{q^2}[x]/\langle x^n - \eta\rangle$ with zero set Z_2, where Z_2 is defined as (3). If $\mathcal{D} \subseteq \mathcal{D}^{\perp_H}$, then $\mathcal{L}_{\mathcal{A}}(\mathcal{C}) \subseteq \mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_H}$.*

According to Theorem 3.3, if $\mathcal{C}$ is an η-constacyclic $[n, k]$ code over $\mathbb{F}_{q^{2m}}$ such that $\mathcal{D} \subseteq \mathcal{D}^{\perp_H}$, then $\mathcal{L}_{\mathcal{A}}(\mathcal{C})$ is Hermitian self-orthogonal and has parameters $[nm, mk]$. By Lemma 3.1, $\mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_H} = \mathcal{L}_{\mathcal{B}}(\mathcal{C}^{\perp_H})$ or $\mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_H} = \mathcal{L}_{\mathcal{B}}(\mathcal{C}^{\perp_H})^q$. Hence, $\mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_H}$ has parameters $[nm, nm - mk, \geq d^{\perp}]$, where $d^{\perp}$ is the minimum Hamming distance of $\mathcal{C}^{\perp_H}$. By the Hermitian construction, a q-ary $[[mn, mn-2mk, \geq d^{\perp}]]$ can be obtained from $\mathcal{L}_{\mathcal{A}}(\mathcal{C})$. To construct quantum codes of length mn, we need to find Hermitian self-orthogonal constacyclic codes over $\mathbb{F}_{q^2}$ of length n. For this, assume that $\eta = \omega^{\ell(q-1)}$, for some $\ell \in \{0, 1, \ldots, q\}$, then the Hermitian dual code of an η-constacyclic code over $\mathbb{F}_{q^2}$ is still η-constacyclic [18]. We now give a sufficient condition for $\mathcal{L}_{\mathcal{A}}(\mathcal{C})$ to be Hermitian self-orthogonal. We first give the following useful lemma.

Lemma 3.4 *Let $\mathcal{C}$ be the η-constacyclic code in $\mathbb{F}_{q^{2m}}[x]/\langle x^n - \eta\rangle$ with nonzero set T_{2m}. Denote $T_2 = \bigcup_{s \in T_{2m}} C_{q^2}[s, nr]$. Then $-qT_2 \bigcap T_2 = \emptyset$ if and only if $aq^{2\ell+1} + b \not\equiv 0 (\mathrm{mod}\ nr)$ for any $a, b \in T_{2m}$ and any nonnegative integer ℓ.*

Proof The necessity directly follows from the condition that $-qT_2 \bigcap T_2 = \emptyset$. We now prove the sufficiency. Suppose that $-qT_2 \bigcap T_2 \neq \emptyset$. Then there exists $z \in \Omega$ such that $z \in -qT_2 \bigcap T_2$. This means that $C_{q^2}[z, nr] \subseteq -qT_2 \bigcap T_2$. Hence, we can find $y \in T_{2m}$ such that $y \in C_{q^2}[z, nr]$. Meanwhile, we can also find $x \in T_2$ such that $y \equiv -qx (\mathrm{mod}\ nr) \in C_{q^2}[z, nr]$. By the condition, x must be not in T_{2m}. From the definition of T_2, there exists $w \in T_{2m}$ such that $x \in C_{q^2}[w, nr]$. This means that $x \equiv wq^{2\ell} (\mathrm{mod}\ nr)$, for some integer ℓ. Hence, $y \equiv -wq^{2\ell+1} (\mathrm{mod}\ nr)$, which contradicts the assumption. Hence, $-qT_2 \bigcap T_2 = \emptyset$. This completes the proof. □

Theorem 3.5 *Let $\mathcal{C}$ be the η-constacyclic code in $\mathbb{F}_{q^{2m}}[x]/\langle x^n - \eta\rangle$ with nonzero set T_{2m}. Assume that $aq^{2\ell+1} + b \not\equiv 0 (\mathrm{mod}\ nr)$ for any $a, b \in T_{2m}$ and any nonnegative integer ℓ. Then $\mathcal{L}_{\mathcal{A}}(\mathcal{C}) \subseteq \mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_H}$.*

