Int J Theor Phys (2018) 57:1829–1838
https://doi.org/10.1007/s10773-018-3708-4

Two Classes of New Optimal Asymmetric Quantum Codes

Xiaojing Chen[1] · Shixin Zhu[1] · Xiaoshan Kai[1]

Received: 28 September 2017 / Accepted: 24 February 2018 / Published online: 5 March 2018

Abstract Let q be an even prime power and ω be a primitive element of $\mathbb{F}_{q^2}$. By analyzing the structure of cyclotomic cosets, we determine a sufficient condition for ω^{q-1}-constacyclic codes over $\mathbb{F}_{q^2}$ to be Hermitian dual-containing codes. By the CSS construction, two classes of new optimal AQECCs are obtained according to the Singleton bound for AQECCs.

Keywords Constacyclic codes · AQECCs · Singleton bound

1 Introduction

Since the pioneering work of Shor [1] and Steane [2] in 1995–1996, the research on quantum error-correcting codes (QECCs) has experienced tremendous growth. Many good QECCs have been constructed by using classical error-correcting codes, such as Bose-Chaudhuri-Hocquenghem (BCH) codes, Reed-Solomon (RS) codes, algebraic geometric codes and so

This research is supported by the National Natural Science Foundation of China (No. 61772168; No. 61572168) and Anhui Provincial Natural Science Foundation (No. 1508085SQA198).

✉ Xiaojing Chen
chenxiaojing0909@126.com

Shixin Zhu
zhushixin@hfut.edu.cn

Xiaoshan Kai
kxs6@sina.com

[1] School of Mathematics, Hefei University of Technology, Hefei, 230009, Anhui, People's Republic of China

on. Calderbank et al. [3] studied quantum error correction via codes over GF(4). Grassl et al. [4] studied optimal maximal distance separable (MDS) quantum codes. Chen et al. [5] constructed good quantum codes from concatenated algebraic-geometric codes. Later, a lot of work has been done for the construction of QECCs (see Refs. [6–10]).

In Ref. [12], Steane initially pointed out that QECCs should take into account the asymmetry which the mechanisms for the occurrence of bit-flip and phase-flip errors are quite different. This class of quantum error-correcting codes is called asymmetric quantum error-correcting codes (AQECCs). Since then, many researchers have focused on constructing AQECCs. In asymmetric quantum channels, the probabilities of occurrence of qudit-flip errors and phase-shift errors are unequal. Currently, we use the parameters $[[n, k, d_z/d_x]]_q$ to denote an AQECC, where d_z is the minimum distance correcting to phase-shift errors and d_x is the minimum distance correcting to qudit-flip errors. Wang et al. [13] studied the characterization and constructions of asymmetric quantum codes. Guardia [14, 15] utilized classical BCH codes to construct new families of asymmetric quantum codes. Later, much good work on AQECCs over finite fields has been done in Refs. [16, 17]. Chen et al. [19] constructed new asymmetric quantum codes from negacyclic codes which achieve the Singleton bound for AQECCs. Wang et al. [18] constructed six families of new optimal AQECCs from dual-containing constacyclic codes over finite fields by using the CSS construction.

Recently, one found that there exist optimal symmetric and asymmetric quantum codes of length $n = \frac{q^2+1}{5}$, where q is some prime power. In Ref. [21], for any odd prime power q with the form $10m + 3$ or $10m + 7$, Kai et al. obtained two classes of quantum MDS codes with parameters $\left[\left[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 2, d\right]\right]$, where $2 \leq d \leq \frac{q+3}{2}$ is even. In Ref. [22], Zhang and Ge enlarged the minimum distance d to $6m + 2$ and $6m + 4$, respectively. For any even prime power $q \equiv 2(\text{mod } 10)$ or $q \equiv 8(\text{mod } 10)$, Li et al. [23] constructed some new quantum MDS codes of length $n = \frac{q^2+1}{5}$ by using pseudo-cyclic codes. In a recent paper [20], Xu et al. obtained two new classes of optimal asymmetric quantum codes from constacyclic codes. One of them has length $n = \frac{q^2+1}{5}$ and $d_z > q + 1$, where q is an odd prime power with the form $10t + 3$ or $10t + 7$ ($t \geq 0$ is integer). Inspired by the above work, we consider the case that $n = \frac{q^2+1}{5}$, where q is some even prime power. We construct two classes of new optimal AQECCs by employing constacyclic codes. Speaking specifically, for any even prime power $q = 2^e$ with e being odd, we construct two classes of asymmetric quantum codes with parameters as follows:

(i) $\left[\left[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2(s + t + 2), (2s + 3)/(2t + 3)\right]\right]_{q^2}$, where $e \equiv 1(\text{mod } 4)$ and $0 \leq t \leq s \leq \frac{3q-16}{10}$.

(ii) $\left[\left[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2(s + t + 2), (2s + 3)/(2t + 3)\right]\right]_{q^2}$, where $e \equiv 3(\text{mod } 4)$ and $0 \leq t \leq s \leq \frac{3q-14}{10}$.

