New quantum MDS codes

Zhang, Guanghui; Chen, Bocong

2014

Zhang, G., & Chen, B. (2014). New quantum MDS codes. International journal of quantum information, 12(04), 1450019-.

<https://hdl.handle.net/10356/106908>

<https://doi.org/10.1142/S0219749914500191>

© 2014 World Scientific Publishing Company. This is the author created version of a work that has been peer reviewed and accepted for publication by International Journal of Quantum Information, World Scientific Publishing Company. It incorporates referee's comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [<http://dx.doi.org/10.1142/S0219749914500191>].

Downloaded on 26 Apr 2023 13:10:17 SGT

New Quantum MDS Codes*

Guanghui Zhang¹, Bocong Chen²

¹School of Mathematical Sciences, Luoyang Normal University, Luoyang, Henan, 471022, China

²School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore, 637616, Singapore

Abstract

In this paper, we construct two classes of new quantum maximum-distance-separable (MDS) codes with parameters $[[\frac{q^2-1}{4}, \frac{q^2-1}{4} - 2d + 2, d]]_q$, where q is an odd prime power with $q \equiv 3 \pmod{4}$ and $2 \leq d \leq \frac{3q-1}{4}$; $[[8(q-1), 8(q-1) - 2d + 2, d]]_q$, where q is an odd prime power with the form $q = 8t - 1$ (t is an even positive integer) and $2 \leq d \leq \frac{q+15}{2}$. Compared the parameters with all known quantum MDS codes, the quantum MDS codes exhibited here have minimum distances bigger than the ones available in the literature.

Keywords: Quantum codes; Quantum MDS codes; Cyclotomic cosets; Constacyclic codes

1 Introduction

After the great discovery in [1] and [2], quantum error-correcting codes have experienced tremendous growth. The first important quantum code construction is given in [2] and [3]. Calderbank *et al.* in [4] discovered that the problem of constructing quantum codes can be diverted into the problem of 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. In recent years, many classes of nonbinary quantum codes have been found by employing different methods (see [5]-[11]).

An important characteristic of a quantum code is its minimum distance. If a quantum code has minimum distance d , then it can detect any $d - 1$ and correct any $\lfloor \frac{d-1}{2} \rfloor$ quantum errors. One of the principal problems in quantum coding theory is to construct quantum codes with the best possible minimum distance. Quantum maximum-distance-separable (MDS) codes are optimal in the sense that they beat the quantum Singleton bound. One can expect that a quantum code with such extremal parameters will have interesting features. For example, Rains [12] showed that all quantum MDS codes are pure. This is an interesting property, since pure quantum codes are easier to study than impure ones. In recent years, constructing quantum MDS codes has become a hot research topic. Some classes of quantum MDS codes have been found by employing different methods (see [13]-[22]). La Guardia in [19] constructed a new class of quantum MDS codes through MDS cyclic codes. Recently, Kai *et al.* [14]-[16] 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 quantum MDS codes are constructed in this paper. More specifically, we obtain two classes of q -ary quantum MDS codes with parameters $[[\frac{q^2-1}{4}, \frac{q^2-1}{4} - 2d + 2, d]]_q$, where q is an odd prime power with $q \equiv 3 \pmod{4}$ and $2 \leq d \leq \frac{3q-1}{4}$; $[[8(q-1), 8(q-1) - 2d + 2, d]]_q$, where q is an odd prime power with the form $q = 8t - 1$ (t is an even positive integer) and $2 \leq d \leq \frac{q+15}{2}$.

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.

*Email addresses: zghui2012@126.com (G. Zhang), bocong.chen@yahoo.com (B. Chen).

