Quantum Inf Process (2017) 16:66
DOI 10.1007/s11128-017-1533-y

A class of constacyclic BCH codes and new quantum codes

Yang liu[1,2] · Ruihu Li[1] · Liangdong Lv[1] · Yuena Ma[1]

Received: 8 October 2016 / Accepted: 17 January 2017 / Published online: 2 February 2017

Abstract Constacyclic BCH codes have been widely studied in the literature and have been used to construct quantum codes in latest years. However, for the class of quantum codes of length $n = q^{2m} + 1$ over F_{q^2} with q an odd prime power, there are only the ones of distance $\delta \leq 2q^2$ are obtained in the literature. In this paper, by a detailed analysis of properties of q^2-ary cyclotomic cosets, maximum designed distance $\delta_{\max}$ of a class of Hermitian dual-containing constacyclic BCH codes with length $n = q^{2m} + 1$ are determined, this class of constacyclic codes has some characteristic analog to that of primitive BCH codes over F_{q^2}. Then we can obtain a sequence of dual-containing constacyclic codes of designed distances $2q^2 < \delta \leq \delta_{\max}$. Consequently, new quantum codes with distance $d > 2q^2$ can be constructed from these dual-containing codes via Hermitian Construction. These newly obtained quantum codes have better code rate compared with those constructed from primitive BCH codes.

Keywords Negacyclic code · Constacyclic code · Quantum code · Cyclotomic coset

1 Introduction

The theory of quantum error-correcting codes (QECCs, for short) has been extensively studied in the literature, see [1–11]. The most widely studied class of quantum codes

✉ Ruihu Li
llzsy2015@163.com

1 School of Science, Air Force Engineering University, Xi'an 710051, Shaanxi, People's Republic of China

2 The First Aeronautical College of Air Force, Xinyang 464000, Henan, People's Republic of China

are stabilizer codes, which can be constructed from classical codes over finite fields F_q or F_{q^2} with certain self-orthogonal properties [3,4,8–10].

As in the classical case, construction of quantum codes from classical codes with special structure has become a central topic for quantum codes in the past decades, see [12–25]. Many classes of quantum codes have been constructed by using cyclic codes, BCH codes, negacyclic codes, and constacyclic codes [12–25]. The following theorem is one of the most frequently used construction methods.

Theorem 1.1 ([8,9] Hermitian Construction) *If there is a classic linear code* $\mathcal{C} = [n, k, d]_{q^2}$ *over* F_{q^2} *such that* $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$, *then there exists a* q*-ary* $[[n, 2k-n, \geq d]]_q$ *quantum code, where* $\mathcal{C}^{\perp_h}$ *is the Hermitian dual code of* C.

To obtain q-ary quantum codes by the Hermitian construction, Theorem 1.1 implies that one only need to find linear codes $\mathcal{C}$ over F_{q^2} such that $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$. From this idea, in [14,15], Aly et.al studied Hermitian dual-containing BCH codes, presented necessary and sufficient conditions for Hermitian dual-containing BCH codes by their designed distances, and constructed many q-ary quantum BCH codes. The necessary and sufficient conditions for a primitive narrow-sense BCH code over F_{q^2} contain its Hermitian dual which are as follows:

Theorem 1.2 ([14] Theorem 4) *A primitive, narrow-sense BCH code of length* q^{2m}*-1 over* F_{q^2}, *where* $m \neq 2$, *contains its Hermitian dual code if and only if its designed distance* δ *satisfies* $\delta \leq \delta_{\max} = q^{m+[m\ even]} - 1 - (q^2-2)[m\ even]$, *where* $[m\ even] = 1$ *if* m *is even and* $[m\ even] = 0$ *if* m *is odd.*

For $m = 2$, the maximal designed distance $\delta_{\max}$ of primitive, narrow-sense BCH code of length q^{2m}- 1 over F_{q^2} was determined by Li et al. in [18].

Proposition 1.3 ([18] Theorem 3.2) *A primitive, narrow-sense BCH code of length* q^4*-1 over* F_{q^2} *contains its Hermitian dual code if and only if its designed distance* δ *satisfies* $\delta \leq \delta_{\max} = q^3 - q^2 + q - 1$.

The class of constacyclic codes, which contains the well-known class of cyclic and negacyclic codes, has been investigated in the literature [19–29]. A class of constacyclic codes called **constacyclic BCH** codes in [23], which is analog to cyclic BCH codes, have some properties similar to that of BCH code, see [21–25]. In [22], Chen et.al. presented elementary number-theoretic conditions for the existence of dual-containing constacyclic codes; for more details, see Theorem 2.11 and Theorem 2.12 in [22].

In [19] and [21], for odd $q \equiv 1(mod\ 4)$ and $q \equiv 3(mod\ 4)$, the authors, respectively, showed that some negacyclic codes (special constacyclic BCH codes) and constacyclic BCH codes of length $n = q^{2m} + 1$ over F_{q^2} with designed distance $\delta \leq 2q^2$ are Hermitian dual-containing codes, their results are as follows:

Theorem 1.4 ([19] Lemma 3.7) *Assume that* $q \equiv 1(mod\ 4)$. *Let* $n = q^{2m} + 1$ *where* $m \geq 2$, *and let* $s = n/2$. *If* $\mathcal{C}$ *is a negacyclic code over* F_{q^2} *of length* n *with define set* $Z = C_{s-2l} \cup C_{s-2(l-1)} \cup \cdots \cup C_{s-2} \cup C_s$, *where* $1 \leq l \leq q^2 - 1$, *then* $\mathcal{C}$ *contains its Hermitian dual code.*

Theorem 1.5 ([21] Lemma 3.4) *Assume that* $q \equiv 3 (mod\ 4)$. *Let* $n = q^{2m} + 1$ *where* $m \geq 2$, *and let* $s = n/2$. *If* $\mathcal{C}$ *is a constacyclic code over* F_{q^2} *of length n with define set* $Z = C_{s-(q+1)l} \cup C_{s-(q+1)(l-1)} \cup \cdots \cup C_{s-(q+1)} \cup C_s$ *where* $1 \leq l \leq q^2 - 1$, *then* $\mathcal{C}$ *contains its Hermitian dual code.*

Inspired by these latter works, in this paper, we discuss a class of Hermitian dual-containing constacyclic BCH codes of length $n = q^{2m} + 1$ over the finite field $\mathbf{F}_{q^2}$, where q is an odd prime power. We will show that one can also deduce from the design parameters whether or not a class constacyclic BCH code contains its Hermitian dual code. Our results on designed distance for Hermitian dual-containing constacyclic BCH codes present analog results for that of primitive BCH codes in [14] and generalize the above Theorems 1.4 and 1.5. Then we make some observations about cyclotomic cosets in the defining set of Hermitian dual-containing constacyclic BCH codes and exactly determine the dimensions of these Hermitian dual-containing codes. Based on the above results, we derive new quantum codes from these constacyclic BCH codes. These quantum codes have good parameters compared with the ones available in the literature.

This paper is organized as follows. In Sect. 2, basic concepts on q^2-cyclotomic cosets and η-constacyclic codes are reviewed. In Sect. 3, some useful properties of q^2-ary cyclotomic coset modulo rn will be given. For $r = 2$ and $q + 1$, the maximum designed distances of Hermitian dual-containing negacyclic and constacyclic codes are determined. In Sect. 4, new quantum negacyclic and constacyclic codes are constructed. In Sect. 5, some new quantum codes are exhibited, and the parameters of the constructed quantum codes are compared with the ones available in the literature, and the final remarks are drawn.

2 Preliminaries

In this section, we introduce some basic knowledge on Hermitian dual-containing codes, η-constacyclic codes, and cyclotomic cosets for the purpose of this paper. For more details, see [27–30].

