Asymmetric Quantum Codes: Characterization and Constructions

Long Wang, Keqin Feng, San Ling, and Chaoping Xing

***Abstract*—The stabilizer method for constructing a class of asymmetric quantum codes (AQC), called additive AQC, has been established by Aly *et al.* In this paper, we present a new characterization of AQC, which generalizes a result of the symmetric case known previously. As an application of the characterization, we establish a relationship of AQC with classical error-correcting codes and show a few examples of good AQC with specific parameters. By using this relationship, we obtain an asymptotic bound on AQCs from algebraic geometry codes.**

***Index Terms*—Algebraic geometry codes, asymptotic bounds, classical codes, mappings, quantum codes.**

I. Introduction

AFTER the works of Shor [13] and Steane [14], [15] in 1995–1996, the theory of quantum error-correcting codes has developed rapidly. In 1998, Calderbank *et al.* [4] presented systematic methods to construct binary quantum codes, called stabilizer codes or additive codes, from classical error-correcting codes. At the same time, the stabilizer method has been generalized to nonbinary quantum codes and new methods have been found to construct nonadditive quantum codes. Recently, a number of new types of quantum codes, such as convolutional quantum codes, subsystem quantum codes, and asymmetric quantum codes (AQC), have been studied and the stabilizer method has been extended to these variations of quantum codes. In particular, there has been intensive activity in the area of AQCs [1], [2], [6], [10], [12].

This paper concentrates on the AQCs which deal with the case where dephasing errors (Z-errors) happen more frequently than qubit-flipping errors (X-errors) [14], [15]. Such codes are used in fault tolerant operations of a quantum computer carrying controlled and measured quantum information over asymmetric channels [6]. Our aim in the paper is to extend the characterization of nonadditive symmetric quantum codes given in [7] and [8] to the asymmetric case and to show several examples of good AQCs.

The paper is organized as follows. We introduce the basic notations and definitions of symmetric and AQCs in Section II. In Section III, we present the characterization of AQCs (Theorem 3.1) and establish a relationship between classical error-correcting codes and AQCs (Theorem 3.2). Finally, in Section IV, an asymptotic bound on AQCs is derived from algebraic geometry codes based on the relationship between classical codes and asymmetric codes given in Section III.

II. Symmetric and Asymmetric Quantum Codes

Let $\mathbb{F}_q$ be the finite field with $q = p^m$, where p is a prime number and $m \geq 1$ is an integer. Let $\mathbb{C}$ be the complex number field. We fix an orthonormal basis of $\mathbb{C}^q$

$$\{|v\rangle : v \in \mathbb{F}_q\}$$

with respect to the Hermitian inner product. For a positive integer n, let $V_n = (\mathbb{C}^q)^{\otimes n} = \mathbb{C}^{q^n}$ be the nth tensor of $\mathbb{C}^q$. Then, V_n has the following orthonormal basis

$$\{|c\rangle = |c_1c_2\cdots c_n\rangle = |c_1\rangle \otimes |c_2\rangle \otimes \cdots \otimes |c_n\rangle : c = (c_1,\ldots,c_n) \in \mathbb{F}_q^n\}. \quad \text{(II.1)}$$

For two quantum states $|u\rangle$ and $|v\rangle$ in V_n with

$$|u\rangle = \sum_{c\in\mathbb{F}_q^n} \alpha(c)|c\rangle, \quad |v\rangle = \sum_{c\in\mathbb{F}_q^n} \beta(c)|c\rangle \quad (\alpha(c),\beta(c) \in \mathbb{C})$$

the Hermitian inner product of $|u\rangle$ and $|v\rangle$ is

$$\langle u|v\rangle = \sum_{c\in\mathbb{F}_q^n} \overline{\alpha(c)}\beta(c) \in \mathbb{C}$$

where $\overline{\alpha(c)}$ is the complex conjugate of $\alpha(c)$. We say $|u\rangle$ and $|v\rangle$ are *orthogonal* if $\langle u|v\rangle = 0$.

A quantum error acting on V_n is a unitary linear operator on V_n and has the following form:

$$e = X(a)Z(b) \quad \big(a = (a_1,\ldots,a_n), b = (b_1,\ldots,b_n) \in \mathbb{F}_q^n\big).$$

The action of e on the basis (II.1) of V_n is

$$e|c\rangle = X(a_1)Z(b_1)|c_1\rangle \otimes X(a_2)Z(b_2)|c_2\rangle \otimes \cdots \otimes X(a_n)Z(b_n)|c_n\rangle$$

where

$$X(a_i)|c_i\rangle = |a_i + c_i\rangle, \quad Z(b_i)|c_i\rangle = \omega^{T(b_ic_i)}|c_i\rangle$$

L. Wang was with the Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China. He is now with the Bank of Communication, Beijing 100032, China (e-mail: wanglong01@mails.tsinghua.edu.cn).

K. Feng is with the Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China (e-mail: kfeng@math.tsinghua.edu.cn).

S. Ling and C. P. Xing are with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371, Singapore (e-mail: lingsan@ntu.edu.sg; xingcp@ntu.edu.sg).

Communicated by P. Hayden, Associate Editor for Quantum Information Theory.

Digital Object Identifier 10.1109/TIT.2010.2046221

with $\omega = e^{\frac{2\pi\sqrt{-1}}{p}} \in \mathbb{C}$ and $T: \mathbb{F}_q \to \mathbb{F}_p$ being the trace mapping

$$T(\alpha)=\alpha+\alpha^p+\alpha^{p^2}+\cdots+\alpha^{p^{m-1}}, \qquad \text{for } \alpha\in\mathbb{F}_q \quad (q=p^m).$$

Therefore

$$X(a_i)Z(b_i)|c_i\rangle = \omega^{T(b_ic_i)}|a_i+c_i\rangle$$

and

$$\begin{aligned} e|c\rangle &= \omega^{T(b\cdot c)}|a_1+c_1\rangle\otimes|a_2+c_2\rangle\otimes\cdots\otimes|a_n+c_n\rangle \\ &= \omega^{T(b\cdot c)}|a+c\rangle \end{aligned}$$

where $b\cdot c=\sum_{i=1}^n b_ic_i\in\mathbb{F}_q$ is the usual inner product in $\mathbb{F}_q^n$.

