Int J Theor Phys (2015) 54:92–99
DOI 10.1007/s10773-014-2204-8

Constructions of New Nonbinary Quantum Codes

Xueqin Hu · Guanghui Zhang · Bocong Chen

Received: 13 April 2014 / Accepted: 21 May 2014 / Published online: 7 June 2014

Abstract Two new families of good nonbinary quantum codes are constructed in this paper. The first one can be regarded as a generalization of [Theorem 3.2, X. Kai, S. Zhu and Y. Tang, Phys. Rev. A 88, 012326 (2013)], in the sense that we drop the constraint $q \equiv 1 \pmod{4}$. The later one is a quantum maximal-distance-separable (MDS) code. Compared the parameters of our quantum MDS codes with the parameters of quantum MDS codes available in the literature, the quantum MDS codes exhibited here have bigger minimum distance.

Keywords Quantum codes · Quantum MDS codes · Cyclotomic cosets · Constacyclic codes

1 Introduction

Errors caused by noise in quantum informational processes are inevitable. Fortunately, it was discovered that, under specific reasonable physical assumptions, quantum information can be protected by encoding it into a quantum error-correcting code [1]. Constructing quantum error-correcting codes is thus having important significance in theory and practice.

However, constructing quantum codes with good parameters is difficult, since it is not an easy task to determine the dimension and minimum distance of a quantum code. The first

X. Hu
School of Mathematical Sciences, Capital Normal University, Beijing, 100048, China
e-mail: sky9708@163.com

G. Zhang (✉)
School of Mathematical Sciences, Luoyang Normal University,Luoyang, Henan, 471022, China
e-mail: zghui2012@126.com

B. Chen
Division of Mathematical Sciences, School of Physical & Mathematical Sciences,
Nanyang Technological University, Singapore 637616, Singapore
e-mail: bocong_chen@yahoo.com

important quantum code construction is given in [2–4]. Calderbank et al. in [5] discovered that the construction of quantum codes can be diverted into finding classical self-orthogonal codes over $\mathbb{F}_2$ or $\mathbb{F}_4$ with respect to certain inner product.

After the realization that nonbinary quantum codes can use fault-tolerant quantum computation, the study of binary quantum codes was generalized to the nonbinary case. Ashikhmin and Knill [6] gave several methods of constructing nonbinary quantum codes. Ketkar et al. [7] obtained many classes of nonbinary quantum codes from classical linear codes. La Guardia [8] derived several families of nonbinary quantum codes from BCH codes. By using negacyclic codes, Chen et al. [9] established two families of asymmetric quantum codes.

Quantum maximum-distance-separable (MDS) codes are optimal in the sense that they beat the quantum Singleton bound. In recent years, constructing quantum MDS codes has become a hot research topic. Many classes of quantum MDS codes have been found by employing different methods (see [10–19]). La Guardia in [16] constructed a new class of quantum MDS codes through MDS cyclic codes. Recently, Kai et al. [11–13] constructed several classes of good nonbinary quantum codes from classical constacyclic codes, including some new classes of quantum MDS codes.

Motivated by the above works, two new families of good nonbinary quantum codes are constructed in this paper. The first one can be regarded as a generalization of [12, Theorem 3.2], in the sense that we drop the constraint $q \equiv 1 \pmod 4$. The later one is a class of quantum MDS codes. More specifically, we obtain two classes of q-ary quantum codes with parameters: (i) $[[n, n-4m\ell-2, \geq 2\ell+2]]_q$, where q is an odd prime power, $n = q^{2m}+1$ with $m \geq 2$, and $1 \leq \ell \leq q^2-1$; (ii) $\left[\left[\frac{q^2-1}{6}, \frac{q^2-1}{6}-2d+2, d\right]\right]_q$, where q satisfies $6 \mid (q+1)$ and $2 \leq d \leq \frac{2q-1}{3}$.

Compared the parameters of our quantum MDS codes with the parameters of quantum MDS codes available in the literature, the quantum MDS codes exhibited here have bigger minimum distance.

2 Preliminaries

In this section, we recall some basic notations and facts about quantum codes and constacyclic codes.

