Quantum Information Processing (2023) 22:390
https://doi.org/10.1007/s11128-023-04148-1

Improved construction of quantum constacyclic BCH codes

Yajing Zhou[1] · **Xiaoshan Kai**[1] · **Shixin Zhu**[1]

Received: 9 April 2023 / Accepted: 4 October 2023 / Published online: 23 October 2023

Abstract
In this work, we investigate a class of narrow-sense constacyclic BCH codes of length $\frac{q^{2m}-1}{a(q+1)}$ over the finite field $\mathbb{F}_{q^2}$, where q is a prime power, $m \geq 2$ is an even integer, and $a \neq 1$ is a divisor of $q-1$. The maximum designed distances such that narrow-sense constacyclic BCH codes contain their Hermitian dual codes are determined. The dimensions of the corresponding Hermitian dual-containing codes are worked out. Further, the related quantum codes are constructed. The construction improves the parameters of quantum codes available in the literature.

Keywords Constacyclic codes · Hermitian dual-containing codes · BCH codes · Quantum codes

1 Introduction

In order to shield quantum information from decoherence and quantum noise, quantum error-correcting codes (QECCs) were discovered from the ground-breaking work of Shor [24] and Steane [26] in the mid-1990s. One of the focuses of quantum coding theory is to find quantum codes with good parameters. In 1998, Calderbank et al. [5] established the links between binary quantum stabilizer codes and quaternary Hermitian dual-containing codes and presented the method of constructing binary quantum codes. Following that, many scholars have dedicated themselves to the construction of non-binary QECCs (see [3, 14, 23]). A famous construction is described in the following theorem.

✉ Yajing Zhou
yjzhou0105@163.com

Xiaoshan Kai
kxs6@sina.com

Shixin Zhu
zhushixin@hfut.edu.cn

[1] School of Mathematics, Hefei University of Technology, Hefei 230009, Anhui, China

Theorem 1 [5, 14] *(Hermitian construction) If $\mathcal{C}$ is an $[n, k, d]$ linear code over $\mathbb{F}_{q^2}$ such that $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$, then there exits an $[[n, 2k-n, \geq d]]_q$ quantum code.*

It is well known that BCH codes are an important class of cyclic codes and process effective encoding and decoding algorithms. The most fascinating feature of BCH codes is good algebraic structure. Their dimensions can be determined by using defining sets, and their minimum distance can be estimated by using BCH bound. For more information on BCH codes, please consult [4, 6, 13, 17]. BCH codes over finite fields have many applications in consumer electronics, communication system and quantum information. In particular, Hermitian dual-containing BCH codes can be utilized to build stabilizer codes. Grassl et al. [9] characterized Hermitian dual-containing BCH codes according to defining sets and constructed some quantum BCH codes with small length. Aly et al. [1, 2] studied Euclidean and Hermitian dual-containing BCH codes more generally. Lots of quantum codes processing nice parameters were derived from BCH codes [19, 20, 25, 33]. Recently, Song et al. [25] obtained q-ary quantum BCH codes of length $r\frac{q^{2m}-1}{q^2-1}$, where $r = 1$ or $r = q-1$. Zhang et al. [32] constructed q-ary quantum codes of length $\frac{r(q^{2m}-1)}{q^2-1}$, where $1 \leq r \leq \frac{q-1}{2}$.

Constacyclic codes are the generalization of cyclic codes, which have been discussed extensively. As an application, constacyclic BCH codes have been considered to construct quantum codes as well (see [11, 12, 18, 27–29, 31, 34, 35]). Lin [21] constructed binary quantum codes of length $\frac{4^m-1}{3}$ from quaternary constacyclic codes. Yuan et al. [31] extended the results in [21] to q-ary quantum constacyclic codes of length $\frac{q^{2m}-1}{q+1}$. More generally, Wang et al. [28] constructed q-ary quantum constacyclic codes of length $\frac{q^{2m}-1}{\rho}$, where ρ divides $q+1$. Zhao et al. [34] derived quantum constacyclic BCH codes of length $\frac{q^{2m}-1}{q+1}$ and improved the parameters of quantum codes in [31].

Inspired by the work above, we explore a family of quantum constacyclic codes based on constacyclic BCH codes over $\mathbb{F}_{q^2}$ of length $\frac{q^{2m}-1}{a(q+1)}$, where q is a prime power, $m \geq 2$ is an even integer, and $a > 1$ is a divisor of $q-1$. The maximum designed distances which make such narrow-sense constacyclic BCH codes be Hermitian dual-containing are determined. The dimension of these codes is computed. Further, the parameters of the resulting quantum codes are obtained, which improve the known ones constructed in [2, 28, 32, 33, 35]. The paper is arranged as follows. Some related knowledge and theorems are listed in Sect. 2. In Sect. 3, we investigate Hermitian dual-containing constacyclic BCH codes and construct quantum constacyclic BCH codes. In Sect. 4, our quantum BCH codes are compared with the known ones. Section 5 gives a conclusion of the paper.

2 Preliminaries

In this section, we will go over the pertinent notations and results about constacyclic BCH codes and q^2-cyclotomic cosets [15, 22].

Let q be a prime power. Let $\mathbb{F}_{q^2}$ denote the finite field with q^2 elements, and $\mathbb{F}_{q^2}^*$ denote the multiplicative group consisted of the nonzero elements of $\mathbb{F}_{q^2}$. For each $\alpha \in \mathbb{F}_{q^2}^*$, the conjugate of α is defined by $\bar{\alpha} = \alpha^q$. For any two vectors $\mathbf{x} = (x_1, x_2, \ldots, x_n), \mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_{q^2}^n$, define Hermitian inner product of $\mathbf{x}$ and $\mathbf{y}$ as

$$(\mathbf{x}, \mathbf{y})_h = \bar{x}_1 y_1 + \bar{x}_2 y_2 + \cdots + \bar{x}_n y_n.$$

A linear code $\mathcal{C}$ over $\mathbb{F}_{q^2}$ of length n is a subspace of $\mathbb{F}_{q^2}^n$. The Hermitian dual code of $\mathcal{C}$ is given by

$$\mathcal{C}^{\perp_h} = \left\{ \mathbf{x} \in \mathbb{F}_{q^2}^n \mid (\mathbf{x}, \mathbf{y})_h = 0, \text{for any } \mathbf{y} \in \mathcal{C} \right\}.$$

If $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$, then $\mathcal{C}$ is said to be a Hermitian dual-containing code.

