International Journal of Quantum Information
Vol. 11, No. 3 (2013) 1350027 (10 pages)

DOI: 10.1142/S0219749913500275

PURE ASYMMETRIC QUANTUM MDS CODES FROM CSS CONSTRUCTION: A COMPLETE CHARACTERIZATION

MARTIANUS FREDERIC EZERMAN

Centre for Quantum Technologies,
National University of Singapore,
Block S15, 3 Science Drive 2, Singapore 117543,
Republic of Singapore
cqtmfe@nus.edu.sg
frederic.ezerman@gmail.com

SOMPHONG JITMAN[*,§], HAN MAO KIAH[†] and SAN LING[‡]

Division of Mathematical Sciences, School of Physical
and Mathematical Sciences,
Nanyang Technological University,
21 Nanyang Link, Singapore 637371,
Republic of Singapore
[*]*sjitman@ntu.edu.sg*
[†]*kiah0001@ntu.edu.sg*
[‡]*lingsan@ntu.edu.sg*

Received 2 November 2012
Revised 25 April 2013
Accepted 27 April 2013
Published 11 June 2013

Using the Calderbank−Shor−Steane (CSS) construction, pure q-ary asymmetric quantum error-correcting codes attaining the quantum Singleton bound are constructed. Such codes are called pure CSS asymmetric quantum maximum distance separable (AQMDS) codes. Assuming the validity of the classical maximum distance separable (MDS) Conjecture, pure CSS AQMDS codes of all possible parameters are accounted for.

Keywords: Asymmetric quantum codes; MDS codes; Singleton bound; generalized Reed-Solomon codes; weight distribution.

1. Introduction

The study of *asymmetric quantum codes* (*AQCs*) began when it was argued in Refs. 1 and 2 that, in many qubit systems, phase-flips (or Z-errors) occur more frequently

[§]Current address: Department of Mathematics, Faculty of Science, Silpakorn University, Nakhonpathom 73000, Thailand; somphong@su.ac.th than bit-flips (or X-errors) do. Steane first hinted the idea of adjusting the error-correction to the particular characteristics of the quantum channel in Ref. 3 and later, Wang *et al.* established a mathematical model of AQCs in the general qudit system in Ref. 4.

To date, the only known class of AQCs is given by the asymmetric version of the Calderbank–Shor–Steane (CSS) construction. In this paper, the CSS construction is used to derive a class of pure[a] AQCs attaining the quantum analogue of the Singleton bound. We call such optimal codes *asymmetric quantum maximum distance separable* (*AQMDS*) codes and if the codes are derived from the CSS construction, we call them CSS AQMDS codes.

Thus far, the only known AQMDS codes are pure CSS AQMDS and many results concerning these codes had been discussed in Ref. 6. This paper provides a complete treatment of such codes by solving the remaining open problems. This enables us to provide a complete characterization. To be precise, assuming the validity of the MDS conjecture, pure CSS AQMDS codes of all possible parameters are constructed.

The paper is organized as follows. In Sec. 2, we discuss some preliminary concepts and results. In Secs. 3 to 5, nested pairs of Generalized Reed–Solomon (GRS) codes and extended GRS codes are used to derive AQMDS codes of lengths up to $q+2$. Sec. 6 presents an alternative view on the construction of AQMDS codes based on the weights of maximum distance separable (MDS) codes. A summary is provided in Sec. 7.

2. Preliminaries

2.1. *Classical linear MDS codes*

Let q be a prime power and $\mathbb{F}_q$ the finite field having q elements. A *linear* $[n,k,d]_q$*-code* C is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$ with *minimum distance* $d := \min\{\mathrm{wt}(\mathbf{v}) : \mathbf{v} \in C\setminus\{\mathbf{0}\}\}$, where $\mathrm{wt}(\mathbf{v})$ denotes the *Hamming weight* of $\mathbf{v} \in \mathbb{F}_q^n$. Given two distinct linear codes C and D, $\mathrm{wt}(C\setminus D)$ denotes $\min\{\mathrm{wt}(\mathbf{u}) : \mathbf{u} \in C\setminus D\}$.

