CSS-like constructions of asymmetric quantum codes

Ezerman, Martianus Frederic; Jitman, Somphong; Ling, San; Pasechnik, Dmitrii V.

2013

Ezerman, M. F., Jitman, S., Ling, S., & Pasechnik, D. V. (2013). CSS-like constructions of asymmetric quantum codes. IEEE Transactions on Information Theory, 59(10), 6732-6754. doi:10.1109/TIT.2013.2272575

https://hdl.handle.net/10356/100356

https://doi.org/10.1109/TIT.2013.2272575

CSS-like Constructions of Asymmetric Quantum Codes

Martianus Frederic Ezerman, *Member, IEEE*, Somphong Jitman, San Ling, and Dmitrii V. Pasechnik

***Abstract*—Asymmetric quantum error-correcting codes (AQCs) may offer some advantage over their symmetric counterparts by providing better error-correction for the more frequent error types. The well-known CSS construction of q-ary AQCs is extended by removing the $\mathbb{F}_q$-linearity requirement as well as the limitation on the type of inner product used. The proposed constructions are called *CSS-like constructions* and utilize pairs of nested subfield linear codes under one of the Euclidean, trace Euclidean, Hermitian, and trace Hermitian inner products.**

After establishing some theoretical foundations, best-performing CSS-like AQCs are constructed. Combining some constructions of nested pairs of classical codes and linear programming, many optimal and good pure q-ary CSS-like codes for $q \in \{2,3,4,5,7,8,9\}$ up to reasonable lengths are found. In many instances, removing the $\mathbb{F}_q$-linearity and using alternative inner products give us pure AQCs with improved parameters than relying solely on the standard CSS construction.

***Index Terms*—asymmetric quantum codes, best-known linear codes, Delsarte bound, group character codes, cyclic codes, inner products, linear programming bound, quantum Singleton bound, subfield linear codes**

I. Introduction

Most of the work to date on quantum error-correcting codes (quantum codes) assumes that the quantum channel is symmetric, *i.e.*, the different types of errors are assumed to occur equiprobably. However, recent papers (see [13] and [20], for instance) argue that in many qubit systems, phase-flips (or Z-errors) occur more frequently than bit-flips (or X-errors). This leads to the idea of adjusting the error-correction to the particular characteristics of the quantum channel and codes that take advantage of the asymmetry are called *asymmetric quantum codes* (AQCs).

Steane first hinted at this concept in [31]. Some results on mostly binary AQCs can be found in [1] and in [30]. While at the moment there is no general agreement on the most appropriate error models for non-qubit asymmetric channels, the most established mathematical model in the general qudit systems available is that of Wang *et al.* [33].

In the symmetric framework, Steane's seminal work [31] and that of Calderbank and Shor [7] provided the connection between a pair of classical codes and a class of quantum stabilizer codes. The construction is now known as the CSS construction which extends naturally to the asymmetric case. In [2] Aly and Ashikhmin supply a proof by modifying Steane's original proof.

Using a functional approach, a general mathematical characterization and some constructions of AQCs from which the CSS construction for AQCs can be derived are given in [33]. The results have been extended to include constructions from $\mathbb{F}_r$-linear codes over its quadratic extension $\mathbb{F}_{r^2}$ in [11] under the trace Hermitian inner product.

This present work provides the following contributions:

1) We extend the functional approach to include the so-called CSS-like constructions based on pairs of nested $\mathbb{F}_r$-linear codes over $\mathbb{F}_q$ where $\mathbb{F}_r$ is any subfield of $\mathbb{F}_q$. At the same time we relax the condition on the inner product used. It is shown that given the appropriate context, the Hermitian, trace Hermitian, and trace Euclidean inner products can be utilized as well.
2) The extensions lead to pure AQCs with better parameters than relying solely on the best ones obtainable from the standard CSS construction. This justifies the effort of considering $\mathbb{F}_r$-linear pairs of nested codes over $\mathbb{F}_q$ and their duals under various inner products.
3) Of purely mathematical interest, our investigation leads to a better structural understanding of the functional approach to AQCs. A diagram detailing the relationships among different CSS-like constructions is given in Section III.
4) Lists of good pure CSS-like AQCs up to some computationally reasonable lengths for $q \in \{2,3,4,5,7,8,9\}$ are given.

The paper is organized into seven sections and four appendices. After this introductory section, some preliminary notions from classical coding theory and some basics on the AQC error model are given in Section II. Section III accomplishes several important tasks. First, a brief review of

M. F. Ezerman was with Laboratoire d'Information Quantique, CP 225, Université Libre de Bruxelles, Av. F. D. Roosevelt 50, B-1050 Belgium. He is now with Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543 (email: frederic.ezerman@gmail.com).

S. Jitman was with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371, Republic of Singapore. He recently joined Department of Mathematics, Faculty of Science, Silpakorn University, Nakhonpathom 73000, Thailand (email: somphong@su.ac.th).

S. Ling, and D. V. Pasechnik are with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371, Republic of Singapore (emails:{lingsan, dima}@ntu.edu.sg).

The work of M. F. Ezerman, S. Jitman and S. Ling was partially supported by Singapore National Research Foundation Competitive Research Program Grant NRF-CRP2-2007-03. D. V. Pasechnik's work was supported by Tier 1 Nanyang Technological University/Singapore Ministry of Education Grant No. RG60/08. M. F. Ezerman and S. Jitman benefitted from travel grants provided through the Merlion Project No.1.02.10 by the Embassy of France in Singapore.

both the standard CSS construction and the functional characterization of AQCs is supplied for convenience. The CSS-like constructions are then proved and their interconnections are shown.

Three systematic constructions of nested pairs of linear and subfield linear codes are presented in Section IV as main ingredients for the CSS-like constructions. A linear programming bound as a measure of the optimality of AQCs is derived in Section V. Combining the results of these two sections, good pure CSS-like codes are listed explicitly with their corresponding pair of nested classical codes in Section VI. The last section contains some conclusion and open problems. The appendices establish results needed in the paper whose detailed justifications may distract us from the paper's main lines of thought.

II. Preliminaries

Throughout this work, let p be a prime number and let $\mathbb{F}_p \subseteq \mathbb{F}_r \subseteq \mathbb{F}_q$ with $r = p^l$ and $q = r^m$ be finite fields. The trace mapping $\mathrm{Tr}_{q/r} : \mathbb{F}_q \to \mathbb{F}_r$ is given by $\mathrm{Tr}_{q/r}(\beta) = \beta + \beta^r + \beta^{r^2} + \ldots + \beta^{r^{m-1}}$. The subscript q/r is omitted whenever $r = p$ and q is clear. Important properties of the trace mapping can be found in [23, Th. 2.23].

If $q = r^2$, let $\overline{a}$ denote a^r for all $a \in \mathbb{F}_q$. For $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_q^n$, $\overline{\mathbf{u}}$ stands for $(\overline{u_1}, \overline{u_2}, \ldots, \overline{u_n})$. Hence, for any nonempty set $C \subseteq \mathbb{F}_q^n$, $\overline{C} := \{\overline{\mathbf{c}} : \mathbf{c} \in C\}$.

A. Coding Theory

Given $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$, let $\mathrm{wt_H}(\mathbf{v})$ denote the *Hamming weight* of $\mathbf{v}$ and $\mathrm{dist}(\mathbf{u}, \mathbf{v})$ denote their *Hamming distance*. A code C of length n over $\mathbb{F}_q$ is a nonempty subset of $\mathbb{F}_q^n$. The *minimum distance* $d(C)$ is given by

$$d(C) = \min\{\mathrm{dist}(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}\}.$$

For two distinct codes C and D, $\mathrm{wt_H}(C \setminus D)$ denotes $\min\{\mathrm{wt_H}(\mathbf{u}) : \mathbf{u} \in C \setminus D, \mathbf{u} \neq \mathbf{0}\}$.

An $[n, k, d]_q$-linear code C is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$ with minimum distance d. For a general, not necessarily $\mathbb{F}_q$-linear, code $C \subseteq \mathbb{F}_q^n$, the notation $(n, M = |C|, d)_q$ is commonly used. A code C is an *$\mathbb{F}_r$-linear code over $\mathbb{F}_q$* if C is a subspace of the $\mathbb{F}_r$-vector space $\mathbb{F}_q^n$. When r is clear from the context, C is said to be a *subfield linear code* over $\mathbb{F}_q$.

For $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ in $\mathbb{F}_q^n$, we define the following inner products:

1) $\langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{E}} := \sum_{i=1}^{n} u_i v_i$ is the *Euclidean inner product* of $\mathbf{u}$ and $\mathbf{v}$.
2) $\langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{Tr}_{q/r}\,\mathrm{E}} := \mathrm{Tr}_{q/r}\left(\langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{E}}\right)$ is the *trace Euclidean inner product* of $\mathbf{u}$ and $\mathbf{v}$ valued in $\mathbb{F}_r$.
3) When $\mathbb{F}_q$ is a quadratic extension of $\mathbb{F}_r$, $\langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{H}} := \sum_{i=1}^{n} u_i \overline{v_i} = \langle \mathbf{u}, \overline{\mathbf{v}} \rangle_{\mathrm{E}}$ is the *Hermitian inner product* of $\mathbf{u}$ and $\mathbf{v}$.
4) Let $q = r^2$. Then there are two cases of *trace Hermitian inner product* depending on the field characteristic:
   a) For even q, $\langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{Tr}_{q/r}\mathrm{H}} := \mathrm{Tr}_{q/r}(\langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{H}})$.
   b) For odd q, $\langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{Tr}_{q/r}\mathrm{H}} := \mathrm{Tr}_{q/r}(\alpha \langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{H}})$ where $\alpha \in \mathbb{F}_q \setminus \{0\}$ is such that $\overline{\alpha} = -\alpha$.

Let $C \subseteq \mathbb{F}_q^n$ be a code. Let $*$ represent one of the Euclidean, trace Euclidean, Hermitian and trace Hermitian inner products, the *dual code* $C^{\perp_*}$ of C is given by

$$C^{\perp_*} := \left\{\mathbf{u} \in \mathbb{F}_q^n : \langle \mathbf{u}, \mathbf{v} \rangle_* = 0 \text{ for all } \mathbf{v} \in C\right\}$$

while the dual distance $d^{\perp_*}$ is defined to be $d(C^{\perp_*})$.

If $C \subseteq C^{\perp_*}$, then C is said to be *self-orthogonal*. C is *self-dual* when equality holds.

A code C is *closed* under $*$ if $(C^{\perp_*})^{\perp_*} = C$. The closure property of linear codes under the Euclidean and Hermitian inner products and of subfield linear codes under the trace Hermitian is well known from [26, Ch. 3]. The said property of subfield linear codes under the trace Euclidean inner product will be established in Theorem 2.2.

Definition 2.1: The *weight enumerator* $W_C(X, Y)$ of an $(n, M, d)_q$-code C is the polynomial

$$W_C(X, Y) = \sum_{i=0}^{n} A_i X^{n-i} Y^i, \tag{II.1}$$

where $A_i := |\{\mathbf{c} \in C : \mathrm{wt_H}(\mathbf{c}) = i\}|$.

Theorem 2.2: Let C be an $\mathbb{F}_r$-linear code over $\mathbb{F}_q$. Then, under the trace Euclidean inner product,

$$W_{C^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}}(X, Y) = \frac{1}{|C|} W_C(X + (q-1)Y, X - Y). \tag{II.2}$$

Moreover, $(C^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}})^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}} = C$.

Proof: The proof can be found in Appendix A. ■

In light of Theorem 2.2, under $*$, the weight enumerator of the dual code of a linear or subfield linear $(n, M = |C|, d)_q$-code C is connected to the weight enumerator of the code C via the MacWilliams Equation

$$W_{C^{\perp_*}}(X, Y) = \frac{1}{|C|} W_C(X + (q-1)Y, X - Y). \tag{II.3}$$

For $0 \leq j \leq n$, let $A_j^{\perp_*}$ denote the number of codewords of weight j in $C^{\perp_*}$. Then

$$A_j^{\perp_*} = \frac{1}{|C|} \sum_{i=0}^{n} A_i K_j^{n,q}(i) \tag{II.4}$$

where $K_j^{n,q}(i)$, the *Krawtchouk polynomial* of degree j in variable i, is given by

$$K_j^{n,q}(i) := \sum_{l=0}^{j} (-1)^l (q-1)^{j-l} \binom{i}{l} \binom{n-i}{j-l}. \tag{II.5}$$

The last two equations will feature prominently in the linear programming set-up in Section VI.

B. Asymmetric Quantum Codes

Let $\mathbb{C}$ be the field of complex numbers and $\eta = e^{\frac{2\pi\sqrt{-1}}{p}} \in \mathbb{C}$. We fix an orthonormal basis of $\mathbb{C}^q$

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

with respect to the Hermitian inner product on $\mathbb{C}^q$. For $n \in \mathbb{N}$, let $V_n = (\mathbb{C}^q)^{\otimes n}$ be the n fold tensor product of $\mathbb{C}^q$. Then we can choose the following orthonormal basis for V_n

$$\left\{|\mathbf{c}\rangle = |c_1 c_2 \ldots c_n\rangle : \mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{F}_q^n\right\},$$

where $|c_1c_2\ldots c_n\rangle$ abbreviates $|c_1\rangle \otimes |c_2\rangle \otimes \cdots \otimes |c_n\rangle$.

For two quantum states $|\boldsymbol{\varphi}\rangle$ and $|\boldsymbol{\psi}\rangle$ in V_n with

$$|\boldsymbol{\varphi}\rangle = \sum_{\mathbf{c}\in\mathbb{F}_q^n} \alpha(\mathbf{c})|\mathbf{c}\rangle \text{ and } |\boldsymbol{\psi}\rangle = \sum_{\mathbf{c}\in\mathbb{F}_q^n} \beta(\mathbf{c})|\mathbf{c}\rangle,$$

where $\alpha(\mathbf{c}), \beta(\mathbf{c}) \in \mathbb{C}$, the Hermitian inner product of $|\boldsymbol{\varphi}\rangle$ and $|\boldsymbol{\psi}\rangle$ is given by

$$\langle\boldsymbol{\varphi}|\boldsymbol{\psi}\rangle = \sum_{\mathbf{c}\in\mathbb{F}_q^n} \widetilde{\alpha(\mathbf{c})}\beta(\mathbf{c}) \in \mathbb{C},$$

where $\widetilde{\alpha(\mathbf{c})}$ is the complex conjugate of $\alpha(\mathbf{c})$. We say $|\boldsymbol{\varphi}\rangle$ and $|\boldsymbol{\psi}\rangle$ are *orthogonal* if $\langle\boldsymbol{\varphi}|\boldsymbol{\psi}\rangle = 0$.

To measure the performance of a quantum code, an appropriate error model must be chosen (see [33] for instance). In defining an AQC Q, one considers the set of error operators that Q can handle. First, a good basis $\mathcal{E}_n$ of the vector space of complex $q^n \times q^n$ matrices $\mathcal{M}_{q^n}(\mathbb{C})$ needs to be chosen. Let $a, b \in \mathbb{F}_q$. The unitary operators $X(a)$ and $Z(b)$ on $\mathbb{C}^q$ are defined by

$$X(a)|\varphi\rangle = |\varphi + a\rangle \text{ and } Z(b)|\varphi\rangle = \eta^{(\langle b,\varphi\rangle_{\mathrm{Tr\,E}})}|\varphi\rangle. \quad \text{(II.6)}$$

Based on (II.6), for $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$, we can write $X(\mathbf{a}) = X(a_1)\otimes\ldots\otimes X(a_n)$ and $Z(\mathbf{a}) = Z(a_1)\otimes\ldots\otimes Z(a_n)$ for the tensor product of n error operators. The set $\mathcal{E}_n := \{X(\mathbf{a})Z(\mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n\}$ can be taken as a good error basis.

The error group G_n of order pq^{2n} is generated by the matrices in $\mathcal{E}_n$

$$G_n := \{\eta^c X(\mathbf{a})Z(\mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n, c \in \mathbb{F}_p\}.$$

Let $E = \eta^c X(\mathbf{a})Z(\mathbf{b}) \in G_n$. Then the *quantum weight* $\mathrm{wt_Q}(E)$ of E is given by $|\{1 \le i \le n : (a_i, b_i) \ne (0,0)\}|$. The number of X-errors $\mathrm{wt_X}(E)$ and the number of Z-errors $\mathrm{wt_Z}(E)$ in the error operator E are given, respectively, by $\mathrm{wt_H}(\mathbf{a})$ and $\mathrm{wt_H}(\mathbf{b})$. A formal definition of q-ary AQC can now be given.

Definition 2.3: A *q-ary quantum code* of length n is a subspace Q of V_n with dimension $K \ge 1$. Let d_x and d_z be positive integers. A quantum code Q in V_n 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 X-errors and, at the same time, $d_z - 1$ qudits of Z-errors, *i.e.*, if $\langle\boldsymbol{\varphi}|\boldsymbol{\psi}\rangle = 0$ for $|\boldsymbol{\varphi}\rangle, |\boldsymbol{\psi}\rangle \in Q$, then $|\boldsymbol{\varphi}\rangle$ and $E|\boldsymbol{\psi}\rangle$ are orthogonal for any $E \in G_n$ such that $\mathrm{wt_X}(E) \le d_x - 1$ and $\mathrm{wt_Z}(E) \le d_z - 1$. Such an asymmetric quantum code Q with dimension $K \ge 2$ is called *pure* if $|\boldsymbol{\varphi}\rangle$ and $E|\boldsymbol{\psi}\rangle$ are orthogonal for any $|\boldsymbol{\varphi}\rangle, |\boldsymbol{\psi}\rangle \in Q$ and any $E \in G_n$ such that $\mathrm{wt_Q}(E) \ge 1$ and E satisfies

$$\begin{cases} \mathrm{wt_X}(E) \le d_x - 1 \\ \mathrm{wt_Z}(E) \le d_z - 1 \end{cases}.$$

By convention, an asymmetric quantum code Q with $K = 1$ is assumed to be pure.

III. CSS-like Constructions

This section constitutes the most technical part of the paper. Note that a main tool in the derivation of the standard CSS construction from the functional approach in [33] is the connection between codes and orthogonal arrays (OAs) due to Delsarte (see [9, Th. 4.5] or [18, Th. 4.9]). The codewords in a general code C can be seen as the rows of an OA $\mathcal{A}$ and vice versa. Since in the construction of the OA $\mathbb{F}_q$-linearity is not strictly required and the duality can be defined over any valid bilinear form, it is of mathematical interest to investigate if the CSS construction can be extended by relaxing the linearity requirement and including other types of inner products.

First, we derive a construction of pure AQCs based on nested pairs of codes over $\mathbb{F}_q$ under the trace Euclidean inner product. Then, we show how this construction is related to other known extensions of the CSS construction discussed in [33] and in [11].

Recall the following characterization of AQCs presented in [33].

Theorem 3.1: [33, Th. 3.1]

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

$$\varphi_i : \mathbb{F}_q^n \to \mathbb{C} \text{ for } 1 \le i \le K \quad \text{(III.1)}$$

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

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

and each $\mathbf{c}_A, \mathbf{c}'_A \in \mathbb{F}_q^{|A|}$, $\mathbf{c}_Z \in \mathbb{F}_q^{|Z|}$ and $\mathbf{a}_X \in \mathbb{F}_q^{|X|}$, we have the equality

$$\sum_{\substack{\mathbf{c}_X \in \mathbb{F}_q^{|X|}, \\ \mathbf{c}_B \in \mathbb{F}_q^{|B|}}} \widetilde{\varphi_i(\mathbf{c}_A, \mathbf{c}_X, \mathbf{c}_Z, \mathbf{c}_B)}\varphi_j(\mathbf{c}'_A, \mathbf{c}_X - \mathbf{a}_X, \mathbf{c}_Z, \mathbf{c}_B)$$

$$= \begin{cases} 0 & \text{for } i \ne j \\ I(\mathbf{c}_A, \mathbf{c}'_A, \mathbf{c}_Z, \mathbf{a}_X) & \text{for } i = j \end{cases}, \quad \text{(III.3)}$$

where $I(\mathbf{c}_A, \mathbf{c}'_A, \mathbf{c}_Z, \mathbf{a}_X)$ is an element of $\mathbb{C}$ which is independent of i. The notation $(\mathbf{c}_A, \mathbf{c}_X, \mathbf{c}_Z, \mathbf{c}_B)$ represents the rearrangement of the entries of the vector $\mathbf{c} \in \mathbb{F}_q^n$ according to the partition of $\{1, 2, \ldots, n\}$ given in (III.2).

2) Let (φ_i, φ_j) stand for $\sum_{\mathbf{c}\in\mathbb{F}_q^n} \widetilde{\varphi_i(\mathbf{c})}\varphi_j(\mathbf{c})$. There exists a pure asymmetric quantum code with parameters $((n, K \ge 1, d_z/d_x))_q$ if and only if there exist K nonzero mappings φ_i as shown in (III.1) such that
   - φ_i are linearly independent for $1 \le i \le K$, i.e., the rank of the $K \times q^n$ matrix $(\varphi_i(\mathbf{c}))_{1\le i\le K, \mathbf{c}\in\mathbb{F}_q^n}$ is K; and
   - for each d with $1 \le d \le \min\{d_x, d_z\}$, a partition in (III.2) and $\mathbf{c}_A, \mathbf{a}_A \in \mathbb{F}_q^{|A|}, \mathbf{c}_Z \in \mathbb{F}_q^{|Z|}$ and $\mathbf{a}_X \in \mathbb{F}_q^{|X|}$, we have the equality

$$\sum_{\substack{\mathbf{c}_X \in \mathbb{F}_q^{|X|}, \\ \mathbf{c}_B \in \mathbb{F}_q^{|B|}}} \varphi_i(\widetilde{\mathbf{c}_A, \mathbf{c}_X, \mathbf{c}_Z, \mathbf{c}_B}) \varphi_j(\mathbf{c}_A + \mathbf{a}_A, \mathbf{c}_X + \mathbf{a}_X, \mathbf{c}_Z, \mathbf{c}_B)$$

$$= \begin{cases} 0 & \text{for } (\mathbf{a}_A, \mathbf{a}_X) \neq (\mathbf{0}, \mathbf{0}) \\ \frac{(\varphi_i, \varphi_j)}{q^{d_z - 1}} & \text{for } (\mathbf{a}_A, \mathbf{a}_X) = (\mathbf{0}, \mathbf{0}) \end{cases}. \quad \text{(III.4)}$$

Remark 3.2: It is important to note that the values d_x and d_z are in fact interchangeable [11, Prop. 4.2]. Physically, such an interchange can be effected by applying the Hadamard transform. In the presentation of the parameters of a particular AQC, it is customary to write $d_z \geq d_x$ since phase-flip errors are taken to be more frequent.

Theorem 3.3: Let $d_x, d_z \in \mathbb{N}$. Let C be an $\mathbb{F}_r$-linear code over $\mathbb{F}_q$ of length n. Assume that $d^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}} = d(C^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}})$ is the minimum distance of the dual code $C^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}$ of C under the trace Euclidean inner product. For a set $V := \{\mathbf{v}_i : 1 \leq i \leq K\}$ of K distinct vectors in $\mathbb{F}_q^n$, let $d_v := \min\{\mathrm{wt_H}(\mathbf{v}_i - \mathbf{v}_j + \mathbf{c}) : 1 \leq i \neq j \leq K, \mathbf{c} \in C\}$. If $d^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}} \geq d_z$ and $d_v \geq d_x$, then there exists an asymmetric quantum code Q with parameters $((n, K, d_z/d_x))_q$.

Proof: The proof follows the same line of argument as the proof of [11, Th. 4.4], substituting the trace Euclidean inner product for the trace Hermitian inner product. The key reason why the same argument works lies in the usage of the close connection between codes and orthogonal arrays [18, Th. 4.9] under any valid bilinear form. Furthermore, the said connection guarantees that the conditions in Part 2) of Theorem 3.1 are satisfied, making the resulting AQCs pure. ■

Theorem 3.4: For $i = 1, 2$, let C_i be an $\mathbb{F}_r$-linear code with parameters $(n, K_i, d_i)_q$. If $C_1^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}} \subseteq C_2$, then there exists an asymmetric quantum code Q with parameters $\left(\left(n, \frac{K_1 \cdot K_2}{q^n}, d_2/d_1\right)\right)_q = [[n, \log_q K_1 + \log_q K_2 - n, d_2/d_1]]_q$.

Proof: We take $C = C_1^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}$ in Theorem 3.3 above. Since $C_1^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}} \subseteq C_2$, we have $C_2 = C_1^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}} \oplus C'$, where C' is an $\mathbb{F}_r$-subspace of C_2 and $\oplus$ is the direct sum so that $|C'| = \frac{|C_2|}{\left|C_1^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}\right|}$. Let $C' = \{\mathbf{v}_1, \ldots, \mathbf{v}_K\}$, where $K = \frac{|C_2|}{\left|C_1^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}\right|} = \frac{K_1 \cdot K_2}{q^n}$ by Theorem 2.2. Then

$$d^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}} = d(C^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}) = d(C_1) = d_1 \text{ and}$$

$$\begin{aligned} d_v &= \min\{\mathrm{wt_H}(\mathbf{v}_i - \mathbf{v}_j + \mathbf{c}) : 1 \leq i \neq j \leq K, \mathbf{c} \in C\} \\ &= \min\left\{\mathrm{wt_H}(\mathbf{v} + \mathbf{c}) : \mathbf{0} \neq \mathbf{v} \in C', \mathbf{c} \in C_1^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}\right\} \geq d_2. \end{aligned}$$

■

The standard CSS construction for pure asymmetric q-ary quantum codes employs the pair $C_1^{\perp_\mathrm{E}} \subseteq C_2$ of $\mathbb{F}_q$-linear codes of length n.

Theorem 3.5: (Standard CSS Construction for AQC) Let C_i be $\mathbb{F}_q$-linear codes with parameters $[n, k_i, d_i]_q$ for $i = 1, 2$ with $C_1^{\perp_\mathrm{E}} \subseteq C_2$. Let

$$d_z := \mathrm{wt_H}(C_2 \setminus C_1^{\perp_\mathrm{E}}) \text{ and } d_x := \mathrm{wt_H}(C_1 \setminus C_2^{\perp_\mathrm{E}}).$$

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

A proof for this construction for the pure case using the functional approach is given in [33, Cor. 3.3]. When $q = r^2$, we can use either the Euclidean or the Hermitian inner product in the statement of Theorem 3.5.