Assume that $\gcd(n, q) = 1$. Let $\lambda \in \mathbb{F}_{q^2}^*$ have order ρ, i.e., $\mathrm{ord}(\lambda) = \rho$. For each vector $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_{q^2}^n$, a λ-constacyclic shift f_λ is given by

$$f_\lambda(\mathbf{a}) = (\lambda a_{n-1}, a_0, \ldots, a_{n-2}).$$

A linear code $\mathcal{C} \subseteq \mathbb{F}_{q^2}^n$ is λ-constacyclic if it is invariant under the map f_λ on $\mathbb{F}_{q^2}^n$. Consider a vector $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ as a polynomial $a(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$. Then, a λ-constacyclic code $\mathcal{C} \subseteq \mathbb{F}_{q^2}^n$ is an ideal in the ring $\mathcal{R}_n = \frac{\mathbb{F}_{q^2}[x]}{\langle x^n - \lambda \rangle}$. Note that each ideal in $\mathcal{R}_n$ is principal. So, there is a monic divisor $g(x)$ of $x^n - \lambda$ in $\mathbb{F}_{q^2}[x]$ satisfying $\mathcal{C} = \langle g(x) \rangle$, where $g(x)$ is the generator polynomial of $\mathcal{C}$. Moreover, the dimension of $\mathcal{C}$ is $n - \deg(g(x))$.

Notice that $\mathrm{ord}(\lambda) = \rho$. Let m be the multiplicative order of q^2 modulo ρn. Then, $\rho n \mid (q^{2m} - 1)$, and so $n \mid (q^{2m} - 1)$. Denote by β a primitive ρn-th root of unity in $\mathbb{F}_{q^{2m}}$. Put $\xi = \beta^\rho \in \mathbb{F}_{q^{2m}}$. Then, ξ is a primitive n-th root of unity. Thus, $\beta \xi^i = \beta^{1+\rho i}$, $0 \le i \le n-1$, are the roots of $x^n - \lambda$. Denote $\Gamma_{\rho n} = \{1 + \rho i \mid 0 \le i \le n-1\}$. The set

$$Z = \{ j \in \Gamma_{\rho n} \mid g(\beta^j) = 0 \}$$

forms the defining set of $\mathcal{C}$. The q^2-cyclotomic coset of i modulo ρn consists of

$$C_i = \left\{ i q^{2j} (\mathrm{mod}\ \rho n) \mid j = 0, 1, \ldots, m_i - 1 \right\},$$

where m_i is the smallest positive integer satisfying $i q^{2m_i} \equiv i (\mathrm{mod}\ \rho n)$. The polynomial $M_s(x) = \prod_{j \in C_s} (x - \beta^j) \in \mathbb{F}_{q^2}[x]$ is called the minimal polynomial of β^s over $\mathbb{F}_{q^2}$. A q^2-cyclotomic coset is skew symmetric if $\rho n - qi \in C_i$, otherwise skew asymmetric. The skew asymmetric cosets C_i and $C_{-qi} = C_{\rho n - qi}$ come in pair. Denote by (C_i, C_{-qi}) such a skew asymmetric pair.

Assume that $\rho \mid (q+1)$. Then, the Hermitian dual code of a λ-constacyclic code over $\mathbb{F}_{q^2}$ is still λ-constacyclic. The following lemma gives an equivalent condition for a Hermitian dual-containing code by its defining set.

Lemma 1 [12] Let $\lambda \in \mathbb{F}_{q^2}^*$ and $\rho = \mathrm{ord}(\lambda) \mid (q+1)$. Let $\mathcal{C}$ be a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set Z. Then, $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$ if and only if $Z \cap Z^{-q} = \emptyset$, where $Z^{-q} = \{-qz \bmod \rho n \mid z \in Z\}$.

Let δ be an integer with $2 \leq \delta \leq n$ and $b = 1 + \rho i \in \Gamma_{\rho n}$. A λ-constacyclic BCH code $\mathcal{C} \subseteq \mathcal{R}_n$ with designed distance δ is a λ-constacyclic code with defining set

$$Z = C_b \cup C_{b+\rho} \cup C_{b+2\rho} \cup \cdots \cup C_{b+(\delta-2)\rho}.$$

If $b = 1$, then $\mathcal{C}$ is called a narrow-sense constacyclic BCH code, otherwise a non-narrow-sense constacyclic BCH code. For a constacyclic code, the minimum distance has the well-known bound.

Lemma 2 [15] (BCH bound for constacyclic codes) Let $\mathcal{C}$ be a λ-constacyclic code over $\mathbb{F}_q$ of length n. Let $\mathrm{ord}(\lambda) = \rho$ and β be a primitive ρn-th root of unity. If the generator polynomial $g(x)$ of $\mathcal{C}$ has the elements $\{\beta^{1+\rho i} \mid 0 \leq i \leq \delta - 2\}$ as the roots, then the minimum distance of $\mathcal{C}$ is not less than δ.

3 Quantum constacyclic BCH codes

Let m be an even integer and $a > 1$ be a divisor of $q-1$. In this section, we take $\lambda \in \mathbb{F}_{q^2}^*$ and $\rho = \mathrm{ord}(\lambda) = q+1$. Let $\mathcal{C}$ be a narrow-sense λ-constacyclic BCH code over $\mathbb{F}_{q^2}$ of length $n = \frac{q^{2m}-1}{a(q+1)}$. Now, we are going to obtain a necessary and sufficient condition on the maximum designed distance to make sure the code $\mathcal{C}$ to be Hermitian dual-containing. Then, we will compute the exact dimension of $\mathcal{C}$ and construct quantum codes from these narrow-sense constacyclic BCH codes by Hermitian construction.

Lemma 3 *Let $\mathcal{C}$ be a λ-constacyclic code over $\mathbb{F}_{q^2}$ of length n with defining set $Z = \bigcup_{i=0}^{\delta} C_{1+\rho i}$. Then, $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$ if and only if $0 \leq \delta \leq \delta^e_{max} - 2$, where*

$$\delta^e_{max} = \frac{q^{m+1} - q^2 - q + 1}{a\rho} + 2. \tag{1}$$

Further, δ^e_{max} is the maximum designed distance such that $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$.

Proof By Lemma 1, $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$ if and only if $Z \cap Z^{-q} = \emptyset$. Assume that $Z \cap Z^{-q} \neq \emptyset$. Then, there exist $0 \leq i_1, i_2 \leq \delta^e_{\max} - 2$ and some positive integer $0 \leq t \leq m-1$ such that

$$(1 + \rho i_1) q^{2t+1} + 1 + \rho i_2 \equiv 0 (\bmod\ \rho n). \tag{2}$$

Notice that Eq. (2) can be written as $(1+\rho i_2)q^{2(m-t-1)+1}+1+\rho i_1 \equiv 0 (\mathrm{mod}\ \rho n)$. We can let $0 \leq t \leq \frac{m}{2}-1$. Then $1+q \leq (1+\rho i_1)q^{2t+1}+1+\rho i_2$ and

$$\begin{aligned}(1+\rho i_1)q^{2t+1}+1+\rho i_2 &\leq \Big(1+\frac{q^{m+1}-q^2-q+1}{a}\Big)q^{m-1}+1+\frac{q^{m+1}-q^2-q+1}{a}\\ &= \frac{q^{2m}-q^m+(a+1)q^{m-1}-q^2-q+a+1}{a}\\ &< \frac{q^{2m}-1}{a} = \rho n.\end{aligned}$$

