IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 21, 2018, accepted June 21, 2018, date of publication June 27, 2018, date of current version July 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2851075

Construction of Some New Quantum BCH Codes

MING ZHANG, ZHUO LI, LIJUAN XING, AND NIANQI TANG
State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China

Corresponding author: Zhuo Li (lizhuo@xidian.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61372072, in part by the 111 Project under Grant B08038, and in part by the Fundamental Research Funds for the Central Universities.

ABSTRACT Classical Bose–Chaudhuri–Hocquenghem (BCH) codes over finite fields have been studied extensively. One can construct quantum stabilizer codes with good parameters using classical BCH codes. In this paper, our goal is to find such classical BCH codes. We study some properties of suitable cyclotomic cosets at first. These results make it possible to construct nonbinary quantum BCH codes with a given parameter set. Several new families of quantum BCH codes obtained are based on Steane's enlargement of nonbinary Calderbank–Shor–Steane codes and Hermitian construction, respectively. Meanwhile, we have shown that the cyclotomic cosets given in our schemes are optimal to design quantum BCH codes. The defining set contains most consecutive integers. Therefore, corresponding quantum stabilizer codes have better lower bound of minimum distance. Furthermore, it is convenient to compute the dimension of new quantum codes. Compared with the ones available in the literature, the quantum BCH codes in our schemes have good parameters. In particular, we extend known results to more general case.

INDEX TERMS Bose-Chaudhuri-Hocquenghem codes, cyclotomic cosets, stabilizer codes.

I. INTRODUCTION

Quantum information theory is rapidly becoming a well-established discipline in quantum communication and quantum computation [10]. However, a major shortcoming of realizing quantum communication is decoherence of qubits. There has been much interest in the subject of quantum error correcting codes to address this issue [2], [6]–[9]. Furthermore, quantum error correcting codes are widely used in quantum cryptography such as BB84 quantum key distribution (QKD) protocol and secure share schemes [4]. Therefore, it is significant to research and design quantum codes.

Cyclic codes in classical information theory have additional algebraic structure to make encoding and decoding more efficient. There exist links to classical coding theory that facilitate the construction of quantum codes [10]. Therefore, quantum error correcting codes are much investigated by applying classical cyclic codes in recently. Nonbinary quantum codes with good parameters were designed from cyclic codes by applying the Calderbank-Shor-Steane (CSS) constructions [18]. Based on characteristics of classical q^2-ary constacyclic codes, some new quantum codes could be obtained via Hermitian constructions [14], [15]. Furthermore, [17] constructed quantum codes from negacyclic codes. The Bose-Chaudhuri-Hocquenghem (BCH) codes, as a special subclass of cyclic codes, play an important role in classical information theory [3]. Many quantum BCH codes have been constructed by classical error correcting codes in recent years. Steane gave a simple criterion to decide whether a binary narrow-sense primitive BCH code contains its dual or not [7]. The design of binary quantum BCH codes is transformed into the problem of finding additive codes over $GF(4)$ in [5]. Afterwards, Ketkar *et al.* [9] extended these results in [5] to nonbinary primitive quantum BCH codes. Steane's result are generalized in various ways, in particular, to narrow-sense (not necessarily primitive) BCH codes over arbitrary finite fields with respect to designed distance [2]. By applying useful properties of cyclotomic cosets, [6] and [8] constructed families of good nonbinary quantum codes based on given parameters. Quantum codes could be designed not only from BCH codes [13] but also from negacyclic BCH codes [16].

Motivated by the construction of quantum BCH codes with good parameters, this paper is then devoted to the study of such codes over finite fields. These new families of nonbinary quantum BCH codes with a given parameter set in our schemes have better parameters. Specifically, fixing code length, the new quantum BCH codes achieve greater values of the number of encoded qubits and lower bound of the minimum distance than the codes available in the literature (see Tables 1 to Table 6). In this paper, the properties of

cyclotomic cosets are applied to determine whether a classical BCH code contains its dual or not firstly. We make sure that cyclotomic cosets chosen are mutually disjoint. Then it is tractable to work out the dimension of quantum BCH codes exactly with the help of some lemmas. In addition, the defining set contains most consecutive integers as much as possible. Quantum BCH codes are constructed by these result with respect to Euclidean and Hermitian duality.

The remainder of this paper is arranged as follows. Section II gives a brief review of classical BCH codes over finite fields. New families of quantum BCH codes are constructed by classical BCH codes over F_q and F_{q^2} in Section III and Section IV, respectively. In Section V, the parameters in our schemes are compared with the ones available in the literature. Finally, conclusions are drawn in Section VI.

II. PRELIMINARIES

The BCH codes as a well-studied class of cyclic codes have found numerous applications in classical [3] and quantum information processing [2], [5], [8]. Before delving into the details, let us present a short overview of relevant concepts on BCH codes.

The finite field is denoted by F_q, where q is a prime power. Let n be the code length such that $\gcd(n, q) = 1$. The smallest positive integer m such that $q^m \equiv 1 \mod n$ is called the multiplicative order of q modulo n denoted by $m = ord_n(q)$.

Given two vectors $\boldsymbol{x} = (x_0, x_1, \cdots, x_{n-1})$ and $\boldsymbol{y} = (y_0, y_1, \cdots, y_{n-1}) \in F_q^n$, Euclidean inner product is defined by

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle_E = x_0y_0 + x_1y_1 + \cdots + x_{n-1}y_{n-1}$$

while Hermitian inner product over F_{q^2} is defined by

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle_H = x_0y_0^q + x_1y_1^q + \cdots + x_{n-1}y_{n-1}^q.$$

The Euclidean dual code of C is defined by

$$C^{\perp E} = \{\boldsymbol{x} \in F_q^n \mid \langle \boldsymbol{x}, \boldsymbol{y} \rangle_E = 0 \text{ for all } \boldsymbol{y} \in C\}.$$

Similarly, the Hermitian dual code of C is defined by

$$C^{\perp H} = \{\boldsymbol{x} \in F_q^n \mid \langle \boldsymbol{x}, \boldsymbol{y} \rangle_H = 0 \text{ for all } \boldsymbol{y} \in C\}.$$

A linear code C is called Euclidean dual-containing if $C^{\perp E} \subseteq C \subsetneq F_q^n$. If $C^{\perp H} \subseteq C \subsetneq F_{q^2}^n$, we say that C is a Hermitian dual-containing code.

A BCH code C over F_q of length n and designed distance δ is a cyclic code with defining set

$$Z = \bigcup_{i=b}^{b+\delta-2} \mathbb{C}[i],$$

where $\mathbb{C}[i] = \{iq^z \mod n \mid z \in \mathbb{Z}, z \geq 0\}$ is the q-ary cyclotomic coset modulo n containing i. If $n = q^m - 1$ then the BCH code is called primitive and if $b = 1$ it is called narrow-sense.

The minimal polynomial over F_q of $\beta \in F_{q^m}$ is the monic polynomial of smallest degree, $M(x)$, with coefficients in F_q such that $M(\beta) = 0$. If $\beta = \alpha^i$ for a fixed primitive n-th root of unity $\alpha \in F_{q^m}$, then the minimal polynomial of β over F_q is denoted by $M^{(i)}(x) = \prod_{i \in \mathbb{C}[i]} (x - \alpha^i)$. We can compute the dimension of BCH codes with $k = n - |Z|$. The problem of finding minimum distance of BCH codes had been a long-standing open problem [11]. From the BCH bound, this code has minimum distance at least δ. A thorough discussion about classical BCH codes is offered in [3].

Steane's enlargement and Hermitian construction are one of the most utilized methods in design of quantum codes. To proceed further, it is necessary to review some useful results.

Theorem 1 (Quantum Code Constructions [2], [12]):

1) If there exists a classical linear $[n, k_1, d_1]_q$ code C_1, which contains its Euclidean dual $C_1^{\perp E}$ and which can be enlarged to an $[n, k_2, d_2]_q$ linear code C_2, where $k_2 - k_1 \geq 2$, then there exists an $[[n, k_1 + k_2 - n, d \geq \min\{d_1, \lceil \frac{q+1}{q} d_2 \rceil\}]]_q$ stabilizer code.
2) If there exists a classical linear $[n, k, d]_{q^2}$ code D such that $D^{\perp H} \subseteq D$, then there exists an $[[n, 2k - n, \geq d]]_q$ stabilizer code.

The following Lemma has the potential to find such classical codes that contain their duals.

Lemma 1 ([2]): Assume that q is a prime power and n is an integer such that $\gcd(n, q) = 1$.

1) A cyclic code of length n over F_q with defining set Z contains its Euclidean dual code if and only if $Z \cap Z^{-1} = \emptyset$, where $Z^{-1} = \{-z \mod n \mid z \in Z\}$.
2) A cyclic code of length n over F_{q^2} with defining set Z contains its Hermitian dual code if and only if $Z \cap Z^{-q} = \emptyset$, where $Z^{-q} = \{-qz \mod n \mid z \in Z\}$.

III. STEANE'S CONSTRUCTIONS

Let $n = r\frac{q^m-1}{q-1}$ and $m = ord_n(q)$. Since $n \mid q^m - 1$, it follows that $r\frac{q^m-1}{q-1} \mid q^m - 1$. One obtains $r(q^m - 1) \mid (q^m - 1)(q - 1)$. Then we have $r \mid q - 1$. If $q = 2$, one has $n = 2^m - 1$, which has been discussed by Steane [7]. Quantum BCH codes with $n = \frac{q^m-1}{q-1}$ for $r = 1$ were studied in [6]. We consider the case where $q \geq 3$ and $r > 1$ in this section.

A. m IS EVEN

Let $Q_0 = \frac{q^{\frac{m}{2}}-1}{q-1}$ and $Q_1 = \frac{q^{\frac{m}{2}-1}-1}{q-1}$ when m is even. Some available results about the q-ary cyclotomic cosets are presented as follows.