Let q be a power of an odd prime, F_{q^2} denote the finite field with q^2 elements, and $F_{q^2}^*$ be the multiplicative group of F_{q^2}. For any $\alpha \in F_{q^2}$, the conjugation of α is denoted by $\overline{\alpha} = \alpha^q$. Given two vectors $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ and $\mathbf{y} = (y_1, y_2, \cdots, y_n) \in F_{q^2}^n$, their Hermitian inner product is defined as

$$(\mathbf{x}, \mathbf{y})_h = \sum \overline{x_i} y_i = \overline{x_1} y_1 + \overline{x_2} y_2 + \cdots + \overline{x_n} y_n.$$

For a linear code $\mathcal{C}$ over F_{q^2} of length n, the Hermitian dual code of $\mathcal{C}$ is denoted as $\mathcal{C}^{\perp_h}$, where $\mathcal{C}^{\perp_h}$ is defined as

$$\mathcal{C}^{\perp_h} = \{x \in F_{q^2}^n | (x, y)_h = 0, \forall y \in \mathcal{C}\}.$$

If $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$, then $\mathcal{C}$ is called a Hermitian dual-containing code, and $\mathcal{C}^{\perp_h}$ is called a Hermitian self-orthogonal code.

For any vector $(c_0, c_1, \cdots, c_{n-1}) \in F_{q^2}^n$ and a nonzero element $\eta \in F_{q^2}$, an η-constacyclic shift τ_η on $F_{q^2}^n$ is the shift

$$\tau_\eta(c_0, c_1, \cdots, c_{n-1}) = (\eta c_{n-1}, c_0, \cdots, c_{n-2}).$$

A q^2-ary linear code $\mathcal{C}$ of length n is called η-**constacyclic** if it is invariant under the η-constacyclic shift τ_η on $F_{q^2}^n$. When $\eta = 1$, η-constacyclic codes are cyclic codes, and when $\eta = -1$, η-constacyclic codes are negacyclic codes. For an η-constacyclic code $\mathcal{C}$, each codeword $c = (c_0, c_1, \cdots, c_{n-1})$ is customarily represented in its polynomial form: $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$, and the code $\mathcal{C}$ is in turn identified with the set of all polynomial representations of its codewords.

From [19,20,26,27], we know a linear code $\mathcal{C}$ of length n over F_{q^2} is η-constacyclic if and only if $\mathcal{C}$ is an ideal of the quotient ring $\mathcal{R}_n = \mathbb{F}_q[x]/(x^n - \eta)$, and $xc(x)$ corresponds to an η-constacyclic shift of $c(x)$ in the ring $\mathcal{R}_n$. It follows that $\mathcal{C}$ is generated by monic factor of $(x^n - \eta)$, i.e., $\mathcal{C} = \langle g(x)\rangle$ and $g(x)|(x^n - \eta)$. The $g(x)$ is called the generator polynomial of $\mathcal{C}$. The dimension of $\mathcal{C}$ is $n - k$, where $k = deg(g(x))$. It can be verified that the Hermitian dual $\mathcal{C}^{\perp_h}$ of an η-constacyclic code $\mathcal{C}$ over F_{q^2} is an $\bar{\eta}^{-1}$-constacyclic code [19,20].

Let ω be a primitive element of F_{q^2}, we assume $gcd(n, q) = 1$ and take $\eta = \omega^{\upsilon(q-1)}$ for some $\upsilon \in \{0, 1, \ldots, q\}$. In this case, we have $\eta\bar{\eta} = 1$, so the Hermitian dual $\mathcal{C}^{\perp_h}$ of an η-constacyclic code over F_{q^2} is η-constacyclic. In particular, if $\upsilon = 0$, the class of η-constacyclic codes is cyclic codes; if q is an odd prime power and $\upsilon = (q+1)/2$, the class of η-constacyclic codes is negacyclic codes. As $\eta^{q+1} = 1$, the order r of η in $F_{q^2}^*$ is equal to $\frac{q+1}{gcd(\upsilon, q+1)}$. Let ζ be a primitive rn-th root of unity in some extension field of F_{q^2} such that $\zeta^n = \eta$. Let $\xi = \zeta^r$. Then ξ is a primitive n-th root of unity. It follows that the roots of $x^n - \eta$ are $\zeta\xi^j = \zeta^{1+jr}$ for $0 \le j \le n - 1$. Set $\Omega = \Omega_{r,n} = \{1 + jr | 0 \le j \le n - 1\}$. The defining set T of a constacyclic code $\mathcal{C} = \langle g(x)\rangle$ of length n is the set $T = \{j \in \Omega \mid \zeta^j$ is a root of g(x)$\}$. For each $i \in \Omega$, let $C_i = \{i, iq^2, i(q^2)^2, ..., i(q^2)^{k-1}\}(mod \ \ rn)$, where k is the smallest positive integer such that $(q^2)^k i \equiv i(\text{mod } rn)$, C_i is called the q^2-cyclotomic coset modulo rn containing i. It is easy to see that the defining set T is a union of some q^2-cyclotomic cosets modulo rn (see [20,27]).

The minimal polynomial of ζ^j over F_{q^2} is denoted by $M^{(j)}(x)$, and it is given by $M^{(j)}(x) = \prod_{i \in C_j}(x - \zeta^i)$. Now one can give the concept of η-constacyclic BCH (CBCH, for short) codes.

Definition 2.1 Let q be a prime power with $gcd(n, q) = 1$. Let ζ be a primitive rn-th root of unity in F_{q^2}. For some $b = 1 + ri$, we have

$$g(x) = lcm\{M^{(b)}(x), M^{(b+r)}(x), \cdots, M^{(b+(\delta-2)r)}(x)\},$$

i.e., $g(x)$ is the monic polynomial of smallest degree over F_{q^2} having $\zeta^b, \zeta^{b+r}, \cdots, \zeta^{b+(\delta-2)r}$ as zeros. An η-constacyclic code $\mathcal{C} = \langle g(x)\rangle$ of length n over F_{q^2} is a CBCH code with designed distance δ.

From Definition 2.1, it follows that an η-constacyclic code $\mathcal{C} = \langle g(x) \rangle$ is a CBCH code if and only if its defining set $T = \bigcup_{i=b}^{b+\delta-2} C_{s+ir}$ with designed distance δ.

Similar to cyclic codes, there exists the following BCH bound for η-constacyclic codes (see [26,27]). According to this lemma, a CBCH code of designed distance δ has minimum distance $d \geq \delta$.

Lemma 2.1 (The BCH bound for η-constacyclic codes) *Let $\mathcal{C}$ be a q^2-ary η-constacyclic code of length n with generator polynomial $g(x)$. If $g(x)$ has the elements $\{\beta^{1+ri} | 0 \leq i \leq \delta - 2\}$ as the roots, where β is a primitive rn-th root of unity, then the minimum distance d of code $\mathcal{C}$ is at least δ.*

It is well known that there is a close relation between cyclotomic cosets and cyclic codes, see [28–32]. The definitions of symmetric coset and asymmetric coset pairs for 2-cyclotomic cosets were first given in [32] to characterize binary cyclic self-dual codes, and were generalized further in [17,18] to characterize q^2-ary Hermitian self-orthogonal cyclic codes. Now we give definition for skew-symmetric property of cyclotomic cosets. For each $i \in \Omega$, let C_i be the q^2-cyclotomic coset modulo rn containing i. A cyclotomic coset C_i is called **skew symmetric** if $-qi \pmod{rn} \in C_i$, otherwise **skew asymmetric**. Skew-asymmetric cosets C_i and C_{-qi} come in pair, we use (C_i, C_{-qi}) to denote such a **skew-asymmetric pair** (SAP, for short). In [20] Lemma 2.2, Kai et.al have shown that an η-constacyclic code $\mathcal{C}$ with defining set T contains its Hermitian dual if and only if $T \cap T^{-q} = \emptyset$, where $T^{-q} = \{-qi (mod \ \ rn) \mid i \in T\}$. Using terminology of symmetric coset and asymmetric cosets pair, an equivalent statement can be given as in Lemma 2.2 [17]. We list these two equivalent statement as the following lemma for later use.

Lemma 2.2 *If $\mathcal{C}$ is an η-constacyclic code of length n over F_{q^2} with defining set T, then $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$ if and only if one of the following holds:*

(1) $T \cap T^{-q} = \emptyset$, where $T^{-q} = \{-qi \mod rn \mid i \in T\}$.
(2) For each $i \in T$, C_i is a skew-asymmetric coset; if $j \in T$ and $j \notin C_i$, then C_j and C_i cannot form a skew-asymmetric cosets pair.