Throughout this paper, q denotes an odd prime power and $\mathbb{F}_{q^2}$ denotes the finite field with q^2 elements. We always assume that n is a positive integer relatively prime to q, i.e., $\gcd(n, q) = 1$. Given integers a, b and z, $a \mid b$ means that a divides b, and $a \equiv b \pmod z$ means $z \mid (a-b)$. Let $\mathbb{F}_{q^2}^n$ be the $\mathbb{F}_{q^2}$-vector space of n-tuples. A *linear code* of length n over $\mathbb{F}_{q^2}$ is an $\mathbb{F}_{q^2}$-subspace of $\mathbb{F}_{q^2}^n$. A linear code of length n over $\mathbb{F}_{q^2}$ is called an $[n, k, d]$ code if its dimension is k and minimum Hamming distance is d.

Given two n-tuples $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1}) \in \mathbb{F}_{q^2}^n$ and $\mathbf{y} = (y_0, y_1, \cdots, y_{n-1}) \in \mathbb{F}_{q^2}^n$, the *Hermitian inner product* is defined as

$$(\mathbf{x}, \mathbf{y})_H = x_0 y_0^q + x_1 y_1^q + \cdots + x_{n-1} y_{n-1}^q.$$

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

$$C^{\perp_H} = \left\{ \mathbf{x} \in \mathbb{F}_{q^2}^n \mid \sum_{i=0}^{n-1} x_i y_i^q = 0, \quad \text{for all } \mathbf{y} \in C \right\}.$$

If $C^{\perp_H} \subseteq C$, then C is called a (Hermitian) dual-containing code.

2.1 Quantum Codes

A q-ary quantum code Q of length n and size K is a K-dimensional subspace of the q^n-dimensional Hilbert space $(\mathbb{C}^q)^{\otimes n}$. Let $k = \log_q(K)$. We use $[[n, k, d]]_q$ to denote a q-ary quantum code of length n with size q^k and minimum distance d.

The parameters of an $[[n, k, d]]_q$ quantum code must satisfy the quantum Singleton bound (see [7] and [20]). (Quantum Singleton Bound): Let Q be a q-ary $[[n, k, d]]$ quantum code. Then $2d \leq n - k + 2$.

A quantum code achieving this quantum Singleton bound is called a *quantum maximum-distance-separable* (MDS) code. Ketkar et al. in [7] pointed out that, for any odd prime power q, if the classical MDS conjecture holds, then the length of nontrivial quantum MDS codes can not exceed $q^2 + 1$. Constructing quantum MDS codes has become one of the central topics for quantum codes in recent years. The following is one of the most frequently-used construction methods. (Hermitian Construction): If C is a q^2-ary $[n, k, d]$-linear code such that $C^{\perp_H} \subseteq C$, then there exists a q-ary quantum code with parameters $[[n, 2k - n, \geq d]]_q$. The Hermitian construction suggests that we can obtain q-ary quantum codes as long as we can construct classical dual-containing linear codes over $\mathbb{F}_{q^2}$. Constacyclic codes form an important class of linear code due to their good algebraic structures. In this paper, we will use the Hermitian construction to obtain quantum codes through constacyclic codes.

2.2 Constacyclic Codes

We adopt the notation in [13]. Let $\mathbb{F}_{q^2}^*$ denote the multiplicative group of nonzero elements of $\mathbb{F}_{q^2}$. For $\beta \in \mathbb{F}_{q^2}^*$ we denote by $\mathrm{ord}(\beta)$ the order of β in the group $\mathbb{F}_{q^2}^*$; then $\mathrm{ord}(\beta)$ is a divisor of $q^2 - 1$, and β is called a *primitive* $\mathrm{ord}(\beta)$*th root of unity*.

For $\lambda \in \mathbb{F}_{q^2}^*$, a linear code C of length n over $\mathbb{F}_{q^2}$ is said to be λ-*constacyclic* if C is an ideal of $\mathbb{F}_{q^2}[X]/\langle X^n - \lambda\rangle$. We then know that C is generated uniquely by a monic divisor $g(X)$ of $X^n - \lambda$; in this case, $g(X)$ is called the *generator polynomial* of C and we write $C = \langle g(X)\rangle$.

