Quantum Codes Derived From Certain Classes of Polynomials

Tao Zhang and Gennian Ge

Abstract— **One central theme in quantum error-correction is to construct quantum codes that have a relatively large minimum distance. In this paper, we first present a construction of classical linear codes based on certain classes of polynomials. Through these classical linear codes, we are able to obtain some new quantum codes. It turns out that some of the quantum codes exhibited here have better parameters than the ones available in the literature.**

Index Terms— **Quantum code, polynomial code, cyclotomic coset.**

I. Introduction

QUANTUM codes were introduced to protect quantum information from decoherence during quantum computations and quantum communications. After the initial work for quantum error-correcting codes [20], [21], researchers have made great progress in developing quantum codes. In [3], the construction of binary quantum codes was diverted into finding classical self-orthogonal codes over GF(4), and then generalized to the nonbinary case [2], [19]. After the establishment of the connection above between quantum codes and classical codes, the construction of quantum codes can be converted to that of classical self-orthogonal codes (see [1], [4], [5], [9], [13]–[17], [22], [25], [26], and the references therein). As in classical coding theory, there is a trade-off between parameters so that one important goal is to achieve a better value in one parameter for given values of the other parameters.

A powerful construction of quantum codes is through classical codes with certain self-orthogonality. Among these self-orthogonalities, the Hermitian self-orthogonal classical codes may give rise to good quantum stabilizer codes, since Hermitian orthogonality produces q-ary quantum codes from q^2-ary classical error-correcting codes.

Manuscript received January 3, 2015; revised December 19, 2015; accepted August 16, 2016. Date of publication September 21, 2016; date of current version October 18, 2016. G. Ge was supported by the National Natural Science Foundation of China under Grant 11431003 and Grant 61571310.

T. Zhang is with the School of Mathematical Sciences, Capital Normal University, Beijing 100048, China. He is also 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. He is 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.2016.2612578

A good family of Hermitian self-orthogonal classical codes is based on Reed-Solomon codes. We know that Reed-Solomon codes are MDS (maximum distance separable) codes [11], as their parameters meet the Singleton bound. But the length of a q-ary Reed-Solomon code is restricted to be less than or equal to q. By using the method of evaluation, several classes of good q-ary linear codes which have lengths larger than q have been successfully constructed (see [7], [12], [18], [23], [24]). However, these codes are usually not Hermitian self-orthogonal.

In this paper, we first give a new construction of linear codes by evaluation and then we determine their dual codes. In this way, we can get Hermitian self-orthogonal codes and obtain new quantum codes. Some of them have better parameters than the quantum codes listed in tables online [6], [10].

This paper is organized as follows. In Section II we recall the basics about classical linear codes and quantum codes. In Section III, we first give a new construction of classical linear codes. From these linear codes, we obtain some new quantum codes. Section IV concludes the paper.

II. Preliminaries

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a prime power. For $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, the Hamming distance $d(\mathbf{x}, \mathbf{y})$ is the number of positions where $\mathbf{x}$ and $\mathbf{y}$ differ. An $[n, k, d]_q$ code C is a linear code of length n, dimension k, and minimum distance $d = \min_{\mathbf{x} \neq \mathbf{y} \in C} d(\mathbf{x}, \mathbf{y})$, whose alphabet set is $\mathbb{F}_q$.

Given two vectors $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1}), \mathbf{y} = (y_0, y_1, \cdots, y_{n-1}) \in \mathbb{F}_q^n$, there are two inner products we are interested in. One is the Euclidean inner product which is defined by

$$\langle \mathbf{x}, \mathbf{y} \rangle_E = x_0 y_0 + x_1 y_1 + \cdots + x_{n-1} y_{n-1}.$$

When $q = l^2$, where l is a prime power, then we can also consider the Hermitian inner product which is defined by

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

The Euclidean dual code of C is defined by

$$C^{\perp E} = \{\mathbf{x} \in \mathbb{F}_q^n \mid \langle \mathbf{x}, \mathbf{y} \rangle_E = 0 \text{ for all } \mathbf{y} \in C\}.$$

Similarly the Hermitian dual code of C is defined by

$$C^{\perp H} = \{\mathbf{x} \in \mathbb{F}_q^n \mid \langle \mathbf{x}, \mathbf{y} \rangle_H = 0 \text{ for all } \mathbf{y} \in C\}.$$

A linear code C is called Euclidean (Hermitian) dual-containing if $C^{\perp E} \subseteq C$ ($C^{\perp H} \subseteq C$, respectively).