Every $[n,k,d]_q$-code C satisfies the Singleton bound

$$d \leq n - k + 1,$$

and C is said to be *maximum distance separable* if $d = n-k+1$. Trivial families of MDS codes include the vector space $\mathbb{F}_q^n$, the codes equivalent to the $[n,1,n]_q$-repetition code and their duals $[n,n-1,2]_q$ for positive integers $n \geq 2$.

MDS codes which are not equivalent to the trivial ones are said to be *nontrivial*. Furthermore, we have the following conjecture which has been shown to be true when q is prime in Ref. 7.

Conjecture 1 (MDS Conjecture). *If there is a nontrivial* $[n,k,d]_q$*-MDS code, then* $n \leq q+1$, *except when* q *is even and* $k = 3$ or $k = q-1$ *in which case* $n \leq q+2$.

[a]Purity in the CSS case is defined in Theorem 2.

For $\mathbf{u} = (u_i)_{i=1}^n$ and $\mathbf{v} = (v_i)_{i=1}^n$, $\langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{E}} := \sum_{i=1}^n u_i v_i$ is the *Euclidean inner product* of $\mathbf{u}$ and $\mathbf{v}$. With respect to this inner product, the *dual* $C^\perp$ of C is given by

$$C^\perp := \{\mathbf{u} \in \mathbb{F}_q^n : \langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{E}} = 0 \text{ for all } \mathbf{v} \in C\}.$$

It is well known that $(C^\perp)^\perp = C$ and that the dual of an MDS code is MDS.

Let $\mathbb{F}_q[X]_k$ denote the set of all polynomials of degree less than k in $\mathbb{F}_q[X]$. The set $\{1, x, \ldots, x^{k-1}\}$ forms the standard basis for $\mathbb{F}_q[X]_k$ as a vector space over $\mathbb{F}_q$.

2.2. *CSS construction and AQMDS codes*

We begin with a formal definition of an AQC.

Definition 1. Let d_x and d_z be positive integers. A quantum code Q in $V_n = (\mathbb{C}^q)^{\otimes n}$ with dimension $K \geq 1$ is called an *asymmetric quantum code* with parameters $((n, K, d_z/d_x))_q$ or $[[n, k, d_z/d_x]]_q$, where $k = \log_q K$, if Q detects $d_x - 1$ qudits of bit-flips (or X-errors) and, at the same time, $d_z - 1$ qudits of phase-flips (or Z-errors).

The correspondence between pairs of classical linear codes and AQCs is given in Refs. 4 and 5.

Theorem 2 (Standard CSS Construction for AQC). *Let C_i be linear codes with parameters $[n, k_i, d_i]_q$ for $i = 1, 2$ with $C_1^\perp \subseteq C_2$. Let*

$$\begin{aligned} d_z &:= \max\{\mathrm{wt}(C_2 \backslash C_1^\perp), \mathrm{wt}(C_1 \backslash C_2^\perp)\} \quad \textit{and} \\ d_x &:= \min\{\mathrm{wt}(C_2 \backslash C_1^\perp), \mathrm{wt}(C_1 \backslash C_2^\perp)\}. \end{aligned} \tag{1}$$

Then there exists an AQC Q with parameters $[[n, k_1 + k_2 - n, d_z/d_x]]_q$. The code Q is said to be *pure* whenever $\{d_z, d_x\} = \{d_1, d_2\}$.

For a CSS AQC, the purity in Theorem 2 is equivalent to the general definition given in Ref. 4.

Furthermore, any CSS $[[n, k, d_z/d_x]]_q$-AQC satisfies the following bound [8, Lemma 3.3],

$$k \leq n - d_x - d_z + 2. \tag{2}$$

This bound is conjectured to hold for all AQCs. A quantum code is said to be *AQMDS* if it attains the equality in (2).

For our construction, the following result holds.

Lemma 1 ([4, Corollary 2.5]). *A pure CSS AQC is an asymmetric quantum MDS code if and only if both C_1 and C_2 in Theorem 2 are* (*classical*) *MDS codes.*

This means that constructing a pure q-ary CSS AQMDS code of a specific set of parameters is equivalent to finding a suitable corresponding nested pair of classical $\mathbb{F}_q$-linear MDS codes.