Lemma 2: If i is an integer such that $rQ_0 \mid i$, then $\mathbb{C}[i] = -\mathbb{C}[i]$.

Proof: It suffices to show $\mathbb{C}[rQ_0] = -\mathbb{C}[rQ_0]$. Since $rQ_0(q^{\frac{m}{2}} + 1) \equiv 0 \mod n$, one has $rQ_0q^{\frac{m}{2}} \equiv -rQ_0 \mod n$, and therefore $\mathbb{C}[rQ_0] = -\mathbb{C}[rQ_0]$. Then the result follows. □

Lemma 3: If $rQ_1 + 1 \leq i \leq rQ_0 - 1$, then $\mathbb{C}[i]$ has m elements.

Proof: Seeking a contradiction, suppose that there is a q-ary cyclotomic coset $\mathbb{C}[i]$ with m_i elements, where $1 \leq m_i \leq \frac{m}{2}$. Then $iq^{m_i} \equiv i \mod n$ and then $i(q^{m_i} - 1) \equiv 0 \mod n$ holds. Since $rQ_1 + 1 \leq i \leq rQ_0 - 1$ and $1 \leq m_i \leq \frac{m}{2}$,

one has

$$0 < i(q^{m_i} - 1) \leq (rQ_0 - 1)(q^{\frac{m}{2}} - 1) < n,$$

which is a contradiction. Therefore, $\mathbb{C}[i]$ has m elements, where $rQ_1 + 1 \leq i \leq rQ_0 - 1$. □

With these results in hand, we can construct quantum BCH codes when m is even.

Theorem 2: Let $q \geq 3$ be a prime power and n be an integer such that $\gcd(n, q) = 1$ and $ord_n(q) = m$ is even. Assume that $n = r\frac{q^m-1}{q-1}$, where $r > 1$. Then there exist quantum codes with parameters $[[n, n - 2rmq^{\frac{m}{2}-1} + 3m, d \geq rQ_0]]_q$.

Proof: Let $\mathbb{C}[rQ_1+1], \mathbb{C}[rQ_1+2], \cdots, \mathbb{C}[rQ_0-1]$ be the q-ary cyclotomic cosets according to Lemma 2. We assume that $\mathbb{C}[ar+x] = \mathbb{C}[br+y]$ such that $ar + x \neq br + y$, where $1 \leq x, y \leq r - 1$ and $Q_1 \leq a, b \leq Q_0 - 1$. It follows that

$$(ar + x)q^l \equiv br + y \mod n, \tag{1}$$

where $1 \leq l \leq m - 1$. One obtains

$$\begin{aligned} r(aq^l - b) &\equiv y - xq^l \mod n \\ \Rightarrow n(aq^l - b) &\equiv (y - xq^l)\frac{q^m - 1}{q - 1} \mod n \\ &\Rightarrow r \mid y - xq^l. \end{aligned}$$

On the other hand, one has $r \mid q^l - 1$ for $r \mid q - 1$. As a result, one has $r \mid (y - xq^l) + x(q^l - 1)$, i.e. $r \mid y - x$. Notice that $0 \leq |y - x| \leq r - 2$. If $y - x = 0$, we have $r(aq^l - b) + x(q^l - 1) \equiv 0 \mod n$. If $1 \leq l \leq \frac{m}{2}$, then

$$\begin{aligned} q - 1 &\leq r(aq^l - b) + x(q^l - 1) \\ &\leq n - r(Q_0 + Q_1 + 1) - q^{\frac{m}{2}} + 1 < n. \end{aligned}$$

We have a contradiction. If $\frac{m}{2} + 1 \leq l \leq m - 1$, then $1 \leq m - l \leq \frac{m}{2} - 1$. Since $q^m \equiv 1 \mod n$, one has $ar + x \equiv (br + y)q^{m-l} \mod n$ which is similar to the case where $1 \leq l \leq \frac{m}{2}$. Hence, the cosets given are mutually disjoint.

We know that $\gcd(n, q) = 1$. Let $C_0 = \langle \prod_i M^{(i)}(x) \rangle$ with the defining set Z_0, where $rQ_1 + 1 \leq i \leq rQ_0 - 1$. Suppose $Z_0 \cap Z_0^{-1} \neq \emptyset$. Then there exist a, b, x, and y such that

$$(ar + x)q^l \equiv -(br + y) \mod n, \tag{2}$$

where $1 \leq x, y \leq r - 1$ and $Q_1 \leq a, b \leq Q_0 - 1$ with $0 \leq l \leq m - 1$. Similarly, one obtains $r \mid x + y$. Notice that $2 \leq x + y \leq 2r - 2$. If $x + y = r$, we have $r(aq^l + b + 1) + x(q^l - 1) \equiv 0 \mod n$. If $0 \leq l \leq \frac{m}{2}$, then

$$0 < r(aq^l + b + 1) + x(q^l - 1) \leq n - (q^{\frac{m}{2}} - 1) - r.$$

It is clear that $r \mid x + y$ is not true. There is a similar processing method for $\frac{m}{2} + 1 \leq l \leq m - 1$. Consequently, $Z_0 \cap Z_0^{-1} = \emptyset$ and then C_0 is Euclidean dual-containing.

Since $1 < r < q$, one has $rQ_1 + 1 \leq q^{\frac{m-2}{2}} < rQ_0 - 1, \cdots, rQ_1 + 1 < Q_1 q \leq rQ_0 - 2$. Then the cyclotomic cosets given include $\mathbb{C}[1], \mathbb{C}[2], \cdots, \mathbb{C}[rQ_1]$. Thus all these cyclotomic cosets have $rQ_0 - 1$ consecutive integers. From the BCH bound and Lemma 3, C_0 is a code with dimension $k_0 = n - rmq^{\frac{m}{2}-1} + m$ and minimum distance $d_0 \geq rQ_0$.

Let $C_0' = \langle \prod_j M^{(j)}(x) \rangle$, where $rQ_1 + 1 \leq j \leq rQ_0 - 2$. Then $C_0' = [n, k_0' = n - rmq^{\frac{m}{2}-1} + 2m, d_0' \geq rQ_0 - 1]_q$, which is an enlargement of C_0 in view of $k_0' - k_0 = m \geq 2$. Since $r > 1$, we know that $\lceil \frac{q+1}{q}(rQ_0 - 1) \rceil \geq rQ_0$. Applying Steane's code construction to the codes C_0 and C_0', we obtain an $[[n, n - 2rmq^{\frac{m}{2}-1} + 3m, d \geq rQ_0]]_q$ quantum code. □

Several key points can already be seen in the proof of Theorem 2. Firstly, the cyclotomic cosets given ensure that cyclic code C_0 is Euclidean dual and C_0' is an enlargement of C_0. Secondly, these cyclotomic cosets are mutually disjoint. Thus, it is easy to compute the dimension of C_0 and C_0'. Finally, the cosets given lead to defining set containing most consecutive integers.

Examples 1: Consider $q = 3$, $r = 2$, $m = 4$, and $n = 80$. It is easy to compute the 3-ary cyclotomic cosets $\mathbb{C}[3] = \{3, 9, 27, 1\}$, $\mathbb{C}[4] = \{4, 12, 36, 28\}$, $\mathbb{C}[5] = \{5, 15, 45, 55\}$, $\mathbb{C}[6] = \{6, 18, 54, 2\}$, $\mathbb{C}[7] = \{7, 21, 63, 29\}$, and $\mathbb{C}[8] = \{8, 24, 72, 56\}$. It is a fact that $\mathbb{C}[8] = -\mathbb{C}[8]$. Let $C_0 = \langle \prod_{i=3}^{7} M^{(i)}(x) \rangle$ and $Z_0 = \bigcup_{i=3}^{7} \mathbb{C}[i]$. It is clear that the cosets are mutually disjoint and $Z_0 \cap Z_0^{-1} = \emptyset$. Since the cosets contain 7 consecutive integers, C_0 is Euclidean dual-containing and has parameters $[80, 60, d \geq 8]_3$. Let $C_0' = \langle \prod_{j=3}^{6} M^{(j)}(x) \rangle$. Similarly, C_0' has parameters $[80, 64, d \geq 7]_3$. Then we obtain an $[[80, 44, d \geq 8]]_3$ quantum BCH code from Theorem 2.

B. m IS ODD

It is rather remarkable that one has $n = r$ and $n \mid q - 1$ when $m = 1$. Since we consider only the case where $n > q$, we impose restrictions on m with $m > 1$. Let $Q_2 = \frac{q^{\frac{m-1}{2}}-1}{q-1}$ when m is odd.

Lemma 4: If $rQ_2 \leq i \leq rqQ_2 - 1$, then $\mathbb{C}[i]$ has m elements.

Proof: It's similar to the proof of Lemma 3. We omit it. □

Theorem 3: Let $q \geq 3$ be a prime power and n be an integer such that $\gcd(n, q) = 1$ and $ord_n(q) = m > 1$ is odd. Assume that $n = r\frac{q^m-1}{q-1}$, where $r > 1$. Then there exists an $[[n, n - 2mr(q^{\frac{m-1}{2}} - 1) + m, d \geq rqQ_2]]_q$ stabilizer code.

Proof: Each q-ary cyclotomic coset is given by $\mathbb{C}[rQ_2]$, $\mathbb{C}[rQ_2 + 1], \cdots$, and $\mathbb{C}[rqQ_2 - 1]$. Similar to the proof in Theorem 2, all these cosets are mutually disjoint.