Proof Let Z_{2m} be the zero set of $\mathcal{C}$. Let $\mathcal{D}$ be the η-constacyclic code over $\mathbb{F}_{q^2}$ of length n with zero set Z_2, where Z_2 is given as (3). Then $\mathcal{D}^{\perp_H}$ has zero set

$$Z_2^{\perp_H} = \{z \in \Omega \mid -qz (\mathrm{mod}\ nr) \notin Z_2\}.$$

Let y be any element in $Z_2^{\perp_H}$. Then $-qy(\bmod\ nr) \notin Z_2$. We claim that $-qy(\bmod\ rn) \in T_2 = \bigcup_{s\in T_{2m}} C_{q^2}[s, nr]$. In fact, if $-qy(\bmod\ nr) \in T_{2m}$, then it is obvious that $-qy(\bmod\ nr) \in T_2$. If $-qy(\bmod\ rn) \notin T_{2m}$, then $-qy(\bmod\ rn) \in Z_{2m}$. By the definition of Z_2, there exists $w \in T_{2m}$ such that $-qy(\bmod\ nr) \in C_{q^2}[w, nr]$, which means that $-qy(\bmod nr) \in T_2$. By Lemma 3.4, we know $-qT_2 \bigcap T_2 = \emptyset$. So, $y \notin T_2$, which means $y \in Z_2$. This shows that $Z_2^{\perp_H} \subseteq Z_2$. Hence, $\mathcal{D} \subseteq \mathcal{D}^{\perp_H}$. By Theorem 3.3, $\mathcal{L}_{\mathcal{A}}(\mathcal{C}) \subseteq \mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_H}$. □

Theorem 3.5 provides a method for constructing Hermitian self-orthogonal codes by exploiting the q^2-ary images of constacyclic codes over $\mathbb{F}_{q^{2m}}$. It is worth mentioning that constacyclic codes over $\mathbb{F}_{q^{2m}}$ in Theorem 3.5 are not necessarily Hermitian self-orthogonal. For any $a, b \in T_{2m}$, note that $aq^{2\ell+1} + b \not\equiv 0(\bmod\ nr)$ for any nonnegative integer ℓ if and only if $C_{q^2}[a, nr] \neq -qC_{q^2}[b, nr]$.

4 Quantum codes

In this section, we will use constacyclic MDS codes over $\mathbb{F}_{q^{2m}}$ to construct two classes of quantum codes.

4.1 Construction I

We first consider constacyclic MDS codes over $\mathbb{F}_{q^{2m}}$ of length $n = q^{2m} + 1$, where $m \geq 2$. We divide the prime power q into two cases.

Case 1: q is even

In this case, all the q^{2m}-cyclotomic cosets modulo n are given by $C_{q^{2m}}[0, n] = \{0\}$ and $C_{q^{2m}}[\frac{n-1}{2} - i, n] = \{\frac{n-1}{2} - i, \frac{n-1}{2} + i + 1\}$, for $0 \leq i \leq \frac{n-3}{2}$ [28]. Define

$$\Delta_1 = \begin{cases} \frac{q^{m+1}-q^2-2}{2}, & \text{if } m = 2\nu \geq 2; \\ \frac{q^m-2}{2}, & \text{if } m = 2\nu + 1 \geq 3. \end{cases} \tag{4}$$

Lemma 4.1 *Let $n = q^{2m} + 1$, where q is an even prime power and $m \geq 2$ is a positive integer. If $\mathcal{C}$ is the cyclic code over $\mathbb{F}_{q^{2m}}$ of length n with nonzero set $T_{2m} = \bigcup_{i=0}^{\delta} C_{q^{2m}}[\frac{n-1}{2} - i, n]$, where $0 \leq \delta \leq \Delta_1$, then $\mathcal{L}_{\mathcal{A}}(\mathcal{C}) \subseteq \mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_H}$.*

Proof We prove that, for any $a, b \in T_{2m}$, $C_{q^2}[a, n] \neq -qC_{q^2}[b, n]$. Suppose that there exist $a = \frac{n-1}{2} - j$ and $b = \frac{n-1}{2} - k$ with $j, k \in \{0, 1, \ldots, \Delta_1\}$ such that $aq^{2\ell+1} + b \equiv 0(\bmod\ n)$ for $0 \leq \ell \leq 2m - 1$. That is, for $0 \leq \ell \leq 2m - 1$,

$$(1 + 2j)q^{2\ell+1} + (1 + 2k) \equiv 0(\bmod\ n). \tag{5}$$

Observe that $(1 + 2j) + (1 + 2k)q^{2(2m-\ell-1)+1} \equiv 0(\bmod\ n)$, so we can assume that $0 \leq \ell \leq m - 1$. We only seek a contradiction for the case that m is even. The case that m is odd is very similar and omitted.