Following Lemma 1, a CSS AQMDS code is said to be *trivial* if both C_1 and C_2 are trivial MDS codes.

From Lemma 1 and the MDS conjecture, the following necessary condition for the existence of a nontrivial pure CSS AQMDS code is immediate.

Proposition 1. *Assuming the validity of the MDS Conjecture, every nontrivial pure q-ary CSS AQMDS code has length $n \leq q+1$ if q is odd and $n \leq q+2$ if q is even.*

Let Q be an AQC with parameters $[[n, k, d_z/d_x]]_q$. We usually require $k > 0$ (equivalently, $K = q^k > 1$) or for error detection purposes, $d_x \geq 2$. However, for completeness, we state the results for the two cases: first, when $d_x = 1$ and second, when $k = 0$.

Proposition 2. *Let n, k be positive integers such that $k \leq n-1$. A pure CSS AQMDS code with parameters $[[n, k, d_z/1]]_q$ where $d_z = n-k+1$ exists if and only if there exists an MDS code with parameters $[n, k, n-k+1]_q$.*

Proof. We show only one direction. Let C be an MDS code with parameters $[n, k, n-k+1]_q$. Apply Theorem 2 with $C_1 = C$ and $C_2 = \mathbb{F}_q^n$ to obtain the required AQMDS code. □

Proposition 3. *Let n, k be positive integers such that $k \leq n-1$. A pure CSS AQMDS code with parameters $[[n, 0, d_z/d_x]]_q$ where $\{d_z, d_x\} = \{n-k+1, k+1\}$ exists if and only if there exists an MDS code with parameters $[n, k, n-k+1]_q$.*

Proof. Again, we show one direction. Let C be an MDS code with parameters $[n, k, n-k+1]_q$ and let $C_1^{\perp} = C_2 = C$. Following Ref. 9, assume that a quantum code with $K = 1$ is pure and hence, there exists an AQMDS with parameters $[[n, 0, d_z/d_x]]_q$ where $\{d_z, d_x\} = \{n-k+1, k+1\}$. □

In the subsequent sections, pure CSS AQMDS codes with $k \geq 1$ and $d_x \geq 2$ are studied.

3. AQMDS Codes of Length $n \leq q$

Let us recall some basic results on GRS codes (see Ref. 10, Sec. 5.3). Choose n distinct elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ in $\mathbb{F}_q$ and define $\boldsymbol{\alpha} := (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Let $\mathbf{v} := (v_1, v_2, \ldots, v_n)$, where $v_1, v_2, \ldots, v_n$ are nonzero elements in $\mathbb{F}_q$. Then, given $\boldsymbol{\alpha}$ and $\mathbf{v}$, a GRS code of length $n \leq q$ and dimension $k \leq n$ is defined as

$$\mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v}) := \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) : f(X) \in \mathbb{F}_q[X]_k\}.$$

Since $\mathbb{F}_q[X]_k \subset \mathbb{F}_q[X]_{k+1}$ for fixed $n, \mathbf{v}$, and $\boldsymbol{\alpha}$, it follows immediately that

$$\mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v}) \subset \mathcal{GRS}_{n,k+1}(\boldsymbol{\alpha}, \mathbf{v}). \tag{3}$$

Based on the standard basis for $\mathbb{F}_q[X]_k$, a generator matrix G for $\mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v})$ is given by

$$G = \begin{pmatrix} v_1 & v_2 & \dots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \dots & v_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \dots & v_n\alpha_n^{k-1} \end{pmatrix} \tag{4}$$

and $\mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v})$ is an MDS code with parameters $[n, k, n-k+1]_q$. Hence, the following result gives a construction of an AQMDS code of length $n \leq q$.

