Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes

Jin, Lingfei; Ling, San; Luo, Jinqun; Xing, Chaoping

2010

Jin, L., Ling, S., Luo, J., & Xing, C. (2010). Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes. *IEEE Transactions on Information Theory*, 56 (9), 4735-4740.

<https://hdl.handle.net/10356/94049>

<https://doi.org/10.1109/TIT.2010.2054174>

© 2010 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at:
<http://dx.doi.org/10.1109/TIT.2010.2054174>.

Downloaded on 26 Apr 2023 18:50:23 SGT

Application of Classical Hermitian Self-Orthogonal MDS Codes to Quantum MDS Codes

Lingfei Jin, San Ling, Jinquan Luo and Chaoping Xing

Abstract—In this paper, we first construct several classes of classical Hermitian self-orthogonal MDS codes. Through these classical codes, we are able to obtain various quantum MDS codes. It turns out that many of our quantum codes are new in the sense that the parameters of our quantum codes cannot be obtained from all previous constructions.

I. INTRODUCTION

Quantum codes were introduced to protect quantum information from decoherence and quantum noise. After the pioneering work of Shor [22] and Steane [24], a systematic mathematical scheme has been employed to construct ℓ -ary quantum codes from classical error-correcting codes over $\mathbb{F}_\ell$ or $\mathbb{F}_{\ell^2}$ with certain orthogonality properties (see [5] for $\ell = 2$, and [2], [6], [12] for nonbinary case), where ℓ is a prime power. The quantum codes obtained in this way are called stabilizer codes. After the establishment of the above connection between quantum codes and classical codes, the construction of stabilizer codes can be converted to that of classical codes with symplectic, Euclidean or Hermitian self-orthogonal property (see [1], [7], [15], [16], [21], [25], etc).

Meanwhile, several bounds concerning the parameters of quantum codes have been investigated. An ℓ -ary $((n, K, d))$ (or $[[n, k = \log K, d]]_\ell$) quantum code is a K (or ℓ^k)-dimensional vector subspace of the Hilbert space $(\mathbb{C}^\ell)^{\otimes n}$ which can detect up to $d - 1$ quantum errors, or equivalently, correct up to $\lfloor (d - 1)/2 \rfloor$ quantum errors. The celebrated Singleton bound saying that an ℓ -ary $((n, K, d))$ quantum code satisfies

$$\log_\ell K \leq n - 2d + 2$$

was proven by various researchers using different techniques. A quantum code achieving this quantum Singleton bound is called a quantum MDS code.

In the past few years, researchers have been working very hard to construct quantum MDS codes (see [4], [8], [10], [11], [16] and [21]). One of the main ideas of these papers is to

construct quantum MDS codes through classical symplectic, Euclidean or Hermitian self-orthogonal MDS codes. In this paper, we also employ this idea by constructing several new classes of classical Hermitian self-orthogonal MDS codes. It turns out that many of our quantum codes are new in the sense that the parameters of our quantum codes cannot be obtained from all previous constructions. Precisely speaking, in the present paper, (i) we construct ℓ -ary quantum MDS codes of length $\ell^2 + 1$ with distance $k + 1$ for any $2 \leq k \leq \ell/2$ (this class of quantum MDS codes has not been constructed before); (ii) we show the existence of ℓ -ary $[[n, n - 4, 3]]$ -quantum MDS codes for any $4 \leq n \leq \ell^2 + 1$, except for the case where $\ell = 2$ and $n = 4$ (this class of quantum MDS codes has not been constructed before for even ℓ); (iii) we construct roughly three times as many quantum MDS codes as all the previously known ones.

The paper is organized as follows. In Section 2, we use generalized Reed-Solomon codes and algebraic geometry codes to construct classical Hermitian self-orthogonal codes. In the last section, we apply our codes in Section 2 to obtain new quantum MDS codes.

II. HERMITIAN SELF-ORTHOGONAL GRS CODES

One of the ideas in this section is to construct Hermitian self-orthogonal MDS codes through generalized Reed-Solomon (RS for short) codes.

We first recall some basic results of generalized Reed-Solomon codes (see [14], [18]). Let $\mathbb{F}_q$ be a finite field of q elements, choose n distinct elements $\alpha_1, \dots, \alpha_n$ of $\mathbb{F}_q$, and n nonzero elements $v_1, \dots, v_n$ of $\mathbb{F}_q$. For k between 1 and n , the generalized RS code $\mathcal{GRS}_k(\mathbf{a}, \mathbf{v})$ is defined by $\mathcal{GRS}_k(\mathbf{a}, \mathbf{v}) = \{(v_1 f(\alpha_1), \dots, v_n f(\alpha_n)) : f(x) \in \mathbb{F}_q[x], \deg(f(x)) \leq k - 1\}$, where $\mathbf{a}$ and $\mathbf{v}$ denote the vectors $(\alpha_1, \dots, \alpha_n)$ and $(v_1, \dots, v_n)$, respectively.

For two vectors $\mathbf{b} = (b_1, \dots, b_n)$ and $\mathbf{c} = (c_1, \dots, c_n)$ in $\mathbb{F}_q^n$, we define the Euclidean inner product $\langle \mathbf{b}, \mathbf{c} \rangle_E$ to be the usual dot product, i.e., $\langle \mathbf{b}, \mathbf{c} \rangle_E = \sum_{i=1}^n b_i c_i$. For a q -ary linear code C of length n , the Euclidean dual $C^\perp$ of C consists of all the vectors of $\mathbb{F}_q^n$ which are orthogonal to the codewords of C with respect to the above Euclidean inner product.

