Construction of $[[n,n-4,3]]_q$ quantum codes for odd prime power q

Ruihu Li[1,2,*] and Zongben Xu[1]

[1] *Institute for Information and System Sciences, Xi'an Jiaotong University, Shaanxi 710049, China*

[2] *College of Science, Air Force Engineering University, Xi'an, Shaanxi 710051, China*

(Received 29 March 2010; published 16 November 2010)

For each odd prime power q, let $4 \leqslant n \leqslant q^2+1$. Hermitian self-orthogonal $[n,2,n-1]$ codes over $\mathbf{F}_{q^2}$ with dual distance three are constructed by using finite field theory. Hence, $[[n,n-4,3]]_q$ quantum maximal-distance-separable (MDS) codes for $4 \leqslant n \leqslant q^2+1$ are obtained.

DOI: 10.1103/PhysRevA.82.052316 PACS number(s): 03.67.Pp

I. INTRODUCTION

The theory of quantum error-correcting codes (QECCs, for short) has been exhaustively studied in the literature; see [1–8]. The most widely studied class of quantum codes are binary quantum stabilizer codes. A thorough discussion on the principles of quantum coding theory was given in [3] and [4] for binary quantum stabilizer codes. An appealing aspect of binary quantum codes is that there exist links to classical coding theory which make easy the construction of good quantum codes [8].

More recently similar theories of nonbinary quantum stabilizer codes were established in [6–8]; characterization of nonbinary quantum stabilizer codes over $\mathbf{F}_q$ (the finite field with q elements) in terms of classical codes over $\mathbf{F}_{q^2}$ was also given. Based on [6–8], many nonbinary quantum stabilizer codes were constructed from classical nonbinary codes; see [6–8] and references therein.

One central theme in quantum error correction is the construction of quantum codes with good parameters [1–22]. Among these codes, quantum maximal-distance-separable (MDS) codes received much attention. Quantum MDS codes are optimal quantum codes, since they meet the quantum Singleton bound.

Lemma 1.1 (quantum Singleton bound [5,8]). An $[[n,k,d]]_q$ quantum stabilizer code satisfies

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

It is known that except for trivial codes (codes with $d \leqslant 2$), there are only two binary quantum MDS codes, $[[5,1,3]]_2$ and $[[6,0,4]]_2$; see [3]. Nonbinary quantum MDS codes are much more complex compared with the binary case. Recently many families of nonbinary quantum MDS codes have been found by various approaches [15–18]. In the simplest nontrivial case $d=3$, despite many efforts to construct nonbinary quantum MDS codes, a systematic construction for all q and all lengths has not been achieved yet; see [15–18] and [23]. If $d \geqslant 3$, Ref. [8] proved that the maximal length n of $[[n,k,d]]_q$ quantum MDS codes satisfies $n \leqslant q^2+d-2$. In [21], we discussed the construction of quantum MDS codes $[[n,n-4,3]]_q$ for odd prime power q. The method of [21] has been used by [22] to construct ternary quantum codes of minimum distance three for all length $n \geqslant 4$, and some new advancement that following [21] has been given in [23].

In this paper (we let $q=p^r$ and p be an odd prime), we will use Hermitian self-orthogonal codes over $\mathbf{F}_{q^2}$ to construct q-ary quantum MDS codes of distance three. This paper is a revised version of [21]; some changes in the notation and proofs are made in this paper. The main result of this paper is as follows.

Theorem 1.1. If $q=p^r$ and p is an odd prime, then there are $[[n,n-4,3]]_q$ quantum MDS codes for $4 \leqslant n \leqslant q^2+1$.

This paper is arranged as follows. In Sec. II some preliminary materials are introduced and a method of proving our main results is explained. In Secs III and IV, the proof of the main result of this paper is presented. In Sec. V, a concluding remark is given.

II. PRELIMINARIES

In order to prove our main result, we make some preparation on quantum codes and finite fields.