Let $\lambda \in \mathbb{F}_{q^2}^*$ be a primitive rth root of unity. Then there exists a primitive rnth root of unity (in some extension field of $\mathbb{F}_{q^2}$), say η, such that $\eta^n = \lambda$. The roots of $X^n - \lambda$ are precisely the elements η^{1+ri} for $0 \leq i \leq n - 1$. Set $\theta_{r,n} = \{1 + ri \,|\, 0 \leq i \leq n - 1\}$. The defining set of a constacyclic code $C = \langle g(X)\rangle$ of length n is the set $Z = \{j \in \theta_{r,n} \,|\, \eta^j \text{ is a root of } g(X)\}$. It is easy to see that the defining set Z is a union of some q^2-cyclotomic cosets modulo rn and $\dim_{\mathbb{F}_{q^2}}(C) = n - |Z|$ (see [13]).

The following results play important roles in constructing quantum codes from constacyclic codes. *The BCH bound for Constacyclic Codes: Let C be a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$, where λ is a primitive rth root of unity. Let η be a primitive rnth root of unity in an extension field of $\mathbb{F}_{q^2}$ such that $\eta^n = \lambda$. Assume the generator polynomial of C has roots that include the set $\left\{\eta^{1+ri} \,|\, i_1 \leq i \leq i_1 + d - 1\right\}$. Then the minimum distance of C is at least d (*[13, Theorem 2.1]*).* Let r be a positive divisor of $q + 1$ and let $\lambda \in \mathbb{F}_{q^2}^*$ be of order r. Assume that C is a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set Z. Then C is a dual-containing code if and only if $Z \bigcap Z^{-q} = \emptyset$, where $Z^{-q} = \{-qz(\mathrm{mod}\ rn) \,|\, z \in Z\}$ ([13, Lemma 2.2]).

3 Quantum Constacyclic Codes

In this section, we construct two families of q-ary quantum codes with good parameters through the Hermitian construction. Following [13], we call them *quantum constacyclic codes*.

3.1 Quantum Codes of Length $q^{2m}+1$

Using the Hermitian construction, we will obtain q-ary quantum codes of length $q^{2m}+1$ from constacyclic codes over $\mathbb{F}_{q^2}$, where $m \geq 2$ is a positive integer. The main result of this subsection extends [12, Theorem 3.2] in the sense that we do not assume that $q \equiv 1 \pmod 4$.

Let $n = q^{2m}+1$, where $m \geq 2$. Suppose $r = q+1$ and $s = \frac{n}{2}$. Let $\lambda \in \mathbb{F}_{q^2}$ be a primitive rth root of unity. We consider λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$. Now, $\theta_{r,n} = \{1+(q+1)i \mid 0 \leq i \leq n-1\}$. We claim that $s = \frac{n}{2} \in \theta_{r,n}$. To see this, note that

$$\frac{n}{2}-1 = \frac{q^{2m}-1}{2} = \frac{q^2-1}{2}\left(q^{2m-2}+q^{2m-4}+\cdots+q^2+1\right).$$

Thus,

$$\frac{n}{2} = 1+(q+1)\frac{q-1}{2}(q^{2m-2}+q^{2m-4}+\cdots+q^2+1).$$

Lemma 3.1 *Let $n = q^{2m}+1$, where $m \geq 2$. Let $r = q+1$ and $s = \frac{n}{2}$. Then $C_s = \{s\}$, where C_s denotes the q^2-cyclotomic coset modulo rn containing s.*

Proof It suffices to prove that $sq^2 \equiv s \pmod{rn}$. Since $rn = (q+1)\left(q^{2m}+1\right)$ divides $\frac{q^{2m}+1}{2}(q^2-1)$, it follows that $sq^2 = \frac{q^{2m}+1}{2}\cdot q^2 = \frac{q^{2m}+1}{2}(q^2-1+1) \equiv \frac{q^{2m}+1}{2} \pmod{rn}$. We are done. □

It is readily seen that $s > \frac{q^4-1}{2} > (q+1)\left(q^2-1\right) > 0$. The following result shows that $|C_{s-(q+1)i}| = 2m$ for any integer i with $1 \leq i \leq q^2-1$.

