Quantum Information Processing (2019) 18:127
https://doi.org/10.1007/s11128-019-2242-5

New quantum constacyclic codes

Ruihu Li[1] · Junli Wang[1] · Yang Liu[1] · Guanmin Guo[1]

Received: 28 October 2018 / Accepted: 4 March 2019 / Published online: 22 March 2019

Abstract

In this paper, by investigating the Hermitian dual-containing conditions of constacyclic codes with lengths $n = \frac{q+1}{r}(q^2+1)$ and $n = \frac{q-1}{b}(q^2+1)$, where $r \mid q+1$ and $b \mid q-1$, we construct two classes of quantum codes from non-narrow-sense constacyclic codes. Most of these new quantum codes have better parameters than quantum twisted codes and quantum BCH codes, some of them are new with relatively larger distance and can not be constructed in the literature.

Keywords Constacyclic code · Cyclotomic coset · Quantum code · Hermitian dual-containing code

1 Introduction

Quantum error-correcting codes (QCs for short) originated from the pioneering work of Shor [1] and Steane [2] to protect quantum information from decoherence and quantum noise. Since then, the theory of QCs has been extensively studied in the literature (see [3–10], for instance). The most widely investigated subclass of codes is quantum stabilizer codes since they are associated with a group-theoretical structure. Their construction can be reduced to find classical self-orthogonal error-correcting codes over the finite field $\mathbb{F}_q$ or $\mathbb{F}_{q^2}$ with certain inner product [3,4,6–9].

From now on, we assume q is a prime power and $\gcd(n, q) = 1$ in the rest of this paper. Let $\mathbb{F}_{q^2}$ be a finite field with q^2 elements and $\mathbb{F}_{q^2}^* = \mathbb{F}_{q^2} \backslash \{0\}$. For each $\alpha \in \mathbb{F}_{q^2}$, the conjugation of α is denoted by $\overline{\alpha} = \alpha^q$. Given two vectors $\mathbf{x} = (x_1, x_2, \ldots, x_n)$

This work is supported by National Natural Science Foundation of China under Grant Nos. 11471011, 11801564 and Natural Science Foundation of Shaanxi under Grant No. 2017JQ1032.

✉ Ruihu Li
llzsy2015@163.com

[1] Department of Basic Sciences, Air Force Engineering University, Xi'an 710051, Shaanxi, People's Republic of China

and $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_{q^2}^n$, their Hermitian inner product is defined by

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

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

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

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

One of the most frequently used construction methods is the following Hermitian Construction.

Theorem 1 ([3,6,8] Hermitian Construction) *If $\mathcal{C} = [n, k, d]_{q^2}$ is a classical linear code over $\mathbb{F}_{q^2}$ such that $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$, then there exists a q-ary $[[n, 2k-n, \geq d]]_q$ quantum code, where $\mathcal{C}^{\perp_h}$ is the Hermitian dual code of $\mathcal{C}$.*

To obtain q-ary QCs by Theorem 1, one only needs to find linear codes $\mathcal{C}$ over $\mathbb{F}_{q^2}$ such that $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$. From this idea, many Hermitian dual-containing constacyclic codes (including cyclic codes and negacyclic codes) have been applied to construct QCs with good parameters in recent years [11–26]. In [11,12], Aly et al. studied Hermitian dual-containing conditions of BCH codes and constructed many q-ary quantum BCH codes in general. More recently, Yuan et al. [23] have constructed QCs from constacyclic BCH codes of length $n = \frac{q^{2m}-1}{q+1}$. Zhu et al. [24] obtained QCs from negacyclic BCH codes of length $n = \frac{q^{2m}-1}{q-1}$. In [25], some quantum BCH codes with $n = r\frac{q^{2m}-1}{q^2-1}$ and $r | (q^2 - 1)$ were obtained.

This article is dedicated to Hermitian dual-containing condition of non-narrow-sense constacyclic codes (including cyclic codes and negacyclic codes) with lengths $n = \frac{q+1}{r}(q^2 + 1)$ and $n = \frac{q-1}{b}(q^2 + 1)$ and aims at constructing new quantum constacyclic BCH codes with good parameters from such codes. Most of the newly obtained codes have better parameters than QCs available in [12,23–25] for the case $m = 2$ and quantum twisted codes (QTCs) listed in code tables of [33]. Moreover, some of our QCs have larger designed distances than the known ones in [12,23–25].

The paper is organized as follows. In Sect. 2, some basic concepts on q^2-cyclotomic cosets and η-constacyclic codes are reviewed. In Sects. 3 and 4, new constructions of QCs with lengths $n = \frac{q+1}{r}(q^2 + 1)$ and $n = \frac{q-1}{b}(q^2 + 1)$ are presented, respectively. In Sect. 5, code comparisons are provided and the final remarks are drawn.

2 Preliminaries

In this section, we introduce some basic notions and results regarding Hermitian dual-containing codes, η-constacyclic codes and cyclotomic cosets for the purpose of this paper. For more details, see [28–31].

2.1 Review of constacyclic codes

For any vector $(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_{q^2}^n$ and $\eta \in \mathbb{F}_{q^2}^*$, an η-constacyclic shift τ_η on $\mathbb{F}_{q^2}^n$ is $\tau_\eta(c_0, c_1, \ldots, c_{n-1}) = (\eta c_{n-1}, c_0, \ldots, c_{n-2})$. A q^2-ary linear code $\mathcal{C}$ of length n is called *η-constacyclic code* if it is invariant under the η-constacyclic shift τ_η on $\mathbb{F}_{q^2}^n$. When $\eta = 1$, η-constacyclic codes are cyclic codes, and when $\eta = -1$, η-constacyclic codes are negacyclic codes. For an η-constacyclic code $\mathcal{C}$, each code word $c = (c_0, c_1, \ldots, c_{n-1})$ is customarily represented in its polynomial form: $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$. Then, $\mathcal{C}$ is in turn identified with the set of all polynomial representations of its code words. From [16,17,27,28], one can know that a linear code $\mathcal{C}$ of length n over $\mathbb{F}_{q^2}$ is η-constacyclic if and only if $\mathcal{C}$ is an ideal of the quotient ring $\mathcal{R}_n = \mathbb{F}_q[x]/(x^n - \eta)$, and $xc(x)$ corresponds to an η-constacyclic shift of $c(x)$ in $\mathcal{R}_n$. It follows that $\mathcal{C}$ is generated by a monic factor of $(x^n - \eta)$, i.e., $\mathcal{C} = \langle g(x)\rangle$ and $g(x)|(x^n - \eta)$. $g(x)$ is called the generator polynomial of $\mathcal{C}$. The dimension of $\mathcal{C}$ is $n - k$, where $k = \deg(g(x))$. It can be verified that the Hermitian dual $\mathcal{C}^{\perp_h}$ of an η-constacyclic code $\mathcal{C}$ over $\mathbb{F}_{q^2}$ is an $\bar{\eta}^{-1}$-constacyclic code [16,17].

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

$$C_i = \{i, iq^2, i(q^2)^2, \ldots, i(q^2)^{e-1}\} \bmod rn,$$

where e is the smallest positive integer such that $i(q^2)^e \equiv i \bmod rn$. It is easy to see that the defining set T is a union of some q^2-cyclotomic cosets modulo rn (see [17,28]).

Let δ be an integer with $2 \le \delta \le n$, an η-constacyclic BCH (CBCH, for short) code $\mathcal{C}$ of length n with designed distance δ is an η-constacyclic code with defining set

$$T = \bigcup_{i=0}^{\delta-2} C_{b+ir},$$

where C_{b+ir} is the q^2-cyclotomic coset modulo rn containing $b + ir$. When $b = 1$, $\mathcal{C}$ is called a *narrow-sense* CBCH code, otherwise, a *non-narrow-sense* CBCH code.

According to the following BCH bound for η-constacyclic codes (see [27,28]), a CBCH code $\mathcal{C}$ of designed distance δ has minimum distance at least δ.

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

2.2 Description of Hermitian dual-containing conditions by cyclotomic cosets

It is well known that there is a close relationship between cyclotomic cosets and cyclic codes; see [29–32]. The definitions of symmetric coset and asymmetric coset pairs for 2-cyclotomic cosets were first given in [32] to characterize binary self-dual cyclic codes and were generalized further in [14,15] to characterize q^2-ary Hermitian self-orthogonal cyclic codes. Now we give the skew symmetric property of cyclotomic cosets. For each $i \in \Omega$, let C_i be the q^2-cyclotomic coset modulo rn containing i.

A cyclotomic coset C_i is called *skew symmetric* if $-qi \bmod rn \in C_i$, and *skew asymmetric*, otherwise. Skew asymmetric cosets C_i and C_{-qi} come in pairs, and we use (C_i, C_{-qi}) to denote such a *skew asymmetric pair* (SAP, for short). In [17], Kai et al. have shown that an η-constacyclic code $\mathcal{C}$ with defining set T contains its Hermitian dual if and only if $T \cap T^{-q} = \emptyset$, where $T^{-q} = \{-qi \bmod rn \mid i \in T\}$. Using terminologies of skew symmetric coset and SAP, an equivalent statement can be given as in Lemma 2.2 of [14]. We list these two equivalent statements in the following lemma for later use.

