Generalization of Steane’ s enlargement construction of quantum codes and applications

Ling, San; Luo, Jinquan; Xing, Chaoping

2010

Ling, S., Luo, J., & Xing, C. (2010). Generalization of Steane’ s enlargement construction of quantum codes and applications. IEEE Transactions on Information Theory, 56(8), 4080-4084.

https://hdl.handle.net/10356/94258

https://doi.org/10.1109/TIT.2010.2050828

Generalization of Steane's Enlargement Construction of Quantum Codes and Applications

San Ling, Jinquan Luo and Chaoping Xing

Abstract— **We generalize Steane's enlargement construction of binary quantum codes to q-ary quantum codes. We then apply this result to BCH codes and the study of asymptotic bounds, and obtain improvements to the quantum BCH codes constructed by Aly and Klappenecker and the quantum asymptotic bounds from algebraic geometry codes obtained by Feng, Ling and Xing.**

Index Terms— **Enlargement, Self-orthogonal, BCH codes, Algebraic geometry codes, Asymptotic bounds**

I. INTRODUCTION

After the work of Calderbank, Rains, Shor and Sloane [5], much work on the constructions of quantum codes from classical block codes has been done. One of the main ideas for these constructions is to construct self-orthogonal classical codes with good parameters (see Section 2 below). In [9], Steane succeeded in extending this idea by enlarging classical block codes to obtain quantum codes with better parameters. However, Steane's original paper only considered binary quantum codes. As q-ary quantum codes have been studied quite extensively for some years, it is natural to ask if we can generalize Steane's enlargement construction to q-ary quantum codes.

The main result of this paper is to obtain a q-ary analogue of Steane's enlargement construction. Once this enlargement construction is generalized, we can naturally apply it to various scenarios to improve upon known results. We focus on only two such applications in this paper, namely, we apply the q-ary analogue of Steane's enlargement construction to BCH codes and asymptotic problems. In particular, we improve the following two results: (i) the quantum BCH codes constructed in [1]; (ii) the quantum asymptotic bounds from algebraic geometry codes given in [7].

The paper is organized as follows. In Section 2, we present the original enlargement construction of Steane and generalize it to a q-ary analogue. This q-ary result is applied to BCH codes in Section 3. Finally, we improve the asymptotic bounds obtained from algebraic geometry codes in Section 4.

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 637616, 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 all the three authors is partially supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03. The work of J. Q. Luo is also partially supported by the NSFC under Grant 60903036 and the NSF of Jiangsu Province under Grant BK2009182.

C. P. Xing is the corresponding author.

II. ENLARGEMENT CONSTRUCTION

Before stating our results, we introduce some definitions and notations.

Let q be a prime power and let $\mathbb{F}_q$ be the finite field of cardinality q. For $\mathbf{u} \in \mathbb{F}_q^n$, denote by $\mathrm{wt}_H(\mathbf{u})$ the *Hamming weight* of $\mathbf{u}$. Now for $(\mathbf{u}|\mathbf{v}) \in \mathbb{F}_q^{2n}$ with $\mathbf{u} = (u_1, \cdots, u_n), \mathbf{v} = (v_1, \cdots, v_n) \in \mathbb{F}_q^n$, define the *symplectic weight* by

$$\mathrm{wt}_s(\mathbf{u}|\mathbf{v}) := \#\{i : \ u_i \neq 0 \text{ or } v_i \neq 0\}.$$

For two vectors $(\mathbf{u}|\mathbf{v}), (\mathbf{u}'|\mathbf{v}') \in \mathbb{F}_q^{2n}$, define the *symplectic inner product* by

$$((\mathbf{u}|\mathbf{v}), (\mathbf{u}'|\mathbf{v}'))_s = \mathbf{u} \cdot \mathbf{v}' - \mathbf{u}' \cdot \mathbf{v} \in \mathbb{F}_q,$$

where $\cdot$ stands for the usual Euclidean inner product.