Let $\mathbf{F}_{q^2}^n$ be the n-dimensional vector space over the finite field $\mathbf{F}_{q^2}$. For $X=(x_1,x_2,\ldots,x_n)$, $Y=(y_1,y_2,\ldots,y_n)\in\mathbf{F}_{q^2}^n$, the Hermitian inner product of X and Y is defined as follows:

$$(X,Y)=x_1y_1^q+x_2y_2^q+\cdots+x_ny_n^q.$$

If $\mathcal{C}$ is an $[n,k]_{q^2}$ linear code over $\mathbf{F}_{q^2}$, its Hermitian dual code is defined by

$$\mathcal{C}^{\perp h}=\left\{X \mid X\in\mathbf{F}_{q^2}^n,(X,Y)=0 \text{ for any } Y\in\mathcal{C}\right\}.$$

$\mathcal{C}$ is Hermitian self-orthogonal if $\mathcal{C}\subseteq\mathcal{C}^{\perp h}$, and self-dual if $\mathcal{C}=\mathcal{C}^{\perp h}$.

The following theorem is well known for constructing q-ary quantum codes from Hermitian self-orthogonal codes over $\mathbf{F}_{q^2}$, which was given in [8] and [16].

Theorem 2.1 (*Hermitian construction*). If $\mathcal{C}$ is an $[n,k]_{q^2}$ linear code such that $\mathcal{C}^{\perp h}\subseteq\mathcal{C}$, and $d=\min\{wt(v): v\in\mathcal{C}\setminus\mathcal{C}^{\perp h}\}$, then there exists $[[n,2k-n,d]]_q$ quantum code.

In the construction of self-orthogonal codes, we also need the following results on finite fields.

Lemma 2.1. If α is a primitive element of $\mathbf{F}_{q^2}$, for each nonzero element ξ of $\mathbf{F}_q$, there are $q+1$ elements α^i of $\mathbf{F}_{q^2}$ such that $(\alpha^i)^{q+1}=\xi$.

Proof. Suppose $(\alpha)^{q+1}=\beta$, then β is a primitive element of F_q. Let $\xi=\beta^i, 0\leqslant i\leqslant q-2$. Then $(\alpha^{i+(q-1)j})^{q+1}=\xi$ for $0\leqslant j\leqslant q$, thus the lemma holds.

Lemma 2.2. If α is a primitive element of $\mathbf{F}_{q^2}$, then $1+(\alpha)^{q+1}+(\alpha^2)^{q+1}+\cdots+(\alpha^{q^2-2})^{q+1}=0$.

*liruihu2008@yahoo.com.cn

Proof. Suppose $(\alpha)^{q+1}=\beta$, then $1+(\alpha)^{q+1}+(\alpha^2)^{q+1}+\cdots+(\alpha^{q^2-2})^{q+1}=(q+1)(1+\beta+\beta^2+\cdots+\beta^{q-2})=0$.

Notation 2.1. We divide the nonzero elements of $\mathbf{F}_{q^2}$ into two subsets, say A and B. Let $A=\{1,-1,\alpha^{\frac{q-1}{2}},-\alpha^{\frac{q-1}{2}},\alpha^{\frac{q-1}{2}}+1,-\alpha^{\frac{q-1}{2}}-1\}$, $B=\{x_1,-x_1,\ldots,x_k,-x_k\}=\mathbf{F}_{q^2}\setminus(A\cup\{0\})$, where $2k=q^2-7$. For k_1 satisfying $0\leqslant k_1\leqslant k$, denote the vector $(x_1,-x_1,\ldots,x_{k_1},-x_{k_1})$ as X_{2k_1}. And we use Y_3 to denote the vector $(1,\alpha^{\frac{q-1}{2}},-\alpha^{\frac{q-1}{2}}-1)$.

Notation 2.2. To save space and simplify statements of the following two sections, we use $\mathbf{1_m}$ to denote the all one vector of length m. For $Z=(z_1,z_2,\ldots,z_m)\in\mathbf{F}_{q^2}^m$ and $\beta\in\mathbf{F}_{q^2}$, we use βZ to denote $(\beta z_1,\beta z_2,\ldots,\beta z_m)$.

Using the previous notation, we have the following.

Lemma 2.3. If A and B are defined as previously mentioned, then $2\Sigma_{i=1}^k(x_i)^{q+1}+2(\alpha^{\frac{q-1}{2}}+1)^{q+1}=0$.