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

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

2.3 Notations and a preliminary result

Firstly, to simplify the following discussions, we give some notations here.
Notation: Denote the set $\{b, b+1, \ldots, e\}$ by $[b, e]$. Given four integers s, r, j and i, where $j \leq i$ and $r|(q+1)$, we use $[j, i; r]_s$ to denote the following set

$$[j, i; r]_s = C_{s+jr} \cup C_{s+(j+1)r} \cup C_{s+(j+2)r} \cup \cdots \cup C_{s+ir}.$$

Next, we give some results on skew asymmetric coset and SAP for our main work in the subsequent sections.

Lemma 3 *Let $ord_{rn}(q^2) = 2$ and $i, j \in \Omega$. If $i \neq j$, then the following hold:*

1. *The cardinality of C_i is at most 2.*
2. *$C_i = C_j$ if and only if $iq^2 \equiv j \bmod rn$, which is equivalent to $jq^2 \equiv i \bmod rn$.*
3. *C_i is skew symmetric if and only if $i(q+1) \equiv 0 \bmod rn$.*
4. *(C_i, C_j) is a SAP if and only if $i + jq \equiv 0 \bmod rn$ or $j + iq \equiv 0 \bmod rn$.*

Proof 1. Since $\mathrm{ord}_{rn}(q^2)=2$, from definition, one can easily know that $|C_i|$ is at most 2.

2. By (1), we assume that $C_i=\{i, iq^2\}$. When $i\neq j$, it is obvious that $C_i=C_j \Leftrightarrow iq^2\equiv j \bmod rn$. Since $iq^2\cdot q^2=i(q^4-1+1)\equiv i$, we have

$$iq^2\equiv j \bmod rn \Leftrightarrow iq^2\cdot q^2\equiv i\equiv jq^2 \bmod rn.$$

3. Assume $C_i=\{i, iq^2\}$. If C_i is skew symmetric, then $-qi\equiv i \bmod rn$ or $-qi\equiv iq^2 \bmod rn$. It is obvious that $-qi\equiv i \bmod rn \Leftrightarrow i(q+1)\equiv 0 \bmod rn$. From $\gcd(q, rn)=1$, one can deduce $-qi\equiv iq^2 \bmod rn \Leftrightarrow i(q+1)\equiv 0 \bmod rn$. Hence, (3) holds.

4. By (1), put $C_i=\{i, iq^2\}$. From definition, we know (C_i, C_j) is a SAP if and only if $i\equiv -jq \bmod rn$ or $i\equiv -jq^3 \bmod rn$. Notice that $i\equiv -jq^3 \bmod rn \Leftrightarrow iq\equiv -jq^3\cdot q\equiv -j \bmod rn$. This completes the proof of (4). □

3 Construction of new QCs of length $n=\frac{q+1}{r}(q^2+1)$

In this section, let q be an odd prime power, $r \mid (q+1)$ and $1\leq r\leq \frac{q+1}{2}$. Then, $q+1=rr', r'\geq 2$ and $n=r'(q^2+1)$. It is easy to check $s=\frac{q^2+1}{2}=1+r'\cdot\frac{q-1}{2}\cdot r \in \Omega_{r,n}=\{1+jr|0\leq j\leq n-1\}$, and $\frac{q^2-1}{2r}=r'\frac{q-1}{2}$. We can define a defining set $T=[-\frac{q^2-1}{2r}, \frac{q^2-1}{2r}; r]_s=[-r'\frac{q-1}{2}, r'\frac{q-1}{2}; r]_s\subseteq \Omega_{r,n}$.

Lemma 4 *Let q, r, r', n, s and T be given as above. If $-\frac{q^2-1}{2r}\leq i, j\leq \frac{q^2-1}{2r}$ and $i\neq j$, then the following hold:*

1. *$C_s=\{s\}$ and each C_{s+ir} contains two elements if $i\neq 0$.*
2. *$C_{s+ir}=C_{s+jr}$ if and only if $j=-i$ and $i\equiv 0 \bmod r'$.*
3. *Each C_{s+ir} is skew asymmetric.*
4. *Any two C_{s+ir} and C_{s+jr} cannot form a SAP.*
   Hence, the CBCH code with defining set T is a Hermitian dual-containing code.

Proof 1. If $C_x=\{x\}$ and $x\in T$, then $xq^2\equiv x \bmod rn$. Since $rn=(q+1)(q^2+1)$ and $\gcd(q-1, q^2+1)=2$, one can imply $x(q^2-1)\equiv 0 \bmod (q+1)(q^2+1)$ and $x\equiv 0 \bmod \frac{q^2+1}{2}$. From $x=s+ri$ and $-\frac{q^2-1}{2r}\leq i\leq\frac{q^2-1}{2r}$, we have $x=s$ and C_{s+ir} contains two elements for $-\frac{q^2-1}{2r}\leq i\leq \frac{q^2-1}{2r}$ and $i\neq 0$.

2. According to Lemma 3, $C_{s+ir}=C_{s+jr}$ if and only if $s+ir\equiv (s+jr)q^2 \bmod rn$, which is equivalent to that $i\equiv jq^2 \bmod n$. Since $n=r'(q^2+1)$, we have $i\equiv jq^2 \bmod n \Leftrightarrow j(q^2+1)-(i+j)\equiv 0 \bmod r'(q^2+1)$.

Let $j=ar'+b$, where $0\leq b\leq r'-1$ and a, b are integers. Then, $j(q^2+1)-(i+j)=ar'(q^2+1)+b(q^2+1)-(i+j)\equiv b(q^2+1)-(i+j) \bmod r'(q^2+1)$. From $-\frac{q^2-1}{2r}\leq i, j\leq \frac{q^2-1}{2r}$, one can deduce $-(q^2+1)<-\frac{q^2-1}{r}\leq i+j\leq\frac{q^2-1}{r}<q^2+1$ and $-(q^2+1)<b(q^2+1)-(i+j)<r'(q^2+1)$. Thus, $j(q^2+1)-(i+j)\equiv 0 \bmod r'(q^2+1)$ implies $b=0$ and $j=-i=-ar'$. Then, (2) holds.

3. Since $1 \le s + ir \le q^2$, we have $(s + ir)(q + 1) \le (q + 1)q^2 < rn = (q + 1)(q^2 + 1)$ and then $(s + ir)(q + 1) \not\equiv 0 \bmod rn$. From Lemma 3, (3) holds.

4. From $1 \le s + ir, s + jr \le q^2$, one can infer that $(s + ir) + (s + jr)q \le (q+1)q^2 < rn = (q+1)(q^2+1)$, and then, $(s+ir)+(s+jr)q \not\equiv 0 \bmod rn$. Also, we know that $(s + jr) + (s + ir)q \not\equiv 0 \bmod rn$. According to Lemma 3, (4) holds. □

Now it is sufficient to construct new QCs and calculate their parameters.

Theorem 2 *Let q, r, r', n, s and T be given as above. For $2 \le \delta \le \frac{q^2-1}{r} + 2$, denote $|T(\delta)| = 2\lceil(\delta-2)(1-\frac{1}{2r'})\rceil + 1$. Then, there are a Hermitian dual-containing CBCH code with parameters $[n, n - |T(\delta)|, \ge \delta]_{q^2}$ and an $[[n, n - 2|T(\delta)|, \ge \delta]]_q$ QC.*

Proof Consider $1 \le i \le \frac{q^2-1}{2r}$. Suppose that $\mathcal{C}$ is a CBCH code of designed distance δ with defining set $T(\delta) \subseteq T$, where $T(\delta = 2) = C_s$ and for $\delta \ge 3$

$$T(\delta) = \begin{cases} [-(i-1), i; r]_s & \text{if } \delta = 2i+1; \\ [-i, i; r]_s & \text{if } \delta = 2i+2. \end{cases}$$

Since $C_{s+ir} = C_{s+jr}$ if and only if $j = -i$ and $i \equiv 0 \bmod r'$, we get that there are

$$\delta - 2 - \left\lfloor \frac{\delta-2}{2r'} \right\rfloor + 1 = \left\lceil (\delta-2)(1-\frac{1}{2r'}) \right\rceil + 1$$

disjoint cosets in $T(\delta)$. Combining $C_s = \{s\}$ and that the other cosets have cardinality 2, it can be derived that

$$|T(\delta)| = 2\left\lceil (\delta-2)(1-\frac{1}{2r'}) \right\rceil + 1.$$

By Lemma 4, one can know that $\mathcal{C}$ is a Hermitian dual-containing CBCH code with parameters $[n, n - |T(\delta)|, \ge \delta]_{q^2}$.