This is in contradiction to Eq. (2). Thus, $Z \cap Z^{-q} = \emptyset$ and $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$. Next, we show that $\delta^e_{\max}$ is the maximum designed distance such that $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$. We have

$$\begin{aligned}\rho n-(1+\rho(\delta^e_{\max}-1))q^{m-1} &= \frac{q^{2m}-1}{a}-\Big(1+\rho\Big(\frac{q^{m+1}-q^2-q+1}{a(q+1)}+1\Big)\Big)q^{m-1}\\ &= \frac{q^{m+1}+q^m-q^{m-1}-1}{a}-q^m-2q^{m-1}\\ &= 1+\rho\frac{q^{m+1}-(a-1)q^m-(2a+1)q^{m-1}-a-1}{a(q+1)}\\ &= 1+\rho\chi,\end{aligned}$$

where

$$\begin{aligned}\chi &= \frac{q^{m+1}-(a-1)q^m-(2a+1)q^{m-1}-a-1}{a(q+1)}\\ &= \frac{q^m-(q^{m-1}+1)/(q+1)}{a}-q^{m-1}-\frac{q^{m-1}+1}{q+1}.\end{aligned}$$

Notice that χ is a positive integer since m is even and $a \mid q-1$. Moreover, $\chi < \delta^e_{\max}-2$. This implies that $(C_{1+\rho(\delta^e_{\max}-1)}, C_{1+\rho\chi})$ is a skew symmetric pair. This completes the proof. □

In order to determine the dimension of the constacyclic BCH codes $\mathcal{C}$, we need to characterize the q^2-cyclotomic cosets module ρn. The following result determines the cardinalities of the q^2-cyclotomic cosets.

Lemma 4 *Let m be an even positive integer and $a \mid q-1$. For $0 \leq i \leq \delta^e_{max}-2$, the cardinality of the q^2-cyclotomic coset $C_{1+\rho i}$ is m, except $|\ C_{1+\rho\gamma}\ | = \frac{m}{2}$ if q is odd and a is even, where $\gamma = \frac{q^m-1}{2(q+1)}$.*

Proof Let $|\ C_{1+\rho i}\ | = l$, for $1 \leq l \leq m$. If there exists some i, $0 \leq i \leq \delta^e_{\max}-2$, such that $l < m$, then $1 \leq l \leq \frac{m}{2}$ since $l \mid m$. This means that

$$(1+\rho i)(q^{2l}-1) \equiv 0 (\mathrm{mod}\ \rho n). \tag{3}$$

- If $1 \le l \le \frac{m}{2} - 1$ ($m \ge 4$), then

$$\begin{aligned} q^2 - 1 \le (1+\rho i)(q^{2l}-1) &< \left(1 + \frac{q^{m+1}-1}{a}\right)(q^{m-2}-1) \\ &= \frac{q^{2m-1} - q^{m+1} + (a-1)q^{m-2} - a + 1}{a} \\ &< \frac{q^{2m}-1}{a} = \rho n, \end{aligned}$$

  which is in contradiction to Eq. (3).
- If $l = \frac{m}{2}$, then Eq. (3) becomes $(1+\rho i)(q^m - 1) \equiv 0 (\mathrm{mod}\ \frac{q^{2m}-1}{a})$. Thus,

$$a(1+\rho i) \equiv 0 (\mathrm{mod}\ q^m + 1). \tag{4}$$

  If q is even, then $\gcd(q-1, q^m+1) = 1$; otherwise, $\gcd(q-1, q^m+1) = 2$. It follows that $\gcd(\frac{q^m+1}{\gcd(2,a)}, a) = 1$ and Eq. (4) becomes

$$1 + \rho i \equiv 0 \left(\mathrm{mod}\ \frac{q^m+1}{\gcd(2,a)}\right). \tag{5}$$

  Note that

$$1 + \rho i \le 1 + \frac{q^{m+1} - q^2 - q + 1}{a} < 1 + \frac{q^{m+1}-1}{a} < q^{m+1}. \tag{6}$$

  - If q is odd and a is even, then by Eqs. (5) and (6), there exists an integer $1 \le t < 2q$ such that $1 + \rho i = \frac{q^m+1}{2} t$. Then, $i = \frac{t(q^m+1)-2}{2(q+1)}$, which is an integer if and only if $(q^m+1)t \equiv 2 (\mathrm{mod}\ 2(q+1))$. Notice that $q^m + 1 \equiv 2 (\mathrm{mod}\ 2(q+1))$. Then, i is an integer if and only if $t \equiv 1 (\mathrm{mod}\ q+1)$. It must be $t = 1$ or $t = q+2$. If $t = q+2$, then $i = \frac{q^{m+1}+2q^m+q}{2(q+1)} > \delta^e_{\max} - 2$, which is a contradiction. Thus, $t = 1$ and $| C_{\frac{q^m+1}{2}} | = | C_{1+\rho\gamma} | = \frac{m}{2}$, where $\gamma = \frac{q^m-1}{\rho}$.
  - If q is odd and a is odd, then by Eqs. (5) and (6), there exists an integer $1 \le t \le q-1$ such that $1 + \rho i = (q^m+1)t$. Then, $i = \frac{(q^m+1)t-1}{q+1}$, which is an integer if and only if $(q^m+1)t \equiv 1 (\mathrm{mod}\ q+1)$, i.e., $2t \equiv 1 (\mathrm{mod}\ q+1)$. However, $q+1$ is even and $2t \equiv 1 (\mathrm{mod}\ q+1)$ has no solution.
  - If q is even, with a similar method as above, one can get that i is an integer if and only if $2t \equiv 1 (\mathrm{mod}\ q+1)$. Since $q+1$ is odd, $2t \equiv 1 (\mathrm{mod}\ q+1)$ has the only solution $t = \frac{q+2}{2}$. Thus, $1 + \rho i = (q^m+1)\frac{q+2}{2}$ and $i = \frac{q^{m+1}+2q^m+q}{2(q+1)} > \delta^e_{\max} - 2$, which is a contradiction.

This completes the proof. □

For the sake of the exact dimension of $\mathcal{C}$, the following lemma is a requirement.

Lemma 5 *Let $m \geq 2$ be an even integer. Let $n = \frac{q^{2m}-1}{a\rho}$, where $a > 1$ is a divisor of $q-1$. For $1 \leq i \leq \delta^e_{max} - 2$, $1+\rho i$ is not a coset leader if $i \equiv q-1 (\mathrm{mod}\ q^2)$ or $i = \frac{(q^m-1)s}{a\rho}$, where $\frac{a}{2} < s < a$.*

Proof If $i \equiv q-1 (\mathrm{mod}\ q^2)$, then there exists a positive integer r such that $i = q-1+q^2r$. Then, $1+(q+1)i = q^2(1+(q+1)r)$. Thus, $1+\rho i \in C_{1+\rho r}$ is not a coset leader.

