Des. Codes Cryptogr. (2017) 84:463–471
DOI 10.1007/s10623-016-0281-9

Quantum MDS codes with relatively large minimum distance from Hermitian self-orthogonal codes

Lingfei Jin[1] · **Haibin Kan**[1] · **Jie Wen**[1]

Received: 27 April 2016 / Revised: 7 September 2016 / Accepted: 13 September 2016 /
Published online: 28 September 2016

Abstract It has become common knowledge that constructing q-ary quantum MDS codes with minimum distance bigger than $q/2+1$ is significantly more difficult than constructing those with minimum distance less than or equal to $q/2+1$. Despite of various constructions of q-ary quantum MDS codes, all known q-ary quantum MDS codes have minimum distance bounded by $q/2+1$ except for some lengths. The purpose of the current paper is to provide some new q-ary quantum MDS codes with minimum distance bigger than $q/2+1$. In this paper, we provide several classes of quantum MDS codes with minimum distance bigger than $q/2+1$. For instance, some examples in these classes include q-ary $[n, n-2k, k+1]$-quantum MDS codes for cases: (i) $q \equiv -1 \bmod 5$, $n = (q^2+4)/5$ and $1 \leq k \leq (3q-2)/5$; (ii) $q \equiv -1 \bmod 7$, $n = (q^2+6)/7$ and $1 \leq k \leq (4q-3)/7$; (iii) $2|q$, $q \equiv -1 \bmod 3$, $n = 2(q^2-1)/3$ and $1 \leq k \leq (2q-1)/3$; and (iv) $2|q$, $q \equiv -1 \bmod 5$, $n = 2(q^2-1)/5$ and $1 \leq k \leq (3q-2)/5$.

Keywords Hermitian self-orthogonality · Generalized Reed-Solomon codes · Quantum MDS codes

Mathematics Subject Classification 94B05 · 81Q99

1 Introduction

In the past two decades, the field of quantum error correction has experienced a great progress since the establishment of the connections between quantum codes and classical codes (see

Communicated by C. Mitchell.

✉ Lingfei Jin
lfjin@fudan.edu.cn

Haibin Kan
hbkan@fudan.edu.cn

[1] School of Computer Science, Shanghai Key Laboratory of Intelligent Information Processing, Fudan University, Shanghai 200433, China

[3]). One of these connections shows that the construction of quantum codes can be reduced to that of classical linear error-correcting codes with certain self-orthogonality properties (see [2,3,13,17,19]). The quantum codes obtained in this way are called stabilizer codes. In the literature, many quantum codes have been obtained from classical linear codes with symplectic, Euclidean or Hermitian self-orthogonality (see [1,14,20], etc).

For a prime power q, a q-ary $((n, K, d))$ quantum code is a K -dimensional vector subspace of the Hilbert space $(\mathbb{C}^q)^{\otimes n}$ which can detect up to $d-1$ quantum errors, or equivalently, correct up to $\lfloor (d-1)/2 \rfloor$ quantum errors. If we put $k = \log_q K$, we denote a q-ary $((n, K, d))$ quantum code by $[[n, k, d]]_q$. It is well known that the parameters of an $[[n, k, d]]_q$ quantum code have to satisfy the quantum Singleton bound: $k \leq n - 2d + 2$. A quantum code achieving this quantum Singleton bound is called a quantum maximum-distance-separable (MDS) code.

In the past few years, a lot of research work has been done for construction of quantum MDS codes and several new families of quantum MDS codes have been constructed (see [4,5,7,8,10–12,14,15,21–23]). If the classical MDS conjecture holds, then the length of a q-ary quantum stabilizer MDS code is upper bounded by $q^2 + 1$ [13]. It is interesting to construct all possible quantum MDS codes. The problem of constructing q-ary quantum MDS codes with $n \leq q + 1$ has been completely solved through classical Euclidean self-orthogonal codes [7,18]. On the other hand, a few families of q-ary quantum MDS codes with $n > q + 1$ have been given as well, most of which have minimum distance less than or equal to $q/2+1$ (see [4,5,7,8,12,18]). Thus, construction of q-ary quantum MDS codes with minimum distance bigger than $q/2 + 1$ turns out to be a more challenging task. Researchers have made a great effort to construct such quantum MDS codes through generalized Reed-Solomon codes, constacyclic codes and negacyclic codes (see [9–12,14,15,21–23]. However, these constructions provide q-ary quantum MDS codes only for some lengths n between $q+1$ and q^2+1. Therefore, the construction of quantum MDS codes with relatively large minimum distance still remains to be solved.