2 Review of constacyclic codes

In this section, we recall some basic notations and facts about 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., $\gcd(n, q) = 1$. 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 $\mathbf{x} = (x_0, x_1, \dots, x_{n-1}) \in \mathbb{F}_{q^2}^n$ and $\mathbf{y} = (y_0, y_1, \dots, y_{n-1}) \in \mathbb{F}_{q^2}^n$, the *Hermitian inner product* is defined as

$$\langle \mathbf{x}, \mathbf{y} \rangle_H = x_0 y_0^q + x_1 y_1^q + \dots + x_{n-1} y_{n-1}^q.$$

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

$$C^{\perp_H} = \{ \mathbf{x} \in \mathbb{F}_{q^2}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle_H = 0, \text{ for all } \mathbf{y} \in C \}.$$

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

We adopt the notation in [16]. 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 $\text{ord}(\beta)$ the order of β in the group $\mathbb{F}_{q^2}^*$; then $\text{ord}(\beta)$ is a divisor of $q^2 - 1$, and β is called a *primitive $\text{ord}(\beta)$ th root of unity*.

Let $\eta \in \mathbb{F}_{q^2}^*$ be a primitive r th root of unity. A linear code C of length n over $\mathbb{F}_{q^2}$ is said to be *η -constacyclic* if $(\eta c_{n-1}, c_0, \dots, c_{n-2}) \in C$ for every $(c_0, c_1, \dots, c_{n-1}) \in C$. Each codeword $c = (c_0, c_1, \dots, c_{n-1}) \in C$ is customarily identified with its polynomial representation $c(X) = c_0 + c_1 X + \dots + c_{n-1} X^{n-1}$. In this way, every η -constacyclic code C is an ideal of $\mathbb{F}_{q^2}[X]/\langle X^n - \eta \rangle$. We then know that C is generated uniquely 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 $C = \langle g(X) \rangle$. There exists a primitive rn th root of unity (in some extension field of $\mathbb{F}_{q^2}$), say δ , such that $\delta^n = \eta$. The roots of $X^n - \eta$ are precisely the elements δ^{1+ri} for $0 \leq i \leq n-1$. Set $\theta_{r,n} = \{1 + ri \mid 0 \leq i \leq n-1\}$. The defining set of a constacyclic code $C = \langle g(X) \rangle$ of length n is the set $Z = \{j \in \theta_{r,n} \mid \delta^j \text{ is a root of } g(X)\}$. 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 [16]).

The following results play important roles in constructing quantum codes from constacyclic codes.

Theorem 2.1. (The BCH bound for Constacyclic Codes) ([16, Theorem 2.1]) *Let C be a η -constacyclic code of length n over $\mathbb{F}_{q^2}$, where η is a primitive r th root of unity. Let δ be a primitive rn th root of unity in an extension field of $\mathbb{F}_{q^2}$ such that $\delta^n = \eta$. Assume the generator polynomial of C has roots that include the set $\{\delta^{1+ri} \mid i_1 \leq i \leq i_1 + d - 2\}$. Then the minimum distance of C is at least d .*

Lemma 2.2. ([16, Lemma 2.2]) *Let r be a positive divisor of $q+1$ and let $\eta \in \mathbb{F}_{q^2}^*$ be of order r . Assume that C is a η -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 $Z \cap Z^{-q} = \emptyset$, where $Z^{-q} = \{-qz \pmod{rn} \mid z \in Z\}$.*

3 Review of quantum codes

In this section, we recall some basic notations and facts about 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 [8] and [23]).

Theorem 3.1. (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 [8] 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.

Theorem 3.2. (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 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 code.

4 New quantum MDS codes

In this section, two classes of dual-containing constacyclic MDS codes are constructed and their parameters are computed. Consequently, new quantum MDS codes are derived from these parameters. We adopt the following notation. Given integers a, b and z , $a \mid b$ means that a divides b , and $a \equiv b \pmod{z}$ means $z \mid (a - b)$.

4.1 New quantum MDS codes of length $\frac{q^2-1}{4}$

Let q be an odd prime power such that $q \equiv 3 \pmod{4}$. Let $n = \frac{q^2-1}{4}$ and $r = 4$. It is clear that $rn = q^2 - 1$, and hence every q^2 -cyclotomic coset modulo rn contains exactly one element. Let $\eta \in \mathbb{F}_{q^2}$ be a primitive r th root of unity.