Theorem 3. *Let $q \geq 3$. Let n, k and j be positive integers such that $n \leq q$, $k \leq n-2$ and $j \leq n-k-1$. Then there exists a nontrivial AQMDS code with parameters $[[n, j, d_z/d_x]]_q$ where $\{d_z, d_x\} = \{n-k-j+1, k+1\}$.*

Proof. Apply Theorem 2 with $C_1^{\perp} = (\mathcal{GRS}_{n,k}(\boldsymbol{\alpha}, \mathbf{v})) \subset C_2 = \mathcal{GRS}_{n,k+j}(\boldsymbol{\alpha}, \mathbf{v})$. $\square$

4. AQMDS Codes of Length $n = q + 1$

Let $\alpha_1, \alpha_2, \dots, \alpha_q$ be distinct elements in $\mathbb{F}_q$ and $v_1, v_2, \dots, v_{q+1}$ be nonzero elements in $\mathbb{F}_q$. Let $k \leq q$ and consider the code E given by

$$E := \left\{ (v_1 f(\alpha_1), \dots, v_q f(\alpha_q), v_{q+1} f_{k-1}) : f(X) = \sum_{i=0}^{k-1} f_i X^i \in \mathbb{F}_q[X]_k \right\}.$$

Let $\mathbf{x} = (0, \dots, 0, v_{q+1})$ and G be as in (4) with $n = q$. Then $G_E := (G|\mathbf{x}^{\mathrm{T}})$ is a generator matrix of E. The code E is an extended GRS code with parameters $[q+1, k, q-k+2]_q$ (see Ref. 10, Sec. 5.3).

Let $1 \leq r \leq k-2$. Then there exists a monic irreducible polynomial $p(X) \in \mathbb{F}_q[X]$ of degree $k-r$ [Ref. 11, Corollary 2.11]. By the choice of $p(X)$, observe that $p(\alpha_i) \neq 0$ for all i. Hence, the matrix

$$G_C = \begin{pmatrix} v_1 p(\alpha_1) & \dots & v_q p(\alpha_q) & 0 \\ v_1\alpha_1 p(\alpha_1) & \dots & v_q\alpha_q p(\alpha_q) & 0 \\ \vdots & \ddots & \vdots & \vdots \\ v_1\alpha_1^{r-2} p(\alpha_1) & \dots & v_q\alpha_q^{r-2} p(\alpha_q) & 0 \\ v_1\alpha_1^{r-1} p(\alpha_1) & \dots & v_q\alpha_q^{r-1} p(\alpha_q) & v_{q+1} \end{pmatrix} \tag{5}$$

is a generator matrix of a $[q+1, r, q-r+2]_q$-MDS code C.

Observe that, for all $g(X) \in \mathbb{F}_q[X]_r$, $p(X)g(X)$ is also a polynomial in $\mathbb{F}_q[X]_k$. Moreover, the coefficient of X^{k-1} in $p(X)g(X)$ is given by the coefficient of X^{r-1} in $g(X)$. Thus, $C \subset E$, leading to the following construction of AQMDS code of length $q+1$.

Theorem 4. *Let $q \geq 3$. Let j, k be positive integers such that $3 \leq k \leq q$ and $2 \leq j \leq k-1$. Then there exists an AQMDS code with parameters $[[q+1, j, d_z/d_x]]_q$ where $\{d_z, d_x\} = \{q-k+2, k-j+1\}$.*

Proof. Let $r = k - j$. Apply Theorem 2 with $C_1 = C^{\perp}$ and $C_2 = E$. □

Note that Theorem 4 gives AQMDS codes with parameters $[[q+1, j, d_z/d_x]]_q$ with $j \geq 2$. The next proposition gives the necessary and sufficient conditions for the existence of pure CSS AQMDS codes with $j = 1$.

Proposition 4. *Let n, k be positive integers such that $k \leq n-1$. There exists a pair of nested MDS codes $C \subset C'$ with parameters $[n, k, n-k+1]_q$ and $[n, k+1, n-k]_q$, respectively, if and only if there exists an MDS code with parameters $[n+1, k+1, n-k+1]_q$.*

Equivalently, there exists a pure CSS AQMDS code with parameters $[[n, 1, d_z/d_x]]_q$ where $\{d_z, d_x\} = \{n-k, k+1\}$ if and only if there exists an MDS code with parameters $[n+1, k+1, n-k+1]_q$.