In this paper, we construct some new quantum MDS codes with minimum distance bigger than $q/2 + 1$ through classical Hermitian self-orthogonal generalized Reed-Solomon codes. More precisely, we select a suitable set of distinct elements $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq \mathbb{F}_{q^2}$ and a set of nonzero elements $\{v_1, v_2, \ldots, v_n\} \subseteq \mathbb{F}_{q^2}^*$ to obtain a Hermitian self-orthogonal generalized Reed-Solomon code $\{(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)) : \deg(f) \leq k-1\}$. The key step in the construction of such a code is to find sets $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ and $\{v_1, v_2, \ldots, v_n\}$. Finding the sets $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ and $\{v_1, v_2, \ldots, v_n\}$ is further reduced to finding a solution in $(\mathbb{F}_q^*)^n$ of the equation $\sum_{\ell=1}^{n} \alpha_\ell^{qi+j} x_\ell = 0$ for all $i, j \in \{0, 1, \ldots, k-1\}$.

1.1 Main result and comparison with previous constructions

Previously, the known q-ary quantum MDS codes with minimum distance bigger than $q/2+1$ have only sporadic and special lengths n. More precisely, there exist q-ary $[[n, n-2d+2, d]]$ quantum MDS codes for the following n and d (we list some of the main results below):

(i) $n = q^2 + 1$ and $d = q + 1$ (see [14]); and $n = q^2 + 1$ and $d \leq q + 1$ for even q and odd d (see [8]); and $n = q^2 + 1$ and $d \leq q + 1$ for $q \equiv 1 \mod 4$ and even d (see [12]).
(ii) $n = q^2$ and $d \leq q$ (see [7,10,14]).
(iii) $n = (q^2 + 1)/2$ and $q/2 + 1 < d \leq q$ for odd q (see [12]).
(iv) $n = r(q + 1)$, $r|q - 1$ and $\frac{q-1}{r}$ is even, $2 \leq d \leq \frac{q+r+1}{2}$ (see [4]).
(v) $n = r(q - 1)$ and $2 \leq d \leq (q + 1)/2 + r - 1$, $q + 1 = rt$ with r even (see [21]).

(vi) $n = r(q-1)+1$ and $d \le (q+r+1)/2$ for $q \equiv r-1 \mod 2r$ (see [9]).
(vii) $n = r(q+1)$ and $2 \le d \le (q+1)/2 + r$ for $r|q-1$, r odd, q odd (see [11]).
(viii) $n = 2r(q+1)$ and $2 \le d \le (q+1)/2 + 2r$ for $r|q-1$, r odd, $q \equiv 1 \mod 4$ odd (see [11]).

Based on the above quantum codes, by using a propagation rule [6], one can obtain more quantum MDS codes with smaller length and minimum distance that are still bigger than $q/2+1$.

Our paper demonstrates new q-ary $[[n, n-2k, k+1]]$ quantum MDS codes with the following parameters:

(i) Let $t \ge 1$ be an integer, $1 \le r \le 2t+1$ and $\gcd(r,q) = 1$.$q \equiv -1 \mod 2t+1$, $n = 1 + \frac{r(q^2-1)}{2t+1}$ and $k \le \frac{t+1}{2t+1} \times q - \frac{t}{2t+1}$.
(ii) Let $t \ge 1$ be an integer, $1 \le r \le 2t+1$ and $\gcd(r,q) > 1$. $q \equiv -1 \mod 2t+1$, $n = \frac{r(q^2-1)}{2t+1}$ and $k \le \frac{t+1}{2t+1} \times q - \frac{t}{2t+1}$.
(iii) $1 \le k \le q-1$, and some $n \in [2k, k^2+1]$.

For instance, some examples in these classes include q-ary $[n, n-2k, k+1]$-quantum MDS codes for the cases: (i) $q \equiv -1 \mod 5$, $n = (q^2+4)/5$ and $1 \le k \le (3q-2)/5$; (ii) $q \equiv -1 \mod 7$, $n = (q^2+6)/7$ and $1 \le k \le (4q-3)/7$; (iii) $2|q$, $q \equiv -1 \mod 3$, $n = 2(q^2-1)/3$ and $1 \le k \le (2q-1)/3$; and (iv) $2|q$, $q \equiv -1 \mod 5$, $n = 2(q^2-1)/5$ and $1 \le k \le (3q-2)/5$.