For a q-ary classical linear block code $\mathcal{C} \subseteq \mathbb{F}_q^{2n}$, the *symplectic dual code* of $\mathcal{C}$ is defined as

$$\mathcal{C}^{\perp_s} = \{\mathbf{a} \in \mathbb{F}_q^{2n} | \ (\mathbf{a}, \mathbf{b})_s = 0 \text{ for all } \mathbf{b} \in \mathcal{C}\}.$$

It is easy to verify that $\mathcal{C} = (\mathcal{C}^{\perp_s})^{\perp_s}$.

A code $\mathcal{C} \subseteq \mathbb{F}_q^{2n}$ is said *self-orthogonal* with respect to the symplectic inner product if $\mathcal{C} \subseteq \mathcal{C}^{\perp_s}$.

The following construction of quantum codes from classical block codes was presented by Ashikhmin and Knill in [2].

Proposition 2.1: If $\mathcal{C}$ is a q-ary self-orthogonal $[2n, k]$ code with respect to the symplectic inner product, then there exists a q-ary $[[n, n-k, d]]$ quantum code with

$$d = \mathrm{wt}_s(\mathcal{C}^{\perp_s} \setminus \mathcal{C}) = \min\{\mathrm{wt}_s(\mathbf{v}) | \ \mathbf{v} \in \mathcal{C}^{\perp_s} \setminus \mathcal{C}\}.$$

In particular, if C is a q-ary classical $[n, k, d]$-linear code which contains its Euclidean dual $C^{\perp}$, then it is easy to see that the code

$$\mathcal{C} := \{(\mathbf{u}|\mathbf{v}) : \ \mathbf{u}, \mathbf{v} \in C^{\perp}\}$$

is self-orthogonal with respect to the symplectic inner product. It is clear that the dimension of $\mathcal{C}$ is $2n - 2k$. Thus, by Proposition 2.1, we obtain a q-ary $[[n, 2k-n, d]]$-quantum code.

The idea of Steane's enlargement is to find a q-ary linear code A that contains B so that the dimension of the resulting quantum code is increased, while its distance remains unchanged. Steane worked out the enlargement construction only for the binary case [9], which is stated below.

Proposition 2.2: (see [9]) Given a classical binary error-correcting code C_1, of parameters $[n, k_1, d_1]$, which contains its Euclidean dual, and which can be enlarged to an $[n, k_2 > k_1 + 1, d_2]$-code C_2 (i.e., $C_1 \subseteq C_2$), a pure binary quantum code of parameters $[[n, k_1 + k_2 - n, \min(d_1, \lceil 3d_2/2 \rceil)]]$ can be constructed.

Before generalizing Steane's enlargement construction to the q-ary case, we need several lemmas.

Lemma 2.3: Let C_1 and C_2 be two q-ary linear codes satisfying $C_1^{\perp} \subseteq C_1 \subsetneqq C_2$. Let G_1, $\binom{D}{G_1}$, H_2 and $\binom{B}{H_2}$ be generator matrices of C_1, C_2, $C_2^{\perp}$ and $C_1^{\perp}$, respectively. Then BD^T is invertible, where T stands for transpose.

Proof: Note that both the sizes of B and D are $k \times n$, where k is the difference between the dimensions of C_2 and C_1, and n is the length of the codes. Thus, BD^T is a square matrix of size k. The desired result is equivalent to the fact that the equation $BD^T\mathbf{x}^T = \mathbf{0}$ has only the trivial solution. Suppose that this was false. Then there exists a nonzero vector $\mathbf{c} \in \mathbb{F}_q^k$ such that $BD^T\mathbf{c}^T = \mathbf{0}$. Thus, $\mathbf{c}D$ is a nonzero codeword of C_2, but not a codeword of C_1. This implies that $H_2(D^T\mathbf{c}^T) = \mathbf{0}$ and $\binom{B}{H_2}(D^T\mathbf{c}^T) \neq \mathbf{0}$. Hence, $BD^T\mathbf{c}^T \neq \mathbf{0}$, a contradiction. ■