By Theorem 1, using the underlying code $\mathcal{C}$, one can then construct an $[[n, n - 2|T(\delta)|, \delta]]_q$ QC for $2 \le \delta \le \frac{q^2-1}{r} + 2$. This completes the proof. □

4 Construction of new QCs of length $n = \frac{q-1}{b}(q^2 + 1)$

In this section, the construction of QCs of length n will be given, where $q - 1 = bb'$ and $n = \frac{q-1}{b}(q^2 + 1) = b'(q^2 + 1)$. We give our discussion in three subsections according to different q.

4.1 $q = 4a + 1 \ge 5$

In this subsection, we set $q = 4a+1 \ge 5$ and $2b \mid (q-1)$. Suppose $s = \frac{a}{b}(q^2+1) = \frac{q-1}{2b} \cdot \frac{q^2+1}{2} = \frac{n}{4}$, then s is an integer.

We define $T = [-\frac{(q-1)^2}{2b}, \frac{(q-1)^2}{2b}; r = 1]_s = [-\frac{(q-1)^2}{2b}, \frac{(q-1)^2}{2b}; 1]_{\frac{n}{4}}$ and discuss cyclic codes of length n over $\mathbb{F}_{q^2}$ with defining set T.

Lemma 5 *Let q, b, b', n, s and T be given as above. If $-\frac{(q-1)^2}{2b} \le i, j \le \frac{(q-1)^2}{2b}$ and $i \neq j$, then*

1. *$C_s = \{s\}$ and each C_{s+i} contains two elements for $i \neq 0$.*
2. *$C_{s+i} = C_{s+j}$ if and only if $j = -i$ and $i \equiv 0 \bmod b'$.*
3. *Each C_{s+i} is skew asymmetric.*
4. *Any two C_{s+i} and C_{s+j} cannot form a SAP.*

Hence, the BCH code with defining set T is a Hermitian dual-containing code.

Proof 1. By definition, for $x \in T$, $C_x = \{x\}$ if and only if $xq^2 \equiv x \bmod n \Leftrightarrow xq^2 - x \equiv 0 \bmod b'(q^2+1) \Leftrightarrow x(q+1)b \equiv 0 \bmod (q^2+1)$. Notice that $\gcd(q+1, q^2+1) = 2$ and $(b, \frac{q^2+1}{2}) = 1$. It then follows that $C_x = \{x\}$ if and only if $x \equiv 0 \bmod \frac{q^2+1}{2}$. From $x \in T$, we have $x = s$. By Lemma 3, we obtain that C_{s+i} contains two elements for $i \neq 0$ and $-\frac{(q-1)^2}{2b} \le i \le \frac{(q-1)^2}{2b}$.

2. By Lemma 3, $C_{s+i} = C_{s+j}$ if and only if $s + i \equiv (s+j)q^2 \bmod n$, which is equivalent to $i \equiv jq^2 \bmod n$ according to $s \equiv sq^2 \bmod n$. Note that $n = b'(q^2+1)$. It is not difficult to derive that $i \equiv jq^2 \bmod n \Leftrightarrow j(q^2+1)-(i+j) \equiv 0 \bmod b'(q^2+1)$. Similar to the proof of (2) in Lemma 4, the conclusion can be obtained.

3. Consider that $(s+i)(q+1) = s(q+1) + i(q+1) = \frac{n}{4}(4a+2) + i(q+1) \equiv \frac{n}{2} + i(q+1) \bmod n$. From $-\frac{(q-1)^2}{2b} \le i \le \frac{(q-1)^2}{2b}$, it follows that $|i(q+1)| \le \frac{(q-1)^2(q+1)}{2b} < \frac{(q^2+1)(q-1)}{2b} = \frac{n}{2}$. Thus, $\frac{n}{2} + i(q+1) \not\equiv 0 \bmod n$. Combining Lemma 3, (3) is straightforward.

4. Notice that $s + i + (s+j)q = s(q+1) + i + jq = \frac{n}{4}(4a+2) + i + jq \equiv \frac{n}{2} + i + jq \bmod n$. Since $-\frac{(q-1)^2}{2b} \le i, j \le \frac{(q-1)^2}{2b}$, we have $|i + jq| \le \frac{(q-1)^2(q+1)}{2b} < \frac{(q^2+1)(q-1)}{2b} = \frac{n}{2}$ and then $\frac{n}{2} + i + jq \not\equiv 0 \bmod n$, i.e., $s + i + (s+j)q \not\equiv 0 \bmod n$. Analogously, we could obtain $s + j + (s+i)q \not\equiv 0 \bmod n$ as well. Hence, (4) holds. □

Theorem 3 *Let q, b, b', n, s and T be given as above. For $2 \le \delta \le \frac{(q-1)^2}{b} + 2$, denote $|T(\delta)| = 2\lceil(\delta-2)(1-\frac{1}{2b'})\rceil + 1$. Then, there are a Hermitian dual-containing BCH code with parameters $[n, n-|T(\delta)|, \ge \delta]_{q^2}$ and an $[[n, n-2|T(\delta)|, \ge \delta]]_q$ QC.*

Proof Consider $1 \le i \le \frac{(q-1)^2}{2b}$. Suppose that $\mathcal{C}$ is a BCH code of designed distance δ with defining set $T(\delta)$, where $T(\delta = 2) = C_s$ and

$$T(\delta) = \begin{cases} [-(i-1), i; 1]_s & \text{if } \delta = 2i+1; \\ [-i, i; 1]_s & \text{if } \delta = 2i+2. \end{cases}$$

Then, the conclusion can be obtained with reference to the proof of Theorem 2. □

4.2 $q = 4a + 3 \geq 7$

In this subsection, let $q = 4a + 3 \geq 7$ be an odd prime power and $b = 1$ or 2. Set

$$r = \begin{cases} \frac{q+1}{2} & \text{if } b = 1; \\ q+1 & \text{if } b = 2. \end{cases}$$

Hence, $rn = \frac{r(q-1)}{b}(q^2+1) = \frac{(q^2-1)(q^2+1)}{2}$. Put $s = ((q+1)a+1)\frac{q^2+1}{2} = \frac{(q-1)^2}{4} \cdot \frac{q^2+1}{2}$. From $s - 1 = ((q+1)a+1)\frac{q^2+1}{2} - 1 = \frac{(q^2+1)(q+1)a}{2} + \frac{q^2-1}{2}$, it follows that $r|(s-1)$ and $s \in \Omega = \Omega_{r,n} = \{1 + jr | 0 \leq j \leq n-1\}$. Then, we shall define $T = [-\frac{(q-1)^2}{2b}, \frac{(q-1)^2}{2b}; r]_s \subseteq \Omega$.

Lemma 6 *Let q, b, b', n, s and T be given as above. If $-\frac{(q-1)^2}{2b} \leq i, j \leq \frac{(q-1)^2}{2b}$ and $i \neq j$, then the following hold:*

1. *$C_s = \{s\}$ and each C_{s+ir} contains two elements for $i \neq 0$.*
2. *Any two $C_{s+ir} = C_{s+jr}$ if and only if $j = -i$ and $i \equiv 0 \bmod b'$.*
3. *Each C_{s+ir} is skew asymmetric.*
4. *Any two C_{s+ir} and C_{s+jr} cannot form a SAP.*

Hence, the CBCH code with defining set T is a Hermitian dual-containing code.

Proof 1. By definition, for $x \in T$, $C_x = \{x\}$ if and only if $xq^2 \equiv x \bmod rn = \frac{(q^2-1)(q^2+1)}{2}$, which is equivalent to that $x \equiv 0 \bmod \frac{q^2+1}{2}$. Thus, from $x = s + ir$ and $-\frac{(q-1)^2}{2b} \leq i \leq \frac{(q-1)^2}{2b}$, we obtain $x = s$. Moreover, for $-\frac{(q-1)^2}{2b} \leq i \leq \frac{(q-1)^2}{2b}$ and $i \neq 0$, by Lemma 3, we obtain that C_{s+ir} contains two elements.

2. By Lemma 3, for $i \neq j$, $C_{s+ir} = C_{s+jr}$ if and only if $s + ir \equiv (s+jr)q^2 \bmod rn = rb'(q^2+1)$. Note that $s \equiv sq^2 \bmod rn$. The above congruence is equivalent to $i \equiv jq^2 \bmod b'(q^2+1)$. Similar to the proof of (2) in Lemma 4, the conclusion can be obtained as well.

3. Note that $(s+ir)(q+1) = s(q+1) + ir(q+1) = \frac{(q-1)^2}{4} \cdot \frac{q^2+1}{2}(q+1) + ir(q+1) \equiv \frac{rn}{2} + ir(q+1) \equiv 0 \bmod rn = \frac{(q^2-1)(q^2+1)}{2} \Leftrightarrow \frac{n}{2} + i(q+1) \equiv 0 \bmod n$. Analogous to the proof of (3) in Lemma 5, (3) follows.

4. Notice that $s + ir + (s+jr)q = s(q+1) + ir + jqr = \frac{(q-1)^2}{4}\frac{q^2+1}{2}(q+1) + ir + jqr \equiv \frac{rn}{2} + ir + jqr \bmod rn = \frac{(q^2-1)(q^2+1)}{2}$.