Proof. Let α be a primitive element of $\mathbf{F}_{q^2}$. Since $(-\alpha^i)^{q+1}=(\alpha^i)^{q+1}$ for $0\leqslant i\leqslant q^2-2$ and $(\alpha^{\frac{q-1}{2}})^{q+1}=-1$. According to Lemma 2.2, one can deduce that

$$\begin{aligned}
&1^{q+1}+(\alpha)^{q+1}+(\alpha^2)^{q+1}+\cdots+(\alpha^{q^2-2})^{q+1}\\
&=2\Sigma_{i=1}^k(x_i)^{q+1}+2+2\big(\alpha^{\frac{q-1}{2}}\big)^{q+1}+2\big(\alpha^{\frac{q-1}{2}}+1\big)^{q+1}\\
&=2\Sigma_{i=1}^k(x_i)^{q+1}+2\big(\alpha^{\frac{q-1}{2}}+1\big)^{q+1}\\
&=0.
\end{aligned}$$

Thus the lemma follows.

According to Theorem 2.1, for each n satisfying $4\leqslant n\leqslant q^2+1$, the problem of constructing $[[n,n-4,3]]_q$ quantum MDS codes can be changed into constructing $[n,2]_{q^2}$ Hermitian self-orthogonal code $\mathcal{C}_{2,n}$ over $\mathbf{F}_{q^2}$ with dual distance three. Hence, it is enough to construct a generator matrix $A_{2,n}$ of $\mathcal{C}_{2,n}$, where $A_{2,n}=\binom{K_n}{L_n}$ satisfies that any two columns of $A_{2,n}$ are linear independent, $(K_n,K_n)=(L_n,L_n)=0$ and $(K_n,L_n)=0$.

Our method of constructing $A_{2,n}$ is as follows: For $4\leqslant n\leqslant q^2-2$ and $n\neq q^2-3$, we construct $A_{2,n}$ by solving equations over $\mathbf{F}_{q^2}$. $A_{2,n}$ has the following form:

$$A_{2,n}=\begin{pmatrix}\gamma & | & \mathbf{1_{2k_1}} & | & a_{2k_1+2} & \cdots & a_{n-2} & 0\\ 0 & | & X_{2k_1} & | & b_{2k_1+2} & \cdots & b_{n-2} & \epsilon\end{pmatrix},$$

where $0\leqslant k_1\leqslant k$ and $4\leqslant n-2k_1\leqslant 6$, and each column $\binom{a_j}{b_j}=\delta_j\binom{1}{y_j}$ with $y_j\in A$ and y_j is different for different j. For $n=q^2-3$, q^2 and q^2+1, we construct $A_{2,n}$ with the following form:

$$A_{2,q^2-3}=\begin{pmatrix}1 & | & \mathbf{1_{2k}} & | & \delta\mathbf{1_3}\\ 0 & | & X_{2k} & | & \delta Y_3\end{pmatrix},$$

where

$$\delta_1^{q+1}=2;$$

$$A_{2,q^2}=\begin{pmatrix}1 & 1 & 1 & 1 & \cdots & 1 & 1\\ 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{q^2-3} & \alpha^{q^2-2}\end{pmatrix};$$

$$A_{2,q^2+1}=\begin{pmatrix}1 & | & \mathbf{1_{2k}} & | & \mathbf{1_3} & | & \delta\mathbf{1_3} & | & 0\\ 0 & | & X_{2k} & | & Y_3 & | & -\delta Y_3 & | & \epsilon\end{pmatrix}$$

for $q=3^r\geqslant 9$, where $\delta,\epsilon\in\mathbf{F}_{q^2}$ satisfying $\delta^{q+1}\in\mathbf{F}_q\setminus\mathbf{F}_3$, $\epsilon^{q+1}=(1-\delta^{q+1})(\alpha^{\frac{q-1}{2}}+1)^{q+1}$;

$$A_{2,q^2+1}=\begin{pmatrix}\gamma & | & \mathbf{1_{2k}} & | & \mathbf{1_3} & | & \delta\mathbf{1_3} & | & 0\\ 0 & | & X_{2k} & | & Y_3 & | & -\delta Y_3 & | & \epsilon\end{pmatrix}$$

for $q=p^r$ and prime $p\geqslant 5$, where $\gamma,\delta,\epsilon\in\mathbf{F}_{q^2}$ such that $\gamma^{q+1}=-2$, $\delta^{q+1}=2$, and $\epsilon^{q+1}=-(\alpha^{\frac{q-1}{2}}+1)^{q+1}$.