Let C be a η -constacyclic code with defining set

$$Z = \left\{ 1 + 4i \left(\text{mod } q^2 - 1 \right) \mid -\frac{q-3}{4} \leq i \leq \frac{q-3}{2} \right\}. \quad (4.1)$$

It is easy to see that $|Z| = \frac{3q-5}{4}$. As we show below, C is a dual-containing code.

Lemma 4.1. *Notation as above. If C is a η -constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set as in (4.1), then C is a dual-containing code.*

Proof. Suppose otherwise that C is not a dual-containing code. It follows from Lemma 2.2 that $Z \cap Z^{-q} \neq \emptyset$. Hence, two integers i, j with $-\frac{q-3}{4} \leq i, j \leq \frac{q-3}{2}$ can be found such that

$$-q(1 + 4i) \equiv 1 + 4j \pmod{q^2 - 1}. \quad (4.2)$$

Suppose that $i = j$. Then from equation (4.2), we get that $(q-1) \mid (1 + 4i)$. Note that $-(q-1) < 1 + 4i < 2(q-1)$. Thus $1 + 4i = 0$ or $q-1$. Since $1 + 4i$ and q are odd, we obtain a contradiction.

Without loss of generality, we may assume that $i > j$. From equation (4.2), we have that $-q(1 + 4i) \equiv 1 + 4j \pmod{q+1}$ and $-q(1 + 4i) \equiv 1 + 4j \pmod{q-1}$, i.e., $\frac{q+1}{4} \mid (i-j)$ and $(q-1) \mid (4i + 4j + 2)$. Note that $0 < i-j < q+1$ and $-2(q-1) < 4i + 4j + 2 < 4(q-1)$. Write $i-j = \ell_1 \cdot \frac{q+1}{4}$, $4i + 4j + 2 = \ell_2(q-1)$, where $1 \leq \ell_1 \leq 3$ and $-1 \leq \ell_2 \leq 3$. Thus, $8i = (q+1)(\ell_1 + \ell_2) - 2(1 + \ell_2)$ and $8j = (q+1)(\ell_2 - \ell_1) - 2(1 + \ell_2)$. Therefore $2 \mid (1 + \ell_2)$, which implies that $\ell_2 = -1, 1$ or 3 .

If $\ell_2 = -1$, then $8j = -(q+1)(1 + \ell_1)$. Since $1 \leq \ell_1 \leq 3$, we have $j \leq -\frac{q+1}{4} < -\frac{q-3}{4}$, contradicting the assumption that $j \geq -\frac{q-3}{4}$.

If $\ell_2 = 1$, then $4i + 4j + 2 = q-1$. So $4j = q-3-4i$. Substituting $4j$ into equation (4.2) yields $-q(1 + 4i) \equiv 1 + (q-3-4i) \pmod{q^2-1}$. Thus $(q+1) \mid (4i+2)$. Note that $-(q+1) < 4i+2 < 2(q+1)$ and $4i+2 \neq 0$. So $4i+2 = q+1$, which implies that $q \equiv 1 \pmod{4}$. This contradicts our assumption $q \equiv 3 \pmod{4}$.

If $\ell_2 = 3$, then $8i = (q+1)(\ell_1 + 3) - 8$. Thus $8i + 8 = (q+1)(\ell_1 + 3) \geq 4(q+1)$, which gives that $i \geq \frac{q-1}{2}$. This contradicts our assumption $i \leq \frac{q-3}{2}$.

□

Theorem 4.2. *Let q be a prime power with the $q \equiv 3 \pmod{4}$. Then, there exist quantum MDS codes with parameters $[[\frac{q^2-1}{4}, \frac{q^2-1}{4} - 2d + 2, d]]_q$, where $2 \leq d \leq \frac{3q-1}{4}$.*