The dual $\mathcal{GRS}_k^\perp(\mathbf{a}, \mathbf{v})$ of $\mathcal{GRS}_k(\mathbf{a}, \mathbf{v})$ is the generalized RS code $\mathcal{GRS}_{n-k}(\mathbf{a}, \mathbf{u})$, where $\mathbf{u}$ is a nonzero solution of the

L. F. Jin is with School of Mathematics, Hefei University of Technology, Hefei, Anhui 280096, China.

L. F. Jin, S. Ling, J. Q. Luo and C. P. Xing are with Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371, Republic of Singapore (email: {lingsan, jqluo, xingcp}@ntu.edu.sg).

J. Q. Luo is also with School of Mathematical Sciences, Yangzhou University, Yangzhou, China.

The work of the last three authors was partially supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03 and the Singapore MoE Academic Research Fund. The work of J. Luo is also supported by NSFC under Grant 60903036 and NSF of Jiangsu Province under Grant BK2009182.

C. P. Xing is the corresponding author.

system

$$\begin{pmatrix} v_1 & v_2 & \dots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \dots & v_n\alpha_n \\ v_1\alpha_1^2 & v_2\alpha_2^2 & \dots & v_n\alpha_n^2 \\ \vdots & \vdots & \dots & \vdots \\ v_1\alpha_1^{n-2} & v_2\alpha_2^{n-2} & \dots & v_n\alpha_n^{n-2} \end{pmatrix} \mathbf{x}^T = \mathbf{0}. \quad (\text{II.1})$$

Note that by deleting any one column of the above coefficient matrix, the remaining matrix is an $(n-1) \times (n-1)$ Vandermonde matrix, hence the solution space of the above system has dimension 1 and every nonzero solution has all coordinates not equal to zero.

To define the Hermitian inner product, we shall assume that $q = \ell^2$ for a prime power ℓ from now on in this paper.

For two vectors $\mathbf{b} = (b_1, \dots, b_n)$ and $\mathbf{c} = (c_1, \dots, c_n)$ in $\mathbb{F}_q^n$, we define the Hermitian inner product $\langle \mathbf{b}, \mathbf{c} \rangle_H$ to be $\langle \mathbf{b}, \mathbf{c} \rangle_H = \sum_{i=1}^n b_i c_i^\ell$. It is easy to see that $\langle \mathbf{b}, \mathbf{c} \rangle_H = \langle \mathbf{c}, \mathbf{b} \rangle_H^\ell$. For a q -ary linear code C of length n , the Hermitian dual $C^{\perp_H}$ of C consists of all the vectors of $\mathbb{F}_q^n$ which are orthogonal to the codewords of C with respect to the above Hermitian inner product. From the fact that the Hermitian inner product is non-degenerate, it follows immediately that $(C^{\perp_H})^{\perp_H} = C$ holds. Moreover, one has $\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(C^{\perp_H}) = n$.

For a vector $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{F}_q^n$, let $\mathbf{v}^m = (v_1^m, \dots, v_n^m)$ for any $m \geq 1$. For a subset S of $\mathbb{F}_q^n$, we define S^m to be the set $\{\mathbf{v}^m : \mathbf{v} \in S\}$. Then it is easy to verify that V^m is also a subspace of $\mathbb{F}_q^n$ whenever V is a subspace of $\mathbb{F}_q^n$ and m is a power of the characteristic of $\mathbb{F}_q$. It is easy to see that for a q -ary linear code C , the Hermitian dual $C^{\perp_H}$ is equal to the Euclidean dual $(C^\ell)^\perp$ of C^ℓ , thus C is Hermitian self-orthogonal if and only if $C \subseteq (C^\ell)^\perp$, i.e., $C^\ell \subseteq C^\perp$.

Remark 2.1: To construct Hermitian self-orthogonal generalized RS codes, a natural way is to find vectors $\mathbf{a} = (\alpha_1, \dots, \alpha_n)$ and $\mathbf{v}$ such that $\mathcal{GRS}_k(\mathbf{a}, \mathbf{v})^\ell \subseteq \mathcal{GRS}_k(\mathbf{a}, \mathbf{v})^\perp$, and hence $\mathcal{GRS}_k(\mathbf{a}, \mathbf{v})$ is Hermitian self-orthogonal. There are at least two ways to achieve this.

- (i) First we note the fact that $\mathcal{GRS}_k(\mathbf{a}, \mathbf{v})^\ell \subseteq \mathcal{GRS}_{\ell(k-1)+1}(\mathbf{a}, \mathbf{v}^\ell)$. Next if we can find a vector $\mathbf{v} \in (\mathbb{F}_q^n)$ such that $\mathbf{v}^{\ell+1}$ is a solution of the following equation

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & \dots & \vdots \\ \alpha_1^{n-2} & \alpha_2^{n-2} & \dots & \alpha_n^{n-2} \end{pmatrix} \mathbf{x}^T = \mathbf{0}, \quad (\text{II.2})$$

then $\mathcal{GRS}_{\ell(k-1)+1}(\mathbf{a}, \mathbf{v}^\ell) = \mathcal{GRS}_{n-\ell(k-1)-1}(\mathbf{a}, \mathbf{v})^\perp$. Thus, $\mathcal{GRS}_k(\mathbf{a}, \mathbf{v})^\ell \subseteq \mathcal{GRS}_k(\mathbf{a}, \mathbf{v})^\perp$ if $k \leq (n-1+\ell)/(\ell+1)$ (note that this inequality implies that $k \leq n-\ell(k-1)-1$ and hence $\mathcal{GRS}_k(\mathbf{a}, \mathbf{v}) \subseteq \mathcal{GRS}_{n-\ell(k-1)-1}(\mathbf{a}, \mathbf{v})$).

