Some New Classes of Quantum MDS Codes From Constacyclic Codes

Tao Zhang and Gennian Ge

***Abstract*— Quantum maximum-distance-separable (MDS) codes form an important family of quantum codes. In this paper, using Hermitian construction and classical constacyclic codes, we construct six classes of quantum MDS codes. Two of these six classes of quantum MDS codes have larger minimum distance than the ones available in the literature. Most of these quantum MDS codes are new in the sense that their parameters are not covered by the codes available in the literature.**

***Index Terms*— Quantum MDS codes, constacyclic codes, Hermitian construction, cyclotomic cosets.**

I. Introduction

QUANTUM codes were introduced to protect quantum information from decoherence during quantum computations. After the pioneering works in [5], [21], and [22], the theory of quantum codes has developed rapidly. One of these constructions shows that the construction of quantum codes can be reduced to the classical linear codes with certain self-orthogonality properties. Recently, many quantum codes are constructed by classical linear codes with Euclidean or Hermitian self-orthogonality [1], [7], [23]. The quantum codes obtained by using self-orthogonality are called stabilizer codes.

Let q be a prime power. A q-ary quantum code Q of length n and size K is a K-dimensional subspace of the q^n-dimensional Hibert space $(\mathbb{C}^q)^{\otimes n} \cong \mathbb{C}^{q^n}$. We use $[[n,k,d]]_q$ to denote a q-ary quantum code of length n with size q^k and minimum distance d. As in classical coding theory, one of the central tasks in quantum coding theory is to construct good quantum codes. The following theorem gives a bound on the achievable minimum distance of a quantum code.

Theorem 1 ([16], [17] Quantum Singleton Bound): Quantum codes with parameters $[[n,k,d]]_q$ satisfy

$$k \leq n - 2d + 2.$$

Manuscript received November 1, 2014; revised March 12, 2015; accepted June 24, 2015. Date of publication June 26, 2015; date of current version August 14, 2015. This work was supported by the Zhejiang Provincial Natural Science Foundation of China under Grant LZ13A010001. G. Ge was supported in part by the National Natural Science Foundation of China under Grant 61171198 and Grant 11431003, in part by the Importation and Development of High-Caliber Talents Project of Beijing Municipal Institutions, and in part by the Scientific and Technological Innovation Capacity Enhancement Program of Beijing Municipal Institutions.

T. Zhang is with the School of Mathematical Sciences, Zhejiang University, Hangzhou 310027, China (e-mail: tzh@zju.edu.cn).

G. Ge is with the School of Mathematical Sciences, Capital Normal University, Beijing 100048, China, and also with the Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing 100048, China (e-mail: gnge@zju.edu.cn).

Communicated by M. Grassl, Associate Editor for Quantum Information Theory.

Digital Object Identifier 10.1109/TIT.2015.2450235

A quantum code achieving this bound is called a quantum maximum-distance-separable (MDS) code. Just as in the classical linear codes, quantum MDS codes form an important family of quantum codes. Constructing quantum MDS codes has become a central topic for quantum codes in recent years. Many classes of quantum MDS codes have been constructed by different methods (see [4], [8], [12], [13]). The following theorem is one of the most frequently used construction methods.

Theorem 2 ([2] 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 $[[n, 2k-n, \geq d]]$-quantum code.

As we know, if the classical MDS conjecture holds, then the length of nontrivial q-ary stabilizer quantum MDS codes cannot exceed q^2+1 [16]. The quantum MDS codes of length up to $q+1$ have been constructed for all possible dimensions [9], [10], and many quantum MDS codes of length between $q+1$ and q^2+1 have also been obtained (see [4], [11]–[15], [18]–[20], [24], [26] and the references therein). However, there are still a lot of quantum MDS codes difficult to be constructed. Moreover, it is a great challenge to construct quantum MDS codes with relatively large minimum distance. As mentioned in [13], except for some sparse lengths, almost all known q-ary quantum MDS codes have minimum distance less than or equal to $\frac{q}{2}+1$.