Lemma 3.2 *Let $n = q^{2m}+1$, where $m \geq 2$. Let $r = q+1$ and $s = \frac{n}{2}$. Then for any integer i with $1 \leq i \leq q^2-1$, the q^2-cyclotomic coset $C_{s-(q+1)i}$ modulo rn has cardinality $2m$.*

Proof Note that $rn = (q+1)\left(q^{2m}+1\right)$. We first show that $\mathrm{ord}_{rn}\left(q^2\right) = 2m$. Clearly, $rn > q^{2m}-1$, which implies that $\mathrm{ord}_{rn}(q^2) > m$. On the other hand, $\left(q^2\right)^{2m} \equiv 1 \pmod{rn}$. Thus, $\mathrm{ord}_{rn}(q)$ is a divisor of $2m$. Therefore, $\mathrm{ord}_{rn}(q^2) = 2m$ and $|C_{s-(q+1)i}|$ is a divisor of $2m$, for any $1 \leq i \leq q^2-1$.

To prove $|C_{s-(q+1)i}| = 2m$, it suffices to show that $|C_{s-(q+1)i}| > m$, i.e., $(s-(q+1)i)q^{2m} \not\equiv (s-(q+1)i)q^{2j} \pmod{rn}$ for any $0 \leq j \leq m-1$. Suppose otherwise that two integers i_0, j_0 such that $1 \leq i_0 \leq q^2-1$ and $0 \leq j_0 \leq m-1$ can be found such that $(s-(q+1)i_0)q^{2m} \equiv (s-(q+1)i_0)q^{2j_0} \pmod{rn}$. We then have $s-(q+1)i_0q^{2m} \equiv s-(q+1)i_0q^{2j_0} \pmod{rn}$, which gives $(q^{2j_0}+1)i_0 \equiv 0 \pmod n$. Since $n = q^{2m}+1 > q^{2m}-q^{2m-2}+q^2-1 = (q^{2m-2}+1)(q^2-1) \geq (q^{2j_0}+1)i_0$, we obtain a contradiction. □

Lemma 3.3 *Let $n = q^{2m}+1$, where $m \geq 2$. Let $r = q+1$ and $s = \frac{n}{2}$. Then for any integer i with $1 \leq i \leq q^2-1$, the q^2-cyclotomic cosets $C_{s-(q+1)i}$ modulo rn are distinct.*

Proof Suppose that two integers i, j with $1 \leq i \neq j \leq q^2 - 1$ can be found such that $C_{s-(q+1)i} = C_{s-(q+1)j}$. Then $s - (q+1)j \equiv (s - (q+1)i)q^{2t} \pmod{rn}$ for some integer t with $0 \leq t \leq 2m - 1$. It follows that

$$j \equiv iq^{2t} \pmod{n}. \tag{3.1}$$

Clearly, $t \neq 0$. If $1 \leq t \leq m-1$, then $iq^{2t} \leq (q^2-1)q^{2m-2} < q^{2m} + 1 = n$. Therefore, $j = iq^{2t}$ by (3.1). This is a contradiction, since $iq^{2t} \geq q^2 > q^2 - 1 \geq j$.

If $m \leq t \leq 2m-1$, then we write $t = m+h$, where $0 \leq h \leq m-1$. Thus, $q^{2t} = q^{2m} \cdot q^{2h}$. Since $q^{2m} \equiv -1 \pmod{n}$, one gets $j \equiv -iq^{2h} \pmod{n}$ by (3.1) again. This leads to $j = n - iq^{2h}$. From $j + iq^{2h} \leq (q^2-1) + (q^2-1)q^{2m-2} < n$, we get the desired contradiction. □