- (ii) Assume that we can find a vector $\mathbf{a}$ such that $\mathcal{GRS}_k(\mathbf{a}, \mathbf{v})^\ell = \mathcal{GRS}_k(\mathbf{a}, \mathbf{v}^\ell)$ for all vectors $\mathbf{v} \in$

$(\mathbb{F}_q^n)$. Thus, if $\mathbf{v}^{\ell+1}$ is a solution of Equation (II.2) and $k \leq n/2$, then $\mathcal{GRS}_k(\mathbf{a}, \mathbf{v})^\ell = \mathcal{GRS}_k(\mathbf{a}, \mathbf{v}^\ell) = \mathcal{GRS}_{n-k}(\mathbf{a}, \mathbf{v})^\perp \subseteq \mathcal{GRS}_k(\mathbf{a}, \mathbf{v})^\perp$.

Lemma 2.2: For $1 < n \leq q$, there exists a q -ary Hermitian self-orthogonal $[n, k]$ -generalized RS code for either of the following cases:

- (i) $k \leq (n-1)/(\ell+1)$ and n is a divisor of $q-1$;
(ii) $k \leq (n+\ell-1)/(\ell+1)$ and $n-1$ is a divisor of $q-1$.

Proof: We slightly modify the method in Remark 2.1(i) to construct our codes in (i), while this method is directly applied for the construction of codes in (ii).

(i) Choose an element $\gamma \in \mathbb{F}_q^*$ of order n and let $\mathbf{c} = \mathbf{v} = (1, \gamma, \dots, \gamma^{n-1})$. Then it is easy to see that $\mathbf{1} = (1, 1, \dots, 1)$ is a solution of (II.1) (note that we should replace both α_i and v_i in Equation (II.1) by γ^{i-1} here). Thus, we have $\mathcal{GRS}_{n-k}(\mathbf{c}, \mathbf{1}) = \mathcal{GRS}_k(\mathbf{c}, \mathbf{v})^\perp$. On the other hand, we have

$$\mathcal{GRS}_k(\mathbf{c}, \mathbf{v})^\ell \subseteq \mathcal{GRS}_{\ell(k-1)+1}(\mathbf{c}, \mathbf{v}^\ell) \subseteq \mathcal{GRS}_{\ell k+1}(\mathbf{c}, \mathbf{1}).$$

Hence, $\mathcal{GRS}_k(\mathbf{c}, \mathbf{v})^\ell \subseteq \mathcal{GRS}_{n-k}(\mathbf{c}, \mathbf{1})$ since $\ell k+1 \leq n-k$. The desired result follows.

(ii) Choose an element $\alpha \in \mathbb{F}_q^*$ of order $n-1$ and let $\mathbf{a} = (0, \alpha^0, \alpha^1, \dots, \alpha^{n-2})$. Note the fact that the norm map is surjective (see [19]), we can assume that $-(n-1) = \beta^{\ell+1}$ for some $\beta \in \mathbb{F}_q$ (this is possible since $-(n-1)$ may be regarded as an element of $\mathbb{F}_\ell$) and let $\mathbf{v} = (\beta, 1, \dots, 1)$. Then it is easy to see that $\mathbf{v}^{\ell+1}$ is a nonzero solution of Equation (II.2) (note that we should replace α_1 and α_i for $2 \leq i \leq n$ in Equation (II.2) by 0 and α^{i-1} here, respectively). Thus, by Remark 2.1(i) we obtain a q -ary self-orthogonal $[n, k]$ -generalized RS code $\mathcal{GRS}_k(\mathbf{a}, \mathbf{v})$. ■

Theorem 2.3: Let t be a divisor of $q-1$. Then for any $r \leq (q-1)/t$ and $k \leq (t-1)/(\ell+1)$, there exists a q -ary Hermitian self-orthogonal $[n, k]$ -generalized RS code for both $n = rt$ and $rt+1$.

Proof: Let $\mathcal{GRS}_k(\mathbf{c}, \mathbf{v})$ be a Hermitian self-orthogonal $[t, k]$ -generalized RS code constructed in (i) of Lemma 2.2 (replace n by t here). Now let $\beta_1, \dots, \beta_r$ belong to distinct cosets of the multiplicative quotient group $\mathbb{F}_q^*/\langle \gamma \rangle$, where γ is as in the proof of Lemma 2.2(i). Thus, it is not difficult to see that $\mathcal{GRS}_k(\mathbf{b}_i, \mathbf{v}) = \mathcal{GRS}_k(\mathbf{c}, \mathbf{v})$, where $\mathbf{b}_i = \beta_i \mathbf{c}$. Therefore, $\mathcal{GRS}_k(\mathbf{b}_i, \mathbf{v})$ is Hermitian self-orthogonal. Put $\mathbf{b} = (\mathbf{b}_1, \dots, \mathbf{b}_r)$ and $\mathbf{v}' = (\mathbf{v}, \dots, \mathbf{v})$. Then it is easy to verify that the code $\mathcal{GRS}_k(\mathbf{b}, \mathbf{v}')$ is Hermitian self-orthogonal.

Now let $\mathcal{GRS}_k(\mathbf{a}, (\beta, \mathbf{1}))$ be a Hermitian self-orthogonal $[t+1, k]$ -generalized RS code constructed in (ii) of Lemma 2.2 (replace $n-1$ by t here), where $\beta \in \mathbb{F}_q$ satisfies $\beta^{\ell+1} = -t$. Put $\mathbf{b} = (\beta_1 \mathbf{a}, \beta_2 \mathbf{c}, \dots, \beta_r \mathbf{c})$ and $\mathbf{u} = (\beta, \mathbf{1}, \mathbf{v}, \dots, \mathbf{v})$, where $\mathbf{c}$ and $\mathbf{v}$ are defined in (i) of Lemma 2.2, respectively. Then $\mathcal{GRS}_k(\mathbf{b}, \mathbf{u})$ is a q -ary self-orthogonal $[n = rt+1, k]$ -generalized RS code. ■

Now we are going to employ the second method in Remark 2.1 to construct Hermitian self-orthogonal codes.