It can be checked that for $e = X(a)Z(b)$ and $e' = X(a')Z(b')\ (a,b,a',b'\in\mathbb{F}_q^n)$

$$ee' = \omega^{T(a\cdot b'-a'\cdot b)}e'e$$

hence the set

$$E_n=\left\{\omega^\lambda X(a)Z(b)|0\le\lambda\le p-1, \quad a,b\in\mathbb{F}_q^n\right\}$$

forms a (nonabelian) group, called the *error group* on V_n.

Definition 2.1: For a quantum error

$$\begin{aligned} e &= \omega^\lambda X(a)Z(b) \\ &\in E_n\ (a=(a_1,\ldots,a_n)\in\mathbb{F}_q^n, b=(b_1,\ldots,b_n)\in\mathbb{F}_q^n) \end{aligned}$$

we define the *quantum weight* $w_Q(e)$, *X-weight* $w_X(e)$ and *Z-weight* $w_Z(e)$ by

$$\begin{aligned} w_Q(e) &= \#\{i|1\le i\le n,\ (a_i,b_i)\ne(0,0)\} \\ w_X(e) &= \#\{i|1\le i\le n,\ a_i\ne 0\} \\ w_Z(e) &= \#\{i|1\le i\le n,\ b_i\ne 0\}. \end{aligned}$$

Namely, $w_Q(e)$ is the number of quantum digits where the action of e is nontrivial by $X(a_i)Z(b_i)\ne I$ (identity); $w_X(e)$ ($w_Z(e)$, respectively) is the number of quantum digits where the X-action (Z-action, respectively) of e is nontrivial. It is easy to see that

$$\max\{w_X(e),w_Z(e)\}\le w_Q(e)\le\min\{w_X(e)+w_Z(e),n\}.$$

Definition 2.2: A q-ary quantum code of length n is a subspace Q of V_n with dimension $K\ge 1$. A quantum code Q of dimension $K\ge 2$ is said to detect $d-1$ quantum digits of errors for $d\ge 1$ if for every orthogonal pair $|u\rangle$, $|v\rangle$ in Q with $\langle u|v\rangle=0$ and every $e\in E_n$ with $w_Q(e)\le d-1$, $|u\rangle$ and $e|v\rangle$ are orthogonal, i.e., $\langle u|e|v\rangle=0$. In this case, we call Q a *symmetric* quantum code with parameters $((n,K,d))_q$ or $[[n,k,d]]_q$, where $k=\log_q K$. Such a quantum code is called *pure* if $\langle u|e|v\rangle=0$ for any $|u\rangle$ and $|v\rangle$ in Q and any $e\in E_n$ with $1\le w_Q(e)\le d-1$. A quantum code Q with $K=1$ is always pure.

Let d_x and d_z be positive integers. A quantum code Q in V_n with dimension $K\ge 2$ is called AQC with parameters $((n,K,d_z/d_x))_q$ or $[[n,k,d_z/d_x]]_q$ ($k=log_qK$) if Q detects d_x-1 quantum digits of X-errors and, at the same time, d_z-1 quantum digits of Z-errors. Namely, if $\langle u|v\rangle=0$ for $|u\rangle,|v\rangle\in Q$, then $\langle u|e|v\rangle=0$ for any $e\in E_n$ such that $w_X(e)\le d_x-1$ and $w_Z(e)\le d_z-1$. Such an AQC Q is called *pure* if $\langle u|e|v\rangle=0$ for any $|u\rangle,|v\rangle\in Q$ and $e\in E_n$ such that $w_X(e)\le d_x-1$, $w_Z(e)\le d_z-1$ and $w_Q(e)\ge 1$. An AQC Q with $K=1$ is assumed to be pure.

Remark 2.3: An AQC with parameters $((n,K,d/d))_q$ is a symmetric quantum code with parameters $((n,K,d))_q$, but the converse is not true since for $e\in E_n$ with $w_X(e)\le d-1$ and $w_Z(e)\le d-1$, the weight $w_Q(e)$ may be bigger than $d-1$.

The stabilizer method has been extended to AQCs and gives the following result (Theorem 2.4) on the construction of AQCs from classical error-correcting codes. Recall that a classical linear code C with parameters $[n,k,d]_q$ is a linear subspace of $\mathbb{F}_q^n$ with dimension $k(\ge 1)$ over $\mathbb{F}_q$ and $1\le d\le d(C)$ is the minimum distance of C defined by

$$\begin{aligned} d(C) &= \min\{d_H(c,c'): c,c'\in C,\ \ c\ne c'\} \\ &= \min\{w_H(c): 0\ne c\in C\} \end{aligned}$$

where $d_H(c,c')=w_H(c-c')$ (note that $w_H(c)$ is the Hamming weight of c). The dual code $C^\perp$ of C is defined by

$$C^\perp=\left\{v\in\mathbb{F}_q^n: v\cdot c=0, \qquad \text{for each } c\in C\right\}.$$

Theorem 2.4 [1, Lemma 214], [2, Lemma 4]: Let C_i be a classical linear code with parameters $[n,k_i,d_i]_q$ ($i=1,2$) and $C_1^\perp\subseteq C_2$ (so that $C_2^\perp\subseteq C_1$ and $k_1+k_2\ge n$). Then, there exists an AQC Q with parameters $[[n,k_1+k_2-n,d_z/d_x]]_q$, where

$$\begin{aligned} d_z &= \max\left\{wt(C_2\backslash C_1^\perp),\ wt(C_1\backslash C_2^\perp)\right\} \\ d_x &= \min\left\{wt(C_2\backslash C_1^\perp),\ wt(C_1\backslash C_2^\perp)\right\} \end{aligned}$$

and for a subset S of $\mathbb{F}_q^n$

$$wt(S)=\min\left\{w_H(v): 0\ne v\in S\right\}.$$

Moreover, such a quantum code with parameters $[[n,k,d_z/d_x]]_q$ is pure if $d_2=wt(C_2)=wt(C_2\backslash C_1^\perp)$ and $d_1=wt(C_1)=wt(C_1\backslash C_2^\perp)$.