Since $\frac{rn}{2} + ir + jqr \equiv 0 \bmod rn \Leftrightarrow \frac{n}{2} + i + jq \equiv 0 \bmod n$, it is easy to deduce that (4) can be verified. □

Theorem 4 *Let q, b, b', n, s and T be given as above. For $2 \leq \delta \leq \frac{(q-1)^2}{b} + 2$, denote $|T(\delta)| = 2\lceil(\delta - 2)(1 - \frac{1}{2b'})\rceil + 1$. Then, there are a Hermitian dual-containing CBCH code with parameters $[n, n - |T(\delta)|, \geq \delta]_{q^2}$ and an $[[n, n - 2|T(\delta)|, \geq \delta]]_q$ QC.*

Proof Consider $1 \leq i \leq \frac{(q-1)^2}{2b}$. Suppose that $\mathcal{C}$ is a CBCH code of designed distance δ and defining set $T(\delta)$, where $T(\delta = 2) = C_s$ and

$$T(\delta) = \begin{cases} [-(i-1), i; r]_s & \text{if } \delta = 2i + 1; \\ [-i, i; r]_s & \text{if } \delta = 2i + 2. \end{cases}$$

Then, the conclusion can be obtained similar to the proof of Theorem 2. □

4.3 $q \geq 4$ is a power of 2

In this subsection, let $q \geq 4$ be a power of 2 and $1 \leq b \leq \frac{q-1}{3}$, or $b' \geq 3$. Put

$$s = \begin{cases} \frac{b'-1}{4}(q^2+1) & \text{if } b' \equiv 1 \bmod 4; \\ \frac{3b'-1}{4}(q^2+1) & \text{if } b' \equiv 3 \bmod 4. \end{cases}$$

It is easy to see that s is an integer. Suppose that $u_1 = \frac{b'-1}{2}(q-1) = \frac{(q-1)^2}{2b} - \frac{q-1}{2}$, $u_2 = \frac{b'+1}{2}(q-1) = \frac{(q-1)^2}{2b} + \frac{q-1}{2}$. Define $T = [-u_1, u_2; r = 1]_s$. We analyze cyclic codes of length n with defining set T.

Lemma 7 *Let q, b, b', n, s and T be given as above. If $-u_1 \leq i, j \leq u_2$ and $i \neq j$, then*

1. *$C_s = \{s\}$ and each C_{s+i} contains two elements for $i \neq 0$.*
2. *Any two $C_{s+i} = C_{s+j}$ if and only if $j = -i$ and $i \equiv 0 \bmod b'$.*
3. *Each C_{s+i} is skew asymmetric.*
4. *Any two C_{s+i} and C_{s+j} cannot form a SAP.*

Hence, the BCH code with defining set T is a Hermitian dual-containing code.

Proof 1. By definition, $C_x = \{x\}$ if and only if $xq^2 \equiv x \bmod n = b'(q^2+1)$. Notice $xq^2 \equiv x \bmod b'(q^2+1) \Leftrightarrow xb(q+1) \equiv 0 \bmod (q^2+1)$ and $(q+1, q^2+1) = 1$, $(b, q^2+1) = 1$. It follows that $C_x = \{x\}$ if and only if $x \equiv 0 \bmod (q^2+1)$.

Clearly, from $x \in T$, we obtain that $x = s$ and C_{s+i} contains two elements for $-u_1 \leq i \leq u_2, i \neq 0$ by Lemma 3.

2. By Lemma 3, for $i \neq j$, we have $C_{s+i} = C_{s+j}$ if and only if $s + i \equiv (s + j)q^2 \bmod n = b'(q^2+1)$, which implies that $i \equiv jq^2 \bmod b'(q^2+1)$ since $s \equiv sq^2 \bmod n$. Similar to the proof of (2) in Lemma 4, the conclusion can be obtained.

3. For either $b' \equiv 1 \bmod 4$ or $b' \equiv 3 \bmod 4$, there holds $n = b'(q^2+1)$. Then, one can infer that $(s+i)(q+1) = s(q+1)+i(q+1) \equiv \frac{n-q^2-1}{2} + i(q+1) \bmod n$. From $-u_1 \leq i \leq u_2$, it is easy to get that $-\frac{n}{2} + \frac{q-1}{b} + \frac{q^2-1}{2} \leq i(q+1) \leq (\frac{(q-1)^2}{2b} + \frac{q-1}{2})(q+1) \leq \frac{n}{2} - \frac{q-1}{b} + \frac{q^2-1}{2}$. It follows that $\frac{q-1}{b} - 1 \leq \frac{n-q^2-1}{2} + i(q+1) \leq n - \frac{q-1}{b} + 1$. Thus, $(s+i)(q+1) \equiv \frac{n-q^2-1}{2} + i(q+1) \not\equiv 0 \bmod n$. By Lemma 3, (3) holds.

4. Analogous to (3), we get that $s + i + (s + j)q = s(q+1) + i + jq \equiv \frac{n-q^2-1}{2} + i + jq \bmod n$. Since $-u_1 \leq i, j \leq u_2$, we have $-\frac{n}{2} + \frac{q-1}{b} + \frac{q^2-1}{2} \leq i + jq \leq (\frac{(q-1)^2}{2b} + \frac{q-1}{2})(q+1) \leq \frac{n}{2} - \frac{q-1}{b} + \frac{q^2-1}{2}$. It follows that $\frac{q-1}{b} - 1 \leq \frac{n-q^2-1}{2} + i + jq \leq n - \frac{q-1}{b} + 1$. Clearly, $\frac{n-q^2-1}{2} + i + jq \not\equiv 0 \bmod n$, which implies that $s + i + (s + j)q \not\equiv 0 \bmod n$. Similarly, we can obtain $s + j + (s + i)q \not\equiv 0 \bmod n$ holds as well. Combining Lemma 3, then (4) follows. □

Theorem 5 *Let q, b, b', n, s and T be given as above. For $2 \le \delta \le b'(q-1)+2 = \frac{(q-1)^2}{b}+2$, denote*

$$|T(\delta)| = \begin{cases} 2\left\lceil(\delta-2)(1-\frac{1}{2b'})\right\rceil+1 \ \textit{if}\ 2 \le \delta \le (b'-1)(q-1)+2; \\ 2\left(\delta-2-\frac{q-1-b}{2}\right)+1 \quad \textit{if}\ (b'-1)(q-1)+3 \le \delta \le b'(q-1)+2. \end{cases}$$

Then, there are a Hermitian dual-containing BCH code with parameters $[n, n-|T(\delta)|, \ge \delta]_{q^2}$ and an $[[n, n-2|T(\delta)|, \ge \delta]]_q$ QC.

Proof We could verify this conclusion by two steps. Suppose that $\mathcal{C}$ is a BCH code of designed distance δ and defining set $T(\delta)$.

1. Consider $2 \le \delta \le (b'-1)(q-1)+2$ and $1 \le i \le \frac{b'-1}{2}(q-1)$. Set $T(\delta=2) = C_s$ and

$$T(\delta) = \begin{cases} [-(i-1), i; 1]_s & \text{if } \delta = 2i+1; \\ [-i, i; 1]_s & \text{if } \delta = 2i+2. \end{cases}$$

   Similar to the proof of Theorem 2, we can derive that if $2 \le \delta \le (b'-1)(q-1)+2$, then $|T(\delta)| = 2\lceil(\delta-2)(1-\frac{1}{2b'})\rceil+1$.
2. For $(b'-1)(q-1)+3 \le \delta \le b'(q-1)+2$ and $\frac{b'-1}{2}(q-1)+1 \le i \le \frac{b'+1}{2}(q-1)$. Put $T(\delta) = [-\frac{b'-1}{2}(q-1), i; 1]_s$. It follows that $\delta = \frac{b'-1}{2}(q-1)+i+2$. From (1–2) of Lemma 7, we can derive that there are

$$(\delta-2-\frac{(b'-1)(q-1)}{2b'})+1 = \delta-2-\frac{q-1-b}{2}+1$$

   disjoint cosets in $T(\delta)$, of which $\delta-2-\frac{q-1-b}{2}$ cosets have cardinality 2 besides $C_s=\{s\}$. We naturally have

$$|T(\delta)| = 2(\delta-2-\frac{q-1-b}{2})+1.$$

Thus, $T(\delta)$ defines a Hermitian dual-containing BCH code with parameters $[n, n-|T(\delta)|, \ge \delta]_{q^2}$, and this code gives an $[[n, n-2|T(\delta)|, \ge \delta]]_q$ QC. □

5 Code comparisons and conclusion

In this paper, Hermitian dual-containing conditions of non-narrow-sense η-constacyclic codes of lengths $n = \frac{q+1}{r}(q^2+1)$ and $n = \frac{q-1}{b}(q^2+1)$ were deeply investigated. Consequently, applying underlying η-constacyclic codes, we have constructed two families of QCs with good parameters from the Hermitian construction. By comparison, it can be shown that the absolute majority of newly obtained QCs have better performance than the ones available in the literature. On the one hand, some of these