Lemma 2.4: Let $\mathbf{u}, \mathbf{v}$ be two vectors in $\mathbb{F}_q^n$, then we have

$$q \cdot \mathrm{wt}_s(\mathbf{u}|\mathbf{v}) = \mathrm{wt}_H(\mathbf{u}) + \mathrm{wt}_H(\mathbf{v}) + \sum_{\alpha \in \mathbb{F}_q^*} \mathrm{wt}_H(\mathbf{u} + \alpha\mathbf{v}).$$

Proof: Let $\mathbf{u} = (u_1, \dots, u_n)$ and $\mathbf{v} = (v_1, \dots, v_n)$. It is sufficient to show that, for any $1 \le i \le n$, one has

$$q \cdot \mathrm{wt}_s(u_i|v_i) = \mathrm{wt}_H(u_i) + \mathrm{wt}_H(v_i) + \sum_{\alpha \in \mathbb{F}_q^*} \mathrm{wt}_H(u_i + \alpha v_i). \tag{II.1}$$

We prove the above identity by considering the four cases.

(i) $u_i = v_i = 0$.
In this case, both sides of (II.1) are equal to 0.

(ii) $u_i = 0$ and $v_i \neq 0$.
The left hand side of (II.1) is clearly equal to q. The right hand side of (II.1) is $\mathrm{wt}_H(v_i) + \sum_{\alpha \in \mathbb{F}_q^*} \mathrm{wt}_H(\alpha v_i)$ which is also equal to q.

(iii) $u_i \neq 0$ and $v_i = 0$.
The left hand side of (II.1) is clearly equal to q. The right hand side of (II.1) is $\mathrm{wt}_H(u_i) + \sum_{\alpha \in \mathbb{F}_q^*} \mathrm{wt}_H(u_i)$ which is also equal to q.

(iv) $u_i \neq 0$ and $v_i \neq 0$.
The left hand side of (II.1) is clearly equal to q. The right hand side of (II.1) is $2 + \sum_{\alpha \in \mathbb{F}_q^*} \mathrm{wt}_H(u_i + \alpha v_i)$. By the fact that $u_i + \alpha v_i = 0$ if and only if $\alpha = -u_i/v_i$, i.e., $\mathrm{wt}_H(u_i + \alpha v_i) = 1$ if and only if $\alpha \in \mathbb{F}^* \setminus \{-u_i/v_i\}$, we get $\sum_{\alpha \in \mathbb{F}_q^*} \mathrm{wt}_H(u_i + \alpha v_i) = q - 2$. The identity (II.1) is also proved in this case.

This finishes the proof. ■

Lemma 2.5: For any monic polynomial $f(x)$ of degree n over $\mathbb{F}_q$, there exists a square matrix A of size n such that the characteristic polynomial of A is equal to $f(x)$.

Proof: Let $f(x) = x_n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$ be any monic polynomial over $\mathbb{F}_q$. Then the characteristic polynomial of the $n \times n$ square matrix

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \cdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-2} & -a_{n-1} \end{pmatrix}$$

is exactly $f(x)$. ■

Now we state the main result of this paper.

Theorem 2.6: Let q be a prime power and let C_1 be a q-ary $[n, k_1, d_1]$-linear code which contains its Euclidean dual $C_1^{\perp}$. Suppose C_1 can be enlarged to an $[n, k_2, d_2]$-code C_2 with $k_2 > k_1 + 1$, i.e., $C_1 \subseteq C_2$. Then a pure q-ary quantum code of parameters $\left[\left[n, k_1 + k_2 - n, \min\left\{d_1, \lceil (1 + \frac{1}{q})d_2 \rceil\right\}\right]\right]$ can be constructed.