This paper is organized as follows. In Section 2, some basic background and results about constacyclic codes are reviewed. In Section 3, we briefly review some basic definitions of AQECCs. In Section 4, we give a sufficient condition for constacyclic codes which contain their Hermitian dual codes first, and then give our construction of AQECCs. Section 5 concludes the paper.

2 Preliminaries

Let $\mathbb{F}_{q^2}$ be a finite field with q^2 elements, where q is a power of a prime p. For any element $x \in \mathbb{F}_{q^2}$, we denote the conjugate x^q of x by $\overline{x}$. Given two vectors $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$ and $\mathbf{y} = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}_{q^2}^n$, their Hermitian inner product is defined as

$$\langle \mathbf{x}, \mathbf{y} \rangle = x_0\overline{y}_0 + x_1\overline{y}_1 + \cdots + x_{n-1}\overline{y}_{n-1} \in \mathbb{F}_{q^2}.$$

The vectors $\mathbf{x}$ and $\mathbf{y}$ are called orthogonal with respect to the Hermitian inner product if $\langle \mathbf{x}, \mathbf{y} \rangle = 0$. A q^2-ary linear code $\mathcal{C}$ of length n is a nonempty subspace of the vector space $\mathbb{F}_{q^2}^n$. For a q^2-ary linear code $\mathcal{C}$, the Hermitian dual code of $\mathcal{C}$ is defined as

$$\mathcal{C}^{\perp_h} = \left\{ \mathbf{x} \in \mathbb{F}_{q^2}^n | \ \langle \mathbf{x}, \mathbf{y} \rangle = 0 \ for\ all\ \mathbf{y} \in \mathcal{C} \right\}.$$

A q^2-ary linear code $\mathcal{C}$ of length n is called Hermitian self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^{\perp_h}$, and it is called Hermitian self-dual if $\mathcal{C} = \mathcal{C}^{\perp_h}$. For a nonzero element η of $\mathbb{F}_{q^2}$, if $\mathcal{C}$ is closed under the η-constacyclic shift, i.e., if $(x_0, x_1, \ldots, x_{n-1}) \in \mathcal{C}$ implies $(\eta x_{n-1}, x_0, \ldots, x_{n-2}) \in \mathcal{C}$, then $\mathcal{C}$ is said to be an η-constacyclic code. Customarily, a codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ in $\mathcal{C}$ is identified with its polynomial representation $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$. It is well known that an η-constacyclic code $\mathcal{C} \in \mathbb{F}_{q^2}^n$ is an ideal of the quotient ring $\mathbb{F}_{q^2}[x]/\langle x^n - \eta \rangle$ and $\mathcal{C}$ can be generated by a monic divisor $g(x)$ of $x^n - \eta$. The polynomial $g(x)$ is called the generator polynomial of $\mathcal{C}$ and the dimension of $\mathcal{C}$ is $n - k$, where $k = \deg(g(x))$.

In the following, let ω be a primitive element of the finite field $\mathbb{F}_{q^2}$ and $\eta = \omega^{q-1}$. In this case, the order r of η in $\mathbb{F}_{q^2}^*$ is equal to $q+1$. Note that $\eta\bar{\eta} = 1$ in $\mathbb{F}_{q^2}$. Hence, the Hermitian dual code of a q^2-ary η-constacyclic code of length n is still η-constacyclic by Lemma 2.1 in Refs. [11]. Assume that $\gcd(q, n) = 1$. Let δ be a primitive rn-th root of unity in some extension field of $\mathbb{F}_{q^2}$ such that $\delta^n = \eta$. Let $\xi = \delta^r$, then ξ is a primitive n-th root of unity. Hence,

$$x^n - \eta = \prod_{j=0}^{n-1}(x - \delta\xi^j) = \prod_{j=0}^{n-1}(x - \delta^{1+jr}).$$

Let $\Omega = \{1 + jr | \ 0 \le j \le n-1\}$. For each $i \in \Omega$, let $\mathbb{C}_i$ be the q^2-cyclotomic coset modulo rn containing i. Then, $e_i(x) = \prod_{l \in \mathbb{C}_i}(x - \delta^l)$ is a monic irreducible divisor of $x^n - \eta$ over $\mathbb{F}_{q^2}$. Each $\mathbb{C}_i$ corresponds to an irreducible divisor of $x^n - \eta$ over $\mathbb{F}_{q^2}$. Let $\mathcal{C}$ be an η-constacyclic code of length n over $\mathbb{F}_{q^2}$ with generator polynomial $g(x)$. Then the set $Z = \{i \in \Omega | \ g(\delta^i) = 0\}$ is called the defining set of $\mathcal{C}$. Obviously, the defining set of $\mathcal{C}$ must be a union of some q^2-cyclotomic cosets modulo rn. It is clear to see that $\mathcal{C}^{\perp_h}$ has defining set $Z^{\perp_h} = \{z \in \Omega | \ -qz \bmod rn \notin Z\}$. Besides, the defining set of $\mathcal{C}$ is a union of some q^2-cyclotomic cosets modulo rn and $\dim(\mathcal{C}) = n - |Z|$. The following lemma in Ref. [21] gives a necessary and sufficient condition of $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$.