Notations: (1) To save space and simplify statements of the following two sections, we use $[1, n-1]$ to denote the set $\{1, 2, ..., n-1\}$, and call the set $\{e, e+1, , ..., f-1, f\}$ as interval $[e, f]$.

(2) From now on till the end of this paper, we assume that q is an odd prime power, for given $m \geq 2$, let $n = n(q, m) = q^{2m} + 1$ and $s = \frac{n}{2}$. If $q \equiv 1 (mod \ \ 4)$, we set $r = 2$, and if $q \equiv 3 (mod \ \ 4)$, we set $r = q + 1$. Let η be an rth root of unity, for $j \in \Omega_{r,n}$, the q^2-cyclotomic cosets modulo rn containing j is denoted as C_j. For $T_i = C_s \cup C_{s+r} \cup C_{s+2r} \cup \cdots \cup C_{s+ir}$, we denote $T_i = T_{<s,s+ir>}$. We define

$$\delta_{\max} = \delta_{\max}(n) = \begin{cases} q^3 - q^2 + q + 1 & \text{if } m = 2; \\ q^{m+1} - q^2 + 2 & \text{if } m = 2l \geq 4; \\ q^m + 1 & \text{if } m = 2l + 1 \geq 3. \end{cases}$$

Theorem 2.3 *Let q, m, n, s and $\delta_{\max}$ be given as above. If $0 \leq i \leq \frac{\delta_{\max}-2}{2}$, then $C_s = \{s\}$ and $C_{s-ir} = C_{s+ir}$.*

Proof Since $sq^2 = s(q^2-1)+s = \frac{(q+1)(q-1)n}{2} + s \equiv s(mod\ \ rn)$, obviously, $C_s = \{s\}$. Further, we can infer $s \equiv sq^2 \cdots \equiv sq^{2(m-1)} \equiv sq^{2m}(mod\ \ rn)$. It follows that $(s+ir)q^{2m} \equiv s + irq^{2m} \equiv s - ir(mod\ \ rn)$, so $s - ir \in C_{s+ir}$. Thus, the theorem holds.

By Theorem 2.3, it is obvious that

$$T_i = C_{s-ir} \cdots \cup C_{s-r} \cup C_s \cdots \cup C_{s-ir} = \bigcup_{j=-i}^{i} C_{s+jr}.$$

Since $C_{s-(i+1)r}$ may be contained by T_i for some $i \leq \frac{\delta_{\max}-2}{2}$ (for details, see Sect. 4), combining the BCH bound for η-constacyclic codes, it follows that the designed distance δ_i of a CBCH code with defining set T_i is greater than or equal to $2i+2$. We will use $\mathcal{C}(n, q^2; \delta_i)$ to denote such a code in the rest of this paper. It will be shown that these CBCH codes are Hermitian dual-containing, and parameters of them will be presented in the following sections. □

3 Hermitian dual-containing condition of CBCH codes

Since the q^2-cyclotomic coset is the core tool by which we study Hermitian dual-containing condition and exactly calculate dimensions of codes below, some useful properties of cyclotomic coset will be firstly given in this section.

Lemma 3.1 *Let q, n, s, r be given above. If $h \equiv 0(mod\ \ 2)$ and $h \geq 2$, then $sq^h \equiv s(mod\ \ rn)$; if $h \equiv 1(mod\ \ 2)$, then $sq^h \equiv (r-1)s(mod\ \ rn)$.*

Proof If $h = 2l$, then $(q^2-1)|(q^h-1)$ and $2(q+1)|(q^h-1)$. Hence $s(q^h-1) = n(q+1)a \equiv 0(mod\ \ rn)$ for some integer a, and $q^h s \equiv s(mod\ \ rn)$ holds.

If $h = 2l+1$, we have $sq^{2l+1} = q \times sq^{2l} \equiv qs \equiv [(q+1)-1]s(mod\ \ rn)$.

When $q \equiv 3(mod\ \ 4)$, then $r = q+1$, we get

$$sq^{2l+1} = [(q+1)-1]sq^{2l}(mod\ \ rn) \equiv (r-1)s(mod\ \ rn).$$

When $q \equiv 1(mod\ \ 4)$ and $r = 2$, let $q = 4u+1$. Then we have

$$sq^{2l+1} \equiv [(q+1)-1]s(mod\ \ 2n) = [(4u+2)-1]s \equiv (2-1)s(mod\ \ 2n).$$

The desired conclusion then follows from the discussion.

By Lemma 3.1, we can further obtain the following Theorem 3.2. □

Theorem 3.2 *For given q and m, let $0 \leq i, j \leq \frac{\delta_{\max}-2}{2}$. Then*

(1) $C_{s+ir} = C_{s+jr}$ if and only if there exists a $t \in [0, \lfloor \frac{m}{2} \rfloor]$ such that $i \pm jq^{2t} \equiv 0(mod\ \ n)$ or $j \pm iq^{2t} \equiv 0(mod\ \ n)$.

(2) If $i \neq j$, then (C_{s+ir}, C_{s+jr}) is a skew-asymmetric pair (SAP) if and only if there exists a $t \in [0, \lfloor \frac{m}{2} \rfloor]$ such that $i \pm jq^{2t+1} \equiv s(mod\ \ n)$ or $j \pm iq^{2t+1} \equiv s(mod\ \ n)$.

(3) C_{s+ir} is skew symmetric if and only if there exists a $t \in [0, \lfloor \frac{m}{2} \rfloor]$ such that $i(1 \pm q^{2t+1}) \equiv s(mod\ n)$.

Proof (1) It is obvious $C_{s+ir} = C_{s+jr}$ if and only if there is an $l \in [0, 2m-1]$ such that $s+ir \equiv (s+jr)q^{2l}(mod\ rn)$. From $s+ir \equiv (s+jr)q^{2l} \equiv s+jrq^{2l}(mod\ rn)$, one has $s+ir \equiv (s+jr)q^{2l}(mod\ rn)$ if and only if $ri \equiv rjq^{2l}(mod\ rn)$, which is also equivalent to $i \equiv jq^{2l}(mod\ n)$. Hence we can deduce that

$C_{s+ir} = C_{s+jr} \Leftrightarrow i \equiv jq^{2l}(mod\ n)$.

Now we will show that

$$i \equiv jq^{2l}(mod\ n) \Leftrightarrow i \pm jq^{2t} \equiv 0(mod\ n) \text{ or } j \pm iq^{2t} \equiv 0(mod\ n) \quad (3.1)$$

for some $t \in [0, \lfloor \frac{m}{2} \rfloor]$.

Since $q^{2m} \equiv -1(mod\ n)$, it is obviously that if $i - jq^{2t} \equiv 0(mod\ n)$ or $j + iq^{2t} \equiv 0(mod\ n)$, then there is $i \equiv jq^{2l}(mod\ n)$. Since $q^{4m} \equiv 1(mod\ n)$, when $i + jq^{2t} \equiv 0(mod\ n)$ or $j - iq^{2t} \equiv 0(mod\ n)$, there is also $i \equiv jq^{2l}(mod\ n)$ holds. Hence, the right-hand side of (3.1) can deduce the left-hand side of (3.1). So, to prove (3.1), we only need to check the left-hand side of (3.1) can implies the right-hand side of (3.1).

Case 1.1: If $l \in [0, \lfloor \frac{m}{2} \rfloor]$, let $t = l$, then we have $i \equiv jq^{2t}\ (mod\ n)$.

Case 1.2: If $m \geq 3$ and $l \in [\lfloor \frac{m}{2} \rfloor + 1, m-1]$, then

$i \equiv jq^{2l}(mod\ n) \Leftrightarrow iq^{2(m-l)} \equiv jq^{2l}q^{2(m-l)} \equiv j(q^{2m} + 1 - 1) \equiv -j(mod\ n)$.

Let $t = m - l$, then $t \in [1, \lfloor \frac{m-1}{2} \rfloor]$. That is to say that there is a $t \in [1, \lfloor \frac{m-1}{2} \rfloor] \subset [0, \lfloor \frac{m}{2} \rfloor]$, such that $j \equiv -iq^{2t}(mod\ n)$.