If $i \not\equiv q-1 (\mathrm{mod}\ q^2)$ and $1+\rho i$ is not a coset leader, then there exists an integer j, $1 \leq j < i \leq \delta^e_{\max} - 2$, such that $1+\rho i \in C_{1+\rho j}$ and $C_{1+\rho i} = C_{1+\rho j}$. It can be seen that $C_{1+\rho i} = C_{1+\rho j}$ if and only if there exists $1 \leq l \leq m$ such that $(1+\rho i)q^{2l} \equiv 1+\rho j (\mathrm{mod}\ \rho n)$, which is equivalent to $1+\rho i \equiv (1+\rho j)q^{2(m-l)} (\mathrm{mod}\ \rho n)$. So, we can assume $1 \leq l \leq \frac{m}{2}$. Then,

$$q^{2l} - 1 + (q+1)(q^{2l}i - j) \equiv 0 \left(\mathrm{mod}\ \frac{q^{2m}-1}{a}\right). \tag{7}$$

If $1 \leq l \leq \frac{m}{2} - 1$ ($m \geq 4$), then

$$\begin{aligned} q^2 - 1 < q^{2l} - 1 + (q+1)(q^{2l}i - j) &< q^{m-2} - 1 + \frac{q^{2m-1} - q^m - q^{m-1} + q^{m-2}}{a} \\ &< \frac{q^{2m}-1}{a} = \rho n, \end{aligned}$$

which is in contradiction to Eq. (7).
If $l = \frac{m}{2}$, then

$$(1+\rho i)q^m \equiv 1 + \rho j \left(\mathrm{mod}\ (q^m+1)\frac{q^m-1}{a}\right) \tag{8}$$

and $(1+\rho i)q^m \equiv 1+\rho j (\mathrm{mod}\ q^m+1)$. Thus, $2+\rho(i+j) \equiv 0 (\mathrm{mod}\ q^m+1)$. Then, there exists a positive integer t such that

$$2 + \rho(i+j) = (q^m+1)t. \tag{9}$$

Notice that

$$\begin{aligned} (q^m+1)t = \rho(i+j) + 2 &\leq 2 \cdot \frac{q^{m+1} - q^2 - q + 1}{a} + 2 \\ &< 2 \cdot \frac{q-1}{a} \cdot \frac{q^{m+1}-1}{q-1} + 2 \\ &= 2 \cdot \frac{q-1}{a} \cdot (q^m + q^{m-1} + \cdots + q + 1) + 2. \end{aligned}$$

Thus, $1 \leq t \leq \frac{2(q-1)}{a}$.

By Eq. (9), we have $j = \frac{(q^m+1)t-2}{q+1} - i$. Putting it into Eq. (8), one can get

$$(1+\rho i)q^m \equiv (q^m+1)t - 1 - \rho i \left(\mathrm{mod}\ \frac{q^{2m}-1}{a}\right).$$

Then, we have $q^m + 1 + \rho i(q^m+1) - (q^m+1)t \equiv 0 (\mathrm{mod}\ \frac{q^{2m}-1}{a})$, implying that $1 + \rho i - t \equiv 0 (\mathrm{mod}\ \frac{q^m-1}{a})$. Thus, there exists a positive integer s such that

$$\rho i = \frac{q^m-1}{a} \cdot s + t - 1. \tag{10}$$

Due to the fact that m is even and $a \mid q-1$, it must be $\rho \mid \frac{q^m-1}{a}$. Hence, by Eq. (10), $\rho \mid t-1$, i.e., $t \equiv 1 (\mathrm{mod}\ q+1)$. Since $1 \le t \le \frac{2(q-1)}{a}$ and $a \ne 1$, we have $t = 1$. Thus, $i = \frac{(q^m-1)s}{a\rho}$ and $j = \frac{(q^m-1)(a-s)}{a\rho}$. Since $1 + \rho i$ is not a coset leader and $1 \le j < i \le \delta^e_{\max} - 2$, we have $\frac{a}{2} < s < a$. This completes the proof. □

Let $\mathcal{C}$ be a narrow-sense λ-constacyclic BCH code over $\mathbb{F}_{q^2}$ of length n with defining set $Z = \bigcup_{i=0}^{\delta-2} C_{1+\rho i}$, where $2 \le \delta \le \delta^e_{\max}$ and $\mathrm{ord}_{\rho n}(\lambda) = \rho$. Let $[statement] = 1$ if the "statement" is true; otherwise, $[statement] = 0$. From preceding lemmas, we can infer the following theorem.

Theorem 2 *Let $m \ge 2$ be an even integer. Let $n = \frac{q^{2m}-1}{a\rho}$, where $a > 1$ is a divisor of $q-1$. Denote $\Delta = \delta - 2 - \left\lfloor \frac{\delta-q-1}{q^2} \right\rfloor$ and $\epsilon = \frac{1}{2}[q\ odd,\ a\ even]$. Assume that $\ell = 1, 2, \ldots, \lceil \frac{a}{2} \rceil - 2$ if $a > 4$ and $\ell = 0$ if $a = 2, 3$ or 4. Put*

$$\kappa = \begin{cases} \Delta, & if\ 2 \le \delta \le \frac{q^m-1}{2\rho} + 1, \\ \Delta - \epsilon, & if\ \frac{q^m-1}{2\rho} + 2 \le \delta \le \frac{q^m-1}{a\rho}(\lfloor \frac{a}{2} \rfloor + 1) + 1, \\ \Delta - \epsilon - \ell, & if\ \frac{q^m-1}{a\rho}(\lfloor \frac{a}{2} \rfloor + \ell) + 2 \le \delta \le \frac{q^m-1}{a\rho}(\lfloor \frac{a}{2} \rfloor + \ell + 1) + 1, \\ \Delta - \epsilon - \lceil \frac{a}{2} \rceil + 1, & if\ \frac{q^m-1}{a\rho}(a-1) + 2 \le \delta \le \delta^e_{max}. \end{cases} \tag{11}$$

Let the code $\mathcal{C}$ be defined as above. Then, $\mathcal{C}$ is an $[n, n - m\kappa, \ge \delta]$ Hermitian dual-containing constacyclic BCH code.

Proof By Lemma 2, the minimum distance of $\mathcal{C}$ is at least δ. By Lemma 3, $\mathcal{C}$ is a Hermitian dual-containing code. From Lemma 4, if $2 \le \delta \le \frac{q^m-1}{2\rho} + 1$, all the q^2-cyclotomic cosets in the defining set Z have cardinality m; if $\frac{q^m-1}{2\rho} + 2 \le \delta \le \delta^e_{\max}$ and $[q\ odd, a\ even] = 1$, then one of the q^2-cyclotomic cosets in Z has cardinality $\frac{m}{2}$ and the others have cardinality m.