Let C_0 and C_0' be cyclic codes generated by the product of the minimal polynomials

$$M^{(rQ_2)}(x)M^{(rQ_2+1)}(x) \cdots M^{(rqQ_2-1)}(x)$$

and

$$M^{(rQ_2)}(x)M^{(rQ_2+1)}(x) \cdots M^{(rqQ_2-2)}(x),$$

respectively. Proceeding similarly as in the proof of Theorem 2, we know that C_0 is Euclidean dual-containing. According to Lemma 4, the dimension of C_0 is $n - rm(q^{\frac{m-1}{2}} - 1)$. Since $1 < r < q$, it follows that $rQ_2 < q^{\frac{m-1}{2}} < rqQ_2 - 1, \cdots, rQ_2 < (rQ_2 - 1)q < rqQ_2 - 1$. The cyclotomic cosets given include $\mathbb{C}[1]$, $\mathbb{C}[2], \cdots, \mathbb{C}[rQ_2 - 1]$. Therefore, all these cyclotomic cosets have $rqQ_2 - 1$ consecutive integers. Then C_0 is a code with parameters $[n, k_0 = n - rm(q^{\frac{m-1}{2}} - 1), d_0 \geq rqQ_2]_q$. Meanwhile, C_0' is an enlargement of C with parameters $[n, k_0' = n - rm(q^{\frac{m-1}{2}} - 1) + m, d_0' \geq rqQ_2 - 1]_q$ in view of $k_0' - k_0 = m > 1$. Since $\lceil \frac{q+1}{q}(rQ_2 - 1) \rceil \geq rQ_2$, one has an $[[n, n - 2mr(q^{\frac{m-1}{2}} - 1) + m, d \geq rqQ_2]]_q$ quantum code. □

Examples 2: Let $q = 7$, $r = 3$, $m = 3$, and $n = 171$. One has $\mathbb{C}[3] = \{3, 21, 147\}$, $\mathbb{C}[4] = \{4, 28, 25\}$, $\cdots$, $\mathbb{C}[19] = \{19, 133, 76\}$, and $\mathbb{C}[20] = \{20, 140, 125\}$. Proceeding similarly, C_0 and C_0' have parameters $[171, 117, d \geq 21]_7$ and $[171, 120, d \geq 20]_7$. One can get quantum codes with parameters $[[171, 66, d \geq 21]]_7$.

IV. HERMITIAN CONSTRUCTIONS

Let $n = r\frac{q^{2m}-1}{q^2-1}$ and $m = ord_n(q^2)$. It follows that $r \mid q^2 - 1$. If $m = 1$, then $n = r$ and $n \mid q^2 - 1$. Since we consider only the case where $n > q^2$, an important assumption made in this section is $m > 1$.

A. m IS ODD

To begin with, let us consider the case where m is odd in this subsection. Suppose that $Q_3 = \frac{q^m-1}{q-1}$, $Q_4 = \frac{q^{m-2}-1}{q-1}$, and $t = \gcd(r, q + 1)$ for the sake of description.

Lemma 5: If i is an integer such that $\frac{r}{t}Q_3 \mid i$, then $\mathbb{C}[i] = -q\mathbb{C}[i]$.

Proof: It is enough to show $\mathbb{C}[\frac{r}{t}Q_3] = -q\mathbb{C}[\frac{r}{t}Q_3]$. In fact, one has $t \mid q + 1$ and $t \mid r$ because $t = \gcd(r, q + 1)$. It follows that $n \mid \frac{q+1}{t}qn$. Then we have $\frac{r}{t}Q_3 q(q^m + 1) \equiv 0 \mod n$. Namely, $\frac{r}{t}Q_3 q^{m+1} \equiv -q\frac{r}{t}Q_3 \mod n$ holds. Since m is odd, we have $\mathbb{C}[\frac{r}{t}Q_3] = -q\mathbb{C}[\frac{r}{t}Q_3]$. The claim follows. □

Lemma 6: Let i and j denote the indexes of cyclotomic cosets. If q is a power of odd prime and $i + j = \frac{r}{t}Q_3$, then

1) $\mathbb{C}[i] \neq -q\mathbb{C}[j]$ when t is even and $4 \nmid r$.
2) $\mathbb{C}[i] \neq -q\mathbb{C}[j]$ when $t \geq \frac{q+1}{2}$ is even and $4 \mid r$.
3) there are i and j such that $\mathbb{C}[i] = -q\mathbb{C}[j]$ when $1 \leq t < \frac{q+1}{2}$ is even and $4 \mid r$.
4) $\mathbb{C}[i] \neq -q\mathbb{C}[j]$ when t is odd such that $t > \frac{q+1}{4}$.
5) there are i and j such that $\mathbb{C}[i] = -q\mathbb{C}[j]$ when $t = \frac{q+1}{4}$ is odd and $r = \frac{q^2-1}{8}$.
6) $\mathbb{C}[i] \neq -q\mathbb{C}[j]$ when t is odd such that $t = \frac{q+1}{4}$ and $r \neq \frac{q^2-1}{8}$.
7) there are i and j such that $\mathbb{C}[i] = -q\mathbb{C}[j]$ when $1 \leq t < \frac{q+1}{4}$ is odd.

Proof: Seeking a contradiction, we assume that there are i and j such that $\mathbb{C}[i] = -q\mathbb{C}[j]$. Then one obtains

$$iq^{2l} \equiv -jq \mod n, \tag{3}$$

where $0 \leq 2l \leq 2(m - 1)$. One has $iq^{2l} + jq \equiv 0 \mod n$.

If $l = 0$, then $i + jq \equiv 0 \mod n$. Since $0 < i + jq \leq (\frac{r}{t}Q_3 - 1)q + 1 < n$, one has a contradiction. If $2 \leq 2l \leq m-1$, one obtains $iq^{2l-1} + j \equiv 0 \mod n$ for $\gcd(n, q) = 1$. It is clear that $0 < iq^{2l-1} + j \leq iq^{2l-1} + j \leq (\frac{r}{t}Q_3 - 1)q^{m-2} + 1 < n$. This case is not true. If $m + 3 \leq 2l \leq 2(m - 1)$, then $3 \leq 2m - 2l + 1 \leq m - 2$. We know that $q^{2m} \equiv 1 \mod n$. One has $i + jq^{2m-2l+1} \equiv 0 \mod n$, which is similar to the case where $2 \leq 2l \leq m - 1$. If $2l = m + 1$, we have $i + jq^m \equiv 0 \mod n$ and $j + iq^m \equiv 0 \mod n$. If $i = j$, one has

$$\begin{aligned}(q^m + 1)j \equiv 0 \mod n &\Rightarrow n \mid (q^m + 1)j \\ &\Rightarrow \frac{r}{t}Q_3 \mid j\frac{q+1}{t} \Rightarrow \frac{r}{t}Q_3 \mid j.\end{aligned}$$

It is not true since $i + j = \frac{r}{t}Q_3$. Without loss of generality, let $j > i$. Then one obtains

$$(i + j)(q^m + 1) \equiv 0 \mod n \Rightarrow \frac{r}{t}Q_3 \mid \frac{q+1}{t}(i + j).$$

Since $\gcd(\frac{r}{t}, \frac{q+1}{t}) = 1$ and $\gcd(Q_3, \frac{q+1}{t}) = 1$, it follows that $\frac{r}{t}Q_3 \mid i + j$. If $i + j = \frac{r}{t}Q_3$, one has $\frac{r}{2t}Q_3 < j \leq \frac{r}{t}Q_3 - 1$ and $\frac{r}{t}Q_3 + (q^m - 1)j \equiv 0 \mod n$. Namely, $\frac{r}{t} + (q - 1)j \equiv 0 \mod r\frac{q^m+1}{q+1}$. Since $\gcd(\frac{r}{t}, \frac{q+1}{t}) = 1$ and $r \mid q^2 - 1$, one obtains $\frac{r}{t} \mid q - 1$. Then $1 + j\frac{q-1}{r}t \equiv 0 \mod t\frac{q^m+1}{q+1}$ holds. Let $r = tb$ and $q - 1 = bd$. We have

$$1 + dj \equiv 0 \mod t\frac{q^m + 1}{q + 1}. \tag{4}$$

Suppose that $1 + dj = st\frac{q^m+1}{q+1}$.

1) Considering $4 \nmid r$ and $\gcd(q-1, q+1) = 2$, let $t = 2t_0$ and $r = 2t_0 b$ such that $\gcd(b, q+1) = 1$. It is clear that $\gcd(r, q-1) = 2b$ and then $2 \mid d$. Since $t\frac{q^m+1}{q+1} \mid 1 + dj$ and $t = 2t_0$, one obtains $2 \mid 1 + dj$. It follows that $2 \mid -dj + (1 + dj)$. Namely, $2 \mid 1$, which is a contradiction. Thus, when t is even and $4 \nmid r$, one has $\mathbb{C}[i] \neq -q\mathbb{C}[j]$.
2) We know $s \in (\frac{q+1}{2t}, \frac{q+1}{t} - 1]$. If $t \geq \frac{q+1}{2}$, it is clear that $\frac{q+1}{2t} \geq \frac{q+1}{t} - 1$. Thus, there exists no s such that $1 + dj = st\frac{q^m+1}{q+1}$. Then one obtains $\mathbb{C}[i] \neq -q\mathbb{C}[j]$ when $t \geq \frac{q+1}{2}$ is even and $4 \mid r$.
3) If $1 \leq t < \frac{q+1}{2}$ and $\gcd(s, d) = t_2 > 1$, it follows that $t_2 \mid s$ and $t_2 \mid d$. Since $s \mid 1 + dj$, one has $t_2 \mid 1 + dj$. Similarly, we know $t_2 \mid 1$, which is a contradiction. If $\gcd(s, d) = 1$, one has $j = \frac{r(stq^m+st-q-1)}{t(q^2-1)}$. If j is an integer, it follows that

$$\begin{aligned}&t(q^2 - 1) \mid r(stq^m + st - q - 1) \\ &\Rightarrow d(q + 1) \mid stq^m + st - q - 1 \\ &\Rightarrow d \mid stq\frac{q^{m-1} - 1}{q + 1} + st - 1.\end{aligned}$$

Since m is odd, then $q-1 \mid \frac{q^{m-1}-1}{q+1}$. Considering $d \mid q-1$, one has $d \mid st-1$. Namely, $q-1 \mid sr-b$. Hence, if $q-1 \mid sr-b$ and $\gcd(s,d)=1$, there are i and j such that $\mathbb{C}[i]=-q\mathbb{C}[j]$ when $1 \le t < \frac{q+1}{2}$ is even and $4 \mid r$.

