Chin. Ann. Math.
37B(6), 2016, 891–898
DOI: 10.1007/s11401-016-1043-8

Chinese Annals of Mathematics, Series B

New Quantum MDS Code from Constacyclic Codes*

Liqin HU[1] Qin YUE[2] Xiaomeng ZHU[2]

Abstract In recent years, there have been intensive activities in the area of constructing quantum maximum distance separable (MDS for short) codes from constacyclic MDS codes through the Hermitian construction. In this paper, a new class of quantum MDS code is constructed, which extends the result of [Theorems 3.14–3.15, Kai, X., Zhu, S., and Li, P., *IEEE Trans. on Inf. Theory,* **60**(4), 2014, 2080–2086], in the sense that our quantum MDS code has bigger minimum distance.

Keywords Cyclotomic coset, Quantum MDS code, Constacyclic code, BCH bound
2000 MR Subject Classification 11T22, 81P45, 94B05, 94B65

1 Introduction

Quantum codes were introduced to protect quantum information from decoherence and quantum noise. After the pioneering work of Shor [24] and Steane [25], a systematic mathematical scheme has been employed to construct q-ary quantum codes from classical error-correcting codes over $\mathbb{F}_q$ or $\mathbb{F}_{q^2}$ with certain orthogonality properties. The quantum codes obtained in this way are called stabilizer codes. After the establishment of the connection between quantum codes and classical codes (see [3]), the construction of stabilizer codes can be converted to that of classical codes with symplectic, Euclidean, or Hermitian self-orthogonal property.

A q-ary quantum code Q of length n and size K is a K-dimensional subspace of a q^n-dimensional Hilbert space $\mathbb{H} = (\mathbb{C}^q)^{\otimes\, n} = \mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q$. An important parameter of a quantum code is its minimum distance: If a quantum code has minimum distance d, then it can detect $d-1$ and correct $\lfloor \frac{d-1}{2} \rfloor$ quantum errors. 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: $2d \leq n-k+2$ (see [19–20]). A quantum code achieving this quantum Singleton bound is called a quantum maximum-distance-separable (MDS for short) code. Ketkar et al. in [19] 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. As mentioned in [16], except for some sparse lengths n such as $n = q^2+1$, $\frac{q^2+1}{2}$

Manuscript received February 22, 2015. Revised December 28, 2015.
[1]School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China. E-mail: huliqin@hdu.edu.cn
[2]Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China. E-mail: yueqin@nuaa.edu.cn mooneernanjing@163.com
*This work was supported by the National Natural Science Foundation of China (Nos. 11171150, 113711138, 11531002) and the Foundation of Science and the Technology on Information Assurance Laboratory (No. KJ-15-009).

and q^2, almost all known q-ary quantum MDS codes have minimum distance less than or equal to $\frac{q}{2}+1$. The following result gives a connection between classical Hermitian self-orthogonal MDS codes and quantum MDS codes.

Theorem 1.1 (see [2]) *If C is a q^2-ary $[n,k,n-k+1]$ MDS code such that $\mathcal{C}\subseteq\mathcal{C}^{\perp_H}$, then there exists a q-ary $[[n,n-2k,k+1]]$ quantum code.*

In recent years, constructing quantum MDS codes has become a hot research topic. Many classes of quantum MDS codes have been found by employing different methods (see [1, 4–5, 7–17, 22–23]). Recently, Kai et al. [17–18] constructed several classes of good quantum codes from classical constacyclic codes, including some new classes of quantum MDS codes.

Motivated by the above works, a new family of quantum MDS code is constructed in this paper. The quantum code in this paper can be regarded as a generalization of [18, Theorems 3.14–3.15], in the sense that our quantum MDS code has bigger minimum distance.

