Asymmetric and Symmetric Subsystem BCH Codes and Beyond

Salah A. Aly
Department of Computer Science
Texas A&M University, College Station, TX 77843, USA
Email: salah@cs.tamu.edu

***Abstract*—Recently, the theory of quantum error control codes has been extended to subsystem codes over symmetric and asymmetric quantum channels – qubit-flip and phase-shift errors may have equal or different probabilities. Previous work in constructing quantum error control codes has focused on code constructions for symmetric quantum channels. In this paper, we develop a theory and establish the connection between asymmetric quantum codes and subsystem codes. We present families of subsystem and asymmetric quantum codes derived, once again, from classical BCH and RS codes over finite fields. Particularly, we derive an interesting asymmetric and symmetric subsystem codes based on classical BCH codes with parameters $[[n,k,r,d]]_q$, $[[n,k,r,d_z/d_x]]_q$ and $[[n,k',0,d_z/d_x]]_q$ for arbitrary values of code lengths and dimensions. We establish asymmetric Singleton and Hamming bounds on asymmetric quantum and subsystem code parameters; and derive optimal asymmetric MDS subsystem codes. Finally, our constructions are well explained by an illustrative example.**

This paper is written on the occasion of the 50th anniversary of the discovery of classical BCH codes and their quantum counterparts were derived nearly 10 years ago.

I. Introduction

In 1996, Andrew Steane stated in his seminal work [43, page 2, col. 2][42], [44] *"The notation $\{n, K, d_1, d_2\}$ is here introduced to identify a 'quantum code,' meaning a code by which n quantum bits can store K bits of quantum information and allow correction of up to $\lfloor (d_1-1)/2 \rfloor$ amplitude errors, and simultaneously up to $\lfloor (d_2-1)/2 \rfloor$ phase errors."* This paper is motivated by this statement, in which we construct efficient quantum codes that correct amplitude (qubit-flip) errors and phase-shift errors separately. In [34], it was said that *"BCH codes are among the powerful codes"*. We address constructions of quantum and subsystem codes based on Bose-Chaudhuri-Hocquenghem (BCH) codes over finite fields for quantum symmetric and asymmetric channels.

Many quantum error control codes (QEC) have been constructed over the last decade to protect quantum information against noise and decoherence. In coding theory, researchers have focused on bounds and the construction aspects of quantum codes for large and asymptomatic code lengths. On the other hand, physicists intend to study the physical realization and mechanical quantum operations of these codes for short code lengths. As a result, various approaches to protect quantum information against noise and decoherence are proposed including stabilizer block codes, quantum convolutional codes, entangled-assisted quantum error control codes, decoherence free subspaces, nonadditive codes, and subsystem codes [13], [18], [21], [22], [38], [33], [36], [27], [47] and references therein.

Asymmetric quantum control codes (AQEC), in which quantum errors have different probabilities — $\Pr Z > \Pr X$, are more efficient than the symmetric quantum error control codes (QEC), in which quantum errors have equal probabilities — $\Pr Z = \Pr X$. It is argued in [26] that dephasing (loss of phase coherence, phase-shifting) will happen more frequently than relaxation (exchange of energy with the environment, qubit-flipping). The noise level in a qubit is specified by the relaxation T_1 and dephasing time T_2; furthermore the relation between these two values is given by $1/T_1 = 1/(2T_1) + \Gamma_p$; this has been well explained by physicists in [19], [26], [46]. The ratio between the probabilities of qubit-flip X and phase-shift Z is typically $\rho \approx 2T_1/T_2$. The interpretation is that T_1 is much larger than T_2, meaning the photons take much more time to flip from the ground state to the excited state. However, they change rapidly from one excited state to another. Motivated by this, **one needs to design quantum codes that are suitable for this physical phenomena.** The fault tolerant operations of a quantum computer carrying controlled and measured quantum information over asymmetric channel have been investigated in [2], [14], [15], [45], [46], [1] and references therein. Fault-tolerant operations of QEC are investigated for example in [3], [1], [22], [37], [41], [45], [30] and references therein.

Subsystem codes (SSC) as we prefer to call them were mentioned in the unpublished work by Knill [31], [29], in which he attempted to generalize the theory of quantum error-correcting codes into subsystem codes. Such codes with their stabilizer formalism were reintroduced recently [11], [14], [15], [28], [32], [35]. The construction aspects of these codes are given in [9], [8], [11]. Here we expand our understanding and introduce asymmetric subsystem codes (ASSC).

The codes derived in [10], [12] for primitive and non-primitive quantum BCH codes assume that qubit-flip errors, phase-shift errors, and their combination occur with equal probability, where $\Pr Z = \Pr X = \Pr Y = p/3$, $\Pr I = 1-p$, and $\{X, Z, Y, I\}$ are the binary Pauli operators P shown in Section II, see [18], [40]. We aim to generalize these codes over asymmetric quantum channels. In this paper we give families of asymmetric quantum error control codes (AQEC's) motivated by the work from [19], [26], [46]. Assume we have a classical good error control code C_i with parameters

$[[n, k_i, d_i]]_q$ for $i \in \{1, 2\}$ — codes with high minimum distances d_i and high rates k_i/n. We can construct a quantum code based on these two classical codes, in which C_1 controls the qubit-flip errors while C_2 takes care of the phase-shift errors, see Lemma 4.

Our following theorem establishes the connection between two classical codes and QEC, AQEC, SCC, ASSC.

***Theorem** 1 (CSS AQEC and ASSC):* Let C_1 and C_2 be two classical codes with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ respectively, and $d_x = \min\big\{\operatorname{wt}(C_1 \backslash C_2^{\perp}), \operatorname{wt}(C_2 \backslash C_1^{\perp})\big\}$, and $d_z = \max\big\{\operatorname{wt}(C_1 \backslash C_2^{\perp}), \operatorname{wt}(C_2 \backslash C_1^{\perp})\big\}$.

i) if $C_2^{\perp} \subseteq C_1$, then there exists an AQEC with parameters $[[n, \dim C_1 - \dim C_2^{\perp}, \operatorname{wt}(C_2 \backslash C_1^{\perp}) / \operatorname{wt}(C_1 \backslash C_2^{\perp})]]_q$ that is $[[n, k_1 + k_2 - n, d_z/d_x]]_q$. Also, there exists a QEC with parameters $[[n, k_1 + k_2 - n, d_x]]_q$.

ii) From [i], there exists an SSC with parameters $[[n, k_1 + k_2 - n - r, r, d_x]]_q$ for $0 \leq r < k_1 + k_2 - n$.

iii) If $C_2^{\perp} = C_1 \cap C_1^{\perp} \subseteq C_2$, then there exists an ASSC with parameters $[[n, k_2 - k_1, k_1 + k_2 - n, d_z/d_x]]_q$ and $[[n, k_1 + k_2 - n, k_2 - k_1, d_z/d_x]]_q$.

Furthermore, all constructed codes are pure to their minimum distances.

A well-known construction on the theory of quantum error control codes is called CSS constructions. The codes $[[5, 1, 3]]_2$, $[[7, 1, 3]]_2$, $[[9, 1, 3]]_2$, and $[[9, 1, 4, 3]]_2$ have been investigated in several research papers that analyzed their stabilizer structure, circuits, and fault tolerant quantum computing operations. On this paper, we present several AQEC codes, including a $[[15, 3, 5/3]]_2$ code, which encodes three logical qubits into 15 physical qubits, detects 2 qubit-flip and 4 phase-shift errors, respectively. As a result, many of the quantum constructed codes and families of QEC for large lengths need further investigations. We believe that their generalization is a direct consequence.

The paper is organized as follows. Sections II, III, and V are devoted to AQEC and two families of AQEC, AQEC-BCH and AQEC-RS. We establish conditions on the existence of these families over finite fields. Sections IV and VI address the subsystem code constructions and their relation to asymmetric quantum codes. We show the tradeoff between subsystem codes and AQEC. Section VI presents the bound on AQEC and ASSC code parameters. Finally, the paper is concluded with a discussion in Section VII.