4) If t is odd, then r and Q_3 both are odd. We know that
$$\frac{\frac{r}{t}Q_3+1}{2} \le j \le \frac{r}{t}Q_3-1$$
$$\Rightarrow \frac{q^m+1+d}{2} \le 1+dj \le q^m-d$$
$$\Rightarrow \frac{q+1}{2t}+1 \le s \le \frac{q+1}{t}-1.$$
Since $t > \frac{q+1}{4}$, we know $\frac{q+1}{t}-1 < \frac{q+1}{2t}+1$, which indicates that there exists no integer s. Thus, one has $\mathbb{C}[i] \ne -q\mathbb{C}[j]$ when $t > \frac{q+1}{4}$ is odd.

5) If $t=\frac{q+1}{4}$ is odd, then $\frac{q+1}{2t}+1=\frac{q+1}{t}-1=3$. One has $s=3$ and $j=\frac{3q^m-1}{8}$ when $r=\frac{q^2-1}{8}$. If $t=\frac{q+1}{4}$, it follows that $q^m+1=4t\Delta$, where $\Delta=\sum_{k=0}^{m-1}(-4t)^k$. Since t and Δ both are odd, then $j=\frac{3t\Delta-1}{2}$ is an integer. Consequently, there are i and j such that $\mathbb{C}[i]=-q\mathbb{C}[j]$ when $t=\frac{q+1}{4}$ is odd and $r=\frac{q^2-1}{8}$.

6) Since $\gcd(q+1,q-1)=2$, if t is odd, then r is odd too. One has $\gcd(b,q+1)=1$ and $d \ge 2$. If $t=\frac{q+1}{4}$, it is clear that $j=\frac{r(3q^m-1)}{4t(q-1)}$. If j is an integer, then $4t(q-1) \mid r(3q^m-1)$ and then $d \mid 3q^m-1$. Since $d \mid q-1$ and $q-1 \nmid q^m-1$, one can derive $d \mid 2$. If $d=2$, then $r=\frac{q^2-1}{8}$ contradicting the fact $r \ne \frac{q^2-1}{8}$. Hence, $\mathbb{C}[i] \ne -q\mathbb{C}[j]$ when $t=\frac{q+1}{4}$ is odd and $r \ne \frac{q^2-1}{8}$.

7) If t is odd such that $1 \le t < \frac{q+1}{4}$, one has $s \in [\frac{q+1}{2t}+1, \frac{q+1}{t}-1]$. According to the proof of 3), we know that if $\gcd(s,d)=1$ and $q-1 \mid sr-b$, there are i and j such that $\mathbb{C}[i]=-q\mathbb{C}[j]$ when $1 \le t < \frac{q+1}{4}$ is odd. □

If $q=2^e$, where e is an integer, then t is just odd since $r \mid q^2-1$. We have similar results in the following.

Lemma 7: Let i and j denote the indexes of cyclotomic cosets. If $q=2^e$ and $i+j=\frac{r}{t}Q_3$, where $e>1$ is an integer, then

1) $\mathbb{C}[i] \ne -q\mathbb{C}[j]$ when $t \ge \frac{q+1}{3}$ is odd.
2) there are i and j such that $\mathbb{C}[i]=-q\mathbb{C}[j]$ when $1 \le t < \frac{q+1}{3}$ is odd.

Proof: According to the proof of Lemma 6, we know $\frac{\frac{q+1}{t}+1}{2} \le s \le \frac{q+1}{t}-1$ since $\frac{\frac{r}{t}Q_3+1}{2} \le j \le \frac{r}{t}Q_3-1$.

If $t > \frac{q+1}{3}$, one has $\frac{\frac{q+1}{t}+1}{2} > \frac{q+1}{t}-1$. There exists no integer s such that $1+dj=st\frac{q^m+1}{q+1}$. If $t=\frac{q+1}{3}$, then $s=2$ and $j=r\frac{2q^m-1}{q^2-1}$. Let $r=\frac{q+1}{3}r_t$ such that $r_t \mid q-1$. One obtains $j=\frac{2q^m-1}{3(q-1)/r_t}$. If j is an integer, then $\frac{q-1}{r_t} \mid 2q^m-1$. Since $\frac{q-1}{r_t} \mid q^m-1$, one has $\frac{q-1}{r_t} \mid q^m$, which is a contradiction because of $\gcd(q-1,q^m)=1$. Therefore, $\mathbb{C}[i] \ne -q\mathbb{C}[j]$ when $t \ge \frac{q+1}{3}$ is odd.

If $1 \le t < \frac{q+1}{3}$, let $r=tb$ and $q-1=bd$. One obtains $q-1 \mid sr-b$ and $\gcd(s,d)=1$ from the proof Lemma 6-7). Thus there are i and j such that $\mathbb{C}[i]=-q\mathbb{C}[j]$ when $1 \le t < \frac{q+1}{3}$ is odd. □

Examples 3: When $q=5$, $r=8$, and $m=3$, one has $t=2$ and $\frac{r}{t}Q_3=124$. From Lemma 6-3), it is found that $\mathbb{C}[41]=-5\mathbb{C}[83]$. When $q=11$, $r=15$, and $m=5$, it is easy to work out that $t=3$ and $\frac{r}{t}Q_3=80525$. From Lemma 6-5), it follows that $\mathbb{C}[20131]=-11\mathbb{C}[60394]$. Similarly, when $q=47$, $r=69$, and $m=3$, it is clear that $t=3$ and $\frac{r}{t}Q_3=51911$. From Lemma 6-7), one has $\mathbb{C}[9733]=-47\mathbb{C}[42178]$, $\mathbb{C}[3244]=-47\mathbb{C}[48667]$, $\mathbb{C}[16222]=-47\mathbb{C}[35689]$, and $\mathbb{C}[22711]=-47\mathbb{C}[29200]$. When $q=2^8$, $m=3$, and $r=21$, then $t=3$, $s \in [86,170]$, and $511 \mid 21s-7$. When $s=122$ such that $\gcd(s,73)=1$, one has $\mathbb{C}[1311749]=-512\mathbb{C}[526850]$.

It should be pointed out that there is an implicit condition where $t \ge 2$ from Lemma 6-1) – Lemma 6-6) and Lemma 7-1). Let us consider $t \ge 2$ at first.

Theorem 4: Let $q \ge 3$ be a prime power and n be an integer such that $\gcd(n,q^2)=1$, where $m=ord_n(q^2)>1$ is odd. Assume that $n=r\frac{q^{2m}-1}{q^2-1}$. If t and r satisfy conditions in 1), 2), 4), or 6) of Lemma 6 or 1) of Lemma 7, then there exists an $[[n, n-2m\frac{r}{t}(Q_3-Q_4)+2m, d \ge \frac{r}{t}Q_3]]_q$ stabilizer code.

Proof: We next show that all the q^2-ary cyclotomic cosets given by $\mathbb{C}[\frac{r}{t}Q_4+1], \mathbb{C}[\frac{r}{t}Q_4+2], \cdots, \mathbb{C}[\frac{r}{t}Q_3-1]$ are mutually disjoint. Seeking a contradiction, we assume that $\mathbb{C}[i]=\mathbb{C}[j]$, where $\frac{r}{t}Q_4+1 \le i \ne j \le \frac{r}{t}Q_3-1$. One has
$$iq^{2l} \equiv j \mod n, \tag{5}$$
where $1 \le l \le m-1$. It is equivalent to $iq^{2l}-j \equiv 0 \mod n$.

It follows from $r \mid q^2-1$ that $\mathrm{lcm}(r,q+1) \le q^2-1$. Since $t=\gcd(r,q+1)$, we have $\frac{r}{t}(q+1) \le q^2-1$. If $1 \le l \le \frac{m-1}{2}$ and $t \ge 2$, one obtains
$$0 < q^2+1-\frac{r}{t}(q+1) \le iq^{2l}-j \le \frac{r}{t}(Q_3q^{m-1}-Q_4)-q^{m-1}-1 < n,$$
which is a contradiction. If $\frac{m+1}{2} \le l \le m-1$, one has $1 \le m-l \le \frac{m-1}{2}$. We can infer from $q^{2m} \equiv 1 \mod n$ that $jq^{2m-2l}-i \equiv 0 \mod n$. It is similar to the case where $1 \le l \le \frac{m-1}{2}$. Therefore, all these q^2-ary cyclotomic cosets are mutually disjoint.

Let $C_0=\langle \prod_i M^{(i)}(x) \rangle$ and $Z_0=\bigcup_i \mathbb{C}[i]$, where $\frac{r}{t}Q_4+1 \le i \le \frac{r}{t}Q_3-1$. From the proof of Lemma 6, we know that $Z_0 \cap Z_0^{-q}=\emptyset$. It implies that C_0 is Hermitian dual-containing.

Suppose there is a q-ary cyclotomic coset with m_i elements, where $m_i \mid m$ and $1 \le m_i \le \frac{m}{3}$ because m is odd. Then $iq^{2m_i} \equiv i \mod n$. Namely, $n \mid i(q^{2m_i}-1)$. Since $\frac{r}{t}Q_4+1 \le i \le \frac{r}{t}Q_3-1$, it follows that $0 < i(q^{2m_i}-1) < n$. Hence, all the cyclotomic cosets given have m elements.