2 Preliminaries

In this section, we recall some definitions and basic properties of constacyclic codes. Throughout this paper, q denotes an odd prime power and $\mathbb{F}_{q^2}$ denotes the finite field with q^2 elements. 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 $\mathcal{C}$ of length n is an $\mathbb{F}_{q^2}$ subspace of $\mathbb{F}_{q^2}^n$. For a nonzero element η of $\mathbb{F}_{q^2}$, a linear code $\mathcal{C}$ of length n over $\mathbb{F}_{q^2}$ is said to be η-constacyclic if $(\eta c_{n-1},c_0,\cdots,c_{n-2})\in\mathcal{C}$ for every $(c_0,c_1,\cdots,c_{n-1})\in\mathcal{C}$. If each codeword $\mathbf{c}=(c_0,c_1,\cdots,c_{n-1})\in\mathcal{C}$ corresponds with its polynomial representation $c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}\in\mathbb{F}_{q^2}[x]$, then the η-constacyclic code $\mathcal{C}$ is identified with exactly one ideal of the quotient ring $\mathbb{F}_{q^2}[x]/(x^n-\eta)$. Since $\mathbb{F}_{q^2}[x]/(x^n-\eta)$ is a principal ideal ring, an η-constacyclic code $\mathcal{C}$ is generated uniquely by a monic divisor $g(x)$ of $x^n-\eta$ and denoted by $\mathcal{C}=\langle g(x)\rangle$. Hence $g(x)$ and $h(x)=\frac{x^n-\eta}{g(x)}$ are called the generator polynomial and the check polynomial of $\mathcal{C}$, respectively.

Similarly to cyclic codes, there exists the following BCH bound for η-constacyclic codes (see [21]).

Lemma 2.1 *Let $\mathcal{C}=\langle g(x)\rangle$ be an η-constacyclic code of length n over $\mathbb{F}_{q^2}$ and $\gcd(q,n)=1$. Suppose that the roots of $g(x)$ include $\gamma\alpha^i$, $i=1,2,\cdots,d-1$ $(\leq\deg g(x))$, where γ and α are nonzero elements in some extension field of $\mathbb{F}_{q^2}$, and α is an element of order n. Then the minimum distance of the code is at least d.*

For two vectors $\mathbf{b}=(b_1,b_2,\cdots,b_n)$ and $\mathbf{c}=(c_1,c_2,\cdots,c_n)$ in $\mathbb{F}_{q^2}^n$, we define the Hermitian inner product $\langle\mathbf{b},\mathbf{c}\rangle_H$ to be $\langle\mathbf{b},\mathbf{c}\rangle_H=\sum_{i=1}^{n}b_i\overline{c_i}$, where $\overline{c_i}=c_i^q$ for each $1\leq i\leq n$. The vectors $\mathbf{b}$ and $\mathbf{c}$ are called orthogonal with respect to Hermitian inner product if $\langle\mathbf{b},\mathbf{c}\rangle_H=0$. For a q^2-ary linear code $\mathcal{C}$, the Hermitian dual codes of $\mathcal{C}$ is defined as

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

A q^2-ary linear code $\mathcal{C}$ of length n is called Hermitian self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^{\perp_H}$. Conversely, if $\mathcal{C}^{\perp_H} \subseteq \mathcal{C}$, we say that $\mathcal{C}$ is a Hermitian dual-containing code.

The automorphism of $\mathbb{F}_{q^2}$ given by " $-$ ", $\overline{a} = a^q$ for any $a \in \mathbb{F}_{q^2}$, can be extended to an automorphism of $\mathbb{F}_{q^2}[x]$ in an obvious way:

$$\mathbb{F}_{q^2}[x] \to \mathbb{F}_{q^2}[x], \quad \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \overline{a_i} x^i$$

for any $a_0, a_1, \cdots, a_n$ in $\mathbb{F}_{q^2}$, which is also denoted by " $-$ " for simplicity.