1.2 Organization

The paper is organized as follows. In Sect. 2, we present a systematic method to construct Hermitian self-orthogonal generalized Reed-Solomon codes. We apply the results in Sect. 2 to obtain quantum MDS codes in Sect. 3.

2 Construction of Hermitian self-orthogonal codes

2.1 Hermitian self-orthogonality

For a vector $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_{q^2}^n$, we denote by $\mathbf{v}^q$ the vector $(v_1^q, v_2^q, \ldots, v_n^q)$. For a subset V in $\mathbb{F}_{q^2}^n$, denote by V^q the set $\{\mathbf{v}^q : \mathbf{v} \in V\}$.

Two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{F}_{q^2}^n$ are called Hermitian orthogonal if $\mathbf{u} \cdot \mathbf{v}^q = 0$, where $\cdot$ denotes the usual Euclidean product or dot product. For an $\mathbb{F}_{q^2}$-linear code C in $\mathbb{F}_{q^2}^n$, the Hermitian dual, denoted by $C^{\perp_H}$, of C is defined to be the set $\{\mathbf{x} \in \mathbb{F}_{q^2}^n : \mathbf{x} \cdot \mathbf{c}^q = 0 \text{ for all } \mathbf{c} \in C\}$. It is easy to see that $C^{\perp_H}$ is an $\mathbb{F}_{q^2}$-linear code and $C^{\perp_H} = \left(C^{\perp_E}\right)^q$, where $C^{\perp_E}$ is the usual Euclidean dual of C. In particular, C is called Hermitian self-orthogonal if $C \subseteq C^{\perp_H}$. The $\mathbb{F}_{q^2}$-dimension of $C^{\perp_H}$ is $n - \dim_{\mathbb{F}_{q^2}}(C)$.

2.2 $\mathbb{F}_q$-solution of equation systems

Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be n distinct elements in $\mathbb{F}_{q^2}$. Let S be a subset of $\{0, 1, \ldots, q^2-2\}$ and consider the set

$$T_S(\alpha_1, \alpha_2, \ldots, \alpha_n) := \{(\alpha_1^{i+qj}, \alpha_2^{i+qj}, \ldots, \alpha_n^{i+qj}) : i, j \in S\}. \quad (1)$$

Here, 0^0 is set to be 1. We simply denote $T_S(\alpha_1, \alpha_2, \ldots, \alpha_n)$ by T_S if there is no confusion.

Lemma 2.1 *The $\mathbb{F}_{q^2}$-linear span* $\mathrm{Span}(T_S)$ *has a basis in $\mathbb{F}_q^n$.*

Proof Let V be the set $\{\mathbf{v} \in \mathrm{Span}(T_S) : \mathbf{v}^q = \mathbf{v}\}$. Then it is clear that $V = \mathrm{Span}(T_S) \cap \mathbb{F}_q^n$. Thus, it is sufficient to show that every vector in $\mathrm{Span}(T_S)$ is an $\mathbb{F}_{q^2}$-linear combination of vectors in V.

Note that $T_S^q = T_S$ since $(\alpha_\ell^{i+qj})^q = \alpha_\ell^{iq+j}$ for all $1 \le \ell \le n$ and $i, j \in S$. This implies that $\mathrm{Span}(T_S)^q = \mathrm{Span}(T_S)$.

Let $1, \alpha$ be an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^2}$. For any $\mathbf{v} \in \mathrm{Span}(T_S)$, consider the vectors $\mathbf{v}_1 = \mathbf{v} + \mathbf{v}^q$ and $\mathbf{v}_2 = \alpha\mathbf{v} + \alpha^q\mathbf{v}^q$. It is easy to see that both $\mathbf{v}_1$ and $\mathbf{v}_2$ belong to V. Since the 2×2 matrix $\begin{pmatrix} 1 & 1 \\ \alpha & \alpha^q \end{pmatrix}$ is invertible, we have

$$\begin{pmatrix} \mathbf{v} \\ \mathbf{v}^q \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \alpha & \alpha^q \end{pmatrix}^{-1} \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \end{pmatrix}. \quad (2)$$

This completes the proof. □

Lemma 2.2 *If the $\mathbb{F}_{q^2}$-linear span* $\mathrm{Span}(T_S)$ *has dimension less than n, then the system of equations $A_S\mathbf{x} = \mathbf{0}$ has a nonzero solution in $\mathbb{F}_q^n$, where the rows of A_S consist of all $|S|^2$ vectors in T_S.*