If $0 \leq \ell \leq \frac{m-2}{2}$, then $1 + q \leq (1 + 2j)q^{2\ell+1} + (1 + 2k) < n$. This gives a contradiction.

If $\frac{m}{2} \leq \ell \leq m - 1$, from (5) we get that $(1 + 2k)q^{2(m-\ell)-1} \equiv 1 + 2j (\bmod n)$. Note that $q \leq (1 + 2k)q^{2(m-\ell)-1} < n$ and $1 \leq 1 + 2j \leq q^{m+1} - q^2 - 1$. It must be $(1 + 2k)q^{2(m-\ell)-1} = 1 + 2j$. This is impossible since $(1 + 2k)q^{2(m-\ell)-1}$ is even and $1 + 2j$ is odd.

Hence, for any $a, b \in T_{2m}$, $C_{q^2}[a, n] \neq -qC_{q^2}[b, n]$. By Theorem 3.5, we have the desired result. □

Based on q^{2m}-ary cyclic codes, we now construct q-ary quantum codes by using the Hermitian construction.

Theorem 4.2 *Let $n = q^{2m} + 1$, where q is an even prime power and $m \geq 2$ is a positive integer. Then there exists a q-ary quantum code with parameters* $[[mn, mn - 4m(\delta + 1), \geq 2\delta + 3]]$, *where* $0 \leq \delta \leq \Delta_1$.

Proof Let $\mathcal{C}$ be the q^{2m}-ary cyclic code of length n with nonzero set

$$T_{2m} = \bigcup_{i=0}^{\delta} C_{q^{2m}}[(n-1)/2 - i, n],$$

where $0 \leq \delta \leq \Delta_1$. By Lemma 4.1, $\mathcal{L}_{\mathcal{A}}(\mathcal{C}) \subseteq \mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_H}$. Note that $\mathcal{C}$ has zero set

$$S_{2m} = C_{q^{2m}}[0, n] \bigcup \bigcup_{i=\delta+1}^{(n-3)/2} C_{q^{2m}}[(n-1)/2 - i, n].$$

Since S_{2m} consists of $(n - 2\delta - 2)$ consecutive integers

$$\left\{0, 1, -1, \ldots, \frac{n-1}{2} - \delta - 1, -\left(\frac{n-1}{2} - \delta - 1\right)\right\},$$

it follows that $\mathcal{C}$ is an $[n, 2\delta + 2, n - 2\delta - 1]$ MDS code over $\mathbb{F}_{q^{2m}}$. Hence, $\mathcal{C}^{\perp_H}$ is MDS and has minimum distance $2\delta + 3$. By Lemma 3.1, $\mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_H} \geq 2\delta + 3$. Hence, $\mathcal{L}_{\mathcal{A}}(\mathcal{C})$ has dimension $2m(\delta + 1)$ and dual distance $d^{\perp} \geq 2\delta + 3$. Applying the Hermitian construction to the code $\mathcal{L}_{\mathcal{A}}(\mathcal{C})$ can yield the desired q-ary quantum code. □

Example 4.3 Let $q = 2$ and $m = 2$. Then $n = 17$. Applying Theorem 4.2, we obtain binary quantum codes with parameters $[[34, 26, \geq 3]]$ and $[[34, 18, \geq 5]]$. They have the same parameters as the best known binary quantum codes in the Database [14].

Example 4.4 Let $q = 2$ and $m = 3$. Then $n = 65$. Applying Theorem 4.2, we can get 4 binary quantum codes of length 195. On this length, the resulting quantum codes have larger code rate than the quantum twisted codes shown in [11]. We list them in Table 1.