Noting that the trace Euclidean inner product is just the Euclidean inner product when the codes involved are $\mathbb{F}_q$-linear, [33, Cor. 3.3] follows immediately from Theorem 3.4.

Let $\mathbb{F}_q$ be a quadratic extension of $\mathbb{F}_r$. Let the codes in the nested pair be $\mathbb{F}_r$-linear codes in $\mathbb{F}_q^n$. Under the trace Hermitian inner product, we can derive AQCs according to [11, Th. 4.5]. When the codes are $\mathbb{F}_q$-linear, the trace Hermitian duals become the Hermitian duals. Hence, the construction with respect to the Hermitian inner product follows.

In summary, the standard CSS construction for pure AQCs can be extended to include the constructions of pure AQCs from nested pairs of classical codes under the Hermitian, trace Hermitian, and trace Euclidean inner products. We call all of the above constructions *CSS-like*.

To show the generality of Theorem 3.4, we demonstrate how to derive [11, Th. 4.5] when $q = r^2$ from it. Given a nested pair $C_1^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}} \subseteq C_2$ of codes yielding a quantum code of parameters $((n, K, d_z/d_x))_q$ we construct a nested pair $D_1^{\perp_{\mathrm{Tr}_{q/r}\mathrm{H}}} \subseteq D_2$ of codes yielding a quantum code of equal parameters and vice versa.

Theorem 3.6: Let $q = r^2$. Then an $((n, K, d_z/d_x))_q$-CSS-like quantum code with respect to the trace Euclidean inner product exists if and only if there exists an $((n, K, d_z/d_x))_q$-CSS-like quantum code with respect to the trace Hermitian inner product.

Proof: See Appendix B. ■

If, in Theorem 3.6, the codes in the nested pairs are $\mathbb{F}_q$-linear, then we get the link between AQCs based on the CSS-like constructions under the Hermitian and Euclidean inner products.

The mathematical structures investigated above reveal that for a pair of nested $\mathbb{F}_q$-linear codes it suffices to consider the Euclidean inner product. In all other cases, it suffices to use the trace Euclidean inner product.

The relationships among different CSS-like constructions is summarized in Fig. 1 with the horizontal arrow signifying that the resulting AQCs have the same parameters.

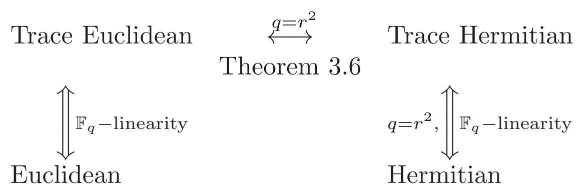


Fig. 1. Relationships among CSS-like Constructions

Applying a suitable CSS-like construction to the pair $C \subseteq C^{\perp_*}$ gives us the following proposition.

Proposition 3.7: Let C be a self-orthogonal $(n, |C|, d)_q$-code. Then there exists an AQC Q with parameters $[[n, n - 2\log_q(|C|), d^{\perp_*}/d^{\perp_*}]]_q$.

The existence of some pure CSS-like AQCs with specified parameters can often be ruled out by examining the parameters of the component codes in the nested pair used.

Example 3.8: There does not exist a pure $[[5, 1, 3/2]]_2$-CSS code.

Proof: First, note that there is no codeword $\mathbf{v}$ of weight 5 in any $[5, 2, 3]_2$-code C. Let $\mathbf{c} \in C$ such that $\mathrm{wt_H}(\mathbf{c}) = 3$. If such a codeword $\mathbf{v}$ exists, then $\mathbf{c}+\mathbf{v}$ is a codeword of weight 2 in C, a contradiction. Another possibility is a nested pair $[5, 1, d]_2 \subset [5, 2, 3]_2$ with $d^{\perp_{\mathrm{E}}} = 2$. But this forces $d = 5$, which has been shown to be impossible above. Since $k \leq n - d + 1$ by the Singleton bound, the remaining candidates of nested pairs, namely $[5, 1, d]_2 \subset [5, 2, 2]_2$ with $d^{\perp_{\mathrm{E}}} = 3$, $[5, 2, d]_2 \subset [5, 3, 2]_2$ with $d^{\perp_{\mathrm{E}}} = 3$, and $[5, 3, d]_2 \subset [5, 4, 2]_2$ with $d^{\perp_{\mathrm{E}}} = 3$, can all be shown to be impossible. ■

The next example provides a partial answer to a question raised in [30, p. 1652].

Example 3.9: A pure $[[12, 1, 5/3]]_2$-CSS code does not exist.

Proof: For a contradiction, assume that such a code exists. Then we have a pair of binary classical codes C_1 with parameters $[12, k_1, d_1]_2$ and C_2 with parameters $[12, k_2, d_2]_2$, such that $C_1^{\perp_{\mathrm{E}}} \subset C_2$ with $k_1 + k_2 - 12 = 1$ and $\{d_1, d_2\} = \{3, 5\}$.

Case 1: $d_1 = 3$ and $d_2 = 5$: From [15], $2 \leq k_2 \leq 4$. This forces $9 \leq k_1 \leq 11$. However, for $[12, k_1, d_1]_2$ with $9 \leq k_1 \leq 11$, $d_1 \leq 2 < 3$.

Case 2: $d_1 = 5$ and $d_2 = 3$: From [15], $2 \leq k_2 \leq 8$. This forces $5 \leq k_1 \leq 11$. However, for $[12, k_1, d_1]_2$ with $5 \leq k_1 \leq 11$, $d_1 \leq 4 < 5$. ■

Now that the theoretical foundations on the CSS-like constructions have been established, we next show that there are indeed gains on the parameters of the resulting AQCs. A two-directional approach is employed in coming up with such AQCs. First, we directly construct nested pairs of classical codes and derive the parameters of the resulting AQCs in the next section. Linear programming is then used to derive the upper bound for $\log_q(K)$ in the section after next.

IV. Three Constructions of Nested Pairs of Codes

In this section, we derive pairs of linear and subfield linear codes which can be used to construct AQCs. Three constructions are considered, namely a construction based on nested cyclic $\mathbb{F}_r$-linear codes over $\mathbb{F}_q$, a construction from nested group character codes, and a construction based on best-known linear codes (BKLC) of length n having a codeword $\mathbf{v}$ such that $\mathrm{wt_H}(\mathbf{v}) = n$. This last construction yields AQCs with $d_x = 2$. All computations are done in MAGMA [5] version V2.16-5.

A. Cyclic Construction

An obvious choice for the construction of nested pairs of $\mathbb{F}_q$-linear codes is the cyclic construction. Earlier construction of AQCs based on $\mathbb{F}_2$-cyclic codes has been done in [2].

Any $\mathbb{F}_q$-linear cyclic codes in $\mathbb{F}_q^n$ is an ideal in the residue class ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ (see [19, Ch. 4] or [25, Ch. 7]). A cyclic code D is a subset of a cyclic code C of equal length over $\mathbb{F}_q$ if and only if the generator polynomial of C divides the generator polynomial of D. Both polynomials divide $x^n - 1$.

Since we are also interested in nested pairs of $\mathbb{F}_r$-linear codes over $\mathbb{F}_q$, a generalization to the construction of $\mathbb{F}_r$-linear nested cyclic codes over $\mathbb{F}_q$ is provided here. Our construction is a further generalization of [6, Th. 14].

Definition 4.1: An $(n, r^l)_q$-code C is said to be cyclic $\mathbb{F}_r$-linear over $\mathbb{F}_q$ if C is a subspace of the $\mathbb{F}_r$-vector space $\mathbb{F}_q^n$ which is closed under one cyclic shift, *i.e.*, if $(c_0, c_1, \ldots, c_{n-1}) \in C$, then so is $(c_{n-1}, c_0, \ldots, c_{n-2})$.

Let $\mathbb{F}_q$ be the field extension of $\mathbb{F}_r$ of degree m such that $\mathbb{F}_q = \mathbb{F}_r(\omega)$. Every polynomial in $\mathbb{F}_q[x]$ can be uniquely written as

$$f_0(x) + \omega f_1(x) + \cdots + \omega^{m-1} f_{m-1}(x),$$

where $f_i(x) \in \mathbb{F}_r[x]$ for all i.

Given a cyclic $\mathbb{F}_r$-linear code C of length n over $\mathbb{F}_q$, we can view the codewords of C as polynomials in $\mathbb{F}_q[x]$. It is often convenient to refer to C as the set

$$\{v(x) = v_0 + v_1 x + \ldots + v_{n-1}x^{n-1} : (v_0, v_1, \ldots, v_{n-1}) \in C\}.$$

Note that, for all $\mathbb{F}_r \subseteq \mathbb{F}_q$, both C and $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ are $\mathbb{F}_r[x]$-modules under the usual polynomial multiplication together with the rule $x^n = 1$.

Theorem 4.2: Let $\mathbb{F}_q = \mathbb{F}_r(\omega)$ be an extension of degree m over $\mathbb{F}_r$. Any $(n, r^l)_q$-cyclic $\mathbb{F}_r$-linear code C over $\mathbb{F}_q$ has m generators, and can be represented as an $\mathbb{F}_r[x]$-module

$$\begin{aligned} C = \langle & a_{0,0}(x) + \omega a_{0,1}(x) + \ldots + \omega^{m-1} a_{0,m-1}(x), \\ & a_{1,0}(x) + \omega a_{1,1}(x) + \ldots + \omega^{m-2} a_{1,m-2}(x), \\ & \vdots \qquad\qquad \vdots \qquad\qquad \iddots \\ & a_{m-2,0}(x) + \omega a_{m-2,1}(x), \\ & a_{m-1,0}(x)\rangle, \end{aligned}$$

where $a_{i,j}(x) \in \mathbb{F}_r[x]$ for all $0 \leq i \leq m-1$ and $0 \leq j \leq i-1$. Moreover, these polynomials can be chosen such that the following properties hold:

i) $a_{i,m-1-i}(x) | (x^n - 1)$ in $\mathbb{F}_r[x]$ for all $0 \leq i \leq m-1$.

ii) $a_{i,m-1-i}(x) | \left(a_{i-1,m-1-i}(x)(x^n - 1)/a_{i-1,m-i}(x)\right)$ in $\mathbb{F}_r[x]$ for all $1 \leq i \leq m-1$.

iii) $l = mn - \sum_{i=0}^{m-1} \deg(a_{i,m-1-i}(x))$.

iv) The sets

$$\{a_{i,m-1-i}(x) : 0 \leq i \leq m-1\} \text{ and}$$
$$\{a_{i,j}(x) \bmod (a_{m-j,j}(x)) : 0 \leq i \leq m-1-j\}$$

are unique for all $1 \leq j \leq m-1$.

Proof: See Appendix C. ■

To construct an AQC, from a given cyclic $\mathbb{F}_r$-linear code C over $\mathbb{F}_q$ with representation

$$\begin{aligned} C = \langle & g_0(x) = a_{0,0}(x) + \omega a_{0,1}(x) + \ldots + \omega^{m-1} a_{0,m-1}(x), \\ & g_1(x) = a_{1,0}(x) + \omega a_{1,1}(x) + \ldots + \omega^{m-2} a_{1,m-2}(x), \end{aligned}$$

$$\vdots \qquad \vdots \qquad \iddots$$
$$g_{m-2}(x) = a_{m-2,0}(x) + \omega a_{m-2,1}(x),$$
$$g_{m-1}(x) = a_{m-1,0}(x)\rangle,$$

define D to be the code generated by

$$\{g_0(x)b_0(x), g_1(x)b_1(x), \ldots, g_{m-1}(x)b_{m-1}(x)\},$$

where $b_i(x)$ is a divisor of $(x^n-1)/a_{i,m-1-i}(x)$ for all $0 \leq i \leq m-1$. D is a cyclic $\mathbb{F}_r$-linear subcode of C.

B. Construction from Group Character Codes

Group character (GC) codes were introduced in [10] based on elementary abelian 2-groups and were further generalized in [24] to include the case where the group is $(\mathbb{Z}/t\mathbb{Z})^l$ for $l, t \in \mathbb{N}$. We use the definitions and results in [24] for generality.

The elements of $(\mathbb{Z}/t\mathbb{Z})^l$ can be written as $(a_1, \ldots, a_l)$ where $0 \leq a_i \leq t-1$ for $1 \leq i \leq l$. Let $||a|| = \sum_{i=1}^{l} a_i \in \mathbb{Z}$. Note that $0 \leq ||a|| \leq (t-1)l$ for all $a \in (\mathbb{Z}/t\mathbb{Z})^l$.

Let r be an integer such that $0 \leq r < l(t-1)$ and let the set $\mathcal{X}(r,l;t)$ be given by

$$\mathcal{X}(r,l;t) = \{a \in (\mathbb{Z}/t\mathbb{Z})^l : ||a|| > r\}. \tag{IV.1}$$

Definition 4.3: Let $\mathbb{F}_q$ be a finite field with $t|(q-1)$ and let $f_0, f_1, \ldots f_{t^l-1}$ be the group characters from $(\mathbb{Z}/t\mathbb{Z})^l$ to $\mathbb{F}_q \setminus \{0\}$. Let $\mathbf{c} = (c_0, c_1, \ldots, c_{t^l-1})$ be a vector in $\mathbb{F}_q^{t^l}$. Let $C_q(r,l;t)$ denote the q-ary code

$$C_q(r,l;t) = \left\{ \mathbf{c} : \sum_{j=0}^{t^l-1} c_j f_j(x) = 0 \text{ for all } x \in \mathcal{X}(r,l;t) \right\}. \tag{IV.2}$$

The properties of $C_q(r,l;t)$ are known.

Theorem 4.4: [24, Th. 8] Writing $r = a(t-1)+b$, where $0 \leq b \leq t-2$, the code $C_q(r,l;t)$ has parameters

$$[t^l, k_l(r), (t-b)t^{l-1-a}]_q, \tag{IV.3}$$

where

$$k_l(r) = \sum_{i=0}^{r}\sum_{j=0}^{l} (-1)^j \binom{l}{j}\binom{l-1+i-jt}{t-1}.$$

The nestedness condition can be deduced directly from (IV.1) and (IV.2).

Lemma 4.5: If $0 \leq r_1 \leq r_2 < l(t-1)$, then $C_q(r_1,l;t) \subseteq C_q(r_2,l;t)$.

Theorem 4.6: [24, Th. 10] The Euclidean dual $(C_q(r,l;t))^{\perp_{\rm E}}$ of $C_q(r,l;t)$ is monomially equivalent[1] to $C_q(l(t-1)-1-r,l;t)$.

Hence, $d\left((C_q(r,l;t))^{\perp_{\rm E}}\right)$ can be computed explicitly.

Theorem 4.7: Let $0 \leq r_1 \leq r_2 < l(t-1)$. Let $a, b, \gamma, \delta, k, d_1$ and d_2 be nonnegative integers satisfying

$$r_2 = a(t-1)+b \text{ where } 0 \leq b < t-1,$$
$$l(t-1)-1-r_1 = \gamma(t-1)+\delta \text{ with } 0 \leq \delta < t-1,$$
$$k = k_l(r_2) - k_l(r_1),$$
$$d_1 = (t-\delta)t^{l-1-\gamma}, \text{ and}$$
$$d_2 = (t-b)t^{l-1-a}.$$

Then there exists an asymmetric stabilizer code Q with parameters $[[t^l, k, d_2/d_1]]_q$.

Proof: Use the nested pair $C_q(r_1,l;t) \subseteq C_q(r_2,l;t)$ in Theorem 3.5. Combining Theorem 4.6 and (IV.3), we get

$$d\left((C_q(r_1,l;t))^{\perp_{\rm E}}\right) = (t-\delta)t^{l-1-\gamma} = d_1,$$

if we write $l(t-1)-1-r_1 = \gamma(t-1)+\delta$ with $0 \leq \delta < t-1$. The other values are clear. ■

[1]A discussion on code equivalence can be found in [19, Sects. 1.6 and 1.7].

C. BKLC construction

Let us start with the following result.

Theorem 4.8: Let C be a linear $[n,k,d]_q$-code. If C has a codeword $\mathbf{v}$ such that ${\rm wt}_{\rm H}(\mathbf{v}) = n$, then there exists an $[[n, k-1, d/2]]_q$-code Q.

Proof: Construct a code $D := \{\lambda\mathbf{v} : \lambda \in \mathbb{F}_q\} \subset C$. Since D is MDS, $D^\perp$ is also MDS with parameters $[n, n-1, 2]_q$. Setting $C_1 = D^\perp$ and $C_2 = C$ in Theorem 3.5 completes the proof. ■

An obvious strategy is to identify the best-known linear codes stored in the database of MAGMA that contain a codeword of weight equal to the length n for small fields $q \in \{2,3,4,5,7,8,9\}$. We call this construction the *BKLC construction*.

Note that sometimes the database does not contain a linear code of specified length n and dimension k satisfying the required condition since this specific requirement has not been recognized as important before. This in no way excludes the possibility of the existence of a linear code that has a codeword of weight n.

V. Linear Programming Bounds

This section details the set-up and the implementation of the linear programming (LP) bounds (more precisely, systems of linear inequalities) that we use to derive the upper bound for $k = \log_q(K)$ (see [30] for an earlier attempt in the binary case). Again, let $*$ stand for any one of the Euclidean, trace Euclidean, Hermitian, and trace Hermitian inner products. In fact, without loss of generality, $*$ can be taken as the trace Euclidean inner product based on Fig. 1.

From Section III, given $q = r^m, n, k, d_x, d_z$, a pure CSS-like $[[n,k,d_z/d_x]]_q$ code exists if and only if there exists a pair C_1, C_2 of $\mathbb{F}_r$-linear codes over $\mathbb{F}_q$ such that $C_1^{\perp_*} \subset C_2$, $k = \log_q\left(\frac{|C_2|}{|C_1^{\perp_*}|}\right)$ with $d_x = d_1$ and $d_z = d_2$.

If LP rules out the existence of such a pair, a negative certificate is issued. Otherwise, the process indicates the values of k which cannot be ruled out and the parameters of the (hypothetical) pair C_1 and C_2 giving such k. This information is useful when we try to come up with some *ad hoc* constructions yielding good codes as illustrated, *e.g.*, in Subsection VI-C

For $0 \leq j \leq n$, let A_j and B_j be, respectively, the number of codewords of weight j in C_2 and C_1. The corresponding numbers $A_j^{\perp_*}$ and $B_j^{\perp_*}$ of their respective duals are given by (II.4). One can write column vectors $B, A, B^{\perp_*}$, and $A^{\perp_*}$, each having $n+1$ entries to represent the weight distributions of C_1, C_2, and of their duals, respectively. Introduce the matrix K in the space of real $(n+1)\times(n+1)$ matrices $\mathcal{M}_{n+1}(\mathbb{R})$ with $K_{j,i} = K_j^{n,q}(i) \in \mathbb{Z}$ from (II.5).

Since $C_1^{\perp_*} \subset C_2$, we obtain $C_2^{\perp_*} \subset C_1$ by taking their duals. Given these two pairs of nested codes one can follow Delsarte's approach [8] to derive bounds for $|C_i|$ and $|C_i^{\perp_*}|$ for $i = 1, 2$. For an arbitrary code $C \subseteq \mathbb{F}_q^n$ of minimum distance d having $\mathcal{W}$ as a feasible column vector representing its weight distribution,

$$|C| \leq \max_{\mathcal{W}\geq \mathbf{0}} \sum_{i=0}^{n} \mathcal{W}_i \text{ such that } \mathcal{D} := K\mathcal{W} \geq \mathbf{0} \qquad \text{(V.1)}$$

provided that $\mathcal{W}_0 = 1$ and $\mathcal{W}_s = 0$ for $1 \leq s \leq d-1$.

If C is $\mathbb{F}_r$-linear, let $d^{\perp_*}$ be the minimum distance of $C^{\perp_*}$ and $\mathcal{W}^{\perp_*}$ be a feasible vector representation of its weight distribution. One can then write, for $|C| = q^l$,

$$K\mathcal{W} = q^l \mathcal{W}^{\perp_*} \geq \mathbf{0}$$

given that $\mathcal{W}_0^{\perp_*} = 1$ and $\mathcal{W}_t^{\perp_*} = 0$ for $1 \leq t \leq d^{\perp_*} - 1$. This means that (V.1) can be improved by adding the constraints that $\mathcal{D}_i = 0$ for $1 \leq i \leq d^{\perp_*} - 1$.

From here on we assume that C is $\mathbb{F}_r$-linear. Let $D(d) := \lfloor \log_r (\max |C| \text{ in (V.1)}) \rfloor$ be the largest possible $\mathbb{F}_r$-dimension of C under Delsarte's bound. Then any such code C of minimum distance d satisfies $|C| \leq r^{D(d)}$. In a similar fashion, let $D(d, d^{\perp_*})$ denote $\lfloor \log_r (\max |C|) \rfloor$ when C has minimum distance d and $C^{\perp_*}$ has minimum distance $d^{\perp_*}$. Under this improved bound, as $|C| = r^{ml} \leq r^{D(d,d^{\perp_*})}$, one has $|C^{\perp_*}| \geq r^{mn - D(d,d^{\perp_*})}$. Thus,[2]

$$D(d^{\perp_*}, d) \geq \dim_{\mathbb{F}_r}(C^{\perp_*}) \geq mn - D(d, d^{\perp_*}).$$

Dually, we get

$$D(d, d^{\perp_*}) \geq \dim_{\mathbb{F}_r}(C) \geq mn - D(d^{\perp_*}, d).$$

To limit our search space, we need to establish feasible values for the pair (k, k') to be used as part of the input to establish the LP bound. Let $|C_1| = q^{k+k'}$ and $|C_2| = q^{n-k'}$ for $mk, mk' \in \mathbb{Z}$. Let $d_x = d(C_1)$ and $d_z = d(C_2)$ be given. Let $\alpha := D(d_x, d_z)$ and $\beta := D(d_z, d_x)$. Since $C_1^{\perp_*} \subset C_2$, the pair of codes $\left(C_1, C_1^{\perp_*}\right)$ satisfies $d(C_1) = d_x$ and $d(C_1^{\perp_*}) \geq d_z$. This gives

$$\alpha \geq \dim_{\mathbb{F}_r}(C_1) = m(k + k') \geq mn - \beta \text{ and}$$
$$\beta \geq \dim_{\mathbb{F}_r}(C_{1^{\perp_*}}) = m(n - k - k') \geq mn - \alpha.$$

Looking at the duals, since $C_2^{\perp_*} \subset C_1$, one has $d(C_2^{\perp_*}) \geq d_x$. The pair of codes $\left(C_2, C_2^{\perp_*}\right)$ satisfies $d(C_2) = d_z$ and $d(C_2^{\perp_*}) \geq d_x$. Hence,

$$\beta \geq \dim_{\mathbb{F}_r}(C_2) = m(n - k') \geq mn - \alpha \text{ and}$$
$$\alpha \geq \dim_{\mathbb{F}_r}(C_2^{\perp_*}) = mk' \geq mn - \beta.$$

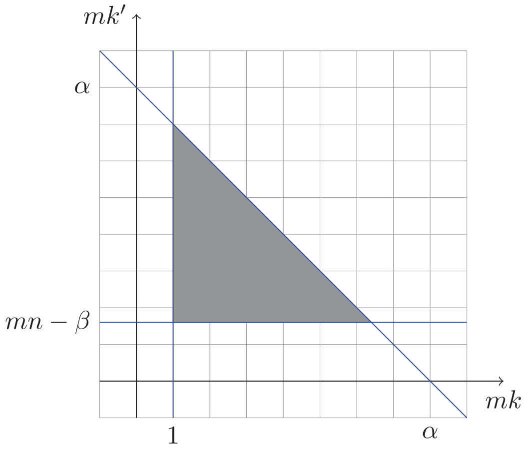
These sets of inequalities are equivalent to the system

$$\begin{cases} m(k + k') \leq \alpha \\ mk' \geq mn - \beta \end{cases} . \qquad \text{(V.2)}$$

[2]The above and what follows do not depend on the particular nature of the bound $D(d, d^{\perp_*})$.

We add $mk \geq 1$ since $C_2^{\perp_*}$ is a strict subset of C_1 and $0 < k' < n - k$ to ensure $d_z, d_x > 1$ since our AQC Q should have both X-error and Z-error detection capability.

Drawing the picture for feasible (mk, mk'), the possible pairs must correspond to the integer points in the gray triangle.



While many tuples (n, q, d_x, d_z) are ruled out this way, there are situations when there will be feasible (mk, mk').

Example 5.1: Consider $(n, q, d_x, d_z) = (7, 4, 5, 2)$ for $m = 2$. By Delsarte's bound, it is known (see [4] for more details) that the largest sizes of $\mathbb{F}_4$-codes with $d = 5$ and $d = 2$ are bounded above by, respectively, 40 and 4096. In this case, $\alpha = 5 = \lfloor \log_2(40) \rfloor$ and $\beta = 12 = \log_2(4096)$. Thus, the gray triangle containing all six possible (mk, mk') values has vertices $(1, 2)$, $(1, 4)$, and $(3, 2)$.

Once feasible (mk, mk') values are found, one can prepare the input tuple (n, q, k, k', d_x, d_z) for the *formal* LP whose objective function[3] is to maximize

$$\sum_{j=1}^{d_z - 1} A_j,$$

subject to the following constraints:

1) $A_0 = B_0 = A_0^{\perp_*} = B_0^{\perp_*} = 1$,
2) $A_j = 0$ for $1 \leq j < d(C_2)$ and $A_j \geq 0$ for $j \geq d(C_2)$,
3) $B_j = 0$ for $1 \leq j < d(C_1)$ and $B_j \geq 0$ for $j \geq d(C_1)$,
4) $A_j^{\perp_*} = 0$ for $1 \leq j < d(C_2^{\perp_*})$ and $A_j^{\perp_*} \geq 0$ for $j \geq d(C_2^{\perp_*})$,
5) $B_j^{\perp_*} = 0$ for $1 \leq j < d(C_1^{\perp_*})$ and $B_j^{\perp_*} \geq 0$ for $j \geq d(C_1^{\perp_*})$,
6) $KA^{\perp_*} = q^{k'} A$,
7) $KB^{\perp_*} = q^{n-k-k'} B$,
8) $A_j = B_j^{\perp_*}$ for $0 \leq j \leq d_z - 1$, $A_{d_z} > B_{d_z}^{\perp_*}$, and $A_j \geq B_j^{\perp_*}$ for all $d_z < j \leq n$,
9) $B_j = A_j^{\perp_*}$ for $0 \leq j \leq d_x - 1$, $B_{d_x} > A_{d_x}^{\perp_*}$, and $B_j \geq A_j^{\perp_*}$ for all $d_x < j \leq n$.