Proof Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in \mathbb{F}_q^n$ be an $\mathbb{F}_{q^2}$-basis of $\mathrm{Span}(T_S)$, where k is the dimension of the $\mathbb{F}_{q^2}$-linear span $\mathrm{Span}(T_S)$. Let A be the $k \times n$ matrix whose rows consist of $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$. Then the system of equations $A\mathbf{x} = \mathbf{0}$ and $A_S\mathbf{x} = \mathbf{0}$ has the same solution space. Since $k < n$ and A is a matrix with entries in $\mathbb{F}_q$, the system $A\mathbf{x} = \mathbf{0}$ has at least one nonzero solution in $\mathbb{F}_q^n$. Thus, it is also a solution of $A_S\mathbf{x} = \mathbf{0}$. The proof is completed. □

Lemma 2.3 *Let $t \ge 1$ be an integer and assume that $q \equiv -1 \bmod 2t+1$ (and hence $(2t+1)|(q^2-1)$). For an integer r with $1 \le r \le 2t+1$ and $\gcd(r, q) = 1$, put $n = 1 + \frac{r(q^2-1)}{2t+1}$. Let $\gamma \in \mathbb{F}_{q^2}$ be a $\frac{q^2-1}{2t+1}$-th primitive root of unity and let $\beta_1, \ldots, \beta_r \in \mathbb{F}_{q^2}^*$ such that $\{\beta_i \langle\gamma\rangle\}_{i=1}^r$ represent distinct cosets of $\mathbb{F}_{q^2}^*/\langle\gamma\rangle$. Label the elements of the set $\{0\} \cup \left(\cup_{i=1}^r \beta_i \langle\gamma\rangle\right)$ by $\alpha_1, \alpha_2, \ldots, \alpha_n$. Then the equation system $A_S\mathbf{x} = \mathbf{0}$ has a nonzero solution in $(\mathbb{F}_q^*)^n$ if $S \subseteq \{0, 1, 2, \ldots, \frac{t+1}{2t+1} \times q - \frac{t}{2t+1} - 1\}$.*

Proof First we claim that, for any $i, j \in S$, $qi + j$ is not divisible by $(q^2-1)/(2t+1)$ unless $i = j = 0$. Suppose that this were not true. Then $qi + j$ is equal to $\ell(q^2-1)/(2t+1)$ for some $1 \le \ell \le 2t$ and $i, j \in S$. By the identity

$$qi + j = \ell \times \frac{q^2-1}{2t+1} = q \times \left(\frac{\ell q + \ell}{2t+1} - 1\right) + q - \frac{\ell(q+1)}{2t+1},$$

we have

$$i = \frac{\ell q + \ell}{2t+1} - 1, \qquad j = q - \frac{\ell(q+1)}{2t+1}. \quad (3)$$

Case 1. $\ell \geq t+1$. Then

$$i \geq \frac{(t+1)(q+1)}{2t+1} - 1 > \frac{t+1}{2t+1} \times q - \frac{t}{2t+1} - 1.$$

Thus, $i \notin S$ and hence this contradicts the fact that $i \in S$.

Case 2. $\ell \leq t$. Then

$$j \geq q - \frac{t(q+1)}{2t+1} > \frac{t+1}{2t+1} \times q - \frac{t}{2t+1} - 1.$$

Thus, $j \notin S$ and hence this contradicts the fact that $j \in S$.

For $i, j \in S$ with $(i, j) \neq (0, 0)$, by the above fact one can write $qi + j = c \times \frac{q^2-1}{2t+1} + a$ for some $c \geq 0$ and $1 \leq a \leq \frac{q^2-1}{2t+1} - 1$.