Case 1.3: If $l \in [m, 2m-1]$, denote $l' = l - m$, then $l' \in [0, m-1]$ such that $i \equiv jq^{2l} = jq^{2l'+2m} = jq^{2l'}(q^{2m} + 1 - 1) \equiv -jq^{2l'}\ (mod\ n)$. From the above two cases, one can deduce that there is a $t \in [0, \lfloor \frac{m}{2} \rfloor]$ such that $i \equiv -jq^{2t}(mod\ n)$ or $j \equiv iq^{2t}(mod\ n)$.

Summarizing the previous three cases and the above discussion, we have showed (3.1) holds, Thus (1) follows.

(2) By the definition of a SAP, (C_{s+ir}, C_{s+jr}) forms a SAP if and only if there is an $l \in [0, 2m-1]$ such that $s + ir \equiv -(s + jr)q^{2l+1}(mod\ rn)$. Since $sq^{2l+1} \equiv (r-1)s(mod\ rn)$, it follows that $(s + jr)q^{2l+1} \equiv (r-1)s + jrq^{2l+1}(mod\ rn)$, $s + ir \equiv -(s + jr)q^{2l+1} \equiv -(r-1)s - jrq^{2l+1}(mod\ rn)$, and

$s + ir \equiv -(s + jr)q^{2l+1}(mod\ rn) \Leftrightarrow i \equiv -jq^{2l+1} + s(mod\ n)$.

Thus, we can deduce that (C_{s+ir}, C_{s+jr}) is a SAP if and only if $i \equiv -jq^{2l+1} + s(mod\ n)$. Next, we can show

$$i \equiv -jq^{2l+1} + s(mod\ n) \Leftrightarrow i \pm jq^{2t} \equiv s(mod\ n) \text{ or } j \pm iq^{2t} \equiv s(mod\ n) \quad (3.2)$$

for some $t \in [0, \lfloor \frac{m}{2} \rfloor]$.

Similar to the discussion of (1), one can show (2) holds.

(3) A coset C_{s+ir} is skew symmetric if and only if there exists an $l \in [0, 2m-1]$ such that $s + ir \equiv -(s + ir)q^{2l+1}(mod\ rn)$. It is not difficult to deduce that $s + ir \equiv -(s + ir)q^{2l+1}(mod\ rn)$ if and only if $i(1 + q^{2l+1}) \equiv s(mod\ n)$. Analog to the discussion of (1), one can show

$i(1+q^{2l+1}) \equiv s(mod\ \ n) \Leftrightarrow i(1 \pm q^{2t+1}) \equiv s(mod\ \ n)$ for some $t \in [0, \lfloor \frac{m}{2} \rfloor]$. Thus, (3) holds.

For proving our main result **Theorem** 3.6 which refers to maximum designed distances of Hermitian dual-containing condition for CBCH codes with defining set T_i, we first give Lemma 3.3, Corollary 3.4, and Lemma 3.5. □

Lemma 3.3 *If* $0 \le i, j \le \frac{\delta_{\max}-2}{2}$ *and* $t \in [0, \lfloor \frac{m}{2} \rfloor]$, *then* $i \pm jq^{2t+1} \not\equiv s(mod\ \ n)$.

Proof We give our discussion in the following three cases:

Case 1: If $m = 2l \ge 4$, then $[0, \lfloor \frac{m}{2} \rfloor] = [0, \frac{m}{2}]$.

Case 1.1: For $t \in [0, \frac{m}{2} - 1]$, then we have $0 \le |i \pm jq^{2t+1}| < \frac{q^{m+1}-q^2}{2}(q^{m-1} + 1) < s$, hence $i \pm jq^{2t+1} \not\equiv s(mod\ \ n)$.

Case 1.2: For $t = \frac{m}{2}$, let $j = q^{m-1}\alpha + \beta$ where $\beta \in [0, q^{m-1}-1]$ if $\alpha \in [0, \frac{q^2}{2}-2]$ and $\beta \in [0, q^{m-1} - \frac{q^2}{2} - 1]$ if $\alpha = \frac{q^2}{2} - 1$.

Since $i + jq^{m+1} = i + (q^{m-1}\alpha + \beta)q^{m+1} \equiv i + \beta q^{m+1} - \alpha(mod\ \ n)$ and $i - jq^{m+1} = i - (q^{m-1}\alpha + \beta)q^{m+1} \equiv n + i - (\beta q^{m+1} - \alpha)(mod\ \ n)$, then we can further deduce that:

i) If $0 \le \beta \le \frac{q^{m-1}-1}{2}$. Then $i + \beta q^{m+1} - \alpha \le \frac{q^{m+1}-q^2}{2} + \frac{q^{2m}-q^{m+1}}{2} = s - \frac{q^2+1}{2} < s$ and $n + i - (\beta q^{m+1} - \alpha) \ge q^{2m} + 1 + \frac{q^{m+1}-q^2}{2} - \frac{q^{2m}-q^{m+1}}{2} = s + q^{m+1} - \frac{q^2-1}{2} > s$.

ii) If $\beta \ge \frac{q^{m-1}+1}{2}$. Then $i + \beta q^{m+1} - \alpha \ge \frac{q^{m+1}-q^2}{2} + \frac{q^{2m}+q^{m+1}}{2} = s + q^{m+1} - \frac{q^2+1}{2} > s$ and $n + i - (\beta q^{m+1} - \alpha) \le q^{2m} + 1 + \frac{q^{m+1}-q^2}{2} - \frac{q^{2m}+q^{m+1}}{2} = s - \frac{q^2-1}{2} < s$.

According to the discussions in (i) and (ii), it can be inferred that $i \pm jq^{2t+1} \not\equiv s(mod\ \ n)$ for $t = \frac{m}{2}$.

Case 2: If $m = 2$, then $[0, \lfloor \frac{m}{2} \rfloor] = [0, 1]$. For $t = 0$, one can deduce $0 \le |i \pm jq^{2t+1}| \le \frac{q^3-q^2+q-1}{2}(q+1) = s - 1 < s$, hence $i \pm jq \not\equiv s(mod\ \ n)$.

For $t = 1$, let $j = q\alpha + \beta$ where $\beta \in [0, q-1]$ if $\alpha \in [0, \frac{q^2-q}{2} - 1]$ and $\beta \in [0, \frac{q}{2} - 2]$ if $\alpha = \frac{q^2-q}{2}$. Similar to the proof of *Case 1*, one can infer that $i \pm jq^{2t+1} \not\equiv s(mod\ \ n)$.

Case 3: If $m = 2l + 1 \ge 3$, then $[0, \lfloor \frac{m}{2} \rfloor] = [0, \frac{m-1}{2}]$. For $t \in [0, \frac{m-1}{2}]$, one can check $0 \le |i + jq^{2t+1}| < \frac{q^m-1}{2}(q^m + 1) = s - 1 < s$, hence $i \pm jq^{2t+1} \not\equiv s(mod\ \ n)$.

Concluding the previous three cases, we have proved the lemma. □

Corollary 3.4 *If* $T_i \subseteq T_{\frac{\delta_{\max}-2}{2}}$, *then* $T_i \bigcap T_i^{-q} = \emptyset$.

Proof To prove the corollary, it is enough to prove $T_{\frac{\delta_{\max}-2}{2}} \bigcap T^{-q}_{\frac{\delta_{\max}-2}{2}} = \emptyset$. According to Theorem 3.2 and Lemma 3.3, we can derive that there does not exist skew-symmetric cyclotomic cosets or any SAP in $T_{\frac{\delta_{\max}-2}{2}}$. Thus, one can deduce $T_{\frac{\delta_{\max}-2}{2}} \bigcap T^{-q}_{\frac{\delta_{\max}-2}{2}} = \emptyset$ and the corollary follows. □

Lemma 3.5 *The following cyclotomic coset pairs are skew-asymmetric pairs:*

$$\begin{cases} (C_{s+\frac{\delta_{\max}}{2}r}, C_{s+\frac{\delta_{\max}-2}{2}r}) & \text{if } m=2; \\ (C_{s+\frac{\delta_{\max}}{2}r}, C_{s+(\frac{\delta_{\max}}{2}-\frac{2q^{m-1}-q^2-1}{2})r}) & \text{if } m=2l\geq 4; \\ (C_{s+\frac{\delta_{\max}}{2}r}, C_{s+\frac{\delta_{\max}-2}{2}r}) & \text{if } m=2l+1\geq 3; \end{cases}$$

Proof According to Lemma 3.1, if h is odd, then $sq^h \equiv (r-1)s(mod\ \ rn)$, hence one can attain the following results:

(1) If $m=2$, we get

$$\begin{aligned} -(s+\frac{\delta_{\max}-2}{2}r)q &= -sq-\frac{q^4-q^3+q^2-q}{2}r \\ &\equiv -(r-1)s-\frac{q^4-q^3+q^2-q}{2}r \\ &\equiv s+\frac{q^3-q^2+q+1}{2}r(mod\ \ rn) \\ &= s+\frac{\delta_{\max}}{2}r \end{aligned}$$

It follows that $C_{s+\frac{\delta_{\max}}{2}r}$ and $C_{s+\frac{\delta_{\max}-2}{2}r}$ form a SAP.