For a monic polynomial $f(x) \in \mathbb{F}_{q^2}[x]$ of degree k with $f(0) \neq 0$, its reciprocal polynomial will be denoted by

$$f(x)^* = f(0)^{-1} x^k f(x^{-1}).$$

The following result gives the generator polynomial of $\mathcal{C}^{\perp_H}$.

Lemma 2.2 (see [26, Lemma 2.1(ii)]) *Let $\mathcal{C} = \langle g(x) \rangle$ be an η-constacyclic code of length n and dimensional k over $\mathbb{F}_{q^2}$. Set $h(x) = \frac{x^n - \eta}{g(x)}$. Then the Hermitian dual code $\mathcal{C}^{\perp_H}$ is an $\overline{\eta}^{-1}$-constacyclic code with the generator polynomial $\overline{h(x)^*}$, where*

$$h(x)^* = \sum_{i=0}^{k} a_i x^i$$

and

$$\overline{h(x)^*} = \sum_{i=0}^{k} a_i^q x^i$$

are the reciprocal and conjugate-reciprocal polynomials of $h(x)$, respectively.

By Lemma 2.2, we can get the following result.

Lemma 2.3 *Let $\eta \in \mathbb{F}_{q^2}$ be a primitive r-th root of unity and let $\mathcal{C}$ be a Hermitian dual-containing η-constacyclic code of length n over $\mathbb{F}_{q^2}$. Then $\eta = \eta^{-q}$, i.e., $r \mid q+1$.*

Let $\mathcal{C} = \langle g(x) \rangle$ be an η-constacyclic code of length n and let $\Omega = \{1 + jr \mid 0 \leq j \leq n-1\}$. The set $Z = \{k \in \Omega \mid g(\zeta^k) = 0\}$ is called the defining set of $\mathcal{C}$, where ζ is a primitive rn-th root of unity in some extension field of $\mathbb{F}_{q^2}$ such that $\zeta^n = \eta$. The following result presents a criterion to determine whether or not an η-constacyclic code of length n over $\mathbb{F}_{q^2}$ is Hermitian dual-containing.

Lemma 2.4 (see [18, 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 $\mathcal{C}$ is an η-constacyclic code of length n over $\mathbb{F}_{q^2}$ with a defining set Z. Then $\mathcal{C}$ is a Hermitian dual-containing code if and only if $Z \cap (-q)Z = \emptyset$, where $(-q)Z = \{-qz \pmod{rn} \mid z \in Z\}$.*

The Hermitian construction suggests that we can obtain q-ary quantum codes as long as we can construct classical Hermitian dual-containing codes over $\mathbb{F}_{q^2}$. Constacyclic codes form an important class of linear codes due to their good algebraic structures. In this paper, we will use the Hermitian construction to obtain MDS quantum codes through constacyclic codes.

3 New Quantum MDS Code

Throughout this section, we always assume that η is a primitive r-th root of unity in $\mathbb{F}_{q^2}$ with $r \mid (q+1)$, and n is a positive integer with $rn \mid (q^4-1)$ and $rn \nmid (q^2-1)$. In this section, we construct a family of q-ary quantum codes with good parameters through the Hermitian construction.

Let $\mathcal{C}$ be an η-constacyclic code and let $\Omega = \{1+jr \mid 0 \le j \le n-1\}$. Since $rn \mid (q^4-1)$, we always have that $|C_{1+jr}| \le 2,\ 0 \le j \le n-1$, where C_{1+jr} is the q^2-cyclotomic coset containing $1+jr$ modulo rn.