II. Asymmetric Quantum Codes

In this section we shall give some primary definitions and introduce AQEC constructions. Consider a quantum system with two-dimensional state space $\mathcal{C}^2$. The basis vectors

$$v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad v_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1}$$

can be used to represent the classical bits 0 and 1. It is customary in quantum information processing to use Dirac's ket notation for the basis vectors; namely, the vector v_0 is denoted by the ket $|0\rangle$ and the vector v_1 is denoted by ket $|1\rangle$. Any possible state of a two-dimensional quantum system is given by a linear combination of the form

$$a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}, \text{ where } a, b \in \mathcal{C} \text{ and } |a|^2 + |b|^2 = 1, \tag{2}$$

In quantum information processing, the operations manipulating quantum bits follow the rules of quantum mechanics, that is, an operation that is not a measurement must be realized by a unitary operator. For example, a quantum bit can be flipped by a quantum NOT gate X that transfers the qubits $|0\rangle$ and $|1\rangle$ to $|1\rangle$ and $|0\rangle$, respectively. Thus, this operation acts on a general quantum state as follows.

$$X(a|0\rangle + b|1\rangle) = a|1\rangle + b|0\rangle.$$

With respect to the computational basis, the quantum NOT gate X represents the qubit-flip errors.

$$X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{3}$$

Also, let $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ be a matrix represents the quantum phase-shift errors that changes the phase of a quantum system (states).

$$Z(a|0\rangle + b|1\rangle) = a|0\rangle - b|1\rangle. \tag{4}$$

Other popular operations include the combined bit and phase-flip $Y = iZX$, and the Hadamard gate H, which are represented with respect to the computational basis by the matrices

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{5}$$

Connection to Classical Binary Codes. Let H_i and G_i be the parity check and generator matrices of a classical code C_i with parameters $[n, k_i, d_i]_2$ for $i \in \{1, 2\}$. The commutativity condition of H_1 and H_2 is stated as

$$H_1.H_2^T + H_2.H_1^T = \mathbf{0}. \tag{6}$$

The stabilizer of a quantum code based on the parity check matrices H_1 and H_2 is given by

$$H_{stab} = \Big(H_1 \mid H_2\Big). \tag{7}$$

One of these two classical codes controls the phase-shift errors, while the other codes controls the bit-flip errors. Hence the CSS construction of a binary AQEC can be stated as follows. Hence the codes C_1 and C_2 are mapped to H_x and H_z, respectively.

***Definition** 2:* Given two classical binary codes C_1 and C_2 such that $C_2^{\perp} \subseteq C_1$. If we form $G = \begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$, and $H = \begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix}$, then

$$H_1.H_2^T - H_2.H_1^T = 0 \tag{8}$$

Let $d_1 = \mathrm{wt}(C_1 \backslash C_2)$ and $d_2 = wt(C_2 \backslash C_1^{\perp})$, such that $d_2 > d_1$ and $k_1 + k_2 > n$. If we assume that C_1 corrects the qubit-flip errors and C_2 corrects the phase-shift errors, then there exists AQEC with parameters

$$[[n, k_1 + k_2 - n, d_2/d_1]]_2. \tag{9}$$

We can always change the rules of C_1 and C_2 to adjust the parameters.

A. Higher Fields and Total Error Groups

We can briefly discuss the theory in terms of higher finite fields $\mathbf{F}_q$. Let $\mathcal{H}$ be the Hilbert space $\mathcal{H} = \mathcal{C}^{q^n} = \mathcal{C}^q \otimes \mathcal{C}^q \otimes ... \otimes \mathcal{C}^q$. Let $|x\rangle$ be the vectors of orthonormal basis of $\mathcal{C}^q$, where the labels x are elements in the finite field $\mathbf{F}_q$. Let $a, b \in \mathbf{F}_q$, the unitary operators $X(a)$ and $Z(b)$ in $\mathcal{C}^q$ are stated as:

$$X(a)|x\rangle = |x + a\rangle, \qquad Z(b)|x\rangle = \omega^{\mathrm{tr}(bx)}|x\rangle, \tag{10}$$

where $\omega = \exp(2\pi i/p)$ is a primitive pth root of unity and tr is the trace operation from $\mathbf{F}_q$ to $\mathbf{F}_p$

Let $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbf{F}_q^n$ and $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbf{F}_q^n$. Let us denote by

$$\begin{aligned} X(\mathbf{a}) &= X(a_1) \otimes \cdots \otimes X(a_n) \text{ and,} \\ Z(\mathbf{b}) &= Z(b_1) \otimes \cdots \otimes Z(b_n) \end{aligned} \tag{11}$$

the tensor products of n error operators. The sets

$$\begin{aligned} \mathbf{E}_x &= \{X(\mathbf{a}) = \bigotimes_{i=1}^{n} X(a_i) \mid \mathbf{a} \in \mathbf{F}_q^n, a_i \in \mathbf{F}_q\}, \\ \mathbf{E}_z &= \{Z(\mathbf{b}) = \bigotimes_{i=1}^{n} Z(b_i) \mid \mathbf{b} \in \mathbf{F}_q^n, b_i \in \mathbf{F}_q\} \end{aligned} \tag{12}$$

form an error basis on $\mathcal{C}^{q^n}$. We can define the error group $\mathbf{G}_x$ and $\mathbf{G}_z$ as follows

$$\begin{aligned} \mathbf{G}_x &= \{\omega^c \mathbf{E}_x = \omega^c X(\mathbf{a}) \,|\, \mathbf{a} \in \mathbf{F}_q^n, c \in \mathbf{F}_p\}, \\ \mathbf{G}_z &= \{\omega^c \mathbf{E}_z = \omega^c Z(\mathbf{b}) \,|\, \mathbf{b} \in \mathbf{F}_q^n, c \in \mathbf{F}_p\}. \end{aligned} \tag{13}$$

Hence the total error group

$$\begin{aligned} \mathbf{G} &= \{\mathbf{G}_x, \mathbf{G}_z\} \\ &= \left\{\omega^c \bigotimes_{i=1}^{n} X(a_i), \omega^c \bigotimes_{i=1}^{n} Z(b_i) \mid a_i, b_i \in \mathbf{F}_q\right\} \end{aligned} \tag{14}$$

Let us assume that the sets $\mathbf{G}_x$ and $\mathbf{G}_z$ represent the qubit-flip and phase-shift errors, respectively.

Many constructed quantum codes assume that the quantum errors resulted from decoherence and noise have equal probabilities, $\Pr X = \Pr Z$. This statement as shown by experimental physics is not true [46], [26]. This means the qubit-flip and phase-shift errors happen with different probabilities. Therefore, it is needed to construct quantum codes that deal with the realistic quantum noise. We derive families of asymmetric quantum error control codes that differentiate between these two kinds of errors, $\Pr Z > \Pr X$.

***Definition** 3 (AQEC):* A q-ary asymmetric quantum code Q, denoted by $[[n, k, d_z/d_x]]_q$, is a q^k dimensional subspace of the Hilbert space $\mathbb{C}^{q^n}$ and can control all bit-flip errors up to $\lfloor \frac{d_x - 1}{2} \rfloor$ and all phase-flip errors up to $\lfloor \frac{d_z - 1}{2} \rfloor$. The code Q detects $(d_1 - 1)$ qubit-flip errors as well as detects $(d_1 - 1)$ phase-shift errors.

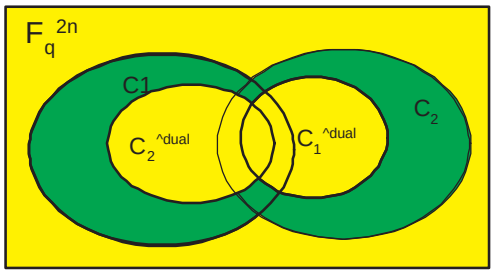

Fig. 1. Constructions of asymmetric quantum codes based on two classical codes C_1 and C_2 with parameters $[n, k_1]$ and $[n, d_2]$ such that $C_i \subseteq C_{1+(i \mod 2)}$ for $i = \{1, 2\}$. AQEC has parameters $[[n, k_1 + k_2 - n, d_z/d_x]]_q$ where $d_x = \mathrm{wt}(C_1 \backslash C_2^{\perp})$ and $d_z = \mathrm{wt}(C_2 \backslash C_1^{\perp})$

We use different notation from the one given in [19]. The reason is that we would like to compare d_z and d_x as a factor $\rho = d_z/d_x$ not as a ratio. Therefore, if $d_z > d_x$, then the AQEC has a factor great than one. Hence, the phase-shift errors affect the quantum system more than qubit-flip errors do. In our work, we would like to increase both the factor ρ and dimension k of the quantum code.

Connection to Classical nonbinary Codes. Let C_1 and C_2 be two linear codes over the finite field $\mathbf{F}_q$, and let $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ be their parameters. For $i \in \{1, 2\}$, if H_i is the parity check matrix of the code C_i, then $\dim C_i^{\perp} = n - k_i$ and rank of $H_i^{\perp}$ is k_i. If $C_i^{\perp} \subseteq C_{1+(i \mod 2)}$, then $C_{1+(i \mod 2)}^{\perp} \subseteq C_i$. So, the rows of H_i which form a basis for $C_i^{\perp}$ can be extended to form a basis for $C_{1+(i \mod 2)}$ by adding some vectors. Also, if $g_i(x)$ is the generator polynomial of a cyclic code C_i then $k_i = n - deg(g_i(x))$, see [34], [25].