Constraints 6 and 7 come from combining (II.4) and the fact that $K^2 = q^n I$ where I is the identity matrix. The last two constraints take care of the purity assumption that $\mathrm{wt}_{\mathrm{H}}(C_2 \setminus C_1^{\perp_*}) = d(C_2)$ and $\mathrm{wt}_{\mathrm{H}}(C_1 \setminus C_2^{\perp_*}) = d(C_1)$.

The latter LP rules out, for instance, the tuple $(n, q, k, k', d_x, d_z) = (6, 2, 2, 1, 3, 2)$, which is not ruled out by

[3]In fact, any linear function can be chosen.

the gray triangle above. Indeed, for $(n, q, d_x, d_z) = (6, 2, 3, 2)$, the integer points (k, k') in the triangle are $(1, 1)$, $(1, 2)$, and $(2, 1)$. For the first two tuples, the LP is feasible. For the third, one can compute a *Farkas-like* certificate of infeasibility for the system 1)–9) as follows.

After reordering the constraints and multiplying some of them, if necessary, by -1, the system can be rewritten as

$$M_1 \cdot \begin{pmatrix} A \\ B \end{pmatrix} = \mathbf{r} \geq \mathbf{0},\ M_2 \cdot \begin{pmatrix} A \\ B \end{pmatrix} \geq \mathbf{0}, \qquad \text{(V.3)}$$

where M_1, M_2 are matrices with $2n + 2$ columns each and $\mathbf{0} \neq \mathbf{r}$ is a nonnegative vector.

One then tries to find a vector $\mathbf{s} = (\mathbf{s}_1 \mathbf{s}_2)$ satisfying $(M_1^{\intercal} M_2^{\intercal}) \binom{\mathbf{s}_1}{\mathbf{s}_2} \leq \mathbf{0}$ such that $\mathbf{s}_2 \geq \mathbf{0}$ and $\mathbf{s}_1^{\intercal} \mathbf{r} > 0$. It follows from an appropriate form of the Farkas Lemma that such an $\mathbf{s}$ exists if and only if the system 1)–9) is infeasible. To see sufficiency, note that $\mathbf{s}^{\intercal} \binom{M_1}{M_2} \binom{A}{B} \leq 0$, whereas $\mathbf{s}^{\intercal} \binom{\mathbf{r}}{\mathbf{0}} > 0$, a contradiction.

The vector $\mathbf{s}$ certifying infeasibility can be found by linear programming. The details of such a computation for $(n, q, k, k', d_x, d_z) = (6, 2, 2, 1, 3, 2)$ is in Appendix D.

VI. Good Pure CSS-like AQCs based on Linear Programming Bound

Based on the LP bound, this section presents good AQCs derived from the nested pairs of classical codes constructed by the methods outlined in Section IV.

By Proposition 3.7, good AQCs with $K = 1$ and $d_z = d_x$ can be derived from self-dual codes having the largest possible minimum distance. Lists of extremal and optimal self-dual codes over various finite fields can be found in [26, Ch. 11]. More recent results are available in [16], [17] as well as prominent references therein. The parameters of the AQCs that can be derived from these extremal or optimal self-dual codes via CSS-like constructions can be computed easily. In the case of $q = 4$, for example, [11, Table I] provides the most updated list. Henceforth, we consider AQCs with $K > 1$.

Among the best pure AQCs is of course the class of codes reaching the equality of the quantum Singleton bound $K \leq q^{n-d_z-d_x+2}$. Such codes are referred to as AQMDS codes whose full treatment can be found in [12]. Assuming the validity of the classical MDS conjecture, the lengths of pure AQMDS codes are bounded above roughly by q. It is of interest, therefore, to identify the best possible pure CSS-like AQCs for lengths beyond the possible values for the MDS type.

According to the LP bound, Table I gives a criterion for the goodness of the constructed AQCs.

To present our findings in as concise a manner as possible, we separate the tables of good pure AQCs according to the fields. When q is a prime, only $\mathbb{F}_q$-linear pairs are possible. The results are presented in Subsection VI-A.

When $\mathbb{F}_q$ is a nontrivial extension of $\mathbb{F}_p$, then we need to consider also the case where the pairs consist of subfield linear codes. For $q \in \{4, 8, 9\}$, we differentiate between the strictly $\mathbb{F}_q$-linear cases and the $\mathbb{F}_r$-linear cases. AQCs from $\mathbb{F}_r$-linear construction beating the best that the strictly $\mathbb{F}_q$-linear construction can achieve are listed as well to highlight the gain that we get from going non-$\mathbb{F}_q$-linear. Subsection VI-B presents the tables.

TABLE I
MEASURE OF GOODNESS

Label	Description
Optimal	The LP bound for k is reached.
BeOpLin	The pair of nested subfield linear codes yields better k than the LP bound value when $\mathbb{F}_q$-linearity is imposed.
OpLin	The LP bound with $\mathbb{F}_q$-linearity required is attained.
ROpLin	The pair of nested subfield linear codes yields the LP bound value when $\mathbb{F}_q$-linearity is imposed.

In both subsections, the tables are ordered according to n, d_x and d_z. The following shorthands are used to distinguish the types of construction:

1) ACC stands for $\mathbb{F}_r$-linear but not $\mathbb{F}_q$-linear nested cyclic pair of codes where at least one of the codes in the pair is not $\mathbb{F}_q$-linear.
2) AH stands for an *ad hoc* pair of codes. Their explicit construction will be provided in detail in Subsection VI-C.
3) BC stands for a nested pair of codes where the supercode is taken from the MAGMA's database of best-known linear codes having a codeword $\mathbf{v}$ with $\mathrm{wt}_{\mathrm{H}}(\mathbf{v}) = n$.
4) CC stands for $\mathbb{F}_q$-linear nested cyclic pair of codes.
5) GC stands for $\mathbb{F}_q$-linear nested pair of group character codes.
6) For $q = 4$, the type SO refers to an AQC which is derived from a self-orthogonal code C discussed in [11, Table II, Sect. VII].

A. Tables of Optimal Pure Asymmetric CSS Codes for $q \in \{2, 3, 5, 7\}$

The lists of optimal pure AQCs for $q \in \{2, 3, 5, 7\}$ are given, respectively for each q, in Tables II, IV, VI, and VIII.

For each q, the table is then followed by the table giving the explicit pairs of cyclic codes $D \subset C$ yielding them. To save space, the generator polynomials of the codes C and D are presented in an abbreviated form. The generator polynomial $g(x)$ of the $[n, k_C]_q$-code C is written as $g = (c_0 c_1 \ldots c_{n-k_C})$ instead of as the polynomial $g(x) = c_0 + c_1 x + \ldots + c_{n-k_C} x^{n-k_C}$. Since $g(x)$ divides the generator polynomial of D, we write the latter as $(d_0 d_1 \ldots d_{k_C - k_D})g$ where k_D is the dimension of D. The details on the explicit cyclic pairs can be found in Tables III, V, VII, and IX.

The list of best-known linear codes from the database of MAGMA yielding good AQCs will not be presented here since they can be searched and checked easily. For AQCs from group character codes, we simply enumerate them in Table X according to the notations used in Theorem 4.7.

B. Tables of Good Pure Asymmetric CSS-like Codes for $q \in \{4, 8, 9\}$

In this subsection we list down good AQCs for $q \in \{4, 8, 9\}$ based on Table I. To qualify the goodness of a specific code under consideration, the theoretical LP bound for $k = \log_q K$

TABLE II
OPTIMAL PURE ASYMMETRIC CSS CODES OVER $\mathbb{F}_2$

No.	AQC Q	Type	No.	AQC Q	Type	No.	AQC Q	Type	No.	AQC Q	Type
1	$[[4,1,2/2]]_2$	AH	22	$[[15,4,4/4]]_2$	CC	43	$[[24,18,3/2]]_2$	BC	64	$[[31,15,6/3]]_2$	CC
2	$[[5,2,2/2]]_2$	AH	23	$[[15,2,5/4]]_2$	CC	44	$[[24,17,4/2]]_2$	BC	65	$[[31,6,11/3]]_2$	CC
3	$[[6,1,3/2]]_2$	CC	24	$[[16,10,4/2]]_2$	BC	45	$[[24,13,6/2]]_2$	BC	66	$[[31,5,12/3]]_2$	CC
4	$[[7,3,3/2]]_2$	CC	25	$[[16,4,8/2]]_2$	BC	46	$[[24,11,8/2]]_2$	BC	67	$[[31,1,15/3]]_2$	CC
5	$[[7,1,3/3]]_2$	CC	26	$[[17,8,5/2]]_2$	CC	47	$[[26,1,13/2]]_2$	CC	68	$[[31,15,5/4]]_2$	CC
6	$[[8,3,4/2]]_2$	BC	27	$[[17,1,5/5]]_2$	CC	48	$[[27,13,7/2]]_2$	BC	69	$[[31,5,11/4]]_2$	CC
7	$[[10,1,5/2]]_2$	CC	28	$[[18,8,6/2]]_2$	BC	49	$[[28,22,3/2]]_2$	BC	70	$[[31,11,5/5]]_2$	CC
8	$[[11,6,3/2]]_2$	BC	29	$[[18,1,9/2]]_2$	CC	50	$[[28,21,4/2]]_2$	CC	71	$[[31,10,6/5]]_2$	CC
9	$[[12,6,4/2]]_2$	CC	30	$[[20,14,3/2]]_2$	BC	51	$[[28,13,8/2]]_2$	BC	72	$[[31,1,11/5]]_2$	CC
10	$[[13,1,5/3]]_2$	AH	31	$[[20,13,4/2]]_2$	BC	52	$[[29,5,13/2]]_2$	BC	73	$[[32,25,4/2]]_2$	BC
11	$[[14,4,6/2]]_2$	CC	32	$[[21,15,3/2]]_2$	CC	53	$[[30,22,4/2]]_2$	CC	74	$[[32,16,8/2]]_2$	BC
12	$[[14,1,7/2]]_2$	CC	33	$[[21,11,5/2]]_2$	CC	54	$[[30,5,14/2]]_2$	BC	75	$[[32,10,12/2]]_2$	BC
13	$[[15,10,3/2]]_2$	CC	34	$[[21,7,5/3]]_2$	CC	55	$[[30,1,15/2]]_2$	CC	76	$[[32,5,16/2]]_2$	BC
14	$[[15,8,4/2]]_2$	CC	35	$[[21,6,6/3]]_2$	CC	56	$[[31,25,3/2]]_2$	CC	77	$[[33,22,5/2]]_2$	BC
15	$[[15,6,5/2]]_2$	CC	36	$[[21,6,5/4]]_2$	CC	57	$[[31,20,5/2]]_2$	CC	78	$[[34,22,6/2]]_2$	BC
16	$[[15,4,7/2]]_2$	CC	37	$[[21,3,5/5]]_2$	CC	58	$[[31,16,7/2]]_2$	BC	79	$[[35,27,4/2]]_2$	CC
17	$[[15,7,3/3]]_2$	CC	38	$[[21,2,6/5]]_2$	CC	59	$[[31,10,11/2]]_2$	CC	80	$[[36,29,3/2]]_2$	BC
18	$[[15,6,4/3]]_2$	CC	39	$[[22,1,11/2]]_2$	CC	60	$[[31,5,15/2]]_2$	CC	81	$[[36,28,4/2]]_2$	BC
19	$[[15,3,5/3]]_2$	CC	40	$[[23,13,5/2]]_2$	BC	61	$[[31,21,3/3]]_2$	CC	82	$[[40,33,3/2]]_2$	BC
20	$[[15,2,6/3]]_2$	CC	41	$[[23,11,7/2]]_2$	CC	62	$[[31,20,4/3]]_2$	CC	83	$[[40,32,4/2]]_2$	BC
21	$[[15,1,7/3]]_2$	CC	42	$[[23,1,7/7]]_2$	CC	63	$[[31,16,5/3]]_2$	CC			

TABLE X
NESTED PAIRS OF GROUP CHARACTER CODES YIELDING OPTIMAL ASYMMETRIC CSS CODES IN TABLES IV, VI, AND VIII

q	(r_1, r_2, l, t)	AQC Q
3	$(1,2,3,2)$	$[[8,3,4/2]]_3$
	$(1,3,4,2)$	$[[16,10,4/2]]_3$
	$(1,4,5,2)$	$[[32,25,4/2]]_3$
5	$(1,2,3,2)$	$[[8,3,4/2]]_5$
7	$(1,3,2,3)$	$[[9,5,3/2]]_7$
	$(2,3,2,3)$	$[[9,2,6/2]]_7$

is explicitly provided. The defect **Def** is measured by subtracting the actual value of k from the theoretical LP value.

Up to reasonable lengths, Tables XI, XIV, and XVII contain good codes for $q \in \{4,8,9\}$. For brevity, in Table XI the convention that $\mathbb{F}_4 = \mathbb{F}_2(w)$ where w is a primitive root of an irreducible degree 2 polynomial in $\mathbb{F}_2[x]$ is followed. Similarly, in Table XIV we use the convention that $\mathbb{F}_8 = \mathbb{F}_2(w)$ where w is a primitive root of an irreducible polynomial of degree 3 in $\mathbb{F}_2[x]$. In Table XVII we let $\mathbb{F}_9 = \mathbb{F}_3(w)$ where w is a primitive root of a monic irreducible polynomial of degree 2 in $\mathbb{F}_3[x]$.

In Tables XII, XV, and XVIII, nested subfield linear cyclic codes yielding good codes are listed down while Tables XIII, XVI, and XIX present the cyclic pairs. We use the notations indicated in Theorem 4.2 and the abbreviation already mentioned above to write the generator polynomials.

C. Some Ad Hoc Constructions

In some cases, an *ad hoc* construction of suitable nested pairs of classical codes indicated by the linear programming output yields AQCs with optimal k.

We show an explicit construction for codes Q with parameters $[[4,1,2/2]]_2$ and $[[5,2,2/2]]_2$ by exhibiting a generator matrix for each of $[4,2,2]_2$ and $[5,3,2]_2$-codes containing a codeword of weight 4 and 5, respectively. The matrices are

$$\begin{pmatrix} 1010 \\ 0101 \end{pmatrix} \text{ and } \begin{pmatrix} 10001 \\ 01011 \\ 00101 \end{pmatrix}.$$

A $[[13,1,5/3]]_2$-code alluded to by a referee of [30] can also be constructed as shown below. It is rather surprising that this CSS code is optimal, given that it is far from reaching the quantum Singleton bound. It is of interest to know if the construction here is essentially the only one possible, up to code equivalence.

Consider the best-known $[13,9,3]_2$-linear code C_2 from the MAGMA database. Its dual $C_2^{\perp_{\mathrm{E}}}$ is a $[13,4,6]_2$-code. Next, we add the row vector $\mathbf{1} := (1,1,\ldots,1)$ to the generator matrix of $C_2^{\perp_{\mathrm{E}}}$ to get a $[13,5,5]_2$-code C_1. The dual of C_1 is a $[13,8,4]_2$-code which is a subcode of C_2. Hence, we can use $C_1^{\perp_{\mathrm{E}}} \subset C_2$ to get a $[[13,1,5/3]]_2$-quantum code Q.

Recently, some new best-known linear codes over $\mathbb{F}_5$ are presented in [21, Sec. 5]. The first one is of parameters $[36,28,6]_5$ and is labeled $\mathcal{C}_{36}$ in the said reference. By shortening this code at the first position a $[35,27,6]_5$-code is derived. If we shorten $\mathcal{C}_{36}$ at the first two positions, we get a $[34,26,6]_5$-code. It can be easily checked, starting with the generator matrix of $\mathcal{C}_{36}$, that each of these three codes contains a codeword $\mathbf{v}$ of weight equal to its length. By Theorem 4.8, we get CSS codes with parameters $[[36,27,6/2]]_5$, $[[35,26,6/2]]_5$, and $[[34,25,6/2]]_5$, all of which are optimal.

VII. CONCLUSION AND OPEN PROBLEMS

It is instructive to consider, by way of simple examples presented in Table XX, the difference between the best performing symmetric quantum codes and their asymmetric counterparts. AQCs allow us to tailor the process of error-correction better once the ratio of asymmetry in the channel is known or can be approximated properly. Extensive data on

TABLE III
NESTED PAIRS OF CYCLIC CODES OVER $\mathbb{F}_2$ YIELDING OPTIMAL ASYMMETRIC CSS CODES IN TABLE II

C and D	Generator Polynomials	AQC Q	C and D	Generator Polynomials	AQC Q
$[6,5,2]_2$	$g=(11)$	$[[6,1,3/2]]_2$	$[21,12,5]_2$	$g=(1110110011)$	$[[21,3,5/5]]_2$
$[6,4,2]_2$	$(11)g$		$[21,9,8]_2$	$(1001)g$	
$[7,4,3]_2$	$g=(1011)$	$[[7,3,3/2]]_2$	$[21,12,5]_2$	$g=(1110110011)$	$[[21,2,6/5]]_2$
$[7,1,7]_2$	$(1101)g$		$[21,10,5]_2$	$(111)g$	
$[7,4,3]_2$	$g=(1011)$	$[[7,1,3/3]]_2$	$[22,21,2]_2$	$g=(11)$	$[[22,1,11/2]]_2$
$[7,3,4]_2$	$(11)g$		$[22,20,2]_2$	$(11)g$	
$[10,9,2]_2$	$g=(11)$	$[[10,1,5/2]]_2$	$[23,12,7]_2$	$g=(110001110101)$	$[[23,11,7/2]]_2$
$[10,8,2]_2$	$(11)g$		$[23,1,23]_2$	$(101011100011)g$	
$[12,11,2]_2$	$g=(11)$	$[[12,6,4/2]]_2$	$[23,12,7]_2$	$g=(110001110101)$	$[[23,1,7/7]]_2$
$[12,5,4]_2$	$(1101011)g$		$[23,11,8]_2$	$(11)g$	
$[14,13,2]_2$	$g=(11)$	$[[14,4,6/2]]_2$	$[26,25,2]_2$	$g=(11)$	$[[26,1,13/2]]_2$
$[14,9,4]_2$	$(11101)g$		$[26,24,2]_2$	$(11)g$	
$[14,2,7]_2$	$g=(1010101010101)$	$[[14,1,7/2]]_2$	$[28,22,4]_2$	$g=(1001011)$	$[[28,21,4/2]]_2$
$[14,1,14]_2$	$(11)g$		$[28,1,28]_2$	$(1110011110101001001101)g$	
$[15,11,3]_2$	$g=(10011)$	$[[15,10,3/2]]_2$	$[30,28,2]_2$	$g=(111)$	$[[30,22,4/2]]_2$
$[15,1,15]_2$	$(11101100101)g$		$[30,6,14]_2$	$(11110010111111100001101)g$	
$[15,13,2]_2$	$g=(111)$	$[[15,8,4/2]]_2$	$[30,29,2]_2$	$g=(11)$	$[[30,1,15/2]]_2$
$[15,5,7]_2$	$(111010001)g$		$[30,28,2]_2$	$(11)g$	
$[15,7,5]_2$	$g=(100010111)$	$[[15,6,5/2]]_2$	$[31,26,3]_2$	$g=(111101)$	$[[31,25,3/2]]_2$
$[15,1,15]_2$	$(1111001)g$		$[31,1,31]_2$	$(10001110101001011110011011)g$	
$[15,14,2]_2$	$g=(11)$	$[[15,4,7/2]]_2$	$[31,21,5]_2$	$g=(10001110001)$	$[[31,20,5/2]]_2$
$[15,10,4]_2$	$(10011)g$		$[31,1,31]_2$	$(11110100111100101111)g$	
$[15,10,4]_2$	$g=(101011)$	$[[15,6,4/3]]_2$	$[31,11,11]_2$	$g=(111001110001010011001)$	$[[31,10,11/2]]_2$
$[15,4,8]_2$	$(1011101)g$		$[31,1,31]_2$	$(10010110111)g$	
$[15,6,6]_2$	$g=(1100111001)$	$[[15,2,6/3]]_2$	$[31,6,15]_2$	$g=(11001011011110101000100111)$	$[[31,5,15/2]]_2$
$[15,4,8]_2$	$(111)g$		$[31,1,31]_2$	$(101001)g$	
$[15,10,4]_2$	$g=(101011)$	$[[15,4,4/4]]_2$	$[31,26,3]_2$	$g=(111101)$	$[[31,21,3/3]]_2$
$[15,6,6]_2$	$(10011)g$		$[31,5,16]_2$	$(1011001010111010100011)g$	
$[15,10,4]_2$	$g=(101011)$	$[[15,2,5/4]]_2$	$[31,25,4]_2$	$g=(1000111)$	$[[31,20,4/3]]_2$
$[15,8,4]_2$	$(111)g$		$[31,5,16]_2$	$(110111001101001100001)g$	
$[15,11,3]_2$	$g=(10011)$	$[[15,7,3/3]]_2$	$[31,21,5]_2$	$g=(10001110001)$	$[[31,16,5/3]]_2$
$[15,4,8]_2$	$(11100111)g$		$[31,5,16]_2$	$(10111001100000011)g$	
$[15,11,3]_2$	$g=(10011)$	$[[15,3,5/3]]_2$	$[31,20,6]_2$	$g=(100110110001)$	$[[31,15,6/3]]_2$
$[15,8,4]_2$	$(1001)g$		$[31,5,16]_2$	$(1101110101011101)g$	
$[15,11,3]_2$	$g=(10011)$	$[[15,1,7/3]]_2$	$[31,11,11]_2$	$g=(111001110001010011001)$	$[[31,6,11/3]]_2$
$[15,10,4]_2$	$(11)g$		$[31,5,16]_2$	$(1110001)g$	
$[17,9,5]_2$	$g=(111010111)$	$[[17,1,5/5]]_2$	$[31,10,12]_2$	$g=(1010010010101101001111)$	$[[31,5,12/3]]_2$
$[17,8,6]_2$	$(11)g$		$[31,5,16]_2$	$(100101)g$	
$[17,9,5]_2$	$g=(111010111)$	$[[17,8,5/2]]_2$	$[31,26,3]_2$	$g=(111101)$	$[[31,1,15/3]]_2$
$[17,1,17]_2$	$(100111001)g$		$[31,25,4]_2$	$(11)g$	
$[18,2,9]_2$	$g=(10101010101010101)$	$[[18,1,9/2]]_2$	$[31,21,5]_2$	$g=(10001110001)$	$[[31,15,5/4]]_2$
$[18,1,18]_2$	$(11)g$		$[31,6,15]_2$	$(1101000100000001)g$	
$[21,20,2]_2$	$g=(11)$	$[[21,15,3/2]]_2$	$[31,11,11]_2$	$g=(111001110001010011001)$	$[[31,5,11/4]]_2$
$[21,5,10]_2$	$(1111011100110101)g$		$[31,6,15]_2$	$(101001)g$	
$[21,20,2]_2$	$g=(11)$	$[[21,11,5/2]]_2$	$[31,21,5]_2$	$g=(10001110001)$	$[[31,11,5/5]]_2$
$[21,9,8]_2$	$(100110000101)g$		$[31,10,12]_2$	$(100110111011)g$	
$[21,12,5]_2$	$g=(1110110011)$	$[[21,7,5/3]]_2$	$[31,20,6]_2$	$g=(100110110001)$	$[[31,10,6/5]]_2$
$[21,5,10]_2$	$(10011111)g$		$[31,10,12]_2$	$(10111011111)g$	
$[21,11,6]_2$	$g=(10101011001)$	$[[21,6,6/3]]_2$	$[31,11,11]_2$	$g=(111001110001010011001)$	$[[31,1,11/5]]_2$
$[21,5,10]_2$	$(1010111)g$		$[31,10,12]_2$	$(11)g$	
$[21,12,5]_2$	$g=(1110110011)$	$[[21,6,5/4]]_2$	$[35,34,2]_2$	$g=(11)$	$[[35,27,4/2]]_2$
$[21,6,7]_2$	$(1110101)g$		$[35,7,14]_2$	$(1110111010100110100100111101)g$	

TABLE XX
SOME EXAMPLES COMPARING SYMMETRIC AND ASYMMETRIC QUANTUM CODES FOR $q=2$

n	k	Symmetric d	Asymmetric (d_z,d_x)
7	3	2	$(3,2)$
8	3	3	$(4,2)$
15	1	5	$(7,3)$

the best-known symmetric quantum codes, given n and k for $q=2$, can be found in [15].

In this paper, the functional approach is used to establish CSS-like constructions allowing us to use pairs of nested subfield linear codes over $\mathbb{F}_q$ to construct pure AQCs. The standard CSS construction is shown to be a special case.

Combining specific constructions of pairs of nested classical codes and linear programming, we show that CSS-like constructions based on pairs of subfield linear codes over $\mathbb{F}_q$ often give us optimal or good q-ary pure AQCs with better parameters than the best that the standard CSS construction can achieve. Lists of optimal or best known pure CSS-like AQCs up to some computationally reasonable length for $q \in \{2,3,4,5,7,8,9\}$ are given in the hope of providing a more comprehensive list of best performing AQCs.