Lemma 3.1 *There exist exactly two q^2-cyclotomic cosets C_{1+rk} and $C_{1+r(k+\frac{n}{2})}$ with $|C_{1+rk}| = |C_{1+r(k+\frac{n}{2})}| = 1$ if and only if $n \mid (q^2+1)$ and n is even, where $rk \equiv -1 \pmod{\frac{n}{2}},\ 0 \le k \le \frac{n}{2}-1$.*

Proof Suppose that $i = 1+jr \in \Omega,\ 0 \le j \le n-1$. Then there are exactly two q^2-cyclotomic cosets C_i and $C_{i'}$ $(i, i' \in \Omega,\ i \ne i')$ with $|C_i| = |C_{i'}| = 1$ if and only if the congruence equation $(1+jr)q^2 \equiv 1+jr \pmod{rn}$ has exactly two different solutions, which implies that

$$(q^2-1)j \equiv -\frac{q^2-1}{r} \pmod{n} \tag{3.1}$$

has two solutions k and k' with $0 \le k \ne k' \le n-1$. As $rn \mid q^4-1$ and $\gcd(q^2-1, q^2+1) = 2$, (3.1) has two solutions if and only if $\gcd(n, q^2-1) = 2$ if and only if $n \mid (q^2+1)$ and n is even, so $i = 1+rk,\ i' = 1+r\big(k+\frac{n}{2}\big)$, where $rk \equiv -1 \pmod{\frac{n}{2}},\ 0 \le k \le \frac{n}{2}-1$.

Suppose that $n \mid q^2+1$ and n is even. By Lemma 3.1, there are exactly two q^2-cyclotomic cosets C_s and $C_{s+\frac{rn}{2}}$ with $|C_s| = |C_{s+\frac{rn}{2}}| = 1$, where $s = \frac{q^2+1}{2}$.

Lemma 3.2 *Let n be an even divisor of q^2+1. Suppose that $s = \frac{q^2+1}{2}$. Then $\Omega = \{1+jr \mid 0 \le j \le n-1\}$ is a disjoint union of q^2-cyclotomic cosets:*

$$\Omega = C_s \cup C_{s+\frac{rn}{2}} \cup \Big(\bigcup_{j=1}^{\frac{n}{2}-1} C_{s-rj} \Big).$$

Proof Since $n \mid q^2+1$ and n is even, by Lemma 3.1 there are exactly two q^2-cyclotomic cosets C_s and $C_{s+\frac{rn}{2}}$ with one element.

For each $j,\ 1 \le j \le \frac{n}{2}-1$,

$$q^2(s+rj) = q^2 s + (q^2+1)rj - rj \equiv s - rj \pmod{rn}.$$

Hence $C_{s+rj} = \{s-rj, s+rj\}$ for $1 \le j \le \frac{n}{2}-1$.

In order to use Lemma 3.2 to construct Hermitian dual-containing MDS constacyclic code, we need the condition that $-qC_s = C_{s+\frac{rn}{2}}$, i.e., $C_s \ne -qC_s$.

Proposition 3.1 *Let n be an even divisor of q^2+1 and $s = \frac{q^2+1}{2}$. Then $C_s \ne -qC_s$ if and only if $2 \nmid \frac{q+1}{r}$, where $C_s = \{s\}$ is the q^2-cyclotomic coset containing s.*

Proof For $s=\frac{q^2+1}{2}$, $s\equiv -qs \pmod{rn}$ if and only if $rn \mid (q+1)s$, which implies $n \mid \frac{(q+1)s}{r}$. By $s=\frac{q^2+1}{2}$, we have $\frac{n}{2}|s$ with s odd, so $n \mid \frac{(q+1)s}{r}$ if and only if $2 \mid \frac{q+1}{r}$. Hence, we get the result.

The following results are given in [18].

Lemma 3.3 (see [18, Theorem 3.14]) *Let q be an odd prime power with the form $20m+3$ or $20m+7$, where m is a positive integer. Let $n=\frac{q^2+1}{5}$. Then, there exists a q-ary $[[n, n-2d+2, d]]$-quantum MDS code, where $2 \le d \le \frac{q+5}{2}$ is even.*

Lemma 3.4 (see [18, Theorem 3.15]) *Let q be an odd prime power with the form $20m-3$ or $20m-7$, where m is a positive integer. Let $n=\frac{q^2+1}{5}$. Then, there exists a q-ary $[[n, n-2d+2, d]]$-quantum MDS code, where $2 \le d \le \frac{q+3}{2}$ is even.*

Using the Hermitian construction, we will obtain q-ary quantum codes of length $\frac{q^2+1}{5}$ from constacyclic codes over $\mathbb{F}_{q^2}$. The main code of this paper has much larger minimum distance than the one of [18] when $q>23$.