Table 1 Code comparison

New quantum codes	Quantum twisted codes in [11]
$[[195, 183, \geq 3]]_2$	$[[195, 183, 3]]_2$
$[[195, 171, \geq 5]]_2$	$[[195, 163, 5]]_2$
$[[195, 159, \geq 7]]_2$	$[[195, 135, 7]]_2$
$[[195, 147, \geq 9]]_2$	$[[195, 123, 9]]_2$

Case 2: q is odd

Let $\eta = \omega^{q-1}$, where ω is a primitive element of $\mathbb{F}_{q^2}$. Let $\mathcal{C}$ be an η-constacyclic code over $\mathbb{F}_{q^{2m}}$ of length $n = q^{2m} + 1$, where $m \geq 2$ is a positive integer. All the q^{2m}-cyclotomic cosets modulo $(q+1)n$ containing the elements in $\Omega = \{1 + (q+1)j \mid 0 \leq j \leq n-1\}$ are given as follows [18].

(1) $C_{q^{2m}}[\frac{n}{2}, (q+1)n] = \{\frac{n}{2}\}$ and $C_{q^{2m}}[\frac{n(q+2)}{2}, (q+1)n] = \left\{\frac{n(q+2)}{2}\right\}$.

(2) $C_{q^{2m}}[\frac{n}{2} - (q+1)j, (q+1)n] = \left\{\frac{n}{2} - (q+1)j, \frac{n}{2} + (q+1)j\right\}$ for $1 \leq j \leq \frac{n-2}{2(q+1)}$, and $C_{q^{2m}}[\frac{n(q+2)}{2} - (q+1)j, (q+1)n] = \left\{\frac{n(q+2)}{2} - (q+1)j, \frac{n(q+2)}{2} + (q+1)j\right\}$ for $1 \leq j \leq \frac{q(n-2)}{2(q+1)}$.

Constacyclic BCH codes in $\mathbb{F}_{q^2}[x]/\langle x^n - \eta\rangle$ with length $n = q^{2m} + 1$ have been studied in [26], where maximum designed distances such that these codes are Hermitian dual-containing codes are given. Now, we use the maximum designed distances for constructing quantum codes. Define

$$\Delta_2 = \begin{cases} \frac{q^3-q^2+q-1}{2}, & \text{if } m = 2; \\ \frac{q^{m+1}-q^2}{2}, & \text{if } m = 2\nu \geq 4; \\ \frac{q^m-1}{2}, & \text{if } m = 2\nu + 1 \geq 3. \end{cases} \tag{6}$$

Lemma 4.5 *Let $\eta = \omega^{q-1}$, where ω is a primitive element of $\mathbb{F}_{q^2}$. Let $n = q^{2m} + 1$, where q is an odd prime power and $m \geq 2$ is a positive integer. If $\mathcal{C}$ is the η-constacyclic code of length n over $\mathbb{F}_{q^{2m}}$ with nonzero set $T_{2m} = \bigcup_{i=0}^{\delta} C_{q^{2m}}[\frac{n}{2} - (q+1)i, (q+1)n]$, where $0 \leq \delta \leq \Delta_2$, then $\mathcal{L}_{\mathcal{A}}(\mathcal{C}) \subseteq \mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_H}$.*

Proof By Corollary 3.4 in [26], we have $-qT_2 \bigcap T_2 = \emptyset$, which means that $C_{q^2}[a, n] \neq -qC_{q^2}[b, n]$ for any $a, b \in T_{2m}$. Hence, $\mathcal{L}_{\mathcal{A}}(\mathcal{C}) \subseteq \mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_H}$. □

Theorem 4.6 *Let $n = q^{2m} + 1$, where q is an odd prime power and $m \geq 2$ is a positive integer. Then there exists a q-ary quantum code with parameters $[[mn, mn - 2m(2\delta + 1), \geq 2\delta + 2]]$, where $0 \leq \delta \leq \Delta_2$.*

Proof Let $\mathcal{C}$ be the η-constacyclic code of length n over $\mathbb{F}_{q^{2m}}$ with nonzero set $T_{2m} = \bigcup_{i=0}^{\delta} C_{q^{2m}}[\frac{n}{2} - (q+1)i, n]$, where $0 \leq \delta \leq \Delta_2$. Then the zero set of $\mathcal{C}$ is $S = \Omega \backslash T_{2m}$, which contains $(n - 2\delta - 1)$ integers at intervals of $q + 1$. It then follows that $\mathcal{C}$ is an $[n, 2\delta + 1, n - 2\delta]$ MDS code over $\mathbb{F}_{q^{2m}}$. Hence, $\mathcal{C}^{\perp_H}$ is MDS and has minimum distance $2\delta + 2$. By Lemma 3.1, the minimum distance of $\mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_H}$ is at least $2\delta + 2$.