Lemma 2.4: Let $\alpha_1, \dots, \alpha_n$ be distinct elements of $\mathbb{F}_\ell$. Then for any $\beta \in \mathbb{F}_q$, there exists a vector $\mathbf{v} \in (\mathbb{F}_q^n)$ such that for any $1 \leq k \leq n/2$, the q -ary $[n, k]$ -generalized RS code $\mathcal{GRS}_k(\mathbf{b}, \mathbf{v})$ is Hermitian self-orthogonal, where $\mathbf{b} = (\beta + \alpha_1, \dots, \beta + \alpha_n)$.

Proof: Let $\mathbf{u} = (u_1, \dots, u_n)$ be a non-trivial solution of (II.2). Note that all the coordinates of $\mathbf{u}$ are not zero. Since all α_i are elements of $\mathbb{F}_\ell$, the solution $\mathbf{u}$ is also a vector of $(\mathbb{F}_\ell^*)^n$. As every element of $\mathbb{F}_\ell$ is an $(\ell + 1)$ -th power in $\mathbb{F}_q$, there exists a vector $\mathbf{v} = (v_1, \dots, v_n) \in (\mathbb{F}_q^*)^n$ such that $\mathbf{v}^{\ell+1} = \mathbf{u}$. Hence, by Remark 2.1(ii) the code $\mathcal{GRS}_k(\mathbf{a}, \mathbf{v})$ is Hermitian self-orthogonal, where $\mathbf{a} = (\alpha_1, \dots, \alpha_n)$.

For a polynomial $g(x) \in \mathbb{F}_q[x]$, we let $g_\beta(x) = g(\beta + x)$. Then it is easy to see that $g_\beta(x)$ runs through all polynomials in $\mathbb{F}_q[x]$ with degree less than k whenever $g(x)$ does so. Thus,

$$\begin{aligned} \mathcal{GRS}_k(\mathbf{b}, \mathbf{v}) &= \{(v_1 g(\beta + \alpha_1), \dots, v_n g(\beta + \alpha_n)) : g(x) \in \mathbb{F}_q[x], \deg(g) < k\} \\ &= \{(v_1 g_\beta(\alpha_1), \dots, v_n g_\beta(\alpha_n)) : g_\beta(x) \in \mathbb{F}_q[x], \deg(g_\beta) < k\} \\ &= \mathcal{GRS}_k(\mathbf{a}, \mathbf{v}). \end{aligned}$$

Hence, $\mathcal{GRS}_k(\mathbf{b}, \mathbf{v})$ is also Hermitian self-orthogonal. ■

Theorem 2.5: For any $2 \leq n \leq q$, we write $n = n_1 + \dots + n_t$ with $1 \leq t \leq \ell$ and $2 \leq n_i \leq \ell$ for all i . Let $1 \leq k \leq \min\{n_1, \dots, n_t\}/2$. Then there exists a q -ary Hermitian self-orthogonal $[n, k]$ -generalized RS code.

Proof: Consider the additive quotient group $\mathbb{F}_q/\mathbb{F}_\ell$. Let $\beta_1, \dots, \beta_t$ belong to distinct cosets in this quotient group. For each $1 \leq i \leq t$, we choose a set of n_i distinct elements $\{\alpha_{i1}, \dots, \alpha_{in_i}\}$ of $\mathbb{F}_\ell$. By Lemma 2.4, there exists a vector $\mathbf{v}_i$ of $\mathbb{F}_q^{n_i}$ such that $\mathcal{GRS}_k(\mathbf{b}_i, \mathbf{v}_i)$ is Hermitian self-orthogonal, where $\mathbf{b}_i = (\beta_i + \alpha_{i1}, \dots, \beta_i + \alpha_{in_i})$. Put $\mathbf{b} = (\mathbf{b}_1, \dots, \mathbf{b}_t)$ and $\mathbf{v} = (\mathbf{v}_1, \dots, \mathbf{v}_t)$, then it is easy to verify that $\mathcal{GRS}_k(\mathbf{b}, \mathbf{v})$ is a q -ary Hermitian self-orthogonal $[n, k]$ -generalized RS code. ■

The length of the q -ary Hermitian self-orthogonal codes that we constructed above through generalized RS codes is at most q . We now consider q -ary Hermitian self-orthogonal codes of length $q + 1$. In order to do so, we have to include a “point at infinity”.

To achieve this, it is more convenient to describe our code construction by using the language of algebraic geometry codes. The reader may refer to [26] for some basic notions and results of algebraic geometry codes.

For $2 \leq k \leq \lfloor (\ell + 1)/2 \rfloor$, consider the divisor $Q - R$, where Q and R correspond to two irreducible polynomials of $\mathbb{F}_\ell[x]$ of degree $2 + k$ and 3 , respectively. Let $\mathcal{L}_\ell(Q - R)$ be the Riemann-Roch space in $\mathbb{F}_\ell(x)$.

Consider the algebraic geometry code C_1 defined by

$$C_1 := \{(f(P_1), \dots, f(P_{\ell+1})) : f \in \mathcal{L}_\ell(2Q - 2R)\},$$

where $P_1, \dots, P_{\ell+1}$ stand for all $\ell + 1$ points of the projective line $\mathbb{P}^1(\mathbb{F}_\ell)$. Then C_1 is an ℓ -ary $[\ell + 1, 2k - 1]$ -MDS code.