If $\frac{r}{t}=1$, one has $\mathbb{C}[2]=\mathbb{C}[2q^{m-3}]$. If $\frac{r}{t}>1$, one obtains $\mathbb{C}[2]=\mathbb{C}[2q^{m-1}]$. Analogously, we know that $\mathbb{C}[1]=\mathbb{C}[q^{m-1}], \cdots, \mathbb{C}[\frac{r}{t}Q_4]=\mathbb{C}[\frac{r}{t}q^2Q_4]$ also hold. The cyclotomic cosets given by $\mathbb{C}[i]$ with $\frac{r}{t}Q_4+1 \le i \le \frac{r}{t}Q_3-1$

include $\mathbb{C}[1]$, $\mathbb{C}[2]$, $\cdots$, $\mathbb{C}[\frac{r}{t}Q_4]$. Hence, these cyclotomic cosets contain $\frac{r}{t}Q_3 - 1$ consecutive integers. Then C_0 has parameters $[n, n - m\frac{r}{t}(Q_3 - Q_4) + m, d_0 \geq \frac{r}{t}Q_3]_{q^2}$. Applying the Hermitian construction to C_0, one can construct an $[[n, n - 2m\frac{r}{t}(Q_3 - Q_4) + 2m, d \geq \frac{r}{t}Q_3]]_q$ code. □

Examples 4: Theorem 4 has variants as follows: $q = 5$, $r = 2$, $m = 3$, and $n = 1302$. Then one has $Q_3 = 31$, $Q_4 = 1$, and $t = 2$. It is easy to work out each 25-ary cyclotomic coset $\mathbb{C}[i]$ for $2 \leq i \leq 31$. It is clear that $\mathbb{C}[31] = -5\mathbb{C}[31]$ since $\mathbb{C}[31] = \{31, 775, 1147\}$. The cosets are given by $\mathbb{C}[2] = \{2, 50, 1250\}$, $\mathbb{C}[3] = \{3, 75, 573\}$, $\cdots$, $\mathbb{C}[30] = \{30, 750, 522\}$. Suppose that $C_0 = \langle \prod_i M^{(i)}(x) \rangle$ and $Z_0 = \bigcup_i \mathbb{C}[i]$, where $i \in \{2, 3, \cdots, 30\}$. It is a fact that cosets are mutually disjoint and $Z_0 \cap Z_0^{-5} = \emptyset$. Then C_0 is Hermitian dual-containing and has parameters $[1302, 1215, d \geq 31]_{25}$ since cosets contain 30 consecutive integers. Applying the Hermitian construction, we have an $[[1302, 1128, d \geq 31]]_5$ quantum code.

The q^2-ary cyclotomic cosets given in the proof of Theorem 4 are optimal from Lemma 6 and Lemma 7. Not only do cosets given make sure that C_0 is Hermitian dual-containing but also it is convenient to compute the dimension of C_0. In particular, the number of consecutive integers reaches the maximum.

From 3), 5) or 7) of Lemma 6 or 2) of Lemma 7 , we know that there are i and j such that $\mathbb{C}[i] = -q\mathbb{C}[j]$ when t and r meet certain conditions. Another issue one might raise is how to design quantum BCH codes for these cases. The following lemma offers a desirable solution to choose cosets in order to facilitate the construction of quantum BCH codes.

Lemma 8: Suppose $\alpha = q^m - \beta t\frac{q^m+1}{q+1}$ such that $0 \leq \beta t \leq \frac{q+1}{2}$, then $\mathbb{C}[\alpha] = -q\mathbb{C}[q^m - \alpha - 1]$.

Proof: Note that $r \mid q^2 - 1$ and $t = \gcd(r, q + 1)$. One has $\frac{r}{t} \mid \frac{q+1}{t}(q - 1)$ and $\gcd(\frac{r}{t}, \frac{q+1}{t}) = 1$. Then $\frac{r}{t} \mid q - 1$ and then $r \mid (q - 1)t$. Since $\beta q(q - 1)t\frac{q^{2m}-1}{q^2-1} \equiv 0 \mod n$ and $q(q^{2m} - 1) \equiv 0 \mod n$, we have $\beta tq(q^m - 1)\frac{q^m+1}{q+1} \equiv 0 \mod n$ and $(q^m - \beta t\frac{q^m+1}{q+1})q^{m+1} \equiv -q(q^m - 1 - q^m + \beta t\frac{q^m+1}{q+1}) \mod n$. Thus, $\alpha q^{m+1} \equiv -q(q^m - 1 - \alpha) \mod n$ holds. Since m is odd, one has $\mathbb{C}[\alpha] = -q\mathbb{C}[q^m - 1 - \alpha]$. □

Let $\alpha' = q^m - \lfloor\frac{q+1}{2t}\rfloor t\frac{q^m+1}{q+1}$. We have Theorem 5 as follows.

Theorem 5: Let $q \geq 3$ be a prime power and n be an integer such that $\gcd(n, q^2) = 1$ and $m = ord_n(q^2) > 1$ is odd. Assume that $n = r\frac{q^{2m}-1}{q^2-1}$, where $r > q + 1$. If t and r satisfy conditions in 3), 5) or 7) of Lemma 6 or 2) of Lemma 7 and $\alpha' \leq \frac{r}{t}Q_3$, then there exist quantum codes with parameters $[[n, n - 2m(\alpha' - \lceil\frac{\alpha'}{q^2}\rceil), d \geq \alpha']]_q$.

Proof: We choose $\mathbb{C}[\lceil\frac{\alpha'}{q^2}\rceil]$, $\mathbb{C}[\lceil\frac{\alpha'}{q^2}\rceil + 1]$, $\cdots$, $\mathbb{C}[\alpha' - 1]$ as the q^2-ary cyclotomic cosets. Suppose $\mathbb{C}[i] = \mathbb{C}[j]$, where $\lceil\frac{\alpha'}{q^2}\rceil \leq i \neq j \leq \alpha' - 1$. It follows that $iq^{2l} \equiv j \mod n$, where $1 \leq l \leq m - 1$. Namely, $iq^{2l} - j \equiv 0 \mod n$. If $1 \leq l \leq \frac{m-1}{2}$ and $r > q + 1$, one has

$$0 < \lceil\frac{\alpha'}{q^2}\rceil q^2 - (\alpha' - 1) \leq iq^{2l} - j$$
$$\leq (\alpha' - 1)q^{m-1} - \lceil\frac{\alpha'}{q^2}\rceil < n,$$

which is a contradiction. If $\frac{m+1}{2} \leq l \leq m - 1$, then $1 \leq m - l \leq \frac{m-1}{2}$. We can infer from $q^{2m} \equiv 1 \mod n$ that $i \equiv jq^{2m-2l} \mod n$. It is similar to the case where $1 \leq l \leq \frac{m-1}{2}$. Thus, all these cosets are mutually disjoint.

Let $C_0 = \langle \prod_i M^{(i)}(x) \rangle$, where $\lceil\frac{\alpha'}{q^2}\rceil \leq i \leq \alpha' - 1$. Proceeding similarly as in the proof of Theorem 4, we can show that C_0 is Hermitian dual-containing and compute its dimension as well as the minimum distance. □

In the proof of Theorem 5, the condition $r > q + 1$ is attributed to mutually disjoint cosets. It has no effect on Hermitian duality. The following Theorem can be applied to show that the q^2-ary cyclotomic cosets given in the proof of Theorem 6 are tight.

Theorem 6: If the q^2-ary cyclotomic cosets are given by $\mathbb{C}[\lceil\frac{\alpha'}{q^2}\rceil - 1]$, $\mathbb{C}[\lceil\frac{\alpha'}{q^2}\rceil]$, $\cdots$, and $\mathbb{C}[\alpha' - 1]$, then there exist i and j such that $\mathbb{C}[i] = \mathbb{C}[j]$, where $\lceil\frac{\alpha'}{q^2}\rceil - 1 \leq i, j \leq \alpha' - 1$.

Proof: If $\lceil\frac{\alpha'}{q^2}\rceil$ is an integer, let $i = \frac{\alpha'}{q^2} - 1$ and $j = iq^2$. Since $\frac{\alpha'}{q^2} - 1 \leq iq^2 \leq \alpha' - 1$, it is obvious that $\mathbb{C}[i] = \mathbb{C}[j]$. If $\lceil\frac{\alpha'}{q^2}\rceil$ is not an integer, let $i = \lceil\frac{\alpha'}{q^2}\rceil - 1 = \lfloor\frac{\alpha'}{q^2}\rfloor$ and $j = iq^2$. Because $\lceil\frac{\alpha'}{q^2}\rceil - 1 \leq iq^2 < \alpha'$, it is clear that $\mathbb{C}[i] = \mathbb{C}[j]$. The result follows. □

Examples 5: When $q = 5$, $r = 8$, and $m = 3$, we know that $n = 5208$, $t = 2$, and $\frac{r}{t}Q_3 = 124$. There are i and j such that $\mathbb{C}[i] = -5\mathbb{C}[j]$ from Lemma 6-3). One has $\alpha' = 83$ and $\mathbb{C}[83] = -5\mathbb{C}[41]$ according to Lemma 8. Let $\mathbb{C}[4]$, $\mathbb{C}[5]$, $\cdots$, $\mathbb{C}[82]$ be the 25-ary cyclotomic cosets to generate cyclic code C_0. The defining set of C_0 is $Z_0 = \bigcup_{i=4}^{82} \mathbb{C}[i]$. Since $Z_0 \cap Z_0^{-5} = \emptyset$, then C_0 is Hermitian dual-containing with parameters $[5208, 4971, d_0 \geq 83]_{25}$. One obtains an $[[5208, 4734, d \geq 83]]_5$ quantum BCH code. If we select $\mathbb{C}[3]$, $\mathbb{C}[4]$, $\cdots$, $\mathbb{C}[82]$ as the 25-ary cyclotomic cosets to generate cyclic code C_0, then there are cosets mutually joint. For example, we know that $\mathbb{C}[3] = \mathbb{C}[75]$.