Lemma 2.1 *Let $\mathcal{C}$ be an η-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set $Z \subseteq \Omega$. Then $\mathcal{C}$ contains its Hermitian dual code if and only if $Z \cap Z^{-q} = \emptyset$, where $Z^{-q} = \{-qz \ mod\ rn | \ z \in Z\}$.*

Similar to cyclic codes, there exists the following BCH bound for η-constacyclic codes in Refs. [24] and [25].

Theorem 2.2 ***(The BCH bound for constacyclic codes)*** *Assume that $gcd(q, n) = 1$. Let $\mathcal{C}$ be an η-constacyclic code of length n over $\mathbb{F}_{q^2}$, and let its generator polynomial $g(x)$ have the elements $\{\delta^{1+jr} | \, 0 \leq j \leq d-2\}$ as the roots, where δ is a primitive rn-th root of unity. Then the minimum distance of $\mathcal{C}$ is at least d.*

Next we recall several lemmas which are important for constructing asymmetric quantum codes in Refs. [24] and [26].

Lemma 2.3 *Let $\mathcal{C}_i$ be q^2-ary η-constacyclic codes of length n with defining set T_i for $i = 1, 2$, then $\mathcal{C}_1 \subseteq \mathcal{C}_2$ if and only if $T_2 \subseteq T_1$.*

Lemma 2.4 ***(Singleton bound)*** *If an $[n, k, d]$ linear code over $\mathbb{F}_q$ exists, then $k \leq n-d+1$. If the equality $k = n - d + 1$ holds, then the code is an MDS code.*

3 Asymmetric Quantum Error-Correcting Codes

In this section, we first give some basic definitions and results of AQECCs and then give the well-known CSS construction and Singleton bound for AQECCs. More details about AQECCs theory, please refer to Refs. [13–20] therein.

Suppose that p is the characteristic of the finite field $\mathbb{F}_q$. Let $\mathbb{H}$ be the Hilbert space $\mathbb{H} = \mathbb{C}^{q^n} = \mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q$, where $\mathbb{C}^q$ denotes a q-dimensional complex vector space representing the states of a quantum mechanical system. Let $|x\rangle$ be the vectors of an orthonormal basis of $\mathbb{C}^q$, where the labels x are elements of $\mathbb{F}_q$. Let a, b be two elements of $\mathbb{F}_q$. The unitary operators $X(a)$ and $Z(b)$ on $\mathbb{C}^q$ are defined as $X(a)|x\rangle = |x+a\rangle$ and $Z(b)|x\rangle = \omega^{tr(bx)}|x\rangle$, respectively, where tr is the trace map from $\mathbb{F}_q$ to the prime field $\mathbb{F}_p$ and $\omega = exp(2\pi i/p)$ is a primitive p-th root of unity. Let $\mathbf{a} = (a_1, a_2, \cdots, a_n) \in \mathbb{F}_q^n$ and $\mathbf{b} = (b_1, b_2, \cdots, b_n) \in \mathbb{F}_q^n$. Denote $X(\mathbf{a}) = X(a_1) \otimes X(a_2) \otimes \cdots \otimes X(a_n)$ and $Z(\mathbf{b}) = Z(b_1) \otimes Z(b_2) \otimes \cdots \otimes Z(b_n)$ by tensor products of n error operators. The set $\varepsilon_n = \{X(\mathbf{a})Z(\mathbf{b}) | \, \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n\}$ is an error basis on $\mathbb{C}^q$ and the set $G_n = \{\omega^c X(\mathbf{a})Z(\mathbf{b}) | \, \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n, c \in \mathbb{F}_p\}$ is the error group associated with ε_n.

For a quantum error $\alpha = \omega^c X(\mathbf{a})Z(\mathbf{b}) \in G_n$, the quantum weight $w_Q(\alpha)$, the X-weight $w_X(\alpha)$ and the Z-weight $w_Z(\alpha)$ of α are defined as:

$$\begin{aligned} w_Q(\alpha) &= \sharp\{i : 1 \leq i \leq n, (a_i, b_i) \neq (0, 0)\}, \\ w_X(\alpha) &= \sharp\{i : 1 \leq i \leq n, a_i \neq 0\}, \\ w_Z(\alpha) &= \sharp\{i : 1 \leq i \leq n, b_i \neq 0\}. \end{aligned}$$

A q-ary asymmetric quantum code $\mathcal{C}$, denoted by $[[n, k, d_z/d_x]]_q$, is a q^k-dimensional subspace of the Hilbert space $\mathbb{H}$ and can control all qubit-flip errors up to $\lfloor (d_x - 1)/2 \rfloor$ and all phase-flip errors up to $\lfloor (d_z - 1)/2 \rfloor$. The code $\mathcal{C}$ also detects $d_x - 1$ qubit-flip errors as well as detects $d_z - 1$ phase-shift errors. Then we give the well-known CSS construction and Singleton bound for AQECCs.