Proof. Let $n = \frac{q^2-1}{4}$ and $r = 4$. Let $\eta \in \mathbb{F}_{q^2}$ be a primitive fourth root of unity. Recall that every q^2 -cyclotomic coset modulo rn contains precisely one element. We assume that $\mathcal{C}_\delta$ is a η -constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set

$$\mathcal{Z}_\delta = \left\{ 1 + 4 \left(i + \frac{q-3}{4} \right) \pmod{q^2-1} \mid 0 \leq i \leq \delta - 1 \right\},$$

where δ is a positive integer with $1 \leq \delta \leq \frac{3q-5}{4}$. We then see that $\mathcal{Z}_\delta$ is a subset of Z , where Z is given in (4.1). Thus, $\mathcal{Z}_\delta \cap \mathcal{Z}_\delta^{-q} = \emptyset$ by Lemma 4.1. It follows from Lemma 2.2 that $\mathcal{C}_\delta$ is a dual-containing code with parameters $[n, n - d + 1, d]_{q^2}$, where $d = \delta + 1$. Using the Hermitian construction and the quantum Singleton bound, we can obtain a quantum MDS code with parameters $[[\frac{q^2-1}{4}, \frac{q^2-1}{4} - 2d + 2, d]]_q$. $\square$

Example 4.3. *In Table 1, we list some quantum codes with parameters obtained from Theorem 4.2 for $q = 7, 11$ and 23 .*

Table 1: Quantum MDS codes

q	$[[n, k, d]]_q$	d
7	$[[12, 12 - 2d + 2, d]]_7$	$2 \leq d \leq 5$
11	$[[30, 30 - 2d + 2, d]]_{11}$	$2 \leq d \leq 8$
23	$[[132, 132 - 2d + 2, d]]_{23}$	$2 \leq d \leq 17$

4.2 New quantum MDS codes of length $8(q-1)$

Let q be an odd prime power with the form $q = 8t - 1$, where t is an even positive integer. It is clear that $t \geq 4$. Let $n = 8(q-1)$ and $r = \frac{q+1}{8} = t$. It is clear that $rn = q^2 - 1$, and hence every q^2 -cyclotomic coset modulo rn contains exactly one element. Let $\eta \in \mathbb{F}_{q^2}$ be a primitive r th root of unity.

Let C be a λ -constacyclic code with defining set

$$Z = \{1 + ti \mid 4t - 8 \leq i \leq 8t - 3\}. \quad (4.3)$$

Recall that t is an even positive integer with $t \geq 4$. It is easy to see that $|Z| = 4t + 6$, which gives that C is an MDS η -constacyclic code with parameters $[n, n - 4t - 6, 4t + 7]$. As we will show shortly, C contains its Hermitian dual code.

Lemma 4.4. *Notation as above. If C is a η -constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set as in (4.3), then C is a dual-containing code.*

Proof. Suppose otherwise that $Z \cap Z^{-q} \neq \emptyset$. Hence, two integers j, k with $4t - 8 \leq i, j \leq 8t - 3$ can be found such that

$$-q(1 + ti) \equiv 1 + tj \pmod{q^2 - 1}. \quad (4.4)$$

We will obtain a contradiction by considering the following cases:

(1) $4t - 8 \leq i \leq 8t - 17$. Let $i = 8\ell + k$, where k is an integer with $0 \leq k \leq 7$. If $\ell \geq t - 2$, then $i = 8\ell + k \geq 8t - 16 > 8t - 17$, which is impossible. We then have $\ell \leq t - 3$. On the other hand, $\ell \geq \frac{t}{2} - 1$. Indeed, if $\ell \leq \frac{t}{2} - 2$, we would obtain $i = 8\ell + k \leq 8(\frac{t}{2} - 2) + 7 = 4t - 9 < 4t - 8$, contradicting the assumption that $4t - 8 \leq i$.

Expanding $-q(1 + t(8\ell + k))$, one gets $-q(1 + t(8\ell + k)) = -q - q^2\ell - q\ell - tkq$. By equation (4.4), we have

$$q^2 - 1 - q - \ell - q\ell - tkq \equiv 1 + tj \pmod{q^2 - 1}.$$

It follows from $t \geq 4$ that $1 + tj \leq 1 + t(8t - 3) < rn = 8t(8t - 2)$. Now, $q + \ell + q\ell + tkq \leq 8t - 1 + t - 3 + (8t - 1)(t - 3) + 7t(8t - 1) = 64t^2 - 23t - 1 < q^2 - 1 = 64t^2 - 16t$. We then have

$$q^2 - 1 - q - \ell - q\ell - tkq = 1 + tj.$$

If $0 \leq k \leq 6$, then $1 + tj + q + \ell + q\ell + tkq \leq 1 + t(8t - 3) + (8t - 1) + (t - 3) + (8t - 1)(t - 3) + 6t(8t - 1) = 64t^2 - 25t < q^2 - 1$. This is a contradiction.