Theorem 2.4 has been proved by the stabilizer method in [1] and [2]. AQCs constructed by Theorem 2.4 are called *additive codes*. A sequence of additive AQCs has been obtained from classical cyclic codes in [1] and [2]. To see whether a quantum code is good in terms of its parameters, we have to introduce some bounds. For a pure AQC with parameters $((n,K,d_z/d_x))_q$, we have the Hamming bound

$$q^n\ge K\left(\sum_{i=0}^{\lfloor\frac{d_z-1}{2}\rfloor}(q-1)^i\binom{n}{i}\right)\left(\sum_{j=0}^{\lfloor\frac{d_x-1}{2}\rfloor}(q-1)^j\binom{n}{j}\right). \tag{II.2}$$

This is because for a pure code Q, the spaces $e(Q)$ with

$$e \in E_n, \quad w_X(e) \le \frac{d_x - 1}{2}, \quad w_Z(e) \le \frac{d_z - 1}{2}$$

are subspaces of V_n with dimension K and they are orthogonal to each other. The code Q is called *perfect* if the inequality (II.2) becomes equality.

On the other hand, from the Singleton bound of classical codes we can get the following bound of any additive AQC with parameters $[[n, k, d_z/d_x]]_q$ [2, Th. 19]:

$$n \ge k + d_z + d_x - 2. \tag{II.3}$$

It seems that this Singleton bound (II.3) may be true for all AQCs. As in the classical case, we say an additive AQC is a maximum distance separable (MDS) code if the equality in (II.3) holds.

Corollary 2.5: Let Q be a pure additive AQC constructed by classical codes C_1 and C_2 in Theorem 2.4. Then:

i) Q is MDS if and only if both C_1 and C_2 are MDS;

ii) Q is perfect if and only if both C_1 and C_2 are perfect.

Proof: Since Q is pure, we know that $\{d_z, d_x\} = \{d_1, d_2\}$ and hence $d_z + d_x = d_1 + d_2$. The Hamming bound and the Singleton bound for the classical codes C_1 and C_2 are

$$q^{n-k_i} \ge \sum_{\lambda=0}^{\lfloor \frac{d_i-1}{2} \rfloor} (q-1)^\lambda \binom{n}{\lambda} \tag{II.4}$$

and

$$n \ge k_i + d_i - 1 \tag{II.5}$$

respectively. Therefore

$$\begin{aligned} Q \text{ is MDS} \Leftrightarrow & n = k_1 + k_2 - n + d_x + d_z - 2 \\ & = k_1 + k_2 - n + d_1 + d_2 - 2 \\ \Leftrightarrow & n = k_1 + d_1 - 1 = k_2 + d_2 - 1 \text{ [by (II.5)]} \\ \Leftrightarrow & C_1 \text{ and } C_2 \text{ are MDS} \end{aligned}$$

and

$$\begin{aligned} Q \text{ is perfect} \Leftrightarrow & q^{n-(k_1+k_2-n)} \\ & = \left(\sum_{\lambda=0}^{\lfloor \frac{d_1-1}{2} \rfloor} (q-1)^\lambda \binom{n}{\lambda} \right) \left(\sum_{\lambda=0}^{\lfloor \frac{d_2-1}{2} \rfloor} (q-1)^\lambda \binom{n}{\lambda} \right) \\ \Leftrightarrow & q^{n-k_i} = \sum_{\lambda=0}^{\lfloor \frac{d_i-1}{2} \rfloor} (q-1)^\lambda \binom{n}{\lambda}, \qquad i = 1, 2 \\ & \qquad \text{[by (II.4)]} \\ \Leftrightarrow & C_1 \text{ and } C_2 \text{ are perfect.} \end{aligned}$$

This completes the proof. □

For instance, by taking C_2 a perfect code (for example, a Hamming code or a Golay code) and $C_1 = \mathbb{F}_q^n$, we get a perfect AQC with $d_x = 1$. On the other hand, if both C_1 and C_2 are Reed–Solomon codes, we obtain MDS AQCs [1, Th. 220].

III. A Characterization of Asymmetric Quantum Codes

In this section, we extend the results of [7, Th. 2.2] and [8, Th. 3.1] to the asymmetric case, and present the following characterization of AQCs.

For a vector $c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$ and a subset A of $\{1, 2, \ldots, n\}$, we denote $c_A = (c_i)_{i \in A}$.

Theorem 3.1:

i) There exists an AQC with parameters $((n, K, d_z/d_x))_q$ $(K \ge 2)$ if and only if there exist K nonzero mappings

$$\varphi_i : \mathbb{F}_q^n \to \mathbb{C}, \qquad 1 \le i \le K \tag{III.1}$$

satisfying the following conditions: for each d, $1 \le d \le \min\{d_x, d_z\}$ and partition of $\{1, 2, \ldots, n\}$

$$\begin{cases} \{1, 2, \ldots, n\} = A \cup X \cup Z \cup B \\ |A| = d - 1, \ |X| = d_x - d \\ |Z| = d_z - d, \ |B| = n + d - d_x - d_z + 1 \end{cases} \tag{III.2}$$

and each $c_A, c'_A \in \mathbb{F}_q^{|A|}$, $c_Z \in \mathbb{F}_q^{|Z|}$ and $a_X \in \mathbb{F}_q^{|X|}$, we have the equality

$$\begin{aligned} & \sum_{\substack{c_X \in \mathbb{F}_q^{|X|} \\ c_B \in \mathbb{F}_q^{|B|}}} \overline{\varphi_i}(c_A, c_X, c_Z, c_B) \varphi_j(c'_A, c_X - a_X, c_Z, c_B) \\ & \qquad = \begin{cases} 0, & \text{for } i \ne j \\ I(c_A, c'_A, c_Z, a_X), & \text{for } i = j \end{cases} \end{aligned} \tag{III.3}$$

where $I(c_A, c'_A, c_Z, a_X)$ is an element of $\mathbb{C}$ which is independent of i.

ii) There exists a pure AQC with parameters $((n, K, d_z/d_x))_q$ $(K \ge 1)$ if and only if there exist K nonzero mappings φ_i $(1 \le i \le K)$ as shown in (III.1) such that:

ii.a) φ_i $(1 \le i \le K)$ are linearly independent, namely, the rank of the $K \times q^n$ matrix $(\varphi_i(c))_{1 \le i \le K, c \in \mathbb{F}_q^n}$ is K;

ii.b) for each $d, 1 \le d \le \min\{d_x, d_z\}$, a partition (III.2) and $c_A, a_A \in \mathbb{F}_q^{|A|}$, $c_Z \in \mathbb{F}_q^{|Z|}$ and $a_X \in \mathbb{F}_q^{|X|}$

$$\begin{aligned} & \sum_{\substack{c_X \in \mathbb{F}_q^{|X|} \\ c_B \in \mathbb{F}_q^{|B|}}} \overline{\varphi_i}(c_A, c_X, c_Z, c_B) \varphi_j(c_A + a_A, c_X + a_X, c_Z, c_B) \\ & \qquad = \begin{cases} 0, & \text{for } (a_A, a_X) \ne (0, 0) \\ \frac{(\varphi_i, \varphi_j)}{q^{d_z} - 1}, & \text{for } (a_A, a_X) = (0, 0) \end{cases} \end{aligned} \tag{III.4}$$

where (φ_i, φ_j) stands for $\sum_{c \in \mathbb{F}_q^n} \overline{\varphi_i}(c) \varphi_j(c)$.