Theorem 3.1 [16] *If $\mathcal{C}_1 = [n, k_1, d_1]_{q^2}$ and $\mathcal{C}_2 = [n, k_2, d_2]_{q^2}$ are classical codes and satisfy $\mathcal{C}_1^{\perp_h} \subset \mathcal{C}_2$, then there is a $\Lambda = [[n, k_1 + k_2 - n, d_z/d_x]]_{q^2}$ AQECC, where*

$$d_z = max\left\{wt\left(\mathcal{C}_2 \backslash \mathcal{C}_1^{\perp_h}\right), wt\left(\mathcal{C}_1 \backslash \mathcal{C}_2^{\perp_h}\right)\right\}, \quad d_x = min\left\{wt\left(\mathcal{C}_2 \backslash \mathcal{C}_1^{\perp_h}\right), wt\left(\mathcal{C}_1 \backslash \mathcal{C}_2^{\perp_h}\right)\right\}.$$

Theorem 3.2 ***(Singleton bound for AQECCs)*** [19] *If asymmetric quantum code $\mathcal{C}$ with parameters $[[n, k_1 + k_2 - n, d_z/d_x]]$ exists, then $\mathcal{C}$ satisfies the asymmetric quantum Singleton bound*

$$k \leq n - d_z - d_x + 2.$$

If $\mathcal{C}$ satisfies the equality $k = n - d_z - d_x + 2$, then it is called an optimal code.

4 Construction of AQECCs

Throughout this section, let q be an even prime power, ω be a primitive element of the finite field $\mathbb{F}_{q^2}$ and $\eta = \omega^{q-1}$. We will use constacyclic codes over $\mathbb{F}_{q^2}$ to construct two classes of new optimal asymmetric quantum codes. Firstly, we give a sufficient condition for η-constacyclic codes over $\mathbb{F}_{q^2}$ of length n which contain their Hermitian dual codes. Secondly, we construct our new optimal AQECCs.

Let $q = 2^e$, where $e > 1$ is odd. Then 5 is a divisor of q^2+1. Let $n = \frac{q^2+1}{5}$, then n is odd. Now, we consider η-constacyclic codes over $\mathbb{F}_{q^2}$ of length n to construct AQECCs. First, we give a sufficient condition for η-constacyclic codes over $\mathbb{F}_{q^2}$ of length n which contain their Hermitian dual codes. To do this, we compute q^2-cyclotomic cosets modulo $(q+1)n$.

Lemma 4.1 *Let $q = 2^e$, where $e > 1$ is odd, $n = \frac{q^2+1}{5}$, $s = \frac{(q+6)n}{2}$ and $\Omega = \{1 + (q+1)j | \ 0 \leq j \leq n-1\}$. Then, for any integer $i \in \Omega$, then q^2-cyclotomic cosets $\mathbb{C}_i$ modulo $(q+1)n$ is given by*

1) $\mathbb{C}_s = \{s\}$;
2) $\mathbb{C}_{s-(q+1)j} = \{s - (q+1)j, s + (q+1)j\}$ *for* $1 \leq j \leq \frac{n-1}{2}$.

Proof 1) If $j = \frac{q^2+5q-4}{10}$, then $1 + (q+1)j = s$. This implies that s must be in Ω. Since $s = \frac{(q+6)n}{2}$, we have $sq^2 \equiv s \mod (q+1)n$. Therefore, $\mathbb{C}_s = \{s\}$.

2) We first prove that for each $i \in \Omega \setminus \{s\}$, the q^2-cyclotomic coset $\mathbb{C}_i$ modulo $(q+1)n$ has exactly two elements. In fact,

$$[s-(q+1)j]q^2 \equiv sq^2 - (q+1)j(q^2+1) + (q+1)j \equiv s + (q+1)j \mod (q+1)n.$$

Similarly, we have

$$[s+(q+1)j]q^2 \equiv sq^2 + (q+1)j(q^2+1) - (q+1)j \equiv s - (q+1)j \mod (q+1)n.$$

Suppose that $\mathbb{C}_i$ contains only one element. Since

$$s - \frac{(q+1)(n-1)}{2} \leq s - (q+1)j \leq s - q - 1$$

and

$$s + q + 1 \leq s + (q+1)j \leq s + \frac{(q+1)(n-1)}{2}$$

holds, it follows that $s - (q+1)j = s + (q+1)j$ or $(q+1)n + s - (q+1)j = s + (q+1)j$. If $s - (q+1)j = s + (q+1)j$, we have $2(q+1)j \equiv 0 \mod (q+1)n$. This implies that $2j = n$. However, $2 \leq 2j \leq n-1$, this gives a contradiction. If $(q+1)n + s - (q+1)j =$

$s+(q+1)j$, then we have $2(q+1)j \equiv 0 \mod (q+1)n$. This implies that $2j = n$. However, $2 \le 2j \le n-1$, this also gives a contradiction. Therefore,

$$\mathbb{C}_{s-(q+1)j} = \{s-(q+1)j, s+(q+1)j\} \; for \; 1 \le j \le \frac{n-1}{2}.$$