In this paper, we construct several classes of quantum MDS codes as follows:

(1) Let q be an odd prime power of the form $10m+3$, then there exists a q-ary $[[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 2, d]]$-quantum MDS code, where $2 \leq d \leq 6m+2$ is even.
(2) Let q be an odd prime power of the form $10m+7$, then there exists a q-ary $[[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 2, d]]$-quantum MDS code, where $2 \leq d \leq 6m+4$ is even.
(3) Let q be an odd prime power of the form $2tm+1$, then there exists a q-ary $[[\frac{q^2-1}{2t}, \frac{q^2-1}{2t} - 2d + 2, d]]$-quantum MDS code, where $2 \leq d \leq (t+1)m+1$.
(4) Let q be an odd prime power of the form $30m+11$, then there exists a q-ary $[[\frac{q^2-1}{30}, \frac{q^2-1}{30} - 2d + 2, d]]$-quantum MDS code, where $2 \leq d \leq 8m+3$.
(5) Let q be an odd prime power of the form $30m+19$, then there exists a q-ary $[[\frac{q^2-1}{30}, \frac{q^2-1}{30} - 2d + 2, d]]$-quantum MDS code, where $2 \leq d \leq 8m+5$.
(6) Let q be an odd prime power of the form $12m+5$, then there exists a q-ary $[[\frac{q^2-1}{12}, \frac{q^2-1}{12} - 2d + 2, d]]$-quantum MDS code, where $2 \leq d \leq 5m+2$.

The first two classes of quantum MDS codes have larger minimum distance than that of quantum MDS codes constructed in [15]. And the third class is a generalization of the three classes of quantum MDS codes obtained in [15]. The other three classes are quantum MDS codes whose lengths have the form $n = \frac{q^2-1}{2t_1t_2}$, where $(2t_1)|(q-1)$ and $t_2|(q+1)$. Most of these quantum MDS codes are new in the sense that their parameters are not covered by the codes available in the literature. We also mention that the quantum MDS codes given by (1) (resp. (2)) have minimum distance $d > \frac{q}{2}+1$ when $q > 3$ (resp. $q > 7$), and the quantum MDS codes given by (3) have minimum distance $d > \frac{q}{2}+1$ for any odd prime power q.

This paper is organized as follows. In Section II we present definitions and basic results about constacyclic codes. In Section III, we give some new classes of quantum MDS codes.

II. Preliminaries

Let $\mathbb{F}_{q^2}$ be the finite field with q^2 elements, where q is a prime power. A linear code of length n over $\mathbb{F}_{q^2}$ is a subspace of $\mathbb{F}_{q^2}^n$. Given two vectors $x = (x_0, x_1, \cdots, x_{n-1})$, $y = (y_0, y_1, \cdots, y_{n-1}) \in \mathbb{F}_{q^2}^n$, the Hermitian inner product is defined by

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

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

$$C^{\perp H} = \{x \in \mathbb{F}_{q^2}^n | \langle x, y\rangle = 0 \text{ for all } y \in C\}$$

is called its Hermitian dual code. A linear code C of length n over $\mathbb{F}_{q^2}$ is called Hermitian self-orthogonal if $C \subseteq C^{\perp H}$, and it is called Hermitian self-dual if $C = C^{\perp H}$.

In the following of this section, we always assume that $\gcd(n, q) = 1$. For $\eta \in \mathbb{F}_{q^2}^*$, a q^2-ary linear code C of length n is called η-constacyclic if it is invariant under the η-constacyclic shift of $\mathbb{F}_{q^2}^n$:

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

If we identify each codeword $c = (c_0, c_1, \cdots, c_{n-1})$ with its polynomial representation $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$, then an η-constacyclic code C of length n over $\mathbb{F}_{q^2}$ is identified with an ideal of the quotient ring $\mathbb{F}_{q^2}[x]/\langle x^n - \eta\rangle$, and $xc(x)$ corresponds to an η-constacyclic shift of $c(x)$. Moreover, $\mathbb{F}_{q^2}[x]/\langle x^n - \eta\rangle$ is a principal ideal ring, and C is generated by a monic divisor $g(x)$ of $x^n - \eta$. In this case, $g(x)$ is called the generator polynomial of C and we write $C = \langle g(x)\rangle$. If $\eta = -1$, then we call such a code by negacyclic code.