According to [24] and notations 2.1 and 2.2, each of the above matrix $A_{2,n}$ generates an $[n,2]_{q^2}$ code with dual distance 3. In particular, we have the following lemma.

Lemma 2.4. Let $q\neq 3$, $n=q^2-3$, q^2 or q^2+1, and $A_{2,n}$ be given as above. Then the code $\mathcal{C}_{2,n}$ generated by $A_{2,n}$ is an $[n,2]_{q^2}$ Hermitian self-orthogonal code with dual distance 3. Hence there is $[[n,n-4,3]]_q$ for these n.

Proof. According to notation 2.1 and 2.2, using Lemmas 2.1 and 2.2, one can deduce that for $n=q^2-3,q^2$, $A_{2,n}$ generates an $[n,2]_{q^2}$ Hermitian self-orthogonal code over $\mathbf{F}_{q^2}$ with dual distance 3.

For $n=q^2+1$, let the rows of A_{2,q^2+1} be K_n and L_n, respectively. If $q=3^r\geqslant 9$, then there is $b\in\mathbf{F}_q\setminus\mathbf{F}_3$. According to Lemma 2.1, one can choose $\delta,\epsilon\in\mathbf{F}_{q^2}$ satisfy $\delta^{q+1}=b$ and $\epsilon^{q+1}=(1-\delta^{q+1})(\alpha^{\frac{q-1}{2}}+1)^{q+1}$. Using Lemma 2.3, we can deduce $(K_n,K_n)=(L_n,L_n)=0$ and $(K_n,L_n)=0$. Thus, for $q=3^r\geqslant 9$, we have proved that A_{2,q^2+1} generate an $[n,2]_{q^2}$ Hermitian self-orthogonal code with dual distance 3.

If $q=p^r$ and prime $p\geqslant 5$, the proof can be given similarly.

Summarizing the previous discussion, the lemma holds.

III. $[[n,n-4,3]]_q$ FOR $q=3^r$

In this section, we will prove Theorem 1.1 holds for $q=3^r$.

First we discuss the construction of the $[[n,n-4,3]]_3$ quantum code.

Let $\mathbf{F}_3=\{0,1,2\}=\{0,1,-1\}$ be the Galois field with three elements. Then $f(x)=x^2+x+2$ is irreducible over $\mathbf{F}_3$. Using $f(x)$, one can construct the Galois field $\mathbf{F}_{q^2}$ with nine elements as $\mathbf{F}_9=\{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}$, where α is a root of $f(x)=x^2+x+2$. It is easy to check that α is a primitive element of $\mathbf{F}_9$, $\alpha^2=2\alpha+1$, $\alpha^3=2\alpha+2$, $\alpha^4=2$, $\alpha^5=2\alpha$, $\alpha^6=\alpha+2$, and $\alpha^7=\alpha+1$. It is obvious that $\alpha^{4+i}=-\alpha^i$ for $0\leqslant i\leqslant 7$.

Construct

$$G_{2,4}=\begin{pmatrix}1 & 1 & 1 & 0\\ 0 & 1 & -1 & 1\end{pmatrix},$$

$$G_{2,5}=\begin{pmatrix}1 & 1 & \alpha & \alpha & 0\\ 0 & 1 & \alpha^2 & \alpha^3 & \alpha\end{pmatrix},$$

$$G_{2,6}=\begin{pmatrix}1 & 1 & 1 & | & \alpha\mathbf{1_3}\\ 0 & \alpha^2 & \alpha^6 & | & \alpha Y_3\end{pmatrix},$$

$$G_{2,7}=\begin{pmatrix}1 & 1 & 1 & 1 & 1 & 1 & 0\\ 0 & 1 & \alpha^1 & \alpha^2 & \alpha^5 & \alpha^7 & 1\end{pmatrix},$$

$$G_{2,8}=\begin{pmatrix}1 & 1 & 1 & 1 & 1 & \alpha & \alpha & 0\\ 0 & 1 & 2 & \alpha^1 & \alpha^5 & 1 & 2 & 1\end{pmatrix},$$

$$G_{2,9}=\begin{pmatrix}1&1&1&\cdots&1\\0&1&\alpha^1&\cdots&\alpha^7\end{pmatrix},$$

$$G_{2,10}=\begin{pmatrix}1&1&1&|&\mathbf{1_3}&|&\alpha\mathbf{1_3}&|&0\\0&1&\alpha&|&\alpha^4Y_3&|&\alpha Y_3&|&1\end{pmatrix}.$$