While working on earlier versions of this paper, we found out that the linear programming (LP) approach was sufficiently effective for small values of q and n. At the same time, the loss of precision due to the extremely large coefficients involved

TABLE IV
OPTIMAL PURE ASYMMETRIC CSS CODES OVER $\mathbb{F}_3$

No.	AQC Q	Type	No.	AQC Q	Type	No.	AQC Q	Type	No.	AQC Q	Type
1	$[[6, 2, 3/2]]_3$	CC	49	$[[17, 11, 4/2]]_3$	BC	97	$[[24, 16, 5/2]]_3$	BC	145	$[[30, 25, 3/2]]_3$	BC
2	$[[6, 1, 4/2]]_3$	CC	50	$[[17, 9, 5/2]]_3$	BC	98	$[[24, 15, 6/2]]_3$	BC	146	$[[30, 23, 4/2]]_3$	BC
3	$[[7, 3, 3/2]]_3$	BC	51	$[[17, 8, 6/2]]_3$	BC	99	$[[24, 11, 9/2]]_3$	BC	147	$[[30, 4, 18/2]]_3$	BC
4	$[[7, 2, 4/2]]_3$	BC	52	$[[17, 6, 7/2]]_3$	BC	100	$[[24, 6, 12/2]]_3$	BC	148	$[[30, 1, 22/2]]_3$	BC
5	$[[8, 4, 3/2]]_3$	CC	53	$[[17, 5, 8/2]]_3$	BC	101	$[[24, 3, 15/2]]_3$	CC	149	$[[31, 26, 3/2]]_3$	BC
6	$[[8, 3, 4/2]]_3$	CC,GC	54	$[[18, 13, 3/2]]_3$	BC	102	$[[24, 16, 3/3]]_3$	CC	150	$[[31, 24, 4/2]]_3$	BC
7	$[[8, 2, 5/2]]_3$	CC	55	$[[18, 12, 4/2]]_3$	BC	103	$[[24, 14, 4/3]]_3$	CC	151	$[[31, 1, 23/2]]_3$	BC
8	$[[8, 2, 3/3]]_3$	CC	56	$[[18, 10, 5/2]]_3$	BC	104	$[[25, 20, 3/2]]_3$	BC	152	$[[32, 27, 3/2]]_3$	BC
9	$[[8, 1, 4/3]]_3$	CC	57	$[[18, 9, 6/2]]_3$	BC	105	$[[25, 18, 4/2]]_3$	BC	153	$[[32, 25, 4/2]]_3$	BC,GC
10	$[[9, 5, 3/2]]_3$	BC	58	$[[19, 14, 3/2]]_3$	BC	106	$[[25, 17, 5/2]]_3$	BC	154	$[[32, 1, 24/2]]_3$	BC
11	$[[9, 4, 4/2]]_3$	BC	59	$[[19, 13, 4/2]]_3$	BC	107	$[[25, 16, 6/2]]_3$	BC	155	$[[33, 28, 3/2]]_3$	BC
12	$[[9, 3, 5/2]]_3$	BC	60	$[[19, 11, 5/2]]_3$	BC	108	$[[25, 7, 12/2]]_3$	BC	156	$[[33, 26, 4/2]]_3$	BC
13	$[[9, 2, 6/2]]_3$	BC	61	$[[19, 10, 6/2]]_3$	BC	109	$[[25, 6, 13/2]]_3$	BC	157	$[[33, 24, 5/2]]_3$	BC
14	$[[10, 6, 3/2]]_3$	BC	62	$[[19, 8, 7/2]]_3$	BC	110	$[[25, 3, 16/2]]_3$	BC	158	$[[33, 16, 10/2]]_3$	BC
15	$[[10, 5, 4/2]]_3$	BC	63	$[[20, 15, 3/2]]_3$	BC	111	$[[26, 21, 3/2]]_3$	CC	159	$[[33, 1, 24/2]]_3$	BC
16	$[[11, 7, 3/2]]_3$	BC	64	$[[20, 14, 4/2]]_3$	CC	112	$[[26, 19, 4/2]]_3$	CC	160	$[[34, 29, 3/2]]_3$	BC
17	$[[11, 5, 5/2]]_3$	CC	65	$[[20, 12, 5/2]]_3$	BC	113	$[[26, 18, 5/2]]_3$	CC	161	$[[34, 27, 4/2]]_3$	BC
18	$[[11, 1, 5/5]]_3$	CC	66	$[[20, 11, 6/2]]_3$	BC	114	$[[26, 17, 6/2]]_3$	BC	162	$[[34, 25, 5/2]]_3$	BC
19	$[[12, 8, 3/2]]_3$	BC	67	$[[20, 9, 7/2]]_3$	BC	115	$[[26, 7, 13/2]]_3$	CC	163	$[[34, 17, 10/2]]_3$	BC
20	$[[12, 6, 4/2]]_3$	CC	68	$[[20, 8, 8/2]]_3$	BC	116	$[[26, 6, 14/2]]_3$	CC	164	$[[34, 1, 25/2]]_3$	BC
21	$[[12, 5, 6/2]]_3$	BC	69	$[[20, 5, 10/2]]_3$	CC	117	$[[26, 3, 17/2]]_3$	CC	165	$[[35, 30, 3/2]]_3$	BC
22	$[[12, 2, 4/4]]_3$	CC	70	$[[20, 4, 11/2]]_3$	CC	118	$[[26, 18, 3/3]]_3$	CC	166	$[[35, 28, 4/2]]_3$	BC
23	$[[13, 9, 3/2]]_3$	CC	71	$[[20, 10, 4/4]]_3$	CC	119	$[[26, 16, 4/3]]_3$	CC	167	$[[35, 26, 5/2]]_3$	BC
24	$[[13, 7, 4/2]]_3$	BC	72	$[[20, 1, 10/4]]_3$	CC	120	$[[26, 15, 5/3]]_3$	CC	168	$[[35, 17, 11/2]]_3$	BC
25	$[[13, 6, 5/2]]_3$	CC	73	$[[21, 16, 3/2]]_3$	BC	121	$[[26, 4, 13/3]]_3$	CC	169	$[[35, 1, 26/2]]_3$	BC
26	$[[13, 3, 7/2]]_3$	CC	74	$[[21, 14, 4/2]]_3$	BC	122	$[[26, 3, 14/3]]_3$	CC	170	$[[36, 31, 3/2]]_3$	BC
27	$[[13, 7, 3/3]]_3$	CC	75	$[[21, 13, 5/2]]_3$	BC	123	$[[26, 14, 4/4]]_3$	CC	171	$[[36, 29, 4/2]]_3$	BC
28	$[[13, 4, 5/3]]_3$	CC	76	$[[21, 12, 6/2]]_3$	BC	124	$[[26, 13, 5/4]]_3$	CC	172	$[[36, 27, 5/2]]_3$	BC
29	$[[13, 3, 6/3]]_3$	CC	77	$[[21, 10, 7/2]]_3$	BC	125	$[[26, 12, 6/4]]_3$	CC	173	$[[36, 17, 12/2]]_3$	BC
30	$[[13, 1, 7/3]]_3$	CC	78	$[[21, 9, 8/2]]_3$	BC	126	$[[26, 2, 13/4]]_3$	CC	174	$[[36, 1, 27/2]]_3$	BC
31	$[[13, 1, 5/5]]_3$	CC	79	$[[21, 8, 9/2]]_3$	BC	127	$[[26, 1, 14/4]]_3$	CC	175	$[[37, 32, 3/2]]_3$	BC
32	$[[14, 9, 3/2]]_3$	BC	80	$[[22, 17, 3/2]]_3$	BC	128	$[[26, 12, 5/5]]_3$	CC	176	$[[37, 30, 4/2]]_3$	BC
33	$[[14, 8, 4/2]]_3$	BC	81	$[[22, 15, 4/2]]_3$	CC	129	$[[26, 1, 13/5]]_3$	CC	177	$[[37, 28, 5/2]]_3$	BC
34	$[[14, 7, 5/2]]_3$	BC	82	$[[22, 14, 5/2]]_3$	BC	130	$[[27, 22, 3/2]]_3$	BC	178	$[[37, 1, 27/2]]_3$	BC
35	$[[14, 6, 6/2]]_3$	BC	83	$[[22, 13, 6/2]]_3$	BC	131	$[[27, 20, 4/2]]_3$	BC	179	$[[38, 33, 3/2]]_3$	BC
36	$[[14, 4, 7/2]]_3$	BC	84	$[[22, 11, 7/2]]_3$	CC	132	$[[27, 19, 5/2]]_3$	BC	180	$[[38, 31, 4/2]]_3$	BC
37	$[[15, 10, 3/2]]_3$	BC	85	$[[22, 5, 12/2]]_3$	CC	133	$[[27, 18, 6/2]]_3$	BC	181	$[[38, 29, 5/2]]_3$	BC
38	$[[15, 9, 4/2]]_3$	BC	86	$[[22, 10, 4/4]]_3$	CC	134	$[[27, 7, 14/2]]_3$	BC	182	$[[38, 1, 28/2]]_3$	BC
39	$[[15, 7, 5/2]]_3$	BC	87	$[[22, 6, 7/4]]_3$	CC	135	$[[27, 6, 15/2]]_3$	BC	183	$[[39, 34, 3/2]]_3$	BC
40	$[[15, 6, 6/2]]_3$	BC	88	$[[22, 2, 7/7]]_3$	CC	136	$[[27, 3, 18/2]]_3$	BC	184	$[[39, 32, 4/2]]_3$	BC
41	$[[16, 11, 3/2]]_3$	BC	89	$[[23, 18, 3/2]]_3$	BC	137	$[[27, 1, 20/2]]_3$	BC	185	$[[39, 30, 5/2]]_3$	BC
42	$[[16, 10, 4/2]]_3$	BC,GC	90	$[[23, 16, 4/2]]_3$	BC	138	$[[28, 23, 3/2]]_3$	BC	186	$[[39, 1, 29/2]]_3$	BC
43	$[[16, 8, 5/2]]_3$	BC	91	$[[23, 15, 5/2]]_3$	BC	139	$[[28, 21, 4/2]]_3$	BC	187	$[[40, 35, 3/2]]_3$	BC
44	$[[16, 7, 6/2]]_3$	BC	92	$[[23, 14, 6/2]]_3$	BC	140	$[[28, 19, 6/2]]_3$	BC	188	$[[40, 33, 4/2]]_3$	BC
45	$[[16, 5, 7/2]]_3$	BC	93	$[[23, 11, 8/2]]_3$	BC	141	$[[28, 1, 21/2]]_3$	BC	189	$[[40, 31, 5/2]]_3$	BC
46	$[[16, 2, 10/2]]_3$	CC	94	$[[23, 1, 8/8]]_3$	CC	142	$[[29, 24, 3/2]]_3$	BC	190	$[[40, 1, 30/2]]_3$	BC
47	$[[16, 2, 5/5]]_3$	CC	95	$[[24, 19, 3/2]]_3$	CC	143	$[[29, 22, 4/2]]_3$	BC	191	$[[40, 28, 4/4]]_3$	CC
48	$[[17, 12, 3/2]]_3$	BC	96	$[[24, 17, 4/2]]_3$	CC	144	$[[29, 1, 21/2]]_3$	BC			

in the computation soon became very limiting as these values grew larger, as long as traditional LP solvers such as CPLEX were used.

To handle larger values of q and n, we started experimenting with arbitrary precision LP solvers, such as PPL [3], which is now equipped with Sage [32] interface, thanks largely to the efforts of Risan, then an undergraduate student at Nanyang Technological University, and the last author as presented in [27] and in [29].

The initial results in this direction were extremely encouraging, and we are able to solve most, if not all, of the LP instances we have previously encountered as intractable by traditional LP solvers. More efforts still need to be exerted in perfecting our software, in coming up with better upper bounds, and in constructing AQCs meeting the bounds.

The stabilizer formalism of symmetric quantum codes can be extended naturally to the asymmetric case. How the CSS-like constructions are connected to stabilizer AQCs is an interesting question to explore.

APPENDIX A: PROOF OF THEOREM 2.2

Given that $\mathbb{F}_p \subseteq \mathbb{F}_r \subseteq \mathbb{F}_q$, we equip the space $\mathbb{F}_q^n$ with the trace Euclidean inner product.

Lemma A.1: $\langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{Tr}_{q/r}\,\mathrm{E}}$ is a valid inner product on $\mathbb{F}_q^n$.

Proof: The only property to check is non-degeneracy since everything else follows immediately from $\langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{E}}$. We show that if $\langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{Tr}_{q/r}\,\mathrm{E}} = 0$ for all $\mathbf{u} \in \mathbb{F}_q^n$, then $\mathbf{v} = \mathbf{0}$, the converse being trivial.

Let us assume that $\mathbf{v} \neq \mathbf{0}$ and construct a vector $\mathbf{u} \in \mathbb{F}_q^n$ such that $\langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{Tr}_{q/r}\,\mathrm{E}} \neq 0$ to settle the claim. Since the trace mapping is onto, there exists $0 \neq a \in \mathbb{F}_q$ such that $\mathrm{Tr}_{q/r}(a) \neq 0$. Let j be the first index for which $v_j \neq 0$. Define $\mathbf{u} \in \mathbb{F}_q^n$ as follows: $u_j = v_j^{-1} a$ and $u_i = 0$ for all $i \neq j$. ■

TABLE V
NESTED PAIRS OF CYCLIC CODES OVER $\mathbb{F}_3$ YIELDING OPTIMAL ASYMMETRIC CSS CODES IN TABLE IV

C **and** D	**Generator Polynomials**	**AQC** Q
$[6,5,2]_3$	$g=(21)$	$[[6,2,3/2]]_3$
$[6,3,3]_3$	$(121)g$	
$[6,5,2]_3$	$g=(21)$	$[[6,1,4/2]]_3$
$[6,4,2]_3$	$(21)g$	
$[8,7,2]_3$	$g=(11)$	$[[8,4,3/2]]_3$
$[8,3,5]_3$	$(22021)g$	
$[8,7,2]_3$	$g=(11)$	$[[8,3,4/2]]_3$
$[8,4,4]_3$	$(1101)g$	
$[8,7,2]_3$	$g=(11)$	$[[8,2,5/2]]_3$
$[8,5,3]_3$	$(211)g$	
$[8,5,3]_3$	$g=(1011)$	$[[8,2,3/3]]_3$
$[8,3,5]_3$	$(101)g$	
$[8,4,4]_3$	$g=(21011)$	$[[8,1,4/3]]_3$
$[8,3,5]_3$	$(21)g$	
$[11,10,2]_3$	$g=(21)$	$[[11,5,5/2]]_3$
$[11,5,6]_3$	$(201211)g$	
$[11,6,5]_3$	$g=(201211)$	$[[11,1,5/5]]_3$
$[11,5,6]_3$	$(21)g$	
$[12,7,4]_3$	$g=(101101)$	$[[12,6,4/2]]_3$
$[12,1,12]_3$	$(1102011)g$	
$[12,7,4]_3$	$g=(101101)$	$[[12,2,4/4]]_3$
$[12,5,4]_3$	$(101)g$	
$[13,10,3]_3$	$g=(2201)$	$[[13,9,3/2]]_3$
$[13,1,13]_3$	$(2022010211)g$	
$[13,7,5]_3$	$g=(1120211)$	$[[13,6,5/2]]_3$
$[13,1,13]_3$	$(1022201)g$	
$[13,4,7]_3$	$g=(2001102121)$	$[[13,3,7/2]]_3$
$[13,1,13]_3$	$(2221)g$	
$[13,10,3]_3$	$g=(2201)$	$[[13,7,3/3]]_3$
$[13,3,9]_3$	$(20102121)g$	
$[13,7,5]_3$	$g=(1120211)$	$[[13,4,5/3]]_3$
$[13,3,9]_3$	$(10011)g$	
$[13,6,6]_3$	$g=(21210201)$	$[[13,3,6/3]]_3$
$[13,3,9]_3$	$(2221)g$	
$[13,4,7]_3$	$g=(2001102121)$	$[[13,1,7/3]]_3$
$[13,3,9]_3$	$(21)g$	
$[13,7,5]_3$	$g=(1120211)$	$[[13,1,5/5]]_3$
$[13,6,6]_3$	$(21)g$	
$[16,3,10]_3$	$g=(20112100201121)$	$[[16,2,10/2]]_3$
$[16,1,16]_3$	$(221)g$	
$[16,9,5]_3$	$g=(10021121)$	$[[16,2,5/5]]_3$
$[16,7,6]_3$	$(101)g$	
$[20,15,4]_3$	$g=(201111)$	$[[20,14,4/2]]_3$
$[20,1,20]_3$	$(122200101001211)g$	
$[20,6,10]_3$	$g=(112100101002221)$	$[[20,5,10/2]]_3$
$[20,1,20]_3$	$(102121)g$	
$[20,5,11]_3$	$g=(1200101111021101)$	$[[20,4,11/2]]_3$
$[20,1,20]_3$	$(12011)g$	
$[20,15,4]_3$	$g=(201111)$	$[[20,10,4/4]]_3$
$[20,5,11]_3$	$(10202020201)g$	
$[20,6,10]_3$	$g=(112100101002221)$	$[[20,1,10/4]]_3$
$[20,5,11]_3$	$(21)g$	
$[22,21,2]_3$	$g=(11)$	$[[22,15,4/2]]_3$
$[22,6,12]_3$	$(1102122222211201)g$	
$[22,21,2]_3$	$g=(11)$	$[[22,11,7/2]]_3$
$[22,10,9]_3$	$(100100210211)g$	
$[22,21,2]_3$	$g=(11)$	$[[22,5,12/2]]_3$
$[22,16,4]_3$	$(201211)g$	
$[22,16,4]_3$	$g=(2100211)$	$[[22,10,4/4]]_3$
$[22,6,12]_3$	$(21221222111)g$	
$[22,12,7]_3$	$g=(22211121121)$	$[[22,6,7/4]]_3$
$[22,6,12]_3$	$(2210021)g$	
$[22,12,7]_3$	$g=(22211121121)$	$[[22,2,7/7]]_3$
$[22,10,9]_3$	$(201)g$	
$[23,12,8]_3$	$g=(222110202001)$	$[[23,1,8/8]]_3$
$[23,11,9]_3$	$(21)g$	
$[24,20,3]_3$	$g=(21201)$	$[[24,19,3/2]]_3$
$[24,1,24]_3$	$(21122012220202101211)g$	
$[24,18,4]_3$	$g=(1012011)$	$[[24,17,4/2]]_3$
$[24,1,24]_3$	$(110122101220021101)g$	
$[24,4,15]_3$	$g=(1201012100222221221101)$	$[[24,3,15/2]]_3$
$[24,1,24]_3$	$(2021)g$	
$[24,20,3]_3$	$g=(21201)$	$[[24,16,3/3]]_3$
$[24,4,15]_3$	$(20101010002020201)g$	
$[24,20,3]_3$	$g=(21201)$	$[[24,14,4/3]]_3$
$[24,6,8]_3$	$(112221000221221)g$	
$[26,22,3]_3$	$g=(21211)$	$[[26,21,3/2]]_3$
$[26,1,26]_3$	$(2111221101212002001201)g$	
$[26,20,4]_3$	$g=(2120111)$	$[[26,19,4/2]]_3$
$[26,1,26]_3$	$(21122201201010111001)g$	
$[26,19,5]_3$	$g=(20012011)$	$[[26,18,5/2]]_3$
$[26,1,26]_3$	$(2221220100021021101)g$	
$[26,8,13]_3$	$g=(2220200112210010121)$	$[[26,7,13/2]]_3$
$[26,1,26]_3$	$(20021221)g$	
$[26,7,14]_3$	$g=(11102200221112020201)$	$[[26,6,14/2]]_3$
$[26,1,26]_3$	$(2211221)g$	
$[26,4,17]_3$	$g=(10212112201110120200221)$	$[[26,3,17/2]]_3$
$[26,1,26]_3$	$(1121)g$	
$[26,22,3]_3$	$g=(21211)$	$[[26,18,3/3]]_3$
$[26,4,17]_3$	$(2210102112021111211)g$	
$[26,22,3]_3$	$g=(21211)$	$[[26,16,4/3]]_3$
$[26,6,15]_3$	$(21212100100021011)g$	
$[26,22,3]_3$	$g=(21211)$	$[[26,15,5/3]]_3$
$[26,7,14]_3$	$(1110010120102021)g$	
$[26,22,3]_3$	$g=(21211)$	$[[26,4,13/3]]_3$
$[26,18,6]_3$	$(21111)g$	
$[26,22,3]_3$	$g=(21211)$	$[[26,3,14/3]]_3$
$[26,19,5]_3$	$(1021)g$	
$[26,20,4]_3$	$g=(2120111)$	$[[26,14,4/4]]_3$
$[26,6,15]_3$	$(202122201211101)g$	
$[26,19,5]_3$	$g=(20012011)$	$[[26,13,5/4]]_3$
$[26,6,15]_3$	$(22221022102101)g$	
$[26,18,6]_3$	$g=(120112011)$	$[[26,12,6/4]]_3$
$[26,6,15]_3$	$(1022001001201)g$	
$[26,20,4]_3$	$g=(2120111)$	$[[26,2,13/4]]_3$
$[26,18,6]_3$	$(201)g$	
$[26,7,14]_3$	$g=(11102200221112020201)$	$[[26,1,14/4]]_3$
$[26,6,15]_3$	$(11)g$	
$[26,19,5]_3$	$g=(20012011)$	$[[26,12,5/5]]_3$
$[26,7,14]_3$	$(1211001221021)g$	
$[26,19,5]_3$	$g=(21020101)$	$[[26,1,13/5]]_3$
$[26,18,6]_3$	$(21)g$	
$[40,34,4]_3$	$g=(1021211)$	$[[40,28,4/4]]_3$
$[40,6,24]_3$	$(1221012010011112201020012020 1)g$	

TABLE VI
OPTIMAL PURE ASYMMETRIC CSS CODES OVER $\mathbb{F}_5$

No.	**AQC** Q	**Type**	**No.**	**AQC** Q	**Type**	**No.**	**AQC** Q	**Type**	**No.**	**AQC** Q	**Type**
1	$[[6,2,4/2]]_5$	CC	48	$[[13,5,4/4]]_5$	CC	95	$[[19,2,14/2]]_5$	BC	142	$[[26,21,4/2]]_5$	BC
2	$[[7,2,4/2]]_5$	BC	49	$[[13,1,7/4]]_5$	CC	96	$[[20,16,3/2]]_5$	CC	143	$[[26,19,5/2]]_5$	BC
3	$[[7,3,3/2]]_5$	BC	50	$[[14,10,3/2]]_5$	BC	97	$[[20,15,4/2]]_5$	BC	144	$[[26,18,6/2]]_5$	BC
4	$[[8,4,3/2]]_5$	CC	51	$[[14,9,4/2]]_5$	BC	98	$[[20,13,5/2]]_5$	BC	145	$[[26,6,16/2]]_5$	BC
5	$[[8,3,4/2]]_5$	BC,GC	52	$[[14,7,5/2]]_5$	BC	99	$[[20,12,6/2]]_5$	BC	146	$[[27,23,3/2]]_5$	BC
6	$[[8,2,5/2]]_5$	BC	53	$[[14,6,6/2]]_5$	BC	100	$[[20,5,12/2]]_5$	BC	147	$[[27,21,4/2]]_5$	BC
7	$[[8,1,6/2]]_5$	CC	54	$[[14,5,7/2]]_5$	BC	101	$[[20,4,13/2]]_5$	BC	148	$[[27,20,5/2]]_5$	BC
8	$[[8,2,3/3]]_5$	CC	55	$[[14,4,8/2]]_5$	BC	102	$[[20,3,14/2]]_5$	BC	149	$[[27,19,6/2]]_5$	BC
9	$[[8,1,4/3]]_5$	CC	56	$[[14,3,9/2]]_5$	BC	103	$[[20,2,15/2]]_5$	CC	150	$[[28,24,3/2]]_5$	BC
10	$[[9,5,3/2]]_5$	BC	57	$[[14,2,10/2]]_5$	BC	104	$[[20,1,16/2]]_5$	CC	151	$[[28,22,4/2]]_5$	BC
11	$[[9,4,4/2]]_5$	BC	58	$[[14,1,11/2]]_5$	BC	105	$[[20,14,3/3]]_5$	CC	152	$[[28,21,5/2]]_5$	BC
12	$[[9,3,5/2]]_5$	BC	59	$[[15,11,3/2]]_5$	BC	106	$[[21,17,3/2]]_5$	BC	153	$[[28,20,6/2]]_5$	BC
13	$[[9,2,6/2]]_5$	BC	60	$[[15,10,4/2]]_5$	BC	107	$[[21,16,4/2]]_5$	BC	154	$[[29,25,3/2]]_5$	BC
14	$[[9,1,7/2]]_5$	BC	61	$[[15,8,5/2]]_5$	BC	108	$[[21,14,5/2]]_5$	BC	155	$[[29,23,4/2]]_5$	BC
15	$[[10,6,3/2]]_5$	CC	62	$[[15,7,6/2]]_5$	BC	109	$[[21,13,6/2]]_5$	BC	156	$[[29,22,5/2]]_5$	BC
16	$[[10,5,4/2]]_5$	CC	63	$[[15,6,7/2]]_5$	BC	110	$[[21,3,15/2]]_5$	BC	157	$[[29,13,12/2]]_5$	BC
17	$[[10,4,5/2]]_5$	BC	64	$[[15,5,8/2]]_5$	BC	111	$[[21,2,16/2]]_5$	BC	158	$[[30,26,3/2]]_5$	BC
18	$[[10,3,6/2]]_5$	BC	65	$[[15,4,9/2]]_5$	BC	112	$[[22,18,3/2]]_5$	BC	159	$[[30,24,4/2]]_5$	CC
19	$[[10,2,7/2]]_5$	BC	66	$[[15,3,10/2]]_5$	BC	113	$[[22,17,4/2]]_5$	BC	160	$[[30,23,5/2]]_5$	BC
20	$[[10,1,8/2]]_5$	CC	67	$[[15,2,11/2]]_5$	BC	114	$[[22,15,5/2]]_5$	BC	161	$[[30,14,12/2]]_5$	BC
21	$[[10,4,3/3]]_5$	CC	68	$[[15,1,12/2]]_5$	CC	115	$[[22,14,6/2]]_5$	BC	162	$[[30,20,4/4]]_5$	CC
22	$[[10,3,4/3]]_5$	CC	69	$[[16,12,3/2]]_5$	BC	116	$[[22,3,16/2]]_5$	BC	163	$[[31,27,3/2]]_5$	CC
23	$[[10,2,4/4]]_5$	CC	70	$[[16,11,4/2]]_5$	BC	117	$[[22,2,17/2]]_5$	BC	164	$[[31,25,4/2]]_5$	BC
24	$[[11,7,3/2]]_5$	BC	71	$[[16,9,5/2]]_5$	BC	118	$[[23,19,3/2]]_5$	BC	165	$[[31,25,3/3]]_5$	CC
25	$[[11,6,4/2]]_5$	BC	72	$[[16,8,6/2]]_5$	BC	119	$[[23,18,4/2]]_5$	BC	166	$[[32,26,4/2]]_5$	BC
26	$[[11,5,5/2]]_5$	CC	73	$[[16,7,7/2]]_5$	BC	120	$[[23,16,5/2]]_5$	BC	167	$[[33,28,3/2]]_5$	BC
27	$[[11,4,6/2]]_5$	BC	74	$[[16,3,11/2]]_5$	BC	121	$[[23,15,6/2]]_5$	BC	168	$[[33,27,4/2]]_5$	BC
28	$[[11,3,7/2]]_5$	BC	75	$[[16,2,12/2]]_5$	BC	122	$[[23,3,17/2]]_5$	BC	169	$[[34,29,3/2]]_5$	BC
29	$[[11,2,8/2]]_5$	BC	76	$[[17,13,3/2]]_5$	BC	123	$[[23,2,18/2]]_5$	BC	170	$[[34,28,4/2]]_5$	BC
30	$[[11,1,5/5]]_5$	CC	77	$[[17,12,4/2]]_5$	BC	124	$[[24,20,3/2]]_5$	CC	171	$[[34,25,6/2]]_5$	AH
31	$[[12,8,3/2]]_5$	CC	78	$[[17,10,5/2]]_5$	BC	125	$[[24,19,4/2]]_5$	CC	172	$[[35,30,3/2]]_5$	BC
32	$[[12,7,4/2]]_5$	CC	79	$[[17,9,6/2]]_5$	BC	126	$[[24,4,16/2]]_5$	BC	173	$[[35,29,4/2]]_5$	BC
33	$[[12,6,5/2]]_5$	BC	80	$[[17,8,7/2]]_5$	BC	127	$[[24,3,18/2]]_5$	CC	174	$[[35,26,6/2]]_5$	AH
34	$[[12,5,6/2]]_5$	BC	81	$[[17,3,11/2]]_5$	BC	128	$[[24,2,19/2]]_5$	CC	175	$[[35,1,28/2]]_5$	CC
35	$[[12,3,8/2]]_5$	BC	82	$[[18,14,3/2]]_5$	BC	129	$[[24,18,3/3]]_5$	CC	176	$[[36,31,3/2]]_5$	BC
36	$[[12,1,9/2]]_5$	CC	83	$[[18,13,4/2]]_5$	BC	130	$[[24,17,4/3]]_5$	CC	177	$[[36,30,4/2]]_5$	BC
37	$[[12,6,3/3]]_5$	CC	84	$[[18,11,5/2]]_5$	BC	131	$[[24,1,18/3]]_5$	CC	178	$[[36,27,6/2]]_5$	AH
38	$[[12,5,4/3]]_5$	CC	85	$[[18,10,6/2]]_5$	BC	132	$[[24,16,4/4]]_5$	CC	179	$[[37,32,3/2]]_5$	BC
39	$[[12,1,7/3]]_5$	CC	86	$[[18,4,11/2]]_5$	BC	133	$[[25,21,3/2]]_5$	BC	180	$[[37,31,4/2]]_5$	BC
40	$[[12,4,4/4]]_5$	CC	87	$[[18,3,12/2]]_5$	BC	134	$[[25,20,4/2]]_5$	BC	181	$[[38,33,3/2]]_5$	BC
41	$[[13,9,3/2]]_5$	BC	88	$[[19,15,3/2]]_5$	BC	135	$[[25,18,5/2]]_5$	BC	182	$[[38,32,4/2]]_5$	BC
42	$[[13,8,4/2]]_5$	CC	89	$[[19,14,4/2]]_5$	BC	136	$[[25,17,6/2]]_5$	BC	183	$[[39,34,3/2]]_5$	CC
43	$[[13,6,5/2]]_5$	BC	90	$[[19,12,5/2]]_5$	BC	137	$[[25,8,13/2]]_5$	BC	184	$[[39,33,4/2]]_5$	BC
44	$[[13,4,7/2]]_5$	CC	91	$[[19,11,6/2]]_5$	BC	138	$[[25,5,16/2]]_5$	BC	185	$[[39,31,3/3]]_5$	CC
45	$[[13,3,8/2]]_5$	BC	92	$[[19,5,11/2]]_5$	BC	139	$[[25,3,19/2]]_5$	BC	186	$[[40,35,3/2]]_5$	CC
46	$[[13,2,9/2]]_5$	BC	93	$[[19,4,12/2]]_5$	BC	140	$[[25,2,20/2]]_5$	BC	187	$[[40,34,4/2]]_5$	BC
47	$[[13,1,10/2]]_5$	BC	94	$[[19,3,13/2]]_5$	BC	141	$[[26,22,3/2]]_5$	BC	188	$[[40,1,32/2]]_5$	CC