If $k = 7$, then $1 + tj + q + \ell + q\ell + tkq \geq 1 + t(4t - 8) + (8t - 1) + (\frac{t}{2} - 1) + (8t - 1)(\frac{t}{2} - 1) + 7t(8t - 1) = 64t^2 - 15t > q^2 - 1$, a contradiction again.

(2) $8t - 16 \leq i \leq 8t - 10$. Simple calculations show that

$$-64t^3 + 88t^2 - 18t + 1 \leq -q(1 + ti) \leq -64t^3 + 136t^2 - 24t + 1.$$

From $(t - 1)(q^2 - 1) = 64t^3 - 80t^2 + 16t$, we have $8t^2 - 2t + 1 \leq (t - 1)(q^2 - 1) - q(1 + ti) \leq 56t^2 - 8t + 1 < q^2 - 1$. We then know from equation (4.4) that $(t - 1)(q^2 - 1) - q(1 + ti) = 1 + tj$. However, $1 + tj \leq 1 + t(8t - 3) = 8t^2 - 3t + 1 < 8t^2 - 2t + 1$. This is a contradiction.

(3) $8t - 9 \leq i \leq 8t - 3$. Similar to the case (2), routine computations show that $-64t^3 + 32t^2 - 11t + 1 \leq -q(1 + ti) \leq -64t^3 + 80t^2 - 17t + 1$, and so $16t^2 - 11t + 1 \leq t(q^2 - 1) - q(1 + ti) \leq 64t^2 - 17t + 1 < q^2 - 1$. Note that $16t^2 - 11t + 1 > 8t^2 - 3t + 1 \geq 1 + tj$, which gives a contradiction. $\square$

Theorem 4.5. *Let q be an odd prime power with the form $q = 8t - 1$, where t is an even positive integer. Then, there exist quantum MDS codes with parameters $[[8(q - 1), 8(q - 1) - 2d + 2, d]]_q$, where $2 \leq d \leq \frac{q+15}{2}$.*

Proof. Let $n = 8(q - 1)$ and $r = t$. Let $\eta \in \mathbb{F}_{q^2}$ be a primitive t th root of unity. Recall that every q^2 -cyclotomic coset modulo rn contains precisely one element. We assume that $\mathcal{C}_\delta$ is a η -constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set

$$\mathcal{Z}_\delta = \{1 + t(i + 4t - 8) \pmod{q^2 - 1} \mid 0 \leq i \leq \delta - 1\}.$$

where δ is a positive integer with $1 \leq \delta \leq \frac{q+13}{2}$. It follows from Lemma 4.4 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 $2 \leq d \leq \frac{q+15}{2}$. Using the Hermitian construction and the quantum Singleton bound, we can obtain a quantum MDS code with parameters $[[8(q - 1), 8(q - 1) - 2d + 2, d]]_q$. $\square$

Example 4.6. *In Table 2, we list some quantum codes with parameters obtained from Theorem 4.5 for $q = 31, 47$ and 79 .*

Table 2: Quantum MDS codes

q	$[[n, k, d]]_q$	d
31	$[[240, 240 - 2d + 2, d]]_{31}$	$2 \leq d \leq 23$
47	$[[368, 368 - 2d + 2, d]]_{47}$	$2 \leq d \leq 31$
79	$[[624, 624 - 2d + 2, d]]_{79}$	$2 \leq d \leq 47$

5 Summary

In Section 3, we have constructed two classes of quantum MDS codes using the Hermitian construction of [27]. We summarize in Table 4 the parameters of all known quantum MDS codes. Classes 21–22 of Table 4 are the new ones.