Let $\eta \in \mathbb{F}_{q^2}$ be a primitive rth root of unity. Since $\gcd(n, q) = 1$, there exists a primitive (rn)-th root of unity ω in some extension field of $\mathbb{F}_{q^2}$ such that $\omega^n = \eta$. It can be verified that

$$x^n - \eta = \prod_{i=0}^{n-1}(x - \omega^{1+ir}).$$

Let $\Omega = \{1 + ir | 0 \le i \le n-1\}$. For each $j \in \Omega$, let C_j be the q^2-cyclotomic coset modulo rn containing j. Let C be an η-constacyclic code of length n over $\mathbb{F}_{q^2}$ with generator polynomial $g(x)$. Then the set $Z = \{j \in \Omega | g(\omega^j) = 0\}$ is called the defining set of C. We can see that the defining set of C is a union of some q^2-cyclotomic cosets modulo rn and $\dim(C) = n - |Z|$. We can also obtain that $C^{\perp H}$ has defining set $Z^{\perp H} = \{j \in \Omega | -qj \pmod{rn} \notin Z\}$.

Similar to cyclic codes, there exists the following BCH bound for constacyclic codes.

Theorem 3 ([3], [25] The BCH Bound for Constacyclic Codes): Let C be an η-constacyclic code of length n over $\mathbb{F}_{q^2}$, where η is a primitive rth root of unity. Let ω be a primitive (rn)-th root of unity in an extension field of $\mathbb{F}_{q^2}$ such that $\omega^n = \eta$. Assume the generator polynomial of C has roots that include the set $\{\omega^{1+ri} | i_1 \le i \le i_1 + d - 2\}$. Then the minimum distance of C is at least d.

The following lemma presents a criterion to determine whether or not an η-constacyclic code of length n over $\mathbb{F}_{q^2}$ contains its Hermitian dual code.

Lemma 4 [15]: Let r be a positive divisor of $q+1$ and $\eta \in \mathbb{F}_{q^2}^*$ be of order r. Let C be an η-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set $Z \subseteq \Omega$, then C contains its Hermitian dual code if and only if $Z \bigcap (-qZ) = \emptyset$, where $-qZ = \{-qz \pmod{rn} | z \in Z\}$.

III. New Quantum MDS Codes

A. New Quantum MDS Codes of Length $\frac{q^2+1}{5}$

Let q be an odd prime power of the form $10m+3$ or $10m+7$, where m is a positive integer. Let $n = \frac{q^2+1}{5}$, $r = q+1$ and $\eta \in \mathbb{F}_{q^2}$ be a primitive rth root of unity. Now, we consider η-constacyclic codes of length n over $\mathbb{F}_{q^2}$ to construct quantum codes. First, we recall the following lemma.

Lemma 5 [15]: Let $n = \frac{q^2+1}{5}$, $s = \frac{q^2+1}{2}$ and $r = q+1$. Then $\Omega = \{1 + ri | 0 \le i \le n-1\}$ is a disjoint union of q^2-cyclotomic cosets:

$$\Omega = C_s \bigcup C_{s+n(q+1)/2} \bigcup \Big(\bigcup_{j=1}^{n/2-1} C_{s-(q+1)j}\Big),$$

where $C_s = \{s\}$, $C_{s+n(q+1)/2} = \{s + n(q+1)/2\}$ and $C_{s-(q+1)j} = \{s - (q+1)j, s + (q+1)j\}$ for $1 \le j \le n/2 - 1$.

Lemma 6:

1) *Suppose q is an odd prime power of the form $10m+3$, where m is a positive integer. If C is an η-constacyclic code of length $n = \frac{q^2+1}{5}$ over $\mathbb{F}_{q^2}$ with defining set $Z = \bigcup_{j=0}^{\delta} C_{s-(q+1)j}$, where η is a primitive rth root of unity and $0 \le \delta \le 3m$, then $C^{\perp H} \subseteq C$.*
2) *Suppose q is an odd prime power of the form $10m+7$, where m is a positive integer. If C is an η-constacyclic code of length $n = \frac{q^2+1}{5}$ over $\mathbb{F}_{q^2}$ with defining set $Z = \bigcup_{j=0}^{\delta} C_{s-(q+1)j}$, where η is a primitive rth root of unity and $0 \le \delta \le 3m+1$, then $C^{\perp H} \subseteq C$.*

Proof: In the following, we only prove the first part. The second part can be handled similarly. We fix $q = 10m+3$ and $0 \le \delta \le 3m$. By Lemma 4, it is sufficient to prove $Z \bigcap (-qZ) = \emptyset$. Suppose there exist integers $0 \le i \le j \le \delta$ such that $C_{s-(q+1)i} = -qC_{s-(q+1)j}$.