Proof of Theorem 2.2: Let $A(Y) := \sum_0^n A_j Y^j$ and $B(Y) := \sum_0^n B_j Y^j$ be, respectively, the weight enumerators of C and of $C^{\perp_{\mathrm{Tr}_{q/r}} \mathrm{E}}$. We first prove the following identity

$$B(Y) = \frac{(1+(q-1)Y)^n}{|C|} \cdot A\left(\frac{1-Y}{1+(q-1)Y}\right). \quad \text{(VII.1)}$$

Let $\mathbf{c} = (c_1, \ldots, c_n), \mathbf{d} = (d_1, \ldots, d_n) \in C$. Let χ be a nontrivial additive character of $\mathbb{F}_r$. Since C is $\mathbb{F}_r$-linear, we can define for every $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$ a character $\chi_{\mathbf{b}}$ of the additive group C by substituting the trace Euclidean form for the argument of the character χ, such that

$$\chi_{\mathbf{b}}(\mathbf{c}) = \chi\left(\langle \mathbf{b}, \mathbf{c} \rangle_{\mathrm{Tr}_{q/r}\,\mathrm{E}}\right) = \chi\left(\sum_{i=1}^n \mathrm{Tr}_{q/r}(b_i c_i)\right) \in \mathbb{C}.$$

The character $\chi_{\mathbf{b}}$ is trivial if and only if $\mathbf{b} \in C^{\perp_{\mathrm{Tr}_{q/r}} \mathrm{E}}$. Thus, we have the orthogonality relation of characters

$$\sum_{\mathbf{c} \in C} \chi_{\mathbf{b}}(\mathbf{c}) = \begin{cases} |C| & \text{if } \mathbf{b} \in C^{\perp_{\mathrm{Tr}_{q/r}} \mathrm{E}} \\ 0 & \text{otherwise} \end{cases}. \quad \text{(VII.2)}$$

By (VII.2),

$$\sum_{\mathbf{c} \in C} \sum_{\mathbf{b} \in \mathbb{F}_q^n} \chi_{\mathbf{b}}(\mathbf{c}) Y^{\mathrm{wt_H}(\mathbf{b})} = \sum_{\mathbf{b} \in \mathbb{F}_q^n} Y^{\mathrm{wt_H}(\mathbf{b})} \sum_{\mathbf{c} \in C} \chi_{\mathbf{b}}(\mathbf{c}) = |C| \sum_{i=0}^n B_i Y^i = |C| \cdot B(Y). \quad \text{(VII.3)}$$

Let us take a closer look at the inner sum on the left hand side of (VII.3). By the property of the trace mapping, we can distribute the trace mapping over each coordinate.

$$\sum_{\mathbf{b} \in \mathbb{F}_q^n} \chi_{\mathbf{b}}(\mathbf{c}) Y^{\mathrm{wt_H}(\mathbf{b})}$$

TABLE VII
NESTED PAIRS OF CYCLIC CODES OVER $\mathbb{F}_5$ YIELDING OPTIMAL ASYMMETRIC CSS CODES IN TABLE VI

C and D	Generator Polynomials	AQC Q	C and D	Generator Polynomials	AQC Q
$[6,3,4]_5$	$g=(1221)$	$[[6,2,4/2]]_5$	$[13,9,4]_5$	$g=(11411)$	$[[13,1,7/4]]_5$
$[6,1,6]_5$	$(141)g$		$[13,8,4]_5$	$(41)g$	
$[8,7,2]_5$	$g=(11)$	$[[8,4,3/2]]_5$	$[15,2,12]_5$	$g=(43210432104321)$	$[[15,1,12/2]]_5$
$[8,3,4]_5$	$(11021)g$		$[15,1,15]_5$	$(41)g$	
$[8,7,2]_5$	$g=(11)$	$[[8,3,4/2]]_5$	$[20,17,3]_5$	$g=(4021)$	$[[20,16,3/2]]_5$
$[8,4,4]_5$	$(4221)g$		$[20,1,20]_5$	$(14331311124411221)g$	
$[8,7,2]_5$	$g=(11)$	$[[8,1,6/2]]_5$	$[20,3,15]_5$	$g=(333210144241242301)$	$[[20,2,15/2]]_5$
$[8,6,2]_5$	$(21)g$		$[20,1,20]_5$	$(121)g$	
$[8,5,3]_5$	$g=(2211)$	$[[8,2,3/3]]_5$	$[20,2,16]_5$	$g=(4321043210432104321)$	$[[20,1,16/2]]_5$
$[8,3,4]_5$	$(311)g$		$[20,1,20]_5$	$(41)g$	
$[8,5,3]_5$	$g=(2211)$	$[[8,1,4/3]]_5$	$[20,17,3]_5$	$g=(4021)$	$[[20,14,3/3]]_5$
$[8,4,4]_5$	$(21)g$		$[20,3,15]_5$	$(104020303020401)g$	
$[10,7,3]_5$	$g=(4411)$	$[[10,6,3/2]]_5$	$[24,23,2]_5$	$g=(11)$	$[[24,20,3/2]]_5$
$[10,1,10]_5$	$(4030201)g$		$[24,3,19]_5$	$(311434221121401242041)g$	
$[10,6,4]_5$	$g=(42031)$	$[[10,5,4/2]]_5$	$[24,23,2]_5$	$g=(11)$	$[[24,19,4/2]]_5$
$[10,1,10]_5$	$(113311)g$		$[24,4,18]_5$	$(1102233024111314013 1)g$	
$[10,2,8]_5$	$g=(432104321)$	$[[10,1,8/2]]_5$	$[24,4,18]_5$	$g=(1424202132043330223 31)$	$[[24,3,18/2]]_5$
$[10,1,10]_5$	$(41)g$		$[24,1,24]_5$	$(2101)g$	
$[10,7,3]_5$	$g=(4411)$	$[[10,4,3/3]]_5$	$[24,3,19]_5$	$g=(20342212301141324404 31)$	$[[24,2,19/2]]_5$
$[10,3,5]_5$	$(10301)g$		$[24,1,24]_5$	$(331)g$	
$[10,7,3]_5$	$g=(4411)$	$[[10,3,4/3]]_5$	$[24,21,3]_5$	$g=(1041)$	$[[24,18,3/3]]_5$
$[10,4,5]_5$	$(4411)g$		$[24,3,19]_5$	$(4241414203021111121)g$	
$[10,6,4]_5$	$g=(42031)$	$[[10,2,4/4]]_5$	$[24,21,3]_5$	$g=(1041)$	$[[24,17,4/3]]_5$
$[10,4,5]_5$	$(401)g$		$[24,4,18]_5$	$(124440331133044421)g$	
$[11,6,5]_5$	$g=(431441)$	$[[11,5,5/2]]_5$	$[24,4,18]_5$	$g=(142420213204333022331)$	$[[24,1,18/3]]_5$
$[11,1,11]_5$	$(411421)g$		$[24,3,19]_5$	$(21)g$	
$[11,6,5]_5$	$g=(431441)$	$[[11,1,5/5]]_5$	$[24,20,4]_5$	$g=(41131)$	$[[24,16,4/4]]_5$
$[11,5,6]_5$	$(41)g$		$[24,4,18]_5$	$(402040400004010201)g$	
$[12,9,3]_5$	$g=(2331)$	$[[12,8,3/2]]_5$	$[30,25,4]_5$	$g=(142241)$	$[[30,24,4/2]]_5$
$[12,1,12]_5$	$(411302441)g$		$[30,1,30]_5$	$(40140244243203213113 01401)g$	
$[12,8,4]_5$	$g=(33301)$	$[[12,7,4/2]]_5$	$[30,25,4]_5$	$g=(142241)$	$[[30,20,4/4]]_5$
$[12,1,12]_5$	$(12144121)g$		$[30,5,18]_5$	$(102030002040200030201)g$	
$[12,11,2]_5$	$g=(11)$	$[[12,1,9/2]]_5$	$[31,30,2]_5$	$g=(41)$	$[[31,27,3/2]]_5$
$[12,10,2]_5$	$(21)g$		$[31,3,25]_5$	$(41310132340322121133 12241021)g$	
$[12,9,3]_5$	$g=(2331)$	$[[12,6,3/3]]_5$	$[31,28,3]_5$	$g=(4031)$	$[[31,25,3/3]]_5$
$[12,3,8]_5$	$(2313311)g$		$[31,3,25]_5$	$(41200111423221200310021331)g$	
$[12,9,3]_5$	$g=(2331)$	$[[12,5,4/3]]_5$	$[35,2,28]_5$	$g=(4321043210432104321043210432104321)$	$[[35,1,28/2]]_5$
$[12,4,6]_5$	$(232141)g$		$[35,1,35]_5$	$(41)g$	
$[12,9,3]_5$	$g=(2331)$	$[[12,1,7/3]]_5$	$[39,35,3]_5$	$g=(14101)$	$[[39,34,3/2]]_5$
$[12,8,4]_5$	$(11)g$		$[39,1,39]_5$	$(1221422004303001441233014132141 1011)g$	
$[12,8,4]_5$	$g=(33301)$	$[[12,4,4/4]]_5$	$[39,35,3]_5$	$g=(14101)$	$[[39,31,3/3]]_5$
$[12,4,7]_5$	$(10401)g$		$[39,4,28]_5$	$(44111344333444200311122211244411)g$	
$[13,9,4]_5$	$g=(11411)$	$[[13,8,4/2]]_5$	$[40,39,2]_5$	$g=(11)$	$[[40,35,3/2]]_5$
$[13,1,13]_5$	$(102343201)g$		$[40,4,20]_5$	$(343224310313431222441243412031241001)g$	
$[13,12,2]_5$	$g=(41)$	$[[13,4,7/2]]_5$	$[40,2,32]_5$	$g=(14220234404133032110142202344041330321 1)$	$[[40,1,32/2]]_5$
$[13,8,4]_5$	$(13031)g$		$[40,1,40]_5$	$(21)g$	
$[13,9,4]_5$	$g=(11411)$	$[[13,5,4/4]]_5$			
$[13,4,8]_5$	$(441411)g$				

$$= \sum_{(b_1,b_2,\ldots,b_n)\in\mathbb{F}_q^n} \left(Y^{\left(\sum_{i=1}^{n} \mathrm{wt}_{\mathrm{H}}(b_i)\right)} \right) \chi\left(\sum_{i=1}^{n} \mathrm{Tr}_{q/r}(b_i c_i) \right)$$

$$= \sum_{(b_1,b_2,\ldots,b_n)\in\mathbb{F}_q^n} \left(\prod_{i=1}^{n} Y^{\mathrm{wt}_{\mathrm{H}}(b_i)} \cdot \chi\left(\mathrm{Tr}_{q/r}(b_i c_i)\right) \right)$$

$$= \prod_{i=1}^{n} \sum_{b_i\in\mathbb{F}_q} Y^{\mathrm{wt}_{\mathrm{H}}(b_i)} \chi\left(\mathrm{Tr}_{q/r}(b_i c_i)\right). \quad \text{(VII.4)}$$

Note that if $(c_i, b_i) = (0, 0)$, the contribution to the sum in the right hand side is 1. If $c_i = 0$ but $b_i \neq 0$, the contribution to the sum is $(q-1)Y$. Similarly, for $c_i \neq 0$, if $b_i = 0$, we get 1, while if $b_i \neq 0$, we get $-Y$. Therefore, the sum in the right hand side of (VII.4) can be simplified to

$$\sum_{b_i\in\mathbb{F}_q} Y^{\mathrm{wt}_{\mathrm{H}}(b_i)} \chi\left(\mathrm{Tr}_{q/r}(b_i c_i)\right) = \begin{cases} 1+(q-1)Y & \text{if } c_i = 0 \\ 1-Y & \text{if } c_i \neq 0 \end{cases}, \quad \text{(VII.5)}$$

yielding, after plugging this result back to (VII.3),

$$B(Y) = \frac{1}{|C|} \sum_{\mathbf{c}\in C} \sum_{\mathbf{b}\in\mathbb{F}_q^n} \chi_{\mathbf{b}}(\mathbf{c}) Y^{\mathrm{wt}_{\mathrm{H}}(\mathbf{b})}$$

$$= \frac{1}{|C|} \sum_{\mathbf{c}\in C} \left(1+(q-1)Y\right)^{n-\mathrm{wt}_{\mathrm{H}}(\mathbf{c})} (1-Y)^{\mathrm{wt}_{\mathrm{H}}(\mathbf{c})}$$

$$= \frac{1}{|C|} \left(1+(q-1)Y\right)^{n} \sum_{\mathbf{c}\in C} \left(\frac{(1-Y)}{1+(q-1)Y} \right)^{\mathrm{wt}_{\mathrm{H}}(\mathbf{c})}$$

$$= \frac{\left(1+(q-1)Y\right)^{n}}{|C|} \cdot A\left(\frac{(1-Y)}{1+(q-1)Y} \right).$$

TABLE VIII
OPTIMAL PURE ASYMMETRIC CSS CODES OVER $\mathbb{F}_7$

No.	AQC Q	Type	No.	AQC Q	Type	No.	AQC Q	Type	No.	AQC Q	Type
1	$[[9,5,3/2]]_7$	GC	39	$[[14,9,4/2]]_7$	BC,CC	77	$[[17,5,10/2]]_7$	BC	115	$[[21,15,3/3]]_7$	CC
2	$[[9,4,4/2]]_7$	BC	40	$[[14,8,5/2]]_7$	BC	78	$[[17,4,11/2]]_7$	BC	116	$[[22,18,3/2]]_7$	BC
3	$[[9,3,5/2]]_7$	BC	41	$[[14,7,6/2]]_7$	BC	79	$[[17,3,12/2]]_7$	BC	117	$[[22,17,4/2]]_7$	BC
4	$[[9,2,6/2]]_7$	BC,GC	42	$[[14,6,7/2]]_7$	BC	80	$[[17,2,13/2]]_7$	BC	118	$[[22,2,18/2]]_7$	BC
5	$[[9,1,7/2]]_7$	BC	43	$[[14,4,8/2]]_7$	BC	81	$[[17,1,14/2]]_7$	BC	119	$[[23,19,3/2]]_7$	BC
6	$[[10,6,3/2]]_7$	BC	44	$[[14,3,10/2]]_7$	BC	82	$[[18,14,3/2]]_7$	BC	120	$[[23,18,4/2]]_7$	BC
7	$[[10,5,4/2]]_7$	BC	45	$[[14,2,11/2]]_7$	BC	83	$[[18,13,4/2]]_7$	BC	121	$[[24,20,3/2]]_7$	BC,CC
8	$[[10,4,5/2]]_7$	BC	46	$[[14,1,12/2]]_7$	CC	84	$[[18,12,5/2]]_7$	BC	122	$[[24,19,4/2]]_7$	BC
9	$[[10,3,6/2]]_7$	BC	47	$[[14,8,3/3]]_7$	CC	85	$[[18,8,8/2]]_7$	BC	123	$[[24,2,19/2]]_7$	BC
10	$[[10,2,7/2]]_7$	BC	48	$[[14,7,4/3]]_7$	CC	86	$[[18,7,9/2]]_7$	BC	124	$[[24,1,20/2]]_7$	CC
11	$[[10,1,8/2]]_7$	BC	49	$[[14,6,4/4]]_7$	CC	87	$[[18,5,11/2]]_7$	BC	125	$[[24,18,3/3]]_7$	CC
12	$[[11,7,3/2]]_7$	BC	50	$[[15,11,3/2]]_7$	BC	88	$[[18,4,12/2]]_7$	BC	126	$[[24,17,4/3]]_7$	CC
13	$[[11,6,4/2]]_7$	BC	51	$[[15,10,4/2]]_7$	BC	89	$[[18,3,13/2]]_7$	BC	127	$[[24,16,4/4]]_7$	CC
14	$[[11,5,5/2]]_7$	BC	52	$[[15,9,5/2]]_7$	BC	90	$[[18,2,14/2]]_7$	BC	128	$[[25,21,3/2]]_7$	BC
15	$[[11,4,6/2]]_7$	BC	53	$[[15,8,6/2]]_7$	BC	91	$[[18,1,15/2]]_7$	BC,CC	129	$[[25,20,4/2]]_7$	BC,CC
16	$[[11,3,7/2]]_7$	BC	54	$[[15,5,8/2]]_7$	BC	92	$[[19,15,3/2]]_7$	BC,CC	130	$[[25,3,19/2]]_7$	BC
17	$[[11,2,8/2]]_7$	BC	55	$[[15,4,9/2]]_7$	BC	93	$[[19,14,4/2]]_7$	BC	131	$[[25,2,20/2]]_7$	BC
18	$[[11,1,9/2]]_7$	BC	56	$[[15,3,10/2]]_7$	BC	94	$[[19,9,8/2]]_7$	BC,CC	132	$[[25,17,4/4]]_7$	CC
19	$[[12,8,3/2]]_7$	BC,CC	57	$[[15,2,12/2]]_7$	BC	95	$[[19,8,9/2]]_7$	BC	133	$[[26,22,3/2]]_7$	BC
20	$[[12,7,4/2]]_7$	BC,CC	58	$[[16,12,3/2]]_7$	BC,CC	96	$[[19,5,12/2]]_7$	BC	134	$[[26,21,4/2]]_7$	BC
21	$[[12,6,5/2]]_7$	BC	59	$[[16,11,4/2]]_7$	BC,CC	97	$[[19,4,13/2]]_7$	BC	135	$[[26,3,20/2]]_7$	BC
22	$[[12,5,6/2]]_7$	BC	60	$[[16,10,5/2]]_7$	BC	98	$[[19,3,14/2]]_7$	BC	136	$[[26,2,21/2]]_7$	BC
23	$[[12,4,7/2]]_7$	BC	61	$[[16,6,8/2]]_7$	BC,CC	99	$[[19,2,15/2]]_7$	BC	137	$[[27,23,3/2]]_7$	BC
24	$[[12,3,8/2]]_7$	BC	62	$[[16,5,9/2]]_7$	BC	100	$[[19,13,3/3]]_7$	CC	138	$[[27,22,4/2]]_7$	BC
25	$[[12,2,9/2]]_7$	BC	63	$[[16,4,10/2]]_7$	BC,CC	101	$[[19,7,8/3]]_7$	CC	139	$[[27,2,22/2]]_7$	BC
26	$[[12,1,10/2]]_7$	BC,CC	64	$[[16,3,11/2]]_7$	BC	102	$[[19,6,9/3]]_7$	CC	140	$[[28,24,3/2]]_7$	BC
27	$[[12,6,3/3]]_7$	CC	65	$[[16,2,12/2]]_7$	BC,CC	103	$[[19,3,12/3]]_7$	CC	141	$[[28,23,4/2]]_7$	BC
28	$[[12,5,4/3]]_7$	CC	66	$[[16,10,3/3]]_7$	CC	104	$[[19,1,8/8]]_7$	CC	142	$[[28,2,23/2]]_7$	BC
29	$[[12,4,4/4]]_7$	CC	67	$[[16,9,4/3]]_7$	CC	105	$[[20,16,3/2]]_7$	BC	143	$[[28,1,24/2]]_7$	CC
30	$[[13,9,3/2]]_7$	BC	68	$[[16,4,8/3]]_7$	CC	106	$[[20,15,4/2]]_7$	BC	144	$[[29,25,3/2]]_7$	BC
31	$[[13,8,4/2]]_7$	BC	69	$[[16,2,10/3]]_7$	CC	107	$[[20,9,9/2]]_7$	BC	145	$[[29,24,4/2]]_7$	BC
32	$[[13,7,5/2]]_7$	BC	70	$[[16,8,4/4]]_7$	CC	108	$[[20,4,14/2]]_7$	BC	146	$[[29,22,5/2]]_7$	BC
33	$[[13,6,6/2]]_7$	BC	71	$[[16,3,8/4]]_7$	CC	109	$[[20,3,15/2]]_7$	BC	147	$[[29,2,24/2]]_7$	BC
34	$[[13,5,7/2]]_7$	BC	72	$[[17,13,3/2]]_7$	BC	110	$[[20,2,16/2]]_7$	BC	148	$[[30,26,3/2]]_7$	BC
35	$[[13,4,8/2]]_7$	BC	73	$[[17,12,4/2]]_7$	BC	111	$[[21,17,3/2]]_7$	BC,CC	149	$[[30,25,4/2]]_7$	BC
36	$[[13,3,9/2]]_7$	BC	74	$[[17,11,5/2]]_7$	BC	112	$[[21,16,4/2]]_7$	BC	150	$[[30,23,5/2]]_7$	BC
37	$[[13,2,10/2]]_7$	BC	75	$[[17,7,8/2]]_7$	BC	113	$[[21,2,17/2]]_7$	BC	151	$[[30,22,6/2]]_7$	BC
38	$[[14,10,3/2]]_7$	BC,CC	76	$[[17,6,9/2]]_7$	BC	114	$[[21,1,18/2]]_7$	CC	152	$[[30,1,25/2]]_7$	CC

TABLE IX
NESTED PAIRS OF CYCLIC CODES OVER $\mathbb{F}_7$ YIELDING OPTIMAL ASYMMETRIC CSS CODES IN TABLE VIII

C and D	Generator Polynomials	AQC Q	C and D	Generator Polynomials	AQC Q
$[12,9,3]_7$	$g=(2441)$	$[[12,6,3/3]]_7$	$[19,10,8]_7$	$g=(6520313561)$	$[[19,7,8/3]]_7$
$[12,3,6]_7$	$(5651121)g$		$[19,3,15]_7$	$(66666221)g$	
$[12,8,4]_7$	$g=(16261)$	$[[12,5,4/3]]_7$	$[19,16,3]_7$	$g=(6331)$	$[[19,6,9/3]]_7$
$[12,3,6]_7$	$(412621)g$		$[19,10,8]_7$	$(1203561)g$	
$[12,8,4]_7$	$g=(16261)$	$[[12,4,4/4]]_7$	$[19,6,12]_7$	$g=(63116244011501)$	$[[19,3,12/3]]_7$
$[12,4,6]_7$	$(21121)g$		$[19,3,15]_7$	$(6331)g$	
$[14,13,2]_7$	$g=(11)$	$[[14,1,12/2]]_7$	$[19,10,8]_7$	$g=(6520313561)$	$[[19,1,8/8]]_7$
$[14,12,2]_7$	$(11)g$		$[19,9,9]_7$	$(61)g$	
$[14,11,3]_7$	$g=(6611)$	$[[14,8,3/3]]_7$	$[21,2,18]_7$	$g=(35152206323440564611)$	$[[21,1,18/2]]_7$
$[14,3,7]_7$	$(622106551)g$		$[21,1,21]_7$	$(31)g$	
$[14,11,3]_7$	$g=(6611)$	$[[14,7,4/3]]_7$	$[21,18,3]_7$	$g=(3121)$	$[[21,15,3/3]]_7$
$[14,4,7]_7$	$(66334411)g$		$[21,3,14]_7$	$(3443550331556441)g$	
$[14,10,4]_7$	$g=(65021)$	$[[14,6,4/4]]_7$	$[24,2,20]_7$	$g=(2564102564102564102564 1)$	$[[24,1,20/2]]_7$
$[14,4,7]_7$	$(6030401)g$		$[24,1,24]_7$	$(61)g$	
$[16,13,3]_7$	$g=(1051)$	$[[16,10,3/3]]_7$	$[24,21,3]_7$	$g=(2031)$	$[[24,18,3/3]]_7$
$[16,3,12]_7$	$(13203030241)g$		$[24,3,18]_7$	$(520320402205052655 1)g$	
$[16,12,4]_7$	$g=(63031)$	$[[16,9,4/3]]_7$	$[24,20,4]_7$	$g=(65161)$	$[[24,17,4/3]]_7$
$[16,3,12]_7$	$(1340044061)g$		$[24,3,18]_7$	$(300162464233164141)g$	
$[16,7,8]_7$	$g=(1265630161)$	$[[16,4,8/3]]_7$	$[24,20,4]_7$	$g=(65161)$	$[[24,16,4/4]]_7$
$[16,3,12]_7$	$(60211)g$		$[24,4,16]_7$	$(25340520601502331)g$	
$[16,5,10]_7$	$g=(611361010341)$	$[[16,2,10/3]]_7$	$[25,21,4]_7$	$g=(14041)$	$[[25,17,4/4]]_7$
$[16,3,12]_7$	$(131)g$		$[25,4,19]_7$	$(636241612561635141)g$	
$[16,12,4]_7$	$g=(16511)$	$[[16,8,4/4]]_7$	$[28,27,2]_7$	$g=(11)$	$[[28,1,24/2]]_7$
$[16,4,8]_7$	$(103020301)g$		$[28,26,2]_7$	$(11)g$	
$[16,7,8]_7$	$g=(1626554051)$	$[[16,3,8/4]]_7$	$[30,29,2]_7$	$g=(11)$	$[[30,1,25/2]]_7$
$[16,4,8]_7$	$(1551)g$		$[30,28,2]_7$	$(31)g$	
$[19,16,3]_7$	$g=(6331)$	$[[19,13,3/3]]_7$			
$[19,3,15]_7$	$(62600465666441)g$				