Let q be an odd prime power with $q \equiv 3 \pmod{10}$ or $q \equiv -3 \pmod{10}$, and $n=\frac{q^2+1}{5}$. We consider η-constacyclic code of length n over $\mathbb{F}_{q^2}$.

In order to construct quantum MDS codes, we give a sufficient condition for η-constacyclic codes which contain their Hermitian duals. For any odd prime power q with $q \equiv \pm 3 \pmod{10}$, we first consider the case $q \equiv 3 \pmod{10}$.

Lemma 3.5 *Assume that q is an odd prime power with $q \equiv 3 \pmod{10}$ and $\frac{q+1}{r}$ odd. Let $s=\frac{q^2+1}{2}$ and $n=\frac{q^2+1}{5}$. If $\mathcal{C}$ is an η-constacyclic code over $\mathbb{F}_{q^2}$ of length n with defining set $Z=\bigcup_{j=0}^{\delta} C_{s-jr}$, where $0 \le \delta \le \frac{3(q-3)}{10}$, then $\mathcal{C}$ is a Hermitian dual-containing code.*

Proof By Lemma 2.4, it is sufficient to prove that $Z \cap (-q)Z = \emptyset$. Suppose that $Z \cap (-q)Z \neq \emptyset$. Then, there exist two integers $j,\ k,\ 0 \le j,k \le \frac{3(q-3)}{10}$, such that $s-rj \equiv -q(s-rk) \pmod{rn}$ or $s-rj \equiv -q(s+rk) \pmod{rn}$.

Case I $s-rj \equiv -q(s-rk) \pmod{rn}$. This is equivalent to

$$\frac{q+1}{r}s \equiv qk+j \pmod{n}.$$

By $s=\frac{q^2+1}{2}$ and $\frac{q+1}{r}$ odd, we obtain

$$qk+j \equiv \frac{n}{2} \pmod{n}.$$

Since $0 \le j,k \le \frac{3(q-3)}{10},\ 0 \le j+qk \le \frac{3(q-3)(q+1)}{10} < \frac{3n}{2}$. We have that $j+qk \equiv \frac{n}{2} \pmod{n}$ if and only if $qk+j=\frac{n}{2}$. Since

$$\frac{n}{2}=\frac{q^2+1}{10}=\frac{q^2-3q+3q+1}{10}=q\cdot\frac{q-3}{10}+\frac{3q+1}{10},$$

we have

$$qk+j=q\cdot\frac{q-3}{10}+\frac{3q+1}{10}.$$

By division algorithm, $j = \frac{3q+1}{10}$. This is impossible, because

$$0 \le j \le \frac{3(q-3)}{10}.$$

Case II $s - rj \equiv -q(s + rk) \pmod{rn}$. This is equivalent to

$$\frac{q+1}{r} s \equiv -qk + j \pmod{n}.$$

As $s = \frac{q^2+1}{2}$ and $\frac{q+1}{r}$ odd, we obtain

$$-qk + j \equiv \frac{n}{2} \pmod{n}.$$

Since $0 \le j, k \le \frac{3(q-3)}{10}$, we have

$$-\frac{3n}{2} < -\frac{3(q-3)q}{10} \le -qk + j \le \frac{3(q-3)}{10} < \frac{n}{2}.$$

We have that $-qk + j \equiv \frac{n}{2} \pmod{n}$ if and only if

$$-qk + j = -\frac{n}{2}.$$

Hence

$$-qk + j = -\Big(q \cdot \frac{q-3}{10} + \frac{3q+1}{10}\Big) = -q \cdot \frac{q+7}{10} + \Big(q - \frac{3q+1}{10}\Big).$$

By division algorithm,

$$j = q - \frac{3q+1}{10} = \frac{7q-1}{10} > \frac{3(q-3)}{10}.$$

This is impossible.