Lemma 3.4 *Let $n = q^{2m}+1$, where $m \geq 2$. Let $r = q+1$ and $s = \frac{n}{2}$. If C is a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set $Z = C_{s-(q+1)l} \bigcup C_{s-(q+1)(l-1)} \bigcup \cdots \bigcup C_s$, where $0 \leq l \leq q^2 - 1$, then C contains its Hermitian dual code.*

Proof Suppose otherwise that C does not contains its Hermitian dual code. We then know that $Z \bigcap Z^{-q} \neq \emptyset$. Hence, there exist two integers i, j with $0 \leq i, j \leq q^2 - 1$ and an integer h with $0 \leq h \leq 2m - 1$ such that

$$-q(s - (q+1)j) \equiv (s - (q+1)i)q^{2h} \pmod{rn},$$

After simplification, we obtain

$$\frac{n}{2} \equiv qj + iq^{2h} \pmod{n}. \tag{3.2}$$

If $h = 0$, then $\frac{n}{2} > q(q^2-1) + q^2 - 1 \geq qj + i$, contradicting $\frac{n}{2} = qj + i$. We obtain a contradiction.

If $1 \leq h \leq m-1$, then $qj + iq^{2h} \leq q(q^2-1) + (q^2-1)q^{2m-2} = q^{2m} + q^3 - q^{2m-2} - q$. At this point, two cases may occur: If $m \geq 3$, then $q^{2m} + q^3 - q^{2m-2} - q < n$; it follows from (3.2) that $\frac{n}{2} = qj + iq^{2h}$, or equivalently, $q^{2m} + 1 = 2qj + 2q^{2h}$; this is a contradiction, since we would obtain $q \mid 1$. If $m = 2$, then $h = 1$. As we did previously, it is impossible that $qj + iq^2 \leq q^4$. Thus, we assume that $qj + iq^2 > q^4$. Note that $qj + iq^2 < 2q^4$, which implies that $\frac{q^4+1}{2} = qj + iq^2 - (q^4+1)$. Then $3q^4 + 3 = 2qj + 2iq^2$. This is impossible, because $2qj + 2iq^2 \leq 2q(q^2-1) + 2q^2(q^2-1) < 3q^4$.

If $m \leq h \leq 2m-1$, then we write $h = m+t$, where $0 \leq t \leq m-1$. From (3.2) and the fact $q^{2m} \equiv -1 \pmod{n}$, we have $\frac{n}{2} + iq^{2t} \equiv qj \pmod{n}$. Since $\frac{n}{2} > qj$, we can assume that $\frac{n}{2} + iq^{2t} > n$. It is readily seen that $\frac{n}{2} + iq^{2t} < 2n$. We then have $\frac{n}{2} + iq^{2t} - n = qj$. Thus, $iq^{2t} = \frac{n}{2} + qj$, which implies that $t > 0$. Expanding this equation, we get $2iq^{2t} = q^{2m} + 1 + 2qj$. This is a contradiction, since we would obtain $q \mid 1$. □

Theorem 3.5 *Let $n = q^{2m} + 1$, where $m \geq 2$. For $1 \leq \ell \leq q^2 - 1$, there exists a quantum code with parameters $[[n, n - 4m\ell - 2, \geq 2\ell + 2]]_q$.*

Proof Let $r = q + 1$ and $s = \frac{n}{2}$. Assume that $\lambda \in \mathbb{F}_{q^2}$ is a primitive rth root of unity. Let C be a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set $Z = C_{s-(q+1)\ell} \bigcup C_{s-(q+1)(\ell-1)} \bigcup \cdots \bigcup C_s$, where $0 \leq \ell \leq q^2 - 1$. It follows from Lemma 3.4 that C contains it Hermitian dual code. Observe that $(s - (q+1)j)q^{2m} \equiv s + (q+1)j \pmod{rn}$ for any integer j, which implies $s + (q+1)j \in C_{s-(q+1)j}$. Hence, the defining set Z contains $2\ell + 1$ integers $s - (q+1)\ell, s - (q+1)(\ell-1), \cdots, s, s +$

$(q+1), \cdots, s+(q+1)\ell$. By the BCH bound for constacyclic codes, the minimum distance of C is at least $2l+2$. It follows from Lemma 3.1-Lemma 3.3 that C has parameters $[n, n-2ml-1, \geq 2l+2]$. By the Hermitian construction, we obtain a quantum code with parameters $[[n, n-4m\ell-2, \geq 2\ell+2]]_q$. □

Example 3.6 In Table 1, we list some quantum codes with parameters obtained from Theorem 3.5 for $q = 3, 5, 7, 9$ and 11.