The error groups $\mathbf{G}_x$ and $\mathbf{G}_z$ can be mapped, respectively, to two classical codes C_1 and C_2 in a similar manner as in QEC. This connection is well-know, see for example [18], [38], [39]. Let C_i be a classical code such that $C_{1+(i \mod 2)}^{\perp} \subseteq C_i$ for $i \in \{1, 2\}$, then we have a symmetric quantum control code (AQEC) with parameters $[[n, k_1 + k_2 - n, d_z/d_x]]_q$. This can be illustrated in the following result.

***Lemma** 4 (CSS AQEC):* Let C_i be a classical code with parameters $[n, k_i, d_i]_q$ such that $C_i^{\perp} \subseteq C_{1+(i \mod 2)}$ for $i \in \{1, 2\}$, and $d_x = \min\left\{\mathrm{wt}(C_1 \backslash C_2^{\perp}), \mathrm{wt}(C_2 \backslash C_1^{\perp})\right\}$, and $d_z = \max\left\{\mathrm{wt}(C_1 \backslash C_2^{\perp}), \mathrm{wt}(C_2 \backslash C_1^{\perp})\right\}$. Then there is asymmetric quantum code with parameters $[[n, k_1 + k_2 - n, d_z/d_x]]_q$. The quantum code is pure to its minimum distance meaning that if $\mathrm{wt}(C_1) = \mathrm{wt}(C_1 \backslash C_2^{\perp})$ then the code is pure to d_x, also if $\mathrm{wt}(C_2) = \mathrm{wt}(C_2 \backslash C_1^{\perp})$ then the code is pure to d_z.

Therefore, it is straightforward to derive asymmetric quantum control codes from two classical codes as shown in Lemma 4. Of course, one wishes to increase the values of d_z vers. d_x for the same code length and dimension.

***Remark** 5:* The notations of purity and impurity of AQEC remain the same as shown for QEC, the interested reader might consider any primary papers on QEC.

III. Asymmetric Quantum BCH and RS Codes

In this section we derive classes of AQEC based on classical BCH and RS codes. We will restrict ourself to the Euclidean construction for codes defined over $\mathbf{F}_q$. However, the generalization to the Hermitian construction for codes defined over $\mathbf{F}_{q^2}$ is straight forward. We keep the definitions of BCH codes to a minimal since they have been well-known, see example [10] or any textbook on classical coding theory [34], [25], [24]. Let q be a power of a prime and n a positive integer such that $\gcd(q,n)=1$. Recall that the cyclotomic coset S_x modulo n is defined as

$$S_x = \{xq^i \bmod n \mid i \in \mathbf{Z}, i \geq 0\}. \tag{15}$$

Let m be the multiplicative order of q modulo n. Let α be a primitive element in $\mathbf{F}_{q^m}$. A nonprimitive narrow-sense BCH code C of designed distance δ and length n over $\mathbf{F}_q$ is a cyclic code with a generator monic polynomial $g(x)$ that has $\alpha, \alpha^2, \ldots, \alpha^{\delta-1}$ as zeros,

$$g(x) = \prod_{i=1}^{\delta-1}(x-\alpha^i). \tag{16}$$

Thus, c is a codeword in $\mathcal{C}$ if and only if $c(\alpha) = c(\alpha^2) = \ldots = c(\alpha^{\delta-1}) = 0$. The parity check matrix of this code can be defined as

$$H_{bch} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{\delta-1} & \alpha^{2(\delta-1)} & \cdots & \alpha^{(\delta-1)(n-1)} \end{bmatrix}. \tag{17}$$

In general the dimensions and minimum distances of BCH codes are not known. However, lower bounds on these two parameters for such codes are given by $d \geq \delta$ and $k \geq n - m(\delta-1)$. Fortunately, in [10], [12] exact formulas for the dimensions and minimum distances are given under certain conditions. The following result shows the dimension of BCH codes.

***Theorem** 6 (Dimension BCH Codes):* Let q be a prime power and $\gcd(n,q)=1$, with $ord_n(q)=m$. Then a narrow-sense BCH code of length $q^{\lfloor m/2 \rfloor} < n \leq q^m - 1$ over $\mathbf{F}_q$ with designed distance δ in the range $2 \leq \delta \leq \delta_{\max} = \min\{\lfloor nq^{\lceil m/2 \rceil}/(q^m-1) \rfloor, n\}$, has dimension of

$$k = n - m\lceil(\delta-1)(1-1/q)\rceil. \tag{18}$$

Proof: See [10, Theorem 10]. ■

Steane first derived binary quantum BCH codes in [43], [44]. In addition Grassl *el. at.* gave a family of quantum BCH codes along with tables of best codes [23].

In [12], [10], while it was a challenging task to derive self-orthogonal or dual-containing conditions for BCH codes, we can relax and omit these conditions by looking for BCH codes that are nested. The following result shows a family of QEC derived from nonprimitive narrow-sense BCH codes.

We can also switch between the code and its dual to construct a quantum code. When the BCH codes contain their duals, then we can derive the following codes.

TABLE I
Families of asymmetric quantum BCH codes [16]

q	C_1 BCH Code	C_2 BCH Code	AQEC
2	$[15,11,3]$	$[15,7,5]$	$[[15,3,5/3]]_2$
2	$[15,8,4]$	$[15,7,5]$	$[[15,0,5/4]]_2$
2	$[31,21,5]$	$[31,16,7]$	$[[31,6,7/5]]_2$
2	$[31,26,3]$	$[31,16,7]$	$[[31,11,7/3]]$
2	$[31,26,3]$	$[31,16,7]$	$[[31,10,8/3]]$
2	$[31,26,3]$	$[31,11,11]$	$[[31,6,11/3]]$
2	$[31,26,3]$	$[31,6,15]$	$[[31,1,15/3]]$
2	$[127,113,5]$	$[127,78,15]$	$[[127,64,15/5]]$
2	$[127,106,7]$	$[127,77,27]$	$[[127,56,25/7]]$

***Theorem** 7:* Let $m = \mathrm{ord}_n(q)$ and $q^{\lfloor m/2 \rfloor} < n \leq q^m - 1$ where q is a power of a prime and $2 \leq \delta \leq \delta_{\max}$, with

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

then there exists a quantum code with parameters

$$[[n, n-2m\lceil(\delta-1)(1-1/q)\rceil, \geq \delta]]_q$$

pure to $\delta_{\max}+1$

Proof: See [10, Theorem 19]. ■

A. AQEC-BCH

Fortunately, the mathematical structure of BCH codes always us easily to show the nested required structure as needed in Lemma 4. We know that $g(x)$ is a generator polynomial of a narrow sense BCH code that has roots $\alpha^2, \alpha^3, \ldots, \alpha^{\delta-1}$ over $\mathbf{F}_q$. We know that the generator polynomial has degree $m\lfloor(\delta-1)(1-1/\delta)\rfloor$ if $\delta \leq \delta_{max}$. Therefore the dimension is given by $k = n - deg(g(x))$. Hence, the nested structure of BCH codes is obvious and can be described as follows. Let

$$\delta_{i+1} > \delta_i > \delta_{i-1} \geq \ldots \geq 2, \tag{19}$$

and let C_i be a BCH code that has generator polynomial $g_i(x)$, in which it has roots $\{2,3,\ldots,\delta-1\}$. So, C_i has parameters $[n, n-deg(g_i(x)), d_i \geq \delta_i]_q$, then

$$C_{i+1} \subseteq C_i \subseteq C_{i-1} \subseteq \ldots \tag{20}$$

We need to ensure that δ_i and δ_{i+1} away of each other, so the elements (roots) $\{2,\ldots,\delta_i-1\}$ and $\{2,\ldots,\delta_{i+1}-1\}$ are different. This means that the cyclotomic cosets generated by δ_i and δ_{i+1} are not the same, $S_1 \cup \ldots \cup S_{\delta_i-1} \neq S_1 \cup \ldots \cup S_{\delta_{i+1}-1}$. Let $\delta_i^\perp$ be the designed distance of the code $C_i^\perp$. Then the following result gives a family of AQEC BCH codes over $\mathbf{F}_q$.