For $4\leqslant n\leqslant 10$, let $G_{2,n}=\binom{K_n}{L_n}$ and $\mathcal{C}_{2,n}$ be the code generated by $G_{2,n}$. Using the arithmetic of $\mathbf{F}_9$, one can check that $(K_n,K_n)=(K_n,L_n)=(L_n,L_n)=0$. Thus, $\mathcal{C}_{2,n}$ is an Hermitian self-orthogonal code over $\mathbf{F}_9$ and $d^\perp=3$, hence there is an $[[n,n-4,3]]_3$ quantum MDS code.

Second, we discuss the construction of the $[[n,n-4,3]]_q$ quantum code for $q=3^r\geqslant 9$. To achieve this, we consider the construction of the $[n,2]_{q^2}$ Hermitian self-orthogonal codes with dual distance three in three cases separately.

Case 3.1. $4\leqslant n\leqslant q^2-4$ and $n\equiv 0\,(\mathrm{mod}\ 2)$.

Let $n-4=2k_1$, $u=2\Sigma_{i=1}^{k_1}(x_i)^{q+1}$. Since $q\geqslant 9$, there is $b\in\mathbf{F}_q\backslash\mathbf{F}_3$ such that $2b+u\neq 0$ and $2k_1+2b\neq 0$. According to Lemma 2.1. one can choose $\gamma,\delta,\epsilon\in\mathbf{F}_{q^2}$ such that $\delta^{q+1}=b$, $\gamma^{q+1}=-(2k_1+2\delta^{q+1})$, $\epsilon^{q+1}=-(u+2\delta^{q+1})$. Construct

$$A_{2,n}=\begin{pmatrix}\gamma&|&\mathbf{1_{2k_1}}&|&\delta&\delta&0\\0&|&X_{2k_1}&|&\delta&-\delta&\epsilon\end{pmatrix}=\begin{pmatrix}M_n\\N_n\end{pmatrix}.$$

Lemma 3.1. Let $4\leqslant n\leqslant q^2-4$ and $n\equiv 0\,(\mathrm{mod}\ 2)$ and $A_{2,n}$ be as previously mentioned. Then the code $\mathcal{C}_{2,n}$ generated by $A_{2,n}$ is an $[n,2]_{q^2}$ Hermitian self-orthogonal code with dual distance 3.

Proof. Since $(M_n,M_n)=\gamma^{q+1}+2k_1+2\delta^{q+1}=-(n-4+2\delta^{q+1})+2k_1+2\delta^{q+1}=0$, $(M_n,N_n)=\gamma\times 0+\Sigma_{i=1}^{k_1}[(x_i)^q+(-x_i)^q]+[\delta^{q+1}-\delta^{q+1}]+0\times\epsilon^q=0$, and $(N_n,N_n)=0+2\Sigma_{i=1}^{k_1}(x_i)^{q+1}+2\delta^{q+1}+\epsilon^{q+1}=0$. Hence $\mathcal{C}_{2,n}$ is an $[n,2]_{q^2}$ Hermitian self-orthogonal code. It is obviously that any two columns of $A_{2,n}$ are not parallel, thus they are linear independent. Therefore the dual distance of $\mathcal{C}_{2,n}$ is 3, and the lemma follows.

Case 3.2. $4\leqslant n\leqslant q^2-4$ and $n\equiv 1(\mathrm{mod}\ 2)$.

Let $n-5=2k_1$, $u=2\Sigma_{i=1}^{k_1}(x_i)^{q+1}$. Similar to the discussion of Case 3.1, one can choose $\gamma,\delta,\epsilon\in\mathbf{F}_{q^2}$, such that $\delta^{q+1}\in\mathbf{F}_q\backslash\mathbf{F}_3$ and $u+\delta^{q+1}[(\alpha^{\frac{q-1}{2}}+1)^{q+1}-2]\neq 0$, $\gamma^{q+1}=-(2k_1+\delta^{q+1})$, $\epsilon^{q+1}=-(u+\delta^{q+1}[(\alpha^{\frac{q-1}{2}}+1)^{q+1}-2])$. Construct

$$A_{2,n}=\begin{pmatrix}\gamma&|&\mathbf{1_{2k_1}}&|&\delta(\alpha^{\frac{q-1}{2}}&1&1)&|&0\\0&|&X_{2k_1}&|&\delta(\alpha^{\frac{q-1}{2}}&-\alpha^{\frac{q-1}{2}}&\alpha^{\frac{q-1}{2}}+1)&|&\epsilon\end{pmatrix}.$$