Let S be a prime divisor corresponding to an irreducible polynomial in $\mathbb{F}_\ell[x]$ of degree $\ell - 1 - (2k - 2)$ and define C_2 to be the code

$$C_2 := \{(f(P_1), \dots, f(P_{\ell+1})) : f \in \mathcal{L}_\ell(S + 2Q - 2R)\}.$$

Then C_2 is an ℓ -ary $[\ell + 1, \ell]$ -MDS code which contains C_1 .

Let G be a generator matrix of C_2 . Let $\mathbf{u} \in \mathbb{F}_\ell^{\ell+1}$ be a nonzero solution of $G\mathbf{x}^T = \mathbf{0}$, i.e., $\mathbf{u}$ belongs to the Euclidean dual of C_2 . It is clear that $\mathbf{u}$ belongs to the Euclidean dual of C_1 as well since $C_1 \subseteq C_2$. As C_2 is an MDS code, every set of ℓ columns of G is linearly independent (see [18, Theorem 5.4.5]). This implies that every coordinate of $\mathbf{u}$ is not zero. Let $\mathbf{v} = (v_1, \dots, v_{\ell+1}) \in (\mathbb{F}_q^*)^{\ell+1}$ such that $\mathbf{v}^{\ell+1} = \mathbf{u}$. This

is possible since every coordinate of $\mathbf{u}$ is a nonzero element of $\mathbb{F}_\ell$.

Now we consider the code

$$C_3 := \{(v_1 f(P_1), \dots, v_{\ell+1} f(P_{\ell+1})) : f \in \mathcal{L}_{\mathbb{F}_q}(Q - R)\},$$

where $\mathcal{L}_{\mathbb{F}_q}(Q - R)$ stands for the Riemann-Roch space in $\mathbb{F}_q(x)$. It is clear that C_3 is a q -ary $[\ell + 1, k]$ -MDS code.

We claim that C_3 is Hermitian self-orthogonal. Let $\{f_1, \dots, f_k\}$ be an $\mathbb{F}_\ell$ -basis of $\mathcal{L}_{\mathbb{F}_\ell}(Q - R)$, then it also forms an $\mathbb{F}_q$ -basis of $\mathcal{L}_{\mathbb{F}_q}(Q - R)$ (see [23, Proposition 5.8 of Chapter 2]). To show that C_3 is Hermitian self-orthogonal, it is sufficient to show that

$$\sum_{i=1}^{\ell+1} v_i f(P_i) (v_i g(P_i))^\ell = 0, \quad (\text{II.3})$$

for any two functions $f, g \in \{f_1, \dots, f_k\}$. In fact, we have

$$\sum_{i=1}^{\ell+1} v_i f(P_i) (v_i g(P_i))^\ell = \sum_{i=1}^{\ell+1} u_i (fg)(P_i) = 0, \quad (\text{II.4})$$

using the facts that (i) $\mathbf{u} = \mathbf{v}^{\ell+1}$; (ii) $g(P_i) \in \mathbb{F}_\ell$; (iii) fg belongs to $\mathcal{L}_{\mathbb{F}_\ell}(2Q - 2R)$ and $\mathbf{u}$ is orthogonal to C_1 .

Theorem 2.6: For any $2 \leq k \leq \ell/2$, there exists a q -ary Hermitian self-orthogonal $[q + 1, k]$ -MDS code.

Proof: We consider the code the q -ary code C defined by

$$C := \{(v_1 f(P_1), \dots, v_{q+1} f(P_{q+1})) : f \in \mathcal{L}_{\mathbb{F}_q}(Q - R)\}$$

for some nonzero elements $v_i \in \mathbb{F}_q$, where $\{P_1, \dots, P_{q+1}\} = \mathbb{P}^1(\mathbb{F}_q)$, and Q and R correspond to two irreducible polynomials $a(x)$ and $b(x)$ of $\mathbb{F}_\ell[x]$ of degree $k + 2$ and 3 , respectively. Then C is a q -ary $[q + 1, k]$ -MDS code.

We partition the $q + 1$ points of $\mathbb{P}^1(\mathbb{F}_q)$ into the $\ell + 1$ points of $\mathbb{P}^1(\mathbb{F}_\ell)$ together with $\ell - 1$ cosets of the type $\beta + \mathbb{F}_\ell$. By the analysis above Theorem 2.6, there exist nonzero elements $v_1, \dots, v_{\ell+1}$ of $\mathbb{F}_q$ such that $\sum_{i=1}^{\ell+1} v_i f(P_i) (v_i g(P_i))^\ell = 0$ for any $f, g \in \mathcal{L}_{\mathbb{F}_q}(Q - R)$. Now it is sufficient to show that for any $\beta \in \mathbb{F}_q$, there exists $\mathbf{c} = (c_1, \dots, c_\ell) \in (\mathbb{F}_q^*)^\ell$ such that

$$C_\beta := \{(c_1 f(\beta + \alpha_1), \dots, c_\ell f(\beta + \alpha_\ell)) : f \in \mathcal{L}_{\mathbb{F}_q}(Q - R)\}$$

is Hermitian self-orthogonal, where $\{\alpha_1, \dots, \alpha_\ell\} = \mathbb{F}_\ell$.

Note that $\{\frac{b(x)}{a(x)} \times 1, \frac{b(x)}{a(x)} \times x, \dots, \frac{b(x)}{a(x)} \times x^{k-1}\}$ forms an $\mathbb{F}_q$ -basis of $\mathcal{L}_{\mathbb{F}_q}(Q - R)$.