***Theorem** 8 (AQEC-BCH):* Let q be a prime power and $\gcd(n,q)=1$, with $ord_n(q)=m$. Let C_1 and C_2 be two narrow-sense BCH codes of length $q^{\lfloor m/2 \rfloor} < n \leq q^m - 1$ over $\mathbf{F}_q$ with designed distances δ_1 and δ_2 in the range $2 \leq \delta_1, \delta_2 \leq \delta_{\max} = \min\{\lfloor nq^{\lceil m/2 \rceil}/(q^m-1) \rfloor, n\}$ and $\delta_1 < \delta_2^\perp \leq \delta_2 < \delta_1^\perp$.

Assume $S_1 \cup \ldots \cup S_{\delta_1-1} \neq S_1 \cup \ldots \cup S_{\delta_2-1}$, then there exists an asymmetric quantum error control code with parameters $[[n, n-m\lceil(\delta_1-1)(1-1/q)\rceil - m\lceil(\delta_2-1)(1-$

$1/q)], \geq d_z/d_x]]_q$, where $d_z = \mathrm{wt}(C_2 \backslash C_1^\perp) \geq \delta_2 > d_x = \mathrm{wt}(C_1 \backslash C_2^\perp) \geq \delta_1$.

Proof: From the nested structure of BCH codes, we know that if $\delta_1 < \delta_2^\perp$, then $C_2^\perp \subseteq C_1$, similarly if $\delta_2 < \delta_1^\perp$, then $C_1^\perp \subseteq C_2$. By Lemma 6, using the fact that $\delta \leq \delta_{\max}$, the dimension of the code C_i is given by $k_i = n - m\lceil(\delta_i - 1)(1 - 1/q)\rceil$ for $i = \{1, 2\}$. Since $S_1 \cup \ldots \cup S_{\delta_1 - 1} \neq S_1 \cup \ldots \cup S_{\delta_2 - 1}$, this means that $deg(g_1(x)) < deg(g_2(x))$, hence $k_2 < k_1$. Furthermore $k_1^\perp < k_2^\perp$.

By Lemma 4 and we assume $d_x = wt(C_1 \backslash C_2^\perp) \geq \delta_1$ and $d_z = wt(C_2 \backslash C_1^\perp) \geq \delta_2$ such that $d_z > d_x$ otherwise we exchange the rules of d_z and d_x; or the code C_i with $C_{1+(i \mod 2)}$. Therefore, there exists AQEC with parameters $[[n, k_1 + k_2 - n, \geq d_z/d_z]]_q$. ∎

The problem with BCH codes is that we have lower bounds on their minimum distance given their arbitrary designed distance. We argue that their minimum distance meets with their designed distance for small values that are particularly interesting to us. One can also use the condition shown in [10, Corollary 11.] to ensure that the minimum distance meets the designed distance.

The condition regarding the designed distances δ_1 and δ_2 allows us to give formulas for the dimensions of BCH codes C_1 and C_2, however, we can derive AQEC-BCH without this condition as shown in the following result. This is explained by an example in the next section.

***Lemma** 9:* Let q be a prime power, $\gcd(m, q) = 1$, and $q^{\lfloor m/2 \rfloor} < n \leq q^m - 1$ for some integers $m = \mathrm{ord}_n(q)$. Let C_1 and C_2 be two BCH codes with parameters $[n, k_1, d_x \geq \delta_1]_q$ and $[n, k_2, d_z \geq \delta_2]_q$, respectively, such that $\delta_1 < \delta_2^\perp \leq \delta_2 < \delta_1^\perp$, and $k_1 + k_2 > n$. Assume $S_1 \cup \ldots \cup S_{\delta_1 - 1} \neq S_1 \cup \ldots \cup S_{\delta_2 - 1}$, then there exists an asymmetric quantum error control code with parameters $[[n, k_1 + k_2 - n, \geq d_z/d_x]]_q$, where $d_z = \mathrm{wt}(C_1 \backslash C_2^\perp) = \delta_2 > d_x = \mathrm{wt}(C_2 \backslash C_1^\perp) = \delta_1$.

In fact the previous theorem can be used to derive any asymmetric cyclic quantum control codes. Also, one can construct AQEC based on codes that are defined over $\mathbf{F}_{q^2}$.

B. RS Codes

We can also derive a family of asymmetric quantum control codes based on Redd-Solomon codes. Recall that a RS code with length $n = q - 1$ and designed distance δ over a finite field $\mathbf{F}_q$ is a code with parameters $[[n, n - d + 1, d = \delta]]_q$ and generator polynomial

$$g(x) = \prod_{i=1}^{d-1} (x - \alpha^i). \tag{21}$$

It is much easier to derive conditions for AQEC derived from RS as shown in the following theorem.

***Theorem** 10:* Let q be a prime power and $n = q - 1$. Let C_1 and C_2 be two RS codes with parameters $[n, n - d_1 + 1, d_1]]_q$ and $[n, n - d_2 + 1, d_2]_q$ for $d_1 < d_2 < d_1^\perp = n - d_1$. Then there exists AQEC code with parameters $[[n, n - d_1 - d_1 + 2, d_z/d_x]]_q$, where $d_x = d_1 < d_z = d_2$.

Proof: since $d_1 < d_2 < d_1^\perp$, then $n - d_1^\perp + 1 < n - d_2 + 1 < n - d_1 + 1$ and $k_1^\perp < k_2 < k_1$. Hence $C_2^\perp \subset C_1$ and $C_1^\perp \subset C_2$. Let $d_z = \mathrm{wt}(C_2 \backslash C_1^\perp) = d_2$ and $d_x = \mathrm{wt}(C_1 \backslash C_2^\perp) = d_1$.

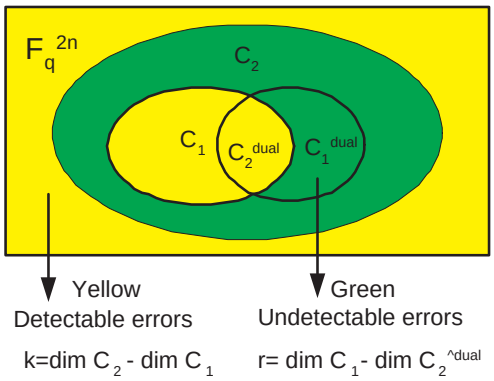

Fig. 2. A quantum code Q is decomposed into two subsystem A (info) and B (gauge)

Therefore there must exist AQEC with parameters $[[n, n - d_1 - d_1 + 2, d_z/d_x]]_q$. ∎

It is obvious from this theorem that the constructed code is a pure code to its minimum distances. One can also derive asymmetric quantum RS codes based on RS codes over $\mathbf{F}_{q^2}$. Also, generalized RS codes can be used to derive similar results. In fact, one can derive AQEC from any two classical cyclic codes obeying the pair-nested structure over $\mathbf{F}_q$.

IV. AQEC and Connection with Subsystem Codes

In this section we establish the connection between AQEC and subsystem codes. Furthermore we derive a larger class of quantum codes called asymmetric subsystem codes (ASSs). We derive families of subsystem BCH codes and cyclic subsystem codes over $\mathbf{F}_q$. In [8], [9] we construct several families of subsystem cyclic, BCH, RS and MDS codes over $\mathbf{F}_{q^2}$ with much more details

We expand our understanding of the theory of quantum error control codes by correcting the quantum errors X and Z separately using two different classical codes, in addition to correcting only errors in a small subspace. Subsystem codes are a generalization of the theory of quantum error control codes, in which errors can be corrected as well as avoided (isolated).

Let Q be a quantum code such that $\mathcal{H} = Q \oplus Q^\perp$, where $Q^\perp$ is the orthogonal complement of Q. We can define the subsystem code $Q = A \otimes B$, see Fig.2, as follows

***Definition** 11 (Subsystem Codes):* An $[[n, k, r, d]]_q$ subsystem code is a decomposition of the subspace Q into a tensor product of two vector spaces A and B such that $Q = A \otimes B$, where $\dim A = q^k$ and $\dim B = q^r$. The code Q is able to detect all errors of weight less than d on subsystem A.

Subsystem codes can be constructed from the classical codes over $\mathbf{F}_q$ and $\mathbf{F}_{q^2}$. Such codes do not need the classical codes to be self-orthogonal (or dual-containing) as shown in the Euclidean construction. We have given general constructions of subsystem codes in [11] known as the subsystem CSS and Hermitian Constructions. We provide a proof for the following special case of the CSS construction.