From Lemma 5, one can get $C_{1+\rho i} = C_{1+\rho(q-1+q^2 r)}$, for some integer r. Thus, the number of the q^2-cyclotomic cosets in Z is reduced by $\left\lfloor \frac{\delta-2-(q-1)}{q^2} \right\rfloor + 1 =$

$\left\lfloor \frac{\delta-q-1}{q^2} \right\rfloor + 1$. In addition, by Lemma 5, one can get that $i = \frac{(q^m-1)s}{a\rho}$ are not coset leaders, where $\frac{a}{2} < s < a$. Notice that s can take $s = \lfloor \frac{a}{2} \rfloor + 1, \lfloor \frac{a}{2} \rfloor + 2, \ldots, a-1$.

Let $\ell = 1, 2, \ldots, \lceil \frac{a}{2} \rceil - 2$ if $a > 4$ and $\ell = 0$ if $a = 2, 3$ *or* 4. If $\frac{q^m-1}{a\rho}(\lfloor \frac{a}{2} \rfloor + \ell) + 2 \leq \delta \leq \frac{q^m-1}{a\rho}(\lfloor \frac{a}{2} \rfloor + \ell + 1) + 1$, then the number of the q^2-cyclotomic cosets in Z is reduced by ℓ. If $\frac{q^m-1}{a\rho}(a-1) + 2 \leq \delta \leq \delta^e_{\max}$, then the number of the q^2-cyclotomic cosets in Z is reduced by $\lceil \frac{a}{2} \rceil - 1$. Combining the discussions above, we have the desired result. □

From Theorems 1 and 2, there exist quantum codes with the following parameters.

Theorem 3 *Let $m \geq 2$ be an even integer. Let $n = \frac{q^{2m}-1}{a\rho}$, where $a > 1$ is a divisor of $q-1$. Then, there exists a quantum code with parameters $[[n, n-2m\kappa, \geq \delta]]_q$, where κ is given as Eq. (11).*

4 Code comparisons

In this section, we compare the newly obtained quantum codes in Sect. 3 with those available in the literature [2, 8, 28, 32, 33, 35]. To our knowledge, there exists the same code length as ours in only these studies at present. To compare more clearly, we now list the related results in detail as follows.

Theorem 4 [2, Theorem 21] *Let $n = \frac{q^{2m}-1}{a(q+1)}$, where $a > 1$ is a divisor of $q-1$ and $m \geq 2$. Let $2 \leq \delta \leq \delta_A = \frac{q^m-1}{a(q+1)}$. Then, there exists a quantum code with parameters $[[n, n-2m\lceil(\delta-1)(1-1/q^2)\rceil, \geq \delta]]_q$.*

Theorem 5 [32, Theorem 6] *Let $q \equiv 1 \pmod m$. Let $n = \frac{r(q^{2m}-1)}{q^2-1}$, where $m \geq 4$ and $1 \leq r \leq \frac{q-1}{2}$. Let $\gamma = \frac{r(q^m-1)}{q^2-1}$, $\zeta_l = \frac{2r(q^{m+1}-q)}{m(q^2-1)} - \lceil \frac{2r}{m} \rceil$, $\zeta_\nu = \frac{(m-2)r(q^{m+1}-q)}{m(q^2-1)} - r + \lfloor \frac{2r}{m} \rfloor$ and $\ell = \frac{q^2-1}{r}$. For $2 \leq \delta \leq \delta_R = \zeta_l + \zeta_\nu + 2$, write $\zeta_l = i_1 q^2 + j_1$ and $\zeta_\nu = i_2 q^2 + j_2$. Set $j = \delta - \zeta_\nu - 2 - i_1 q^2$, $r_1 = \min\left\{ \lfloor \frac{\delta-2-i_1 q^2}{\gamma} \rfloor, \lfloor \frac{i_1 q^2}{\gamma} \rfloor \right\}$, $r_2 = \lfloor \frac{i_1 q^2 \gcd(2,\ell)}{q^m+1} \rfloor$, $r_3 = \lfloor \frac{(\delta-2-i_1 q^2)\gcd(2,\ell)}{q^m+1} \rfloor$, $r_4 = \lfloor \frac{\zeta_\nu \gcd(2,\ell)}{q^m+1} \rfloor$, $r_5 = \lfloor \frac{(\delta-2-\zeta_\nu)\gcd(2,\ell)}{q^m+1} \rfloor$, $r_6 = \lfloor \frac{(\delta-2)\gcd(2,\ell)}{q^m+1} \rfloor$ and $r_7 = \min\left\{ \lfloor \frac{\delta-2-\zeta_\nu}{\gamma} \rfloor, \lfloor \frac{2(q-1)}{m} \rfloor \right\}$. Let*

$$\delta_\theta = \begin{cases} m(\lceil(\delta-2)(1-1/q^2)\rceil + \frac{1}{2}r_6) + 1, & if\ 2 \leq \delta \leq i_1 q^2 + 2, \\ m(\lceil(\delta-2)(1-1/q^2)\rceil - \frac{1}{2}(r_2+r_3) - r_1) + 1, & if\ i_1 q^2 + 2 \leq \delta \leq i_1 q^2 + 2 + \zeta_\nu, \\ m(\lceil(\delta-2)(1-1/q^2)\rceil + 1 - \frac{1}{2}(r_4+r_5) - r_7) + 1, & if\ i_1 q^2 + 2 + \zeta_\nu \leq \delta \leq \delta_R \text{ and } j_2 + j \geq q^2, \\ m(\lceil(\delta-2)(1-1/q^2)\rceil - \frac{1}{2}(r_4+r_5) - r_7) + 1, & if\ i_1 q^2 + 2 + \zeta_\nu \leq \delta \leq \delta_R \text{ and } j_2 + j < q^2. \end{cases}$$

Then, there exists a quantum code with parameters $[[n, n-2\delta_\theta, \geq \delta]]_q$.

Theorem 6 [33, Theorem 9] *Let* $q \geq 3$ *be a prime power. Let* $n = r\frac{q^{2m}-1}{q^2-1}$, *where* $m = ord_n(q^2)$ *is even and* $1 \leq r \leq \frac{q+1}{2}$. *Then, there exists an* $[[n, n-2rm(q^{m-1}-q^{m-2}), \geq r\frac{q^m-1}{q+1}+1]]_q$ *quantum code.*

Theorem 7 [35, Corollary 3] *Let* q *be an odd prime power and* $m \geq 2$ *be an even integer,* $n = \frac{q^{2m}-1}{q^2-1}$. *Then, for any* $2 \leq \delta \leq \delta_Z = \frac{q^{m+1}-q}{q^2-1}$, *there exists a quantum code with parameters* $[[n, n-2m\lceil(\delta-3/2)(1-q^{-2})\rceil, \geq \delta]]_q$.