Proof: Let G_1, $\binom{D}{G_1}$, H_2 and $\binom{B}{H_2}$ be generator matrices of C_1, C_2, $C_2^{\perp}$ and $C_1^{\perp}$, respectively. Let $\mathcal{C}$ be the q-ary $[2n, k_1 + k_2]$-linear code with generator matrix

$$\begin{pmatrix} D & AD \\ G_1 & 0 \\ 0 & G_1 \end{pmatrix},$$

where A is a $(k_2 - k_1) \times (k_2 - k_1)$ non-singular matrix with no eigenvalues in $\mathbb{F}_q$ (Lemma 2.5 guarantees the existence of such a matrix). By Lemma 2.3, the matrix BD^T is invertible. Thus, we can define a matrix $\tilde{A} := BD^T(A^T)^{-1}(BD^T)^{-1}$.

Let $\mathcal{C}^{\perp_s}$ be the symplectic dual of $\mathcal{C}$. Then it is not difficult to verify that a generator matrix of $\mathcal{C}^{\perp_s}$ is

$$\begin{pmatrix} \tilde{A}B & B \\ H_2 & 0 \\ 0 & H_2 \end{pmatrix}.$$

From the above generator matrix of $\mathcal{C}^{\perp_s}$, we know that $\mathcal{C}$ contains its symplectic dual $\mathcal{C}^{\perp_s}$. Thus, by Proposition 2.1, there exists a q-ary $[[n, k_1 + k_2 - n, d]]$-quantum code with $d = \mathrm{wt}_s(\mathcal{C} \backslash \mathcal{C}^{\perp_s})$.

It then remains to prove $d \ge \min\{d_1, \lceil (1 + 1/q)d_2 \rceil\}$. It suffices to show that, for any nonzero $(\mathbf{u}|\mathbf{v}) \in \mathcal{C}$, $\mathrm{wt}_s(\mathbf{u}|\mathbf{v}) \ge \min\{d_1, \lceil (1 + 1/q)d_2 \rceil\}$.

Assume that

$$(\mathbf{u}|\mathbf{v}) = (\mathbf{x}, \mathbf{y}, \mathbf{z}) \begin{pmatrix} D & AD \\ G_1 & 0 \\ 0 & G_1 \end{pmatrix}$$

for some vectors $\mathbf{x}, \mathbf{y}$ and $\mathbf{z}$. Then we have

$$\mathbf{u} = \mathbf{x}D + \mathbf{y}G_1, \quad \mathbf{v} = \mathbf{x}AD + \mathbf{z}G_1.$$

Case 1. $\mathbf{u} = \mathbf{0}$. Then we have $\mathbf{x} = \mathbf{0}$ and hence $\mathbf{v} = \mathbf{z}G_1$ is a nonzero codeword of C_1. Therefore, $\mathrm{wt}_s(\mathbf{u}|\mathbf{v}) = \mathrm{wt}_H(\mathbf{v}) \ge d_1$.

Case 2. $\mathbf{v} = \mathbf{0}$. The same argument gives that $\mathrm{wt}_s(\mathbf{u}|\mathbf{v}) = \mathrm{wt}_H(\mathbf{u}) \ge d_1$.

Case 3. $\mathrm{wt}_H(\mathbf{u}) \ge d_1$ or $\mathrm{wt}_H(\mathbf{v}) \ge d_1$. In this case, it is clear that $\mathrm{wt}_s(\mathbf{u}|\mathbf{v}) \ge d_1$.

Case 4. $0 < \mathrm{wt}_H(\mathbf{u}) < d_1$ and $0 < \mathrm{wt}_H(\mathbf{v}) < d_1$. In this case, both $\mathbf{u}$ and $\mathbf{v}$ are not codewords of C_1. This implies that $\mathbf{x} \neq \mathbf{0}$. We claim that $\mathbf{u}$ and $\mathbf{v}$ are $\mathbb{F}_q$-linearly independent. Suppose that this was false, then there exists a nonzero element $\beta \in \mathbb{F}_q$ such that $\mathbf{u} = \beta\mathbf{v}$, i.e., $\mathbf{x}D + \mathbf{y}G_1 = \beta\mathbf{x}AD + \beta\mathbf{z}G_1$. This gives $(\mathbf{x}(I - \beta A), \mathbf{y} - \beta\mathbf{z})\binom{D}{G_1} = \mathbf{0}$. Therefore, we must have $\mathbf{x}(I - \beta A) = \mathbf{0}$. This implies that $1/\beta$ is an eigenvalue of A, which contradicts the choice of A.