Table 1 Comparisons of quantum codes with $n = \frac{q+1}{r}(q^2+1)$ over $\mathbb{F}_q$

q, r	QC in Theorem 2	QTC in [33]	QC in [25]	QC in [12]
$q = 3, r = 2$	$\ast[[20, 14, \geq 3]]_3$	$[[20, 12, 3]]_3$		
	$\Diamond[[20, 10, \geq 4]]_3$			
	–		$[[20, 4, \geq 5]]_3$	
	$\Diamond[[20, 6, \geq 6]]_3$			
$q = 5, r = 3$	$[[52, 46, \geq 3]]_5$	$[[52, 46, 3]]_5$		
	$[[52, 42, \geq 4]]_5$	$[[52, 42, 4]]_5$		
	–	$[[52, 38, 5]]_5$		
	$\Diamond[[52, 38, \geq 6]]_5$			
	$\Diamond[[52, 34, \geq 7]]_5$			
	$\Diamond[[52, 30, \geq 8]]_5$			
	–		$[[52, 20, \geq 9]]_5$	
	$\Diamond[[52, 26, \geq 10]]_5$			
$r = 2$	$\ast[[78, 72, \geq 3]]_5$	$[[78, 70, 3]]_5$		$[[78, 70, \geq 3]]_5$
	$\ast[[78, 68, \geq 4]]_5$	$[[78, 66, 4]]_5$		
	$\ast[[78, 64, \geq 5]]_5$	$[[78, 62, 5]]_5$		
	$\ast[[78, 60, \geq 6]]_5$	$[[78, 58, 6]]_5$		
	–	$[[78, 54, 7]]_5$		
	$\ast[[78, 56, \geq 8]]_5$	$[[78, 50, 8]]_5$		
	$\ast[[78, 52, \geq 9]]_5$	$[[78, 46, 9]]_5$		
	$\ast[[78, 48, \geq 10]]_5$	$[[78, 42, 10]]_5$		
	$\ast[[78, 44, \geq 11]]_5$	$[[78, 38, 11]]_5$		
	$\ast[[78, 40, \geq 12]]_5$	$[[78, 34, 12]]_5$		
	–		$[[78, 30, \geq 13]]_5$	
	$\Diamond[[78, 36, \geq 14]]_5$			
$q = 7, r = 4$	$[[100, 94, \geq 3]]_7$	$[[100, 92, 3]]_7$		
	$[[100, 90, \geq 4]]_7$	$[[101, 91, 4]]_7$		
	$\ast[[100, 86, \geq 5]]_7$	$[[101, 87, 5]]_7$		
	$\Diamond[[100, 86, \geq 6]]_7$	–		
	$\dots$	$\dots$		
	$\Diamond[[100, 70, \geq 11]]_7$	–		
	$\Diamond[[100, 66, \geq 12]]_7$	–	$[[100, 52, \geq 12]]_7$	
	$\Diamond[[100, 62, \geq 14]]_7$	$[[101, 51, 14]]_7$		
$r = 2$	$\ast[[200, 194, \geq 3]]_7$	$[[200, 192, 3]]_7$		$[[200, 192, \geq 3]]_7$
	$\ast[[200, 190, \geq 4]]_7$	$[[200, 188, 4]]_7$		$[[200, 188, \geq 4]]_7$
	$\ast[[200, 186, \geq 5]]_7$	$[[200, 184, 5]]_7$		
	$\ast[[200, 182, \geq 6]]_7$	$[[200, 180, 6]]_7$		
	$\ast[[200, 178, \geq 7]]_7$	$[[200, 176, 7]]_7$		
	$\ast[[200, 174, \geq 8]]_7$	$[[200, 172, 8]]_7$		
	–	$[[200, 168, 9]]_7$		

Table 1 continued

q, r	QC in Theorem 2	QTC in [33]	QC in [25]	QC in [12]
	$\ast[[200, 170, \geq 10]]_7$	$[[200, 164, 10]]_7$		
	$\ast[[200, 166, \geq 11]]_7$	$[[200, 160, 11]]_7$		
	...	...		
	$\ast[[200, 122, \geq 23]]_7$	$[[200, 112, 23]]_7$		
	$\ast[[200, 118, \geq 24]]_7$	$[[200, 108, 24]]_7$	$[[200, 104, \geq 24]]_7$	
	$-$	$[[200, 104, 25]]_7$		
	$\ast[[200, 114, \geq 26]]_7$	$[[201, 103, 26]]_7$		
$q = 9, r = 5$	$[[164, 158, \geq 3]]_9$	$[[164, 158, 3]]_9$		
	$[[164, 154, \geq 4]]_9$	$[[164, 154, 4]]_9$		
	$-$	$[[164, 150, 5]]_9$		
	$\ast[[164, 150, \geq 6]]_9$			
	$\diamond[[164, 146, \geq 7]]_9$			
	...			
	$\diamond[[164, 118, \geq 16]]_9$			
	$-$		$[[164, 100, \geq 17]]_9$	
	$\diamond[[164, 114, \geq 18]]_9$			
$r = 2$	$\ast[[410, 404, \geq 3]]_9$	$[[410, 402, 3]]_9$		$[[410, 402, \geq 3]]_9$
	$\ast[[410, 400, \geq 4]]_9$	$[[410, 398, 4]]_9$		$[[410, 398, \geq 4]]_9$
	$\ast[[410, 396, \geq 5]]_9$	$[[410, 394, 5]]_9$		$[[410, 394, \geq 5]]_9$
	$\ast[[410, 392, \geq 6]]_9$	$[[410, 390, 6]]_9$		
	...	...		
	$\ast[[410, 344, \geq 19]]_9$	$[[410, 338, 19]]_9$		
	$\ast[[410, 340, \geq 20]]_9$	$[[410, 334, 20]]_9$		
	$-$	$[[410, 330, 21]]_9$		
	$\ast[[410, 336, \geq 22]]_9$	$[[410, 326, 22]]_9$		
	$\ast[[410, 332, \geq 23]]_9$	$[[410, 322, 23]]_9$		
	...	...		
	$\ast[[410, 308, \geq 29]]_9$	$[[410, 298, 29]]_9$		
	$\ast[[410, 304, \geq 30]]_9$	$[[410, 294, 30]]_9$		
	$-$	$[[410, 290, 31]]_9$		
	$\ast[[410, 300, \geq 32]]_9$	$[[410, 286, 32]]_9$		
	$\ast[[410, 296, \geq 33]]_9$	$[[410, 282, 33]]_9$		
	...	...		
	$\ast[[410, 272, \geq 39]]_9$	$[[410, 258, 39]]_9$		
	$\ast[[410, 268, \geq 40]]_9$	$[[410, 254, 40]]_9$		
	$-$	$[[410, 250, 41]]_9$	$[[410, 250, \geq 41]]_9$	
	$\diamond[[410, 264, \geq 42]]_9$			

Table 2 Comparisons of quantum codes with $n = \frac{q-1}{b}(q^2+1)$ and $r = 1$ over $\mathbb{F}_q$

q, b	QC in Theorem 3	QTC in [33]	QC in [25]	QC in [23]	QC in [12]
$q = 5$	$[[52, 46, \geq 3]]_5$	$[[52, 46, 3]]_5$			
$b = 2$	$[[52, 42, \geq 4]]_5$	$[[52, 42, 4]]_5$			
	–	$[[52, 38, 5]]_5$			
	$\diamond[[52, 38, \geq 6]]_5$	–			
	$\diamond[[52, 34, \geq 7]]_5$	–			
	$\cdots$	–			
	$\diamond[[52, 26, \geq 10]]_5$	–			
$b = 1$	$[[104, 98, \geq 3]]_5$	$[[104, 98, 3]]_5$		$[[104, 96, \geq 3]]_5$	$[[104, 94, \geq 3]]_5$
	$[[104, 94, \geq 4]]_5$	$[[104, 94, 4]]_5$		$[[104, 92, \geq 4]]_5$	$[[104, 90, \geq 4]]_5$
	$[[104, 90, \geq 5]]_5$	$[[104, 90, 5]]_5$		–	
	$[[104, 86, \geq 5]]_5$	$[[104, 86, 6]]_5$		$[[104, 88, \geq 5]]_5$	
	$\cdots$	$\cdots$		$\cdots$	
	$[[104, 78, \geq 8]]_5$	$[[104, 78, 8]]_5$		$[[104, 80, \geq 8]]_5$	
	–	–		$[[104, 76, \geq 9]]_5$	
	$[[104, 74, \geq 10]]_5$	$[[104, 74, 10]]_5$		$[[104, 72, \geq 10]]_5$	
	$[[104, 66, \geq 12]]_5$	$[[104, 66, 12]]_5$		$[[104, 64, \geq 12]]_5$	
	$[[104, 62, \geq 13]]_5$	$[[104, 62, 13]]_5$		$[[104, 60, \geq 13]]_5$	
	$[[104, 58, \geq 14]]_5$	$[[104, 58, 14]]_5$		$[[104, 56, \geq 14]]_5$	
	$[[104, 54, \geq 15]]_5$	$[[104, 54, 15]]_5$		$[[104, 52, \geq 15]]_5$	
	$[[104, 50, \geq 16]]_5$	$[[104, 50, 16]]_5$		$[[104, 48, \geq 16]]_5$	