Finally, let us consider $t = 1$. It is a fact that $r \mid q - 1$. In addition, one has $\gcd(q - 1, q + 1) = 2$ when q is an odd prime power. We know that r and Q_3 are both odd.

Lemma 9: Suppose $\zeta = rQ_3 - r\frac{q^m-q}{q^2-1} - \eta\frac{q^m+1}{q+1}$, where $0 \leq \eta \leq \frac{r-1}{2}$, then $\mathbb{C}[\zeta] = -q\mathbb{C}[rQ_3 - \zeta]$.

Proof: It is a fact that $-q(rQ_3 - \zeta) = r\frac{q^2-q^{m+1}}{q^2-1} - \eta\frac{q^{m+1}+q}{q+1}$. Thus, we have $\zeta q^{m+1} \equiv r\frac{q^2-q^{m+1}}{q^2-1} - \eta\frac{q+q^{m+1}}{q+1} \equiv -q(rQ_3 - \zeta) \mod n$. Since m is odd, then $\mathbb{C}[\zeta] = -q\mathbb{C}[rQ_3 - \zeta]$ holds. If we consider $\zeta \geq rQ_3 - \zeta$, one has $0 \leq \eta \leq \frac{r-1}{2}$ because r is odd. □

Theorem 7: Let $q \geq 3$ be a prime power and n be an integer such that $\gcd(n, q^2) = 1$, $\gcd(r, q + 1) = 1$, and

$m = ord_n(q) > 1$ is odd. Assume that $n = r\frac{q^{2m}-1}{q^2-1}$ and $\zeta' = r\frac{q^{m+1}-1}{q^2-1} - \frac{r-1}{2}\frac{q^m+1}{q+1}$. Then there exist quantum codes with parameters $[[n, n-2m(\zeta'-\lceil\frac{\zeta'}{q^2}\rceil), d \geq \alpha']]_q$.

Proof: Each q^2-ary cyclotomic coset is given by $\mathbb{C}[\lceil\frac{\zeta'}{q^2}\rceil]$, $\mathbb{C}[\lceil\frac{\zeta'}{q^2}\rceil+1]$, $\cdots$, $\mathbb{C}[\zeta'-1]$. Similar to the proof of Theorem 4, these q^2-ary cyclotomic cosets are mutually disjoint.

Let $C_0 = \langle\prod_i M^{(i)}(x)\rangle$, where $\lceil\frac{\zeta'}{q^2}\rceil \leq i \leq \zeta'-1$. Assume that $\mathbb{C}[i] = -q\mathbb{C}[j]$, where $\lceil\frac{\zeta'}{q^2}\rceil \leq i,j \leq \zeta'-1$. One has $iq^{2l} \equiv -qj \mod n$, where $0 \leq 2l \leq 2(m-1)$. We only consider $l = \frac{m+1}{2}$ since the other cases are similar to the proof of Theorem 4. If $l = \frac{m+1}{2}$, one has $i + jq^m \equiv 0 \mod n$ and $j+iq^m \equiv 0 \mod n$. Then $(i+j)(q^m+1) \equiv 0 \mod n$. We have $rQ_3 \mid i+j$ in that $\gcd(r, q+1) = 1$ and $\gcd(Q_3, q+1) = 1$. If $i = j$, then $i(q^m+1) \equiv 0 \mod n$. One has $rQ_3 \mid i$ which is not true for $i \leq \zeta'-1 \leq rQ_3$. Without loss of generality, we assume that $i < j$. Since $i+j < 2j < 2rQ_3$, one has $i+j = rQ_3$ and $\frac{rQ_3+1}{2} \leq j \leq \zeta'-1$. It follows that

$$\begin{aligned} & j + (rQ_3 - j)q^m \equiv 0 \mod n \\ \Rightarrow\ & rq^m - j(q-1) \equiv 0 \mod r\frac{q^m+1}{q+1} \\ \Rightarrow\ & j(q-1) \equiv r\frac{q^m-q}{q+1} \mod r\frac{q^m+1}{q+1}. \end{aligned}$$

Let $q-1 = t_0 r$. Then $t_0 j \equiv \frac{q^m-q}{q+1} \mod \frac{q^m+1}{q+1}$. Since $\gcd(\frac{q^m+1}{q+1}, q-1) = 1$ and $t_0 \mid q-1$, one obtains

$$j \equiv \frac{q^m-q}{t_0(q+1)} \mod \frac{q^m+1}{q+1} \Rightarrow \frac{q^m+1}{q+1} \mid j - \frac{q^m-q}{t_0(q+1)}.$$

Let $j - \frac{q^m-q}{t_0(q+1)} = s\frac{q^m+1}{q+1}$. Then we know that $s \in (\frac{r}{2}, \frac{r+1}{2})$, which is a contradiction. The way of determining the dimension and the minimum distance is similar to the proof of Theorem 4. □

Similar to Theorem 6, we can show that the q^2-ary cyclotomic cosets given are tight. Namely, when q^2-ary cyclotomic cosets are given by $\mathbb{C}[\lceil\frac{\zeta'}{q^2}\rceil-1]$, $\mathbb{C}[\lceil\frac{\zeta'}{q^2}\rceil]$, $\cdots$, and $\mathbb{C}[\zeta'-1]$, there are i and j such that $\mathbb{C}[i] = \mathbb{C}[j]$.

Examples 6: Let $q = 4$, $r = 3$, and $m = 3$. It follows that $n = 819$ and $Q_3 = 21$. One has $\zeta' = 38$ and $\mathbb{C}[38] = -4\mathbb{C}[25]$ according to Lemma 9. We choose $\mathbb{C}[3]$, $\mathbb{C}[4]$, $\cdots$, $\mathbb{C}[37]$ as the 16-ary cyclotomic cosets to generate the cyclic code C_0. The defining set of C_0 is $Z_0 = \bigcup_{i=3}^{37}\mathbb{C}[i]$. Since $Z_0 \cap Z_0^{-4} = \emptyset$, then C_0 is Hermitian dual-containing with parameters $[819, 714, d \geq 38]_{16}$. One has an $[[819, 609, d \geq 38]]_4$ quantum BCH code. If we select $\mathbb{C}[2]$, $\mathbb{C}[3]$, $\cdots$, $\mathbb{C}[37]$ as the 16-ary cyclotomic cosets to generate cyclic code C_0, then $\mathbb{C}[2] = \mathbb{C}[32]$. That is to say that cosets given in this way are mutually joint. It shows that the cyclotomic cosets selected by Theorem 7 are tight.

B. m IS EVEN

We assume that $Q_5 = \frac{q^m-1}{q^2-1}$ when $m = ord_n(q^2)$ is even. One has the similar results in the following.

Lemma 10: If λ is an integer such that $0 \leq \lambda < r$, then $\mathbb{C}[rqQ_5 - \lambda] = -q\mathbb{C}[rQ_5 + \lambda q^{m-1}]$.

Proof: Notice that $(rqQ_5 - \lambda)q^m \equiv -r\frac{q^{m+1}-q}{q^2-1} - \lambda q^m \equiv -q(rQ_5+\lambda q^{m-1}) \mod n$. Since m is even, we have $\mathbb{C}[rqQ_5 - \lambda] = -q\mathbb{C}[rQ_5 + \lambda q^{m-1}]$. If we consider $rQ_5 + \lambda q^{m-1} \leq rqQ_5 - \lambda$, it is clear that $\lambda < r$. Especially, $\mathbb{C}[rqQ_5] = -q\mathbb{C}[rQ_5]$ when $\lambda = 0$. □

Applied Lemma 10, it is convenient to select the q^2-ary cyclotomic cosets. Hence, we obtain the following result.

Theorem 8: Let $q \geq 3$ be a prime power and n be an integer such that $\gcd(n, q^2) = 1$ and $m = ord_n(q^2)$ is even. Assume that $n = r\frac{q^{2m}-1}{q^2-1}$. Then there exists an $[[n, k \geq n - 2mr(q^{m-1}-1), d \geq rqQ_5 - r + 1]]_q$ quantum code.

Proof: Let $C_0 = \langle\prod_i M^{(i)}(x)\rangle$ and $Z_0 = \bigcup_i \mathbb{C}[i]$, where $r\frac{Q_5-1}{q}+1 \leq i \leq rqQ_5 - r$. Similar to the proof of Theorem 4, we know that C_0 is Hermitian dual-containing. The number of disjoint cyclotomic cosets is smaller than or equal to $r(q^{m-1}-1)$. In addition, each q^2-ary cyclotomic coset has at most m elements. Hence, one has $C = [n, k_0 \geq n - mr(q^{m-1}-1), d_0 \geq rqQ_5 - r + 1]_{q^2}$. We have an $[[n, k \geq n - 2mr(q^{m-1}-1), d \geq rqQ_5 - r + 1]]_q$ code. □

Although Theorem 8 does not ensure that each q^2-ary cyclotomic coset is mutually disjoint, its minimum distance is comparatively good when we consider the random error correcting capacity.

For example, one has $n = 130208$ and $Q_5 = 26$, when $q = 5$, $r = 8$, and $m = 4$. If we choose $\mathbb{C}[41]$, $\cdots$, $\mathbb{C}[1032]$ as the 25-ary cyclotomic cosets according to Theorem 8, it is easy to find that designed cyclic code C_0 is Hermitian dual-containing. However, there are cosets mutually joint such as $\mathbb{C}[209] = \mathbb{C}[417]$.

If we wish to compute the dimension of C_0 accurately, the result in Theorem 8 can be strengthened under some restrictions.