Theorem 8 [28, Theorem 10] *Let* $m \geq 4$ *be even and* $q \geq 3$ *be a prime power. Let* $n = \frac{q^{2m}-1}{e}$, *where* $e \mid q^m-1$ *and* $q^2-q \leq e \leq q^2-1$. *For* $2 \leq \delta \leq \frac{q^{m+1}-q}{e}$, *denote the* q*-adic expansion of* $e(\delta-1)$ *by* $e(\delta-1) = \sum_{i=0}^{m} \delta_i' q^i$.

(1) *If* $\delta_i' = 0$ *for* $i = 1, \ldots, m-1$, $\delta_m' \geq 1$ *and* $\delta_m' > \delta_0'$, *then there exists a quantum code with parameters* $[[n, n-2m\lceil(\delta-1)(1-q^2)\rceil - \lceil\frac{\delta_0'}{e}\rceil, \geq \delta]]_q$.

(2) *Otherwise, there exists a quantum code with parameters* $[[n, n-2m\lceil(\delta-1)(1-q^2)\rceil, \geq \delta]]_q$.

Next, we compare the maximum designed distances with ours in details. Let δ_A, δ_R and δ_Z denote the maximum designed distances in Theorems 4, 5 and 7, respectively. When $m \geq 2$ is even, our maximum designed distance $\delta^e_{\max} = q\delta_A - \frac{q-1}{a} + 2$. The designed distance in Theorem 6 only takes $\delta = r\frac{q^m-1}{q+1}+1$. Thus, our construction can give much more new quantum codes than the constructions in Theorem 4 and Theorem 6. Under the conditions that $r \mid q-1$ and $m \geq 4$, if $m \nmid 2r$, then $\delta^e_{\max} = \delta_R + 1$; otherwise, $\delta^e_{\max} = \delta_R$. For $a = q-1$, $\delta^e_{\max} = \delta_Z + 1$. Hence, our construction can get one more new quantum codes than the constructions in Theorem 5 and Theorem 7.

For fixed length n and designed distance δ, we contrast the dimensions of quantum codes to provide further information. Let k_A, k_R, k_Z and k_W denote the dimensions of quantum codes of length $n = \frac{q^{2m}-1}{a(q+1)}$ in Theorems 4, 5, 7 and 8, respectively. Let k_E denote the dimension of our quantum codes when $m \geq 2$ is even. Let $\delta - 1 = \delta_1 q^2 + \delta_0 \leq \delta_A - 1$, where $0 \leq \delta_0 \leq q^2-1$. Then, $k_E > k_A$ if $q+1 \leq \delta_0 \leq q^2-1$. In rare cases, $k_E = k_A$. Thus, our quantum codes have higher dimension than those in Theorem 4.

If q is odd and $a = q-1$, then $n = \frac{q^{2m}-1}{q^2-1}$. We compare our quantum codes with those in Theorem 7. From Theorems 2 and 3, one can see that if $\frac{q^m-1}{2(q+1)}+2 \leq \delta \leq \delta_Z$, then $k_E > k_Z$, and if $2 \leq \delta \leq \frac{q^m-1}{2(q+1)}+1$, then $k_E \geq k_Z$. Thus, our construction can produce many quantum codes with better parameters than those in Theorem 7. Moreover, for the case that q is even, we can obtain quantum codes from constacyclic BCH codes as well. In Table 1, we compare our quantum codes for $(q, m, a) = (3, 4, 2)$ with quantum codes obtained in Theorem 7 and the Database [8]. It indicates that quantum codes in Theorem 3 have higher rate than quantum codes in Theorem 7 and the Database [8]. The symbol " - " represents that there exist no quantum codes with the given length or designed distance.

Table 1 Quantum codes of length $n = \frac{q^{2m}-1}{a(q+1)}$ with $(q, m, a) = (3, 4, 2)$

$[[n, k, \geq \delta]]_q$ in Thm 3	$[[n, k, d]]_q$ in [8]	$[[n, k, \geq \delta]]_q$ in Thm 7 [35]	$[[n, k, \geq \delta]]_q$ in Thm 8 [28]
$[[820, 804, \geq 4]]_3$	$[[820, 800, 4]]_3$	$[[820, 796, \geq 4]]_3$	$[[820, 796, \geq 4]]_3$
$[[820, 796, \geq 5]]_3$	$[[820, 792, 5]]_3$	$[[820, 788, \geq 5]]_3$	$[[820, 788, \geq 5]]_3$
...	...	...	...
$[[820, 744, \geq 13]]_3$	$[[820, 740, 13]]_3$	$[[820, 732, \geq 13]]_3$	$[[820, 732, \geq 13]]_3$
$[[820, 736, \geq 14]]_3$	$[[820, 732, 14]]_3$	$[[820, 724, \geq 14]]_3$	$[[820, 724, \geq 14]]_3$
$[[820, 728, \geq 15]]_3$	$[[820, 724, 15]]_3$	$[[820, 724, \geq 15]]_3$	$[[820, 716, \geq 15]]_3$
$[[820, 720, \geq 16]]_3$	$[[820, 716, 16]]_3$	$[[820, 716, \geq 16]]_3$	$[[820, 708, \geq 16]]_3$
$[[820, 712, \geq 17]]_3$	$[[820, 708, 17]]_3$	$[[820, 708, \geq 17]]_3$	$[[820, 700, \geq 17]]_3$
$[[820, 704, \geq 18]]_3$	$[[820, 700, 18]]_3$	$[[820, 700, \geq 18]]_3$	$[[820, 692, \geq 18]]_3$
$[[820, 696, \geq 19]]_3$	$[[820, 680, 19]]_3$	$[[820, 692, \geq 19]]_3$	$[[820, 692, \geq 19]]_3$
$[[820, 680, \geq 22]]_3$	$[[820, 676, 22]]_3$	$[[820, 668, \geq 22]]_3$	$[[820, 668, \geq 22]]_3$
$[[820, 672, \geq 23]]_3$	$[[820, 668, 23]]_3$	$[[820, 660, \geq 23]]_3$	$[[820, 660, \geq 23]]_3$
$[[820, 664, \geq 24]]_3$	$[[820, 660, 24]]_3$	$[[820, 660, \geq 24]]_3$	$[[820, 652, \geq 24]]_3$
$[[820, 656, \geq 25]]_3$	$[[820, 652, 25]]_3$	$[[820, 652, \geq 25]]_3$	$[[820, 644, \geq 25]]_3$
$[[820, 648, \geq 26]]_3$	$[[820, 644, 26]]_3$	$[[820, 644, \geq 26]]_3$	$[[820, 636, \geq 26]]_3$
$[[820, 640, \geq 27]]_3$	$[[820, 636, 27]]_3$	$[[820, 636, \geq 27]]_3$	$[[820, 628, \geq 27]]_3$
$[[820, 632, \geq 28]]_3$	$[[820, 616, 28]]_3$	$[[820, 628, \geq 28]]_3$	$[[820, 628, \geq 28]]_3$
$[[820, 616, \geq 31]]_3$	$[[820, 612, 31]]_3$	–	–

In Theorem 5, quantum codes are constructed under the constraint that $q \equiv 1 (\bmod m)$ and $m \geq 4$ is even. However, we can construct quantum codes from constacyclic BCH codes for any prime power q, and we can handle the case $m = 2$. For example, if $m = 2$ and $(q, a) = (7, 3)$, our construction can produce 7-ary quantum codes with parameters $[[100, 80, \geq 8]]_7$ and $[[100, 76, \geq 9]]_7$, which are better than those in [18, Theorem 2]. Many of our quantum codes have better parameters than the codes in Theorem 5. In Table 2, we compare our quantum codes when $(q, m) = (5, 4)$ and $a = 2, 4$ with quantum codes in Theorem 5. From Table 2, we see that our quantum codes have higher rate in many cases.