Table 2 continued

q, b	QC in Theorem 3	QTC in [33]	QC in [25]	QC in [23]	QC in [12]
	–	$[[104, 46, 17]]_5$		$[[104, 46, \geq 17]]_5$	
	$*[[104, 46, \geq 18]]_5$	$[[104, 42, 18]]_5$		$[[104, 40, \geq 18]]_5$	
$q = 9$	$[[164, 158, \geq 3]]_9$	$[[164, 158, 3]]_9$			
$b = 4$	$[[164, 154, \geq 4]]_9$	$[[164, 154, 4]]_9$			
	–	$[[164, 150, 5]]_9$			
	$\diamond[[164, 150, \geq 6]]_9$	–			
	$\diamond[[164, 146, \geq 7]]_9$	–			
	$\cdots$	$\cdots$			
	$*[[164, 114, \geq 17]]_9$	–	$[[164, 100, \geq 17]]_9$		
	$\diamond[[164, 114, \geq 18]]_9$	–			
$b = 2$	$[[328, 322, \geq 3]]_9$	$[[328, 322, 3]]_9$			$[[328, 320, \geq 3]]_9$
	$[[328, 318, \geq 4]]_9$	$[[328, 318, 4]]_9$			$[[328, 316, \geq 4]]_9$
	$\cdots$	$\cdots$			
	$*[[328, 298, \geq 10]]_9$	$[[328, 294, 10]]_9$			
	$*[[328, 294, \geq 11]]_9$	$[[328, 290, 11]]_9$			
	$*\cdots$	$\cdots$			
	$*[[328, 218, \geq 32]]_9$	$[[328, 204, 32]]_9$			
	–	$[[328, 200, 33]]_9$	$[[328, 200, \geq 33]]_9$		
	$\diamond[[328, 214, \geq 34]]_9$	–			

Table 2 continued

q, b	QC in Theorem 3	QTC in [33]	QC in [25]	QC in [23]	QC in [12]
$b = 1$	$[[656, 650, \geq 3]]_9$	$[[656, 650, 3]]_9$		$[[656, 648, \geq 3]]_9$	$[[656, 648, \geq 3]]_9$
	$[[656, 646, \geq 4]]_9$	$[[656, 646, 4]]_9$		$[[656, 644, \geq 4]]_9$	$[[656, 644, \geq 4]]_9$
	$\ldots$	$\ldots$		$\ldots$	$\ldots$
	$[[656, 630, \geq 8]]_9$	$[[656, 630, 8]]_9$		$[[656, 628, \geq 8]]_9$	$[[656, 628, \geq 8]]_9$
	$\ldots$	$\ldots$		$\ldots$	
	$[[656, 422, \geq 63]]_9$	$[[656, 422, 63]]_9$		$[[656, 412, \geq 63]]_9$	
	$[[656, 418, \geq 64]]_9$	$[[656, 418, 64]]_9$		$[[656, 408, \geq 64]]_9$	
	–	$[[656, 414, 65]]_9$		$[[656, 404, \geq 65]]_9$	
	$*[[656, 414, \geq 66]]_9$	$[[656, 410, 66]]_9$		$[[656, 400, \geq 66]]_9$	

Table 3 Comparisons of quantum codes with $n = \frac{q-1}{b}(q^2+1)$ over $\mathbb{F}_q$ for $q = 7$

b, r	QC in Theorem 4	QTC in [33]	QC in [25]	QC in [23]	QC in [12]
$b = 1$	$[[300, 294, \geq 3]]_7$	$[[300, 294, 3]]_7$		$[[300, 292, \geq 3]]_7$	$[[300, 292, \geq 3]]_7$
$r = 4$	$[[300, 290, \geq 4]]_7$	$[[300, 290, 4]]_7$		$[[300, 288, \geq 4]]_7$	$[[300, 288, \geq 4]]_7$
	$[[300, 286, \geq 5]]_7$	$[[300, 286, 5]]_7$		$[[300, 284, \geq 5]]_7$	$[[300, 284, \geq 5]]_7$
	$[[300, 282, \geq 6]]_7$	$[[300, 282, 6]]_7$		$[[300, 280, \geq 6]]_7$	$[[300, 280, \geq 6]]_7$
	$[[300, 278, \geq 7]]_7$	$[[300, 278, 7]]_7$		–	
	$\ldots$	$\ldots$		$\ldots$	
	$[[300, 254, \geq 14]]_7$	$[[300, 254, 14]]_7$		$[[300, 252, \geq 14]]_7$	
	$[[300, 250, \geq 15]]_7$	$[[300, 250, 15]]_7$		$[[300, 248, \geq 15]]_7$	
	$[[300, 246, \geq 16]]_7$	$[[300, 246, 16]]_7$		$[[300, 244, \geq 16]]_7$	
	$\ldots$	$\ldots$		$\ldots$	
	$[[300, 170, \geq 36]]_7$	$[[300, 170, 36]]_7$		$[[300, 164, \geq 36]]_7$	
	–	$[[300, 166, 37]]_7$		$[[300, 160, \geq 37]]_7$	
	$*[[300, 166, \geq 38]]_7$	$[[300, 162, 38]]_7$		$[[300, 156, \geq 38]]_7$	
$b = 2$	$[[150, 144, \geq 3]]_7$	$[[150, 144, 3]]_7$			$[[150, 142, \geq 3]]_7$
$r = 8$	$\ldots$	$\ldots$			
	$[[150, 132, \geq 6]]_7$	$[[150, 132, 6]]_7$			
	$*[[150, 128, \geq 8]]_7$	$[[150, 124, 8]]_7$			
	$*[[150, 124, \geq 9]]_7$	$[[150, 120, 9]]_7$			
	$*[[150, 120, \geq 10]]_7$	$[[150, 116, 10]]_7$			
	$*[[150, 116, \geq 11]]_7$	$[[150, 112, 11]]_7$			
	$*[[150, 112, \geq 12]]_7$	$[[150, 108, 12]]_7$			
	–	$[[150, 104, 13]]_7$			

Table 3 continued

b, r	QC in Theorem 4	QTC in [33]	QC in [25]	QC in [23]	QC in [12]
	$*[[150, 108, \geq 14]]_7$	$[[150, 100, 14]]_7$			
	$\diamond[[150, 104, \geq 15]]_7$	–			
	$\cdots$	$\cdots$			
	$\diamond[[150, 92, \geq 18]]_7$	–			
	–		$[[150, 78, \geq 19]]_7$		
	$\diamond[[150, 88, \geq 20]]_7$	–			

Table 4 Comparisons of quantum codes with $n = \frac{q-1}{b}(q^2 + 1)$ over $\mathbb{F}_q$

q	r, b	QC in Theorem 5	QTC in [33]	QC in [23]	QC in [12]
$q = 4$	$b = 1, r = 1$	$[[51, 45, \geq 3]]_4$	$[[51, 45, 3]]_4$	$[[51, 43, \geq 3]]_4$	$[[51, 43, \geq 3]]_4$
		$[[51, 41, \geq 4]]_4$	$[[51, 41, 4]]_4$	–	
		$[[51, 37, \geq 5]]_4$	$[[51, 39, 5]]_4$	$[[51, 39, \geq 5]]_4$	
		$[[51, 33, \geq 6]]_4$	$[[51, 35, 6]]_4$	$[[51, 35, \geq 6]]_4$	
		–	$[[51, 31, 7]]_4$	$[[51, 31, \geq 7]]_4$	
		$*[[51, 29, \geq 8]]_4$	$[[51, 27, 8]]_4$	$[[51, 27, \geq 8]]_4$	
		$*[[51, 25, \geq 9]]_4$	$[[51, 23, 9]]_4$	$[[51, 23, \geq 9]]_4$	
		$*[[51, 21, \geq 10]]_4$	$[[51, 19, 10]]_4$	$[[51, 19, \geq 10]]_4$	
		$*[[51, 17, \geq 11]]_4$	$[[51, 15, 11]]_4$	$[[51, 15, \geq 11]]_4$	
$q = 8$	$b = 1, r = 1$	$*[[455, 449, \geq 3]]_8$		$[[455, 447, \geq 3]]_8$	$[[455, 447, \geq 3]]_8$
		$*[[455, 445, \geq 4]]_8$		$[[455, 443, \geq 4]]_8$	$[[455, 443, \geq 4]]_8$
		$*[[455, 441, \geq 5]]_8$		$[[455, 439, \geq 5]]_8$	$[[455, 439, \geq 5]]_8$
		$*[[455, 437, \geq 6]]_8$		$[[455, 435, \geq 6]]_8$	$[[455, 435, \geq 6]]_8$
		$*[[455, 433, \geq 7]]_8$		$[[455, 431, \geq 7]]_8$	$[[455, 431, \geq 7]]_8$
		$*[[455, 429, \geq 8]]_8$		–	
		...		...	
		$*[[455, 353, \geq 28]]_8$		$[[455, 351, \geq 28]]_8$	
		–		$[[455, 347, \geq 29]]_8$	
		$*[[455, 349, \geq 30]]_8$		$[[455, 343, \geq 30]]_8$	
		$*[[455, 345, \geq 31]]_8$		$[[455, 339, \geq 31]]_8$	
		...		...	
		$*[[455, 325, \geq 36]]_8$		$[[455, 319, \geq 36]]_8$	
		$*[[455, 321, \geq 37]]_8$		–	
		$*[[455, 317, \geq 38]]_8$		$[[455, 315, \geq 38]]_8$	
		...		...	
		$*[[455, 301, \geq 42]]_8$		$[[455, 295, \geq 42]]_8$	
		–		$[[455, 291, \geq 43]]_8$	
		$*[[455, 297, \geq 44]]_8$		$[[455, 287, \geq 44]]_8$	
		$*[[455, 293, \geq 45]]_8$		$[[455, 283, \geq 45]]_8$	
		...		...	
		$*[[455, 273, \geq 50]]_8$		$[[455, 263, \geq 50]]_8$	
		$*[[455, 269, \geq 51]]_8$		$[[455, 259, \geq 51]]_8$	