3.2 New Quantum MDS Codes of Length $\frac{q^2-1}{6}$

Let q be an odd prime power such that $6 \mid (q+1)$. Let $n = \frac{q^2-1}{6}$ and $r = 6$. It is readily seen that every q^2-cyclotomic coset modulo rn contains exactly one element. Let $\lambda \in \mathbb{F}_{q^2}$ be a primitive rth root of unity.

Let C be a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set

$$Z = \left\{1 + 6i \left(\bmod\ q^2-1\right) \,\middle|\, \frac{q+1}{3} \leq i \leq q-2\right\}. \tag{3.3}$$

It is easy to see that $0 < q-2 < n$, which gives that $|Z| = \frac{2q-4}{3}$ and that C is an MDS λ-constacyclic code with parameters $\left[\frac{q^2-1}{6}, \frac{q^2-1}{6} - \frac{2q-4}{3}, \frac{2q-1}{3}\right]$. The following result shows that C satisfies $Z \bigcap Z^{-q} = \emptyset$.

Lemma 3.7 *If C is a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set Z defined in (3.3), then C is a dual-containing code.*

Proof If $q = 5$ then $Z = \{13, 19\}$ and $Z^{-q} = \{1, 7\}$, which shows that $Z \bigcap Z^{-q} = \emptyset$. If $q = 11$ then $Z = \{25, 31, 37, 43, 49, 55\}$ and $Z^{-q} = \{7, 19, 61, 73, 85, 115\}$. It is readily seen that $Z \bigcap Z^{-q} = \emptyset$. We can assume, therefore, that $q \geq 17$.

Suppose otherwise that $Z \bigcap Z^{-q} \neq \emptyset$. Then, we can find two integers i, j with $\frac{q+1}{3} \leq i, j \leq q-2$ such that

$$-q\big(1+6i\big) \equiv 1 + 6j \ (\bmod\ q^2-1). \tag{3.4}$$

We will obtain a contradiction by considering the following cases:

(1) $\frac{q+1}{3} \leq i \leq \frac{2(q+1)}{3} - 1$. Let $i = \frac{q+1}{6}\ell + k$, where ℓ, k are nonnegative integers with $k \leq \frac{q+1}{6} - 1$. From $\frac{q+1}{3} \leq i \leq \frac{2q-1}{3}$, ℓ must be equal to 2 or 3. It is easy to see that $-q(1+6i) = -q - q^2\ell - q\ell - 6qk$. It follows from (3.4) that

$$-q - \ell - q\ell - 6qk \equiv 1 + 6j \ (\bmod\ q^2-1). \tag{3.5}$$

Table 1 Quantum constacyclic codes

q	m	n	$[[n,k,d]]_q$	ℓ
3	2	82	$[[82, 82-8\ell-2, \geq 2\ell+2]]_3$	$1 \leq \ell \leq 8$
5	2	626	$[[626, 626-8\ell-2, \geq 2\ell+2]]_5$	$1 \leq \ell \leq 24$
7	2	2402	$[[2402, 2402-8\ell-2, \geq 2\ell+2]]_7$	$1 \leq \ell \leq 48$
9	2	6562	$[[6562, 6562-8\ell-2, \geq 2\ell+2]]_9$	$1 \leq \ell \leq 80$
11	2	14642	$[[14642, 14642-8\ell-2, \geq 2\ell+2]]_{11}$	$1 \leq \ell \leq 120$

If $0 \leq k \leq \frac{q+1}{6}-2$, we want to prove that $q^2-1-q-\ell-q\ell-6qk > 1+6j$. To see this, it suffices to show that $1+6j+1+q+\ell+q\ell+6qk < q^2$. Indeed, $1+6j+1+q+\ell+q\ell+6qk \leq 1+6(q-2)+1+q+3+3q+6q\left(\frac{q+1}{6}-2\right) = q^2-q-7 < q^2$. Clearly, $1+6j < q^2-1$, and so $q^2-1-q-\ell-q\ell-6qk = 1+6j$ by (3.5). This is impossible.