Proof: We follow the argument in the proof of [7, Th. 2.2] and the following two simple facts on the Fourier transform. For a mapping $\varphi : \mathbb{F}_q^n \to \mathbb{C}$ and its Fourier transform

$$\Phi : \mathbb{F}_q^n \to \mathbb{C}, \quad \Phi(y) = \sum_{x \in \mathbb{F}_q^n} \varphi(x) \omega^{T(x \cdot y)}.$$

Fact (I): $\Phi \equiv 0$ if and only if $\varphi \equiv 0$.

Fact (II): $\Phi(a) = 0$ for all $0 \ne a \in \mathbb{F}_q^n$ if and only if φ is a constant.

i) Let Q be a K-dimensional subspace of $V_n = \mathbb{C}^{q^n}$ with an orthonormal basis

$$|v_i\rangle = \sum_{c\in\mathbb{F}_q^n} \varphi_i(c)|c\rangle, \qquad 1 \le i \le K, \qquad \varphi_i(c) \in \mathbb{C}$$

then

$$(\varphi_i, \varphi_j) = \sum_{c\in\mathbb{F}_q^n} \overline{\varphi_i(c)}\varphi_j(c) = \langle v_i|v_j\rangle = \begin{cases} 0, & \text{if } i \neq j \\ 1, & \text{if } i = j. \end{cases}$$

For two vectors in Q

$$|u\rangle = \sum_{i=1}^{K} \alpha_i|v_i\rangle, \quad |u'\rangle = \sum_{i=1}^{K} \alpha_i'|v_i\rangle, \qquad \alpha, \alpha' \in \mathbb{C}$$

we have

$$\langle u|u'\rangle = \sum_{i,j=1}^{K} \overline{\alpha_i}\alpha_j'\langle v_i|v_j\rangle = \sum_{i=1}^{K} \overline{\alpha_i}\alpha_i'.$$

For each $e = X(a)Z(b)$ $(a, b \in \mathbb{F}_q^n)$ with $w_X(e) \le d_x - 1$ and $w_Z(e) \le d_z - 1$, let

$$\begin{aligned} A &= \{i | 1 \le i \le n,\ a_i \neq 0, b_i \neq 0\} \\ X &= \{i | 1 \le i \le n,\ a_i \neq 0\} \backslash A \\ Z &= \{i | 1 \le i \le n,\ b_i \neq 0\} \backslash A \\ B' &= \{1, 2, \ldots, n\} \backslash (A \cup X \cup Z). \end{aligned}$$

Then, $|A| \le \min\{d_x - 1, d_z - 1\}$, so that we can find a partition (III.2) such that e can be expressed by

$$e = X(a_A a_X 0_Z 0_B)Z(b_A 0_X b_Z 0_B). \tag{III.5}$$

The action of e on $|u'\rangle$ is

$$\begin{aligned} e|u'\rangle &= \sum_{j=1}^{K} \alpha_j' \sum_{c\in\mathbb{F}_q^n} \varphi_j(c)e|c\rangle \\ &= \sum_{j=1}^{K} \alpha_j' \sum_{c_A, c_X, c_Z, c_B} \varphi_j(c_A, c_X, c_Z, c_B) \\ &\quad \times \omega^{T(b_A\cdot c_A + b_Z\cdot c_Z)}|c_A + a_A, c_X + a_X, c_Z, c_B\rangle \\ &= \sum_{j=1}^{K} \alpha_j' \sum_{c_A, c_X, c_Z, c_B} \varphi_j(c_A - a_A, c_X - a_X, c_Z, c_B) \\ &\quad \times \omega^{T(b_A\cdot(c_A - a_A) + b_Z\cdot c_Z)}|c_A, c_X, c_Z, c_B\rangle. \end{aligned}$$

By Definition 2.2, Q is an AQC with parameters $((n, K, d_z/d_x))_q$ if and only if, under the condition $\sum_{i=1}^{K} \overline{\alpha_i}\alpha_i' (= \langle u|u'\rangle) = 0$, we have

$$\begin{aligned} 0 &= \langle u|e|u'\rangle \\ &= \omega^{T(-b_A\cdot a_A)} \sum_{i,j=1}^{K} \overline{\alpha_i}\alpha_j' \sum_{c_A, c_X, c_Z, c_B} \overline{\varphi_i}(c_A, c_X, c_Z, c_B) \\ &\quad \times \varphi_j(c_A - a_A, c_X - a_X, c_Z, c_B)\omega^{T(b_A\cdot c_A + b_Z\cdot c_Z)}. \end{aligned}$$

Since b_A and b_Z are any vectors, from Fact (I) we know that the above equality is equivalent to

$$\sum_{i,j=1}^{K} \overline{\alpha_i}\alpha_j' \sum_{c_X, c_B} \overline{\varphi_i}(c_A, c_X, c_Z, c_B)\varphi_j(c_A', c_X - a_X, c_Z, c_B) = 0$$

for any c_A, c_A', a_X, and c_Z. Consider the matrix

$$M = (m_{ij})_{1\le i,j\le K}$$

with

$$m_{ij} = \sum_{c_X, c_B} \overline{\varphi_i}(c_A, c_X, c_Z, c_B)\varphi_j(c_A', c_X - a_X, c_Z, c_B).$$

Our statement now becomes that for any $\alpha, \alpha' \in \mathbb{C}^K$, $\overline{\alpha}\cdot\alpha'^T = 0$ implies that $\overline{\alpha}M\alpha'^T = 0$. It is easy to see that under the assumption $K \ge 2$, this statement is equivalent to $M = fI_K$, where I_K is the identity matrix and $f = f(c_A, c_A', c_Z, a_X) \in \mathbb{C}$. Namely

$$m_{ij} = \begin{cases} 0, & \text{for } i \neq j \\ f = f(c_A, c_A', c_Z, a_X) \text{ (independent of } i), & \text{for } i = j \end{cases}$$

which is the condition (III.3).