Now we recall the basics of quantum codes. Let q be a power of a prime number p. A qudit is a quantum state in a q-level quantum system. If a given qudit represents a pure state, it may be expressed by a unit vector: $|v\rangle = \sum_{x\in\mathbb{F}_q} c_x|x\rangle$ in a q-dimensional complex Hilbert space $\mathbb{C}^q$, where $\{|x\rangle \mid x \in \mathbb{F}_q\}$ is a basis of $\mathbb{C}^q$, $c_x \in \mathbb{C}$ and $\sum_{x\in\mathbb{F}_q} |c_x|^2 = 1$. For $n \geq 1$, an n-qudit is a joint state of n qudits in the q^n-dimensional space $(\mathbb{C}^q)^{\otimes n}$. A pure n-qudit state can be represented by $|\mathbf{v}\rangle = \sum_{\mathbf{a}\in\mathbb{F}_q^n} c_{\mathbf{a}}|\mathbf{a}\rangle$, where $c_{\mathbf{a}} \in \mathbb{C}$, $\sum_{\mathbf{a}\in\mathbb{F}_q^n} |c_{\mathbf{a}}|^2 = 1$, and $\{|\mathbf{a}\rangle = |a_1\cdots a_n\rangle = |a_1\rangle \bigotimes \cdots \bigotimes |a_n\rangle \mid (a_1,\cdots,a_n) \in \mathbb{F}_q^n\}$ is a basis of $(\mathbb{C}^q)^{\otimes n}$. For $|\mathbf{v}\rangle = \sum_{\mathbf{a}\in\mathbb{F}_q^n} c_{\mathbf{a}}|\mathbf{a}\rangle$ and $|\mathbf{u}\rangle = \sum_{\mathbf{a}\in\mathbb{F}_q^n} d_{\mathbf{a}}|\mathbf{a}\rangle$ $(c_{\mathbf{a}}, d_{\mathbf{a}} \in \mathbb{C})$, the Hermitian inner product of $|\mathbf{v}\rangle$ and $|\mathbf{u}\rangle$ is defined by

$$\langle \mathbf{u}|\mathbf{v}\rangle = \sum_{\mathbf{a}\in\mathbb{F}_q^n} c_{\mathbf{a}}\overline{d_{\mathbf{a}}} \in \mathbb{C}.$$

Let ζ_p be a complex primitive p-th root of unity. The quantum errors in a q-ary quantum system are linear operators acting on $\mathbb{C}^q$ and can be represented by the set of error operators: $\varepsilon_n = \{T(a)R(b) \mid a, b \in \mathbb{F}_q\}$, where $T(a)R(b)$ is defined by

$$T(a)R(b)|x\rangle = \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(bx)}|x+a\rangle.$$

Let $\mathbf{a} = (a_1,\cdots,a_n) \in \mathbb{F}_q^n$, denote $T(\mathbf{a}) = T(a_1)\otimes\cdots\otimes T(a_n)$ and $R(\mathbf{a}) = R(a_1)\otimes\cdots\otimes R(a_n)$ for the tensor products of n error operators. Then the set

$$E_n = \{\zeta_p^l T(\mathbf{a})R(\mathbf{b}) \mid 0 \leq l \leq p-1, \mathbf{a} = (a_1,\cdots,a_n), \mathbf{b} = (b_1,\cdots,b_n) \in \mathbb{F}_q^n\}$$

forms an error group, where $\zeta_p^l T(\mathbf{a})R(\mathbf{b})$ is defined by

$$\begin{aligned}\zeta_p^l T(\mathbf{a})R(\mathbf{b})|\mathbf{x}\rangle &= \zeta_p^l T(a_1)R(b_1)|x_1\rangle \otimes\cdots\otimes T(a_n)R(b_n)|x_n\rangle \\ &= \zeta_p^{l+\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathbf{b}\cdot\mathbf{x})}|\mathbf{x}+\mathbf{a}\rangle,\end{aligned}$$

for any $|\mathbf{x}\rangle = |x_1\rangle\otimes\cdots\otimes|x_n\rangle$, $\mathbf{x} = (x_1,\cdots,x_n) \in \mathbb{F}_q^n$. For an error $\mathbf{e} = \zeta_p^l T(\mathbf{a})R(\mathbf{b})$, its quantum weight is defined by

$$w_Q(\mathbf{e}) = \sharp\{1 \leq i \leq n \mid (a_i, b_i) \neq (0,0)\}.$$

A K-dimensional subspace Q of $\mathbb{C}^{q^n}$ is called a q-ary quantum code with length n. Let $E_n(i) = \{\mathbf{e} \in E_n \mid w_Q(\mathbf{e}) \leq i\}$, then the q-ary quantum code Q has minimum distance d if d is the largest positive integer such that $\langle \mathbf{u}|\mathbf{e}|\mathbf{v}\rangle = 0$ when $|\mathbf{u}\rangle, |\mathbf{v}\rangle \in Q$, $\langle \mathbf{u}|\mathbf{v}\rangle = 0$ and $\mathbf{e} \in E_n(d-1)$. In this case, we call Q a quantum code with parameters $((n, K, d))_q$ or $[[n, k, d]]_q$, where $k = \log_q(K)$. A quantum $((n, K, d))_q$ code Q is called pure if $\langle \mathbf{u}|\mathbf{e}|\mathbf{v}\rangle = 0$ for all $|\mathbf{u}\rangle, |\mathbf{v}\rangle \in Q$ and $\mathbf{e} \in E_n$ with $1 \leq w_Q(\mathbf{e}) \leq d-1$.