Since both $\mathbf{u}$ and $\mathbf{v}$ are vectors of C_2, we have that $\mathrm{wt}_H(\mathbf{v}) \geq d_2$ and $\mathrm{wt}_H(\mathbf{u}+\alpha\mathbf{v}) \geq d_2$ for all $\alpha \in \mathbb{F}_q$. Now by Lemma 2.4, we have

$$q\cdot \mathrm{wt}_s(\mathbf{u}|\mathbf{v}) = \mathrm{wt}_H(\mathbf{u})+\mathrm{wt}_H(\mathbf{v})+\sum_{\alpha\in\mathbb{F}_q^*} \mathrm{wt}_H(\mathbf{u}+\alpha\mathbf{v}) \geq (q+1)d_2.$$

The desired result follows. ■

III. Application to BCH codes

From the previous section, we know that, to construct quantum codes from classical linear block codes, we need to find classical codes that contain their Euclidean duals. We can explore among some well-known codes from classical coding theory. In this section, we use classical BCH codes to construct quantum codes.

To apply the results of the previous section, we need to find classical BCH codes that contain their Euclidean duals. In [1], a sufficient condition for a classical BCH code to contain its Euclidean dual is given.

Let $\mathcal{BCH}(n, q; \delta)$ denote the q-ary narrow-sense BCH code of length n with designed distance δ.

Let

$$x[m \text{ odd}] = \begin{cases} x & \text{if } m \text{ is odd,} \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 3.1: (see [1]) Let n be a positive integer coprime to q and let $m = \mathrm{ord}_n(q)$ be the order of q modulo n. Then

(i) if $2 \leq \delta \leq \delta_{\max}$, where

$$\delta_{\max} := \left\lfloor \frac{n}{q^m-1}\left(q^{\lceil m/2\rceil} - 1 - (q-2)[m \text{ odd}]\right)\right\rfloor,$$

then $\mathcal{BCH}(n, q; \delta)$ contains its Euclidean dual $\mathcal{BCH}(n, q; \delta)^{\perp}$;

(ii) if $q^{\lfloor m/2\rfloor} < n \leq q^m - 1$ and $2 \leq \delta \leq \min\{\lfloor nq^{\lfloor m/2\rfloor}/(q^m-1)\rfloor, n\}$, then the dimension of $\mathcal{BCH}(n, q; \delta)$ is $n - m\lceil(\delta-1)(1-q^{-1})\rceil$.

By applying Proposition 3.1 and the construction in the paragraph after Proposition 2.1, we obtain a q-ary $[[n, k, \delta]]$-quantum code with $k = n - 2m\lceil(\delta-1)(1-q^{-1})\rceil$. This is one of the main results of [1] which is stated in [1, Theorem 19].

By applying our enlargement construction of Theorem 2.6, we can obtain a better quantum code.

Theorem 3.2: Let $m = \mathrm{ord}_n(q)$. Let n be in the range $q^{\lfloor m/2\rfloor} < n \leq q^m - 1$ and let δ be in the range $2 \leq \delta \leq \delta_{\max}$, with

$$\delta_{\max} = \frac{n}{q^m-1}\left(q^{\lceil m/2\rceil} - 1 - (q-2)[m \text{ odd}]\right),$$

then there exists a quantum code with parameters

$$[[n, k, \geq \delta]]_q$$

where

$$k = n - m\left(\lceil(\delta-1)\left(1-q^{-1}\right)\rceil + \left\lceil\left(\left\lceil\frac{q\delta}{q+1}\right\rceil - 1\right)\left(1-q^{-1}\right)\right\rceil\right).$$