ii) Let $|v_i\rangle = \sum_{c\in\mathbb{F}_q^n} \varphi_i(c)|c\rangle$ $(1 \le i \le K)$ be a basis of Q. Then, the condition ii.a) is satisfied. By Definition 2.2, Q is a pure AQC with parameters $((n, K, d_z/d_x))_q$ if and only if $\langle v_i|e|v_j\rangle = 0 (1 \le i, j \le K)$ for each $e \neq I$ in the form (III.5). By arguments similar to those in i), this requirement can be transformed into

$$\begin{aligned} &\sum_{c_A, c_X, c_Z, c_B} \overline{\varphi_i}(c_A, c_X, c_Z, c_B) \\ &\quad \varphi_j(c_A - a_A, c_X - a_X, c_Z, c_B)\omega^{T(b_A\cdot c_A + b_Z\cdot c_Z)} = 0 \end{aligned} \tag{III.6}$$

for each $(a_A, a_X, b_A, b_Z) \neq (0, 0, 0, 0)$. If $(a_A, a_X) \neq (0, 0)$, then (III.6) is true for any b_A and b_Z. Then, we get the first equality of (III.4). If $(a_A, a_X) = (0, 0)$, then (III.6) becomes

$$\begin{aligned} &\sum_{c_A, c_X, c_Z, c_B} \overline{\varphi_i}(c_A, c_X, c_Z, c_B) \\ &\quad \varphi_j(c_A, c_X, c_Z, c_B)\omega^{T(b_A\cdot c_A + b_Z\cdot c_Z)} = 0 \end{aligned}$$

for any $(b_A, b_Z) \neq (0, 0)$. By Fact (II), this means

$$\sum_{c_X, c_B} \overline{\varphi_i}(c_A, c_X, c_Z, c_B)\varphi_j(c_A, c_X, c_Z, c_B) = I_{ij}.$$

Note that I_{ij} is independent of c_A and c_Z. Then

$$(\varphi_i, \varphi_j) = \sum_{c\in\mathbb{F}_q^n} \overline{\varphi_i}(c)\varphi_j(c) = \sum_{c_A, c_Z} I_{ij} = I_{ij}q^{d_z - 1}.$$

Therefore, $I_{ij} = \frac{(\varphi_i, \varphi_j)}{q^{d_z - 1}}$. This completes the proof. □

Now, we give an application of Theorem 3.1.

Theorem 3.2: Let d_x and d_z be positive integers. Let C be a classical linear code in $\mathbb{F}_q^n$. Assume that $d^\perp = d(C^\perp)$ is the

minimum distance of the dual code $C^{\perp}$ of C. For a set $V = \{v_i \quad |1 \le i \le K\}$ of K distinct vectors in $\mathbb{F}_q^n$, define

$$d_v = \min\{w_H(v_i - v_j + c) : 1 \le i \ne j \le K,\, c \in C\}.$$

If $d^{\perp} \ge d_z$ and $d_v \ge d_x$, then there exists an AQC Q with parameters $((n, K, d_z/d_x))_q$.

Proof: For each i $(1 \le i \le K)$, we define a mapping $\varphi_i : \mathbb{F}_q^n \to \mathbb{C}$ by

$$\varphi_i(u) = \begin{cases} 0, & \text{if } u \notin v_i + C \\ 1, & \text{otherwise.} \end{cases}$$

We have to show that the condition (III.3) is true for the mappings φ_i $(1 \le i \le K)$.

For each partition (III.2), we have

$$\overline{\varphi_i}(c_A, c_X, c_Z, c_B)\varphi_j(c_A + a_A, c_X + a_X, c_Z, c_B) \ne 0$$
$$\Leftrightarrow (c_A, c_X, c_Z, c_B) \in v_i + C$$

and

$$(c_A + a_A, c_X + a_X, c_Z, c_B) \in v_j + C$$
$$\Leftrightarrow (a_A, a_X, 0_Z, 0_B) \in v_j - v_i + C$$

and

$$(c_A, c_X, c_Z, c_B) \in v_i + C. \tag{III.7}$$

Since $w_H(a_A a_X) \le |A| + |X| = d_x - 1$, we know that $(a_A, a_X, 0_Z, 0_B) \in v_j - v_i + C$ implies that $i = j$. Therefore

$$\sum_{c_X, c_B} \overline{\varphi_i}(c_A, c_X, c_Z, c_B)\varphi_j(c_A + a_A, c_X + a_X, c_Z, c_B) = 0 \tag{III.8}$$

if $i \ne j$.

For $i = j$, from (III.7), we get

$$\sum_{c_X, c_B} \overline{\varphi_i}(c_A, c_X, c_Z, c_B)\varphi_j(c_A + a_A, c_X + a_X, c_Z, c_B) = \sum_{\substack{c_X, c_B \\ (a_A, a_X, 0_Z, 0_B) \in C \\ (c_A, c_X, c_Z, c_B) \in v_i + C}} 1. \tag{III.9}$$

It is a well-known fact that, under the assumption $d^{\perp} \ge d_z$, there exist exactly $\frac{|C|}{q^{d_z - 1}}$ vectors $(c_A, c_X, c_Z, c_B) \in v_i + C$ for any fixed $(c_A c_Z) \in \mathbb{F}_q^{d_z - 1}$. Then, from (III.9), we get

$$\sum_{c_X, c_B} \overline{\varphi_i}(c_A, c_X, c_Z, c_B)\varphi_i(c_A + a_A, c_X + a_X, c_Z, c_B) = \begin{cases} 0, & \text{if } (a_A, a_X, 0_Z, 0_B) \notin C \\ \frac{|C|}{q^{d_z - 1}}, & \text{if } (a_A, a_X, 0_Z, 0_B) \in C \end{cases} \tag{III.10}$$

which is independent of i. By Theorem 3.1, we have an AQC Q with parameters $((n, K, d_z/d_x))_q$. □

Though the following corollary can be derived from Theorem 2.4, we are able to apply Theorem 3.2 to obtain it as well.