Now it is clear that the first row of A_S is the all-one vector $\mathbf{1}$ and every other row has the form

$$\left(0, \beta_1^{qi+j}, \beta_1^{qi+j}\gamma^a, \beta_1^{qi+j}\gamma^{2a} \ldots, \beta_1^{qi+j}\gamma^{\left(\frac{q^2-1}{2t+1}-1\right)a}, \ldots,\right.$$

$$\left.\beta_r^{qi+j}, \beta_r^{qi+j}\gamma^a, \beta_r^{qi+j}\gamma^{2a}, \ldots, \beta_r^{qi+j}\gamma^{\left(\frac{q^2-1}{2t+1}-1\right)a}\right)$$

for some $i, j \in S$ with $(i, j) \neq (0, 0)$ and $1 \leq a \leq \frac{q^2-1}{2t+1} - 1$. Therefore, the vector $\left(-\frac{r(q^2-1)}{2t+1}, 1, 1, \ldots, 1\right)$ is a solution of the equation $A_S\mathbf{x} = \mathbf{0}$. The proof is completed. □

Lemma 2.4 *Let $t \geq 1$ be an integer and assume that $q \equiv -1 \bmod 2t+1$. For an integer r with $1 \leq r \leq 2t+1$ and $\gcd(r, q) > 1$, put $n = \frac{r(q^2-1)}{2t+1}$. Let $\gamma \in \mathbb{F}_{q^2}$ be a $\frac{q^2-1}{2t+1}$-th primitive root of unity and let $\beta_1, \ldots, \beta_r \in \mathbb{F}_{q^2}^*$ such that $\{\beta_i\langle\gamma\rangle\}_{i=1}^r$ represent distinct cosets of $\mathbb{F}_{q^2}^*/\langle\gamma\rangle$. Label the elements of the set $\cup_{i=1}^r \beta_i\langle\gamma\rangle$ by $\alpha_1, \alpha_2, \ldots, \alpha_n$. Then the equation system $A_S\mathbf{x} = \mathbf{0}$ has a nonzero solution in $(\mathbb{F}_q^*)^n$ if $S \subseteq \{0, 1, 2, \ldots, \frac{t+1}{2t+1} \times q - \frac{t}{2t+1} - 1\}$.*

Proof First of all, the condition $\gcd(r, q) > 1$ implies that the length n is divisible by the characteristic of $\mathbb{F}_q$.

From the proof of Lemma 2.3, we know that, for $i, j \in S$ with $(i, j) \neq (0, 0)$, one can write $qi + j = c \times \frac{q^2-1}{2t+1} + a$ for some $c \geq 0$ and $1 \leq a \leq \frac{q^2-1}{2t+1} - 1$.

Now it is clear that the first row of A_S is the all-one vector $\mathbf{1}$ and every other row has the form

$$\left(\beta_1^{qi+j}, \beta_1^{qi+j}\gamma^a, \beta_1^{qi+j}\gamma^{2a} \ldots, \beta_1^{qi+j}\gamma^{\left(\frac{q^2-1}{2t+1}-1\right)a}, \ldots,\right.$$

$$\left.\beta_r^{qi+j}, \beta_r^{qi+j}\gamma^a, \beta_r^{qi+j}\gamma^{2a}, \ldots, \beta_r^{qi+j}\gamma^{\left(\frac{q^2-1}{2t+1}-1\right)a}\right)$$

for some $i, j \in S$ with $(i, j) \neq (0, 0)$ and $1 \leq a \leq \frac{q^2-1}{2t+1} - 1$. Therefore, the vector $(1, 1, \ldots, 1)$ is a solution of the equation $A_S\mathbf{x} = \mathbf{0}$. The proof is completed. □

2.3 Hermitian self-orthogonal codes

For a subset S of $\{0, 1, 2, \ldots, q^2-1\}$, denote by $\mathcal{P}_S$ the $\mathbb{F}_{q^2}$-linear space of polynomials

$$\mathcal{P}_S := \mathrm{Span}\{x^i : i \in S\}. \tag{4}$$

In particular, for $S = \{0, 1, 2, \ldots, k-1\}$, we denote $\mathcal{P}_S$ by $\mathcal{P}_k$. It is clear that the dimension of $\mathcal{P}_S$ is $|S|$. Furthermore, for a vector $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^2}^*)^n$ and n distinct elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ in $\mathbb{F}_{q^2}$, we define the $\mathbb{F}_{q^2}$-linear code

$$C_S(\mathbf{a}, \mathbf{v}) = \{(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)) : f \in \mathcal{P}_S\}, \tag{5}$$

where $\mathbf{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Assume that the largest number $i_{\max}$ of S is less than n, then $C_S(\mathbf{v})$ is an $[n, |S|, \geq n - i_{\max}]$-linear code over $\mathbb{F}_{q^2}$.