In Theorem 8, under the conditions that $q^2 - q \leq e \leq q^2 - 1$ and $m \geq 4$, we have $k_E \geq k_W$ when the lengths and designed distances are given. We provide some examples in Tables 1 and 2 for comparing quantum codes in Theorem 3 with quantum codes in Theorem 8. Our construction can produce a number of quantum codes with better parameters than those in [28].

5 Conclusion

In this paper, we investigated constacyclic narrow-sense BCH codes of length $\frac{q^{2m}-1}{a(q+1)}$ over $\mathbb{F}_{q^2}$, where $m \geq 2$ is even and $a > 1$ is a divisor of $q - 1$. The maximum designed distance such that the codes contain their Hermitian duals were determined. The exact dimensions of the Hermitian dual-containing constacyclic BCH codes were calculated by tracing the q^2-cyclotomic cosets. With the aid of these results, we constructed a number of quantum codes by Hermitian construction. Many of these quantum codes have higher rate than those available in the literature. Throughout the study, we assume that a divides $q - 1$ so that an explicit formula on the designed distance of constacyclic dual-containing codes can be described. For a general a, there exist quantum codes with good parameters from narrow-sense constacyclic BCH codes when we conduct experiments. It is worthwhile to make further research for a general a and other lengths.

Quantum constacyclic BCH codes are an important class of quantum error-correcting codes. Due to good algebraic structure, the minimum distance of quantum constacyclic BCH codes can be estimated by virtue of the BCH bound for classical constacyclic codes. Hence, we can measure the error-correcting capacity of the resulting quantum constacyclic BCH codes. At the application level, our quantum constacyclic BCH codes can be theoretically encoded and decoded by quantum shift registers [9, 30], which are performed by the ion traps or nuclear magnetic resonance (NMR) in the experiments [7, 16]. Meanwhile, the constructed codes contain many lengths and hence provide alternative quantum systems. Thus, quantum constacyclic BCH codes are the preferred code resource in quantum error correction and have potential applications in quantum computation and communication. At the physical level, how to realize the error correction and reduce error rate in quantum channels is a crucial problem related to application of quantum constacyclic BCH codes.

Table 2 Quantum codes of length $n = \frac{q^{2m}-1}{a(q+1)}$ with $m = 4$

(q, m, a)	δ	$[[n, k, \delta]]_q$ in Thm 3	$[[n, k, \delta]]_q$ in Thm 5 [32]	$[[n, k, \delta]]_q$ in Thm 8 [28]	$[[n, k, \delta]]_q$ in Thm 2 [2]
(4, 4, 3)	$5 \le \delta \le 16$	$[[4369, 4385 - 8\delta, \ge \delta]]_4$	–	$[[4369, 4377 - 8\delta, \ge \delta]]_4$	$[[4369, 4377 - 8\delta, \ge \delta]]_4$
	$21 \le \delta \le 32$	$[[4369, 4393 - 8\delta, \ge \delta]]_4$	–	$[[4369, 4385 - 8\delta, \ge \delta]]_4$	–
	$37 \le \delta \le 48$	$[[4369, 4409 - 8\delta, \ge \delta]]_4$	–	$[[4369, 4393 - 8\delta, \ge \delta]]_4$	–
	$49 \le \delta \le 52$	$[[4369, 4409 - 8\delta, \ge \delta]]_4$	–	$[[4369, 4401 - 8\delta, \ge \delta]]_4$	–
	$53 \le \delta \le 64$	$[[4369, 4417 - 8\delta, \ge \delta]]_4$	–	$[[4369, 4401 - 8\delta, \ge \delta]]_4$	–
	$65 \le \delta \le 68$	$[[4369, 4417 - 8\delta, \ge \delta]]_4$	–	$[[4369, 4409 - 8\delta, \ge \delta]]_4$	–
	$\delta = 69$	$[[4369, 3873, \ge \delta]]_4$	–	–	–
(5, 4, 2)	$6 \le \delta \le 25$	$[[32552, 32568 - 8\delta, \ge \delta]]_5$	$[[32552, 32566 - 8\delta, \ge \delta]]_5$	–	$[[32552, 32560 - 8\delta, \ge \delta]]_5$
	$31 \le \delta \le 50$	$[[32552, 32576 - 8\delta, \ge \delta]]_5$	$[[32552, 32574 - 8\delta, \ge \delta]]_5$	–	$[[32552, 32568 - 8\delta, \ge \delta]]_5$
	$56 \le \delta \le 76$	$[[32552, 32588 - 8\delta, \ge \delta]]_5$	$[[32552, 32582 - 8\delta, \ge \delta]]_5$	–	–
	$81 \le \delta \le 101$	$[[32552, 32596 - 8\delta, \ge \delta]]_5$	$[[32552, 32590 - 8\delta, \ge \delta]]_5$	–	–
	$106 \le \delta \le 126$	$[[32552, 32604 - 8\delta, \ge \delta]]_5$	$[[32552, 32598 - 8\delta, \ge \delta]]_5$	–	–
	$131 \le \delta \le 151$	$[[32552, 32612 - 8\delta, \ge \delta]]_5$	$[[32552, 32606 - 8\delta, \ge \delta]]_5$	–	–
	$156 \le \delta \le 176$	$[[32552, 32620 - 8\delta, \ge \delta]]_5$	$[[32552, 32614 - 8\delta, \ge \delta]]_5$	–	–
	...	...	...		
(5, 4, 4)	$6 \le \delta \le 25$	$[[16276, 16292 - 8\delta, \ge \delta]]_5$	$[[16276, 16290 - 8\delta, \ge \delta]]_5$	$[[16276, 16284 - 8\delta, \ge \delta]]_5$	$[[16276, 16284 - 8\delta, \ge \delta]]_5$
	$31 \le \delta \le 50$	$[[16276, 16300 - 8\delta, \ge \delta]]_5$	$[[16276, 16298 - 8\delta, \ge \delta]]_5$	$[[16276, 16292 - 8\delta, \ge \delta]]_5$	–
	$56 \le \delta \le 75$	$[[16276, 16312 - 8\delta, \ge \delta]]_5$	$[[16276, 16306 - 8\delta, \ge \delta]]_5$	$[[16276, 16300 - 8\delta, \ge \delta]]_5$	–
	$81 \le \delta \le 100$	$[[16276, 16328 - 8\delta, \ge \delta]]_5$	$[[16276, 16322 - 8\delta, \ge \delta]]_5$	$[[16276, 16308 - 8\delta, \ge \delta]]_5$	–
	$106 \le \delta \le 118$	$[[16276, 16336 - 8\delta, \ge \delta]]_5$	$[[16276, 16330 - 8\delta, \ge \delta]]_5$	$[[16276, 16316 - 8\delta, \ge \delta]]_5$	–
	$\delta = 131$	$[[16276, 15296, \ge \delta]]_5$	–	–	–