***Lemma** 12 (SSC Euclidean Construction):* If C_1 is a k'-dimensional $\mathbf{F}_q$-linear code of length n that has a k''-

dimensional subcode $C_2 = C_1 \cap C_1^{\perp}$ and $k' + k'' < n$, then there exist

$$[[n, n-(k'+k''), k'-k'', \mathrm{wt}(C_2^{\perp} \setminus C_1)]]_q$$

$$[[n, k'-k'', n-(k'+k''), \mathrm{wt}(C_2^{\perp} \setminus C_1)]]_q$$

subsystem codes.

Proof: Let us define the code $X = C_1 \times C_1 \subseteq \mathbf{F}_q^{2n}$, therefore $X^{\perp_s} = (C_1 \times C_1)^{\perp_s} = C_1^{\perp_s} \times C_1^{\perp_s}$. Hence $Y = X \cap X^{\perp_s} = (C_1 \times C_1) \cap (C_1^{\perp_s} \times C_1^{\perp_s}) = C_2 \times C_2$. Thus, $\dim_{\mathbf{F}_q} Y = 2k''$. Hence $|X||Y| = q^{2(k'+k'')}$ and $|X|/|Y| = q^{2(k'-k'')}$. By Theorem [11, Theorem 1], there exists a subsystem code $Q = A \otimes B$ with parameters $[[n, \log_q \dim A, \log_q \dim B, d]]_q$ such that

i) $\dim A = q^n/(|X||Y|)^{1/2} = q^{n-k'-k''}$.
ii) $\dim B = (|X|/|Y|)^{1/2} = q^{k'-k''}$.
iii) $d = \mathrm{swt}(Y^{\perp_s} \backslash X) = \mathrm{wt}(C_2^{\perp} \setminus C_1)$.

Exchanging the rules of the codes C_1 and $C_1^{\perp}$ gives us the other subsystem code with the given parameters. ∎

Subsystem codes (SCC) require the code C_2 to be self-orthogonal, $C_2 \subseteq C_2^{\perp}$. AQEC and SSC are both can be constructed from the pair-nested classical codes, as we call them. From this result, we can see that any two classical codes C_1 and C_2 such that $C_2 = C_1 \cap C_1^{\perp} \subseteq C_2^{\perp}$, in which they can be used to construct a subsystem code (SCC), can be also used to construct asymmetric quantum code (AQEC). Asymmetric subsystem codes (ASSCs) are much larger class than the class of symmetric subsystem codes, in which the quantum errors occur with different probabilities in the former one and have equal probabilities in the later one. In short, AQEC does does not require the intersection code to be self-orthogonal.

The construction in Lemma 12 can be generalized to ASSC CSS construction in a similar way. This means that we can look at an AQEC with parameters $[[n, k, d_z/d_x]]_q$. as subsystem code with parameters $[[n, k, 0, d_z/d_x]]_q$. Therefore all results shown in [9], [8], [11] are a direct consequence by just fixing the minimum distance condition.

We have shown in [9], [8] that All stabilizer codes (pure and impure) can be reduced to subsystem codes as shown in the following result.

***Theorem** 13 (Trading Dimensions of SSC and Co-SCC):* Let q be a power of a prime p. If there exists an $\mathbf{F}_q$-linear $[[n, k, r, d]]_q$ subsystem code (stabilizer code if $r = 0$) with $k > 1$ that is pure to d', then there exists an $\mathbf{F}_q$-linear $[[n, k-1, r+1, \geq d]]_q$ subsystem code that is pure to $\min\{d, d'\}$. If a pure ($\mathbf{F}_q$-linear) $[[n, k, r, d]]_q$ subsystem code exists, then a pure ($\mathbf{F}_q$-linear) $[[n, k+r, d]]_q$ stabilizer code exists.

We have shown in [10], [12] that narrow sense BCH codes, primitive and non-primitive, with length n and designed distance δ are Euclidean dual-containing codes if and only if

$$2 \leq \delta \leq \delta_{\max} = \frac{n}{q^m - 1}(q^{\lceil m/2 \rceil} - 1 - (q-2)[m \text{ odd}]). \quad (22)$$

We use this result and [9, Theorem 2] to derive nonprimitive subsystem BCH codes from classical BCH codes over $\mathbf{F}_q$ and $\mathbf{F}_{q^2}$ [11], [12]. The subsystem codes derived in [8] are only for the primitive case.

***Lemma** 14:* If q is power of a prime, m is a positive integer, and $q^{\lfloor m/2 \rfloor} < n \leq q^m - 1$. Let $2 \leq \delta \leq \delta_{\max} = \frac{n}{q^m-1}(q^{\lceil m/2 \rceil} - 1 - (q-2)[m \text{ odd}])$, then there exists a subsystem BCH code with parameters $[[n, n-2m\lceil(\delta-1)(1-1/q)\rceil - r, r, \geq \delta]]_q$ where $0 \leq r < n - 2m\lceil(\delta-1)(1-1/q)\rceil$.

Proof: We know that if $2 \leq \delta \leq \delta_{\max} = \frac{n}{q^m-1}(q^{\lceil m/2 \rceil} - 1 - (q-2)[m \text{ odd}])$, the the classical BCH codes contain their Euclidean dual code by [10, Theorem 3.]. But existence of this code gives a stabilizer code with parameters $[[n, n-2m\lceil(\delta-1)(1-1/q)\rceil, \geq \delta]]_q$ using [10, Theorem 19.].

We know that every stabilizer code can be reduced to a subsystem code by Theorem 13. Let r be an integer in the range $0 \leq r < n - 2m\lceil(\delta-1)(1-1/q)\rceil$. From [9, Theorem 2] or Theorem 13, then there must exist a subsystem BCH code with parameters $[[n, n-2m\lceil(\delta-1)(1-1/q)\rceil - r, r, \geq \delta]]_q$. ∎

We can also construct subsystem BCH codes from stabilizer codes using the Hermitian constructions where the classical BCH codes are defined over $\mathbf{F}_{q^2}$.

***Lemma** 15:* If q is a power of a prime, $m = \mathrm{ord}_n(q^2)$ is a positive integer, and δ is an integer in the range $2 \leq \delta \leq \delta_{\max} = \lfloor n(q^m-1)/(q^{2m}-1) \rfloor$, then there exists a subsystem code Q with parameters

$$[[n, n-2m\lceil(\delta-1)(1-1/q^2)\rceil - r, r, d_Q \geq \delta]]_q$$

that is pure up to δ, where $0 \leq r < n - 2m\lceil(\delta-1)(1-1/q^2)\rceil$.

Proof: We knot that if $2 \leq \delta \leq \delta_{\max} = \lfloor n(q^m - 1)/(q^{2m}-1) \rfloor$, then exists a classical BCH code with parameters $[n, n-m\lceil(\delta-1)(1-1/q^2)\rceil, \geq \delta]_q$ which contains its Hermitian dual code using [10, Theorem 14.]. But existence of the classical code that contains its Hermtian code gives us quantum codes by [10, Theorem 21.]. From [9, Theorem 2], then there must exist a subsystem code with the given parameters $[[n, n-2m\lceil(\delta-1)(1-1/q^2)\rceil - r, r, d_Q \geq \delta]]_q$ that is pure up to δ, for all range of r in $0 \leq r < n - 2m\lceil(\delta-1)(1-1/q^2)\rceil$.. ∎

If fact there is a tradeoff between the construction of subsystem codes and asymmetric quantum codes. The condition $C_2 = C_1 \cap C_1^{\perp}$ used for the construction of SSC, is not needed in the construction of AQEC.

Instead of constructing subsystem codes from stabilizer BCH codes as shown in Lemmas 14, 15, we can also construct subsystem codes from classical BCH codes over $\mathbf{F}_q$ and $\mathbf{F}_{q^2}$ under some restrictions on the designed distance δ. Let S_i be a cyclotomic coset defined as $\{iq^j \mod n \mid j \in \mathbf{Z}\}$. We will derive only SSC from nonprimitive BCH codes over $\mathbf{F}_q$; for codes over $\mathbf{F}_{q^2}$ and further details see [8]. Also, the generator polynomial can be used instead of the defining set (cylotomic cosets) to derive BCH codes.