Let $\mathcal{C}_{2,n}$ be the code generated by $A_{2,n}$, and M_n and N_n be the first and second row of $A_{2,n}$, respectively. As in the proof of Lemma 3.1, one can check that $(M_n,M_n)=(M_n,N_n)=(N_n,N_n)=0$; this proves that $\mathcal{C}_{2,n}$ is an Hermitian self-orthogonal code. Therefore, we have proved that $\mathcal{C}_{2,n}$ is an Hermitian self-orthogonal code with dual distance 3.

Case 3.3. $q^2-2\leqslant n\leqslant q^2-1$.

If $n=q^2-1$, similar to the discussion of Case 3.1, we can choose $\gamma,\delta,\epsilon\in\mathbf{F}_{q^2}$ such that $\delta^{q+1}\in\mathbf{F}_q\backslash\mathbf{F}_3$ and $1-\delta^{q+1}-(\alpha^{\frac{q-1}{2}}+1)^{q+1}\neq 0$, $\gamma^{q+1}=5-2\delta^{q+1}$, $\epsilon^{q+1}=2[\delta^{q+1}+(\alpha^{\frac{q-1}{2}}+1)^{q+1}-1]$. Construct

$$A_{2,n}=\begin{pmatrix}\gamma&|&\mathbf{1_{2k}}&|&1&1&\delta&\delta&0\\0&|&X_{2k}&|&1&-1&\delta\alpha^{\frac{q-1}{2}}&-\delta\alpha^{\frac{q-1}{2}}&\epsilon\end{pmatrix}.$$

If $n=q^2-2$, choose $\epsilon=\alpha^{\frac{q-1}{2}}+1$, and construct

$$A_{2,n}=\begin{pmatrix}1&|&\mathbf{1_{2k}}&|&\mathbf{1_3}&|&0\\0&|&X_{2k}&|&Y_3&|&\epsilon\end{pmatrix}.$$

Let $\mathcal{C}_{2,n}$ be the code generated by $A_{2,n}$ in each of the previously mentioned two subcases. As in the proof of Lemma 3.1, one can check that $\mathcal{C}_{2,n}$ is an Hermitian self-orthogonal code with dual distance 3.

In the previously mentioned three Cases 3.1–3.3, we have proved that the code generated by $A_{2,n}$ is an $[n,2]_{q^2}$ Hermitian self-orthogonal code over $\mathbf{F}_{q^2}$, and its dual distance is 3. Hence, there are $[[n,n-4,3]]_q$ quantum MDS codes for $4\leqslant n\leqslant q^2+1$, where $q=3^r\geqslant 9$.

Summarizing the previous discussion and Lemma 2.4, Theorem 1.1 holds for $q=3^r$.

IV. $[[n,n-4,3]]_q$ FOR $q=p^r$ AND PRIME $p\geqslant 5$

In this section, we will prove Theorem 1.1 holds for $q=p^r$, and we always assume that $p\geqslant 5$ is an odd prime and α is a primitive element of $\mathbf{F}_{q^2}$. To give the construction of quantum $[[n,n-4,3]]_q$ codes, we consider three cases separately.

Case 4.1. $4\leqslant n\leqslant q^2-4$ and $n\equiv 0\,(\mathrm{mod}\ 2)$.

Let $n-4=2k_1$ and $w=2\Sigma_{i=1}^{k_1}(x_i)^{q+1}$. Since $q\geqslant 5$, there is $b\in\mathbf{F}_q$ and $b\neq 0$, such that $2b+w\neq 0$ and $2k_1+2b\neq 0$. Choose $\gamma,\delta,\epsilon\in\mathbf{F}_{q^2}$ such that $\delta^{q+1}=b$, $\gamma^{q+1}=-(2k_1+2\delta^{q+1})$, and $\epsilon^{q+1}=-(w+2\delta^{q+1})$. Construct

$$A_{2,n}=\begin{pmatrix}\gamma&|&\mathbf{1_{2k_1}}&|&\delta&\delta&0\\0&|&X_{2k_1}&|&\delta&-\delta&\epsilon\end{pmatrix}=\begin{pmatrix}P_n\\Q_n\end{pmatrix}.$$