There are many methods to construct quantum codes, and the following theorem is one of the most frequently used construction methods.

Theorem 1 ([2] Hermitian Construction): If C is a Hermitian dual-containing $[n, k, d]_{q^2}$ code, then there exists an $[[n, 2k-n, \geq d]]_q$-quantum code.

We also mention that quantum codes have propagation rules as classical linear codes.

Theorem 2 ([8] Propagation Rules): Suppose there is an $[[n, k, d]]_q$ quantum code. Then

1) (Subcode) there exists an $[[n, k-1, \geq d]]_q$ quantum code;
2) (Lengthening) there exists an $[[n+1, k, \geq d]]_q$ quantum code;
3) (Puncturing) there exists an $[[n-1, k, \geq d-1]]_q$ quantum code;
4) there exists an $[[n, k, d-1]]_q$ quantum code.

III. New Quantum Codes From Polynomial Codes

This section gives a new construction of classical linear codes and provides a family of quantum codes. The following notations are fixed in this section.

- Let $q = p^{\alpha_1}$, where p is a prime number and α_1 is a positive integer.
- Let m be a positive integer with $\gcd(q, m) = 1$ and $\mathrm{ord}_m(q) = p^{\alpha_2}$, that is, p^{α_2} is the smallest positive integer l such that $m|(q^l - 1)$.
- Let $t = p^{\alpha_2}$ and $s = p^{\alpha_2 - 1}$.

A. Polynomial Codes

Note that $\mathrm{ord}_m(q) = t$. For any $a \in \mathbb{Z}_m = \{0, 1, \cdots, m-1\}$, the q-cyclotomic coset C_a belonging to a is defined by

$$C_a := \{aq^j \pmod m \mid 0 \leq j \leq t-1\}.$$

Now we choose a representation of the q-cyclotomic coset with maximum length:

$$A := \{\max(C_a) \mid 0 \leq a \leq m-1, |C_a| = t\},$$

where $\max(C_a)$ is the maximum element of the set C_a. We are ready to define the following polynomials.

Definition 1: For every $a \in A$ and every integer k such that $0 \leq k \leq s-1$, let

$$e_{a,k}(x) = \sum_{j=0}^{t-1} \gamma^{q^{j+k}} x^{q^j a},$$

where γ is a fixed normal element of $\mathbb{F}_{q^s}/\mathbb{F}_q$, i.e., the set $\{\gamma, \gamma^q, \cdots, \gamma^{q^{s-1}}\}$ forms an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^s}$.

Let U_m be the subgroup of the m-th roots of unity in $\mathbb{F}_{q^t}^*$. In the following, we assume that the polynomials above are always defined over U_m. Let $P := \{e_{a,k}(x) \mid a \in A, 0 \leq k \leq s-1\}$. Then we have the following result.

Lemma 1: The polynomials $e_{a,k}(x)$ have the following properties:

(i) *For $a \in A$ and $0 \leq k \leq s-1$, the polynomial $e_{a,k}(x)$ has coefficients in $\mathbb{F}_{q^s}$ and degree equal to a.*
(ii) *The polynomials $e_{a,k}(x)$ for $a \in A$ and $0 \leq k \leq s-1$ are linearly independent over $\mathbb{F}_q$.*
(iii) *$e_{a,k}(\beta) \in \mathbb{F}_q$ for all $\beta \in U_m$.*
(iv) *$e_{a,k}(u) = 0$ for all $u \in (\mathbb{F}_{q^s} \bigcap U_m) \bigcup \{0\}$.*
(v) *$|P| = \frac{m-\gcd(m, q^s-1)}{p}$.*

Proof: (i). All the assertions are clear.

(ii). Suppose $\sum_{a\in A}\sum_{k=0}^{s-1} c_{a,k}e_{a,k}(x)=0$, where $c_{a,k}\in\mathbb{F}_q$. Then the coefficient of x^a is $\sum_{k=0}^{s-1} c_{a,k}\gamma^{q^k}=0$, therefore $c_{a,k}=0$ $(0\le k\le s-1)$, since the set $\{\gamma,\gamma^q,\cdots,\gamma^{q^{s-1}}\}$ forms an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^s}$. Hence the polynomials $e_{a,k}(x)$ for $a\in A$ and $0\le k\le s-1$ are linearly independent over $\mathbb{F}_q$.