Table 3: Quantum MDS codes

Class	Length	Distance	Reference
1	$n \leq q + 1$	$d \leq \lfloor n/2 \rfloor + 1$	[24], [25], [26]
2	$mq - l$ $0 \leq l < m, 1 < m < q$	$d \leq m - l + 1$	[13], [28]
3	$mq - l$ $0 \leq l \leq q - 1, 1 \leq m \leq q$	$3 \leq d \leq (q + 1 - \lfloor l/m \rfloor)/2$	[18]
4	$r(q - 1) + 1$ $q + 1 \equiv r \pmod{2r}$	$d \leq (q + r + 1)/2$	[22]
5	$q^2 - s$ $0 \leq s < q/2 - 1$	$q/2 + 1 < d \leq q - s$	[22]
6	$(q^2 + 1)/2 - s$ $0 \leq s < q/2 - 1$	$q/2 + 1 < d \leq q - s$	[22]
7	$(q^2 + 1)/2, q$ odd	$3 \leq d \leq q, d$ odd	[14]
8	$4 \leq n \leq q^2 + 1$ $q \neq 2$ and $n \neq 4$	3	[29], [18], [17]
9	$q^2 - l$	$d \leq q - l, 0 \leq l \leq q - 2$	[25], [13]
10	$q^2 + 1$	$2 \leq d \leq q + 1$	[18], [22], [14], [19]
11	$(q^2 - 1)/2, q$ odd	$2 \leq d \leq q$	[16]
12	$\frac{q^2-1}{r}, q$ odd $r \mid (q + 1), r$ even and $r \neq 2$	$2 \leq d \leq (q + 1)/2$	[16]
13	$\lambda(q + 1), q$ odd λ odd, $\lambda \mid (q - 1)$	$2 \leq d \leq (q + 1)/2 + \lambda$	[16]
14	$2\lambda(q + 1), q \equiv 1 \pmod{4}$ λ odd, $\lambda \mid (q - 1)$	$2 \leq d \leq (q + 1)/2 + 2\lambda$	[16]
15	$(q^2 + 1)/5, q = 20m + 3$ or $20m + 7$	$2 \leq d \leq (q + 5)/2,$ d even	[16]
16	$(q^2 + 1)/5, q = 20m - 3$ or $20m - 7$	$2 \leq d \leq (q + 3)/2,$ d even	[16]
17	$n = \frac{q^2-1}{3}, 3 \mid (q + 1)$	$2 \leq d \leq \frac{2q-1}{3}$	[30]
18	$n = \frac{q^2-1}{5}, 5 \mid (q + 1)$	$2 \leq d \leq \frac{3q-2}{5}$	[30]
19	$n = \frac{q^2-1}{7}, 7 \mid (q + 1)$	$2 \leq d \leq \frac{4q-3}{7}$	[30]
20	$n = \frac{q^2+1}{10},$ $q = 10m + 3$ or $q = 10m + 7$	$3 \leq d \leq 4m + 1$ d odd	[30]
21	$n = \frac{q^2-1}{4}$ $q \equiv 3 \pmod{4}$	$2 \leq d \leq \frac{3q-1}{4}$	New
22	$n = 8(q - 1)$ $q = 8t - 1, t$ even	$2 \leq d \leq \frac{q+15}{2}$	New

In Table 4, fixing the value of q yields the value (or range of values) of the length n . We next compare the minimum distance of the new quantum MDS codes of length n with that of previously known ones of the same length. It can be seen that the new quantum MDS codes exhibited here often have minimum distance bigger than what was previously known in the literature, for the same q and length.

For example, with $q = 11$ and $\lambda = 3$, Class 21 gives $n = 3(11 - 1) = 30$. We then search among Classes 1–20 of Table 4 to see in which classes can the length 30 be attained. For example, in Class 12, we find a appropriate integer $r = 4$ such that $30 = \frac{11^2-1}{r}$; but in Class 4, there does not exist any positive

integer r such that $r \times (11 - 1) + 1 = 30$. In fact, with $q = 11$, it can be verified that the length 30 can only be attained in Classes 3, 8 and 12. We then compare the largest possible minimum distances of these codes of the same length (as in the row with $q = 11$ in Table 5).