Proof. Let G be a generator matrix of C. Pick $\mathbf{w} \in C' \backslash C$ and observe that $\left(\frac{G}{\mathbf{w}}\right)$ is agenerator matrix for C'. It can be verified that

$$\left(\begin{array}{c|c} \mathbf{0} & G \\ \hline 1 & \mathbf{w} \end{array}\right)$$

is a generator matrix of an $[n+1, k+1, n-k+1]_q$-MDS code.

Conversely, let D be an $[n+1, k+1, n-k+1]_q$-MDS code with $k \leq n-1$. Shortening the code D at the last coordinate yields an $[n, k, n-k+1]_q$-MDS code C. Puncturing the code D at the last coordinate gives an $[n, k+1, n-k]_q$-MDS code C'. A quick observation confirms that $C \subset C'$. □

This proposition leads to the following characterization.

Corollary 1. *Assuming the validity of the MDS conjecture, there exists a pure CSS AQMDS code with parameters $[[q+1, 1, d_z/d_x]]_q$ if and only if q is even and $\{d_z, d_x\} = \{3, q-1\}$.*

Proof. There exists a $[2^m+2, 3, 2^m]_{2^m}$-MDS code (see Ref. 12, Ch. 11, Theorem 10). By Proposition 4, an AQMDS code with the indicated parameters exists.

The necessary condition follows from combining the MDS conjecture and Proposition 4. Assume that there exists a $[[q+1, 1, d_z/d_x]]_q$-AQMDS code Q with $d_x \geq 2$. If q is odd, the existence of Q would imply the existence of a nontrivial MDS code of length $q+2$, contradicting the MDS conjecture. For even q, suppose $\{d_z, d_x\} \neq \{q-1, 3\}$. Without loss of generality, assume $d_z \geq d_x \neq 3$. Then there exists a nested pair $[q+1, q+1-d_x, d_x+1]_q \subset [q+1, q+2-d_x, d_x]_q$. By Proposition 4, there exists a $[q+2, q+2-d_x, d_x+1]_q$-MDS code. If $d_x = 2$, then

$q+2-d_x = q \notin \{3, q-1\}$, contradicting the MDS conjecture. If $d_x > 3$, then $d_z < q-1$ and $3 < q+2-d_z \leq q+2-d_x < q-1$, a contradiction to the MDS conjecture. □

5. AQMDS Codes of Length $n = 2^m + 2 \geq 6$ with $d_z = d_x = 4$

MDS codes of length $q+2$ are known to exist for $q = 2^m$, and $k \in \{3, 2^m - 1\}$ (see Ref. 12, Ch. 11, Theorem 10). Let $v_1, v_2, \ldots, v_{q+2}$ be nonzero elements in $\mathbb{F}_q$ and fix $\alpha_q = 0$ in the notations of Sec. 3.

For $m \geq 2$, a generator matrix for $k = 3$ or a parity check matrix for $k = 2^m - 1$ is given by

$$H = \begin{pmatrix} v_1 & \cdots & v_{q-1} & v_q & 0 & 0 \\ v_1\alpha_1 & \cdots & v_{q-1}\alpha_{q-1} & 0 & v_{q+1} & 0 \\ v_1\alpha_1^2 & \cdots & v_{q-1}\alpha_{q-1}^2 & 0 & 0 & v_{q+2} \end{pmatrix}. \tag{6}$$

Let C be a $[2^m+2, 2^m-1, 4]_{2^m}$-code with parity check matrix H given in (6). Let D be the $[2^m+2, 3, 2^m]_{2^m}$-code whose generator matrix G is given by

$$G = \begin{pmatrix} v_1^{-1} & \cdots & v_{q-1}^{-1} & v_q^{-1} & 0 & 0 \\ v_1^{-1}\alpha_1^{-1} & \cdots & v_{q-1}^{-1}\alpha_{q-1}^{-1} & 0 & v_{q+1}^{-1} & 0 \\ v_1^{-1}\alpha_1^{-2} & \cdots & v_{q-1}^{-1}\alpha_{q-1}^{-2} & 0 & 0 & v_{q+2}^{-1} \end{pmatrix}. \tag{7}$$

The following theorem gives a construction of an AQMDS code of length $q+2$.