Proof: Proposition 3.1 implies that the q-ary narrow-sense BCH code $C_1 := \mathcal{BCH}(n, q; \delta)$ with parameters $[n, n - m\lceil(\delta-1)(1-q^{-1})\rceil, \geq \delta]$ contains its Euclidean dual. By taking $\delta' = \left\lceil\frac{q\delta}{1+q}\right\rceil$ and letting $C_2 := \mathcal{BCH}(n, q; \delta')$ be the narrow-sense q-ary BCH code with parameters $[n, n-m\lceil(\delta'-1)(1-q^{-1})\rceil, \geq \delta']$, we obtain the desired result from Theorem 2.6. ■

IV. Application to asymptotic bounds

As in classical coding theory, asymptotical problems of quantum codes have been discussed in several papers (see, for example, [2], [3], [4], [6], [7]). We first recall some definitions and results from [7].

For a q-ary quantum code Q, we denote by $n(Q), K(Q)$, and $d(Q)$ the length, the dimension over $\mathbb{C}$, and the minimum distance of Q, respectively. In this case, we say that Q is an $((n(Q), K(Q), d(Q)))$- or $[[n(Q), \log_q K(Q), d(Q)]]$-quantum code. Let U_q^Q be the set of ordered pairs $(\delta, R) \in \mathbb{R}^2$ for which there exists a family $\{Q_i\}_{i=1}^{\infty}$ of q-ary quantum codes with $n(Q_i) \to \infty$ and

$$\delta = \lim_{i\to\infty}\frac{d(Q_i)}{n(Q_i)}, \quad R = \lim_{i\to\infty}\frac{\log_q K(Q_i)}{n(Q_i)},$$

where $\log_q$ denotes the logarithm to the base q. The following description on the domain U_q^Q is given in [7].

Proposition 4.1: There exists a function $\alpha_q^Q(\delta), \delta \in [0, 1]$, such that U_q^Q is the union of the domain

$$\{(\delta, R) \in \mathbb{R}^2 : \ 0 \leq R < \alpha_q^Q(\delta), \ 0 \leq \delta \leq 1\}$$

with some points on the boundary $\alpha_q^Q(\delta)$. Moreover, $\alpha_q^Q(0) = 1, \alpha_q^Q(\delta) = 0$ for $\delta \in [1/2, 1]$, and $\alpha_q^Q(\delta)$ decreases on the interval $[0, 1]$.

Some upper bounds on the function $\alpha_q^Q(\delta)$ were investigated in [3]. The first lower bound on $\alpha_2^Q(\delta)$ was derived in [4] using algebraic geometry codes and later this bound was improved by Chen-Ling-Xing [6] and Matsumoto [8]. A very good existence lower bound for p-ary quantum codes was introduced by Ashikhmin and Knill [2]. It is called the quantum Gilbert-Varshamov bound, which is a benchmark for the function $\alpha_q^Q(\delta)$. In [7], two lower bounds on q-ary quantum codes were derived from classical algebraic geometry codes and these two bounds improved the quantum Gilbert-Varshamov bound for square prime powers $q \geq 19^2$. In this section, we apply our enlargement construction to classical algebraic geometry codes again to obtain an improvement on these two algebraic geometry quantum bounds.

Before proceeding to the algebraic geometry bounds, we recall some background on classical algebraic geometry codes and a result on self-orthogonal algebraic geometry codes given in [11]. The reader may refer to [10], [12] for more details on algebraic geometry codes.

Let $\mathcal{X}/\mathbb{F}_q$ be an algebraic curve of genus g. We denote by $\mathbb{F}_q(\mathcal{X})$ the function field of $\mathcal{X}$. An element of $\mathbb{F}_q(\mathcal{X})$ is called a function. We write ν_P for the normalized discrete valuation corresponding to the point P of $\mathcal{X}/\mathbb{F}_q$.