***Lemma** 16:* If q is a power of a prime, $m = \mathrm{ord}_n(q)$ is a positive integer and $2 \leq \delta \leq \delta_{\max} = \frac{n}{q^m-1}(q^{\lceil m/2 \rceil} - 1 - (q-2)[m \text{ odd}])$. Let C_2 be a BCH code with length $q^{\lfloor m/2 \rfloor} < n \leq q^m - 1$ and defining set $T_{C_2} = \{S_0, S_1, \ldots, S_{n-\delta}\}$, such that $\gcd(n, q) = 1$. Let $T \subseteq \{0\} \cup \{S_\delta, \ldots, S_{n-\delta}\}$ be a nonempty set. Assume $C_1 \subseteq \mathbf{F}_q^n$ be a BCH code with the defining set $T_{C_1} = \{S_0, S_1, \ldots, S_{n-\delta}\} \setminus (T \cup T^{-1})$ where $T^{-1} = \{-t \bmod n \mid t \in T\}$. Then there exists a subsystem

TABLE II
SUBSYSTEM BCH CODES USING THE EUCLIDEAN CONSTRUCTION

Subsystem Code	Parent BCH Code	Designed distance
$[[15,4,3,3]]_2$	$[15,7,5]_2$	4
$[[15,6,1,3]]_2$	$[15,5,7]_2$	6
$[[31,10,1,5]]_2$	$[31,11,11]_2$	8
$[[31,20,1,3]]_2$	$[31,6,15]_2$	12
$[[63,6,21,7]]_2$	$[63,39,9]_2$	8
$[[63,6,15,7]]_2$	$[63,36,11]_2$	10
$[[63,6,3,7]]_2$	$[63,30,13]_2$	12
$[[63,18,3,7]]_2$	$[63,24,15]_2$	14
$[[63,30,3,5]]_2$	$[63,18,21]_2$	16
$[[63,32,1,5]]_2$	$[63,16,23]_2$	22
$[[63,44,1,3]]_2$	$[63,10,27]_2$	24
$[[63,50,1,3]]_2$	$[63,7,31]_2$	28
$[[15,2,5,3]]_4$	$[15,9,5]_4$	4
$[[15,2,3,3]]_4$	$[15,8,6]_4$	6
$[[15,4,1,3]]_4$	$[15,6,7]_4$	7
$[[15,8,1,3]]_4$	$[15,4,10]_4$	8
$[[31,10,1,5]]_4$	$[31,11,11]_4$	8
$[[31,20,1,3]]_4$	$[31,6,15]_4$	12
$[[63,12,9,7]]_4$	$[63,30,15]_4$	15
$[[63,18,9,7]]_4$	$[63,27,21]_4$	16
$[[63,18,7,7]]_4$	$[63,26,22]_4$	22

$*$ punctured code
$+$ Extended code

BCH code with the parameters $[[n, n-2k-r, r, \geq \delta]]_q$, where $k = m\lceil(\delta-1)(1-1/q)\rceil$ and $0 \leq r = |T \cup T^{-1}| < n-2k$.

Proof: The proof can be divided into the following parts:

i) We know that $T_{C_2} = \{S_0, S_1, \ldots, S_{n-\delta}\}$ and $T \subseteq \{0\} \cup \{S_\delta, \ldots, S_{n-\delta}\}$ be a nonempty set. Hence $T_{C_2}^{\perp} = \{S_1, \ldots, S_{\delta-1}\}$. Furthermore, if $2 \leq \delta \leq \delta_{\max} = \frac{n}{q^m-1}(q^{\lceil m/2\rceil} - 1 - (q-2)[m \text{ odd}])$, then $C_2 \subseteq C_2^{\perp}$. Furthermore, let $k = m\lceil(\delta-1)(1-1/q)\rceil$, then $\dim C_2^{\perp} = n-k$ and $\dim C_2 = k$.
ii) We know that $C_1 \in \mathbf{F}_q^n$ is a BCH code with defining set $T_{C_1} = T_{C_2} \setminus (T \cup T^{-1}) = \{S_0, S_1, \ldots, S_{n-\delta}\} \setminus (T \cup T^{-1})$ where $T^{-1} = \{-t \bmod n \mid t \in T\}$. Then the dual code $C_1^{\perp}$ has defining set $T_{C_1}^{\perp} = \{S_1, \ldots, S_{\delta-1}\} \cup T \cup T^{-1} = T_{C_2^{\perp}} \cup T \cup T^{-1}$. We can compute the union set T_{C_2} as $T_{C_1} \cup T_{C_1}^{\perp} = \{S_0, S_1, \ldots, S_{n-\delta}\} = T_{C_2}$. Therefore, $C_1 \cap C_1^{\perp} = C_2$. Furthermore, if $0 \leq r = |T \cup T^{-1}| < n-2k$, then $\dim C_1 = k + r$.
iii) From step (i) and (ii), and for $0 \leq r < n-2k$, and by Lemma 12, there exits a subsystem code with parameters $[[n, \dim C_2^{\perp} - \dim C_1, \dim C_1 - \dim C_2, d]]_q = [[n, n-2k-r, r, d]]_q$, $d = \min wt(C_2^{\perp} - C_1) \geq \delta$.

■

One can also construct asymmetric subsystem BCH codes in a natural way meaning the distances d_x and d_z can be defined using the AQEC definition. In other words one can obtain ASSCs with parameters $[[n, n-2k-r, r, d_z/d_x]]_q$ and $[[n, r, n-2k-r, d_z/d_x]]_q$. The extension to ASSCs based on RS codes is straight forward and similar to our constructions in [9], [8].

A. Cyclic Subsystem Codes

Now, we shall give a general construction for subsystem cyclic codes. This would apply for all cyclic codes including BCH, RS, RM and duadic codes. We show that if a classical cyclic code is self-orthogonal, then one can easily construct cyclic subsystem codes. We say that a code C_2 is self-orthogonal if and only if $C_2 \subseteq C_2^{\perp}$. We will derive subsystem cyclic codes over $\mathbf{F}_q$, and the case of $\mathbf{F}_{q^2}$ is illustrated in [8].

***Theorem** 17:* Let C_2 be a k-dimensional self-orthogonal cyclic code of length n over $\mathbf{F}_q$. Let T_{C_2} and $T_{C_2^{\perp}}$ respectively denote the defining sets of C_2 and $C_2^{\perp}$. If T is a subset of $T_{C_2} \setminus T_{C_2^{\perp}}$ that is the union of cyclotomic cosets, then one can define a cyclic code C_1 of length n over $\mathbf{F}_q$ by the defining set $T_{C_1} = T_{C_2} \setminus (T \cup T^{-1})$. If $r = |T \cup T^{-1}|$ is in the range $0 \leq r < n-2k$, and $d = \min \mathrm{wt}(C_2^{\perp} \setminus C)$, then there exists a subsystem code with parameters $[[n, n-2k-r, r, d]]_q$.

Proof: see [8] and more details are shown in in [4]. ■

Now it is straight forward to derive asymmetric cyclic subsystem codes with parameters $[[n, n-2k-r, r, d_z/d_x]]_q$ for all $0 \leq r < n-2k$ using Theorem 17 where $d_x = \min\{\mathrm{wt}(C_2^{\perp} \setminus C_1), \mathrm{wt}(C_2^{\perp} \setminus C_1^{\perp})\}$ and $d_z = \max\{\mathrm{wt}(C_1^{\perp} \setminus C_2), \mathrm{wt}(C_1^{\perp} \setminus C_2)\}$.

V. ILLUSTRATIVE EXAMPLE

We have demonstrated a family of asymmetric quantum codes with arbitrary length, dimension, and minimum distance parameters. We will present a simple example to explain our construction.

Consider a BCH code C_1 with parameters $[15, 11, 3]_2$ that has designed distance 3 and generator matrix given by

$$\begin{bmatrix} 1&0&0&0&0&0&0&0&0&0&0&1&1&0&0 \\ 0&1&0&0&0&0&0&0&0&0&0&0&1&1&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&1&1 \\ 0&0&0&1&0&0&0&0&0&0&0&1&1&0&1 \\ 0&0&0&0&1&0&0&0&0&0&0&1&0&1&0 \\ 0&0&0&0&0&1&0&0&0&0&0&0&1&0&1 \\ 0&0&0&0&0&0&1&0&0&0&0&1&1&1&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&1&1&1 \\ 0&0&0&0&0&0&0&0&1&0&0&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0&1&0&1&0&1&1 \\ 0&0&0&0&0&0&0&0&0&0&1&1&0&0&1 \end{bmatrix} \quad (23)$$

and the code $C_1^{\perp}$ has parameters $[15, 4, 8]_2$ and generator matrix

$$\begin{bmatrix} 1&0&0&0&1&0&0&1&1&0&1&0&1&1&1 \\ 0&1&0&0&1&1&0&1&0&1&1&1&1&0&0 \\ 0&0&1&0&0&1&1&0&1&0&1&1&1&1&0 \\ 0&0&0&1&0&0&1&1&0&1&0&1&1&1&1 \end{bmatrix} \quad (24)$$