Theorem 9: Let $q \geq 3$ be a prime power and n be an integer such that $\gcd(n, q^2) = 1$ and $m = ord_n(q^2)$ is even. Assume that $n = r\frac{q^{2m}-1}{q^2-1}$, where $1 \leq r \leq \frac{q+1}{2}$. Then there exist an $[[n, n-2rm(q^{m-1}-q^{m-2}), d \geq r\frac{q^m-1}{q+1}+1]]_q$ quantum code.

Proof: Let $\mathbb{C}[i]$ be the q^2-ary cyclotomic coset to generate C_0, where $r\frac{q^{m-2}-1}{q+1} + 1 \leq i \leq r\frac{q^m-1}{q+1}$. Since selective cosets belong to the cosets given in the proof of Theorem 8. Hence, C_0 is Hermitian dual-containing.

Let us show that the cosets given are mutually disjoint. In fact, if $\mathbb{C}[i] = \mathbb{C}[j]$, it follows that $iq^{2l} \equiv j \mod n$, where $r\frac{q^{m-2}-1}{q+1} + 1 \leq i \neq j \leq r\frac{q^m-1}{q+1}$ and $1 \leq l \leq m-1$. It is equivalent to $iq^{2l} - j \equiv 0 \mod n$. If $1 \leq l \leq \frac{m-2}{2}$ and $1 \leq r \leq \frac{q+1}{2}$, one has $0 < q^2 - r(q-1) \leq iq^{2l} - j \leq r\frac{q^{2m-2}-2q^{m-2}+1}{q+1} - 1 < n$. If $\frac{m+2}{2} \leq l \leq m-1$, we have $1 \leq m-l \leq \frac{m-2}{2}$. It follows from $q^{2m} \equiv 1 \mod n$

that $i \equiv jq^{2m-2l} \mod n$, which is similar to the case where $1 \le l \le \frac{m-2}{2}$. Let us concentrate on the case where $l = \frac{m}{2}$. Then one has

$$\begin{aligned} iq^m &\equiv j \mod n \\ jq^m &\equiv i \mod n \end{aligned} \Rightarrow (i+j)(q^m-1) \equiv 0 \mod n$$

$$\Rightarrow q^m + 1 \mid (i+j)\frac{q^2-1}{r}.$$

Since $1 \le r \le \frac{q+1}{2}$ and $r\frac{q^{m-2}-1}{q+1} + 1 \le i \ne j \le r\frac{q^m-1}{q+1}$, it is clear that $i + j \le 2r\frac{q^m-1}{q+1} - 1 \le q^m - 2$. When $q \ne 2^e$, where e is an integer, one has $\gcd(q^m+1, q^2-1) = 2$. If $\gcd(q^m + 1, \frac{q^2-1}{r}) = 1$, we know that $q^m + 1 \mid i+j$ contradicting the fact $i+j \le q^m-2$. If $\gcd(q^m+1, \frac{q^2-1}{r}) = 2$, then $\gcd(\frac{q^m+1}{2}, \frac{q^2-1}{2r}) = 1$ and then $\frac{q^m+1}{2} \mid i+j$. If $i + j = \frac{q^m+1}{2}$, one obtains

$$\begin{aligned} \frac{q^m+1}{2} &\equiv j(q^m+1) \mod n \\ \Rightarrow q^m + 1 &\equiv 2j(q^m+1) \mod 2n \\ \Rightarrow 2j - 1 &\equiv 0 \mod 2r\frac{q^m-1}{q^2-1}. \end{aligned}$$

It is clear that we have a contradiction, because $2j-1$ is odd and $2\frac{q^m-1}{q-1}$ is even. When $q = 2^e$, where e is an integer, one has $\gcd(q^m + 1, q^2 - 1) = 1$, which is similar to above case where $\gcd(q^m + 1, \frac{q^2-1}{r}) = 1$. In a word, the cyclotomic cosets given by $\mathbb{C}[i]$, where $r\frac{q^{m-2}-1}{q+1} + 1 \le i \le r\frac{q^m-1}{q+1}$ are mutually disjoint.

Suppose the q^2-ary cyclotomic coset $\mathbb{C}[i]$ has m_i elements, where $m_i \mid m$ and $1 \le m_i \le \frac{m}{2}$, then $iq^{2m_i} \equiv i \mod n$. If $1 \le m_i \le \frac{m}{2} - 1$, the maximum of $iq^{2m_i} - i$ is smaller than n. If $m_i = \frac{m}{2}$, one has $q^m + 1 \mid i\frac{q^2-1}{r}$ because $n \mid i(q^{2m_i} - 1)$. According to the proof above, we know that this is not true. Then each q^2-ary cyclotomic coset given has m elements.

Since $\mathbb{C}[1] = \mathbb{C}[q^{m-2}]$, $\mathbb{C}[2] = \mathbb{C}[2q^{m-2}]$, $\cdots$, $\mathbb{C}[r\frac{q^{m-2}-1}{q+1}] = \mathbb{C}[r\frac{q^m-q^2}{q+1}]$, the cyclotomic cosets given contain $r\frac{q^m-1}{q+1}$ consecutive integers. Therefore, C_0 is a cyclic code with parameters $[n, n - rm(q^{m-1} - q^{m-2}), d_0 \ge r\frac{q^m-1}{q+1} + 1]_{q^2}$. One obtains an $[[n, n - 2rm(q^{m-1} - q^{m-2}), d \ge r\frac{q^m-1}{q+1} + 1]]_q$ code. □

Examples 7: Taking $q = 3$, $m = 4$, and $r = 2$ into consideration, it is easy to compute $n = 1640$ and $Q_5 = 10$. If one choose $\mathbb{C}[5], \mathbb{C}[6], \cdots, \mathbb{C}[40]$ as the 9-ary cyclotomic cosets to design cyclic code C_0, its defining set is $Z_0 = \bigcup_{i=5}^{40} \mathbb{C}[i]$. It' clear that $Z_0 \cap Z_0^{-3} = \emptyset$. Meanwhile, all these cosets are mutually disjoint and contain 40 consecutive integers. Therefore, C_0 is Hermitian dual-containing with parameters $[1640, 1496, d \ge 41]_9$. Applying Hermitian construction, one has an $[[1640, 1352, d \ge 41]]_3$ quantum BCH code.

V. CODE COMPARISONS

We compare the parameters of quantum BCH codes in our schemes with the ones available in the literature as follows.

Steane constructed quantum BCH codes with $n = 2^m - 1$ in [7]. It is a special case for $q = 2$. In this paper, we generalize to $q \ge 3$. Quantum BCH codes for $n = \frac{q^m-1}{q-1}$ have been studied, where q is a power of odd prime number [6]. We extend its results to the case where $r > 1$. In particular, q is an arbitrary prime power in our schemes.

Concerning Steane's construction, quantum BCH codes have parameters $[[n, n - 2m\lceil(\delta-1)(1-1/q)\rceil, d \ge \delta]]_q$ with $2 \le \delta \le r\frac{q^{\frac{m}{2}}-1}{q-1}$ when m is even in [2]. It is similar to the case in Theorem 2. However, the dimension of quantum BCH codes in our scheme is superior to the result in [2]. Similarly, when m is odd, one has $2 \le \delta \le r\frac{q^{\frac{m+1}{2}}-q}{q-1} + \frac{r}{q-1}$ in [2]. Suppose that we only consider nonprimitive BCH codes, it follows that $2 \le \delta \le r\frac{q^{\frac{m+1}{2}}-q}{q-1}$. This is similar to the case in Theorem 3. Whereas the dimension of quantum BCH codes in our scheme is larger than the dimension in [2]. For example, we can construct $[[312, 244, d \ge 12]]_5$ quantum codes with $r = 2$ and $m = 4$ while one has $[[312, 240, d \ge 12]]_5$ in [2]. Focusing on Hermitian construction, [2] constructed quantum BCH codes with $[[n, n - 2m\lceil(\delta-1)(1-1/q^2)\rceil, d \ge \delta]]_q$ where $2 \le \delta \le \lfloor r\frac{q^m-1}{q^2-1}\rfloor$ for $n = r\frac{q^{2m}-1}{q^2-1}$. It is clear that $\lfloor r\frac{q^m-1}{q^2-1}\rfloor \le \frac{r}{t}\frac{q^m-1}{q-1}$ when m is odd and $r\frac{q^m-1}{q^2-1} < r\frac{q^m-1}{q+1} + 1$ when m is even, respectively. Namely, the new codes in our schemes have better lower bound for the minimum distance than the ones in [2]. Quantum BCH codes with parameters $[[1953, 1869, d \ge 15]]_5$ can be obtained in [2]. In our scheme, one has an $[[1953, 1779, d \ge 31]]_5$ code. Table 1 and Table 2 show above results in a concrete way.

TABLE 1. Codes comparison for $n = r\frac{q^m-1}{q-1}$.

New codes	Steane's codes in [2]
$[[80, 44, d \ge 8]]_3$	$[[80, 40, d \ge 8]]_3$
$[[312, 244, d \ge 12]]_5$	$[[312, 240, d \ge 12]]_5$
$[[364, 175, d \ge 36]]_9$	$[[364, 172, d \ge 36]]_9$
$[[728, 530, d \ge 26]]_3$	$[[728, 524, d \ge 26]]_3$

TABLE 2. Codes comparison for $n = r\frac{q^{2m}-1}{q^2-1}$.