(iii). Let $\beta\in U_m$, then

$$\begin{aligned}(e_{a,k}(\beta))^q &= (\sum_{j=0}^{t-1}\gamma^{q^{j+k}}\beta^{q^j a})^q\\ &=\sum_{j=0}^{t-1}\gamma^{q^{j+k+1}}\beta^{q^{j+1}a}\\ &=\sum_{j=1}^{t-1}\gamma^{q^{j+k}}\beta^{q^j a}+\gamma^{q^{t+k}}\beta^{q^t a}\\ &=\sum_{j=0}^{t-1}\gamma^{q^{j+k}}\beta^{q^j a},\end{aligned}$$

so $e_{a,k}(\beta)\in\mathbb{F}_q$.

(iv). It is clear that $e_{a,k}(0)=0$. Let $u\in\mathbb{F}_{q^s}\bigcap U_m$, then

$$\begin{aligned}e_{a,k}(u) &= \sum_{j=0}^{t-1}\gamma^{q^{j+k}}u^{q^j a}\\ &=\frac{t}{s}\sum_{j=0}^{s-1}\gamma^{q^{j+k}}u^{q^j a}\\ &=p\sum_{j=0}^{s-1}\gamma^{q^{j+k}}u^{q^j a}\\ &=0.\end{aligned}$$

(v). We can verify that $|C_a|<t$ if and only if $m|a(q^s-1)$, that is, $\frac{m}{\gcd(m,q^s-1)}|a$. Since every q-cyclotomic coset with t elements corresponds to s polynomials, we have $|P|=\frac{m-\gcd(m,q^s-1)}{p}$. ∎

In order to give our construction, let

- $L\subseteq A$, $S:=\bigcup_{a\in L}C_a$, $\mathfrak{A}:=\bigcup_{a\in A}C_a$,
- $P(S):=\{e_{a,k}(x)\mid a\in(S\bigcap A),0\le k\le s-1\}$,
- $V(S):=\mathrm{span}_{\mathbb{F}_q}(P(S))$,
- $\{\beta_1,\beta_2,\cdots,\beta_n\}$ be a complete set of representatives of elements from $U_m\backslash(U_m\bigcap\mathbb{F}_{q^s}^*)$ which are pairwise nonconjugate over $\mathbb{F}_{q^s}$.

It is clear that $n=\frac{m-\gcd(m,q^s-1)}{p}$.

Remark 1: We give some explanations on the particular choice of polynomials and points.

1) *We want to construct polynomials which map U_m to $\mathbb{F}_q$. From the lemma above, the polynomials $e_{a,k}(x)$ $(a\in A,\ 0\le k\le s-1)$ are the polynomials satisfying this condition. These polynomials can also be found in [12] and [23].*
2) *Since $e_{a,k}(u)=0$ for all $u\in(\mathbb{F}_{q^s}\bigcap U_m)\bigcup\{0\}$, in order to construct good linear codes, we choose the points from the set $U_m\backslash(U_m\bigcap\mathbb{F}_{q^s}^*)$. By the definition of polynomials $e_{a,k}(x)$, we have $e_{a,k}(u)=e_{a,k}(u^{q^s})$ for all $u\in U_m\backslash(U_m\bigcap\mathbb{F}_{q^s}^*)$. Hence we take the points to be a complete set of representatives of elements from $U_m\backslash(U_m\bigcap\mathbb{F}_{q^s}^*)$ which are pairwise nonconjugate over $\mathbb{F}_{q^s}$.*
3) *Note that we have constructed $\frac{m-\gcd(m,q^s-1)}{p}$ polynomials and $\frac{m-\gcd(m,q^s-1)}{p}$ points.*

Our construction is:

Proposition 1: Let

$$C(S):=\{(f(\beta_1),f(\beta_2),\cdots,f(\beta_n))\mid f\in V(S)\}.$$

Then $C(S)$ is an $[n,k,d]_q$ code, with $n=\frac{m-\gcd(m,q^s-1)}{p}$, $k=|P(S)|$, $d\ge\lceil\frac{m+1-c}{p}\rceil$, where c is the maximum element of the set S.

Proof: We only need to show that $d\ge\lceil\frac{m+1-c}{p}\rceil$. On one hand, by Lemma 1, $f(u)=0$ for all $u\in(\mathbb{F}_{q^s}\bigcap U_m)\bigcup\{0\}$. On the other hand, if β_i is a root of $f(x)$, then so are all the p conjugate elements $\beta_i,\cdots,\beta_i^{q^{s(p-1)}}$. Therefore $f(x)$ has at most $\frac{\deg(f(x))-\gcd(m,q^s-1)-1}{p}$ roots among $\{\beta_1,\beta_2,\cdots,\beta_n\}$. Hence its Hamming weight is at least $n-\frac{c-\gcd(m,q^s-1)-1}{p}=\frac{m+1-c}{p}$. ∎

Remark 2: The construction above of linear codes is a generalization of Construction IV in [23].