By Lemma 2.4, there exists a vector $\mathbf{e} = (e_1, \dots, e_\ell) \in (\mathbb{F}_q^*)^\ell$ such that $\mathcal{GRS}_k(\mathbf{b}, \mathbf{e})$ with $\mathbf{b} = (\beta + \alpha_1, \dots, \beta + \alpha_\ell)$ is Hermitian self-orthogonal. Let $c_i = e_i a(\beta + \alpha_i) / b(\beta + \alpha_i)$ for $i = 1, \dots, \ell$. Then it is clear that the generalized RS code $\mathcal{GRS}_k(\mathbf{b}, \mathbf{e})$ is identical to C_β . This finishes the proof. ■

III. QUANTUM MDS CODES

The main idea of this section is based on the Hermitian self-orthogonal MDS codes constructed in the previous section and a result by Ashikhmin and Knill which is stated below.

Lemma 3.1: (see [2]) There is an ℓ -ary $[[n, n - 2k, d^\perp]]$ -quantum code whenever there exists a q -ary classical Hermitian self-orthogonal $[n, k]$ -linear code with dual distance $d^\perp$.

Thus, if we apply the above result to Hermitian self-orthogonal MDS codes, we can immediately obtain the following corollary.

Corollary 3.2: There is an ℓ -ary $[[n, n-2k, k+1]]$ -quantum MDS code whenever there exists a q -ary classical Hermitian self-orthogonal $[n, k]$ -MDS code.

A. General results

We first consider ℓ -ary quantum MDS codes of length equal to $\ell^2 + 1$, ℓ^2 and $\ell^2 - 1$, respectively.

Theorem 3.3: (i) For any $2 \leq k \leq \ell/2$, there exists an ℓ -ary $[[\ell^2 + 1, \ell^2 + 1 - 2k, k + 1]]$ -quantum MDS code.

(ii) For any $2 \leq k \leq \ell - 2$, there exists an ℓ -ary $[[\ell^2, \ell^2 - 2k, k + 1]]$ -quantum MDS code.

(iii) For any $2 \leq k \leq \ell - 2$, there exists an ℓ -ary $[[\ell^2 - 1, \ell^2 - 1 - 2k, k + 1]]$ -quantum MDS code.

Proof: Combining Theorem 2.6 with Corollary 3.2 gives the desired result in (i).

Combining Theorem 2.3 with Corollary 3.2 gives the desired results in (ii) and (iii). ■

Next we consider ℓ -ary quantum MDS codes of arbitrary length.

Theorem 3.4: Let n be an integer between 4 and ℓ^2 . Write $n = m\ell - r$ with $1 \leq m \leq \ell$ and $0 \leq r \leq \ell - 1$. Then for any $2 \leq k \leq (\ell - 1 - \lfloor r/m \rfloor)/2$, there exists an ℓ -ary $[[n, n - 2k, k + 1]]$ -quantum MDS code.

Proof: Note that n can be written into

$$n = \left(m + m \left\lfloor \frac{r}{m} \right\rfloor - r\right) \left(\ell - \left\lfloor \frac{r}{m} \right\rfloor\right) + \left(r - m \left\lfloor \frac{r}{m} \right\rfloor\right) \left(\ell - 1 - \left\lfloor \frac{r}{m} \right\rfloor\right).$$

Thus, n can be written as a sum $n_1 + \dots + n_m$, where the first $m + m \lfloor r/m \rfloor - r$ lengths n_i are equal to $\ell - \lfloor r/m \rfloor$ and the remaining lengths n_i are equal to $\ell - 1 - \lfloor r/m \rfloor$. Applying Theorem 2.5 and Corollary 3.2 gives the desired result. ■

B. Quantum MDS codes with smaller distance

In this subsection, we fix the minimum distance d of a quantum code and show that there always exists an ℓ -ary quantum MDS code if $\ell \geq 4d - 5$.

Theorem 3.5: Let $k \geq 1$ be an integer. Then for any prime power $\ell \geq 4k - 1$ and $2k \leq n \leq \ell^2$, there exists an ℓ -ary $[[n, n - 2k, k + 1]]$ -quantum MDS code.

Proof: By Corollary 3.2, it is sufficient to show the existence of a q -ary Hermitian self-orthogonal $[n, k]$ -generalized RS code, where $q = \ell^2$.

Write n into $a\ell + b$ with $0 \leq a \leq \ell - 1$ and $1 \leq b \leq \ell$. If $b \geq 2k$, then n can be written as $n = n_1 + \dots + n_{a+1}$, where the first a lengths n_i are equal to ℓ and the last length n_{a+1} is b . Since $k \leq \min\{\ell, b\}/2$, by Theorem 2.5 there exists a q -ary Hermitian self-orthogonal $[n, k]$ -generalized RS code.

Now we assume that $1 \leq b \leq 2k - 1$. Then we must have $a \geq 1$. Thus, $n = (a - 1)\ell + 2k + (\ell - 2k + b)$. Note that $2k \leq \ell - 2k + b \leq \ell - 1$. Thus, n can be written as $n = n_1 + \dots + n_{a+1}$, where the first $a - 1$ lengths n_i are equal to ℓ , the length n_a is $2k$ and the last length n_{a+1} is $\ell - 2k + b$.

Since $k = \min\{\ell, 2k, \ell - 2k + b\}/2$, by Theorem 2.5 there exists a q -ary Hermitian self-orthogonal $[n, k]$ -generalized RS code. ■

We now look at quantum MDS codes with minimum distance equal to 3.

Corollary 3.6: For all ℓ and $4 \leq n \leq \ell^2 + 1$, there exist ℓ -ary $[[n, n - 4, 3]]$ -quantum MDS codes except for the case where $\ell = 2$ and $n = 4$.