TABLE XI
GOOD PURE ASYMMETRIC CSS-LIKE CODES OVER $\mathbb{F}_4$

No.	AQC Q	Type	LP	Def	Remarks
1	$[[6,2,4/2]]_4$	ACC	2	0	Optimal
2	$[[6,1,3/3]]_4$	ACC	1	0	Optimal
3	$[[7,3,3/2]]_4$	BC	3.5	0.5	OpLin
4	$[[7,2,4/2]]_4$	BC	2.5	0.5	OpLin
5	$[[7,1.5,5/2]]_4$	ACC	1.5	0	Optimal,BeOpLin
6	$[[8,4,3/2]]_4$	BC	4.5	0.5	OpLin
7	$[[8,3,4/2]]_4$	BC	3.5	0.5	OpLin
8	$[[8,2,5/2]]_4$	BC	2.5	0.5	OpLin
9	$[[8,1,6/2]]_4$	BC	1.5	0.5	OpLin
10	$[[9,5,3/2]]_4$	BC	5.5	0.5	OpLin
11	$[[9,4,4/2]]_4$	BC	4.5	0.5	OpLin
12	$[[9,3,5/2]]_4$	BC	3.5	0.5	OpLin
13	$[[9,2,6/2]]_4$	BC	2.5	0.5	OpLin
14	$[[10,6,3/2]]_4$	BC	6	0	Optimal
15	$[[10,5,4/2]]_4$	BC	5.5	0.5	OpLin
16	$[[10,4,5/2]]_4$	BC	4.5	0.5	OpLin
17	$[[10,3,6/2]]_4$	BC	3.5	0.5	OpLin
18	$[[10,4,3/3]]_4$	SO	4	0	Optimal
19	$[[11,7,3/2]]_4$	BC	7	0	Optimal
20	$[[11,6,4/2]]_4$	BC	6	0	Optimal
21	$[[11,5,5/2]]_4$	BC	5	0	Optimal
22	$[[11,5,3/3]]_4$	SO	5	0	Optimal
23	$[[11,1,5/5]]_4$	CC	1	0	Optimal
24	$[[12,8,3/2]]_4$	BC	8	0	Optimal
25	$[[12,7,4/2]]_4$	BC	7	0	Optimal
26	$[[12,5.5,5/2]]_4$	ACC	5.5	0	Optimal,BeOpLin
27	$[[12,5,6/2]]_4$	BC	5	0	Optimal
28	$[[12,3,7/2]]_4$	BC	3.5	0.5	OpLin
29	$[[12,2,8/2]]_4$	BC	2.5	0.5	OpLin
30	$[[12,1,9/2]]_4$	ACC	1.5	0.5	ROpLin
31	$[[12,6,3/3]]_4$	ACC,SO	6	0	Optimal
32	$[[12,3.5,5/3]]_4$	ACC	3.5	0	Optimal,BeOpLin
33	$[[12,3,6/3]]_4$	ACC	3	0	Optimal
34	$[[12,4,4/4]]_4$	ACC,SO	4	0	Optimal
35	$[[12,2,5/4]]_4$	ACC	2.5	0.5	ROpLin
36	$[[12,1,5/5]]_4$	ACC	1.5	0.5	ROpLin
37	$[[13,9,3/2]]_4$	BC	9	0	Optimal
38	$[[13,8,4/2]]_4$	BC	8	0	Optimal
39	$[[13,6,5/2]]_4$	BC	6.5	0.5	OpLin
40	$[[13,5,6/2]]_4$	BC	5.5	0.5	OpLin
41	$[[13,4,7/2]]_4$	BC	4.5	0.5	OpLin
42	$[[13,2,9/2]]_4$	BC	4.5	0.5	OpLin
43	$[[13,7,3/3]]_4$	SO	7	0	Optimal
44	$[[14,10,3/2]]_4$	BC	10	0	Optimal
45	$[[14,9,4/2]]_4$	BC	9	0	Optimal
46	$[[14,7,5/2]]_4$	BC	7.5	0.5	OpLin
47	$[[14,6,6/2]]_4$	BC	6.5	0.5	OpLin
48	$[[14,5,7/2]]_4$	BC	5.5	0.5	OpLin
49	$[[14,4,8/2]]_4$	BC	4.5	0.5	OpLin
50	$[[14,3,9/2]]_4$	BC	3.5	0.5	OpLin
51	$[[14,2,10/2]]_4$	BC	2.5	0.5	OpLin
52	$[[14,8,3/3]]_4$	ACC,SO	8	0	Optimal
53	$[[14,7,4/3]]_4$	ACC	7	0	Optimal
54	$[[14,5,5/3]]_4$	ACC	5.5	0.5	ROpLin
55	$[[14,4,6/3]]_4$	ACC	4.5	0.5	ROpLin
56	$[[14,3,7/3]]_4$	ACC	3.5	0.5	ROpLin
57	$[[14,6,4/4]]_4$	ACC,SO	6	0	Optimal
58	$[[14,4,5/4]]_4$	ACC	4.5	0.5	ROpLin
59	$[[14,3,6/4]]_4$	ACC	3.5	0.5	ROpLin
60	$[[15,11,3/2]]_4$	BC	11	0	Optimal
61	$[[15,10,4/2]]_4$	BC	10	0	Optimal
62	$[[15,8,5/2]]_4$	BC	8.5	0.5	OpLin
63	$[[15,7,6/2]]_4$	BC	7.5	0.5	OpLin
64	$[[15,6,7/2]]_4$	BC	6.5	0.5	OpLin
65	$[[15,3,10/2]]_4$	BC	3	0	Optimal
66	$[[15,2,11/2]]_4$	BC	2	0	Optimal
67	$[[15,9,3/3]]_4$	CC,SO	9	0	Optimal
68	$[[15,8,4/3]]_4$	CC	8	0	Optimal
69	$[[15,6,5/3]]_4$	CC	6.5	0.5	OpLin
70	$[[15,5,6/3]]_4$	CC	5.5	0.5	OpLin
71	$[[15,4,7/3]]_4$	CC	4.5	0.5	OpLin
72	$[[15,1,10/3]]_4$	CC	1	0	Optimal
73	$[[15,5,5/4]]_4$	CC	5.5	0.5	OpLin
74	$[[15,4,6/4]]_4$	CC	4.5	0.5	OpLin
75	$[[16,12,3/2]]_4$	BC	12	0	Optimal
76	$[[16,11,4/2]]_4$	BC	11	0	Optimal
77	$[[16,9,5/2]]_4$	BC	9.5	0.5	OpLin
78	$[[16,8,6/2]]_4$	BC	8.5	0.5	OpLin
79	$[[16,7,7/2]]_4$	BC	7.5	0.5	OpLin
80	$[[16,6,8/2]]_4$	BC	6.5	0.5	OpLin
81	$[[16,3,11/2]]_4$	BC	3	0	Optimal
82	$[[16,2,12/2]]_4$	BC	2	0	Optimal
83	$[[16,10,3/3]]_4$	SO	10	0	Optimal
84	$[[17,13,3/2]]_4$	BC	13	0	Optimal
85	$[[17,12,4/2]]_4$	BC	12	0	Optimal
86	$[[17,10,5/2]]_4$	BC	10.5	0.5	OpLin
87	$[[17,9,6/2]]_4$	BC	9.5	0.5	OpLin
88	$[[17,8,7/2]]_4$	BC	8.5	0.5	OpLin
89	$[[17,9,4/4]]_4$	CC,SO	9	0	Optimal
90	$[[17,5,7/4]]_4$	CC	5.5	0.5	OpLin
91	$[[17,4,8/4]]_4$	CC	4.5	0.5	OpLin
92	$[[18,14,3/2]]_4$	BC	14	0	Optimal
93	$[[18,12,4/2]]_4$	BC	12.5	0.5	OpLin
94	$[[18,11,5/2]]_4$	BC	11.5	0.5	OpLin
95	$[[18,10,6/2]]_4$	BC	10.5	0.5	OpLin
96	$[[18,8,8/2]]_4$	BC	8.5	0.5	OpLin
97	$[[18,5,10/2]]_4$	BC	5.5	0.5	OpLin
98	$[[19,15,3/2]]_4$	BC	15	0	Optimal
99	$[[19,13,4/2]]_4$	BC	13.5	0.5	OpLin
100	$[[19,12,5/2]]_4$	BC	12.5	0.5	OpLin
101	$[[19,11,6/2]]_4$	BC	11.5	0.5	OpLin
102	$[[20,16,3/2]]_4$	BC	16	0	Optimal
103	$[[20,14,4/2]]_4$	BC	14.5	0.5	OpLin
104	$[[20,13,5/2]]_4$	BC	13.5	0.5	OpLin
105	$[[20,12,6/2]]_4$	BC	12.5	0.5	OpLin
106	$[[20,10,7/2]]_4$	BC	10.5	0.5	OpLin
107	$[[21,17,3/2]]_4$	BC	17	0	Optimal
108	$[[21,15,4/2]]_4$	BC	15.5	0.5	OpLin
109	$[[21,14,5/2]]_4$	BC	14	0	Optimal
110	$[[21,11,7/2]]_4$	BC	11.5	0.5	OpLin
111	$[[21,15,3/3]]_4$	SO	15	0	Optimal
112	$[[22,17,3/2]]_4$	BC	17.5	0.5	OpLin
113	$[[22,16,4/2]]_4$	BC	16.5	0.5	OpLin
114	$[[22,4,14/2]]_4$	BC	4.5	0.5	OpLin
115	$[[23,18,3/2]]_4$	BC	18.5	0.5	OpLin
116	$[[23,17,4/2]]_4$	BC	17.5	0.5	OpLin
117	$[[23,4,15/2]]_4$	BC	4.5	0.5	OpLin
118	$[[24,19,3/2]]_4$	BC	19.5	0.5	OpLin
119	$[[24,18,4/2]]_4$	BC	18.5	0.5	OpLin
120	$[[24,8,12/2]]_4$	BC	8.5	0.5	OpLin
121	$[[25,20,3/2]]_4$	BC	20.5	0.5	OpLin
122	$[[25,19,4/2]]_4$	BC	19.5	0.5	OpLin
123	$[[26,21,3/2]]_4$	BC	21.5	0.5	OpLin
124	$[[26,20,4/2]]_4$	BC	20.5	0.5	OpLin
125	$[[26,10,12/2]]_4$	BC	10.5	0.5	OpLin
126	$[[27,22,3/2]]_4$	BC	22.5	0.5	OpLin
127	$[[27,21,4/2]]_4$	BC	21.5	0.5	OpLin
128	$[[28,23,3/2]]_4$	BC	23.5	0.5	OpLin
129	$[[28,22,4/2]]_4$	BC	22.5	0.5	OpLin
130	$[[28,13,11/2]]_4$	BC	13.5	0.5	OpLin
131	$[[28,12,12/2]]_4$	BC	12.5	0.5	OpLin
132	$[[29,24,3/2]]_4$	BC	24.5	0.5	OpLin
133	$[[29,23,4/2]]_4$	BC	23.5	0.5	OpLin
134	$[[30,22,5/2]]_4$	BC	22.5	0.5	OpLin
135	$[[30,14,12/2]]_4$	BC	14.5	0.5	OpLin

TABLE XII
NESTED PAIRS OF $\mathbb{F}_2$-LINEAR CYCLIC CODES OVER $\mathbb{F}_4$ YIELDING OPTIMAL OR GOOD ASYMMETRIC CSS-LIKE CODES IN TABLE XI

C and D	Generator Polynomials	AQC Q
$(6,2^6,4)_4$	$g_4=(1011)+w(11)$, $g_2=(111111)$	$[[6,2,4/2]]_4$
$(6,2^2,6)_4$	$(10101)g_4$, $(1)g_2$	
$(6,2^7,3)_4$	$g_4=(101)+w(11)$, $g_2=(10101)$	$[[6,1,3/3]]_4$
$(6,2^5,4)_4$	$(11)g_4$, $(11)g_2$	
$(7,2^5,5)_4$	$g_4=(11101)+w(1011)$, $g_2=(1111111)$	$[[7,1.5,5/2]]_4$
$(7,2^2,7)_4$	$(1101)g_4$, $(1)g_2$	
$(12,2^{13},5)_4$	$g_4=(001110001)+w(1)$, $g_2=(111111111111)$	$[[12,5.5,5/2]]_4$
$(12,2^2,12)_4$	$(111111111111)g_4$, $(1)g_2$	
$(12,2^4,9)_4$	$g_4=(00100010001)+w(1100110011)$, $g_2=(111111111111)$	$[[12,1,9/2]]_4$
$(12,2^2,12)_4$	$(101)g_4$, $(1)g_2$	
$(12,2^{18},3)_4$	$g_4=(0001)+w(11)$, $g_2=(101101)$	$[[12,6,3/3]]_4$
$(12,2^6,8)_4$	$(1101011)g_4$, $(1101011)g_2$	
$(12,2^{13},5)_4$	$g_4=(000101001)+w(11)$, $g_2=(10101010101)$	$[[12,7/2,5/3]]_4$
$(12,2^6,8)_4$	$(1101011)g_4$, $(11)g_2$	
$(12,2^{12},6)_4$	$g_4=(001110101)+w(11)$, $g_2=(111111111111)$	$[[12,3,6/3]]_4$
$(12,2^6,8)_4$	$(1101011)g_4$, $(1)g_2$	
$(12,2^7,7)_4$	$g_4=(1000010011)+w(1110111)$, $g_2=(111111111111)$	$[[12,0.5,7/3]]_4$
$(12,2^6,8)_4$	$(1)g_4$, $(11)g_2$	
$(12,2^{16},4)_4$	$g_4=(1101)+w(111)$,$g_2=(1110111)$	$[[12,4,4/4]]_4$
$(12,2^8,6)_4$	$(10101)g_4$, $(10101)g_2$	
$(12,2^{12},5)_4$	$g_4=(1000101)+w(111)$, $g_2=(11011011011)$	$[[12,2,5/4]]_4$
$(12,2^8,7)_4$	$(10101)g_4$, $(1)g_2$	
$(12,2^{10},6)_4$	$g_4=(01100101)+w(10101)$, $g_2=(11011011011)$	$[[12,1,6/4]]_4$
$(12,2^8,6)_4$	$(111)g_4$, $(1)g_2$	
$(12,2^{13},5)_4$	$g_4=(001101)+w(11)$, $g_2=(10101010101)$	$[[12,1,5/5]]_4$
$(12,2^{11},5)_4$	$(11)g_4$, $(11)g_2$	
$(14,2^{22},3)_4$	$g_4=(011)+w(1)$, $g_2=(1000101)$	$[[14,8,3/3]]_4$
$(14,2^6,10)_4$	$(101010001)g_4$, $(100010101)g_2$	
$(14,2^{20},4)_4$	$g_4=(00001011)+w(1)$,$g_2=(101010001)$	$[[14,7,4/3]]_4$
$(14,2^6,10)_4$	$(101010001)g_4$, $(1010001)g_2$	
$(14,2^{22},3)_4$	$g_4=(010111)+w(1)$,$g_2=(1000101)$	$[[14,5,5/3]]_4$
$(14,2^{12},6)_4$	$(101)g_4$, $(100010101)g_2$	
$(14,2^{14},6)_4$	$g_4=(110011101)+w(101)$, $g_2=(1010101010101)$	$[[14,4,6/3]]_4$
$(14,2^6,10)_4$	$(1010001)g_4$, $(101)g_2$	
$(14,2^{12},7)_4$	$g_4=(010111011)+w(101)$, $g_2=(100000000000001)$	$[[14,3,7/3]]_4$
$(14,2^6,10)_4$	$(1000101)g_4$, $(1)g_2$	
$(14,2^{20},4)_4$	$g_4=(001011)+w(11)$,$g_2=(11001111)$	$[[14,6,4/4]]_4$
$(14,2^8,8)_4$	$(1010001)g_4$, $(1010001)g_2$	
$(14,2^{20},4)_4$	$g_4=(01001)+w(1011)$,$g_2=(100111)$	$[[14,4,5/4]]_4$
$(14,2^{12},6)_4$	$(101)g_4$, $(1010001)g_2$	
$(14,2^{14},6)_4$	$g_4=(0001010111)+w(11)$, $g_2=(11111111111111)$	$[[14,3,6/4]]_4$
$(14,2^8,8)_4$	$(1000101)g_4$, $(1)g_2$	

TABLE XIII
NESTED PAIRS OF LINEAR CYCLIC CODES OVER $\mathbb{F}_4$ YIELDING OPTIMAL OR GOOD ASYMMETRIC CSS CODES IN TABLE XI

C and D	Generator Polynomials	AQC Q	C and D	Generator Polynomials	AQC Q
$[11,6,5]_4$	$g=(1w^2 11w1)$	$[[11,1,5/5]]_4$	$[15,12,3]_4$	$g=(w^2 011)$	$[[15,1,10/3]]_4$
$[11,5,6]_4$	$(11)g$		$[15,11,4]_4$	$(w1)g$	
$[15,12,3]_4$	$g=(w^2 011)$	$[[15,9,3/3]]_4$	$[15,9,5]_4$	$g=(1w11w^2 w^2 1)$	$[[15,5,5/4]]_4$
$[15,3,11]_4$	$(w^2 0w00w^2 10w1)g$		$[15,4,10]_4$	$(w^2 w0w^2 01)g$	
$[15,12,3]_4$	$g=(w^2 011)$	$[[15,8,4/3]]_4$	$[15,8,6]_4$	$g=(ww^2 w0w0w^2 1)$	$[[15,4,6/4]]_4$
$[15,4,10]_4$	$(w^2 w^2 111ww^2 w^2 1)g$		$[15,4,10]_4$	$(w1001)g$	
$[15,12,3]_4$	$g=(w^2 011)$	$[[15,6,5/3]]_4$	$[17,13,4]_4$	$g=(11w11)$	$[[17,9,4/4]]_4$
$[15,6,8]_4$	$(www0w^2 01)g$		$[17,4,12]_4$	$(1001111001)g$	
$[15,8,6]_4$	$g=(ww^2 w0w0w^2 1)$	$[[15,5,6/3]]_4$	$[17,9,7]_4$	$g=(1w^2 0w^2 w^2 w^2 0w^2 1)$	$[[17,5,7/4]]_4$
$[15,3,11]_4$	$(ww^2 0w01)g$		$[17,4,12]_4$	$(1wwww1)g$	
$[15,12,3]_4$	$g=(w^2 011)$	$[[15,4,7/3]]_4$	$[17,8,8]_4$	$g=(1ww^2 w^2 00w^2 w^2 w1)$	$[[17,4,8/4]]_4$
$[15,8,6]_4$	$(1w^2 w^2 w^2 1)g$		$[17,4,12]_4$	$(1w^2 1w^2 1)g$	

TABLE XIV
GOOD PURE ASYMMETRIC CSS-LIKE CODES OVER $\mathbb{F}_8$

No.	AQC Q	Type	LP	Def	Remarks	No.	AQC Q	Type	LP	Def	Remarks
1	$[[10, 19/3, 3/2]]_8$	ACC	$20/3$	$1/3$	BeOpLin	44	$[[15, 7, 7/2]]_8$	BC	$23/3$	$2/3$	OpLin
2	$[[10, 6, 4/2]]_8$	BC	6	0	Optimal	45	$[[15, 6, 8/2]]_8$	BC	$20/3$	$2/3$	OpLin
3	$[[10, 4, 5/2]]_8$	BC	$14/3$	$2/3$	OpLin	46	$[[15, 4, 10/2]]_8$	BC	$13/3$	$1/3$	OpLin
4	$[[10, 3, 6/2]]_8$	BC	$11/3$	$2/3$	OpLin	47	$[[15, 3, 11/2]]_8$	BC	$10/3$	$1/3$	OpLin
5	$[[10, 2, 8/2]]_8$	BC	2	0	Optimal	48	$[[15, 2, 12/2]]_8$	BC	$7/3$	$1/3$	OpLin
6	$[[11, 7, 3/2]]_8$	BC	$23/3$	$2/3$	OpLin	49	$[[16, 12, 3/2]]_8$	BC	$38/3$	$2/3$	OpLin
7	$[[11, 6, 4/2]]_8$	BC	$20/3$	$2/3$	OpLin	50	$[[16, 11, 4/2]]_8$	BC	$35/3$	$2/3$	OpLin
8	$[[11, 5, 5/2]]_8$	BC	$17/3$	$2/3$	OpLin	51	$[[16, 10, 5/2]]_8$	BC	$32/3$	$2/3$	OpLin
9	$[[11, 4, 6/2]]_8$	BC	$14/3$	$2/3$	OpLin	52	$[[16, 9, 6/2]]_8$	BC	$29/3$	$2/3$	OpLin
10	$[[11, 3, 7/2]]_8$	BC	$11/3$	$2/3$	OpLin	53	$[[16, 7, 8/2]]_8$	BC	$23/3$	$2/3$	OpLin
11	$[[11, 2, 8/2]]_8$	BC	$8/3$	$2/3$	OpLin	54	$[[16, 3, 12/2]]_8$	BC	$10/3$	$1/3$	OpLin
12	$[[11, 1, 9/2]]_8$	BC	$5/3$	$2/3$	OpLin	55	$[[17, 40/3, 3/2]]_8$	ACC	$41/3$	$1/3$	BeOpLin
13	$[[12, 8, 3/2]]_8$	BC	$26/3$	$2/3$	OpLin	56	$[[17, 12, 4/2]]_8$	BC	$38/3$	$2/3$	OpLin
14	$[[12, 7, 4/2]]_8$	BC	$23/3$	$2/3$	OpLin	57	$[[17, 11, 5/2]]_8$	BC	$35/3$	$2/3$	OpLin
15	$[[12, 6, 5/2]]_8$	BC	$20/3$	$2/3$	OpLin	58	$[[17, 10, 6/2]]_8$	BC	$32/3$	$2/3$	OpLin
16	$[[12, 5, 6/2]]_8$	BC	$17/3$	$2/3$	OpLin	59	$[[18, 14, 3/2]]_8$	BC	$43/3$	$1/3$	OpLin
17	$[[12, 4, 7/2]]_8$	BC	$14/3$	$2/3$	OpLin	60	$[[18, 13, 4/2]]_8$	BC	$41/3$	$2/3$	OpLin
18	$[[12, 3, 8/2]]_8$	BC	$11/3$	$2/3$	OpLin	61	$[[18, 12, 5/2]]_8$	BC	$38/3$	$2/3$	OpLin
19	$[[12, 2, 9/2]]_8$	BC	$8/3$	$2/3$	OpLin	62	$[[18, 11, 6/2]]_8$	BC	$35/3$	$2/3$	OpLin
20	$[[12, 1, 10/2]]_8$	BC	$4/3$	$1/3$	OpLin	63	$[[19, 15, 3/2]]_8$	BC	$46/3$	$1/3$	OpLin
21	$[[13, 9, 3/2]]_8$	BC	$29/3$	$2/3$	OpLin	64	$[[19, 14, 4/2]]_8$	BC	$43/3$	$1/3$	OpLin
22	$[[13, 8, 4/2]]_8$	CC	$26/3$	$2/3$	OpLin	65	$[[19, 13, 5/2]]_8$	BC	$40/3$	$1/3$	OpLin
23	$[[13, 7, 5/2]]_8$	BC	$23/3$	$2/3$	OpLin	66	$[[19, 12, 6/2]]_8$	CC	$38/3$	$2/3$	OpLin
24	$[[13, 6, 6/2]]_8$	BC	$20/3$	$2/3$	OpLin	67	$[[20, 16, 3/2]]_8$	BC	$49/3$	$1/3$	OpLin
25	$[[13, 5, 7/2]]_8$	BC	$17/3$	$2/3$	OpLin	68	$[[20, 15, 4/2]]_8$	BC	$46/3$	$1/3$	OpLin
26	$[[13, 4, 8/2]]_8$	BC	$14/3$	$2/3$	OpLin	69	$[[20, 14, 5/2]]_8$	BC	$43/3$	$1/3$	OpLin
27	$[[13, 3, 9/2]]_8$	BC	$11/3$	$2/3$	OpLin	70	$[[21, 17, 3/2]]_8$	CC	$52/3$	$1/3$	OpLin
28	$[[13, 2, 10/2]]_8$	BC	$7/3$	$1/3$	OpLin	71	$[[21, 16, 4/2]]_8$	CC	$49/3$	$1/3$	OpLin
29	$[[13, 1, 11/2]]_8$	BC	$4/3$	$1/3$	OpLin	72	$[[21, 15, 3/3]]_8$	CC	$47/3$	$2/3$	OpLin
30	$[[14, 10, 3/2]]_8$	CC	$32/3$	$2/3$	OpLin	73	$[[21, 14, 4/3]]_8$	CC	$44/3$	$2/3$	OpLin
31	$[[14, 9, 4/2]]_8$	CC	$29/3$	$2/3$	OpLin	74	$[[21, 13, 4/4]]_8$	CC	$41/3$	$2/3$	OpLin
32	$[[14, 8, 5/2]]_8$	BC	$26/3$	$2/3$	OpLin	75	$[[22, 18, 3/2]]_8$	BC	$55/3$	$1/3$	OpLin
33	$[[14, 7, 6/2]]_8$	BC	$23/3$	$2/3$	OpLin	76	$[[22, 17, 4/2]]_8$	BC	$52/3$	$1/3$	OpLin
34	$[[14, 6, 7/2]]_8$	BC	$20/3$	$2/3$	OpLin	77	$[[23, 19, 3/2]]_8$	BC	$58/3$	$1/3$	OpLin
35	$[[14, 5, 8/2]]_8$	BC	$17/3$	$2/3$	OpLin	78	$[[23, 18, 4/2]]_8$	BC	$55/3$	$1/3$	OpLin
36	$[[14, 4, 9/2]]_8$	BC	$14/3$	$2/3$	OpLin	79	$[[24, 20, 3/2]]_8$	BC	$61/3$	$1/3$	OpLin
37	$[[14, 3, 10/2]]_8$	BC	$10/3$	$1/3$	OpLin	80	$[[24, 19, 4/2]]_8$	BC	$58/3$	$1/3$	OpLin
38	$[[14, 2, 11/2]]_8$	BC	$7/3$	$1/3$	OpLin	81	$[[25, 21, 3/2]]_8$	BC	$64/3$	$1/3$	OpLin
39	$[[14, 1, 12/2]]_8$	CC	$4/3$	$1/3$	OpLin	82	$[[25, 20, 4/2]]_8$	BC	$61/3$	$1/3$	OpLin
40	$[[15, 34/3, 3/2]]_8$	ACC	$35/3$	$1/3$	BeOpLin	83	$[[26, 22, 3/2]]_8$	BC	$67/3$	$1/3$	OpLin
41	$[[15, 31/3, 4/2]]_8$	ACC	$32/3$	$1/3$	BeOpLin	84	$[[26, 21, 4/2]]_8$	BC	$64/3$	$1/3$	OpLin
42	$[[15, 9, 5/2]]_8$	BC	$29/3$	$2/3$	OpLin	85	$[[27, 23, 3/2]]_8$	BC	$70/3$	$1/3$	OpLin
43	$[[15, 8, 6/2]]_8$	BC	$26/3$	$2/3$	OpLin	86	$[[27, 22, 4/2]]_8$	BC	$67/3$	$1/3$	OpLin