New codes	Hermitian codes in [2]
$[[182, 116, d \ge 13]]_3$	$[[182, 152, d \ge 6]]_3$
$[[1302, 1128, d \ge 31]]_5$	$[[1302, 1248, d \ge 10]]_5$
$[[1640, 1352, d \ge 41]]_3$	$[[1640, 1504, d \ge 20]]_3$
$[[1953, 1779, d \ge 31]]_5$	$[[1953, 1869, d \ge 15]]_5$

G. G. La Guardia proposed three constructions to generate primitive quantum BCH codes in [13]. The first two ones are derived from Hermitian's constructions with $r = q^2 - 1$. In terms of lower bound for the minimum distance, quantum BCH codes have $d \ge q^2$ when $m = ord_n(q^2) = 2$ and $d \ge 2q^2 + 2$ when $m = ord_n(q^2) \ge 3$ and $q \ge 4$ in [13]. From Theorem 4 and Theorem 8, one obtains $d \ge q^m - 1$

when $m = ord_n(q^2) > 1$ is odd and $d \geq q^{m+1} - q^2 - q + 2$ when $m = ord_n(q^2)$ is even, respectively. The third one is obtained from Steane's constructions when $r = q - 1$ with parameters $[[n = q^m - 1, n - m(4q - 5) - 2, d \geq 2q + 2]]_q$ for $q \geq 4$ and $m \geq 3$. We can construct $[[n = q^m - 1, n - 2m(q^{m/2} - q^{m/2-1}) + 3m, d \geq q^{m/2} - 1]]_q$ quantum BCH code when m is even from Theorem 2 and $[[n = q^m - 1, n-2m(q^{(m+1)/2}-q^{(m-1)/2}-q)-m, d \geq q^{(m+1)/2}-q]]_q$ when $m > 1$ is odd from Theorem 3. From Table 3 and Table 4, we can see that the lower bound for the minimum distance in our schemes are better than the results in [13].

TABLE 3. Codes comparison for $n = q^{2m} - 1$.

New codes	Hermitian codes in [13]
$[[80, 22, d \geq 17]]_3$	$[[80, 50, d \geq 9]]_3$
$[[255, 91, d \geq 46]]_4$	$[[255, 197, d \geq 16]]_4$
$[[624, 270, d \geq 97]]_5$	$[[624, 530, d \geq 25]]_5$
$[[4095, 3741, d \geq 63]]_4$	$[[4095, 3913, d \geq 34]]_4$

TABLE 4. Codes comparison for $n = q^m - 1$.

New codes	Steane's codes in [13]
$[[124, 31, d \geq 20]]_5$	$[[124, 77, d \geq 12]]_5$
$[[255, 171, d \geq 15]]_4$	$[[255, 209, d \geq 10]]_4$
$[[342, 129, d \geq 42]]_7$	$[[342, 271, d \geq 16]]_7$
$[[624, 476, d \geq 24]]_5$	$[[624, 562, d \geq 12]]_5$

Afterwards, G. G. La Guardia designed quantum BCH codes with $m = 2$ in [8]. When we consider Steane's construction, one has $n = r'(q - 1)$ in [8] and $n = r(q + 1)$ in this paper. We can see that the results in our constructions are comparable to those in [8, Table 5]. With respect to Hermitian's construction, new quantum BCH codes with $n = r(q^2 + 1)$ from Table 6 have better lower bound for the minimum distance than the ones with $n = r'(q^2 - 1)$ in [8]. He further studied quantum BCH codes with $m \geq 3$ [8]. However, his results need to meet certain conditions when $m \geq 3$. For example, the codes length n is a prime number. In addition, the cosets given need to be mutually disjoint such that $Z \cap Z^{-1} = \emptyset$. Therefore, his methods are inflexible to construct quantum codes and are suitable for computer searching. We come up with an effective solution to choosing suitable cosets. As a result, these cosets are mutually disjoint and the defining set contains most consecutive integers from the proof of theorems in our schemes. Meanwhile, the code generated is Euclidean dual-containing or Hermitian dual-containing. In particular, the code length is not necessary a prime. It can be seen that constructions presented in this paper are more general than [8].

TABLE 5. Codes comparison for $m = 2$.

New codes	Steane's codes in [8]
$[[24, 14, d \geq 4]]_5$	$[[24, 12, d \geq 5]]_5$
$[[60, 46, d \geq 5]]_{11}$	$[[60, 48, d \geq 5]]_{11}$
$[[63, 41, d \geq 7]]_8$	$[[63, 39, d \geq 8]]_8$
$[[168, 126, d \geq 12]]_{13}$	$[[168, 124, d \geq 13]]_{13}$

TABLE 6. Codes comparison for $m = 2$.

New codes	Hermitian codes in [8]
$[[40, 10, d \geq 9]]_3$	$[[40, 26, d \geq 5]]_3$
$[[80, 22, d \geq 17]]_3$	$[[80, 46, d \geq 10]]_3$
$[[255, 91, d \geq 46]]_4$	$[[255, 193, d \geq 17]]_4$
$[[312, 134, d \geq 49]]_5$	$[[312, 266, d \geq 13]]_5$

VI. CONCLUSION

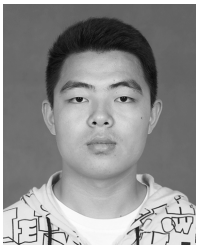
We have constructed quantum BCH codes by classical non-binary BCH codes over F_q and F_{q^2}, respectively. We characterized the properties of cyclotomic cosets and these results make it possible to construct more families of quantum BCH codes, since the BCH codes are nested and are amenable to the Steane enlargement technique [7]. Not only do our schemes facilitate to figure out the dimension of quantum BCH codes but also their defining sets contain consecutive integers as far as possible.

In this paper, We extend to more general case where $n = r\frac{q^m-1}{q-1}$ relative to results in [6] and [7]. Especially, q is just a prime power in our schemes. Compared with the results in [2], [8], and [13] one can see that the new codes in this paper have parameters better than the codes in [2], [8], and [13]. It is interesting to note that the quantum BCH code for $n = r\frac{q^m-1}{q-1}$ is the special case for $n = r\frac{q^{mm'}-1}{q^{m'}-1}$ when $m' = 1$. Therefore, this more general case needs further study in the future.

REFERENCES

[1] M. Hamada, "Concatenated quantum codes constructible in polynomial time: Efficient decoding and error correction," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5689–5704, Dec. 2008.
[2] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, "On quantum and classical BCH codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1183–1188, Mar. 2007.
[3] F. J. MacWilliams and N. J. A. Sloane, *The Theory Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977, pp. 201–215.
[4] C. Crépeau, D. Gottesman, and A. Smith, "Approximate quantum error-correcting codes and secret sharing schemes," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 3494. Berlin, Germany: Springer, 2005, pp. 285–301.
[5] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.
[6] Z. Ma, X. Lu, K. Feng, and D. Feng, "On non-binary quantum BCH codes," in *Theory and Applications of Models of Computation* (Lecture Notes in Computer Science), vol. 3959. Berlin, Germany: Springer, Jan. 2006, pp. 675–683.
[7] A. M. Steane, "Enlargement of Calderbank–Shor–Steane quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2492–2495, Nov. 1999.
[8] G. G. L. Guardia, "On the construction of nonbinary quantum BCH codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 3, pp. 1528–1535, Mar. 2014.
[9] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4892–4914, Nov. 2006.
[10] M. A. Nielsen and I. L. Chuang, *Chuang, Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2010, pp. 450–453.
[11] P. Charpin, "Open problems on cyclic codes," in *Handbook of Coding Theory*. Amsterdam, The Netherlands: North-Holland, 1998, pp. 963–1063.

[12] S. Ling, J. Luo, and C. Xing, "Generalization of Steane's enlargement construction of quantum codes and applications," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 4080–4084, Aug. 2010.
[13] G. G. L. Guardia, "Constructions of new families of nonbinary quantum codes," *Phys. Rev. A, Gen. Phys.*, vol. 80, no. 4, pp. 042331-1–042331-11, 2009.
[14] J. Yuan, S. Zhu, X. Kai, and P. Li, "On the construction of quantum constacyclic codes," *Des., Codes Cryptogr.*, vol. 85, no. 1, pp. 179–180, Oct. 2017.
[15] J. Chen, Y. Huang, C. Feng, and R. Chen, "Some families of optimal quantum codes derived from constacyclic codes," *Linear Multilinear Algebra*, to be published, doi: doi: 10.1080/03081087.2018.1432544.
[16] S. Zhu, Z. Sun, and P. Li, "A class of negacyclic BCH codes and its application to quantum codes," *Des., Codes Cryptogr.*, to be published, doi: 10.1007/s10623-017-0441-6.
[17] J. Gao and Y. Wang, "Quantum codes derived from negacyclic codes," *Int. J. Theor. Phys*, vol. 57, no. 3, pp. 682–686, Mar. 2018.
[18] G. G. L. Guardia, "Quantum codes derived from cyclic codes," *Int. J. Theor. Phys*, vol. 56, no. 8, pp. 2479–2484, Aug. 2017.



MING ZHANG was born in 1991. He received the B.E. degree from the School of Telecommunications Engineering, Xidian University, Xi'an, China, in 2014, where he is currently pursuing the Ph.D. degree. His research interests include information theory, coding theory, and quantum information and computing.

ZHUO LI was born in Baoji, Shannxi, China, in 1980. He received the B.S. degree (Hons.) in mathematics, the M.S. degree in computer science, and the Ph.D. degree in information and communication engineering from Xidian University, Xi'an, China, in 2002, 2005, and 2008, respectively. His research interests include information theory, coding theory, and quantum information and computing.

From 2016 to 2017, he was a Visiting Scholar with Texas A&M University, College Station, TX, USA. Since 2005, he has been with the School of Telecommunications Engineering, Xidian University, where he is currently a Professor.

LIJUAN XING received the B.E. and Ph.D. degrees in information and communication engineering from Xidian University, Xi'an, China, in 2004 and 2008, respectively. Her research interests include communication systems, channel coding, and quantum information and computing.

Since 2010, she has been with the School of Telecommunications Engineering, Xidian University, where she is currently an Associate Professor.

NIANQI TANG received the B.E. degree in communication engineering from Northeast Petroleum University, China, in 2012. He is currently pursuing the Ph.D. degree with the School of Telecommunications Engineering, Xidian University, Xi'an, China. His research interests include coding theory, information theory, and quantum information.