B. New Quantum Codes

In this section, we will construct some new quantum codes from polynomial codes. First of all, we determine the dual of the code $C(S)$. Let $\overline{C_a}=\{m-i\mid i\in C_a\}$ and $\overline{S}=\bigcup_{a\in S}\overline{C_a}$, then we have

Proposition 2: The Euclidean dual of $C(S)$ is $C(R)$, where $R=\mathfrak{A}\backslash\overline{S}$.

Proof: Since $\dim(C(S))+\dim(C(R))=n$, we only need to show that every codeword in $C(S)$ is orthogonal to all codewords of $C(R)$.

For $a\in S$, $b\in R$ and $0\le k_1,k_2\le s-1$, we have

$$\begin{aligned}&\sum_{i=1}^{n}e_{a,k_1}(\beta_i)e_{b,k_2}(\beta_i)\\ &=\sum_{i=1}^{n}(\sum_{j=0}^{t-1}\gamma^{q^{j+k_1}}\beta_i^{q^j a})(\sum_{l=0}^{t-1}\gamma^{q^{l+k_2}}\beta_i^{q^l b})\\ &=\sum_{i=1}^{n}\sum_{j=0}^{t-1}\sum_{l=0}^{t-1}\gamma^{q^{j+k_1}+q^{l+k_2}}\beta_i^{q^j a+q^l b}\\ &=\sum_{j=0}^{t-1}(\sum_{l=0}^{t-1}(\sum_{i=1}^{n}\gamma^{q^{j+k_1}+q^{k_2}}\beta_i^{q^j a+b})^{q^l})\\ &=\sum_{j=0}^{t-1}(\sum_{l_1=0}^{s-1}\sum_{l_2=0}^{p-1}(\sum_{i=1}^{n}\gamma^{q^{j+k_1}+q^{k_2}}\beta_i^{q^j a+b})^{q^{l_1+l_2 s}})\\ &=\sum_{j=0}^{t-1}\sum_{l_1=0}^{s-1}\gamma^{q^{j+k_1+l_1}+q^{k_2+l_1}}(\sum_{l_2=0}^{p-1}(\sum_{i=1}^{n}\beta_i^{q^j a+b})^{q^{l_1+l_2 s}}).\end{aligned}$$

TABLE I
NEW QUANTUM CODES

q	m	$\max(S)$	quantum codes	q	m	$\max(S)$	quantum codes
4	15	9	$[[6,0,\geq 4]]_2$	4	15	13	$[[6,4,\geq 2]]_2$
4	255	226	$[[120,40,\geq 15]]_2$	4	255	229	$[[120,48,\geq 14]]_2$
4	255	230	$[[120,52,\geq 13]]_2$	4	255	233	$[[120,60,\geq 12]]_2$
4	255	234	$[[120,64,\geq 11]]_2$	4	255	237	$[[120,72,\geq 10]]_2$
4	255	241	$[[120,80,\geq 8]]_2$	4	255	242	$[[120,84,\geq 7]]_2$
4	255	245	$[[120,92,\geq 6]]_2$	4	255	246	$[[120,96,\geq 5]]_2$
4	255	249	$[[120,104,\geq 4]]_2$	4	255	250	$[[120,108,\geq 3]]_2$
4	255	253	$[[120,116,\geq 2]]_2$	9	104	90	$[[32,12,\geq 5]]_3$
9	104	94	$[[32,16,\geq 4]]_3$	9	104	98	$[[32,22,\geq 3]]_3$
9	104	101	$[[32,28,\geq 2]]_3$	9	728	704	$[[240,198,\geq 9]]_3$
9	728	707	$[[240,204,\geq 8]]_3$	9	728	709	$[[240,208,\geq 7]]_3$
9	728	713	$[[240,214,\geq 6]]_3$	9	728	716	$[[240,220,\geq 5]]_3$
9	728	718	$[[240,224,\geq 4]]_3$	9	728	722	$[[240,230,\geq 3]]_3$
9	728	725	$[[240,236,\geq 2]]_3$	16	85	67	$[[40,12,\geq 10]]_4$
16	85	71	$[[40,16,\geq 8]]_4$	16	85	73	$[[40,20,\geq 7]]_4$
16	85	75	$[[40,22,\geq 6]]_4$	16	85	77	$[[40,26,\geq 5]]_4$
16	85	79	$[[40,30,\geq 4]]_4$	16	85	81	$[[40,34,\geq 3]]_4$
16	85	83	$[[40,38,\geq 2]]_4$	16	255	203	$[[120,36,\geq 27]]_4$
16	255	209	$[[120,40,\geq 24]]_4$	16	255	211	$[[120,44,\geq 23]]_4$
16	255	213	$[[120,48,\geq 22]]_4$	16	255	215	$[[120,52,\geq 21]]_4$
16	255	217	$[[120,56,\geq 20]]_4$	16	255	219	$[[120,60,\geq 19]]_4$
16	255	220	$[[120,62,\geq 18]]_4$	16	255	225	$[[120,66,\geq 16]]_4$
16	255	227	$[[120,70,\geq 15]]_4$	16	255	229	$[[120,74,\geq 14]]_4$
16	255	231	$[[120,78,\geq 13]]_4$	16	255	233	$[[120,82,\geq 12]]_4$
16	255	235	$[[120,86,\geq 11]]_4$	16	255	237	$[[120,90,\geq 10]]_4$
16	255	241	$[[120,94,\geq 8]]_4$	16	255	243	$[[120,98,\geq 7]]_4$
16	255	245	$[[120,102,\geq 6]]_4$	16	255	247	$[[120,106,\geq 5]]_4$
16	255	249	$[[120,110,\geq 4]]_4$	16	255	251	$[[120,114,\geq 3]]_4$
16	255	253	$[[120,118,\geq 2]]_4$				