(2) If $m=2l\geq 4$, we have

$$\begin{aligned} -(s+\frac{\delta_{\max}}{2}r)q^{m-1} &= -sq^{m-1}-\frac{q^{m+1}-q^2+2}{2}q^{m-1}r \\ &\equiv -(r-1)s-\frac{q^{m+1}-q^2+2}{2}q^{m-1}r \\ &\equiv s+\frac{q^{m+1}-q^2+2-2q^{m-1}+q^2-1}{2}r(mod\ \ rn) \\ &= s+(\frac{\delta_{\max}}{2}-\frac{2q^{m-1}-q^2-1}{2})r \end{aligned}$$

Hence $C_{s+\frac{\delta_{\max}}{2}r}$ and $C_{s+(\frac{\delta_{\max}}{2}-\frac{2q^{m-1}-q^2-1}{2})r}$ form a SAP.

(3) If $m=2l+1\geq 3$, we obtain

$$\begin{aligned} -(s+\frac{\delta_{\max}-2}{2}r)q^m &= -sq^m-\frac{q^m-1}{2}q^m r \\ &\equiv -(r-1)s-\frac{q^m-1}{2}q^m r \\ &\equiv s+\frac{q^m+1}{2}r(mod\ \ rn) \\ &= s+\frac{\delta_{\max}}{2}r. \end{aligned}$$

It implies $C_{s+\frac{\delta_{\max}}{2}r}$ and $C_{s+\frac{\delta_{\max}-2}{2}r}$ form a SAP. □

Theorem 3.6 *Let $q, m, n, \delta_{\max}$ be given as above. If δ_i is even and $\mathcal{C}(n, q^2; \delta_i)$ is the CBCH code with defining set T_i, then $\mathcal{C}(n, q^2; \delta_i)^{\perp_h} \subseteq \mathcal{C}(n, q^2; \delta_i)$ if and only if $2 \leq \delta_i \leq \delta_{\max}$.*

Proof (1) If δ_i is even and $\delta_i \leq \delta_{\max}$, then $T_{\frac{\delta_i-2}{2}} \subseteq T_{\frac{\delta_{\max}-2}{2}}$. It follows that $T_{\frac{\delta_i-2}{2}} \bigcap T^{-q}_{\frac{\delta_i-2}{2}} = \emptyset$ from Corollary 3.4 above, hence $\mathcal{C}(n, q^2; \delta_i)^{\perp_h} \subseteq \mathcal{C}(n, q^2; \delta_i)$ by Lemma 2.2, the sufficiency holds.

(2) If $\delta_i > \delta_{\max}$, then $C_{s+\frac{\delta_{\max}}{2}r} \subseteq T_{\frac{\delta_i-2}{2}r}$. Thus we can infer $T_{\frac{\delta_i-2}{2}} \bigcap T^{-q}_{\frac{\delta_i-2}{2}} \neq \emptyset$ from Lemma 2.2 and Lemma 3.5 above, so $\mathcal{C}(n, q^2; \delta_i)^{\perp_h} \nsubseteq \mathcal{C}(n, q^2; \delta_i)$ from Lemma 2.2, the necessity holds.

□

4 Dimensions of CBCH codes and new quantum codes

Consider $\mathcal{C}(n, q^2; \delta_i)$ is the CBCH code with defining set T_i, according to Theorem 3.6, $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$ when $0 < i \leq \frac{\delta_{\max}-2}{2}$. While Theorem 3.6 above and Hermitian Construction are sufficient to tell us one can construct some new quantum CBCH codes, they are still unsatisfactory because one does not know the dimension of these codes and their designed distances. In order to exactly calculate these parameters, we will first study the cardinality of each cyclotomic coset in T_i by Lemma 4.1 and talk about which cyclotomic cosets are equal to another in T_i by Lemmas 4.2 and 4.3.

Lemma 4.1 *Let $n, s, r, \delta_{\max}$ be given above. If $0 < i \leq \frac{\delta_{\max}-2}{2}$, then $|C_{s+ir}| = 2m$.*

Proof If $|C_{s+ir}| = t < 2m$, then $t|2m$ and $s + ir \equiv (s + ir)q^{2t} \equiv s + irq^{2t} (mod\ rn)$ $\Rightarrow i(q^{2t} - 1) \equiv 0 (mod\ n)$. From $t|2m$, we have $t = \frac{2m}{2}, t = \frac{2m}{3}, t = \frac{2m}{4}$ or $t \leq \frac{2m}{5}$.

i) If $t = \frac{2m}{2} = m$, then $(q^{2t} - 1, n) = (q^{2m} - 1, q^{2m} + 1) = 2$. Since $i < \frac{n}{2}$, one can deduce $i(q^{2t} - 1) \not\equiv 0 (mod\ n)$, a contradiction.

ii) If $m \equiv 0 (mod\ 3)$ and $t = \frac{2m}{3}$, then $(q^{2t} - 1, n = q^{2m} + 1) = q^{\frac{2m}{3}} + 1$ and $1 \leq i \leq \frac{\delta_{\max}-2}{2} < \frac{n}{q^{\frac{2m}{3}}+1} = (q^{\frac{4m}{3}} - q^{\frac{2m}{3}} + 1)$. Thus $i(q^{2t} - 1) \not\equiv 0 (mod\ n)$, a contradiction.

iii) If $m \equiv 0 (mod\ 2)$ and $t = \frac{2m}{4} = \frac{m}{2}$, then $(q^{2t} - 1, n) = (q^m - 1, q^{2m} + 1) = 2$. Since $i < \frac{n}{2}$, $i(q^{2t} - 1) \not\equiv 0 (mod\ n)$, a contradiction.

iv) If $t \leq \frac{2m}{5}$, then $i(q^{2t} - 1) \leq \frac{\delta_{\max}-2}{2}(q^{\frac{4m}{5}} - 1) < n$. Thus $i(q^{2t} - 1) \not\equiv 0 (mod\ n)$, a contradiction. □

Summarizing the previous discussions, thus the lemma holds.

Lemma 4.2 *Let n, s, r be given above. If $m = 2l + 1 > 3$, $\delta_{\max} = q^m + 1$ and $0 \leq j < i \leq \frac{\delta_{\max}-2}{2}$, then $C_{s+ir} = C_{s+jr}$ if and only if $i = jq^{2t}$ for some $t \in [1, \frac{m-1}{2}]$.*

Proof According to (1) of Theorem 3.2, $C_{s+ir} = C_{s+jr} \Leftrightarrow \exists t \in [0, \frac{m-1}{2}]$ such that $j \pm iq^{2t} \equiv 0 (mod\ n)$ or $i \pm jq^{2t} \equiv 0 (mod\ n)$.

From $t \in [0, \frac{m-1}{2}]$, we have $0 < i + jq^{2t} \leq \frac{\delta_{\max}-2}{2}(q^{m-1}+1) = \frac{q^m-1}{2}(q^{m-1}+1) < n$, and $0 \leq |i - jq^{2t}| \leq \frac{q^m-1}{2}(q^{m-1}+1) < n$. Thus, one can deduce $i \pm jq^{2t} \equiv 0(mod\ n) \Leftrightarrow i = jq^{2t}$. Since $j < i$, it can be easily checked that $j \pm iq^{2t} \not\equiv 0(mod\ n)$.