Case 1: $s-(q+1)i \equiv -q(s-(q+1)j) \pmod{(q+1)n}$. After routine computations, we have

$$\frac{q^2+1}{2} \equiv i+qj \pmod{\frac{q^2+1}{5}}.$$

Since $q = 10m+3$, we obtain

$$10m^2+6m+1 \equiv i+(10m+3)j \pmod{20m^2+12m+2}.$$

Note that $0 \le i+(10m+3)j \le 3m+30m^2+9m < 3(10m^2+6m+1)$, we get that

$$10m^2+6m+1 = i+(10m+3)j,$$

that is

$$i = 10m^2+6m+1-(10m+3)j.$$

If $j \le m$, then $i \ge 3m+1$, which is a contradiction.

If $j \ge m+1$, then $i \le -7m-2$, which is also a contradiction.

Case 2: $s-(q+1)i \equiv -q(s+(q+1)j) \pmod{(q+1)n}$. In this case, we have

$$\frac{q^2+1}{2} \equiv i-qj \pmod{\frac{q^2+1}{5}}.$$

Since $q = 10m+3$, we get

$$10m^2+6m+1 \equiv i-(10m+3)j \pmod{20m^2+12m+2}.$$

We can verify that $3m \ge i-(10m+3)j \ge -30m^2-9m > -3(10m^2+6m+1)$, which implies

$$-(10m^2+6m+1) = i-(10m+3)j,$$

consequently,

$$i = (10m+3)j-(10m^2+6m+1).$$

If $j \le m$, then $i \le -3m-1$, we have reached a contradiction.

If $j \ge m+1$, then $i \ge 7m+2$, we have again reached a contradiction. ■

Theorem 7:

(1) *Let q be an odd prime power of the form $10m+3$, then there exists a q-ary $[[\frac{q^2+1}{5}, \frac{q^2+1}{5}-2d+2, d]]$-quantum MDS code, where $2 \le d \le 6m+2$ is even.*

(2) *Let q be an odd prime power of the form $10m+7$, then there exists a q-ary $[[\frac{q^2+1}{5}, \frac{q^2+1}{5}-2d+2, d]]$-quantum MDS code, where $2 \le d \le 6m+4$ is even.*

Proof: Note that every q^2-cyclotomic coset has two elements except C_s and $C_{s+n(q+1)/2}$, then by the Hermitian construction and Lemma 6, the conclusion follows. ■

Remark 8: In [15], Kai et al. constructed two classes of quantum MDS codes.

(1) *If q is an odd prime power of the form $20m+3$ or $20m+7$, then there exists a q-ary $[[\frac{q^2+1}{5}, \frac{q^2+1}{5}-2d+2, d]]$-quantum MDS code, where $2 \le d \le \frac{q+5}{2}$ is even.*

(2) *If q is an odd prime power of the form $20m-3$ or $20m-7$, then there exists a q-ary $[[\frac{q^2+1}{5}, \frac{q^2+1}{5}-2d+2, d]]$-quantum MDS code, where $2 \le d \le \frac{q+3}{2}$ is even.*

Obviously, our result has larger minimum distance.

Example 9:

1) *Let $q = 43$, applying Theorem 7 (1) produces a new quantum MDS code with parameters $[[370, 320, 26]]_{43}$.*
2) *Let $q = 37$, applying Theorem 7 (2) produces a new quantum MDS code with parameters $[[274, 232, 22]]_{37}$.*

B. New Quantum MDS Codes of Length $\frac{q^2-1}{2t}$

Let q be an odd prime power of the form $2tm+1$. Let $n = \frac{q^2-1}{2t}$ and $r = 2$. Since $2n|(q^2-1)$, then for each odd i in the range $1 \le i \le 2n$, the q^2-cyclotomic coset C_i modulo $2n$ is $C_i = \{i\}$.

Lemma 10: Let q be an odd prime power of the form $2tm+1$ and $n = \frac{q^2-1}{2t}$. If C is a q^2-ary negacyclic code of length n with defining set $Z = \bigcup_{j=0}^{\delta} C_{1+2j}$, where $0 \le \delta \le (t+1)m-1$, then $C^{\perp H} \subseteq C$.