Lemma 2.5 *Let S be a subset of $\{0, 1, 2, \ldots, q^2-1\}$. Assume that $A_S\mathbf{x} = \mathbf{0}$ has a solution $(b_1, b_2, \ldots, b_n) \in (\mathbb{F}_q^*)^n$. Let $v_i \in \mathbb{F}_{q^2}^*$ such that $v_i^{q+1} = b_i$ for all $1 \leq i \leq n$. Then the code $C_S(\mathbf{a}, \mathbf{v})$ is Hermitian self-orthogonal.*

The proof of Lemma 2.5 is straightforward. Note that v_i always exists since $b_i \in \mathbb{F}_q$.

Now we apply Lemmas 2.3 and 2.4 to obtain two classes of Hermitian self-orthogonal codes.

Theorem 2.6 *Let $t \geq 1$ be an integer and assume that $q \equiv -1 \bmod 2t+1$.*

(i) *For an integer r with $1 \leq r \leq 2t+1$ and $\gcd(r, q) = 1$, put $n = 1 + \frac{r(q^2-1)}{2t+1}$. Then for any $k \leq \frac{t+1}{2t+1} \times q - \frac{t}{2t+1}$, there exists a Hermitian self-orthogonal $[n, k]$-MDS code over $\mathbb{F}_{q^2}$.*

(ii) *For an integer r with $1 \leq r \leq 2t+1$ and $\gcd(r, q) > 1$, put $n = \frac{r(q^2-1)}{2t+1}$. Then for any $k \leq \frac{t+1}{2t+1} \times q - \frac{t}{2t+1}$, there exists a Hermitian self-orthogonal $[n, k]$-MDS code over $\mathbb{F}_{q^2}$.*

Proof (i) Consider the set $S = \{0, 1, 2, \ldots, k-1\}$. Let $\gamma \in \mathbb{F}_{q^2}$ be a $\frac{q^2-1}{2t+1}$-th primitive root of unity and let $\beta_1, \ldots, \beta_r \in \mathbb{F}_{q^2}^*$ such that $\{\beta_i \langle\gamma\rangle\}_{i=1}^r$ represent distinct cosets of $\mathbb{F}_{q^2}^*/\langle\gamma\rangle$. Label the elements of the set $\{0\} \cup \left(\cup_{i=1}^r \beta_i \langle\gamma\rangle\right)$ by $\alpha_1, \alpha_2, \ldots, \alpha_n$. Let $v_i = 1$ for all $2 \leq i \leq n$ and $v_i \in \mathbb{F}_{q^2}^*$ such that $v_1^{q+1} = -\frac{r(q^2-1)}{2t+1}$. Then by Lemmas 2.3 and 2.5, the code $C_S(\mathbf{a}, \mathbf{v})$ is Hermitian self-orthogonal.

(ii) Similarly, this part follows from Lemmas 2.4 and 2.5.

□

For certain given length n, Theorem 2.6 provides Hermitian self-orthogonal codes with dimension bigger than $q/2$. In the following theorem, for given dimension k, we provide Hermitian self-orthogonal codes for certain length.

Theorem 2.7 *For any k with $1 \leq k \leq q-1$, there exists a Hermitian self-orthogonal $[n, k]$-MDS code for some n with $2k \leq n \leq k^2+1$.*

Proof Choose a subset $\mathcal{A} = \{\beta_1, \beta_2, \ldots, \beta_{k^2+1}\}$ of $\mathbb{F}_{q^2}$ and consider the generalized Reed-Solomon code $C = \{(f(\beta_1), f(\beta_2), \ldots, f(\beta_{k^2+1})) : f \in \mathcal{P}_k\}$. Then the Euclidean dual

$C^{\perp_E}$ of C has minimum distance $k+1$. Let $S = \{0, 1, 2, \ldots, k-1\}$ and consider the $(k^2+1) \times k^2$ matrix A_S whose rows consists of $(\beta_1^{qi+j}, \beta_2^{qi+j}, \ldots, \beta_{k^2+1}^{qi+j})$ for all $0 \le i, j \le k-1$. By Lemma 2.2, the equation $A_S \mathbf{x} = \mathbf{0}$ has a nonzero solution $\mathbf{b} = (b_1, b_2, \ldots, b_{k^2+1}) \in \mathbb{F}_q^n$. It is clear that $\mathbf{b}$ is a codeword of $C^{\perp_E}$ and hence the Hamming weight $\mathrm{wt}_H(\mathbf{b}) \ge k+1$. Let the support of $\mathbf{b}$ be $\{i_1, i_2, \ldots, i_n\}$ and denote β_{i_j} by α_j. Let $v_j \in \mathbb{F}_{q^2}$ such that $v_j^{q+1} = b_{i_j}$. Then it is easy to see that $C_S(\mathbf{a}, \mathbf{v})$ is Hermitian self-orthogonal, where $S = \{0, 1, \ldots, k-1\}$. Furthermore, it is clear that $C_S(\mathbf{a}, \mathbf{v})$ is an $[n, k]$-MDS code. Since C is Hermitian self-orthogonal, we must have $n \ge 2k$. The proof is completed. □

3 Construction of Quantum codes

The construction of quantum codes in this section is based on a connection between classical Hermitian self-orthogonal codes and quantum codes given in [2].