It remains to prove that $\mathbb{C}_{s-(q+1)k}$ and $\mathbb{C}_{s-(q+1)l}$ are distinct for $1 \le k \ne l \le \frac{n-1}{2}$. Suppose that $\mathbb{C}_{s-(q+1)k} = \mathbb{C}_{s-(q+1)l}$ for some integers k and l with $1 \le k \ne l \le \frac{n-1}{2}$. Then we can obtain a contradiction as follows:

Since $s-\frac{(q+1)(n-1)}{2} \le s-(q+1)k \le s-q-1$ and $s-\frac{(q+1)(n-1)}{2} \le s-(q+1)l \le s-q-1$, we have

$$s-(q+1)k = s-(q+1)l \; or \; s-(q+1)k = s+(q+1)l.$$

If the former holds, then it follows that $k = l$, a contradiction. If the latter holds, then $k+l = mn$, where $m \in \mathbb{Z}$, this also give a contradiction. Thus, for $1 \le k \ne l \le \frac{n-1}{2}$, $\mathbb{C}_{s-(q+1)k}$ and $\mathbb{C}_{s-(q+1)l}$ are distinct.

Note that $\mathbb{C}_{s-(q+1)}, \mathbb{C}_{s-2(q+1)}, \cdots, \mathbb{C}_{s-\frac{(q+1)(n-1)}{2}}$ are distinct which has two elements and $\mathbb{C}_s$ has only one element, so the result gives all q^2-cyclotomic cosets modulo $(q+1)n$. This completes the proof. □

In order to construct AQECCs, we give a sufficient condition for η-constacyclic codes which contain their Hermitian dual codes. We consider two cases.

Case 1: $e \equiv 1 (\mathrm{mod}\ 4)$

Theorem 4.2 *Let $q = 2^e$ with $e \equiv 1 (\mathrm{mod}\ 4)$. Let $n = \frac{q^2+1}{5}$, $s = \frac{(q+6)n}{2}$ and $r = \frac{q^2-q}{2}$, where $r = s - \frac{(q+1)(n+1)}{2}$. If $\mathcal{C}$ is an η-constacyclic code over $\mathbb{F}_{q^2}$ of length n with defining set $Z = \bigcup_{j=0}^{\delta} \mathbb{C}_{r-(q+1)j}$, where $0 \le \delta \le \frac{3q-16}{10}$, then $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$.*

Proof First note that $q \equiv 2 \mod 10$. By Lemma 2.1, it is sufficient to prove that $Z \cap Z^{-q} = \emptyset$. Suppose that $Z \cap Z^{-q} \ne \emptyset$. Then, there exist two integers k, l, where $0 \le k,\ l \le \frac{3q-16}{10}$, such that $r-(q+1)k \equiv -[r-(q+1)l]q^{\epsilon} \mod (q+1)n$ for $\epsilon = 1$ and $\epsilon = 3$.

If $\epsilon = 1$, then $r-(q+1)k \equiv -[r-(q+1)l]q \mod (q+1)n$. It is equivalent to $(q+1)r \equiv (q+1)(k+lq) \mod (q+1)n$, which means $q^2-5q-4 \equiv 10k+10lq \mod 2(q^2+1)$. As $0 \le k,\ l \le \frac{3q-16}{10}$, it follows that $0 \le 10k,\ 10l \le 3q-16$, we can obtain a contradiction by considering the following two cases.

(i) $0 \le 10k \le 2q-1$. Then $0 \le 10k+10lq \le 3q^2-14q-1$. We express $10k$ in the form $10k = tq+u$, where $t = 0, 1$ and $0 \le u \le q-1$. If $0 \le 10k+10lq \le 2q^2+1$, then $q^2-5q-4 \equiv 10k+10lq \mod 2(q^2+1)$, where $q^2-5q-4 = (q-6)q+q-4$ and $10k+10lq = (10l+t)q+u$. By the division algorithm, it must be $q-6 = 10l+t$, then we have $q = 10l+t+6$. This contradicts the form of q. If $2q^2+2 \le 10k+10lq \le 3q^2-14q-1$, then $0 \le 10k+10lq-2(q^2+1) \le q^2-14q-3$. This gives that $q^2-5q-4 = 10k+10lq-2(q^2+1)$, which is equivalent to $(3q-6)q+q-2 = (10l+t)q+u$. By the division algorithm, there is $3q = 10l+t+6$. Since $l = \frac{3q-t-6}{10} > \frac{3q-16}{10}$, it is impossible.

(ii) $2q \le 10k \le 3q-16$. Then $2q \le 10k+10lq \le 3q^2-13q-16$. We express $10k$ in the form $10k = 2q+u$, where $0 \le u \le q-16$. If $2q \le 10k+10lq \le 2q^2+1$, then $q^2-5q-4 = 10k+10lq = (2+10l)q+u$. Hence we have $q = 10l+8$ by the division algorithm immediately. This contradicts the form of q. If $2q^2+2 \le$

$10k + 10lq \leq 3q^2 - 13q - 16$, then $0 \leq 10k + 10lq - 2(q^2+1) \leq q^2 - 13q - 18$. This gives that $q^2 - 5q - 4 = 10k + 10lq - 2(q^2+1)$, which is equivalent to $3q^2 - 5q - 2 = (3q-6)q + q - 2 = (10l+2)q + u$. Then we have $3q - 6 = 10l + 2$. Since $l = \frac{3q-8}{10} > \frac{3q-16}{10}$, it is also a contradiction.