Then the desired conclusion follows. □

Lemma 4.3 *Let $n, s, r, \delta_{\max}$ be given above. If $m = 2l \geq 2$, $1 \leq \beta \leq \frac{q-1}{2}$ and $0 \leq j < i \leq \frac{\delta_{\max}-2}{2}$, then $C_{s+ir} = C_{s+jr}$ if and only if i and j satisfy the following conditions:*

(1) $1 \leq i < q^m$, $i = jq^{2t}$ *for some* $t \in [0, \frac{m-2}{2}]$;
(2) $i = \beta q^m = jq^{2t}$ *for some* $t \in [0, \frac{m}{2}]$.
(3) $i = \beta q^m - \alpha$ *and* $j = \alpha q^m + \beta (1 \leq \alpha < \beta)$.
(4) $i = \beta q^m + \alpha$ *and* $j = \alpha q^m - \beta (1 \leq \alpha \leq \beta)$.
(5) $\beta(q^m+1)+1 \leq i \leq (\beta+1)(q^m-1)-1$ *with* $1 \leq \beta \leq \frac{q-3}{2}$, $i = \beta q^m + \gamma q^2$ *and* $j = i/q^2 = \beta q^{m-2} + \gamma$ *where* $1 \leq \gamma \leq q^{m-2} - 1$.
(6) $\beta(q^m+1)+1 \leq i \leq \frac{\delta_{\max}-2}{2}$ *with* $\beta = \frac{q-1}{2}$, $i = \beta q^m + \gamma q^2$ *and* $j = i/q^2 = \beta q^{m-2} + \gamma$ *where* $1 \leq \gamma \leq \frac{\delta_{\max}-2}{2q^2}$.

Proof We only give the proof for $m \geq 4$, the situation for $m = 2$ can be given Similarly. According to (1) of Theorem 3.2, $C_{s+ir} = C_{s+jr} \Leftrightarrow \exists t \in [0, \frac{m}{2}]$ such that $j \pm iq^{2t} \equiv 0(mod\ \ n)$ or $i \pm jq^{2t} \equiv 0(mod\ \ n)$. Now we manage to determine the equal cosets $C_{s+ir} = C_{s+jr}$ step by step.

Step 1: If $1 \leq j < i < q^m$, we can derive $i = jq^{2t}$ as we did in Lemma 4.2.

Step 2: If $q^m \leq i \leq \frac{\delta_{\max}-2}{2}$, one can denote $i = \beta q^m + \alpha$, where $\alpha \in [0, q^m - 1]$.

When $t \in [0, \frac{m}{2} - 1]$, from $0 < j < i$, similar to the proof of Lemma 4.2, we can deduce $i = jq^{2t}$.

When $t = \frac{m}{2}$, from $i \pm jq^m \equiv 0(mod\ \ n)$ or $j \pm iq^m \equiv 0(mod\ \ n)$, one has $\beta q^m + \alpha \pm jq^m \equiv 0(mod\ \ n)$ or $j \pm (\beta q^m + \alpha)q^m \equiv 0(mod\ \ n)$. Since $(q^m, n) = 1$, we can derive $\beta q^{2m} + \alpha q^m \pm jq^{2m} \equiv (\alpha q^m - \beta) \mp j \equiv 0(mod\ n)$ or $j \pm \beta q^{2m} + \alpha q^m \equiv j \pm (\alpha q^m - \beta) \equiv 0(mod\ n)$. Thus, one can attain $j = \alpha q^m - \beta$ or $j = n - (\alpha q^m - \beta)$. Thus we study the case for $t = \frac{m}{2}$ by following three steps:

Step 2.1: If $\alpha = 0$ and $i = \beta q^m$, we have $j \mp \beta \not\equiv 0(mod\ n)$, from $1 \leq j + \beta < n$ and $0 \leq j - \beta < n$, one can attain $j = \beta$.

Step 2.2: If $1 \leq \alpha \leq \beta$, Since $0 \leq j < i \leq \frac{\delta_{\max}-2}{2}$, we have $j = \alpha q^m - \beta$.

Step 2.3: If $q^m - \frac{q-1}{2} \leq \alpha \leq q^m - 1$, from $0 \leq j < i \leq \frac{\delta_{\max}-2}{2}$, we have $j = n - (\alpha q^m - \beta) = (q^m - \alpha)q^m + \beta + 1$. We assume $\beta' = \beta + 1$ and $\alpha' = q^m - \alpha$, where $\beta' \in [1, \frac{q-1}{2}]$ and $\alpha' \in [0, \frac{q-1}{2}]$. It follows that $i = \beta' q^m - \alpha'$, $j = \alpha' q^m + \beta'$, which is equivalent to that $i = \beta q^m - \alpha$ and $j = \alpha q^m + \beta (1 \leq \alpha \leq \beta)$.

Step 2.4: If $\beta < \alpha < q^m - \frac{q-1}{2}$, let $\alpha = \gamma q^2 + \lambda$ and γ, j be given in (5) and (6), it is easily verified that $C_{s+ir} = C_{s+jr}$ where $i = jq^2 = \beta q^m + \gamma q^2$ with $\lambda = 0$.

Next, we will show there exists no $j < i$ such that $C_{s+ir} = C_{s+jr}$ for $1 \leq \lambda \leq q^2 - 1$. The reason is that:

from $0 < j < i < \frac{\delta_{\max}-2}{2}$, similar to the proof of Lemma 4.2, since $i \not\equiv 0 mod\ \ q^2$, we can deduce $0 < |i \pm jq^{2t}| < \frac{q^{m+1}-q^2}{2}(1+q^{m-2}) < n$ and $0 < |j \pm iq^{2t}| < n$ when

$t \in [0, \frac{m-2}{2}]$. As for $t = \frac{m}{2}$, according to the discussion of *Step 2* for $t = \frac{m}{2}$, when $\beta < \alpha < q^m - \frac{q-1}{2}$, we can infer $i \pm jq^{2t} \not\equiv 0 (mod\ \ n)$ and $j \pm iq^{2t} \not\equiv 0 (mod\ \ n)$.

According to the previous two steps, one can see the lemma follows.

By these above results about q^2-cyclotomic cosets modulo rn, it is feasible to analyze the parameters of Hermitian containing CBCH codes, and one can derive new quantum CBCH codes from them via Hermitian Construction. We will show these results in the following Theorems 4.4 and 4.5. □

Theorem 4.4 *Let $m = 2l + 1 \geq 3$, $n, s, r, \delta_{\max}$ be given above. If $i \in [0, \frac{\delta_{\max}-2}{2}]$, let $\delta_i = 2i + 2$ for $i + 1 \not\equiv 0 (mod\ \ q^2)$, let $\delta_i = 2i + 4$ for $i + 1 \equiv 0 (mod\ \ q^2)$. Then*

(1) there exists a Hermitian dual-containing CBCH code with parameters $[n, n - |T_i|, \geq \delta_i]_{q^2}$ where $|T_i| = 2m\lceil i(1 - q^{-2})\rceil + 1$.

(2) there exists a quantum CBCH code with parameters $[[n, n - 2|T_i|, \geq \delta_i]]_q$.

Proof (1) Let $T_i = C_s \cup C_{s+r} \cup C_{s+2r} \cup \cdots \cup C_{s+ir}$ for $i \in [0, \frac{\delta_{\max}-2}{2}]$. Then $T_i = \bigcup_{j=-i}^{i} C_{s+jr}$ according to Theorem 2.3. If $i + 1 \not\equiv 0 (mod\ q^2)$, then $T_i \neq T_{i+1}$, and the CBCH code with defining set T_i has designed distance $\delta = 2i + 2$. If $i + 1 \equiv 0 (mod\ q^2)$, then $T_i = T_{i+1} = \bigcup_{j=-(i+1)}^{i+1} C_{s+jr}$ according to Lemma 4.2, and the CBCH code with defining set T_i has designed distance $\delta = 2(i + 1) + 2$.

If $1 \leq i \leq \frac{\delta_{\max}-2}{2}$ and i is a multiple of q^2, then $C_{s+ir} = C_{s+ir/q^2}$. Therefore, the number of cosets is reduced by $\lfloor i/q^2 \rfloor$. By lemma 4.2, if $i \neq j$ and $i, j \not\equiv 0 (mod\ q^2)$, then $C_{s+ir} \neq C_{s+jr}$. Thus, T_i is the union of $i - \lfloor i/q^2 \rfloor + 1 = \lceil i(1-q^{-2})\rceil + 1$ distinct cyclotomic cosets. By Theorem 2.3 and Lemma 4.1, all these cosets have cardinality $2m$ besides $C_s = \{s\}$, then we can deduce $|T_i| = 2m\lceil i(1 - q^{-2})\rceil + 1$, which proves our claim about the parameters of the code.