Theorem 5. *Let $q = 2^m \geq 4$. Then there exists an AQMDS code with parameters $[[2^m+2, 2^m-4, 4/4]]_{2^m}$.*

Proof. First we prove that $D \subset C$ by showing that $M = (m_{i,j}) := GH^T = \mathbf{0}$. Note that

$$m_{i,j} = \sum_{l=1}^{q+2} g_{i,l} \cdot h_{j,l}$$

for $1 \leq i, j \leq 3$. If $i = j$, then $m_{i,j} = q = 0$. If $i \neq j$, the desired conclusion follows since

$$\sum_{i=1}^{q-1} \alpha_i = \sum_{i=1}^{q-1} \alpha_i^{-1} = 0 \quad \text{and} \quad \sum_{i=1}^{q-1} \alpha_i^{-2} = \sum_{i=1}^{q-1} \alpha_i^2 = \left(\sum_{i=1}^{q-1} \alpha_i \right)^2 = 0.$$

Applying Theorem 2 with $C_1 = D^\perp$ and $C_2 = C$ completes the proof. □

6. AQMDS Codes with $d_z \geq d_x = 2$, an Alternative Look

In the previous sections, suitable pairs of GRS or extended GRS codes were chosen for the CSS construction. This section singles out the case of $d_x = 2$ where the particular type of the MDS code chosen is inessential. The following theorem gives a construction on an AQC with $d_x = 2$.

Theorem 6 ([Ref. 6 Theorem 7]). *Let C be a linear (not necessarily MDS) $[n, k, d]_q$-code with $k \geq 2$. If C has a codeword $\mathbf{u}$ such that $\mathrm{wt}(\mathbf{u}) = n$, then there exists an $[[n, k-1, d/2]]_q$-AQC.*

Let C be an $[n, k, n-k+1]_q$-MDS code. Ezerman *et al.* in Ref. 13 showed that C has a codeword $\mathbf{u}$ with $\mathrm{wt}(\mathbf{u}) = n$, except when either C is the dual of the binary repetition code of odd length $n \geq 3$, or C is a simplex code with parameters $[q+1, 2, q]_q$. Hence, the following corollary can be derived.

Corollary 2. *The following statements hold:*

(1) *For even integers n, there exists an $[[n, n-2, 2/2]]_2$-AQMDS code.*
(2) *For positive integers $n, q \geq 3$, there exists an $[[n, n-2, 2/2]]_q$-AQMDS code.*
(3) *Given positive integers $q \geq n \geq 4$, there exists an AQMDS code for $2 \leq k \leq n-2$ with parameters $[[n, k-1, d_z/2]]_q$ with $d_z = n-k+1$.*
(4) *Given $q \geq 4$, there exists an AQMDS code for $3 \leq k \leq q-1$ with parameters $[[q+1, k-1, d_z/2]]_q$ with $d_z = q-k+2$.*
(5) *Given positive integer $m \geq 2$ and $q = 2^m$, there exists an AQMDS code with parameters $[[2^m+2, 2, 2^m/2]]_{2^m}$ and an AQMDS code with parameters $[[2^m+2, 2^m-2, 4/2]]_{2^m}$.*

Wang *et al.* (Ref. 4, Corollary 3.4) gave a different proof of the existence of $[[n, n-2, 2/2]]_q$-AQMDS codes Q for $n, q \geq 3$.

In this section, it is shown for $d_x = 2$ that the specific construction of the classical MDS codes used in the CSS construction is inconsequential. This is useful as there are many classical MDS codes which are not equivalent to the GRS codes (see Ref. 14, for instance).

7. Summary

While the ingredients to construct a pure AQC under the CSS construction, namely a pair of nested codes, the knowledge on the codimension and the dual distances of the codes, are all classical, computing the exact set of parameters and establishing the optimality of the resulting AQC are by no means trivial.

This work shows how to utilize the wealth of knowledge available regarding classical MDS codes to completely classify under which conditions there exists a particularly pure CSS AQMDS code and how to construct such a code explicitly. Outside the MDS framework, more work needs to be done in determining the exact values of d_x and d_z and in establishing optimality.

We summarize the results of the paper in the following theorem.