TABLE XV
NESTED PAIRS OF $\mathbb{F}_2$-LINEAR CYCLIC CODES OVER $\mathbb{F}_8 = \mathbb{F}_2(w)$ YIELDING OPTIMAL OR GOOD ASYMMETRIC CSS-LIKE CODES IN TABLE XIV

C and D	Generator Polynomials	AQC Q
$(10, 2^{22}, 3)_8$	$g_1 = (000011) + w(0) + w^2(1)$, $g_2 = (1101001) + w(1)$, $g_3 = (101010101)$	$[[10, 19/3, 3/2]]_8$
$(10, 2^3, 10)_8$	$(1111111111)g_1$, $(1111111111)g_2$, $(11)g_3$	
$(15, 2^{37}, 3)_8$	$g_1 = (1001) + w(0) + w^2(111)$, $g_2 = (010011) + w(1)$, $g_3 = (1001111)$	$[[15, 34/3, 3/2]]_8$
$(15, 2^3, 15)_8$	$(1001001001001)g_1$, $(11011011011011)g_2$, $(1001110011)g_3$	
$(15, 2^{34}, 4)_8$	$g_1 = (111011111) + w(0) + w^2(111)$, $g_2 = (0000111) + w(1)$, $g_3 = (1001110011)$	$[[15, 31/3, 4/2]]_8$
$(15, 2^3, 15)_8$	$(1001001001001)(111)g_1$, $(11011011011011)g_2 + (1001001001001)(011)g_1$, $(1001111)g_3$	
$(17, 2^{43}, 3)_8$	$g_1 = (00100101) + w(0) + w^2(1)$, $g_2 = (01000101) + w(1)$, $g_3 = (111010111)$	$[[17, 40/3, 3/2]]_8$
$(17, 2^3, 17)_8$	$(11111111111111111)g_1$, $(11111111111111111)g_2$, $(100111001)g_3$	

TABLE XVI
NESTED PAIRS OF LINEAR CYCLIC CODES OVER $\mathbb{F}_8$ YIELDING OPTIMAL OR GOOD ASYMMETRIC CSS CODES IN TABLE XIV

C and D	Generator Polynomials	AQC Q	C and D	Generator Polynomials	AQC Q
$[13, 9, 4]_8$	$g = (1w^3w^5w^31)$	$[[13, 8, 4/2]]_8$	$[21, 20, 2]_8$	$g = (11)$	$[[21, 17, 3/2]]_8$
$[13, 1, 13]_8$	$(1w0w^5w^2w^50w1)g$		$[21, 3, 14]_8$	$(w^5w^6w^4w^21w^31w^6w^3w^20w^4w^5w00w1)g$	
$[14, 11, 3]_8$	$g = (w^2w^3w^61)$	$[[14, 10, 3/2]]_8$	$[21, 20, 2]_8$	$g = (11)$	$[[21, 16, 4/2]]_8$
$[14, 1, 14]_8$	$(w^5ww^5w^41w^2w^4w0w^21)g$		$[21, 4, 14]_8$	$(w^50w^3ww^5w^3w^3w^4w^5w^2w^4w^4ww^6ww^31)g$	
$[14, 10, 4]_8$	$g = (ww^41w^21)$	$[[14, 9, 4/2]]_8$	$[21, 18, 3]_8$	$g = (110w^31)$	$[[21, 15, 3/3]]_8$
$[14, 1, 14]_8$	$(ww^6ww^2w1w^6w^6w^31)g$		$[21, 3, 14]_8$	$(w^5w^6w^2w^6w01w^5ww^4w^3w^4w^2w^301)g$	
$[14, 2, 12]_8$	$g = (w^6w^51w^3110w^6w^51w^311)$	$[[14, 1, 12/2]]_8$	$[21, 17, 4]_8$	$g = (1ww^3w1)$	$[[21, 14, 4/3]]_8$
$[14, 1, 14]_8$	$(w^61)g$		$[21, 3, 14]_8$	$(11w^6w^6w^61w^3w^61ww^4ww^5w^31)g$	
$[19, 13, 6]_8$	$g = (1w^3w^6w^6w^6w^31)$	$[[19, 12, 6/2]]_8$	$[21, 17, 4]_8$	$g = (1ww^3w1)$	$[[21, 13, 4/4]]_8$
$[19, 1, 19]_8$	$(1www^31w^6ww^61w^3ww1)g$		$[21, 4, 14]_8$	$(w^6w^4ww^6w^3w^2w^6w^5w^6w^5w^6w^611)g$	

TABLE XVII
GOOD PURE ASYMMETRIC CSS-LIKE CODES OVER $\mathbb{F}_9$

No.	AQC Q	Type	LP	Def	Remarks	No.	AQC Q	Type	LP	Def	Remarks
1	$[[10,7,3/2]]_9$	BC	7	0	Optimal	50	$[[15,9,5/2]]_9$	BC	9.5	0.5	OpLin
2	$[[10,6,4/2]]_9$	CC	6	0	Optimal	51	$[[15,8,6/2]]_9$	BC	8.5	0.5	OpLin
3	$[[10,5,5/2]]_9$	BC	5	0	Optimal	52	$[[15,7,7/2]]_9$	BC	7.5	0.5	OpLin
4	$[[10,4,6/2]]_9$	CC	4	0	Optimal	53	$[[15,6,8/2]]_9$	BC	6.5	0.5	OpLin
5	$[[10,3,7/2]]_9$	BC	3	0	Optimal	54	$[[15,5,9/2]]_9$	BC	5.5	0.5	OpLin
6	$[[10,2,8/2]]_9$	CC	2	0	Optimal	55	$[[15,4,10/2]]_9$	BC	4.5	0.5	OpLin
7	$[[10,2,6/4]]_9$	CC	2	0	Optimal	56	$[[15,3,11/2]]_9$	BC	3.5	0.5	OpLin
8	$[[11,7.5,3/2]]_9$	ACC	7.5	0	Optimal,BeOpLin	57	$[[15,2,12/2]]_9$	BC	2.5	0.5	OpLin
9	$[[11,6,4/2]]_9$	BC	6.5	0.5	OpLin	58	$[[15,1,13/2]]_9$	BC	1.5	0.5	OpLin
10	$[[11,5,5/2]]_9$	CC	5.5	0.5	OpLin	59	$[[16,12,3/2]]_9$	CC	12.5	0.5	OpLin
11	$[[11,4,6/2]]_9$	BC	4.5	0.5	OpLin	60	$[[16,11,4/2]]_9$	CC	11.5	0.5	OpLin
12	$[[11,3,7/2]]_9$	BC	3.5	0.5	OpLin	61	$[[16,10,5/2]]_9$	ACC	10.5	0.5	ROpLin
13	$[[11,2,8/2]]_9$	BC	2.5	0.5	OpLin	62	$[[16,9,6/2]]_9$	BC	9.5	0.5	OpLin
14	$[[11,1,9/2]]_9$	BC	1.5	0.5	OpLin	63	$[[16,8,7/2]]_9$	BC	8.5	0.5	OpLin
15	$[[11,6,3/3]]_9$	ACC	6	0	Optimal	64	$[[16,7,8/2]]_9$	BC	7.5	0.5	OpLin
16	$[[11,3,6/3]]_9$	ACC	3.5	0.5	ROpLin	65	$[[16,6,9/2]]_9$	BC	6.5	0.5	OpLin
17	$[[12,8.5,3/2]]_9$	ACC	8.5	0	Optimal,BeOpLin	66	$[[16,5,10/2]]_9$	BC	5.5	0.5	OpLin
18	$[[12,7,4/2]]_9$	ACC	7.5	0.5	ROpLin	67	$[[16,4,11/2]]_9$	BC	4.5	0.5	OpLin
19	$[[12,6,5/2]]_9$	ACC	6.5	0.5	ROpLin	68	$[[16,3,12/2]]_9$	BC	3.5	0.5	OpLin
20	$[[12,5,6/2]]_9$	ACC	5.5	0.5	ROpLin	69	$[[16,1,14/2]]_9$	CC	1.5	0.5	OpLin
21	$[[12,4,7/2]]_9$	ACC	4.5	0.5	ROpLin	70	$[[17,13,3/2]]_9$	BC	13.5	0.5	OpLin
22	$[[12,2,9/2]]_9$	BC	2.5	0.5	OpLin	71	$[[17,12,4/2]]_9$	BC	12.5	0.5	OpLin
23	$[[12,1,10/2]]_9$	BC	1.5	0.5	OpLin	72	$[[17,11,5/2]]_9$	BC	11.5	0.5	OpLin
24	$[[12,7,3/3]]_9$	ACC	7	0	Optimal	73	$[[17,9,7/2]]_9$	BC	9.5	0.5	OpLin
25	$[[13,9,3/2]]_9$	CC	9.5	0.5	OpLin	74	$[[17,8,8/2]]_9$	BC	8.5	0.5	OpLin
26	$[[13,8,4/2]]_9$	ACC	8.5	0.5	ROpLin	75	$[[17,7,9/2]]_9$	BC	7.5	0.5	OpLin
27	$[[13,7.5,5/2]]_9$	ACC	7.5	0	Optimal,BeOpLin	76	$[[17,6,10/2]]_9$	BC	6.5	0.5	OpLin
28	$[[13,6,6/2]]_9$	ACC	6.5	0.5	ROpLin	77	$[[17,2,14/2]]_9$	BC	2.5	0.5	OpLin
29	$[[13,5,7/2]]_9$	BC	5.5	0.5	OpLin	78	$[[18,14,3/2]]_9$	BC	14.5	0.5	OpLin
30	$[[13,4,8/2]]_9$	BC	4.5	0.5	OpLin	79	$[[18,13,4/2]]_9$	BC	13.5	0.5	OpLin
31	$[[13,3,9/2]]_9$	BC	3.5	0.5	OpLin	80	$[[18,12,5/2]]_9$	BC	12.5	0.5	OpLin
32	$[[13,2,10/2]]_9$	BC	2.5	0.5	OpLin	81	$[[18,9,8/2]]_9$	BC	9.5	0.5	OpLin
33	$[[13,1,11/2]]_9$	BC	1.5	0.5	OpLin	82	$[[18,8,9/2]]_9$	BC	8.5	0.5	OpLin
34	$[[13,6,5/3]]_9$	ACC	6	0	Optimal	83	$[[18,7,10/2]]_9$	BC	7.5	0.5	OpLin
35	$[[13,6,4/4]]_9$	ACC	6	0	Optimal	84	$[[18,2,14/2]]_9$	BC	2.5	0.5	OpLin
36	$[[13,5,5/4]]_9$	ACC	5	0	Optimal	85	$[[19,15,3/2]]_9$	BC	15.5	0.5	OpLin
37	$[[13,4,5/5]]_9$	ACC	4	0	Optimal	86	$[[19,14,4/2]]_9$	BC	14.5	0.5	OpLin
38	$[[14,10,3/2]]_9$	BC	10.5	0.5	OpLin	87	$[[19,13,5/2]]_9$	BC	13.5	0.5	OpLin
39	$[[14,9,4/2]]_9$	CC	9.5	0.5	OpLin	88	$[[19,9,9/2]]_9$	BC	9.5	0.5	OpLin
40	$[[14,8,5/2]]_9$	BC	8.5	0.5	OpLin	89	$[[19,8,10/2]]_9$	BC	8.5	0.5	OpLin
41	$[[14,7,6/2]]_9$	ACC	7.5	0.5	ROpLin	90	$[[20,16,3/2]]_9$	CC	16.5	0.5	OpLin
42	$[[14,6,7/2]]_9$	ACC	6.5	0.5	ROpLin	91	$[[20,15,4/2]]_9$	CC	15.5	0.5	OpLin
43	$[[14,5,8/2]]_9$	BC	5.5	0.5	OpLin	92	$[[20,14,5/2]]_9$	BC	14.5	0.5	OpLin
44	$[[14,4,9/2]]_9$	BC	4.5	0.5	OpLin	93	$[[20,9,10/2]]_9$	BC	9.5	0.5	OpLin
45	$[[14,3,10/2]]_9$	BC	3.5	0.5	OpLin	94	$[[21,17,3/2]]_9$	BC	17.5	0.5	OpLin
46	$[[14,2,11/2]]_9$	BC	2.5	0.5	OpLin	95	$[[21,16,4/2]]_9$	BC	16.5	0.5	OpLin
47	$[[14,1,12/2]]_9$	BC	1.5	0.5	OpLin	96	$[[22,18,3/2]]_9$	BC	18.5	0.5	OpLin
48	$[[15,11,3/2]]_9$	BC	11.5	0.5	OpLin	97	$[[22,17,4/2]]_9$	BC	17.5	0.5	OpLin
49	$[[15,10,4/2]]_9$	BC	10.5	0.5	OpLin						

This establishes (VII.1).

Hence, by using the definition of $A(Y)$, $B(Y)$ can now be written as

$$B(Y) = \frac{1}{|C|}\sum_{i=0}^{n} A_i (1+(q-1)Y)^{n-i}(1-Y)^i.$$

Comparing the coefficients of Y^j on both sides gives us the claimed MacWilliams equation for the single variable Y. Replacing Y by $\frac{Y}{X}$ and multiplying both sides by X^n give the desired expression for the two-variable case.

Note that $|C^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}}|$ can be derived by substituting $Y = 1$ in (VII.1) from whence we have $|C||C^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}}| = q^n$. This is sufficient to establish the closure property of C under the trace Euclidean inner product. ∎

Remark A.2: The closure property and the MacWilliams equation for an $\mathbb{F}_r$-linear code C over $\mathbb{F}_q$ under the trace Euclidean inner product can also be deduced from [26, Cor. 3.2.3 on p. 88]. The explicit approach above is preferred so as to eliminate the need for a more sophisticated algebraic build-up in the exposition.

APPENDIX B: PROOF OF THEOREM 3.6

We begin with some preparatory lemmas. Recall that for $C \subseteq \mathbb{F}_q^n$, $\overline{C} := \{\overline{\mathbf{c}} : \mathbf{c} \in C\}$.

Lemma B.1: Suppose that $q = r^2$ is odd. Let C_1 and C_2 be $\mathbb{F}_r$-linear codes of length n over $\mathbb{F}_q$. For $\alpha \in \mathbb{F}_q \setminus \{0\}$ such that $\overline{\alpha} = -\alpha$, the following statements hold:

i) If $C_1^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}} \subseteq C_2$, then

$$\alpha^{-1}\overline{C_1^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}}} \subseteq \left(C_2^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}}\right)^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}}.$$

TABLE XVIII
NESTED PAIRS OF $\mathbb{F}_3$-LINEAR CYCLIC CODES OVER $\mathbb{F}_9 = \mathbb{F}_3(w)$ YIELDING OPTIMAL OR GOOD ASYMMETRIC CSS-LIKE CODES IN TABLE XVII

C **and** D	**Generator Polynomials**	**AQC** Q
$(11, 3^{17}, 3)_9$	$g_9 = (011) + w(1)$, $g_3 = (201211)$	$[[11, 7.5, 3/2]]_9$
$(11, 3^2, 11)_9$	$(11111111111)g_9$, $(221201)g_3$	
$(11, 3^{17}, 3)_9$	$g_9 = (011) + w(1)$, $g_3 = (201211)$	$[[11, 6, 3/3]]_9$
$(11, 3^5, 8)_9$	$(1012221)g_9$, $(1012221)g_3$	
$(11, 3^{11}, 6)_9$	$g_9 = (1010211) + w(21)$, $g_3 = (11111111111)$	$[[11, 3, 6/3]]_9$
$(11, 3^5, 8)_9$	$(201211)g_9$, $(21)g_3$	
$(12, 3^{19}, 3)_9$	$g_9 = (001) + w(11)$, $g_3 = (12221)$	$[[12, 8.5, 3/2]]_9$
$(12, 3^2, 12)_9$	$(10101010101)g_9$, $(20112201)g_3$	
$(12, 3^{16}, 4)_9$	$g_9 = (1112121) + w(11)$,$g_3 = (21000021)$	$[[12, 7, 4/2]]_9$
$(12, 3^2, 12)_9$	$(10101010101)g_9$, $(10101)g_3$	
$(12, 3^{14}, 5)_9$	$g_9 = (02021012) + w(11)$, $g_3 = (1221001221)$	$[[12, 6, 5/2]]_9$
$(12, 3^2, 12)_9$	$(10101010101)g_9$, $(201)g_3$	
$(12, 3^{12}, 6)_9$	$g_9 = (2021201) + w(2211)$, $g_3 = (1221001221)$	$[[12, 5, 6/2]]_9$
$(12, 3^2, 12)_9$	$(111000111)g_9$, $(121)g_3$	
$(12, 3^{10}, 7)_9$	$g_9 = (0110212102) + w(2211)$, $g_3 = (111111111111)$	$[[12, 4, 7/2]]_9$
$(12, 3^2, 12)_9$	$(111000111)g_9$, $(1)g_3$	
$(12, 3^{19}, 3)_9$	$g_9 = (001) + w(11)$, $g_3 = (12221)$	$[[12, 7, 3/3]]_9$
$(12, 3^5, 8)_9$	$(20112201)g_9$, $(20112201)g_3$	
$(13, 3^{19}, 4)_9$	$g_9 = (2221011) + w(1)$,$g_3 = (21210201)$	$[[13, 8, 4/2]]_9$
$(13, 3^3, 12)_9$	$(12020111211)g_9$, $(1100101)g_3$	
$(13, 3^{17}, 5)_9$	$g_9 = (122001222) + w(1)$, $g_3 = (2001102121)$	$[[13, 7.5, 5/2]]_9$
$(13, 3^2, 13)_9$	$(1111111111111)g_9$, $(2221)g_3$	
$(13, 3^{14}, 6)_9$	$g_9 = (110200000122) + w(1)$, $g_3 = (1111111111111)$	$[[13, 6, 6/2]]_9$
$(13, 3^2, 13)_9$	$(1111111111111)g_9$, $(1)g_3$	
$(13, 3^{17}, 5)_9$	$g_9 = (122001222) + w(1)$, $g_3 = (2001102121)$	$[[13, 6, 5/3]]_9$
$(13, 3^5, 10)_9$	$(2001102121)g_9$, $(2221)g_3$	
$(13, 3^{19}, 4)_9$	$g_9 = (2221011) + w(1)$,$g_3 = (21210201)$	$[[13, 6, 4/4]]_9$
$(13, 3^7, 9)_9$	$(1100101)g_9$, $(1100101)g_3$	
$(13, 3^{17}, 5)_9$	$g_9 = (011100002) + w(1)$, $g_3 = (2022010211)$	$[[13, 5, 5/4]]_9$
$(13, 3^7, 9)_9$	$(22001211)g_9$, $(2201)g_3$	
$(13, 3^{17}, 5)_9$	$g_9 = (122001222) + w(1)$, $g_3 = (2001102121)$	$[[13, 4, 5/5]]_9$
$(13, 3^9, 8)_9$	$(10011)g_9$, $(10011)g_3$	
$(14, 3^{16}, 6)_9$	$g_9 = (1121101101) + w(1)$, $g_3 = (1010101010101)$	$[[14, 7, 6/2]]_9$
$(14, 3^2, 14)_9$	$(1010101010101)g_9$, $(201)g_3$	
$(14, 3^{14}, 7)_9$	$g_9 = (122202010101) + w(21)$, $g_3 = (11111111111111)$	$[[14, 6, 7/2]]_9$
$(14, 3^2, 14)_9$	$(1010101010101)g_9$, $(1)g_3$	
$(16, 3^{22}, 5)_9$	$g_9 = (02102001) + w(201)$, $g_3 = (220210221)$	$[[16, 10, 5/2]]_9$
$(16, 3^2, 16)_9$	$(1000100010001)g_9$, $(121110211)g_3$	

ii) If $C_1^{\perp_{\mathrm{Tr}\ q/r}\mathrm{H}} \subseteq C_2$, then

$$\alpha\overline{C_1^{\perp_{\mathrm{Tr}\ q/r}\mathrm{H}}} \subseteq \left(C_2^{\perp_{\mathrm{Tr}\ q/r}\mathrm{H}}\right)^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}}.$$

Proof: Let $\mathbf{u} \in C_1^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}}$ and $\mathbf{v} \in C_2^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}}$. Then,

$$0 = \langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{Tr}_{q/r}\mathrm{E}} = \langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{E}} + \overline{\langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{E}}}.$$

Therefore,

$$\begin{aligned} \langle \alpha^{-1}\overline{\mathbf{u}}, \mathbf{v} \rangle_{\mathrm{Tr}\ q/r\mathrm{H}} &= \alpha \langle \alpha^{-1}\overline{\mathbf{u}}, \mathbf{v} \rangle_{\mathrm{H}} + \overline{\alpha \langle \alpha^{-1}\overline{\mathbf{u}}, \mathbf{v} \rangle_{\mathrm{H}}} \\ &= \overline{\langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{E}}} + \langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{E}} = 0. \end{aligned}$$

Hence, $\alpha^{-1}\overline{C_1^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}}} \subseteq \left(C_2^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}}\right)^{\perp_{\mathrm{Tr}\ q/r}\mathrm{H}}$. This proves *i)*.

To prove *ii)*, let $\mathbf{u} \in C_1^{\perp_{\mathrm{Tr}\ q/r}\mathrm{H}}$ and $\mathbf{v} \in C_2^{\perp_{\mathrm{Tr}\ q/r}\mathrm{H}}$. Then

$$0 = \langle \mathbf{u}, \mathbf{v} \rangle_{\mathrm{Tr}\ q/r\mathrm{H}} = \alpha \langle \mathbf{u}, \overline{\mathbf{v}} \rangle_{\mathrm{E}} + \overline{\alpha} \langle \overline{\mathbf{u}}, \mathbf{v} \rangle_{\mathrm{E}}.$$

Since $\overline{\alpha} = -\alpha$,

$$\begin{aligned} \langle \alpha\overline{\mathbf{u}}, \mathbf{v} \rangle_{\mathrm{Tr}_{q/r}\mathrm{E}} &= \langle \alpha\overline{\mathbf{u}}, \mathbf{v} \rangle_{\mathrm{E}} + \langle \overline{\alpha}\mathbf{u}, \overline{\mathbf{v}} \rangle_{\mathrm{E}} \\ &= \alpha \langle \overline{\mathbf{u}}, \mathbf{v} \rangle_{\mathrm{E}} + \overline{\alpha} \langle \mathbf{u}, \overline{\mathbf{v}} \rangle_{\mathrm{E}} \\ &= -\left(\overline{\alpha} \langle \overline{\mathbf{u}}, \mathbf{v} \rangle_{\mathrm{E}} + \alpha \langle \mathbf{u}, \overline{\mathbf{v}} \rangle_{\mathrm{E}}\right) = 0. \end{aligned}$$

Therefore, $\alpha\overline{C_1^{\perp_{\mathrm{Tr}\ q/r}\mathrm{H}}} \subseteq \left(C_2^{\perp_{\mathrm{Tr}\ q/r}\mathrm{H}}\right)^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}}$. ■

Lemma B.2: Suppose that $q = r^2$ is even. Let C_1 and C_2 be $\mathbb{F}_r$-linear codes of length n over $\mathbb{F}_q$. Then the following statements hold:

i) If $C_1^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}} \subseteq C_2$, then

$$\overline{C_1^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}}} \subseteq \left(C_2^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}}\right)^{\perp_{\mathrm{Tr}\ q/r}\mathrm{H}}.$$

ii) If $C_1^{\perp_{\mathrm{Tr}\ q/r}\mathrm{H}} \subseteq C_2$, then

$$\overline{C_1^{\perp_{\mathrm{Tr}\ q/r}\mathrm{H}}} \subseteq \left(C_2^{\perp_{\mathrm{Tr}\ q/r}\mathrm{H}}\right)^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}}.$$

Proof: The proof follows from the proof of Lemma B.1 by setting $\alpha = 1$. ■

Proof of Theorem 3.6: Assume there exists a pair of $\mathbb{F}_r$-linear codes C_1 and C_2 of length n over $\mathbb{F}_q$ such that $C_1^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}} \subseteq C_2$ with $\frac{|C_2|}{\left|C_1^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}}\right|} = K$, $d_x = \mathrm{wt}_{\mathrm{H}}(C_1 \setminus C_2^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}})$ and $d_z = \mathrm{wt}_{\mathrm{H}}(C_2 \setminus C_1^{\perp_{\mathrm{Tr}_{q/r}}\mathrm{E}})$.