Table 2 Code comparison

New quantum codes	Punctured codes	Quantum twisted codes in [11]
$[[164, 128, \geq 10]]_3$	$[[161, 128, \geq 7]]_3$	$[[161, 127, 7]]_3$
$[[164, 120, \geq 12]]_3$	$[[161, 120, \geq 9]]_3$	$[[161, 115, 9]]_3$
$[[164, 112, \geq 14]]_3$	$[[161, 112, \geq 11]]_3$	$[[161, 111, 11]]_3$
$[[164, 104, \geq 16]]_3$	$[[161, 104, \geq 13]]_3$	$[[161, 99, 13]]_3$
$[[164, 96, \geq 18]]_3$	$[[161, 96, \geq 15]]_3$	$[[161, 87, 15]]_3$
$[[164, 88, \geq 20]]_3$	$[[161, 88, \geq 17]]_3$	$[[161, 75, 17]]_3$

Also, $\mathcal{L}_{\mathcal{A}}(\mathcal{C})$ has dimension $m(2\delta+1)$. By the Hermitian construction, a q-ary quantum code with parameters $[[mn, mn-2m(2\delta+1), \geq 2\delta+2]]$ is obtained. □

Example 4.7 Let $q=3$ and $m=2$. Then $n=82$. Using Theorem 4.6, we obtain 11 new ternary quantum codes of length 164. Further, we can obtain 10 ternary quantum codes of length 161 by using a propagation rule [12]. Six codes of them have larger code rate than the quantum twisted codes with the same length. We list these codes in Table 2.

4.2 Construction II

Now, let us consider cyclic codes over $\mathbb{F}_{q^{2m}}$ of length $n=\frac{q^{2m}+1}{q^2+1}$, where q is an even prime power and $m \geq 3$ is odd. It is easy to obtain that, for $1 \leq i \leq \frac{n-1}{2}$, all the q^{2m}-cyclotomic cosets modulo n are given by $C_{q^{2m}}[0,n]=\{0\}$ and $C_{q^{2m}}[i,n]=\{i, n-i\}$. Define

$$\Delta_3 = \begin{cases} \frac{q^{m+1}+q^m-3q^2-q-2}{2(q^2+1)}, & \text{if } m \equiv 1 (\text{mod } 4); \\ \frac{q^{m+1}+q^m-3q^2+q-4}{2(q^2+1)}, & \text{if } m \equiv 3 (\text{mod } 4). \end{cases} \tag{7}$$

Lemma 4.8 *Let $n=\frac{q^{2m}+1}{q^2+1}$, where q is an even prime power and $m \geq 3$ is odd. If $\mathcal{C}$ is the cyclic code of length n over $\mathbb{F}_{q^{2m}}$ with nonzero set $T_{2m}=\bigcup_{i=0}^{\delta} C_{q^{2m}}[(n-1)/2-i, n]$, where $0 \leq \delta \leq \Delta_3$, then $\mathcal{L}_{\mathcal{A}}(\mathcal{C}) \subseteq \mathcal{L}_{\mathcal{A}}(\mathcal{C})^{\perp_H}$.*

Proof We only prove the case that $m \equiv 1(\text{mod } 4)$, and the other case is similar. By Theorem 3.5, we only need to prove that, for any $a, b \in T_{2m}$, $C_{q^2}[a,n] \neq -qC_{q^2}[b,n]$. Suppose that there exist $a=\frac{n-1}{2}-j$ and $b=\frac{n-1}{2}-k$ with $j, k \in \{0, 1, \ldots, \Delta_3\}$ such that $aq^{2\ell+1}+b \equiv 0(\text{mod } n)$ for $0 \leq \ell \leq 2m-1$. This means that, for $0 \leq \ell \leq 2m-1$,

$$(q^2+1)\left[(1+2j)q^{2\ell+1}+(1+2k)\right] \equiv 0(\text{mod } q^{2m}+1). \tag{8}$$

Note that $q^{4m} \equiv 1(\text{mod } q^{2m}+1)$, so we can assume that $0 \leq \ell \leq m-1$.