Acknowledgements This study is supported by the National Natural Science Foundation of China under Grant Nos. 61972126, 62002093, U21A20428 and 12171134)

Data availability Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study

Declarations

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

References

1. Aly, S.A., Klappenecker, A., Sarvepalli, P.K.: Primitive quantum BCH codes over finite fields. In: Proceedings of IEEE International Symposium on Information Theory, pp. 1114-1118 (2006)
2. Aly, S.A., Klappenecker, A., Sarvepalli, P.K.: On quantum and classical BCH codes. IEEE Trans. Inf. Theory **53**(3), 1183–1188 (2007)
3. Ashikhim, A., Knill, E.: Non-binary quantum stabilizer codes. IEEE Trans. Inf. Theory **47**(7), 3065–3072 (2001)
4. Berlekamp, E.R.: The enumeration of information symbols in BCH codes. Bell Syst. Tech. J. **46**(8), 1861–1880 (1967)
5. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via codes over GF(4). IEEE. Trans. Inf. Theory **44**(4), 1369–1387 (1998)
6. Charpin, P.: On a class of primitive BCH codes. IEEE Trans. Inf. Theory **36**(1), 222–228 (1990)
7. Chuang, L.L., Gershenfeld, N., Kubinec, M.: Experimental implementation of fast quantum searching. Phys. Rev. Lett. **80**(15), 3408–3411 (1998)
8. Edel, Y.: Some good quantum twisted codes. [Online] https://www.mathi.uni-heidelberg.de/~yves/Matritzen/QTBCH/QTBCHIndex.html. Accessed Apr 2023
9. Grassl, M., Beth, T.: Quantum BCH codes. In: Proceedings of International Symposium on Theoretical Electrical Engineering, pp. 207-212 (1999)
10. Grassl, M., Beth, T.: Cyclic quantum error-correcting codes and quantum shift registers. Proc. R. Soc. Lond. A **456**(2003), 2689–2706 (2000)
11. Kai, X., Li, P., Zhu, S.: Construction of quantum negacyclic BCH codes. Int. J. Quantum Inf. **16**(7), 1850059 (2018)
12. Kai, X., Zhu, S., Li, P.: Constacyclic codes and some new quantum MDS codes. IEEE Trans. Inf. Theory **60**(4), 2080–2086 (2014)
13. Kasami, T., Lin, S.: Some results on the minimum weight of BCH codes. IEEE Trans. Inf. Theory **18**(6), 824–825 (1972)
14. Ketkar, A., Klappenecker, A., Kumar, S.: Nonbinary stablizer codes over finite fields. IEEE Trans. Inf. Theory **52**(11), 4892–4914 (2006)
15. Krishna, A., Sarwate, D.V.: Pseudocyclic maximum-distance-separable codes. IEEE Trans. Inf. Theory **36**(4), 880–884 (1990)
16. Lee, J., Lee, E.K., Kim, J., Lee, S.: Quantum shift registers. arXiv:quant-ph/0112107
17. Li, F., Sun, X.: The Hermitian dual containing non-primitive BCH codes. IEEE Commun. Lett. **25**(2), 379–382 (2021)
18. Li, R., Wang, J., Liu, Y., Guo, G.: New quantum constacyclic codes. Quantum Inf. Process. **18**(5), 127 (2019)
19. Li, R., Zuo, F., Liu, Y., Xu, Z.: Hermitian dual-containing BCH codes and construction of new quantum codes. Quantum Inf. Comput. **13**(1–2), 21–35 (2013)
20. Liu, Y., Li, R., Guo, G., Wang, J.: Some nonprimitive BCH codes and related quantum codes. IEEE Trans. Inf. Theory **65**(12), 7829–7839 (2019)
21. Lin, X.: Quantum cyclic and constacyclic codes. IEEE Trans. Inf. Theory **50**(3), 547–549 (2004)
22. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977)
23. Rains, E.M.: Non-binary quantum codes. IEEE Trans. Inf. Theory **45**(6), 1827–1832 (1999)

24. Shor, P.W.: Scheme for reducing decoherence in quantum computing memory. Phys. Rev. A **52**(4), R2493 (1995)
25. Song, H., Li, R., Wang, J., Liu, Y.: Two families of BCH codes and new quantum codes. Quantum Inf. Process. **17**(10), 270 (2018)
26. Steane, A.M.: Multiple particle interference and quantum error correction. Proc. R. Soc. Lond. A **452**(1), 2551–2577 (1996)
27. Wang, J., Li, R., Liu, Y., Guo, G.: Some negacyclic BCH codes and quantum codes. Quantum Inf. Process. **19**(2), 74 (2020)
28. Wang, L., Sun, Z., Zhu, S.: Hermitian dual-containing narrow-sense constacyclic BCH codes and quantum codes. Quantum Inf. Process. **18**(10), 323 (2019)
29. Wang, L., Zhu, S.: New quantum MDS codes derived from constacyclic codes. Quantum Inf. Process. **14**(3), 881–889 (2015)
30. Wilde, M.M.: Quantum-shift-register circuits. Phys. Rev. A **79**(6), 062325(1–16) (2009)
31. Yuan, J., Zhu, S., Kai, X., Li, P.: On the construction of quantum constacyclic codes. Des. Codes Cryptogr. **85**(1), 179–190 (2017)
32. Zhang, J., Li, P., Kai, X., Zhu, S.: Some new classes of quantum BCH codes. Quantum Inf. Process. **21**(12), 396 (2022)
33. Zhang, M., Li, Z., Xing, L., Tang, N.: Constructions some new quantum BCH codes. IEEE Access **4**, 36122 (2018)
34. Zhao, X., Li, X., Wang, Q., Yan, T.: A family of Hermitian dual-containing constacyclic codes and related quantum codes. Quantum Inf. Process. **20**(5), 186 (2021)
35. Zhu, S., Sun, Z., Li, P.: A class of negacyclic BCH codes and its application to quantum codes. Des. Codes Cryptogr. **86**(10), 2139–2165 (2018)