Lemma 3.1 ([2]) *There exists a q-ary $[[n, n-2k, k+1]]$ quantum code whenever there is a q^2-ary classical Hermitian self-orthogonal $[n, k]$ MDS code.*

3.1 Quantum MDS codes

Combining Theorem 2.6 with Lemma 3.1 gives the following quantum MDS codes.

Theorem 3.2 *There exists a q-ary $[[n, n-2k, k+1]]$-quantum MDS code for the following q, n and k.*

(i) *Let $t \ge 1$ be an integer and let r satisfy $1 \le r \le 2t+1$ and $\gcd(r, q) = 1$. The parameters q, n and k satisfy $q \equiv -1 \bmod 2t+1$, $n = 1 + \frac{r(q^2-1)}{2t+1}$ and $k \le \frac{t+1}{2t+1} \times q - \frac{t}{2t+1}$.*

(ii) *Let $t \ge 1$ be an integer and let r satisfy $1 \le r \le 2t+1$ and $\gcd(r, q) > 1$. The parameters q, n and k satisfy $q \equiv -1 \bmod 2t+1$, $n = \frac{r(q^2-1)}{2t+1}$ and $k \le \frac{t+1}{2t+1} \times q - \frac{t}{2t+1}$.*

Remark 1 The family of quantum MDS codes constructed in Theorem 3.2 are new except for the case of $t = r = 1$ in Theorem 3.2(i) which was presented in [9].

In the following example, we show some quantum MDS codes from Theorem 3.2(i).

Example 3.3 By taking $r = 1$ and $t = 1, 2, 3, 4$ in Theorem 3.2(i), respectively, we obtain the following q-ary quantum codes.

(i) If $q \equiv -1 \bmod 3$, then there exists a q-ary $[(q^2+2)/3, (q^2+2)/3-2k, k+1]$ quantum MDS code for any $k \le (2q-1)/3$. This class was presented in [9].

(ii) If $q \equiv -1 \bmod 5$, then there exists a q-ary $[(q^2+4)/5, (q^2+4)/5-2k, k+1]$ quantum MDS code for any $k \le (3q-2)/5$.

(iii) If $q \equiv -1 \bmod 7$, then there exists a q-ary $[(q^2+6)/7, (q^2+6)/7-2k, k+1]$ quantum MDS code for any $k \le (4q-3)/7$.

Example 3.4 Let q be even. By taking $r = 2$ and $t = 1, 2, 3, 4$ in Theorem 3.2(ii), respectively, we obtain the following q-ary quantum codes.

(i) If $q \equiv -1 \bmod 3$, then there exists a q-ary $[2(q^2-1)/3, 2(q^2-1)/3-2k, k+1]$ quantum MDS code for any $k \le (2q-1)/3$.

(ii) If $q \equiv -1 \bmod 5$, then there exists a q-ary $[2(q^2-1)/5, 2(q^2-1)/5 - 2k, k+1]$ quantum MDS code for any $k \leq (3q-2)/5$.
(iii) If $q \equiv -1 \bmod 7$, then there exists a q-ary $[2(q^2-1)/7, 2(q^2-1)/7 - 2k, k+1]$ quantum MDS code for any $k \leq (4q-3)/7$.

Remark 2 To the best of our knowledge, except for the quantum MDS codes given in Example 3.3(i), all other quantum MDS codes in Examples 3.3 and 3.4 are new.

Theorem 3.5 *For any $1 \leq k \leq q-1$, one can find some $n \in [2k, k^2+1]$ such that there exists a q-ary $[[n, n-2k, k+1]]$-quantum MDS code.*

Remark 3 Theorem 3.5 in fact produces some new quantum codes. For instance, for even q, we obtain an $[n, n-q-2, q/2+2]$-quantum MDS codes for some $n \in [q+2, (q/2+1)^2+1]$. This code could not be produced by propagation rules from known codes.