If $0 \le \ell \le \frac{m-3}{2}$, then it is easy to verify that the left-hand side of (8) is between $(q+1)(q^2+1)-1$ and $q^{2m}+1$. This gives a contradiction.

If $\ell = \frac{m-1}{2}$, then (8) becomes

$$(q^2+1)\left[(1+2j)q^m+(1+2k)\right] \equiv 0(\text{mod } q^{2m}+1).$$

Then

$$(q^2+1)\left[(1+2j)q^m+(1+2k)\right] = \lambda(q^{2m}+1), \tag{9}$$

for some odd integer λ. Since $(q^2+1)(q^m+1) \le (q^2+1)[(1+2j)q^m+(1+2k)] < (q+1)(q^{2m}+1)$ holds, it follows that $1 \le \lambda \le q-1$. By taking (9) modulo q^m, we obtain $(q^2+1)(1+2k)-\lambda \equiv 0(\text{mod } q^m)$. Let

$$(q^2+1)(1+2k)-\lambda = \mu q^m, \tag{10}$$

for some integer μ. Since

$$q^2-q+2 \le (q^2+1)(1+2k)-\lambda \le q^{m+1}+q^m-2q^2-q-2$$

holds, we have $1 \le \mu \le q$. Taking (10) modulo q^2+1 can get $\mu q+\lambda \equiv 0(\text{ mod } q^2+1)$. Then $\mu q+\lambda = q^2+1$, which implies that $\mu = q$ and $\lambda = 1$. By putting them into (9) and (10), it can be obtained from the obtained equations that $(q^2+1)(1+2j) = q^m-q$. But, $(q^2+1)(1+2j)$ is odd and q^m-q is even, which is a contradiction.

If $\frac{m+1}{2} \le \ell \le m-1$, then it follows from (8) that $(q^2+1)(1+2k)q^{2(m-\ell)-1} \equiv (q^2+1)(1+2j)(\text{ mod } q^{2m}+1)$. Note that two sides are both between 1 and $q^{2m}+1$. Hence, $(1+2k)q^{2(m-\ell)-1} = 1+2j$. This is a contradiction since $(1+2k)q^{2(m-\ell)-1}$ is even and $1+2k$ is odd. □

According to Lemma 4.8, similar to Theorem 4.2, we easily obtain the following result.

Theorem 4.9 *Let $n = \frac{q^{2m}+1}{q^2+1}$, where q is an even prime power and $m \ge 3$ is odd. Then there exists a q-ary quantum code with parameters $[[mn, mn-4m(\delta+1), \ge 2\delta+3]]$, where $0 \le \delta \le \Delta_3$.*

Example 4.10 Let $q = 4$ and $m = 3$. Then $n = 241$. By using Theorem 4.9, we can get 9 quaternary quantum codes of length 723. The resulting quantum codes have larger minimum distance than the quantum twisted codes with the same dimension shown in [11]. These codes are listed in Table 3.

5 Conclusion

In this paper, we gave a sufficient condition for the images of η-constacyclic codes over $\mathbb{F}_{q^{2m}}$ to be Hermitian self-orthogonal codes over $\mathbb{F}_{q^2}$, where η is a nonzero element of

Table 3 Code comparison

New quantum codes	Quantum twisted codes in [11]
$[[723, 711, \geq 3]]_4$	$[[723, 709, 3]]_4$
$[[723, 687, \geq 7]]_4$	$[[723, 687, 5]]_4$
$[[723, 675, \geq 9]]_4$	$[[723, 675, 6]]_4$
$[[723, 663, \geq 11]]_4$	$[[723, 663, 7]]_4$
$[[723, 651, \geq 13]]_4$	$[[723, 651, 8]]_4$
$[[723, 639, \geq 15]]_4$	$[[723, 639, 9]]_4$
$[[723, 627, \geq 17]]_4$	$[[723, 627, 11]]_4$
$[[723, 615, \geq 19]]_4$	$[[723, 615, 12]]_4$