Consider a BCH code C_2 with parameters $[15, 7, 5]_2$ that has designed distance 5 and generator matrix given by

$$\begin{bmatrix} 1&0&0&0&0&0&0&1&0&0&0&1&0&1&1\\ 0&1&0&0&0&0&0&1&1&0&0&1&1&1&0\\ 0&0&1&0&0&0&0&0&1&1&0&0&1&1&1\\ 0&0&0&1&0&0&0&1&0&1&1&1&0&0&0\\ 0&0&0&0&1&0&0&0&1&0&1&1&1&0&0\\ 0&0&0&0&0&1&0&0&0&1&0&1&1&1&0\\ 0&0&0&0&0&0&1&0&0&0&1&0&1&1&1 \end{bmatrix} \quad (25)$$

and the code $C_2^{\perp}$ has parameters $[15, 8, 4]_2$ and generator matrix

$$\begin{bmatrix} 1&0&0&0&0&0&0&0&1&1&0&1&0&0&0\\ 0&1&0&0&0&0&0&0&0&1&1&0&1&0&0\\ 0&0&1&0&0&0&0&0&0&0&1&1&0&1&0\\ 0&0&0&1&0&0&0&0&0&0&0&1&1&0&1\\ 0&0&0&0&1&0&0&0&1&1&0&1&1&1&0\\ 0&0&0&0&0&1&0&0&0&1&1&0&1&1&1\\ 0&0&0&0&0&0&1&0&1&1&1&0&0&1&1\\ 0&0&0&0&0&0&0&1&1&0&1&0&0&0&1 \end{bmatrix} \quad (26)$$

AQEC. We can consider the code C_1 corrects the bit-flip errors such that $C_2^{\perp} \subset C_1$. Furthermore, $C_1^{\perp} \subset C_2$. Furthermore and $d_x = \mathrm{wt}(C_1 \backslash C_2^{\perp}) = 3$ and $d_z = \mathrm{wt}(C_2 \backslash C_1^{\perp}) = 5$. Hence, the quantum code can detect four phase-shift errors and two bit-flip errors, in other words, the code can correct two phase-shift errors and one bit-flip errors. There must exist asymmetric quantum error control codes (AQEC) with parameters $[[n, k_1 + k_2 - n, d_z/d_x]]_2 = [[15, 3, 5/3]]_2$. We ensure that this quantum code encodes three qubits into 15 qubits, and it might also be easy to design a fault tolerant circuit for this code similar to $[[9, 1, 3]]_2$ or $[[7, 1, 3]]_2$, but one can use the cyclotomic structure of this code. We ensure that many other quantum BCH can be constructed using the approach given in this paper that may or may not have better fault tolerant operations and better threshold values.

SSC. We can also construct a subsystem code (SSC) based on the codes C_1 and C_2. First we notice that $C_1^{\perp} = C_2 \cap C_2^{\perp} \neq \emptyset$, $C_2 \subset C_1$ and $C_2^{\perp} \subset C_1$. Let $k = \dim C_1 - \dim C_2 = 4$ and $r = \dim C_2 - \dim C_1^{\perp} = 3$. Furthermore $d = \mathrm{wt}(C_1 \backslash C_2) = 3$. Therefore, there exists a subsystem code with parameters $[[15, 4, 3, 3]]_2$ also an ASSC code with parameters $[[15, 4, 3, 5/3]]_2$.

***Remark** 18:* An $[7, 3, 4]_2$ BCH code is used to derive Steane's code $[[7, 1, 4/3]]_2$. AQEC might not be interesting for Steane's code because it can only detect 3 shift-errors and 2 bit-flip errors, furthermore, the code corrects one bit-flip and one phase-shift at most. Therefore, one needs to design AQEC with d_z much larger than d_x.

One might argue on how to choose the distances d_z and d_x, we think the answer comes from the physical system point of view. The time needed to phase-shift errors is much less that the time needed for qubit-flip errors, hence depending on the factor between them, one can design AQEC with factor a d_z/d_x.

VI. Bounds on Asymmetric QEC and Subsystem Codes

One might wonder whether the known bounds on QEC and SSC parameters would also apply for AQEC and ASSC code parameters. We can show that AQECs and ASSCs obey the asymmetric Singleton bound as follows. In fact we can trade the dimensions of SCC and ASSC in a similar manner as shown in [9], [8].

A. Singleton Bound

[Asymmetric Singleton Bound]

***Theorem** 19:* An $[[n, k, d_z/d_x]]_q$ asymmetric pure quantum code with $k \geq 1$ satisfies $d_x \leq (n - k + 2)/2$, and the bound

$$d_x + d_z \leq (n - k + 2). \quad (27)$$

Proof: From the construction of AQEC, existence of the AQEC with parameters $[[n, k, d_z/d_x]]_q$ implies existence of two codes C_1 and C_2 such that $C_2^{\perp} \subseteq C_1$ and $C_1^{\perp} \subseteq C_2$. furthermore $d_x = \mathrm{wt}(C_1 \backslash C_2^{\perp})$ and $d_z = \mathrm{wt}(C_2 \backslash C_1^{\perp})$. Hence we have $d_x \leq (n - k_1 + 1)$ and $d_z \leq (n - k_2 + 1)$, and by adding these two terms we obtain $d_x + d_z \leq n - (k_1 + k_2 - n) + 2 = n - k + 2$. ■

It is much easy to show that the bound for d_x than the bound for d_z since QEC's with parameters $[[n, k, d_x]]_q$ obey this bound. Also, impure AQECs obey this bound $d_x + d_z \leq (n - k + 2)$. The proof is straight forward to the case QECs and we omit it here.

One can also show that Asymmetric subsystem codes obey the Singleton bound

***Lemma** 20:* Asymmetric subsystem codes with parameters $[[n, k, r, d_z/d_x]]_q$ for $0 \leq r < k$ satisfy

$$k + r \leq n - d_x - d_z + 2. \quad (28)$$

***Remark** 21:* In fact, the AQEC RS codes derived in Section III are optimal and asymmetric MDS codes in a sense that they meet asymmetric Singleton bound with equality. The conclusion is that MDS QECs are also MDS AQEC. Furthermore, MDS SCC are also MDS ASSC.

B. Hamming Bound

Based on the discussion presented in the previous sections, we can treat subsystem code constructions as a special class of asymmetric quantum codes where $C_i^{\perp} \subset C_{1+(i \mod 2)}$, for $i \in \{1, 2\}$ and $C_2 = C_1 \cap C_1^{\perp}$. Furthermore, the more general theory of quantum error control codes would be asymmetric subsystem codes.

***Lemma** 22:* A pure $((n, K, K', d_z/d_x))_q$ asymmetric subsystem code satisfies

$$\sum_{j=0}^{\lfloor \frac{d_x - 1}{2} \rfloor} \binom{n}{j} (q^2 - 1)^j \leq q^n / KK'. \quad (29)$$

Proof: We know that a pure $((n, K, K', d_z/d_x)))_q$ code implies the existence of a pure $((n, KK', d_x))_q$ stabilizer code this is direct by looking at an AQEC as a QEC. But this obeys

the quantum Hamming bound [20], [11]. Therefore it follows that

$$\sum_{j=0}^{\lfloor \frac{d_x-1}{2} \rfloor} \binom{n}{j} (q^2-1)^j \leq q^n/KK'.$$

■

In terms of packing codes, it is easy to show that the impure asymmetric subsystem codes does not obey the quantum Hamming bound. Since the special case does not obey this bound, so why the general case does.

***Lemma** 23:* An impure $((n, K, K', d_z/d_x))_q$ asymmetric subsystem code does not satisfy

$$\sum_{j=0}^{\lfloor \frac{d_x-1}{2} \rfloor} \binom{n}{j} (q^2-1)^j \leq q^n/KK'.$$

It is obvious that the distance of phase-shift would not obey this bound as well, $d_z > d_x$. Finally one can always look at asymmetric quantum codes (AQECs) as a special class of asymmetric subsystem codes (ASSCs). In other words every an $[[n, k, d_z/d_x]]_q$ is also an $[[n, k, 0, d_z/d_x]]_q$, and this is the main contribution of this paper. Also, a SSC with parameters $[[n, k, r, d_x]]_q$ can produce $ASSC$ with parameters $[[n, k, r, d_z/d_x]]_q$. One can also go from ASSCs to AQECs using the results derived in [9], [8]. and Finally an ASSC with parameters $[[n, k, r, d_z/d_x]]_q$ is also an ASSC with parameters $[[n, r, k, d_z/d_x]]_q$. The proof for all these facts is a direct consequence by writing the $\mathbf{F}_q$ bases for the codes AQEC and ASSC.