Proof: By Lemma 4, it is sufficient to prove $Z \bigcap (-qZ) = \emptyset$. Suppose there exist integers $0 \le i \le j \le \delta$ such that $C_{1+2i} = -qC_{1+2j}$, that is

$$1+2i \equiv -q(1+2j) \pmod{\frac{q^2-1}{t}}.$$

Since $q = 2tm+1$, we have

$$(2tm+1)(1+2j)+1+2i \equiv 0 \pmod{4tm^2+4m}.$$

Note that $0 < (2tm+1)(1+2j)+1+2i < (t+1)(4tm^2+4m)$, we get

$$(2tm+1)(1+2j)+1+2i = x(4tm^2+4m),$$

where $1 \le x \le t$. Equivalently,

$$1+2i = x(4tm^2+4m)-(2tm+1)(1+2j).$$

If $j \ge mx$, then $1+2i \le 2mx-2mt-1 < 0$, a contradiction.

If $j \le mx-1$, then $1+2i \ge 2mx+2mt+1$, this is a contradiction. ■

Theorem 11: Let q be an odd prime power of the form $2tm+1$, then there exists a q-ary $[[\frac{q^2-1}{2t}, \frac{q^2-1}{2t}-2d+2, d]]$-quantum MDS code, where $2 \le d \le (t+1)m+1$.

Proof: Note that every q^2-cyclotomic coset has exactly one element, then by the Hermitian construction and Lemma 10, the conclusion follows. ■

Remark 12: Let $t = 1$ and $q = 2m+1$. Applying Theorem 11, there exists a q-ary $[[\frac{q^2-1}{2}, \frac{q^2-1}{2}-2d+2, d]]$-quantum MDS code, where $2 \le d \le q$. This result was obtained in [15].

Remark 13: Let m be an odd integer and $q = 2tm+1$. By Theorem 11, there exists a q-ary $[[m(q+1), m(q+1)-2d+2, d]]$-quantum MDS code, where $2 \le d \le (t+1)m+1$. This result was obtained in [15].

Remark 14: Let $q \equiv 1 \pmod 4$: Suppose m is an odd integer and $q = 4tm+1$. By Theorem 11, there exists a q-ary $[[2m(q+1), 2m(q+1)-2d+2, d]]$-quantum MDS code, where $2 \le d \le 2(t+1)m+1$. This code was constructed in [15] as well.

Example 15: Let $q = 17$, $t = 2$, $m = 4$, applying Theorem 11 produces new quantum MDS codes with parameters $[[72, 74-2d, d]]_{17}$, where $2 \le d \le 13$.

Remark 16: Theorem 11 was also obtained independently in [6].

C. New Quantum MDS Codes of Length $\frac{q^2-1}{2t_1t_2}$

In this subsection, we construct some classes of q-ary quantum MDS codes of length $\frac{q^2-1}{2t_1t_2}$, where q is an odd prime power, $(2t_1)|(q-1)$, $t_2|(q+1)$ and t_2 is an odd integer. Let $n = \frac{q^2-1}{2t_1t_2}$ and $r = 2$. Since $2n|(q^2-1)$, then for each odd i in the range $1 \le i \le 2n$, the q^2-cyclotomic coset C_i modulo $2n$ is $C_i = \{i\}$.

Lemma 17:

1) *Let q be an odd prime power of the form $30m + 11$ and $n = \frac{q^2-1}{30}$. If C is a q^2-ary negacyclic code of length n with defining set $Z = \bigcup_{j=2m+1}^{\delta} C_{1+2j}$, where $2m+1 \le \delta \le 10m+2$, then $C^{\perp H} \subseteq C$.*
2) *Let q be an odd prime power of the form $30m + 19$ and $n = \frac{q^2-1}{30}$. If C is a q^2-ary negacyclic code of length n with defining set $Z = \bigcup_{j=m+1}^{\delta} C_{1+2j}$, where $m+1 \le \delta \le 9m+4$, then $C^{\perp H} \subseteq C$.*
3) *Let q be an odd prime power of the form $12m+5$ and $n = \frac{q^2-1}{12}$. If C is a q^2-ary negacyclic code of length n with defining set $Z = \bigcup_{j=2m+1}^{\delta} C_{1+2j}$, where $2m+1 \le \delta \le 7m+1$, then $C^{\perp H} \subseteq C$.*