Lemma 4.1. Let $q=p^r$ and prime $p\geqslant 5$, $4\leqslant n\leqslant q^2-4$ and $n\equiv 0(\mathrm{mod}\ 2)$, and $A_{2,n}$ be as previously mentioned. Then the code $\mathcal{C}_{2,n}$ generated by $A_{2,n}$ is an $[n,2]_{q^2}$ Hermitian self-orthogonal code with dual distance is 3.

Proof. Since $2\delta^{q+1}+2k_1\neq 0$, $w+2\delta^{q+1}\neq 0$, $\gamma^{q+1}=-(n-4+2\delta^{q+1})$, and $\epsilon^{q+1}=-(w+2\delta^{q+1})$. We have $(P_n,P_n)=\gamma^{q+1}+2k_1+2\delta^{q+1}=-(n-4+2\delta^{q+1})+2k_1+2\delta^{q+1}=0$, $(P_n,Q_n)=\gamma\times 0+\Sigma_{i=1}^{k_1}[(x_i)^q+(-x_i)^q]+[\delta^{q+1}-\delta^{q+1}]+0\times\epsilon^q=0$, and $(Q_n,Q_n)=0+2\Sigma_{i=1}^{k_1}(x_i)^{q+1}+2\delta^{q+1}+\epsilon^{q+1}=0$. Hence $\mathcal{C}_{2,n}$ is an $[n,2]_{q^2}$ Hermitian self-orthogonal code with dual distance 3, and the lemma holds.

Case 4.2. $4\leqslant n\leqslant q^2-4$ and $n\equiv 1(\mathrm{mod}\ 2)$.

Let $n-5=2k_1$ and $w=2\Sigma_{i=1}^{k_1}(x_i)^{q+1}$. Similar to the discussion of Case 4.1, we can choose nonzero elements $\gamma,\delta,\epsilon\in\mathbf{F}_{q^2}$ such that $3\delta^{q+1}+2k_1\neq 0$ and $w+\delta^{q+1}(\alpha^{\frac{q-1}{2}}+1)^{q+1}\neq 0$, $\gamma^{q+1}=-(n-5+3\delta^{q+1})$, $\epsilon^{q+1}=-[w+\delta^{q+1}(\alpha^{\frac{q-1}{2}}+1)^{q+1}]$. Construct

$$A_{2,n}=\begin{pmatrix}\gamma&|&\mathbf{1_{2k_1}}&|&\delta\mathbf{1_3}&|&0\\0&|&X_{2k_1}&|&\delta Y_3&|&\epsilon\end{pmatrix}.$$

Similarly to the proof of Lemma 4.1, it is easy to prove that the code generated by $A_{2,n}$ is an Hermitian self-orthogonal code with dual distance 3.

Case 4.3. $q^2-2\leqslant n\leqslant q^2-1$.

If $n = q^2 - 1$, choose $\gamma,\epsilon \in \mathbf{F}_{q^2}$ such that $\gamma^{q+1} = 3$, $\epsilon^{q+1} = 2(\alpha^{\frac{q-1}{2}} + 1)^{q+1}$, and construct

$$A_{2,n} = \begin{pmatrix} \gamma & | & \mathbf{1_{2k}} & | & 1 & 1 & 1 & 1 & 0 \\ 0 & | & X_{2k} & | & 1 & -1 & \alpha^{\frac{q-1}{2}} & -\alpha^{\frac{q-1}{2}} & \epsilon \end{pmatrix}.$$

If $n = q^2 - 2$, choose $\gamma,\epsilon \in \mathbf{F}_{q^2}$ such that $\gamma^{q+1} = 4$, $\epsilon^{q+1} = (\alpha^{\frac{q-1}{2}} + 1)^{q+1}$. Construct

$$A_{2,n} = \begin{pmatrix} \gamma & | & \mathbf{1_{2k}} & | & \mathbf{1_3} & | & 0 \\ 0 & | & X_{2k} & | & Y_3 & | & \epsilon \end{pmatrix}.$$

Let $\mathcal{C}_{2,n}$ be the code generated by $A_{2,n}$ in each of the previously mentioned two subcases. As in the proof of Lemma 4.1, using Lemma 2.3 one can check that $\mathcal{C}_{2,n}$ is an Hermitian self-orthogonal code with dual distance 3.