QCs have better code rate than QCs obtained in Refs. [12,23–25] and QTCs listed in the code tables given by Yves Edel [33]. On the other hand, some of our QCs have larger maximum designed distances. For clarity, the previous results and some code comparisons are shown below. The following are the known conclusions for the case $m = 2$ given in Refs. [12,25].

Table 5 General comparisons of quantum codes with $n = \frac{q+1}{r}(q^2+1)$ over $\mathbb{F}_q$ for $q \geq 5$

$r = 1$	k in Theorem 2	k' [24]	k'' in [12]	δ
$q \equiv 3 \bmod 4 \geq 7$	$n - 4\delta + 6$	$n - 4\delta + 4$	$n - 4\delta + 4$	$[2, \frac{q+1}{r}]$
	$n - 4\delta + 6 + 4\lfloor \frac{(\delta-2)}{2(q+1)} \rfloor$	$< n - 4\delta + 6$	–	$[\frac{q+1}{r} + 1, \frac{(q+1)(q+3)}{4} + 1]$
	$n - 4\delta + 6 + 4\lfloor \frac{(\delta-2)}{2(q+1)} \rfloor$	–	–	$[\frac{(q+1)(q+3)}{4} + 2, q^2 + 1]$
$q \equiv 1 \bmod 4 \geq 9$	$n - 4\delta + 6$	$n - 4\delta + 4$	$n - 4\delta + 4$	$[2, \frac{q+1}{r}]$
	$n - 4\delta + 6 + 4\lfloor \frac{(\delta-2)}{2(q+1)} \rfloor$	$< n - 4\delta + 6$	–	$[\frac{q+1}{r} + 1, \frac{(q+1)^2}{4} + 1]$
	$n - 4\delta + 6 + 4\lfloor \frac{(\delta-2)}{2(q+1)} \rfloor$	–	–	$[\frac{(q+1)^2}{4} + 2, q^2 + 1]$
$2 \leq r \leq \frac{q+1}{2}$	k in Theorem 2	k' [25]	k'' in [12]	δ
q odd	$n - 4\delta + 6$	–	$n - 4\delta + 4$	$[2, \frac{q+1}{r}]$
	$n - 4\delta + 6 + 4\lfloor \frac{(\delta-2)r}{2(q+1)} \rfloor$	–	–	$[\frac{q+1}{r} + 1, \frac{q^2-1}{r}]$
	$n - \frac{4(q^2-1)}{r} + 2(q-2)$	$n - \frac{4(q^2-1)}{r}$	–	$\frac{q^2-1}{r} + 1$
	$n - \frac{4(q^2-1)}{r} + 2(q-2)$	–	–	$\frac{q^2-1}{r} + 2$

Table 6 General comparisons of quantum codes with $n=\frac{q-1}{b}(q^2+1)$ over $\mathbb{F}_q$ for $q\geq 5$

$b=1$	k in Theorems 3, 4 and 5	k' [23]	k'' in [12]	δ
$q\geq 5$ odd	$n-4\delta+6$	$n-4\delta+4$	$n-4\delta+4$	$[2,q-1]$
	$n-4\delta+6$	$n-4\delta+8$	–	$[q+1,2q-2]$
	$n-4\delta+10+4\lfloor\frac{\delta-2q}{2(q-1)}\rfloor$	$n-4\delta+8$	–	$[2q,(q-1)^2+2]$
$q\geq 8$ even	$n-4\delta+6$	$n-4\delta+4$	$n-4\delta+4$	$[2,q-1]$
	$n-4\delta+6$	$n-4\delta+8$	–	$[q+1,2q-2]$
	$n-4\delta+10+4\lfloor\frac{\delta-2q}{2(q-1)}\rfloor$	$n-4\delta+8$	–	$[2q,\frac{q^2+q}{2}+2]$
	$n-4\delta+10+4\lfloor\frac{\delta-2q}{2(q-1)}\rfloor$	$n-4\delta+10$	–	$[\frac{q^2+q}{2}+3,q^2-3q+4]$
	$n-4\delta+10+2(q-4)$	$n-4\delta+10$	–	$[q^2-3q+5,(q-1)^2+2]$
$2\leq b\leq\frac{q+1}{2}$	k in Theorems 3, 4 and 5	k' [25]	k''in [12]	δ
$q\geq 5$ odd	$n-4\delta+6$	–	$n-4\delta+4$	$[2,\frac{q-1}{b}]$
	$n-4\delta+6+4\lfloor\frac{(\delta-2)b}{2(q-1)}\rfloor$	–	–	$[\frac{q-1}{r}+1,\frac{(q-1)^2}{b}]$
	$n-\frac{4(q-1)^2}{b}+2(q-2)$	$n-\frac{4(q-1)^2}{b}$	–	$\frac{(q-1)^2}{b}+1$
	$n-\frac{4(q-1)^2}{b}+4\lfloor\frac{(\delta-2)b}{2(q-1)}\rfloor$	–	–	$\frac{(q-1)^2}{b}+2$
$q\geq 8$ even	$n-4\delta+6$	–	$n-4\delta+4$	$[2,\frac{q-1}{b}]$
	$n-4\delta+6+4\lfloor\frac{(\delta-2)b}{2(q-1)}\rfloor$	–	–	$[\frac{q-1}{r}+1,\frac{(q-1)^2}{b}-q+1]$
	$n-4\delta+10+2(q-b)$	–	–	$[\frac{(q-1)^2}{b}-q+2,\frac{(q-1)^2}{b}]$
	$n-\frac{4(q-1)^2}{b}+2(q-b)$	$n-\frac{4(q-1)^2}{b}$	–	$\frac{(q-1)^2}{b}+1$
	$n-\frac{4(q-1)^2}{b}+2(q-b-2)$	–	–	$\frac{(q-1)^2}{b}+2$

Table 7 Actual parameters of some quantum codes

	q, r	QCs in Theorem 2	CBCH codes	CBCH$^{\perp_h}$	Actual parameters of QCs
	$q = 3, r = 2$	$[[20, 14, \geq 3]]_3$	$[20, 17, 3]_9$	$[20, 3, 16]_9$	$[[20, 14, 3]]_3$
		$[[20, 10, \geq 4]]_3$	$[20, 15, 4]_9$	$[20, 5, 8]_9$	$[[20, 10, 4]]_3$
		–	–	–	–
		$[[20, 6, \geq 6]]_3$	$[20, 13, 6]_9$	$[20, 7, 8]_9$	$[[20, 6, 6]]_3$
	$q = 5, r = 3$	$[[52, 46, \geq 3]]_5$	$[52, 49, 3]_{25}$	$[52, 3, 48]_{25}$	$[[52, 46, 3]]_5$
		$[[52, 42, \geq 4]]_5$	$[52, 47, 4]_{25}$	$[52, 5, 24]_{25}$	$[[52, 42, 4]]_5$
		–	–	–	–
		$[[52, 38, \geq 6]]_5$	$[52, 45, 6]_{25}$	$[52, 7, 24]_{25}$	$[[52, 38, 6]]_5$
		$[[52, 34, \geq 7]]_5$	$[52, 43, 7]_{25}$	$[52, 9, 24]_{25}$	$[[52, 34, 7]]_5$
		$[[52, 30, \geq 8]]_5$	$[52, 41, 8]_{25}$	$[52, 11, 20]_{25}$	$[[52, 30, 8]]_5$
q	r, b	QCs in Theorem 5	BCH codes	BCH$^{\perp_h}$	Actual parameters of QCs
$q = 4$	$r = 1, b = 1$	$[[51, 45, \geq 3]]_4$	$[51, 48, 3]_{16}$	$[51, 3, 47]_{16}$	$[[51, 45, 3]]_4$
		$[[51, 41, \geq 4]]_4$	$[51, 46, 4]_{16}$	$[51, 5, 32]_{16}$	$[[51, 41, 4]]_4$
		$[[51, 37, \geq 5]]_4$	$[51, 44, 6]_{16}$	$[51, 7, 32]_{16}$	$[[51, 37, 6]]_4$
		$[[51, 33, \geq 6]]_4$	$[51, 42, 6]_{16}$	$[51, 9, 26]_{16}$	$[[51, 33, 6]]_4$
		–	–	–	–
		$[[51, 29, \geq 8]]_4$	$[51, 40, 8]_{16}$	$[51, 11, 26]_{16}$	$[[51, 29, 8]]_4$
		$[[51, 25, \geq 9]]_4$	$[51, 38, 9]_{16}$	$[51, 13, 26]_{16}$	$[[51, 25, 9]]_4$
		$[[51, 21, \geq 10]]_4$	$[51, 36, 10]_{16}$	$[51, 15, 26]_{16}$	$[[51, 21, 10]]_4$