Theorem 3.1 *Let q be an odd prime power with $q \equiv 3 \pmod{10}$. Then, there exist quantum MDS codes with parameters $\big[\big[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 2, d\big]\big]_q$, where d $\big(2 \le d \le \frac{3q+1}{5}\big)$, is even.*

Proof Put $s = \frac{q^2+1}{2}$ with $\frac{q+1}{r}$ odd. Let η be an r-th primitive root in $\mathbb{F}_{q^2}$. Consider the η-constacyclic code $\mathcal{C}$ over $\mathbb{F}_{q^2}$ of length $n = \frac{q^2+1}{5}$ with defining set $Z = \bigcup_{j=0}^{\delta} C_{s-jr}$, where $0 \le \delta \le \frac{3(q-3)}{10}$. From Lemma 3.5, $\mathcal{C}^{\perp} \subseteq \mathcal{C}$. From Lemma 3.2 we can see that Z contains $2\delta + 1$ consecutive integers. This implies that $\mathcal{C}$ has minimum distance at least $2\delta + 2$. Hence, $\mathcal{C}$ is an $[n, n - 2\delta - 1, 2\delta + 2]$ MDS constacyclic code. Combining the Hermitian construction with quantum Singleton bound, we can obtain a quantum MDS code with parameters $\big[\big[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 2, d\big]\big]_q$, where d, $2 \le d \le \frac{3q+1}{5}$, is even.

Compare our quantum MDS codes in Theorem 3.1 with quantum MDS codes in [18], our quantum MDS codes has much bigger minimum distance than the known codes in [18] when $q > 23$, because

$$\frac{3q+1}{5} > \frac{q+5}{2}$$

for $q > 23$.

Example 3.1 Take $q = 43$, and so $n = 370$. Using Theorem 3.1 produces a new quantum MDS code with parameters $[[370, 320, 26]]_{43}$.

For the case $q \equiv -3 \pmod{10}$, we can produce the following quantum MDS codes. The proof is similar to that in the case $q \equiv 3 \pmod{10}$ and we omit it.

Theorem 3.2 *Let q be an odd prime power with $q \equiv -3 \pmod{10}$. Then, there exist quantum MDS codes with parameters $\left[\left[\frac{q^2+1}{5}, \frac{q^2+1}{5} - 2d + 2, d\right]\right]_q$, where $2 \leq d \leq \frac{3q-1}{5}$ is even.*

Example 3.2 Take $q = 37$, and so $n = 137$. Using Theorem 3.2 produces a new quantum MDS code with parameters $[[137, 95, 22]]_{37}$.

References

[1] Aly, S. A., Klappenecker, A. and Sarvepalli, P. K., On quantum and classical BCH codes, *IEEE Trans. Inf. Theory*, **53**(3), 2007, 1183–1188.

[2] Ashikhmin, A. and Knill, E., Nonbinary quantum stablizer codes, *IEEE Trans. Inf. Theory*, **47**(7), 2001, 3065–3072.

[3] Calderbank, A. R., Rains, E. M., Shor, P. W. and Sloane, N. J. A., Quantum error correction via codes over GF(4), *IEEE Trans. Inf. Theory*, **44**(4), 1998, 1369–1387.

[4] Chen, H., Some good quantum error-correcting codes from algebraic-geometric codes, *IEEE Trans. Inf. Theory*, **47**(5), 2001, 2059–2061.

[5] Chen, H., Ling, S. and Xing, C., Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound, *IEEE Trans. Inf. Theory*, **47**(5), 2001, 2055–2058.