In the previously mentioned three Cases 4.1–4.3, we have proved that the code generated by $A_{2,n}$ is an $[n,2]_{q^2}$ Hermitian self-orthogonal code with dual distance 3. Hence, there are $[[n,n-4,3]]_q$ quantum MDS codes for $4 \leqslant n \leqslant q^2 - 1$, where $q = p^r$ and $p \geqslant 5$.

Summarizing the previous discussion and Lemma 2.4, Theorem 1.1 holds for $q = p^r$ and odd prime $p \geqslant 5$.

V. CONCLUDING REMARKS

For each odd prime power q, we have constructed an $[[n,n-4,3]]_q$ quantum MDS code for $4 \leqslant n \leqslant q^2 + 1$. In June 2010 (after we submitted this paper), we knew that [23] gave the construction of $[[n,n-4,3]]_q$ quantum MDS codes for $q = 2^r \geqslant 4$ and $4 \leqslant n \leqslant q^2 + 1$ by using our method given in [21] and other technical. For $d \geqslant 4$, using generalized Reed-Solomon codes and algebraic geometry, Ref. [23] also discussed constructing quantum MDS codes with distance d from Hermitian self-orthogonal codes.

For given $q \geqslant 3$ and $d \geqslant 4$, how one can use our method given in this paper to construct q-nary quantum MDS codes with distance d needs further study.

ACKNOWLEDGMENTS

The authors are very grateful to the anonymous referees for their valuable comments and suggestions, which helped to improve the manuscript significantly. This work is supported by National Natural Science Foundation of China under Grant No. 11071255, National Basic Research Program of China (973 Program) under Grant No. 2007CB311002, and Natural Science Basic Research Plan in Shaanxi Province of China under Program No. SJ08A02.

[1] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[2] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[3] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, IEEE Trans. Inf. Theory **44**, 1369 (1998).
[4] D. Gottesman, Ph.D. thesis, California Institute of Technology, 1997.
[5] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[6] E. M. Rains, IEEE Trans. Inf. Theory **45**, 1827 (1999).
[7] A. Ashikhim and E. Knill, IEEE Trans. Inf. Theory **47**, 3065 (2001).
[8] A. Ketkar, A. Klappenecker, and S. Kumar, IEEE Trans. Inf. Theory **52**, 4892 (2006).
[9] A. M. Steane, IEEE Trans. Inf. Theory **45**, 1701 (1999).
[10] A. M. Steane, IEEE Trans. Inf. Theory **45**, 2492 (1999).
[11] A. Thangaraj and S. W. McLaughlin, IEEE Trans. Inf. Theory **47**, 1176 (2001).
[12] J. Bierbrauer and Y. Edel, J. Comb. Designs **8**, 174 (2000).
[13] X. Lin, IEEE Trans. Inf. Theory **50**, 547 (2004).
[14] R. Li and X. Li, IEEE Trans. Inf. Theory **50**, 1331 (2004).
[15] K. Feng, IEEE Trans. Inf. Theory **48**, 2384 (2002).
[16] M. Grassl, T. Beth, and M. Rotteler, Int. J. Quantum. Inf. **2**, 55 (2004).
[17] D. Hu, W. Tang, M. Zhao, Q. Chen, S. Yu, and C. H. Oh, Phys. Rev. A **78**, 012306 (2008).
[18] Z. Li, L. Xing, and X. M. Wang, Phys. Rev. A **77**, 012308 (2008).
[19] G. G. La Guardia, Phys. Rev. A **80**, 042331 (2009).
[20] R. Li, X. Li, and Z. Xu, Int. J. Quantum. Inf. **4**, 265 (2006).
[21] R. Li and Z. Xu, e-print arXiv:0906.2509vl [cs.IT].
[22] J. Liu, Int. J. Quantum. Inf. (in press).
[23] L. Jin, S. Ling, J. Luo, and C. Xing, *Application of Hermitian Self-Orthogonal MDS Codes to Quantum MDS Codes* (preprint, June 2010).
[24] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes* (North-Holland, Amsterdam, 1977).