If $\epsilon = 3$, then $r - (q+1)k \equiv -[r - (q+1)l]q^3 \mod (q+1)n$. Since $q^4 \equiv 1 \mod (q+1)n$, we have

$$[r - (q+1)k]q \equiv -[r - (q+1)l]q^4 \mod (q+1)n,$$

which is equivalent to $r - (q+1)l \equiv -[r - (q+1)k]q \mod (q+1)n$. Since k and l is equivalent in case (1), then we know that it is also a contradiction. Hence, we conclude that $Z \cap Z^{-q} = \emptyset$. The desired result follows. □

By using Theorem 4.2, we give the first construction of AQECCs in this paper.

Theorem 4.3 *Let $q = 2^e$ with $e \equiv 1 (\mathrm{mod}\ 4)$. Let $n = \frac{q^2+1}{5}$, then there exist asymmetric quantum codes with parameters $[[n, n-2(s+t+2), (2s+3)/(2t+3)]]_{q^2}$, where $0 \leq t \leq s \leq \frac{3q-16}{10}$.*

Proof Suppose that $\mathcal{C}_2$ is a q^2-ary η-constacyclic code of length $n = \frac{q^2+1}{5}$, $r = \frac{q^2-q}{2}$, where $r = s - \frac{(q+1)(n+1)}{2}$, with defining set $Z_2 = \bigcup_{i=0}^{t} \mathbb{C}_{r-(q+1)i}$, where $0 \leq t \leq \frac{3q-16}{10}$. Then the dimension of $\mathcal{C}_2$ is $n - (2t+2)$. Observe that Z_2 consists of $2t+2$ consecutive integers $\{r-(q+1)t, \cdots, r, r+(q+1), \cdots, r+(q+1)(t+1)\}$. From Theorem 2.2, the minimum distance of $\mathcal{C}_2$ is at least $2t+3$. From Lemma 2.4, we can see that the minimum distance of $\mathcal{C}_2$ is $2t+3$. Hence $\mathcal{C}_2$ is a q^2-ary η-constacyclic code with parameters $[n, n-(2t+2), 2t+3]_{q^2}$.

Now suppose that $\mathcal{C}_1$ is q^2-ary η-constacyclic code of length $n = \frac{q^2+1}{5}$, $r = \frac{q^2-q}{2}$, where $r = s - \frac{(q+1)(n+1)}{2}$, with defining set $Z_1 = \bigcup_{i=0}^{s} \mathbb{C}_{r-(q+1)i}$, where $0 \leq t \leq s \leq \frac{3q-16}{10}$. Similar to discussion of $\mathcal{C}_2$, $\mathcal{C}_1$ has parameters $[n, n-(2s+2), 2s+3]_{q^2}$. Then from Lemma 2.3, Theorem 3.1 and 4.2, there exist asymmetric quantum codes with parameters $[[n, n-2(s+t+2), (2s+3)/(2t+3)]]_{q^2}$. □

Remark 4.4 From Theorem 4.3, $d_z + d_x = 2s + 2t + 6$. Then from Theorem 3.2, the constructed asymmetric quantum codes with parameters $[[n, n-2(s+t+2), (2s+3)/(2t+3)]]_{q^2}$ attain asymmetric quantum Singleton bound. Hence, these asymmetric quantum codes are optimal.

Case 2: $e \equiv 3 (\mathrm{mod}\ 4)$

In this case, we can obtain the sufficient condition for η-constacyclic codes which contain their Hermitian dual codes as follows. The proof is similar to that in Theorem 4.2 and we omit it here.

Theorem 4.5 *Let $q = 2^e$ with $e \equiv 3 (\mathrm{mod}\ 4)$. Let $n = \frac{q^2+1}{5}$, $s = \frac{(q+6)n}{2}$ and $r = \frac{q^2-q}{2}$, where $r = s - \frac{(q+1)(n+1)}{2}$. If $\mathcal{C}$ is an η-constacyclic code over $\mathbb{F}_{q^2}$ of length n with defining set $Z = \bigcup_{j=0}^{\delta} \mathbb{C}_{r-(q+1)j}$, where $0 \leq \delta \leq \frac{3q-14}{10}$, then $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$.*

We can use Theorem 4.5 to construct the second family of AQECCs in this paper.