(2) By Hermitian construction, one can construct a quantum CBCH code with parameters $[[n, n - 2|T_i|, \geq \delta_i]]_q$ from a Hermitian dual-containing CBCH code of (1), hence (2) holds. □

Theorem 4.5 *Let $m = 2l \geq 2$, $n, s, r, \delta_{\max}$ be given above. If $i \in [0, \frac{\delta_{\max}-2}{2}]$, let $\delta_i = 2i + 2$ for $i + 1 \not\equiv 0 (mod\ \ q^2)$, let $\delta_i = 2i + 4$ for $i + 1 \equiv 0 (mod\ \ q^2)$. Then the following hold:*

(1) If $1 \leq i \leq q^m - 2$, then there exists a Hermitian dual-containing CBCH code with parameters $[n, n - 2|T_i|, \geq \delta_i]_{q^2}$ where $|T_i| = 2m\lceil i(1 - q^{-2})\rceil + 1$.

(2) If $\beta(q^m + 1) \leq i \leq (\beta + 1)(q^m - 1) - 1$ with $\beta \in [1, \frac{q-3}{2}]$, or $\frac{q-1}{2}(q^m + 1) \leq i \leq \frac{\delta_{\max}-2}{2}$, then there exists a Hermitian dual-containing CBCH code with parameters $[n, n - 2|T_i|, \geq \delta_i]_{q^2}$ where $|T_i| = 2m(\lceil i(1 - q^{-2})\rceil - \lfloor iq^{-m} \rfloor^2) + 1$.

(3) If i and δ_i are given as above, then there exists a quantum CBCH code with parameters $[[n, n - 2|T_i|, \geq \delta_i]]_q$, where $|T_i|$ is given as in (1) and (2), respectively.

Proof Let $T_i = C_s \cup C_{s+r} \cup C_{s+2r} \cup \cdots \cup C_{s+ir}$.

(1) If $1 \leq j \leq i \leq q^m - 2$, then $C_{s+jr} = C_{s+ir}$ if and only if $i = jq^{2t}$ according to Lemma 4.3. Similar to the discussion given in the proof of (1) of Theorem 4.4, we can derive (1) holds.

(2) From Lemma 4.3, if $\beta \in [1, \frac{q-1}{2}]$, we can deduce

$$\begin{aligned} T_{q^m-1} = T_{q^m} &= T_{q^m+1}, \\ T_{2(q^m-1)} = T_{2q^m-1} = T_{2q^m} &= T_{2q^m+1} = T_{2(q^m+1)}, \\ &\vdots \\ T_{\beta(q^m-1)} = T_{\beta q^m-\beta+1} = \cdots = T_{\beta q^m} &= \cdots = T_{\beta q^m+\beta-1} = T_{\beta(q^m+1)}. \end{aligned}$$

Hence, if

$$\begin{cases} \beta(q^m+1) \le i \le (\beta+1)(q^m-1)-1 & \beta \in [1, \frac{q-3}{2}]; \\ \beta(q^m+1) \le i \le \frac{\delta_{\max}-2}{2} & \beta = \frac{q-1}{2}, \end{cases}$$

then the number of different cosets contained in T_i is u_i, where

$$\begin{aligned} u_i &= 1 + (i - \lfloor i/q^2 \rfloor) - (1 + 3 + \cdots + 2\beta - 1) \\ &= 1 + \lceil i(1-q^{-2}) \rceil - \beta^2 \\ &= 1 + (\lceil i(1-q^{-2}) \rceil - \lfloor iq^{-m} \rfloor^2). \end{aligned}$$

Thus, similar to Theorem 4.4, we can obtain

$$|T_i| = 2m(\lceil i(1-q^{-2}) \rceil - \lfloor iq^{-m} \rfloor^2) + 1.$$

Furthermore, if $i+1 \not\equiv 0 (mod\ q^2)$, then T_i defines a CBCH code with designed distance $\delta_i = 2i+2$; if $i+1 \equiv 0 (mod\ q^2)$, then $T_i = T_{i+1}$ defines a CBCH code with designed distance $\delta_i = 2i+4$. □

Summarizing the above, we have showed (2) holds.

(3) Using the Hermitian dual-containing CBCH codes presented in (1) and (2), we get the conclusion of (3).

Table 1 New quantum constacyclic code for $q = 3$

m	n	$\delta \equiv 0 (mod\ 2)$	$[[n, k, d]]_q$
2	82	$2 \le \delta \le 16$	$[[82, 88-4\delta, \ge \delta]]_3$ in [21]
2	82	22	$[[82, 16, \ge \delta]]_3$
3	730	$2 \le \delta \le 16$	$[[730, 740-6\delta, \ge \delta]]_3$ [21]
3	730	$20 \le \delta \le 28$	$[[730, 752-6\delta, \ge \delta]]_3$
4	6562	$2 \le \delta \le 16$	$[[6562, 6576-8\delta, \ge \delta]]_3$[21]
4	6562	$18\alpha+2 \le \delta \le 18\alpha+16 (\alpha \in [1,7])$	$[[6562, 6576-8\delta+16\alpha, \ge \delta]]_3$
4	6562	$146 \le \delta \le 160$	$[[6562, 6704-8\delta, \ge \delta]]_3$
4	6562	$166 \le \delta \le 178$	$[[6562, 6736-8\delta, \ge \delta]]_3$
4	6562	$18\alpha+164 \le \delta \le 18\alpha+178 (\alpha \in [1,3])$	$[[6562, 6736-8\delta+16\alpha, \ge \delta]]_3$
4	6562	236	$[[6562, 4912, \ge \delta]]_3$

Table 2 New quantum negacyclic code for $q = 5$

m	n	$\delta \equiv 0 (mod\ 2)$	$[[n, k, d]]_q$
2	626	$2 \le \delta \le 48$	$[[626, 632 - 4\delta, \ge \delta]]_5$ in [19]
2	626	$54 \le \delta \le 96$	$[[626, 648 - 4\delta, \ge \delta]]_5$
2	626	106	$[[626, 256, \ge \delta]]_5$
3	15626	$2 \le \delta \le 48$	$[[15626, 15636 - 6\delta, \ge \delta]]_5$ in [19]
3	15626	$52 \le \delta \le 98$	$[[15626, 15648 - 6\delta, \ge \delta]]_5$
3	15626	$102 \le \delta \le 126$	$[[15626, 15660 - 6\delta, \ge \delta]]_5$
4	390626	$2 \le \delta \le 48$	$[[390626, 390640 - 8\delta, \ge \delta]]_5$ in [19]
4	390626	$50\alpha + 2 \le \delta \le 50\alpha + 48 (\alpha \in [1, 23])$	$[[390626, 390640 - 8\delta + 16\alpha, \ge \delta]]_5$
4	390626	$1202 \le \delta \le 1248$	$[[390626, 391024 - 8\delta, \ge \delta]]_5$
4	390626	$1254 \le \delta \le 1298$	$[[390626, 391056 - 8\delta, \ge \delta]]_5$
4	390626	$50\alpha + 1252 \le \delta \le 50\alpha + 1298 (\alpha \in [1, 23])$	$[[390626, 391056 - 8\delta + 16\alpha, \ge \delta]]_5$
4	390626	$2452 \le \delta \le 2496$	$[[390626, 391440 - 8\delta, \ge \delta]]_5$
4	390626	$2506 \le \delta \le 2598$	$[[390626, 391504 - 8\delta, \ge \delta]]_5$
4	390626	$50\alpha + 2502 \le \delta \le 50\alpha + 2548 (\alpha \in [1, 11])$	$[[390626, 391504 - 8\delta + 16\alpha, \ge \delta]]_5$
4	390626	3102	$[[390626, 366880, \ge \delta]]_5$