Proof: We will only prove the first part since the other parts can be obtained similarly. We fix $q = 30m + 11$ and $2m+1 \le \delta \le 10m+2$. By Lemma 4, it is sufficient to prove $Z \bigcap (-qZ) = \emptyset$. Suppose there exist integers $2m+1 \le i \le j \le \delta$ such that $C_{1+2i} = -qC_{1+2j}$, that is

$$1 + 2i \equiv -q(1+2j) \pmod{\frac{q^2-1}{15}}.$$

Since $q = 30m + 11$, we get that

$$(30m+11)(1+2j) + 1 + 2i \equiv 0 \pmod{60m^2 + 44m + 8}.$$

Note that $2(60m^2+44m+8) < (30m+11)(1+2j)+1+2i < 10(60m^2+44m+8)$, then

$$(30m+11)(1+2j) + 1 + 2i = x(60m^2+44m+8),$$

where $3 \le x \le 9$. Equivalently

$$\begin{aligned} 1 + 2i &= x(60m^2+44m+8) \\ &\quad -(30m+11)(1+2j), \quad 3 \le x \le 9. \end{aligned}$$

Note that $4m+3 \le 1+2i \le 20m+5$.

For the case $3 \le x \le 4$. If $j \ge mx+1$, then $1+2i \le -2m-1$. If $j \le mx$, then $1+2i \ge 36m+13$. We have reached a contradiction.

For the case $5 \le x \le 7$. If $j \ge mx+2$, then $1+2i \le 4m+1$. If $j \le mx+1$, then $1+2i \ge 20m+7$. We have again reached a contradiction.

For the case $8 \le x \le 9$. If $j \ge mx+3$, then $1+2i \le -12m-5$. If $j \le mx+2$, then $1+2i \ge 26m+9$. We have got a contradiction. ■

Theorem 18:

(1) *Let q be an odd prime power of the form $30m+11$, then there exists a q-ary $[[\frac{q^2-1}{30}, \frac{q^2-1}{30} - 2d + 2, d]]$-quantum MDS code, where $2 \le d \le 8m+3$.*

(2) *Let q be an odd prime power of the form $30m+19$, then there exists a q-ary $[[\frac{q^2-1}{30}, \frac{q^2-1}{30} - 2d + 2, d]]$-quantum MDS code, where $2 \le d \le 8m+5$.*

(3) *Let q be an odd prime power of the form $12m+5$, then there exists a q-ary $[[\frac{q^2-1}{12}, \frac{q^2-1}{12} - 2d + 2, d]]$-quantum MDS code, where $2 \le d \le 5m+2$.*

Proof: Note that every q^2-cyclotomic coset has exactly one element, then by the Hermitian construction and Lemma 17, the conclusion follows. ■

Example 19:

1) *Let $q = 41$, applying Theorem 18 (1) produces new quantum MDS codes with parameters $[[56, 58 - 2d, d]]_{41}$, where $2 \le d \le 11$.*
2) *Let $q = 49$, applying Theorem 18 (2) produces new quantum MDS codes with parameters $[[80, 82 - 2d, d]]_{49}$, where $2 \le d \le 13$.*
3) *Let $q = 17$, applying Theorem 18 (3) produces new quantum MDS codes with parameters $[[24, 26 - 2d, d]]_{17}$, where $2 \le d \le 7$.*

Acknowledgments

The authors express their gratitude to the two anonymous reviewers for their detailed and constructive comments which are very helpful to the improvement of the presentation of this paper, and to Dr. Markus Grassl, the associate editor, for his excellent editorial job.

References

[1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, "On quantum and classical BCH codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1183–1188, Mar. 2007.

[2] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3065–3072, Nov. 2001.

[3] N. Aydin, I. Siap, and D. K. Ray-Chaudhuri, "The structure of 1-generator quasi-twisted codes and new linear codes," *Designs, Codes Cryptogr.*, vol. 24, no. 3, pp. 313–326, 2001.

[4] J. Bierbrauer and Y. Edel, "Quantum twisted codes," *J. Combinat. Designs*, vol. 8, no. 3, pp. 174–188, 2000.

[5] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.

[6] B. Chen, S. Ling, and G. Zhang, "Application of constacyclic codes to quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 3, pp. 1474–1484, Mar. 2015.