Corollary 3.3: Let C_i be classical linear codes with parameters $[n, k_i, d_i]_q$ $(i = 1, 2)$ with $C_1^{\perp} \subseteq C_2$. Then, there exists an AQC Q with parameters $[[n, k_1 + k_2 - n, d_z/d_x]]_q$, where $\{d_z, d_x\} = \{d_1, d_2\}$.

Proof: We take $C = C_1^{\perp}$ in Theorem 3.2. Since $C_1^{\perp} \subseteq C_2$, we have $C_2 = C_1^{\perp} \oplus C'$, where C' is a subspace of C_2 and $\oplus$ is the direct sum so that $|C'| = \frac{|C_2|}{|C_1^{\perp}|} = q^{k_2 - (n - k_1)} = q^{k_2 + k_1 - n}$. Let $C' = \{v_1, \ldots, v_K\}$ where $K = q^{k_2 + k_1 - n}$. Then

$$d^{\perp} =: d(C^{\perp}) = d_1$$
$$d_v =: \min\{w_H(v_i - v_j + c) | 1 \le i \ne j \le K,\, c \in C\}$$
$$=: \min\{w_H(v + c) | 0 \ne v \in C',\, c \in C_1^{\perp}\} \ge d_2. \quad \square$$

By using Corollary 3.3, we can get a sequence of asymmetric MDS quantum codes for $d_x = d_z = 2$ as shown in the following result.

Corollary 3.4: Let $n \ge 3$. If $q \ge 3$, then there exists an asymmetric MDS quantum code with parameters $[[n, n - 2, 2/2]]_q$.

Proof: First, we prove the following claims.

For $n \ge 3, q \ge 3$, there exist nonzero elements $a_i, b_i \in \mathbb{F}_q$ $(1 \le i \le n)$ such that $a_1 b_1 + \cdots + a_{n-1} b_{n-1} + a_n b_n = 0$.

In order to prove the claim, we take any nonzero elements $a_i, b_i \in \mathbb{F}_q$ $(1 \le i \le n - 1)$. From $q \ge 3$, we have $\beta \in \mathbb{F}_q$ such that $\beta \ne 0$ and $\beta \ne a_1 b_1 + \cdots + a_{n-1} b_{n-1}$.

Then, we take nonzero elements a_n and $b_n \in \mathbb{F}_q$ such that $a_n b_n = -\beta (\ne 0)$ and we have $a_1 b_1 + \cdots + a_{n-1} b_{n-1} + a_n b_n = \beta - \beta = 0$.

Now we come back to the proof of this corollary.

For $q \ge 3$ and $n \ge 3$, by the claim, we have nonzero elements $a_i, b_i \in \mathbb{F}_q$ $(1 \le i \le n)$ such that $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n)$ are orthogonal vectors in $\mathbb{F}_q^n$. Let $C_1^{\perp}$ and $C_2^{\perp}$ be the 1-D subspaces of $\mathbb{F}_q^n$ spanned by a and b, respectively. The parameters of $C_i^{\perp}$ are $[n, 1, n]_q$ and the parameters of C_i are $[n, n - 1, 2]_q$ $(i = 1, 2)$. From $a \cdot b = a_1 b_1 + \cdots + a_n b_n = 0$, we have $C_1^{\perp} \subset C_2$. By Corollary 3.3, we get an AQC Q with parameters $[[n, k, 2/2]]_q$ $(i = 1, 2)$ with $k = (n - 1) + (n - 1) - n = n - 2$. Since $k + d_x + d_z - 2 = n - 2 + 2 + 2 - 2 = n$, we know that Q is an MDS code. □

Now we apply Theorem 3.2 to obtain Corollary 3.5.

Corollary 3.5: Let $d \ge 2$ be an integer and let $n \ge d$.

i) If $n - d$ is even, there exists a binary AQC with parameters $((n, K, 2/d))$, where

$$K = \sum_{i=0}^{\lfloor (n-d)/(2d) \rfloor} A(n, d, (n - d)/2 - di)$$

and $A(n, d, w)$ stands for the maximal cardinality of a binary constant weight code of length n, distance d, and weight w.

ii) If $n - d$ is odd, there exists a binary AQC with parameters $((n, K, 2/d))$, where

$$K = \sum_{i=0}^{\lfloor (n-d-1)/(2d) \rfloor} A(n, d, (n - d - 1)/2 - di).$$

Proof: Let C be the 1-D subspace of $\mathbb{F}_2^n$ generated by $(1, \ldots, 1)$. Then, $d^{\perp} = d(C^{\perp}) = 2$.

Let C_w denote the constant weight code of length n, weight w, minimum distance d, and size $A(n,d,w)$.

Define a set V as follows.

Case 1) $n-d$ is even

$$V := \bigcup_{0\le i\le (n-d)/(2d)} C_{(n-d)/2-di}.$$

Case 2) $n-d$ is odd:

$$V := \bigcup_{0\le i\le (n-d-1)/(2d)} C_{(n-d-1)/2-di}.$$

Let $V=\{v_1,\ldots,v_K\}$. If we can prove that

$$d_v = \min\{w_H(v_i - v_j + c) : 1 \le i \ne j \le K,\, c\in C\}$$

is at least d, then the desired result follows from Theorem 3.2.

We show this only for the case where $n-d$ is even. The other case can be proved by the same argument.

It is sufficient to show that the Hamming weight $w_H(v_i-v_j+c)$ is at least d for any v_i, v_j with $1\le i\ne j\le K$ and $c\in C$. We discuss it case by case.

Case 1) $c=(1,\ldots,1)$. Note that the Hamming weight of every vector in V is at most $(n-d)/2$. Thus, we have

$$\begin{aligned} &w_H(v_i-v_j+c)\\ &\quad\ge w_H(c)-w_H(v_i)-w_H(v_j)\\ &\quad\ge n-(n-d)/2-(n-d)/2=d. \end{aligned}$$

Case 2) $c=(0,\ldots,0)$. Both v_i and v_j belong to the same code C_w for some w. Then, $w_H(v_i-v_j+c)=w_H(v_i-v_j)$ is bigger than or equal to the minimum distance d of C_w.