Table 3 Codes comparisons for $q = 5$ and $m = 2$

New quantum codes	QBCH codes in [15]	New quantum codes	QBCH codes in [15]
$[[626, 432, \ge 54]]_5$	$[[624, 420, \ge 54]]_5$	$[[626, 336, \ge 78]]_5$	$[[624, 328, \ge 78]]_5$
$[[626, 424, \ge 56]]_5$	$[[624, 412, \ge 56]]_5$	$[[626, 328, \ge 80]]_5$	$[[624, 320, \ge 80]]_5$
$[[626, 416, \ge 58]]_5$	$[[624, 404, \ge 58]]_5$	$[[626, 320, \ge 82]]_5$	$[[624, 312, \ge 82]]_5$
$[[626, 408, \ge 60]]_5$	$[[624, 396, \ge 60]]_5$	$[[626, 312, \ge 84]]_5$	$[[624, 304, \ge 84]]_5$
$[[626, 400, \ge 62]]_5$	$[[624, 388, \ge 62]]_5$	$[[626, 304, \ge 86]]_5$	$[[624, 296, \ge 86]]_5$
$[[626, 392, \ge 64]]_5$	$[[624, 380, \ge 64]]_5$	$[[626, 296, \ge 88]]_5$	$[[624, 288, \ge 88]]_5$
$[[626, 384, \ge 66]]_5$	$[[624, 372, \ge 66]]_5$	$[[626, 288, \ge 90]]_5$	$[[624, 280, \ge 90]]_5$
$[[626, 376, \ge 68]]_5$	$[[624, 364, \ge 68]]_5$	$[[626, 280, \ge 92]]_5$	$[[624, 272, \ge 92]]_5$
$[[626, 368, \ge 70]]_5$	$[[624, 356, \ge 70]]_5$	$[[626, 272, \ge 94]]_5$	$[[624, 264, \ge 94]]_5$
$[[626, 360, \ge 72]]_5$	$[[624, 348, \ge 72]]_5$	$[[626, 264, \ge 96]]_5$	$[[624, 256, \ge 96]]_5$
$[[626, 352, \ge 74]]_5$	$[[624, 340, \ge 74]]_5$	$[[626, 256, \ge 106]]_5$	$[[624, 220, \ge 106]]_5$
$[[626, 344, \ge 76]]_5$	$[[624, 336, \ge 76]]_5$		

5 Conclusion and discussion

We have explored the Hermitian dual-containing condition and determined the maximum designed distances of CBCH codes with length $n = q^{2m} + 1$, the dimensions and designed distances of these dual-containing codes are completely settled. Based on these, we constructed a class of new quantum CBCH codes of length $n = q^{2m} + 1$ and determined the parameters of quantum CBCH codes from the designed distances of CBCH codes.

For clarity to show our results, we list a lot of new quantum constacyclic codes for $q = 3$ in Table 1 and quantum negacyclic codes for $q = 5$ in Table 2, respectively. Further, in Table 3, we extract a small part of quantum negacyclic codes from Table 2 and compare them with some of quantum BCH (QBCH) codes derived from primitive BCH codes in Theorem 13 of [15] for $54 \leq \delta \leq 106$. From Table 3, one can see that for given designed distance δ, our new quantum codes $[n+2, k, \geq \delta]$ use two more qubits than $[n, k', \geq \delta]$ QBCH of the same minimum distance derived from primitive BCH codes but have much higher code rate than the QBCH codes of the same minimum distance ($k - k' \geq 8$). Hence our codes are much more efficient than those QBCH codes of the same designed distances.

Acknowledgements This work was supported by National Natural Science Foundation of China under Grant No.11471011 and Natural Science Foundation of Shaanxi under Grant No.2015JM1023.

References

1. Shor, P.W.: Scheme for reducing decoherence in quantum computing memory. Phys. Rev. A **52**, R2493 (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. Gottesman, D.: Stabilizer codes and quantum error correction. Ph.D. Thesis, California Institute of Technology (1997)
5. Steane, A.M.: Enlargement of Calderbank-Shor-Steane quantum codes. IEEE. Trans. Inf. Theory **45**, 2492–2495 (1999)
6. Li, R., Li, X.: Binary construction of quantum codes of minimum distance three and four. IEEE. Trans. Inf. Theory **50**, 1331–1336 (2004)
7. Rains, E.M.: Non-binary quantum codes. IEEE. Trans. Inf. Theory **45**, 1827–1832 (1999)
8. Ashikhim, A., Knill, E.: Non-binary quantum stabilizer codes. IEEE. Trans. Inf. Theory **47**, 3065–3072 (2001)
9. Ketkar, A., Klappenecker, A., Kumar, S.: Nonbinary stabilizer codes over finite fields. IEEE. Trans. Inf. Theory **52**, 4892–4914 (2006)
10. Ling, S., Luo, J., Xing, C.: Generalization of Steane's enlargement construction of quantum codes and applications. IEEE Trans. Inf. Theory **56**, 4080–4084 (2010)
11. Hamada, M.: Concatenated quantum codes constructible in polynomial time: efficient decoding and error correction. IEEE. Trans. Inf. Theory **54**, 5689–5704 (2008)
12. Grassl, M., Beth, T.: Quantum BCH codes. Proc. X. int'l. Symp. Theoretical. Electrical Engineering Magdeburg, 207-212 (1999)
13. Li, R., Li, X.: Quantum codes constructed from binary cyclic codes. Int. J. Quantum Inf. **2**, 265–272 (2004)
14. Aly, S.A., Klappenecker, A., Sarvepalli, P.K.: Primitive quantum BCH codes over finite fields. Proc. Int. Symp. Inf. Theory, 1114-1118 (2006)
15. Aly, S.A., Klappenecker, A., Sarvepalli, P.K.: On quantum and classical BCH codes. IEEE. Trans. Inf. Theory **53**, 1183–1188 (2007)
16. Guardia, G.G.La: Constructions of new families of nonbinary quantum codes. Phys. Rev. A **80**, 042331 (2009)
17. Li, R., Zuo, F., Liu, Y.: A study of skew symmetric q^2-cyclotomic coset and its application. J. Air Force Eng. Univ. **12**(1), 87–89 (2011)
18. Li, R., Zuo, F., Liu, Y., Xu, Z.: Hermitian dual-containing BCH codes and construction of new quantum codes. Quantum Inf. Comput. **12**, 0021–0035 (2013)
19. Kai, X., Zhu, S.: Quantum negacyclic codes. Phys. Rev. A **88**, 012326 (2013)
20. Kai, X., Zhu, S., Li, P.: Constacyclic codes and some new quantum MDS codes. IEEE Trans. Inf. Theory **60**, 2080–2086 (2014)

21. Hu, X., Zhang, G., Chen, B.: Constructions of new nonbinary quantum codes. Int. J. Theory Phys. **54**, 92–99 (2015)
22. Chen, B., Ling, S., Zhang, G.: Application of constacyclic codes to quantum MDS codes. IEEE Trans. Inf. Theory **61**, 1474–1484 (2015)
23. Guardia, G.G.La: On optimal constacyclic codes. Linear Algebra Appl. **496**, 594–610 (2016)
24. Wang, L., Zhu, S.: New quantum MDS codes derived from constacyclic codes. Quantum Inf. Processing **14** 3, 881-889(2015). See also arXiv:1405.5421v1
25. Zhang, T., Ge, G.: Some new class of quantum MDS codes from constacyclic codes. IEEE Trans. Inf. Theory **61**, 5224–5228 (2015)
26. Aydin, N., Siap, I., Ray-Chaudhuri, D.K.: The structure of 1-generator quasi-twisted codes and new linear codes. Des. codes cryptogr. **24**, 313–326 (2001)
27. Krishna, A., Sarwate, D.V.: Pseudo-cyclic maximum-distance separable codes. IEEE Trans. Inf. Theory **36**, 880–884 (1990)
28. Peterson, W.W., Weldon, E.J.: Error-correcting codes. The M.I.T. Press, Cambridge (1972)
29. Macwilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, Amsterdam (1977)
30. Guardia, G.G.La: New quantum MDS codes. IEEE Trans. Inf. Theory **57**, 5551–5554 (2011)
31. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)
32. Sloane, N.J.A., Thompson, J.G.: Cyclic self-dual codes. IEEE Trans. Inf. Theory **29**, 364–366 (1983)