If $k = \frac{q+1}{6}-1$, then $-q-\ell-q\ell-6qk = -q-\ell-q\ell-q^2-q+6q$. If follows from (3.5) that

$$4q-\ell-q\ell-1 \equiv 1+6j \pmod{q^2-1}.$$

Recall that $\ell \in \{2, 3\}$, and so $0 < 4q-\ell-q\ell-1 < q^2-1$. By (3.5) again, we have $4q-\ell-q\ell-1 = 1+6j$. However, $1+6j+\ell+q\ell+1 \geq 1+6\cdot\frac{q+1}{3}+2+2q+1 = 4q+6 > 4q$, which is a contradiction.

(2) $\frac{2q+2}{3} \leq i \leq \frac{5q-7}{6}$. Recall that $q \geq 17$, and so $\frac{5q-7}{6} > \frac{2q+2}{3}$. Simple computations show that $-5q^2+6q \leq -q(1+6i) \leq -4q^2-5q$, which gives $6q-5 \leq 5(q^2-1)-q(1+6i) \leq q^2-5q-5$. From (3.4), one gets $5(q^2-1)-q(1+6i) = 1+6j$. However, $1+6j \leq 1+6(q-2) < 6q-5$, which gives a contradiction.

(3) $\frac{5q-1}{6} \leq i \leq q-2$. As we did previously, $-6q^2+11q \leq -q(1+6i) \leq -5q^2$, and hence $11q-6 \leq 6(q^2-1)-q(1+6i) \leq q^2-6$. We then have $6(q^2-1)-q(1+6i) = 1+6j$. But $1+6j \leq 6q-11 < 11q-6$. This is a contradiction.

□

Theorem 3.8 *Let q be an odd prime power with $6 \mid (q+1)$. Then there exist quantum MDS codes with parameters $\left[\left[\frac{q^2-1}{6}, \frac{q^2-1}{6}-2d+2, d\right]\right]_q$, where $2 \leq d \leq \frac{2q-1}{3}$.*

Proof Let $n = \frac{q^2-1}{6}$ and $r = 6$. Let $\lambda \in \mathbb{F}_{q^2}$ be a primitive sixth root of unity. Recall that every q^2-cyclotomic coset modulo rn contains precisely one element. We assume that $\mathcal{C}_\delta$ is a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set

$$\mathcal{Z}_\delta = \left\{1+6\left(i+\frac{q+1}{3}\right)\left(\bmod\ q^2-1\right)\Big|\, 0 \leq i \leq \delta-1\right\}.$$

where δ is a positive integer with $1 \leq \delta \leq \frac{2q-4}{3}$. It follows from Lemma 3.7 and $\mathcal{Z}_\delta \subseteq Z$ that $\mathcal{C}_\delta$ is a dual-containing code with parameters $[n, n-d+1, d]_{q^2}$, where d is a positive integer with $2 \leq d \leq \frac{2q-1}{3}$. Using the Hermitian construction and the quantum Singleton bound, we can obtain a quantum MDS code with parameters $\left[\left[\frac{q^2-1}{6}, \frac{q^2-1}{6}-2d+2, d\right]\right]_q$.

□

Example 3.9 In Table 2, we list some quantum MDS codes with parameters obtained from Theorem 3.8 for $q = 11, 17, 23$ and 29.

Table 2 Quantum MDS codes

q	$[[n,k,d]]_q$	d
11	$[[20, 20-2d+2, d]]_{11}$	$2 \leq d \leq 7$
17	$[[48, 48-2d+2, d]]_{17}$	$2 \leq d \leq 11$
23	$[[88, 88-2d+2, d]]_{23}$	$2 \leq d \leq 15$
29	$[[140, 140-2d+2, d]]_{29}$	$2 \leq d \leq 19$

4 Code Comparisons

In this section, we compare the parameters of quantum codes available in the literature with the quantum constacyclic codes given in Section 3. We mention that [21, Table 1] collects the known quantum MDS codes in the literature.