Note that

$$\sum_{l_2=0}^{p-1}\Big(\sum_{i=1}^{n}\beta_i^{q^j a+b}\Big)^{q^{l_1+l_2 s}} = \sum_{\beta\in U_m}\beta^{q^j a+b} - \sum_{\beta\in \mathbb{F}_{q^s}\bigcap U_m}\beta^{q^j a+b} = \begin{cases} 0; & \text{if } \gcd(m,q^s-1)\nmid q^j a+b,\\ -\gcd(m,q^s-1); & \text{if } \gcd(m,q^s-1)\mid q^j a+b,\end{cases}$$

we have

$$\begin{aligned}&\sum_{i=1}^{n} e_{a,k_1}(\beta_i)e_{b,k_2}(\beta_i)\\ &= -\gcd(m,q^s-1)\sum_{\substack{j=0\\ \gcd(m,q^s-1)\mid q^j a+b}}^{t-1}\ \sum_{l_1=0}^{s-1}\gamma^{\,q^{j+k_1+l_1}+q^{k_2+l_1}}\\ &= -\gcd(m,q^s-1)\,p\sum_{\substack{j=0\\ \gcd(m,q^s-1)\mid q^j a+b}}^{s-1}\ \sum_{l_1=0}^{s-1}\gamma^{\,q^{j+k_1+l_1}+q^{k_2+l_1}}\\ &= 0.\end{aligned}$$

■

In order to apply our result to quantum codes, we need to discuss the Hermitian dual of $C(S)$ as well.

Proposition 3: Let $q=l^2$, then the Hermitian dual of $C(S)$ is $C(R)$, where $R=\mathfrak{A}\backslash\overline{lS}$, $lS=\{ls \mid s\in S\}$.

Proof: It is clear that the Hermitian dual of $C(S)$ is the Euclidean dual of $C(lS)$. Then the desired result follows from Proposition 2. ■

Now we state our main result.

Theorem 3: Let $q=p^{2e}$ be a prime power, where p is a prime number and e is a positive integer. If there exist both an integer m and a finite set S satisfying the following conditions:

1) *$\gcd(q,m)=1$ and $\mathrm{ord}_m(q)=p^b$, where $b\geq 1$ is a positive integer;*
2) *$L\subseteq A$, $S=\bigcup_{a\in L}C_a$, $\mathfrak{A}=\bigcup_{a\in A}C_a$, $S\bigcup\overline{p^eS}\supseteq\mathfrak{A}$, where C_a is a q-cyclotomic coset modulo m and $A=\{\max(C_a)\mid 0\leq a\leq m-1, |C_a|=p^b\}$,*

then there exists an $[[n,k,d]]_{p^e}$ quantum code, with $n=\frac{m-\gcd(m,q^{p^{b-1}}-1)}{p}$, $k=\frac{2|S|-m+\gcd(m,q^{p^{b-1}}-1)}{p}$ and $d\geq\lceil\frac{m+1-c}{p}\rceil$, where c is the maximum element of the set S.

Proof: By Proposition 3, we have $C(\mathfrak{A}\backslash\overline{p^eS})=C(S)^{\perp H}$. If $S\bigcup\overline{p^eS}\supseteq\mathfrak{A}$, then $C(S)^{\perp H}\subseteq C(S)$. Applying Theorem 1 and Proposition 1, the result follows. ■

Table I lists some quantum codes obtained from Theorem 3, where $\max(S)$ is the maximum element of the set S. In order to do comparisons in Table II, we use the propagation rule (Theorem 2) to obtain some of the codes with lengths that are listed in the table online [6]. Tables II and III show that our quantum codes have larger minimum distance (larger dimension) than the previous quantum codes available when they have the same length and dimension (minimum distance, respectively).