Acknowledgements The authors would like to thank the referees for many helpful comments. The research work of the first author is supported in part by Shanghai Sailing Program under the Grant 15YF1401200 and by the National Natural Science Foundation of China under Grant 11501117. The research work of the second author and third author are supported in part by the National Natural Science Foundation of China under Grant 61672166, in part by the Shanghai Excellent Academic Leaders under Grant 16XD1400200, and in part by the Shanghai Innovation Plan of Science and Technology under Grant 16JC1402700.

References

1. Aly S.A., Klappenecker A., Sarvepalli P.K.: On quantum and classical BCH codes. IEEE Trans. Inf. Theory **53**(3), 1183–1188 (2007).
2. Ashikhmin A., Knill E.: Nonbinary quantum stabilizer codes. IEEE Trans. Inf. Theory **47**(7), 3065–3072 (2001).
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**(4), 1369–1387 (1998).
4. Chen B., Ling S., Zhang G.: "Apllication of constacyclic codes to quantum MDS codes", exists. IEEE Trans. Inf. Theory **61**(3), 1474–1484 (2015).
5. Feng K.: Quantum code $[[6, 2, 3]]_p$ and $[[7, 3, 3]]_p (p \geq 3)$ exists. IEEE Trans. Inf. Theory **48**(8), 2384–2391 (2002).
6. Feng K., Ling S., Xing C.: Asymptotic bounds on quantum codes from algebraic geometry codes. IEEE Trans. Inf. Theory **52**(3), 986–991 (2006).
7. Grassl M., Beth T., Röttler M.: On optimal quantum codes. Int. J. Quantum Inf. **2**(1), 757–775 (2004).
8. Guardia G.G.L.: New quantum MDS codes. IEEE Trans. Inf. Theory **57**(8), 5551–5554 (2011).
9. Jin L.F., Xing C.P.: A construction of new Quantum MDS codes. IEEE Trans. Inf. Theory **60**, 2921–2925 (2014).
10. Jin L.F., Ling S., Luo J.Q., Xing C.P.: Application of classical Hermitian self-orthogonal MDS codes to Quantum MDS codes. IEEE Trans. Inf. Theory **56**, 4735–4740 (2010).
11. Kai X., Zhu S., Li P.: Constacyclic codes and some new quantum MDS codes. IEEE Trans. Inf. Theory **60**(4), 2080–2086 (2014).
12. Kai X., Zhu S.: New quantum MDS codes from negacyclic codes. IEEE Trans. Inf. Theory **59**(2), 1193–1197 (2012).
13. Ketkar A., Klappenecker A., Kumar S., Sarvepalli P.: Nonbinary stablizer codes over finite fields. IEEE Trans. Inf. Theory **52**(11), 4892–4914 (2006).
14. Li Z., Xing L.J., Wang X.M.: Quantum generalized Reed-Solomon codes: unified framework for quantum MDS codes. Phys. Rev. A **77**, 012308-1–012308-4 (2008).
15. Li R., Xu Z.: Construction of $[[n, n-4, 3]]_q$ quantum MDS codes for odd prime power q. Phys. Rev. A **82**, 052316-1–052316-4 (2010).
16. Ling S., Xing C.P.: Coding Theory—A First Course. Cambridge University Press, Cambridge (2004).
17. Rains E.M.: Nonbinary quantum codes. IEEE. Trans. Inf. Theory **45**(6), 1827–1832 (1999).
18. Röttler M., Grassl M. Beth,T.: On quantum MDS codes. In: Proceedings of the International Symposium on Information Thoory, Chicago, USA, pp. 356 (2004).

19. Shor P.W.: Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A **52**(4), R2493–R2496 (1995).
20. Steane A.M.: Enlargement of Calderbank–Shor–Steane quantum codes. IEEE. Trans. Inf. Theory **45**(7), 2492–2495 (1999).
21. Wang L.Q., Zhu S.X.: New quantum MDS codes derived from constacyclic codes. Quantum Inf. Process. **14**(3), 881–889 (2015).
22. Zhang G., Chen B.: New quantum MDS codes. Int. J. Quantum Inf. **12**(4), 1450019 (2014).
23. Zhang T., Ge G.: Some new classes of quantum MDS codes from constacyclic codes. IEEE Trans. Inf. Theory **61**(9), 52240–52248 (2015).