VII. Conclusion and Discussion

This paper introduced a new theory of asymmetric quantum codes. It establishes a link between asymmetric and symmetric quantum control codes, as well as subsystem codes. Families of AQEC are derived based on RS and BCH codes over finite fields. Furthermore we introduced families of subsystem BCH codes. Tables of AQEC-BCH and CSS-BCH are shown over $\mathbf{F}_q$.

We pose it as open quantum to study the fault tolerance operations of the constructed quantum BCH codes in this paper. Some BCH codes are turned out to be also LDPC codes. Therefore, one can use the same method shown in to construct asymmetric quantum LDPC codes [5].

Acknowledgments.

I thank A. Klappenecker for his support and I think my family, teachers, and colleagues.

Part of this research on SSC and QEC has been done at CS/TAMU in Spring '07 and during a research visit to Bell-Labs & alcatel-Lucent in Summer '07, the generalization to ASSC is a consequence.

Sharing knowledge, in which we all born knowing nothing, is better than proving or canceling it. S.A.A.

VIII. Appendix

A. Quantum BCH Codes

This paper is written on the occasion of the 50th anniversary of the discovery of classical BCH codes and their quantum counterparts were derived nearly 10 years ago. This powerful class of codes has been used for the construction of quantum block and convolutional codes, entangled-assisted quantum convolutional codes, and subsystem codes; in addition to the constructions of classes of low-density parity check (LDPC) codes [12], [10], [4], [6], [43], [44], [17], [7], [9].

References

[1] P. Aliferis. *fault tolerance quantum computing*. PhD thesis, 2007.

[2] P. Aliferis and A. W. Cross. Subsystem fault tolerance with the bacon-shor code. *Physical Review Letters*, 98(220502), 2007. quant-ph/0610063.

[3] P. Aliferis, D. Gottesman, and J. Preskill. *Quant. Inf. Comp.*, 6(97), 2006.

[4] S. A. Aly. *Quantum Error Control Codes*. PhD thesis, Texas A&M University, January 2008.

[5] S. A. Aly. Families of LDPC codes derived from nonprimitive BCH codes and cyclotomic cosets. Technical report, Department of Computer Science, Texas A&M University, January 2008, cs.IT:arXiv:0802.4079.

[6] S. A. Aly. A class of quantum LDPC codes constructed from finite geometries. In *Proc. 2008 IEEE International Symposium on Information Theory*, Toronto, Canada, Submitted 2008. arXiv:quant-ph/0712.4115.

[7] S. A. Aly, M. Grassl, A. Klappenecker, M. Rötteler, and P. K. Sarvepalli. Quantum convolutional BCH codes. In *10th Canadian Workshop on Information Theory, CWIT '07*, pages 180 – 183, June, 6-8 2007.

[8] S. A. Aly and A. Klappenecker. Structures and constructions of subsysem codes over finite fields. *Phys. Rev. A.*, 2008. on submission.

[9] S. A. Aly and A. Klappenecker. Subsysem code constructions. *Proc. 2008 IEEE International Symposium on Information Theory, Toronto, CA*, Submitted. arXiv:quant-ph:0712.4321v2.

[10] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. On quantum and classical BCH codes. *IEEE Trans. Inform. Theory*, 53(3):1183–1188, 2007.

[11] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. Subsystem codes. In *44th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, Illinois, September 2006.

[12] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. Primitive quantum BCH codes over finite fields. In *Proc. 2006 IEEE International Symposium on Information Theory*, pages 1114 – 1118, Seattle, USA, July 2006.

[13] A. E. Ashikhmin and S. Litsyn. Upper bounds on the size of quantum codes. *IEEE Trans. Inform. Theory*, 45(4):1206–1215, 1999.

[14] D. Bacon. Operator quantum error correcting subsystems for self-correcting quantum memories. *Phys. Rev. A.*, 73(012340), 2006.

[15] D. Bacon and A. Casaccino. Quantum error correcting subsystem codes from two classical linear codes. In *Proc. of the 45th Allerton Conference on Communication, Control, and Computing*, Monticello, Illinois, September 2006.

[16] W. Bosma, J.J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comp.*, 24:235–266, 1997.

[17] T. Brun, I. Devetak, and M. Hsieh. Catalytic quantum error correction. 2006. arXiv:quant-ph-0608027v2.

[18] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory*, 44:1369–1387, 1998.

[19] 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.

[20] K. Feng and Z. Ma. A finite Gilbert-Varshamov bound for pure stabilizer quantum codes. *IEEE Trans. Inform. Theory*, 50(12):3323–3325, 2004.

[21] G. D. Forney Jr., M. Grassl, and S. Guha. Convolutional and tail-biting quantum error-correcting codes. *IEEE Trans. Inform. Theory*, 53(3):865–880, 2007.

[22] D. Gottesman. Stabilizer codes and quantum error correction. Caltech Ph. D. dissertation, eprint: quant-ph/9705052, 1997.

[23] M. Grassl and T. Beth. Quantum BCH codes. In *Proc. X. Int'l. Symp. Theoretical Electrical Engineering*, pages 207–212, Magdeburg, 1999.

[24] A. Hocquenghem. Codes correcteurs d'erreurs. *Chiffres*, 2:147–156, 1959.

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

[26] L. Ioffe and M. Marc Mzard. Asymmetric quantum error-correcting codes. *Phys. Rev. A*, 75(032345), 2007.

[27] G. Smith J.A. Smolin and S. Wehner. A simple family of nonadditive quantum codes. 2007.

[28] A. Klappenecker and P.K. Sarvepalli. Clifford code constructions of operator quantum error correcting codes. arXiv:quant-ph/0604161, 2006.

[29] E. Knill. Group representations, error bases and quantum codes. Los Alamos National Laboratory Report LAUR-96-2807, 1996.

[30] E Knill. Fault-tolerant postselected quantum computation: Threshold analysis. *arXiv.org:quant-ph/0404104*, 2004.

[31] E. Knill. On protected realizations of quantum information. eprint: quant-ph/0603252, 2006.

[32] D. W. Kribs, R. Laflamme, and D. Poulin. Unified and generalized approach to quantum error correction. *Phys. Rev. Lett.*, 94(180501), 2005.

[33] D.A. Lidar, I.L. Chuang, and K.B. Whaley. Decoherence-free subspaces for quantum-computation. *Phys. Rev. Letters*, 81:2594–2597, 1998.

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

[35] D. Poulin. Stabilizer formalism for operator quantum error correction. *Phys. Rev. Lett.*, 95(230504), 2005.

[36] D. Poulin, J.-P. Tillich, and H. Ollivier. Quantum serial turbo-codes. *Phys. Rev. A*, 2007.

[37] J. Preskill. Reliable quantum computers. In *Proc. Roy. Soc.*, volume A 454, pages 385–410, 1998.

[38] E.M. Rains. Nonbinary quantum codes. *IEEE Trans. Inform. Theory*, 45(6):1827–1832, 1999.

[39] P. K. Sarvepalli, S. A. Aly, and A. Klappenecker. Nonbinary stabilizer codes. In G. Chen, L. Kauffman, and S. Lomonaco, editors, *The Mathematics of Quantum Computation and Quantum Technology*. Taylor & Francis, 2007.

[40] P. W. Shor. Scheme for reducing decoherence in quantum memory. *Phys. Rev. A*, 2:2493–2496, 1995.

[41] P. W. Shor. Fault-tolerant quantum computation. In *Proc. 37th Ann. Symp. on the Foundations of Computer Science*, page 56, IEEE Computer Society Press, Los Alamitos, CA, 1996. quant-ph/9605011.

[42] A. M. Steane. Multiple-particle interference and quantum error correction. In *Proc. Roy. Soc., London A*, volume 452, pages 2551–2577, 1996.

[43] A. M. Steane. Simple quantum error correcting codes. *Phys. Rev. Lett.*, 77:793–797, 1996.

[44] A. M. Steane. Enlargement of Calderbank-Shor-Steane codes. *IEEE Trans. Inform. Theory*, 45(7):2492–2495, 1999.

[45] A. M. Steane and B. Ibinson. Fault-tolerant logical gate networks for Calderbank-Shor-Steane codes. *Phys. Rev. A.*, 72(052335), 2005.

[46] A. M. Stephens, Z. W. E. Evans, S. J. Devitt, and L. C. L. Hollenberg. Universal quantum computation under asymmetric quantum error correction, 2007.

[47] P. Zanardi and M. Rasetti. Noiseless quantum codes. *Phys. Rev. Lett.*, 79:3306, 1997.