Lemma 8 ([12]; Theorem 21) *Let $m = ord_n(q^2) = 2$, where q is a power of a prime and $2 \leq \delta \leq \delta_{max} = \frac{n}{q^2+1}$, then there exists a quantum code with parameters $[[n, n - 4\lfloor(\delta - 1)(1 - q^{-2})\rfloor, \geq \delta]]_q$.*

Lemma 9 ([25]; Theorem 9) *Let $q \geq 3$ be a prime power and n be an integer such that $\gcd(n, q^2) = 1$. Assume that $n = r(q^2 + 1)$, where $r \mid (q^2 - 1)$, $1 \leq r \leq \frac{q+1}{2}$. Then, there exists an $[[n, n - 4r(q - 1), d \geq r(q - 1) + 1]]_q$ quantum code.*

Remark Observe that our QCs have the same parameters with QTCs in [33] for $n = (q + 1)(q^2 + 1)$. Thus, we do not list them in the following tables although they are better than corresponding QCs in [12,24].

Tables 1, 2, 3 and 4 provide some examples and list code comparisons between QCs in Theorems 2, 3, 4, 5 and QTCs in [33] as well as QCs in Refs. [12,23–25], respectively. From these tables, it is easy to see that our QCs have better performance. Tables 5 and 6 list general code comparisons of lengths $n = \frac{q+1}{r}(q^2 + 1)$ and $n = \frac{q-1}{b}(q^2 + 1)$ for $q \geq 5$.

These symbols k, k' and k'' are denoted as the dimensions of QCs with given length and designed distance in corresponding references, respectively. Additionally, the QC marked with an asterisk "*" has the best parameters among the ones in every row. The symbol "—" implies that there is no QC with given length and designed distance. And "$\diamond$" denotes new QCs from our construction.

Utilizing the computer algebra system MAGMA [34], we calculated actual parameters of QCs $[[20, k_1, \geq \delta]]_3$, $[[52, k_2, \geq \delta]]_5$, $[[51, k_3, \geq \delta]]_4$ presented above, for details see Table 7. From this table, one can see all the QCs are non-degenerate, and actual distances of almost all QCs are equal to their designed distances except for the $[[51, 37, \geq 5]]_4$ code with actual distance 6.

Generally, it is a hard work to determine the minimum distances of these dual-containing codes, their dual codes and the actual parameters of QCs given in Theorems 2, 3, 4 and 5. Yet, we conjecture that all the QCs given in these theorems are non-degenerate, and this is a problem that needs further study.

Acknowledgements The authors are very grateful to the anonymous reviewers and the Associate Editor, Prof. Michael Frey, for their constructive comments and suggestions on our manuscript, which improve the manuscript significantly.

References

1. Shor, P.W.: Scheme for reducing decoherence in quantum computing memory. Phys. Rev. A **52**, R2493 (1995)
2. Steane, A.M.: Multiple particle interference and quantum error correction. Proc. R. Soc. Lond. A **452**, 2551–2577 (1996)
3. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via codes over GF (4). IEEE. Trans. Inf. Theory **44**, 1369–1387 (1998)
4. Gottesman, D.: Stabilizer codes and quantum error correction. Ph.D. Thesis, California Institute of Technology (1997)
5. Steane, A.M.: Enlargement of Calderbank–Shor–Steane quantum codes. IEEE. Trans. Inf. Theory **45**, 2492–2495 (1999)

6. Ashikhim, A., Knill, E.: Non-binary quantum stabilizer codes. IEEE. Trans. Inf. Theory **47**, 3065–3072 (2001)
7. Li, R., Li, X.: Binary construction of quantum codes of minimum distance three and four. IEEE Trans. Inf. Theory **50**, 1331–1336 (2004)
8. Ketkar, A., Klappenecker, A., Kumar, S.: Nonbinary stablizer codes over finite fields. IEEE Trans. Inf. Theory **52**, 4892–4914 (2006)
9. Ling, S., Luo, J., Xing, C.: Generalization of Steane's enlargement construction of quantum codes and applications. IEEE Trans. Inf. Theory **56**, 4080–4084 (2010)
10. Grassl, M., Beth, T.: Quantum BCH codes. In: Proceedings of Xth international symposium on theoretical. electrical engineering Magdeburg, pp 207–212 (1999)
11. Aly, S.A., Klappenecker, A., Sarvepalli, P.K.: Primitive quantum BCH codes over finite fields. In: Proceedings of international symposium on information theory, pp 1114–1118 (2006)
12. Aly, S.A., Klappenecker, A., Sarvepalli, P.K.: On quantum and classical BCH codes. IEEE. Trans. Inf. Theory **53**, 1183–1188 (2007)
13. La Guardia, G.G.: Constructions of new families of nonbinary quantum codes. Phys. Rev. A **80**, 042331 (2009)
14. Li, R., Zuo, F., Liu, Y.: A study of skew symmetric q^2-cyclotomic coset and its application. J. Air Force Eng. Univ. **12**(1), 87–89 (2011)
15. Li, R., Zuo, F., Liu, Y., Xu, Z.: Hermitian dual-containing BCH codes and construction of new quantum codes. Quantum Inf. Comput. **12**, 0021–0035 (2013)
16. Kai, X., Zhu, S.: Quantum negacyclic codes. Phys. Rev. A **88**, 012326 (2013)
17. Kai, X., Zhu, S., Li, P.: Constacyclic codes and some new quantum MDS cods. IEEE Trans. Inf. Theory **60**, 2080–2086 (2014)
18. Chen, B., Ling, S., Zhang, G.: Application of constacyclic codes to quantum MDS codes. IEEE Trans. Inf. Theory **61**, 1474–1484 (2015)
19. Guardia, G.G.La: On optimal constacyclic codes. Linear Algebra Appl. **496**, 594–610 (2016)
20. Wang, L., Zhu, S.: New quantum MDS codes derived from constacyclic codes. Quantum Inf. Process. **14**(3), 881–889 (2015). See also arXiv:1405:5421v1
21. Zhang, T., Ge, G.: Some new class of quantum MDS codes from constacyclic codes. IEEE Trans. Inf. Theory **61**, 5224–5228 (2015)
22. Liu, Y., Li, R., Lv, L., Ma, Y.: A class of constacyclic BCH codes and new quantum codes. Quantum Inf. Process. **16**(3), 1–16 (2017)
23. Yuan, J., Zhu, S., Kai, X., Li, P.: On the construction of quantum constacyclic codes. Des. Codes Cryptogr. **85**(1), 179–190 (2017)
24. Zhu, S., Sun, Z., Li, P.: A class of negacyclic BCH codes and its application to quantum codes. Des. Codes Cryptogr. **86**(10), 1–27 (2018)
25. Zhang, M., Li, Z., Xing, L., Tang, N.: Construction of some new quantum BCH codes. IEEE Access **4**, 36122 (2018)
26. Song, H., Li, R., Wang, J., Liu, Y.: Two classes of BCH codes and new quantum codes. Quantum Inf. Process. **17**(10), 1–24 (2018)
27. Aydin, N., Siap, I., Ray-Chaudhuri, D.K.: The structure of 1-generator quasi-twisted codes and new linear codes. Des. Codes Cryptogr. **24**, 313–326 (2001)
28. Krishna, A., Sarwate, D.V.: Pseudo-cyclic maximum-distance separable codes. IEEE Trans. Inf. Theory **36**, 880–884 (1990)
29. Peterson, W.W., Weldon, E.J.: Error-Correcting Codes. The M.I.T. Press, Cambridge (1972)
30. Macwilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, Amsterdam (1977)
31. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)
32. Sloane, N.J.A., Thompson, J.G.: Cyclic self-dual codes. IEEE Trans. Inf. Theory **29**, 364–366 (1983)
33. Yves Edel's homepage. https://www.mathi.uni-heidelberg.de/~yves/Matritzen/QTBCH/QTBCHIndex.html
34. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system I: the user language. J. Symb. Comput. **24**, 235–266 (1997)