Case 1. If q is odd, then by Lemma B.1 *i)*, we have

TABLE XIX
NESTED PAIRS OF LINEAR CYCLIC CODES OVER $\mathbb{F}_9$ YIELDING OPTIMAL OR GOOD ASYMMETRIC CSS CODES IN TABLE XVII

C and D	Generator Polynomials	AQC Q	C and D	Generator Polynomials	AQC Q
$[10,7,4]_9$	$g=(1w^2w^21)$	$[[10,6,4/2]]_9$	$[14,10,4]_9$	$g=(2w^2w^2w^21)$	$[[14,9,4/2]]_9$
$[10,1,10]_9$	$(1w^5w^2w^6w^2w^51)g$		$[14,1,14]_9$	$(1w011110w^31)g$	
$[10,9,2]_9$	$g=(21)$	$[[10,4,6/2]]_9$	$[16,13,3]_9$	$g=(1w^3w^51)$	$[[16,12,3/2]]_9$
$[10,5,6]_9$	$(1w^20w^21)g$		$[16,1,16]_9$	$(1ww^70w^6w^721w^3w^51w^21)g$	
$[10,9,2]_9$	$g=(21)$	$[[10,2,8/2]]_9$	$[16,12,4]_9$	$g=(w^6w^5021)$	$[[16,11,4/2]]_9$
$[10,7,4]_9$	$(1w^51)g$		$[16,1,16]_9$	$(w0w^7w^3w^31w^6w^3w^5w^6w^21)g$	
$[10,7,4]_9$	$g=(1w^2w^21)$	$[[10,2,6/4]]_9$	$[16,2,14]_9$	$g=(w^3w^3w21w10w^3w^3w21w1)$	$[[16,1,14/2]]_9$
$[10,5,6]_9$	$(1w^71)g$		$[16,1,16]_9$	$(w^21)g$	
$[11,6,5]_9$	$g=(201211)$	$[[11,5,5/2]]_9$	$[20,17,3]_9$	$g=(1w^2w^51)$	$[[20,16,3/2]]_9$
$[11,1,11]_9$	$(221201)g$		$[20,1,20]_9$	$(w^20w20w^7ww^2w^2w^20w^21w^7w^221)g$	
$[13,10,3]_9$	$g=(2111)$	$[[13,9,3/2]]_9$	$[20,16,4]_9$	$g=(w^62w^701)$	$[[20,15,4/2]]_9$
$[13,1,13]_9$	$(2121022001)g$		$[20,1,20]_9$	$(2w^2ww^21ww^3w^3w^7w^7w^52w^6w^5w^61)g$	

$\alpha^{-1}\overline{C_1^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}} \subseteq \left(C_2^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}\right)^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}}$ with

$$K = \frac{|C_2|}{\left|C_1^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}\right|} = \frac{\left|\left(C_2^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}\right)^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}}\right|}{\left|\alpha^{-1}\overline{C_1^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}}\right|}.$$

Since the codes $\alpha^{-1}\overline{C_1^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}}$ and $C_2^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}$ are equivalent and it follows from (II.3) that $C_2 = (C_2^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}})^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}$ and $(C_2^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}})^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}}$ share the same weight enumerator, we have

$$\mathrm{wt}_{\mathrm{H}}\left(\left(C_2^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}\right)^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}} \setminus \alpha^{-1}\overline{C_1^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}}\right)$$
$$= \mathrm{wt}_{\mathrm{H}}(C_2 \setminus C_1^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}) = d_z.$$

The code C_1 is equivalent to $(\alpha^{-1}\overline{C_1^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}})^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}$ which, by (II.3), shares the same weight enumerator with $(\alpha^{-1}\overline{C_1^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}})^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}}$. Hence

$$\mathrm{wt}_{\mathrm{H}}\left(\left(\alpha^{-1}\overline{C_1^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}}\right)^{\perp_{Tr_{q/r}H}} \setminus C_2^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}\right)$$
$$= \mathrm{wt}_{\mathrm{H}}(C_1 \setminus C_2^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}) = d_x.$$

The conclusion follows from [11, Th. 4.5].

Case 2. If q is even, then the proof is similar to that of Case 1 with $\alpha = 1$ and using Lemma B.2 $i)$ instead of Lemma B.1 $i)$.

Conversely, assume that there exists a pair of $\mathbb{F}_r$-linear codes C_1 and C_2 of length n over $\mathbb{F}_q$ such that $C_1^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}} \subseteq C_2$ with $\frac{|C_2|}{\left|C_1^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}}\right|} = K$, $d_x = \mathrm{wt}_{\mathrm{H}}(C_1 \setminus C_2^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}})$ and $d_z = \mathrm{wt}_{\mathrm{H}}(C_2 \setminus C_1^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}})$.

Case 1. If q is odd, then by Lemma B.1 $ii)$, we have $\alpha C_1^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}} \subseteq \left(C_2^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}}\right)^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}$ with

$$K = \frac{|C_2|}{\left|C_1^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}}\right|} = \frac{\left|\left(C_2^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}}\right)^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}}\right|}{\left|\alpha\overline{C_1^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}}}\right|}.$$

Using similar observation as in Case 1 of the necessary part, we have

$$\mathrm{wt}_{\mathrm{H}}\left(\left(C_2^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}}\right)^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}} \setminus \alpha\overline{C_1^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}}}\right) = d_z$$

and

$$\mathrm{wt}_{\mathrm{H}}\left(\left(\alpha\overline{C_1^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}}}\right)^{\perp_{\mathrm{Tr}_{q/r}\,\mathrm{E}}} \setminus C_2^{\perp_{\mathrm{Tr}\,q/r}\mathrm{H}}\right) = d_x.$$

The conclusion follows from Theorem 3.4.

Case 2. If q is even, then the proof is similar to that of Case 1 with $\alpha = 1$ and using Lemma B.2 $ii)$ instead of Lemma B.1 $ii)$.

■

APPENDIX C: PROOF OF THEOREM 4.2

We will need the following lemma in the proof.

Lemma C.1: Let $\mathbb{F}_q = \mathbb{F}_r(\omega)$ be a quadratic extension of $\mathbb{F}_r$. Then the following statements hold:

i) Any $(n, r^l)_q$-cyclic $\mathbb{F}_r$-linear code C over $\mathbb{F}_q$ has two generators and can be written as $C := \langle a(x) + \omega b(x), c(x)\rangle$, where $a(x), b(x)$, and $c(x)$ are polynomials in $\mathbb{F}_r[x]$, $b(x)$ and $c(x)$ are monic divisors of $x^n - 1$ in $\mathbb{F}_r[x]$, $c(x)$ divides $a(x)(x^n-1)/b(x)$ in $\mathbb{F}_r[x]$, and $l = 2n - \deg(b(x)) - \deg(c(x))$.

ii) If $\langle a'(x) + \omega b'(x), c'(x)\rangle$ is another representation of C in the above sense, then $b'(x) = b(x)$, $c'(x) = c(x)$ and $a'(x) \equiv a(x)(\mathrm{mod}\, c(x))$.

Proof: To prove $i)$, let C be an $(n, r^l)_q$-cyclic $\mathbb{F}_r$-linear code over $\mathbb{F}_q$. Define an $\mathbb{F}_r[x]$-module homomorphism

$$\varphi : C \to \mathbb{F}_r[x]/\langle x^n - 1\rangle \text{ sending}$$
$$v(x) := f_0(x) + \omega f_1(x) \mapsto f_1(x),$$

where $f_0(x)$ and $f_1(x)$ are polynomials in $\mathbb{F}_r[x]$.

The zero code is viewed as the one generated by $x^n - 1$. The kernel $\ker(\varphi) = \{v(x) \in C : f_1(x) \equiv 0\} = \{f_0(x) \in C\}$ and the image $\varphi(C) = \{f_1(x) : v(x) \in C\}$ are linear cyclic codes over $\mathbb{F}_r$. Hence, there exist unique, monic generators $c(x)$ and $b(x)$ of minimal degree, respectively, such that $\ker(\varphi) = \langle c(x)\rangle$ and $\varphi(C) = \langle b(x)\rangle$.

Note that for all $a(x) \in \mathbb{F}_r[x]$,

$$\dim_{\mathbb{F}_r}(C) = \dim_{\mathbb{F}_r}(\langle c(x)\rangle) + \dim_{\mathbb{F}_r}(\langle b(x)\rangle)$$

$$= \dim_{\mathbb{F}_r}(\langle c(x), \omega b(x)\rangle) \tag{VII.6}$$
$$\leq \dim_{\mathbb{F}_r}(\langle c(x), a(x) + \omega b(x)\rangle). \tag{VII.7}$$

The first equation is clear from the definition of φ. To justify (VII.6), let $0 \leq i \leq n - \deg(c(x)) - 1$ and $0 \leq j \leq n - \deg(b(x)) - 1$. The sets $\{x^i c(x)\}$ and $\{x^j b(x)\}$ serve, respectively, as bases for $\langle c(x)\rangle$ and $\langle b(x)\rangle$. Since the set $\{x^i c(x), x^j \omega b(x)\}$ is $\mathbb{F}_r$-linearly independent,

$$\begin{aligned}\dim_{\mathbb{F}_r}(\langle c(x), \omega b(x)\rangle) &\geq 2n - \deg(b(x)) - \deg(c(x)) \\ &= \dim_{\mathbb{F}_r}(\langle c(x)\rangle) + \dim_{\mathbb{F}_r}(\langle b(x)\rangle).\end{aligned}$$

The other direction is clear.

To establish (VII.7), notice that the set $\{x^i c(x), x^j(a(x) + \omega b(x))\} \subseteq \langle c(x), (a(x) + \omega b(x))\rangle$ is again $\mathbb{F}_r$-linearly independent.

If $a(x) + \omega b(x)$ is a preimage of $b(x)$ under φ, then $\langle c(x), (a(x) + \omega b(x))\rangle \subseteq C$. By (VII.7), we conclude that $\langle c(x), (a(x) + \omega b(x))\rangle = C$ and that C has the claimed $\mathbb{F}_r$-dimension.

Clearly, $c(x)$ and $b(x)$ divide $x^n - 1$ in $\mathbb{F}_r[x]$. Let $g(x) := (x^n - 1)/b(x)$. Since

$$a(x)g(x) \equiv (a(x) + \omega b(x))g(x) \in \ker(\varphi),$$

$c(x)$ divides $a(x)g(x)$ in $\mathbb{F}_r[x]$.

To prove $ii)$, assume $C := \langle a'(x) + \omega b'(x), c'(x)\rangle$. Then $b(x)|b'(x)$, $c(x)|c'(x)$ and

$$\begin{aligned}\deg(b'(x)c'(x)) &= \deg(b'(x)) + \deg(c'(x)) \\ &= 2n - l = \deg(b(x)) + \deg(c(x)) \\ &= \deg(b(x)c(x)).\end{aligned}$$

Hence, we have $b(x) = b'(x)$ and $c(x) = c'(x)$.

Since $a'(x) + \omega b(x) \in \langle a(x) + \omega b(x), c(x)\rangle$, there exist polynomials $s(x), t(x) \in \mathbb{F}_r[x]$ such that

$$a'(x) + \omega b(x) = s(x)(a(x) + \omega b(x)) + t(x)c(x).$$

Without loss of generality, $\deg(s(x)) < n - \deg(b(x))$ and $\deg(t(x)) < n - \deg(c(x))$ can be assumed. By comparing the coefficients on both sides of the equation, $s(x) = 1$. Therefore, $a'(x) = a(x) + t(x)c(x)$, making $a'(x) \equiv a(x) \pmod{c(x)}$. ∎

With the lemma established, the theorem can now be settled.

Proof of Theorem 4.2: We prove by induction on m. If $m = 2$, the statement follows from Lemma C.1. Assume that the theorem holds for $m - 1$. Let C be an $(n, r^l)_q$-cyclic $\mathbb{F}_r$-linear code over $\mathbb{F}_q$ and let $\mathbb{F}_s$ be the field extension of $\mathbb{F}_r$ of degree $m - 1$ such that $\mathbb{F}_s = \mathbb{F}_r(\alpha)$.

Let $\phi : C \to \mathbb{F}_s[x]/\langle x^n - 1\rangle$ be an $\mathbb{F}_r[x]$-module homomorphism defined by

$$\begin{aligned}&f_0(x) + \omega f_1(x) + \omega^2 f_2(x) + \cdots + \omega^{m-1} f_{m-1}(x) \\ &\mapsto f_1(x) + \alpha f_2(x) + \cdots + \alpha^{m-2} f_{m-1}(x).\end{aligned}$$

The kernel $\ker(\phi)$ and the image $\phi(C)$ are a linear cyclic code over $\mathbb{F}_r$ and a cyclic $\mathbb{F}_r$-linear code over $\mathbb{F}_s$, respectively.

Let $a_{m-1,0}(x)$ be the unique monic generator of $\ker(\phi)$ of minimal degree. By the induction hypothesis, $\phi(C)$ has $m-1$ generators, say

$$\begin{aligned}\phi(C) = \langle &a_{0,1}(x) + \alpha a_{0,2}(x) + \ldots + \alpha^{m-2} a_{0,m-1}(x), \\ &a_{1,1}(x) + \alpha a_{1,2}(x) + \ldots + \alpha^{m-3} a_{1,m-2}(x), \\ &\vdots \qquad\qquad \vdots \qquad\qquad \iddots \\ &a_{m-3,1}(x) + \alpha a_{m-3,2}(x), \\ &a_{m-2,1}(x)\rangle,\end{aligned}$$

satisfying properties $i)$ to $iv)$. Therefore, C is an $\mathbb{F}_r[x]$-module generated by

$$\begin{aligned}\langle &a_{0,0}(x) + \omega a_{0,1}(x) + \ldots + \omega^{m-1} a_{0,m-1}(x), \\ &a_{1,0}(x) + \omega a_{1,1}(x) + \ldots + \omega^{m-2} a_{1,m-2}(x), \\ &\vdots \qquad\qquad \vdots \qquad\qquad \iddots \\ &a_{m-2,0}(x) + \omega a_{m-2,1}(x), \\ &a_{m-1,0}(x)\rangle,\end{aligned}$$

where $a_{i,0}(x) + \omega a_{i,1}(x) + \ldots + \omega^{m-1-i} a_{i,m-1-i}(x)$ is an inverse image of $a_{i,1}(x) + \alpha a_{i,2}(x) + \ldots + \alpha^{m-2-i} a_{i,m-1-i}(x)$ for all $0 \leq i \leq m - 2$. Clearly, property $i)$ holds.

Using a similar reasoning to the proof of Lemma C.1, by the inductive hypothesis we obtain the fact that $a_{m-2,0}(x)(x^n - 1)/a_{m-2,1}(x)$ is divisible by $a_{m-1,0}(x)$. Hence, property $ii)$ follows.

Since

$$\dim_{\mathbb{F}_r}(\ker(\phi)) = n - \deg(a_{m-1,0}(x))$$

and

$$\dim_{\mathbb{F}_r}(\phi(C)) = (m-1)n - \sum_{i=0}^{m-2} \deg(a_{i,m-1-i}(x)),$$

we have

$$\begin{aligned}l &= \dim_{\mathbb{F}_r}(\ker(\phi)) + \dim_{\mathbb{F}_r}(\phi(C)) \\ &= mn - \sum_{i=0}^{m-1} \deg(a_{i,m-1-i}(x)).\end{aligned}$$

This proves property $iii)$.

The uniqueness stated in property $iv)$ can be obtained from an argument similar to the one used in the proof of $b)$ in Lemma C.1. ∎

Appendix D: Farkas Certificate of Infeasibility

Referring to (V.3), the tuple

$$(n, q, k, k', d_x, d_z) = (6, 2, 2, 1, 3, 2)$$

has a vector $\mathbf{r}$ with $\mathbf{r}^\intercal = (1, 0, 0, 0, 1, 0, 0, \ldots, 0)$ and the matrices M_1 and M_2 below.

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 4 & 2 & 0 & -2 & -4 & -6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 15 & 5 & -1 & -3 & -1 & 5 & 15 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 4 & 2 & 0 & -2 & -4 & -6 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & 32 & 0 & 0 & 0 & 0 & 0 & 0 \\ -6 & -4 & -2 & 0 & 2 & 4 & 6 & 0 & 32 & 0 & 0 & 0 & 0 & 0 \\ -15 & -5 & 1 & 3 & 1 & -5 & -15 & 0 & 0 & 32 & 0 & 0 & 0 & 0 \\ 8 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 0 & 8 & 0 & 0 & 0 & 0 & 0 & -6 & -4 & -2 & 0 & 2 & 4 & 6 \end{pmatrix},$$

$$M_2 = \begin{pmatrix} 20 & 0 & -4 & 0 & 4 & 0 & -20 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 15 & -5 & -1 & 3 & -1 & -5 & 15 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & -4 & 2 & 0 & -2 & 4 & -6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 15 & 5 & -1 & -3 & -1 & 5 & 15 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 20 & 0 & -4 & 0 & 4 & 0 & -20 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 15 & -5 & -1 & 3 & -1 & -5 & 15 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & -4 & 2 & 0 & -2 & 4 & -6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -20 & 0 & 4 & 0 & -4 & 0 & 20 & 0 & 0 & 0 & 32 & 0 & 0 & 0 \\ -15 & 5 & 1 & -3 & 1 & 5 & -15 & 0 & 0 & 0 & 0 & 32 & 0 & 0 \\ -6 & 4 & -2 & 0 & 2 & -4 & 6 & 0 & 0 & 0 & 0 & 0 & 32 & 0 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 32 \\ 0 & 0 & 8 & 0 & 0 & 0 & 0 & -15 & -5 & 1 & 3 & 1 & -5 & -15 \\ 0 & 0 & 0 & 8 & 0 & 0 & 0 & -20 & 0 & 4 & 0 & -4 & 0 & 20 \\ 0 & 0 & 0 & 0 & 8 & 0 & 0 & -15 & 5 & 1 & -3 & 1 & 5 & -15 \\ 0 & 0 & 0 & 0 & 0 & 8 & 0 & -6 & 4 & -2 & 0 & 2 & -4 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 8 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \end{pmatrix}.$$

Letting

$$\mathbf{s}_1^{\mathsf{T}} = \left(0, \tfrac{14}{3}, -\tfrac{2}{3}, -\tfrac{3}{4}, 4, -1, -1, -\tfrac{1}{12}, -\tfrac{1}{3}, -1, -1, -1, -1\right),$$
$$\mathbf{s}_2^{\mathsf{T}} = \left(\tfrac{1}{8}, 0, \tfrac{1}{32}, 0, 0, 0, 0, 0, 1, 0, 0, \tfrac{11}{96}, \tfrac{1}{12}, 0, \tfrac{1}{24}, 0, 0, 0\right),$$

one can see that

$$\mathbf{s}_1^{\mathsf{T}} M_1 + \mathbf{s}_2^{\mathsf{T}} M_2 = \left(0, 0, 0, 0, 0, 0, 0, 0, -\tfrac{88}{3}, -29, 0, 0, \ldots, 0\right),$$

$\mathbf{s}_1^{\mathsf{T}} \mathbf{r} = 4$ and $\mathbf{s}_2 \geq \mathbf{0}$, as required by our criterion.

Acknowledgements

We gratefully acknowledge IBM for CPLEX, which is the LP/ILP solver in IBM ILOG CPLEX Optimization Studio 12.2 that IBM provides free of charge via the IBM Academic Initiative. The authors thank Markus Grassl for useful discussions.

References

[1] S. A. Aly, "On quantum and classical error control codes: Constructions and applications," 2008 [Online]. Available: http://arxiv.org/pdf/0812.5104

[2] S. A. Aly and A. Ashikhmin, "Nonbinary quantum cyclic and subsystem codes over asymmetrically-decohered quantum channels," *IEEE Information Theory Workshop (ITW) 2010*, pp. 1–5, Jan. 2010.

[3] R. Bagnara, P. M. Hill, and E. Zaffanella, "The Parma polyhedra library: Toward a complete set of numerical abstractions for the analysis and verification of hardware and software systems," *Science of Computer Programming*, vol. 72, pp. 3–21, 2008 [Online]. Available: http://bugseng.com/products/ppl

[4] G. T. Bogdanova, A. E. Brouwer, S. N. Kapralov, and P. R. J. Östergård, "Error-correcting codes over an alphabet of four elements," *Designs, Codes and Cryptography*, vol. 23, pp. 333–342, 2001.

[5] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system. I. The user language," *J. Symbolic Comput.*, vol. 24, no. 3-4, pp. 235–265, 1997.

[6] 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, pp. 1369–1387, Jul. 1998.

[7] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098–1105, Aug. 1996.

[8] P. Delsarte, "Bounds for unrestricted codes by linear programming," *Phillips Research Report*, vol. 27, pp. 47–64, 1972.

[9] P. Delsarte, "Four fundamental parameters of a code and their combinatorial significance," *Information and Control*, vol. 23, pp. 407–438, 1973.

[10] C. Ding, D. R. Kohel, and S. Ling, "Elementary 2-group character codes," *IEEE Trans. Inf. Theory*, vol. 46, pp. 280–284, Jan. 2000.

[11] M. F. Ezerman, S. Ling, and P. Solé, "Additive asymmetric quantum codes," *IEEE Trans. Inf. Theory*, vol. 57, pp. 5536–5550, Aug. 2011.

[12] M. F. Ezerman, S. Jitman, H. M. Kiah, and S. Ling, "Pure asymmetric quantum MDS codes from CSS construction: A complete characterization," *Int. J. of Quantum Information*, vol. 11, 1350027, Jun. 2013.

[13] 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: http://arxiv.org/pdf/0709.3875

[14] K. Feng, S. Ling, and C. Xing, "Asymptotic bounds on quantum codes from algebraic geometry codes," *IEEE Trans. Inf. Theory*, vol. 52, pp. 986–991, Mar. 2006.

[15] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*. Online available at http://www.codetables.de, accessed on July 20, 2012.

[16] M. Grassl and T. A. Gulliver, "On circulant self-dual codes over small fields," *Designs, Codes and Cryptography*, vol. 52, pp. 57–81, 2009.

[17] T. A. Gulliver, J-L. Kim, and Y. Lee, "New MDS or Near-MDS self-dual codes," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4354–4360, Sep. 2008.

[18] A. S. Hedayat, N. J. A. Sloane, and J. Stufken, *Orthogonal Arrays, Theory and Applications*. New York: Springer-Verlag, 1999.

[19] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge: Cambridge Univ. Press, 2003.

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

[21] S. Jitman, S. Ling, H. Liu, and X. Xie, "Checkable codes from group rings," preprint, 2010 [Online]. Available: http://arxiv.org/pdf/1012.5498

[22] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 52, pp. 4892–4914, Nov. 2006.

[23] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications vol. 20. Cambridge: Cambridge Univ. Press, 1997.

[24] S. Ling, "A family of group character codes," *European J. of Combinatorics*, vol. 25, pp. 579–590, 2004.

[25] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.

[26] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Self-Dual Codes and Invariant Theory*, Algorithms and Computation in Mathematics vol. 17. Berlin, Heidelberg: Springer-Verlag, 2006.

[27] D. V. Pasechnik, "Adding Delsarte bound for codes," Jun. 2012 [Online]. Available:http://trac.sagemath.org/12418

[28] E. M. Rains, "Nonbinary quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, pp. 1827–1832, Sep. 1999.

[29] Risan and D. V. Pasechnik, "Arbitrary precision LP solver backend," Jun. 2012 [Online]. Available:http://trac.sagemath.org/12533

[30] P. K. Sarvepalli, A. Klappenecker, and M. Rötteler, "Asymmetric quantum codes: Constructions, bounds and performance," *Proc. of the Royal Soc. A*, vol. 465, pp. 1645–1672, 2009.

[31] A. M. Steane, "Multiple particle interference and quantum error correction," *Proc. of the Royal Soc. A*, vol. 452, pp. 2551-2577, 1996.

[32] W. A. Stein and others, *Sage Mathematics Software (Version 5.0)*, The Sage Development Team, 2012 [Online]. Available: http://www.sagemath.org

[33] L. Wang, K. Feng, S. Ling, and C. Xing, "Asymmetric quantum codes: Characterization and constructions," *IEEE Trans. Inf. Theory*, vol. 56, pp. 2938–2945, Jun. 2010.

Martianus Frederic Ezerman (M'10) grew up in East Java Indonesia. He received the B.A. degree in philosophy and the B.Sc. degree in mathematics in 2005 as well as the M.Sc. degree in mathematics in 2007, all from Ateneo de Manila University, Philippines. In 2011 he obtained the Ph.D. degree in mathematics from Nanyang Technological University, Singapore. After a year of postdoctoral fellowship at Laboratoire d'Information Quantique, Université Libre de Bruxelles, Belgium, he joined the Centre for Quantum Technologies at the National University of Singapore in October of 2012.

His main research interests are error-correcting codes, both classical and quantum, and related structures in algebra and combinatorics.

Somphong Jitman received the B.Sc. degree from Prince of Songkla University, Thailand, in 2005 and the M.Sc. and Ph.D. degrees in mathematics from Chulalongkorn University, Thailand, in 2007 and 2011, respectively. He was a Research Fellow with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, at Nanyang Technological University in Singapore for two years prior to returning to Thailand in May of 2013 to become a Lecturer with the Department of Mathematics, Faculty of Science, Silpakorn University.

His research interests cover classical error-correcting codes, codes over rings as well as quantum error-correcting codes.

San Ling received the B.A. degree in mathematics from the University of Cambridge 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, in 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 applications of number theory to combinatorial designs, coding theory, cryptography and sequences.

Dmitrii V. Pasechnik received the M.Sc. degree in computing from Moscow Institute for Steel and Alloys in 1988 and the Ph.D. degree in mathematics from the University of Western Australia in 1996. Prior to joining the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, in Nanyang Technological University, Singapore in January 2006 he held a number of postdoctoral positions in the Netherlands and Germany.

His research interests include combinatorics, optimisation, computational algebra and geometry, and complexity of algorithms.