Theorem 4.6 *Let $q = 2^e$ with $e \equiv 3 (\mathrm{mod}\ 4)$. Let $n = \frac{q^2+1}{5}$, then there exist asymmetric quantum codes with parameters $[[n, n-2(s+t+2), (2s+3)/(2t+3)]]_{q^2}$, where $0 \leq t \leq s \leq \frac{3q-14}{10}$.*

Proof Suppose that $\mathcal{C}_2$ is a q^2-ary η-constacyclic code of length $n = \frac{q^2+1}{5}$, $r = \frac{q^2-q}{2}$, where $r = s - \frac{(q+1)(n+1)}{2}$ with defining set $Z_2 = \bigcup_{i=0}^{t} \mathbb{C}_{r-(q+1)i}$, where $0 \leq t \leq \frac{3q-14}{10}$. Then the dimension of $\mathcal{C}_2$ is $n-(2t+2)$. Observe that Z_2 consists of $2t+2$ consecutive integers $\{r-(q+1)t, \cdots, r, r+(q+1), \cdots, r+(q+1)(t+1)\}$. From Theorem 2.2, the minimum distance of $\mathcal{C}_2$ is at least $2t+3$. From Lemma 2.4, we can see that the minimum distance of $\mathcal{C}_2$ is $2t+3$. Hence $\mathcal{C}_2$ is a q^2-ary η-constacyclic code with parameters $[n, n-(2t+2), 2t+3]_{q^2}$.

Now suppose that $\mathcal{C}_1$ is q^2-ary η-constacyclic code of length $n = \frac{q^2+1}{5}$, $r = \frac{q^2-q}{2}$, where $r = s - \frac{(q+1)(n+1)}{2}$, with defining set $Z_1 = \bigcup_{i=0}^{s} \mathbb{C}_{r-(q+1)i}$, where $0 \leq t \leq s \leq \frac{3q-14}{10}$. Similar to the discussion of $\mathcal{C}_2$, $\mathcal{C}_1$ has parameters $[n, n-(2s+2), 2s+3]_{q^2}$. Then from Lemma 2.3, Theorem 3.1 and 4.5, there exist asymmetric quantum codes with parameters $[[n, n-2(s+t+2), (2s+3)/(2t+3)]]_{q^2}$. □

Remark 4.7 From Theorem 4.6, $d_z + d_x = 2s + 2t + 6$. Then from Theorem 3.2, the constructed asymmetric quantum codes with parameters $[[n, n-2(s+t+2), (2s+3)/(2t+3)]]_{q^2}$ attain asymmetric quantum Singleton bound. Hence, these asymmetric quantum codes are optimal.

Example 4.8 Let $q = 2^5 = 32$, then $n = \frac{q^2+1}{5} = 205$, $r = \frac{q^2-q}{2} = 496$. Suppose that the defining set of η-constacyclic code $\mathcal{C}_2$ is given by $Z_2 = \mathcal{C}_{496} = \{496, 529\}$. Then $\mathcal{C}_2$ is a MDS code with parameters $[205, 203, 3]_{1024}$. We also suppose the defining set of η-constacyclic code $\mathcal{C}_1$ is given by $Z_1 = \mathcal{C}_{496} = \{496, 529\}$. Then, $\mathcal{C}_1$ is a MDS code with parameters $[205, 203, 3]_{1024}$. From Theorem 3.2, there exists an optimal asymmetric quantum code with parameters $[[205, 201, 3/3]]_{1024}$. By taking the different defining sets of $\mathcal{C}_1$ and $\mathcal{C}_2$, we can get optimal asymmetric quantum codes in Table 1.

Table 1 Optimal asymmetric quantum codes

$[[205, 201, 3/3]]_{1024}$	$[[205, 185, 17/5]]_{1024}$	$[[205, 185, 11/11]]_{1024}$
$[[205, 199, 5/3]]_{1024}$	$[[205, 183, 19/5]]_{1024}$	$[[205, 183, 13/11]]_{1024}$
$[[205, 197, 7/3]]_{1024}$	$[[205, 193, 7/7]]_{1024}$	$[[205, 181, 15/11]]_{1024}$
$[[205, 195, 9/3]]_{1024}$	$[[205, 191, 9/7]]_{1024}$	$[[205, 179, 17/11]]_{1024}$
$[[205, 193, 11/3]]_{1024}$	$[[205, 189, 11/7]]_{1024}$	$[[205, 177, 19/11]]_{1024}$
$[[205, 191, 13/3]]_{1024}$	$[[205, 187, 13/7]]_{1024}$	$[[205, 181, 13/13]]_{1024}$
$[[205, 189, 15/3]]_{1024}$	$[[205, 185, 15/7]]_{1024}$	$[[205, 179, 15/13]]_{1024}$
$[[205, 187, 17/3]]_{1024}$	$[[205, 183, 17/7]]_{1024}$	$[[205, 177, 17/13]]_{1024}$
$[[205, 185, 19/3]]_{1024}$	$[[205, 181, 19/7]]_{1024}$	$[[205, 175, 19/13]]_{1024}$
$[[205, 197, 5/5]]_{1024}$	$[[205, 189, 9/9]]_{1024}$	$[[205, 177, 15/15]]_{1024}$
$[[205, 195, 7/5]]_{1024}$	$[[205, 187, 11/9]]_{1024}$	$[[205, 175, 17/15]]_{1024}$
$[[205, 193, 9/5]]_{1024}$	$[[205, 185, 13/9]]_{1024}$	$[[205, 173, 19/15]]_{1024}$
$[[205, 191, 11/5]]_{1024}$	$[[205, 183, 15/9]]_{1024}$	$[[205, 173, 17/17]]_{1024}$
$[[205, 189, 13/5]]_{1024}$	$[[205, 181, 17/9]]_{1024}$	$[[205, 171, 19/17]]_{1024}$
$[[205, 187, 15/5]]_{1024}$	$[[205, 179, 19/9]]_{1024}$	$[[205, 169, 19/19]]_{1024}$

5 Conclusion

In this paper, we have constructed two classes of AQECCs from constacyclic codes over the finite field $\mathbb{F}_{q^2}$ of length $n = \frac{q^2+1}{5}$, where q is an odd power of an even prime. The construction is through cyclotomic cosets and ideal theory. According to the asymmetric quantum Singleton bound, the resulting AQECCs are optimal and different from the codes available in the literature. It would be interesting to construct optimal AQECCs from other types of constacyclic codes.