For a divisor G, we form the Riemann-Roch space

$$\mathcal{L}(G) = \{x \in \mathbb{F}_q(\mathcal{X})\backslash\{0\} : \mathrm{div}(x) + G \geq 0\} \cup \{0\}.$$

Then $\mathcal{L}(G)$ is a finite-dimensional vector space over $\mathbb{F}_q$, and we denote its dimension by $\ell(G)$. By the Riemann-Roch theorem we have

$$\ell(G) \geq \deg(G) + 1 - g,$$

and equality holds if $\deg(G) \geq 2g - 1$.

Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ be a subset of $\mathcal{X}(\mathbb{F}_q)$.

Choose a divisor G such that $\mathrm{supp}(G) \cap \mathcal{P} = \emptyset$. Then $\nu_{P_i}(f) \geq 0$ for all $1 \leq i \leq n$ and any $f \in \mathcal{L}(G)$.

Consider the map

$$\phi \ : \ \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n, \quad f \mapsto (f(P_1), f(P_2), \ldots, f(P_n)).$$

Then the image of ϕ forms a subspace of $\mathbb{F}_q^n$ that was defined as an algebraic geometry code by Goppa. The image of ϕ is denoted by $C_L(G; \mathcal{P})$. If n is bigger than the degree of G, then ϕ is an embedding and the dimension k of $C_L(G; \mathcal{P})$ is equal to $\ell(G)$. The Riemann-Roch theorem makes it possible to estimate the parameters of the code $C_L(G; \mathcal{P})$.

H. Stichtenoth showed in [11] that there exists a family of algebraic geometry codes achieving the TVZ bound that are equivalent to self-orthogonal codes. More precisely:

Proposition 4.2: Let q be the square of a prime power. Then there exists a family $\{\mathcal{X}/\mathbb{F}_q\}$ of curves over $\mathbb{F}_q$ and a family of algebraic geometry codes $C(G; \mathcal{P})$ of length n from the curves $\mathcal{X}/\mathbb{F}_q$ together with a family of vectors $\mathbf{v} \in (\mathbb{F}_q^*)^n$ such that

(i) $\mathbf{v}C(G; \mathcal{P})$ is self-orthogonal if its dimension is less than or equal to $n/2$; and $\mathbf{v}C(G; \mathcal{P})$ contains its Euclidean dual if its dimension is bigger than or equal to $n/2$;

(ii) the code $C(G; \mathcal{P})$ achieves the asymptotic TVZ bound, i.e.,

$$\lim_{n\to\infty} \frac{\dim(C(G; \mathcal{P})) + d_H(C(G; \mathcal{P}))}{n} \geq 1 - \frac{1}{\sqrt{q} - 1}, \tag{IV.1}$$

where $d_H(\cdot)$ denotes the Hamming distance of a code.

We note that the curves $\mathcal{X}$ contain rational points other than those that are contained in $\mathcal{P}$. For instance, the rational points lying over the pole of z of the rational function field $\mathbb{F}_q(z)$ do not belong to $\mathcal{P}$. See [11] for the details.

From Proposition 4.2 and the paragraph after Proposition 2.1, we can construct q-ary $[[n, 2k - n, d]]$-quantum codes with $k = \dim(C(G; \mathcal{P}))$ and $d = d_H(C(G; \mathcal{P}))$. If we let $\lim_{n\to\infty} d/n = \delta$, then, by the TVZ bound (IV.1), we obtain

$$\alpha_q^Q(\delta) \geq 1 - 2\delta - \frac{2}{\sqrt{q} - 1}. \tag{IV.2}$$

The bound (IV.2) was derived in [7] using algebraic geometry codes as well, but through a different approach. One notes that the bound (IV.2) beats the quantum Gilbert-Varshamov bound if $q \geq 19^2$ is an even power of a prime .