Remark 3: For fixed p and e, there are infinitely many choices of m in Theorem 3 (for example, take $m=q^{p^b}-1$ for some integer b). But, in general, we can not decide whether there exists nontrivial S ($S\neq\mathfrak{A}$) such that $S\bigcup\overline{p^eS}\supseteq\mathfrak{A}$. Table I suggests that there are many choices of S for each m

TABLE II
QUANTUM CODES COMPARISON

quantum codes from Table I	using propagation rule	quantum codes from [6]
$[[240, 220, \geq 5]]_3$	$[[238, 220, \geq 3]]_3$	$[[238, 216, 3]]_3$
$[[40, 16, \geq 8]]_4$		$[[40, 2, 8]]_4$
$[[40, 20, \geq 7]]_4$		$[[40, 8, 7]]_4$
$[[40, 22, \geq 6]]_4$		$[[40, 14, 6]]_4$
$[[40, 26, \geq 5]]_4$		$[[40, 20, 5]]_4$
$[[40, 30, \geq 4]]_4$		$[[40, 26, 4]]_4$
$[[40, 34, \geq 3]]_4$		$[[40, 32, 3]]_4$
$[[120, 52, \geq 21]]_4$	$[[117, 52, \geq 18]]_4$	$[[117, 49, 14]]_4$
$[[120, 56, \geq 20]]_4$	$[[117, 56, \geq 17]]_4$	$[[117, 49, 14]]_4$
$[[120, 60, \geq 19]]_4$	$[[117, 60, \geq 16]]_4$	$[[117, 49, 14]]_4$
$[[120, 62, \geq 18]]_4$	$[[117, 62, \geq 15]]_4$	$[[117, 49, 14]]_4$

TABLE III
QUANTUM CODES COMPARISON

quantum codes from Table I	quantum codes from [10]
$[[120, 40, \geq 15]]_2$	$[[120, 40, 14]]_2$
$[[120, 48, \geq 14]]_2$	$[[120, 48, 13]]_2$
$[[120, 52, \geq 13]]_2$	$[[120, 52, 12]]_2$
$[[120, 60, \geq 12]]_2$	$[[120, 60, 11]]_2$
$[[120, 64, \geq 11]]_2$	$[[120, 64, 10]]_2$
$[[120, 72, \geq 10]]_2$	$[[120, 72, 9]]_2$

and the corresponding quantum codes are better than previous results.

Now we give an example to illustrate our construction.

Example 1: Take $q = 4$, $m = 15$. *Then* $\mathrm{ord}_{15}(4) = 2$, *hence* $t = 2$ *and* $s = 1$. *All* 4*-cyclotomic cosets modulo* 15 *are*

$$C_0 = \{0\}, \quad C_1 = \{1, 4\}, \quad C_2 = \{2, 8\}, \quad C_3 = \{3, 12\},$$
$$C_5 = \{5\}, \quad C_6 = \{6, 9\}, \quad C_7 = \{7, 13\}, \quad C_{10} = \{10\},$$
$$C_{11} = \{11, 14\}.$$

Then $A = \{4, 8, 9, 12, 13, 14\}$, *and we have the following six polynomials:*

$$e_4(x) = x^4 + x,$$
$$e_8(x) = x^8 + x^2,$$
$$e_9(x) = x^9 + x^6,$$
$$e_{12}(x) = x^{12} + x^3,$$
$$e_{13}(x) = x^{13} + x^7,$$
$$e_{14}(x) = x^{14} + x^{11}.$$

Let γ *be a fixed primitive element of* $\mathbb{F}_{16}$. *We may take* $\{\gamma, \gamma^2, \gamma^3, \gamma^6, \gamma^7, \gamma^{11}\}$ *as a set of representatives of elements from* $U_{15}\backslash\mathbb{F}_4^*$ *which are pairwise nonconjugate over* $\mathbb{F}_4$.

If we take $S = C_1 \bigcup C_2 \bigcup C_6$, *then* $\overline{2S} = C_7 \bigcup C_{11} \bigcup C_3$. *Let* $V(S)$ *be the* $\mathbb{F}_4$*-vector space generated by the polynomials* $e_4(x), e_8(x), e_9(x)$, *then the code* $\{(f(\gamma), f(\gamma^2), f(\gamma^3), f(\gamma^6), f(\gamma^7), f(\gamma^{11})) \mid f \in V(S)\}$ *is a* $[6, 3, 4]_4$ *Hermitian dual-containing code. Hence we obtain a* $[[6, 0, \geq 4]]_2$ *quantum code.*

IV. CONCLUSION

In this paper, by using polynomial codes, we constructed some quantum codes with parameters better than the ones available in the literature. A general framework of polynomial codes is:

1) let $F = \mathbb{F}_q$, $K = \mathbb{F}_{q^s}$, $E = \mathbb{F}_{q^t}$;
2) take $\mathfrak{S} = \{a_1, ..., a_n\}$ as a subset of E;
3) choose $f_i(x) \in K[x]$, $1 \leq i \leq k$, such that $f_i(a_j) \in F$ for all i, j, and $f_i(x)$ $(1 \leq i \leq k)$ are linearly independent over F;
4) let $V = \mathrm{span}\langle f_i(x) : 1 \leq i \leq k\rangle_F$;
5) then $C := \{(f(a_1), \cdots, f(a_n)) \mid f \in V\}$ is a linear $[n, k]$ code over F.