• Comparing the quantum constacyclic code given in Theorem 3.5 with the one given in [12] (Construction II), we see that our construction of quantum codes in Section 3 is new when we take $q \equiv -1 \pmod 4$.

• The quantum MDS codes given in Section 3 have length $\frac{q^2-1}{6}$ and minimum distance $d \leq \frac{2q-1}{3}$, where q satisfies $6 \mid (q+1)$ (for example, we can take $q = 23$, so $n = 88$ and $d = 15$). We calculate the code lengths from Class 1 to Class 20 as listed in [21, Table 1] to see which classes can achieve the length 88. After easy computations, we see that only the length of Classes 3, 8 and 12 can achieve 88 when $q = 23$. In Class 3, $88 = 4 \times 23 - 4$ and $d \leq 11$; in Class 8, $d \leq 3$; in Class 12, $88 = \frac{23^2-1}{6}$ with $6 \mid (23+1)$ and $d \leq 12$. We then know that $n = 88$ and $d \leq 15$ is a new quantum MDS code, and so the quantum MDS codes given in Section 3 contain new codes that are not covered in the literature.

Acknowledgments The authors would like to thank the referees for a very meticulous reading of this manuscript. The second author is supported by NSFC (Grant No. 11171370), the Youth Backbone Teacher Foundation of Henan's University (Grant No. 2013GGJS-152), and Science and Technology Development Program of Henan Province in 2014 (144300510051). The research of the third author is partially supported by NSFC (Grant No. 11271005) and Nanyang Technological University's research grant number M4080456.

References

1. Shor, P.W.: In Proceedings of the 35th Annual Symposium on the Foundations of Computer Science (1994). arXiv:quantph/9508027
2. Steane, A.M.: Rev, Phys. Lett. **77**, 793 (1996)
3. Calderbank, A.R., Shor, P.W.: Phys. Rev. A **54**, 1098 (1996)
4. Steane, A.M.: Roy, Proc. Soc. Lond. A **452**, 2551 (1996)
5. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: IEEE Trans. Inf. Theory **44**, 1369 (1998)
6. Ashikhmin, A., Knill, E.: IEEE Trans. Inf. Theory **47**, 3065 (2001)
7. Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.K.: IEEE Trans. Inf. Theory **52**, 4892 (2006)
8. La Guardia, G.G.: Rev, Phys. A **042331**, 80 (2009)
9. Chen, J., Li, J., Lin, J.: Int. J. Theor. Phys **53**, 72 (2014)
10. Li, Z., Xing, L.J., Wang, X.M.: Phys. Rev. A, vol. 77, p. 012308 (2008)
11. Kai, X., Zhu, S.: IEEE Trans. Inf. Theory **59**, 1193 (2013)
12. Kai, X., Zhu, S., Tang, Y.: Phys. Rev. A **012326**, 88 (2013)
13. Kai, X., Zhu, S., Li, P.: IEEE Trans. Inf. Theory **60**, 2080 (2014)
14. Li, R., Xu, Z.: Phys. Rev. A **052316**, 82 (2010)
15. Jin, L., Ling, S., Luo, J., Xing, C.: IEEE Trans. Inform. Theory **56**, 4735 (2010)
16. Guardia, G.G.L.: IEEE, Trans. Inf Theory **57**, 5551 (2011)
17. Jin, L., Xing, C.: IEEE Trans. Inform. Theory **58**, 5484 (2012)
18. Ezerman, M.F., Jitman, S., Ling, S., Pasechnik, D.V. IEEE Trans. Inf. Theory **59**, 6732 (2013)
19. Jin, J., Xing, C.: IEEE Trans. Inf. Theory **60**, 2921 (2014)
20. Knill, E., Laflamme, R.: Phys. Rev. A **55**, 900 (1997)
21. Chen, B., Ling, S. G. Zhang (2014). arXiv:1403.2499