Theorem 7. *Let q be a prime power, n, k be positive integers and j be a nonnegative integer. Assuming the validity of the MDS conjecture, there exists a pure CSS*

AQMDS code with parameters $[[n,j,d_z/d_x]]_q$, *where* $\{d_z,d_x\} = \{n-k-j+1, k+1\}$ *if and only if one of the following holds*:

(1) [*Proposition* 2, *Proposition* 3] q *is arbitrary*, $n \geq 2$, $k \in \{1, n-1\}$ *and* $j \in \{0, n-k\}$.
(2) [*Corollary* 2] $q = 2$, n *is even*, $k = 1$ *and* $j = n-2$.
(3) [*Corollary* 2] $q \geq 3$, $n \geq 2$, $k = 1$ *and* $j = n-2$.
(4) [*Proposition* 2, *Proposition* 3, *Theorem* 3] $q \geq 3$, $2 \leq n \leq q$, $k \leq n-1$ *and* $0 \leq j \leq n-k$.
(5) [*Proposition* 2, *Proposition* 3, *Theorem* 4] $q \geq 3$, $n = q+1$, $k \leq n-1$ *and* $j \in \{0, 2, \ldots, n-k\}$.
(6) [*Corollary* 1] $q = 2^m$, $n = q+1$, $j = 1$ *and* $k \in \{2, 2^m - 2\}$.
(7) [*Proposition* 2, *Proposition* 3, *Theorem* 5, *Corollary* 2] $q = 2^m$ *where* $m \geq 2$, $n = q+2$,

$$\begin{cases} k = 1, \quad \text{and} \quad j \in \{2, 2^m - 2\}, \\ k = 3, \quad \text{and} \quad j \in \{0, 2^m - 4, 2^m - 1\}, \quad \text{or}, \\ k = 2^m - 1, \quad \text{and} \quad j \in \{0, 3\}. \end{cases}$$

As a concluding remark, note that all AQMDS codes constructed here are pure CSS codes. The existence of a degenerate CSS AQMDS code or an AQMDS code derived from non-CSS method with parameters different from those in Theorem 7 remains an open question.

Acknowledgments

The authors thank Markus Grassl for useful discussions and for suggesting Proposition 4. The work of S. Jitman was supported by the Institute for the Promotion of Teaching Science and Technology of Thailand. The work of all of the authors is partially supported by Singapore National Research Foundation Competitive Research Program Grant NRF-CRP2-2007-03.

References

1. Z. W. E. Evans *et al.*, Error correction optimisation in the presence of x/z asymmetry, quant-ph/07093875.
2. L. Ioffe and M. M. Mézard, *Phys. Rev. A* **75** (2007) 032345.
3. A. M. Steane, *Proc. R. Soc. A* **452** (1996) 2551.
4. L. Wang *et al.*, *IEEE Trans. Inform. Theory* **56** (2010) 2938.
5. S. A. Aly and A. Ashikhmin, Nonbinary quantum cyclic and subsystem codes over asymmetrically decohered quantum channels, in *Proc. IEEE Inform. Theory Workshop*, Dublin, Ireland (2010), pp. 1–5.
6. M. F. Ezerman *et al.*, Pure asymmetric quantum MDS codes from CSS construction, in *Proc. 3rd International Castle Meeting on Coding Theory and Applications (3ICMCTA)*, Castell de Cardona Spain, 11–15 September 2011 (Servei de Publicacions de la Universitat Autònoma de Barcelona, 2011), pp. 97–102.

7. S. Ball, *J. Eur. Math. Soc.* **14** (2012) 733.
8. P. K. Sarvepalli *et al.*, *Proc. R. Soc. A* **465** (2009) 1645.
9. A. R. Calderbank *et al.*, *IEEE Trans. Inform. Theory* **44** (1998) 1369.
10. W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes* (Cambridge University Press, Cambridge, 2003).
11. R. Lidl and H. Niederreiter, *Finite Fields (Encyclopedia Math. Appl. 20)* (Cambridge University Press, Cambridge, 1997).
12. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1977).
13. M. F. Ezerman *et al.*, *IEEE Trans. Inform. Theory* **57** (2011) 392.
14. R. M. Roth and A. Lempel, *IEEE Trans. Inform. Theory* **35** (1989) 655.