The difficulty of constructing quantum codes via polynomial codes lies in the determination of the dual codes.

In [12], the authors considered the polynomial codes over $F = \mathbb{F}_q$ with $\gcd(m, q) = 1$, $\mathrm{ord}_m(q) = t$, $K = E = \mathbb{F}_{q^t}$ and $\mathfrak{S} = U_m \bigcup\{0\}$, where U_m is the subgroup of E^* with order m. In this paper, we considered the polynomial codes over $F = \mathbb{F}_q$ with $q = p^\alpha$ being a prime power, $\gcd(m, q) = 1$, $\mathrm{ord}_m(q) = p^b$, $K = \mathbb{F}_{q^{p^{b-1}}}$, $E = \mathbb{F}_{q^{p^b}}$ and $\mathfrak{S}$ being a complete set of representatives of elements from $U_m\backslash(U_m \bigcap K)$ which are pairwise nonconjugate over K, where U_m is the subgroup of E^* with order m. Since there are many choices of fields, points and polynomials, we expect that more quantum codes (or linear codes) with good parameters can be constructed from the framework above.

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] 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.
[4] 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.
[5] Y. Ding, L. Jin, and C. Xing, "Good linear codes from polynomial evaluations," *IEEE Trans. Commun.*, vol. 60, no. 2, pp. 357–363, Feb. 2012.

[6] Y. Edel. *Some Good Quantum Twisted Codes*, accessed on Dec. 21, 2014. [Online]. Available: https://www.mathi.uni-heidelberg.de/~yves/Matritzen/QTBCH/QTBCHIndex.html
[7] M. F. Ezerman, S. Jitman, and P. Solé, "Xing-Ling codes, duals of their subcodes, and good asymmetric quantum codes," *Designs, Codes Cryptogr.*, vol. 75, no. 1, pp. 21–42, 2015.
[8] K. Feng, S. Ling, and C. Xing, "Asymptotic bounds on quantum codes from algebraic geometry codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 986–991, Mar. 2006.
[9] K. Feng and C. Xing, "A new construction of quantum error-correcting codes," *Trans. Amer. Math. Soc.*, vol. 360, no. 4, pp. 2007–2019, Apr. 2008.
[10] M. Grassl. (2007). *Bounds on the Minimum Distance of Linear Codes and Quantum Codes*, accessed on Dec. 21, 2014. [Online]. Available: http://wwwcodetables.de
[11] W. C. Huffman and V. Pless, *Fundamentals Error-Correcting Codes*. Cambridge, MA, USA: Cambridge Univ. Press, 2003.
[12] L. Jin and C. Xing, "A construction of quantum codes via a class of classical polynomial codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2012, pp. 339–342.
[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] G. G. L. Guardia, "On the construction of nonbinary quantum BCH codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 3, pp. 1528–1535, Mar. 2014.
[15] S. Li, M. Xiong, and G. Ge, "Pseudo-cyclic codes and the construction of quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 62, no. 4, pp. 1703–1710, Apr. 2016.
[16] Z. Li, L. Xing, and X. Wang, "Quantum generalized reed-solomon codes: Unified framework for quantum maximum-distance-separable codes," *Phys. Rev. A*, vol. 77, no. 1, p. 012308, 2008.
[17] L. Xiaoyan, "Quantum cyclic and constacyclic codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 547–549, Mar. 2004.
[18] S. Ling, H. Niederreiter, and C. Xing, "Symmetric polynomials and some good codes," *Finite Fields Appl.*, vol. 7, no. 1, pp. 142–148, Jan. 2001.
[19] E. M. Rains, "Nonbinary quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1827–1832, Sep. 1999.
[20] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, no. 4, p. R2493, Oct. 1995.
[21] A. Steane, "Multiple-particle interference and quantum error correction," *Proc. R. Soc. Lond. A Math. Phys. Eng. Sci.*, vol. 452, pp. 2551–2577, Nov. 1996.
[22] A. M. Steane, "Enlargement of calderbank-shor-steane quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2492–2495, Nov. 1999.
[23] M. Steinbach and D. Hachenberger, "A class of quaternary linear codes improving known minimum distances," *Designs, Codes Cryptogr.*, vol. 78, no. 3, pp. 615–627, 2016.
[24] C. Xing and S. Ling, "A class of linear codes with good parameters," *IEEE Trans. Inf. Theory*, vol. 46, no. 6, pp. 2184–2188, Sep. 2000.
[25] T. Zhang and G. Ge, "Quantum mds Codes With Large Minimum Distance," *Designs Codes Cryptogr.*, to appear. [Online]. Available: http://dx.doi.org/10.1007/s10623-016-0245-0
[26] T. Zhang and G. Ge, "Some new classes of quantum MDS codes from constacyclic codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 9, pp. 5224–5228, Sep. 2015.

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.