Proof: By Theorem 3.5, there exist ℓ -ary $[[n, n - 4, 3]]$ -quantum MDS code for all $\ell \geq 7$ and $4 \leq n \leq \ell^2$. For $n = \ell^2 + 1$ and $\ell \geq 4$, the desired result follows from Theorem 3.3. By [17], we can show this is also true for $\ell = 3, 5$. The desired result for $(\ell, n) = (2, 5), (4, 15), (4, 16)$ can be derived from Theorem 3.3. From [16], we know the existence of ℓ -ary $[[n, n - 4, 3]]$ -quantum MDS codes for $(\ell, n) = (4, 8), (4, 11), (4, 12)$. Now the only remaining cases are $\ell = 4$ and $n = 4, 5, 6, 7, 9, 10, 13, 14$. In the appendix, we explicitly construct generator matrices of classical Hermitian self-orthogonal codes to produce the quantum codes for these missing cases. ■

Remark 3.7: Except for a few exceptional cases, the length of an ℓ -ary quantum MDS stabilizer code cannot exceed $\ell^2 + 1$ provided that the classical MDS conjecture holds. To our best knowledge, the parameters of all known non-trivial quantum $[[n, n - 2d + 2, d]]$ -MDS codes are given below.

- (i) $n = \ell^2 + 1$ and $d = \ell + 1$ (see [16]);
- (ii) $n = \ell^2 - r, d \leq \ell - r$ for $0 \leq r \leq \ell - 2$ (see [16]);
- (iii) $n = m\ell - r, d \leq m - r + 1$, for $0 \leq r < m, 1 < m < \ell$ (see [16]);
- (iv) $n \leq \ell$ and $d \leq \lfloor n/2 \rfloor + 1$ (see [10] and [16]);
- (v) $4 \leq n \leq \ell^2 + 1$ and $d = 3$ for odd prime power ℓ (see [17]).

Besides, there are several other constructions of quantum MDS codes ([4], [8], [10], [11] and [21]) which produce quantum MDS codes with parameters covered in the above list.

To conclude, we compare part of our results with the above list.

- (I) For length $\ell^2 + 1$, we obtain an ℓ -ary $[[\ell^2 + 1, \ell^2 + 1 - 2k, k + 1]]$ -quantum MDS code for any $2 \leq k \leq \ell/2$ in Theorem 3.3. This class is not covered in the above list.
- (II) For $d = 3$, in Corollary 3.6 we constructed an ℓ -ary $[[n, n - 4, 3]]$ -quantum MDS code for any $4 \leq n \leq \ell^2 + 1$ except for the case where $\ell = 2$ and $n = 4$. For even ℓ , this class is not covered in the above list.
- (III) For sufficiently large ℓ , the total number of distinct pairs (n, k) for which quantum MDS codes constructed in Theorem 3.4 have parameters $[[n, n - 2k]]$ is $\ell^3/2 - (\ell^2/2) \log q + \mathcal{O}(\ell^2)$, while the total number of distinct pairs (n, k) in the above list is $\ell^3/6 + \mathcal{O}(\ell^2)$. This means that we have constructed roughly three times as many quantum codes as all the previously known ones.

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. Ashikhmin and S. Litsyn, "Upper bounds on the size of quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1206–1215, May 1999.

- [4] J. Bierbrauer and Y. Edel, "Quantum twisted codes," *J. Comb. Designs*, vol. 8, pp. 174–188, 2000.
- [5] 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, July 1998.
- [6] H. F. Chau, "Five quantum register error correction code for higher spin systems," *Phys. Rev. A*, 56, R1, 1997.
- [7] 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.
- [8] K. Feng, "Quantum code $[[6, 2, 3]]_p$ and $[[7, 3, 3]]_p$ ($p \geq 3$) exists," *IEEE Trans. Inf. Theory*, vol. 48, no. 8, pp. 2384–2391, Aug. 2002.
- [9] M. Grassl and T. Beth, "Quantum BCH codes," see: <http://arxiv.org/abs/quant-ph/9910060>
- [10] M. Grassl, T. Beth and M. Röttler, "On optimal quantum codes," *Int. J. Quantum Inf.*, vol. 2, no. 1, pp. 757–775, 2004.
- [11] D. Hu, W. Tang, M. Zhao, Q. Chen, S. Yu and C. H. Oh, "Graphical nonbinary quantum error-correcting codes," *Phys. Rev. A*, vol. 78, no. 1, 012306, Jul. 2008.
- [12] A. Ketkar, A. Klappenecker, S. Kumar and P. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE. Trans. Inform. Theory*, vol. 52, no. 11, pp.4892–4914, Nov. 2006.
- [13] E. Knill and R. Laflamme, "A theory of quantum error-correcting codes," *Phys. Rev. A*, vol. 55, no. 2, pp. 900–911, 1997.
- [14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977
- [15] Z. Li, L. J. Xing and X. M. Wang, "A family of asymptotically good quantum codes based on code concatenation," *IEEE. Trans. Inform. Theory*, vol. 55, no. 8, pp.3821–3824, Aug. 2009.
- [16] Z. Li, L. J. Xing and X. M. Wang, "Quantum generalized Reed-Solomon codes: unified framework for quantum MDS codes," preprint, see arxiv: 0812.4514
- [17] R. Li and Z. Xu, "On $[[n, n - 4, 3]]_q$ quantum MDS codes for odd prime power q ," in press, see arxiv:0906.2509v1
- [18] S. Ling and C. P. Xing, *Coding Theory – A First Course*, Cambridge University Press, 2004.
- [19] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, 1997.
- [20] E.M. Rains, "Nonbinary quantum codes," *IEEE. Trans. Inform. Theory*, vol. 45, no. 6, pp.1827–1832, Sept. 1999.
- [21] P.K. Sarvepalli and A. Klappenecker, "Nonbinary quantum Reed-Muller codes," *Proc. Inter. Sym. Inf. Theory 2005*, Adelaide, Australia, pp. 1023–1027.
- [22] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, no. 4, pp. R2493–R2496, 1995.
- [23] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.
- [24] A. M. Steane, "Multiple particle interference and quantum error correction," *Proc. Roy. Soc. Lond. A*, vol. 452, pp. 2551–2577, 1996.
- [25] A. M. Steane, "Enlargement of Calderbank-Shor-Steane quantum codes," *IEEE. Trans. Inform. Theory*, vol. 45, no. 7, pp. 2492–2495, Nov. 1999.
- [26] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer Verlag, 1993.