$\mathbb{F}_{q^2}$. Then, by choosing constacyclic MDS codes over $\mathbb{F}_{q^{2m}}$, we obtained Hermitian self-orthogonal codes over $\mathbb{F}_{q^2}$. Further, we constructed quantum codes with good parameters. The resulting quantum codes are actually concatenated codes, and hence they can be encoded and decoded by using the spectral techniques (see [16]). Based on the twisted discrete Fourier transform over finite fields, we can copy the syndrome of an error vector to auxiliary qubits using the controlled NOT (CNOT) gate. Through measuring the syndromes of bit-flip and phase-flip errors, the most likely positions of errors are determined. A further work is to provide an efficient encoding and decoding algorithm for this class of concatenated quantum codes.

Funding This study is supported by the National Natural Science Foundation of China under Grant Nos. 61972126, 61772168 and 61802102, the Natural Science Foundation of Anhui Province under Grant No. 1808085MA15 and the Key University Science Research Project of Anhui Province under Grant No. KJ2018A0497.

Compliance with Ethical Standards

Conflict of Interest All the authors declare that they have no conflict of interest.

Ethical approval All the procedures performed in this study were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki Declaration and its later amendments or comparable ethical standards.

Informed consent Informed consent was obtained from all individual participants included in the study.

References

1. Aly, S.A., Klappenecker, A., Sarvepalli, P.K.: On quantum and classical BCH codes. IEEE Trans. Inf. Theory **53**(3), 1183–1188 (2007)
2. Ashikhmin, A.R., Knill, E.: Nonbinary quantum stablizer codes. IEEE Trans. Inf. Theory **47**(7), 3065–3072 (2001)
3. Aydin, N., Siap, I., Ray-Chaudhuri, D.J.: The structure of 1-generator quasi-twisted codes and new linear codes. Des. Codes Cryptogr. **24**, 313–326 (2001)
4. Bierbrauer, J., Edel, Y.: Quantum twisted codes. J. Comb. Des. **8**, 174–188 (2000)
5. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via codes over GF(4). IEEE Trans. Inf. Theory **44**(4), 1369–1389 (1998)