By using more careful analysis, the bound (IV.2) was further improved to the following in [7]

$$\alpha_q^Q(\delta) \geq 1 - 2\delta - \frac{2}{\sqrt{q} - 1} + \log_q \left(1 + \frac{1}{q^3}\right). \tag{IV.3}$$

Now we are ready to state and prove our main result of this section.

Theorem 4.3: Let q be a prime power square, then one has

$$\alpha_q^Q(\delta) \geq 1 - \left(2 - \frac{1}{q+1}\right)\delta - \frac{2}{\sqrt{q} - 1}. \tag{IV.4}$$

Proof: Let $C(G; \mathcal{P})$ be the algebraic geometry codes achieving the TVZ bound (IV.1) in Proposition 4.2 and let $\mathbf{v} \in (\mathbb{F}_q^*)^n$ be a vector such that $\mathbf{v}C(G; \mathcal{P})$ contains its Euclidean dual. Let $C_1 := \mathbf{v}C(G; \mathcal{P})$, with parameters $[n, k_1, d_1]$. Choose a rational point P outside of $\mathcal{P}$ (see paragraph after Proposition 4.2) and consider the code $C_2 := \mathbf{v}C(G + rP; \mathcal{P})$, with parameters $[n, k_1 + r, d_1 - r]$ for some integer $r \geq 2$. Then it is clear that C_1 is a subspace of C_2. Moreover, C_1 contains its Euclidean dual if $k_1 \geq n/2$. Applying Theorem 2.6, we obtain a quantum $[[n, 2k_1 + r - n, \min\{d_1, (1 + 1/q)(d_1 - r)\}]]$-code. By letting $r = \lfloor d_1/(q+1) \rfloor$ and letting $\lim_{n\to\infty} d_1/n = \delta$, we obtain the desired result from the bound (IV.1). ∎

REFERENCES

[1] S. A. Aly and A. Klappenecker, "On quantum and classical BCH codes," *IEEE Trans. Inform. Theory,* vol. 53, no. 3, pp. 1183–1188, Mar. 2007.

[2] A. E. Ashikhmin and E. Knill, "Nonbinary quantum stablizer codes," *IEEE Trans. Inform. Theory,* vol. 47, no. 7, pp. 3065–3072, Nov. 2001.

[3] A. Ashikhmin and S. Litsyn, "Upper bounds on the size of quantum codes," Sep., 1997, quant-ph/9709049.

[4] A. Ashikhmin, S. Litsyn and M. A. Tsfasman, "Asymptotically good quantum codes," *Phys. Rev. A,* vol. 63, no. 3, p.032311, March, 2001.

[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. Inform. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.

[6] H. Chen, S. Ling and C. P. Xing, "Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound," *IEEE Trans. Inform. Theory*, vol. 47, no.5, pp. 2055–2058, Jul. 2001.

[7] K. Q. Feng, S. Ling and C. P. Xing, "Asymptotic bounds on quantum codes from algebraic geometry codes," *IEEE Trans. Inform. Theory,* vol. 52, no. 3, pp. 986–991, Mar. 2006.

[8] R. Matsumoto, "Improvement of the Ashikhmin-Litsyn-Tsfasman bound for quantum codes", *IEEE Trans. Inform. Theory*, Vol. 48, pp. 2122–2124, 2002.

[9] A. M. Steane, "Enlargement of Calderbank-Shor-Steane quantum codes," *IEEE Trans. Inform. Theory,* vol. 45, no. 7, pp. 2492–2495, Nov. 1999.

[10] H. Stichtenoth, *Algebraic Function Fields and Codes.* Berlin, Germany: Springer-Verlag, 1993.

[11] H. Stichtenoth, "Transitive and Self-Dual Codes Attaining the Tsfasman-Vlăduţ-Zink Bound", *IEEE Trans. Inform. Theory,* vol. 52, no. 5, pp. 2218–2224, May 2006.

[12] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric codes.* Kluwer, Holland, 1991.

AUTHORS' BIOGRAPHIES

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.