[6] Chen, H., Ling, S. and Xing, C., Quantum codes from concatenated algebraic-geometric codes, *IEEE Trans. Inf. Theory*, **51**(8), 2005, 2915–2920.

[7] Chen, B., Ling, S. and Zhang, G., Application of constacyclic codes to quantum MDS codes, *IEEE Trans. Inf. Theory*, **61**(3), 2015, 1474–1484.

[8] Feng, K., Quantum codes $[[6, 2, 3]]_p$ and $[[7, 3, 3]]_p$ ($p \geq 3$) exist, *IEEE Trans. Inf. Theory*, **48**(8), 2002, 2384–2391.

[9] Feng, K., Ling, S. and Xing, C., Asymptotic bounds on quantum codes from algebraic geometry codes, *IEEE Trans. Inf. Theory*, **52**(3), 2006, 986–991.

[10] Grassl, M., Beth, T. and Rötteler, M., On optimal quantum codes, *Int. J. Quantum Inform.*, **2**(1), 2004, 757–766.

[11] Rötteler, M., Grassl, M. and Beth, T., On quantum MDS codes, Information Theory, Proceedings International Symposium on IEEE, 2004, 356.

[12] Guardia, G. G. L., New quantum MDS codes, *IEEE Trans. Inf. Theory*, **57**(8), 2011, 5551–5554.

[13] Hu, X., Zhang, G. and Chen, B., Constructions of new nonbinary quantum codes, *Int. J. Theor. Phys.*, **54**(1), 2014, 92–99.

[14] Jin, L., Ling, S., Luo, J. and Xing, C., Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes, *IEEE Trans. Inf. Theory*, **56**(9), 4735–4740, 2010.

[15] Jin, L. and Xing, C., Euclidean and Hermitian self-orthogonal algebraic geometry codes and their application to quantum codes, *IEEE Trans. Inf. Theory*, **58**, 2012, 5484–5489.

[16] Jin, L. and Xing, C., A construction of new quantum MDS codes, *IEEE Trans. Inf. Theory*, **60**, 2014, 2921–2925.

[17] Kai, X. and Zhu, S., New quantum MDS codes from negacyclic codes, *IEEE Trans. Inf. Theory*, **59**(2), 2013, 1193–1197.

[18] Kai, X., Zhu, S. and Li, P., Constacyclic codes and some new quantum MDS codes, *IEEE Trans. Inf. Theory*, **60**(4), 2014, 2080–2086.

[19] Ketkar, A., Klappenecker, A., Kumar, S. and Sarvepalli, P. K., Nonbinary stabilizer codes over finite fields, *IEEE Trans. Inf. Theory*, **52**(11), 2006, 4892–4914.

[20] Knill, E. and Laflamme, R., Theory of quantum error-correcting codes, *Phys. Rev. A*, **55**(2), 1997, 900–911.

[21] Krishna, A. and Sarwate, D. V., Pseudocyclic maximum-distance separable codes, *IEEE Trans. Inf. Theory*, **36**(4), 1990, 880–884.

[22] Li, Z., Xing, L. J. and Wang, X. M., Quantum generalized Reed-Solomon codes: Unified framework for quantum maximum-distance separable codes, *Phys. Rev. A*, **77**, 2008, 012308(1)–012308(4).

[23] Ling, S., Luo, L. and Xing, C., Generalization of Steane's enlargement construction of quantum codes and applications, *IEEE Trans. Inf. Theory*, **56**(8), 2010, 4080–4084.

[24] Shor, P. W., Scheme for reducing decoherence in quantum computer memory, *Phys. Rev. A*, **52**(4), 1995, 2493–2496.

[25] Steane, A. M., Multiple particle interference and quantum error correction, *Proc. Roy. Soc. London A*, **452**(1), 1996, 2551–2577.

[26] Yang, Y. and Cai, W., On self-dual constacyclic codes over finite fields, *Des., Codes Cryptogr.*, **74**(2), 2013, 355–364.