6. Chen, B., Ling, S., Zhang, G.: Applications of constacyclic codes of quantum MDS codes. IEEE Trans. Inf. Theory **61**(3), 1474–1484 (2015)
7. Chen, H., Ling, S., Xing, C.: Quantum codes from concatenated algebraic-geometric codes. IEEE Trans. Inf. Theory **51**(8), 2915–2920 (2005)
8. Chen, J., Chen, Y., Huang, Y., Feng, C.: New optimal asymmetric quantum codes and quantum convolutional codes derived from constacyclic codes. Quantum Inf. Process. **18**, 40 (2019)
9. Chuang, L.L., Gershenfeld, N., Kubinec, M.: Experimental implementation of fast quantum searching. Phys. Rev. Lett. **80**(15), 3408–3411 (1998)
10. Cohen, G., Encheva, S., Litsyn, S.: On binary constructions of quantum codes. IEEE Trans. Inf. Theory **45**(7), 2495–2498 (1999)
11. Edel, Y.: Some good quantum twisted codes. https://www.mathi.uniheidelberg.de/yves/Matritzen/QTBCH/QTBCHIndex.html (2020). Accessed 12 Apr 2020
12. Feng, K., Ling, S., Xing, C.: Asymptotic bounds on quantum codes from algebraic geometry codes. IEEE Trans. Inf. Theory **52**(3), 986–991 (2006)
13. Gadim, M.R., Navimipour, N.J.: Quantum-dot cellular automata in designing the arithmetic and logic unit: systematic literature review, classification and current trends. J. Circuits Syst. Comput. **27**(10), 1830005(1-24) (2018)
14. Grassl, M.: Bounds on the minimum distance of linear codes. http://www.codetables.de (2020). Accessed on 12 Apr 2020
15. Grassl, M., Beth, T.: Cyclic quantum error-correcting codes and quantum shift registers. Proc. R. Soc. Lond. A **456**(2003), 2689–2706 (2000)
16. Grassl, M., Geiselmann, W., Beth, T.: Quantum Reed–Solomon codes. In: Proceedings of AAECC, vol. 13, pp. 231–244 (1999)
17. Hu, X., Zhang, G., Chen, B.: Constructions of new nonbinary quantum codes. Int. J. Theor. Phys. **54**(1), 92–99 (2015)
18. Kai, X., Zhu, S., Li, P.: Constacyclic codes and some new quantum MDS codes. IEEE Trans. Inf. Theory **60**(4), 2080–2086 (2014)
19. Kai, X., Zhu, S., Tang, Y.: Quantum negacyclic codes. Phys. Rev. A **88**(7), 012326(1-5) (2013)
20. Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.K.: Nonbinary stabilizer codes over finite fields. IEEE Trans. Inf. Theory **52**(11), 4892–4914 (2006)
21. Krishna, A., Sarwate, D.V.: Pseudocyclic maximum-distance-separable codes. IEEE Trans. Inf. Theory **36**(4), 880–884 (1990)
22. La Guardia, G.G.: Constructions of new families of nonbinary quantum codes. Phys. Rev. A **80**(10), 042331(1-11) (2009)
23. Lee, J., Lee, E.K., Kim, J., Lee, S.: Quantum shift registers. arXiv:quant-ph/0112107
24. Lin, X.: Quantum cyclic and constacyclic codes. IEEE Trans. Inf. Theory **50**(3), 547–549 (2004)
25. Ling, S., Luo, J., Xing, C.: Generalization of Steane's enlargement construction of quantum codes and applications. IEEE Trans. Inf. Theory **56**(8), 4080–4084 (2010)
26. Liu, Y., Li, R., Lv, L., Ma, M.: A class of constacyclic BCH codes and new quantum codes. Quantum Inf. Process. **16**(2), 66(1-16) (2017)
27. Ma, Z., Lu, X., Feng, K., Feng, D.: On non-binary quantum BCH codes. In: Lecture Notes in Computer Science, vol. 3959, pp. 675–683 (2006)
28. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977)
29. Marinescu, D.C., Marinescu, G.M.: Classical and Quantum Information. Elsevier/Academic Press, Amsterdam (2012)
30. Moharrami, E., Navimipour, N.J.: Designing nanoscale counter using reversible gate based on quantum-dot cellular automata. Int. J. Theor. Phys. **57**(4), 1060–1081 (2018)
31. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
32. Seyedi, S., Darbandi, M., Navimipour, N.J.: Designing an efficient fault tolerance D-latch based on quantum-dot cellular automata nanotechnology. Optics **185**(5), 827–837 (2019)
33. Shor, P.W.: Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A **52**(4), 2493–2496 (1995)
34. Steane, A.M.: Error correcting codes in quantum theory. Phys. Rev. Lett. **77**(5), 793–797 (1996)
35. Steane, A.M.: Enlargement of Calderbank–Shor–Steane quantum codes. IEEE Trans. Inf. Theory **45**(7), 2492–2495 (1999)

36. Sundeep, B., Thangaraj, A.: Self-orthogonality of q-ary images of q^m-ary codes and quantum code construction. IEEE Trans. Inf. Theory **53**(7), 2480–2489 (2007)
37. Thangaraj, A., McLaughlin, S.W.: Quantum codes from cyclic codes over GF(4^m). IEEE Trans. Inf. Theory **47**(3), 1176–1178 (2001)
38. Wan, Z.X.: Lectures on Finite Fields and Galois Rings. World Scientific, Singapore (2003)
39. Wang, L., Zhu, S.: New quantum MDS codes derived from constacyclic codes. Quantum Inf. Process. **14**(3), 881–889 (2015)
40. Wang, Y., Gao, J.: Constacyclic codes over the ring $\mathbb{F}_q + v\mathbb{F}_q$ and their applications of constructing new non-binary quantum codes. Int. J. Inf. Coding Theory **5**(2), 130–141 (2018)
41. Wilde, M.M.: Quantum-shift-register circuits. Phys. Rev. A **79**(6), 062325(1-16) (2009)
42. Wooters, W.K., Zurek, W.H.: A single quantum cannot be cloned. Nature **299**(5886), 802–803 (1982)