[7] H. Chen, S. Ling, and C. Xing, "Quantum codes from concatenated algebraic-geometric codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2915–2920, Aug. 2005.

[8] K. Feng, "Quantum codes $[[6, 2, 3]]_p$ and $[[7, 3, 3]]_p$ ($p \ge 3$) exist," *IEEE Trans. Inf. Theory*, vol. 48, no. 8, pp. 2384–2391, Aug. 2002.

[9] M. Grassl, T. Beth, and M. Rötteler, "On optimal quantum codes," *Int. J. Quantum Inf.*, vol. 2, no. 1, pp. 55–64, 2004.

[10] M. Rötteler, M. Grassl, and T. Beth, "On quantum MDS codes," in *Proc. Int. Symp. Inf. Theory*, Chicago, IL, USA, Jun. 2004, p. 355.

[11] X. Hu, G. Zhang, and B. Chen, "Constructions of new nonbinary quantum codes," *Int. J. Theoretical Phys.*, vol. 54, no. 1, pp. 92–99, 2015.

[12] L. Jin, S. Ling, J. Luo, and C. Xing, "Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4735–4740, Oct. 2010.

[13] L. Jin and C. Xing, "A construction of new quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2921–2925, May 2014.

[14] X. Kai and S. Zhu, "New quantum MDS codes from negacyclic codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 1193–1197, Feb. 2013.

[15] X. Kai, S. Zhu, and P. Li, "Constacyclic codes and some new quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2080–2086, Apr. 2014.

[16] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4892–4914, Nov. 2006.
[17] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Phys. Rev. A*, vol. 55, no. 2, pp. 900–911, Feb. 1997.
[18] G. G. La Guardia, "New quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5551–5554, Aug. 2011.
[19] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting code," *Phys. Rev. Lett.*, vol. 77, no. 1, p. 198, Jul. 1996.
[20] Z. Li, L.-J. Xing, and X.-M. Wang, "Quantum generalized Reed–Solomon codes: Unified framework for quantum maximum-distance-separable codes," *Phys. Rev. A*, vol. 77, no. 1, p. 012308, Jan. 2008.
[21] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, no. 4, p. R2493, Oct. 1995.
[22] A. N. Steane, "Multiple-particle interference and quantum error correction," *Proc. Roy. Soc. London A, Math., Phys. Eng. Sci.*, vol. 452, no. 1954, pp. 2551–2577, 1996.
[23] A. M. Steane, "Enlargement of Calderbank–Shor–Steane quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2492–2495, Nov. 1999.
[24] L. Wang and S. Zhu, "New quantum MDS codes derived from constacyclic codes," *Quantum Inf. Process.*, vol. 14, no. 3, pp. 881–889, 2015.
[25] Y. Yang and W. Cai, "On self-dual constacyclic codes over finite fields," *Designs, Codes Cryptogr.*, vol. 74, no. 2, pp. 355–364, 2013.
[26] G. Zhang and B. Chen, "New quantum MDS codes," *Int. J. Quantum Inf.*, vol. 12, no. 4, p. 1450019, 2014.

Tao Zhang is currently a Ph.D. student at Zhejiang University, Hangzhou, Zhejiang, P. R. China. His research interests include combinatorial design theory, coding theory, algebraic combinatorics, and their interactions.

Gennian Ge received the M.S. and Ph.D. degrees in mathematics from Suzhou University, Suzhou, Jiangsu, P. R. China, in 1993 and 1996, respectively. After that, he became a member of Suzhou University. He was a postdoctoral fellow in the Department of Computer Science at Concordia University, Montreal, QC, Canada, from September 2001 to August 2002, and a visiting assistant professor in the Department of Computer Science at the University of Vermont, Burlington, Vermont, USA, from September 2002 to February 2004. He was a full professor in the Department of Mathematics at Zhejiang University, Hangzhou, Zhejiang, P. R. China, from March 2004 to February 2013. Currently, he is a full professor in the School of Mathematical Sciences at Capital Normal University, Beijing, P. R. China. His research interests include the constructions of combinatorial designs and their applications to codes and crypts.

Dr. Ge is on the Editorial Board of *Journal of Combinatorial Designs*, *Science China Mathematics*, *Applied Mathematics–A Journal of Chinese Universities*. He received the 2006 Hall Medal from the Institute of Combinatorics and its Applications.