Case 3) $c=(0,\ldots,0)$. v_i and v_j belong to two different codes $C_{(n-d)/2-ds}$ and $C_{(n-d)/2-dt}$, respectively, for some $0\le s<t\le (n-d)/(2d)$. Then, we have

$$\begin{aligned} &w_H(v_i-v_j+c)\\ &\quad= w_H(v_i-v_j)\ge w_H(v_i)-w_H(v_j)\\ &\quad= (n-d)/2-ds-((n-d)/2-dt)\\ &\quad= d(t-s)\ge d. \end{aligned}$$

This finishes the proof. □

Remark 3.6:

i) In Corollary 3.5, let $d=2$. Then, we have $A(n,2,w)=\binom{n}{w}$ and hence get a binary $((n,K,2/2))$-quantum code with

$$K=\begin{cases} 2^{n-2}, & \text{if } n \text{ is even}\\ 2^{n-2}-\frac{1}{2}\binom{n-1}{(n-1)/2}, & \text{if } n \text{ is odd.}\end{cases}$$

This result coincides with [7, Example 2.7].

ii) In Corollary 3.5, let $d=3$. Then, we have $A(n,4,w)\ge \binom{n}{w}/n$ (see [9]) and hence get a binary $((n,K,2/3))$-quantum code with

$$K=\begin{cases} \sum_{i=0}^{\lfloor (n-4)/6\rfloor}\binom{n}{(n-4)/2-3i}/n, & \text{if } n \text{ is even}\\ \sum_{i=0}^{\lfloor (n-3)/6\rfloor}\binom{n}{(n-3)/2-3i}/n, & \text{if } n \text{ is odd.}\end{cases}$$

IV. Asymptotically Good Asymmetric Quantum Codes From AG Codes

For a given pair (δ_x,δ_z) of real numbers and a family $\mathbb{Q}=\{((n^{(i)},K^{(i)},d_z^{(i)}/d_x^{(i)}))\}_{i=1}^{\infty}$ of asymptotic quantum codes with

$$\liminf_{i\to\infty}\frac{d_x^{(i)}}{n^{(i)}}\ge\delta_x,\qquad \liminf_{i\to\infty}\frac{d_z^{(i)}}{n^{(i)}}\ge\delta_z$$

we define the asymptotic quantity

$$R_{\mathbb{Q}}(\delta_x,\delta_z)=\limsup_{i\to\infty}\frac{\log_q K^{(i)}}{n^{(i)}}$$

where $\log_q$ denotes the logarithm to the base q. One of the central asymptotic problems for quantum codes is to find families $\mathbb{Q}$ of asymptotic quantum codes such that for a fixed pair (δ_x,δ_z), the value $R_{\mathbb{Q}}(\delta_x,\delta_z)$ is as large as possible.

In this section, we are mainly interested in the above asymptotic problem of AQCs. In particular, two asymptotic lower bounds on AQCs are given by applying algebraic geometry codes to Theorem 3.2 and Corollary 3.3, respectively.

Before proceeding to the asymptotic bounds from algebraic geometry codes, we recall some background on classical 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 vector space

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

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

$$\ell(G)\ge\deg(G)+1-g$$

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

Let $\mathcal{P}$ be a subset of $\mathcal{X}(\mathbb{F}_q)$ and label the points in $\mathcal{P}$ as follows:

$$\mathcal{P}=\{P_1,P_2,\ldots,P_n\}.$$

Choose a divisor G such that $\operatorname{Supp}(G)\cap\mathcal{P}=\emptyset$. Then, $\nu_{P_i}(f)\ge 0$ for all $1\le i\le n$ 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 $C_L(G;\mathcal{P})$.

Proposition 4.1 [17, Th. 3.1.1]: Let $\mathcal{X}/\mathbb{F}_q$ be an algebraic curve of genus g and let $\mathcal{P}$ be a set of n points on $\mathcal{X}$. Choose a divisor G with $g \le \deg(G) < n$ and $\mathrm{Supp}(G) \cap \mathcal{P} = \emptyset$. Then, $C_L(G;\mathcal{P})$ is an $[n,k,d]$-linear code over $\mathbb{F}_q$ with

$$k \ge \deg(G) - g + 1, \qquad d \ge n - \deg(G).$$

Moreover, the dimension k is equal to $\deg(G) - g + 1$ if $\deg(G) \ge 2g - 1$. Furthermore, the minimum distance $d(C_L^{\perp}(G;\mathcal{P}))$ of its dual code is at least $\deg(G) - 2g + 2$.

Proposition 4.2: If there is an algebraic curve $\mathcal{X}/\mathbb{F}_q$ with at least $n+1$ rational points and genus g, then one has a q-ary $[[n, \ell - m, d_z/d_x]]$-AQC with $d_z \ge m - 2g + 2$ and $d_x \ge n - \ell$ for any ℓ, m satisfying $2g - 2 < m < \ell < n$.

Proof: Let $P_0, P_1, \ldots, P_n$ be $n+1$ distinct rational points of $\mathcal{X}$. Putting $\mathcal{P} = \{P_1, \ldots, P_n\}$, $C_1^{\perp} = C_L(mP_0, \mathcal{P})$, $C_2 = C_L(\ell P_0, \mathcal{P})$ and applying Corollary 3.3, we obtain the desired result. □

Remark 4.3: If $\mathcal{X}/\mathbb{F}_q$ is the projective line, i.e., $g = 0$, then we get q-ary $[[n, n - d_x - d_z + 2, d_z/d_x]]$-asymptotic quantum MDS codes.

Let $N(\mathcal{X})$ denote the number of $\mathbb{F}_q$-rational points of a curve $\mathcal{X}/\mathbb{F}_q$ of genus $g(\mathcal{X})$. According to the Weil bound

$$N(\mathcal{X}) \le q + 1 + 2g(\mathcal{X})\sqrt{q}$$

the following two definitions make sense.

For any prime power q and any integer $g \ge 0$, put

$$N_q(g) := \max N(\mathcal{X})$$

where the maximum is extended over all curves $\mathcal{X}/\mathbb{F}_q$ with $g(\mathcal{X}) = g$.

We also define the following asymptotic quantity:

$$A(q) := \limsup_{g \to \infty} \frac{N_q(g)}{g}.$$

We know from [17] that $A(q) = \sqrt{q} - 1$ if q is a square.

Theorem 4.4: For a prime power q and a pair (δ_x, δ_z) of non-negative real numbers satisfying $\delta_x + \delta_z \le 1 - 2/A(q)$, there exists a family $\mathcal{Q}$ of asymptotic quantum codes from algebraic geometry codes such that

$$R_{\mathcal{Q}}(\delta_x, \delta_z) \ge 1 - \delta_x - \delta_z - \frac{2}{A(q)}. \qquad \text{(IV.1)}$$

Proof: Let $\{\mathcal{X}/\mathbb{F}_q\}$ be a family of curves such that $g(\mathcal{X}) \to \infty$ and $\limsup_{g(\mathcal{X})\to\infty} N(\mathcal{X})/g(\mathcal{X}) = A(q)$.