APPENDIX

Let α be a primitive element of $\mathbb{F}_{16}$ satisfying $\alpha^4 + \alpha + 1 = 0$. Define

$$\begin{aligned}
 G_4 &= \begin{pmatrix} 1 & 1 & \alpha^{10} & 1 \\ 1 & \alpha^5 & \alpha^{10} & 0 \end{pmatrix}, & G_5 &= \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & \alpha & \alpha & \alpha^2 & \alpha^5 \end{pmatrix}, \\
 G_6 &= \begin{pmatrix} 1 & 1 & \alpha^{10} & 1 & \alpha^6 & \alpha^{11} \\ 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^6 & \alpha^{11} \end{pmatrix}, \\
 G_7 &= \begin{pmatrix} 1 & 1 & \alpha^{11} & \alpha^5 & \alpha^5 & \alpha^5 & \alpha^{10} \\ \alpha & \alpha^6 & \alpha^{11} & 1 & \alpha^5 & \alpha^{10} & 0 \end{pmatrix}, \\
 G_9 &= \begin{pmatrix} 1 & 1 & \alpha^{13} & \alpha^3 & 0 & 1 & 1 & 1 & \alpha^2 & \alpha^{10} \\ \alpha^3 & \alpha^8 & \alpha^{13} & 0 & \alpha & 1 & \alpha & \alpha^2 & \alpha^{10} & \end{pmatrix}, \\
 G_{10} &= \begin{pmatrix} 1 & 1 & \alpha^{10} & 1 & \alpha^6 & \alpha^{11} & \alpha^2 & \alpha^7 & \alpha^{12} & 1 \\ 1 & \alpha^5 & \alpha^{10} & \alpha & \alpha^6 & \alpha^{11} & \alpha^2 & \alpha^7 & \alpha^{12} & 0 \end{pmatrix}, \\
 G_{13} &= \begin{pmatrix} 1 & 1 & \alpha^{11} & \alpha^2 & \alpha^7 & \alpha^{12} & \alpha^3 \\ \alpha & \alpha^6 & \alpha^{11} & \alpha^2 & \alpha^7 & \alpha^{12} & \alpha^3 \\ & & & 1 & 1 & \alpha^5 & \alpha^5 & \alpha^5 & \alpha^{10} \end{pmatrix}, \\
 G_{14} &= \begin{pmatrix} 1 & 1 & \alpha^{13} & \alpha & 0 & \alpha^2 & \alpha^{10} & 1 & \alpha^6 & \alpha^7 \\ \alpha^3 & \alpha^8 & \alpha^{13} & 0 & \alpha^2 & \alpha^{10} & 1 & \alpha^6 & \alpha^7 & \\ & & & 1 & 1 & \alpha^{12} & \alpha^2 & \alpha^2 & \alpha^2 & \end{pmatrix}.
 \end{aligned}$$

Let C_n be the $\mathbb{F}_{16}$ -linear code with generator matrix G_n defined above, for $n = 4, 5, 6, 7, 9, 10, 13, 14$. Then it is straightforward to verify that each of these C_n is a 16-ary Hermitian self-orthogonal MDS code. This implies the existence of 4-ary $[[n, n - 4, 3]]$ -quantum MDS codes, for $n = 4, 5, 6, 7, 9, 10, 13, 14$, by Corollary 3.2.

AUTHORS' BIOGRAPHIES

Lingfei Jin received the B.A. degree in mathematics from the Hefei University of Technology, China, in 2009. She is currently a Project Officer with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. Her research interests include coding theory and cryptography.

San Ling received the B.A. degree in mathematics from the University of Cambridge, Cambridge, U.K., in 1985 and the Ph.D. degree in mathematics from the University of California, Berkeley, in 1990.

Since April 2005, he has been a Professor with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. Prior to that, he was with the Department of Mathematics, National University of Singapore. His research fields include arithmetic of modular curves and application of number theory to combinatorial designs, coding theory, cryptography and sequences.

Jinquan Luo was born in February 1980. He got his bachelor degree from Zhejiang University, China in July 2001 and Ph.D in January 2007 from Tsinghua University, China. He is now a lecturer in Yangzhou University, China. From February 2009 to February 2010, he was a research fellow at Nanyang Technological University, Singapore. His major research interests are coding theory, cryptology and number theory.

Chaoping Xing received his PhD degree in 1990 from University of Science and Technology of China. From 1990 to 1993 he was a lecturer and associate professor in the same university. He joined University of Essen, Germany as an Alexander von Humboldt fellow from 1993 to 1995. After this he spent most time in Institute of Information Processing, Austrian Academy of Sciences until 1998. From March of 1998 to November of 2007, he was working in National University of Singapore. Since December of 2007, he has been with Nanyang Technological University and currently is a full Professor. Dr. Xing has been working on the areas of algebraic curves over finite fields, coding theory, cryptography and quasi-Monte Carlo methods, etc.