References

1. Shor, P.W.: Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A. **52**, 2493–2496 (1995)
2. Steane, A.M.: Error correcting codes in quantum theory. Phys. Rev. Lett. **77**, 793–797 (1996)
3. 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**, 1369–1387 (1998)
4. Grassl, M., Beth, T.: On optimal quantum codes. Int. J. Quantum Inf. **2**, 55–64 (2004)
5. Chen, H., Ling, S., Xing, C.P.: Quantum codes from concatenated algebraic-geometric codes. IEEE Trans. Inf. Theory. **51**, 2915–2920 (2005)
6. Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.K.: Nonbinary quantum stabilizer codes over finite fields. IEEE Trans. Inf. Theory. **52**, 4892–4914 (2006)
7. Aly, S.A., Klappenecker, A., Sarvepalli, P.K.: On quantum and classical BCH codes. IEEE Trans. Inf. Theory. **53**, 1183–1188 (2007)
8. La Guardia, G.G., Palazzo, J.R.: Constructions of new families of nonbinary CSS codes. Discrete Math. **310**, 2935–2945 (2010)
9. Kai, X.S., Zhu, S.X.: Quaternary construction of quantum codes from cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$. Int. J. Quantum Inf. **9**, 689–700 (2011)
10. Li, R.H., Zuo, F., Liu, Y., Xu, Z.B.: Hermitian dual-containing BCH codes and construction of new quantum codes. Quantum Inf. Comput. **13**, 21–35 (2013)
11. Yang, Y.S., Cai, W.C.: On self-dual constacyclic codes over finite fields. Des. Codes Crypt. **74**, 355–364 (2015)
12. Steane, A.M.: Simple quantum error-correcting codes. Phys. Rev. A. **54**, 4741–4751 (1996)
13. Wang, L., Feng, K.Q., Ling, S., Xing, C.P.: Asymmetric quantum codes: characterization and constructions. IEEE. Trans. Inf. Theory **56**, 2938–2945 (2010)
14. La Guardia, G.G.: New families of asymmetric quantum BCH codes. Quantum Inf. Comput. **11**, 239–252 (2011)
15. La Guardia, G.G.: On the construction of asymmetric quantum codes. Int. J. Theor. Phys. **53**, 2312–2322 (2014)
16. Ezerman, M.F., Ling, S., Solé, P.: Additive asymmetric quantum codes. IEEE. Trans. Inf. Theory. **57**, 5536–5550 (2011)
17. Zhang, G.H., Chen, B.C., Li, L.C.: New optimal asymmetric quantum codes from constacyclic codes. Mod. Phys. Lett. B **28**(1–9), 1450126 (2014)
18. Wang, L.Q., Zhu, S.X.: On the construction of optimal asymmetric quantum codes. Int. J. Quantum Inf. **12**(1–11), 1450017 (2014)
19. Chen, J.Z., Li, J.P., Lin, J.: New optimal asymmetric quantum codes derived from negacyclic codes. Int. J. Theor. Phys. **53**, 72–79 (2014)
20. Xu, G., Li, R.H., Guo, L.B., Lü, L.D.: New optimal asymmetric quantum codes constructed from constacyclic codes. Int. J. Mod. Phys. B **31**(1–14), 1750030 (2017)
21. Kai, X.S., Zhu, S.X., Li, P.: Constacyclic codes and some new quantum MDS codes. IEEE Trans. Inf. Theory. **60**, 2080–2086 (2014)
22. Zhang, T., Ge, G.N.: Some new classes of quantum MDS codes from constacyclic codes. IEEE Trans. Inf. Theory. **61**, 5224–5228 (2015)
23. Li, S.X., Xiong, M.S., Ge, G.N.: Pseudo-cyclic codes and the contruction of quantum MDS codes. IEEE Trans. Inf. Theory. **62**, 1703–1710 (2016)

24. Aydin, N., Siap, I., Ray-Chaudhuri, D.K.: The structure of 1-Generator Quasi-Twisted codes and new linear codes. Des. Codes Crypt. **24**, 313–326 (2001)
25. Krishna, A., Sarwate, D.V.: Pseudocyclic maximum-distance-separable codes. IEEE Trans. Inf. Theory. **60**, 2080–2086 (2014)
26. Macwilliams, F.J., Sloane, N.J.A.: The theory of error-correcting codes. North-holland, Amsterdam (1997)