Define three families of integers $\{n = N(\mathcal{X}) - 1\}_{\mathcal{X}}$, $\{m = \lfloor \delta_z(N(\mathcal{X}) - 1) \rfloor + 2g - 2\}_{\mathcal{X}}$, and $\{\ell = n - \lfloor \delta_x(N(\mathcal{X}) - 1) \rfloor\}_{\mathcal{X}}$. Then, $n/g(\mathcal{X}) \to A(q)$, $(m - 2g + 2)/n \to \delta_z$, and $(n - \ell)/n \to \delta_x$.

By Proposition 4.2, from each curve $\mathcal{X}$ in the family, we can construct a q-ary $[[n, \ell - m, d_z/d_x]]$-AQC with $d_z \ge m - 2g + 2$ and $d_x \ge n - \ell$. Thus

$$\liminf_{i\to\infty} \frac{d_x}{n} \ge \delta_x, \qquad \liminf_{i\to\infty} \frac{d_z}{n} \ge \delta_z$$

and

$$\limsup_{i\to\infty} \frac{\ell - m}{n} \ge 1 - \delta_x - \delta_z - \frac{2}{A(q)}.$$

The proof is completed. □

By using the same techniques as in [7] and applying Theorem 3.2, we can improve the bound (IV.1) to the following.

Theorem 4.5: For a prime power q and a pair (δ_x, δ_z) of non-negative real numbers satisfying $\delta_x + \delta_z \le 1 - 2/A(q)$, there exists a family $\mathcal{Q}$ of asymptotic quantum codes from algebraic geometry codes such that

$$R_{\mathcal{Q}}(\delta_x, \delta_z) \ge 1 - \delta_x - \delta_z - \frac{2}{A(q)} + \log_q\left(1 + \frac{1}{q^3}\right). \qquad \text{(IV.2)}$$

We omit the proof of this theorem as one can use the same arguments as in the proof of [7, Th. 3.8].

Acknowledgment

The authors would like to thank the anonymous referee and the associate editor Prof. P. Hayden for their invaluable suggestions and comments. Without these suggestions and comments, this paper would not have appeared in the current form.

References

[1] S. A. Aly, "Quantum error control codes," Ph.D. dissertation, Dept. Comput. Sci., Texas A&M Univ., College Station, TX, 2008.

[2] S. A. Aly, "Asymmetric and symmetric subsystem BCH codes and beyond," 2008 [Online]. Available: arXiv:quant-ph/0803.0764v1

[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] I. L. Chuang, A. W. Cross, G. Smith, J. Smolin, and B. Zeng, "Codeword stabilized quantum codes: Algorithm and structure," 2008 [Online]. Available: arXiv:quant-ph/0803.3232v1

[5] L. E. Danielsen, "On self-dual quantum codes, graphs and Boolean functions," 2005 [Online]. Available: arXiv:quant-ph/0503236

[6] Z. W. E. Evans, A. M. Stephens, J. H. Cole, and L. C. L. Hollenberg, "Error correction optimisation in the presence of x/z asymmetry," 2007 [Online]. Available: arXiv:quant-ph/0709.3875

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

[8] K. Feng and C. P. Xing, "A new construction on quantum error-correcting codes," *Trans. Amer. Math. Soc.*, vol. 360, no. 2008, pp. 2007–2019.

[9] R. Graham and N. J. A. Sloane, "Lower bounds for constant weight codes," *IEEE Trans. Inf. Theory*, vol. IT-26, no. 1, pp. 37–43, Jan. 1980.

[10] L. Ioffe and M. M. Mézard, "Asymmetric quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 75, 2007, 032345.

[11] C. Riera and M. G. Parker, "Generalized bent criteria for Boolean functions (I)," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 4142–4159, Sep. 2006.

[12] P. K. Sarvepalli, M. Rotteler, and A. Klappennecker, "Asymmetric quantum LDPC codes," 2008 [Online]. Available: arXiv:quant-ph/08044316v1

[13] P. W. Shor, "Scheme for reducing decoherence in quantum memory," *Phys. Rev. A, Gen. Phys.*, vol. 52, no. 1995, pp. 2493–2496.

[14] A. M. Steane, "Multiple particle interference and quantum error correction," *Proc. R. Soc. Lond. A*, vol. 452, no. 1996, pp. 2551–2557.

[15] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, no. 5, pp. 793–797, 1996.
[16] A. M. Stephens, Z. W. E. Evans, S. J. Devitt, and L. C. L. Hollenberg, "Universal quantum computation under asymmetric quantum error correction," 2007 [Online]. Available: arXiv:quant-ph/0708.3969
[17] M. A. Tsfasman and S. G. Vladuţ, *Algebraic-Geometric Codes*. Amsterdam, The Netherlands: Kluwer, 1991.

Long Wang received the Ph.D. degree from Tsinghua University, Beijing, China, in 2009.

Since August 2009, he has been working at the Bank of Communication, China. His research interest mainly includes application of number theory to coding theory, especially to quantum codes.

Keqin Feng received the M.S. degree from the University of Science and Technology of China (USTC), Beijing, China, in 1968.

Since 1973, he has been with the Department of Mathematics, USTC, and then with the State Key Laboratory of Information Safety of USTC, Beijing, China. Currently, he is with the Department of Mathematical Science, Tsinghua University, Beijing, China. His current research interests include coding theory, cryptography, and algebraic number theory.

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.

Chaoping Xing received the Ph.D. degree from the University of Science and Technology of China (USTC), Beijing, China, in 1990.

From 1990 to 1993, he was a Lecturer and Associate Professor at USTC. He was with the University of Essen, Germany, as an Alexander von Humboldt Fellow from 1993 to 1995. After that, he spent most time at the Institute of Information Processing, Austrian Academy of Sciences, until 1998. From March of 1998 to November of 2007, he was with the National University of Singapore, Singapore. Since December of 2007, he has been with Nanyang Technological University, Singapore, and currently is a Full Professor. He has been working on the areas of algebraic curves over finite fields, coding theory, cryptography, and quasi-Monte Carlo methods.