Table 4: Comparison between Class 21 and Previously Known Quantum MDS Codes

q	Length	d (Class 21)	d (Class 3)	d (Class 8)	d (Class 12)
7	12	5	3	3	4
11	30	8	5	3	6
23	132	17	11	3	12

Table 5: Comparison between Class 22 and Previously Known Quantum MDS Codes

q	Length	d (Class 22)	d (Class 3)	d (Class 8)	d (Class 12)
31	240	23	15	3	16
47	368	31	23	3	24
79	624	47	39	3	40

Acknowledgements The authors thank NSFC for the support by Grant No. 11171370. The first author is supported by 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).

References

- [1] P. W. Shor, Phys. Rev. A, **52** (1995) 2493.
- [2] A. M. Steane, Proc. Roy. Soc. Lond. A, **452** (1996) 2551.
- [3] A. M. Steane, Phys. Rev. Lett., **77** (1996) 793.
- [4] A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane, IEEE Trans. Inf. Theory, **44** (1998) 1369.
- [5] S. A. Aly, A. Klappenecker, P. K. Sarvepalli, Proc IEEE Int Symp Inform Theory, (2006) 1114.
- [6] S. A. Aly, A. Klappenecker, P. K. Sarvepalli, IEEE Trans. Inf. Theory, **53** (2007) 1183.
- [7] A. Ashikhmin, E. Knill, IEEE Trans. Inf. Theory, **47** (2001) 3065.
- [8] A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli, IEEE Trans. Inf. Theory, **52** (2006) 4892.
- [9] G. G. La Guardia, Phys. Rev. A, **80** (2009) 042331.
- [10] J. Qian, L. Zhang, Mod. Phys. Lett. B, **27** (2013) v1350053.
- [11] J. Chen, J. Li, J. Lin, Int. J Theor. Phys., **53** (2014) 72.
- [12] E. Rains, IEEE Trans. Inf. Theory, **45** (1999) 1827.
- [13] Z. Li, L. J. Xing, X. M. Wang, Phys. Rev. A, **77** (2008) 012308.

- [14] X. Kai, S. Zhu, IEEE Trans. Inf. Theory, **59** (2013) 1193.
- [15] X. Kai, S. Zhu, Y. Tang, Phys. Rev. A, **88** (2013) 012326.
- [16] X. Kai, S. Zhu, P. Li, IEEE Trans. Inf. Theory, (2014), DOI: 10.1109/TIT.2014.2308180.
- [17] R. Li, Z. Xu, Phys. Rev. A, **82** (2010) 052316.
- [18] L. Jin, S. Ling, J. Luo, C. Xing, IEEE Trans. Inf. Theory, **56** (2010) 4735.
- [19] G. G. L. Guardia, IEEE Trans. Inf. Theory, **57** (2011) 5551.
- [20] L. Jin, C. Xing, IEEE Trans. Inf. Theory, **58** (2012) 5484.
- [21] M. F. Ezerman, S. Jitman, S. Ling, and D. V. Pasechnik, IEEE Trans. Inf. Theory, **59** (2013) 6732.
- [22] L. Jin, C. Xing, IEEE Trans. Inf. Theory, (2014) DOI: 10.1109/TIT.2014.2299800.
- [23] E. Knill, R. Laflamme, Phys. Rev. A, **55** (1997) 900.
- [24] K. Feng , IEEE Trans. Inf. Theory, **48** (2002) 2384.
- [25] M. Grassl, T. Beth, M. Rötteler Int. J. Quantum Inform., **2** (2004) 757.
- [26] M. Grassl , M. Rötteler , T. Beth , In Proc. Int. Symp. Inf. Theory, Chicago, USA, (2004) 356
- [27] A. Ashikhmin, E. Knill, IEEE Trans. Inf. Theory, **47** (2001) 3065.
- [28] P. K. Sarvepalli, A. Klappenecker, In Proc. Int. Symp. Inf. Theory, Adelaide, Australia, (2005) 1023.
- [29] J. Bierbrauer, Y. Edel, J. Comb. Designs, **8** (2000) 174.
- [30] B. Chen, S. Ling, G. Zhang, (2014) arXiv:1403.2499.