

# Asymmetric and Symmetric Quantum BCH Control 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 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 subsystem codes based on BCH code with parameters  $[[n, k, r, d_z/d_x]]_q$  and  $[[n, k', d_z/d_x]]_q$  for certain values of code lengths and dimensions. We establish bounds on asymmetric quantum and subsystem code parameters. 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 said in his seminal work [100, page 2, col. 2][99], [102] “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 [79], it was said that “BCH codes are among the powerful codes”. We address constructions of quantum codes based on Bose-Chaudhuri-Hocquenghem (BCH) codes over finite fields.

Many quantum error control codes (QEC) have been constructed over the last decade. 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 are proposed including stabilizer block codes, quantum convolutional codes, entangled-assisted quantum error control codes, decoherence free subspaces, nonadditive codes, and subsystem codes; see Section VIII-B for a short historical overview.

Subsystem codes (SSC) as we prefer to call them were mentioned in the unpublished work by Knill [69], [67], 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 [16], [23], [24], [66], [73], [84]. The construction aspects of these codes are given in [13], [12], [16]

Asymmetric quantum control codes, in which quantum errors have different probabilities —  $\Pr Z > \Pr X$ , are more efficient than the symmetric quantum error control codes, in which quantum errors have equal probabilities —  $\Pr Z = \Pr X$ . It is argued in [59] that dephasing (loss of phase coherence, phase-shifting) will happen more frequently than relaxation (exchange of energy with the environment, qubit-flipping). Asymmetric quantum control codes (AQEC) are reintroduced in [37], [59], [104]. 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 [37], [59], [104]. 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 photon takes 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 [5], [23], [24], [103], [104], [3] and references therein. Fault-tolerant operations of QEC are investigated for example in [5], [44], [87], [98], [103], [68], [2] and references therein.

The codes derived in [14], [18] 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 [31], [97]. We aim to generalize these codes over asymmetric quantum channels. In this paper we give a family of asymmetric quantum error control codes motivated by the work from [37], [59]. 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 distance  $d_i$  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.

**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  $d_x = \min \{ \text{wt}(C_1 \setminus C_2^\perp), \text{wt}(C_2 \setminus C_1^\perp) \}$ , and  $d_z = \max \{ \text{wt}(C_1 \setminus C_2^\perp), \text{wt}(C_2 \setminus C_1^\perp) \}$ .

- i) if  $C_1^\perp \subset C_2$  and  $C_2^\perp \subset C_1$ , then there is asymmetric quantum stabilizer code with parameters  $[[n, \dim C_1 - \dim C_2^\perp, \text{wt}(C_2 \setminus C_1^\perp) / \text{wt}(C_1 \setminus C_2^\perp)]]_q$  that is  $[[n, k_1 + k_2 - n, d_z/d_x]]_q$ .
- ii) From [i], there exists a subsystem code (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  $C_2^\perp \subset C_2$  and  $C_2^\perp = C_1 \cap C_1^\perp$ , then there exist asymmetric subsystem codes (ASSC) with parameters  $[[n, k_2 - k_1, k_1 + k_2 - n, d_z/d_x]]_q$  and  $[[n, k_1 + k_2 - n, k_2 - k_1, d_z/d_x]]_q$ .

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 and 4 qubit-flip and phase-shift errors, respectively. As a result, many of the quantum constructed codes and families of QEC for large lengths need further investigations.

The paper is organized as follows. In Section VIII-B, we give an overview of QEC constructions and a short historical highlight on the previous work. 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. Finally, the paper is concluded with a discussion in Section VII.

## II. ASYMMETRIC QUANTUM CODES

Consider a quantum system with two-dimensional state space  $\mathcal{C}^2$ . The basis vectors

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

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

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

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.

$$X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (2)$$

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

$$Z(a|0\rangle + b|1\rangle) = a|0\rangle - b|1\rangle. \quad (3)$$

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

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (4)$$

**Connection to Classical 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

$$H_1.H_2^T + H_2.H_1^T = 0. \quad (5)$$

The stabilizer of the code is given by

$$H_{stab} = (H_1 | H_2). \quad (6)$$

One of these two classical codes controls the phase flip error, 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 codes  $C_1$  and  $C_2$  such that  $C_2^\perp \subset C_1$ . If we form

$$G = \begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}, \quad \text{and } H = \begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix}, \quad (7)$$

then

$$H_1.H_2^T - H_2.H_1^T = 0 \quad (8)$$

Let  $d_1 = \text{wt}(C_1 \setminus C_2)$  and  $d_2 = \text{wt}(C_2 \setminus C_1^\perp)$ , 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

$$[[n, k_1 + k_2 - n, d_2/d_1]]_2. \quad (9)$$

### A. Higher Fields and Total Error Groups

In terms of higher finite fields  $\mathbf{F}_q$ . Let  $\mathcal{H}$  be the Hilbert space  $\mathcal{H} = \mathcal{C}^{q^n} = \mathcal{C}^q \otimes \mathcal{C}^q \otimes \dots \otimes \mathcal{C}^q$ . 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:

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

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

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

$$X(\mathbf{a}) = X(a_1) \otimes \dots \otimes X(a_n) \text{ and ,}$$

$$Z(\mathbf{b}) = Z(b_1) \otimes \dots \otimes Z(b_n)$$

the tensor products of  $n$  error operators. The sets

$$\mathbf{E}_x = \{Z(\mathbf{b}) = \bigotimes_{i=1}^n X(a_i) \mid \mathbf{a} \in \mathbf{F}_q^n, a_i \in \mathbf{F}_q\}, \quad (11)$$

$$\mathbf{E}_z = \{Z(\mathbf{b}) = \bigotimes_{i=1}^n Z(b_i) \mid \mathbf{b} \in \mathbf{F}_q^n, b_i \in \mathbf{F}_q\} \quad (12)$$

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

$$\mathbf{G}_x = \{\omega^c \mathbf{E}_x = \omega^c X(\mathbf{a}) \mid \mathbf{a} \in \mathbf{F}_q^n, c \in \mathbf{F}_p\}, \quad (13)$$

$$\mathbf{G}_z = \{\omega^c \mathbf{E}_z = \omega^c Z(\mathbf{b}) \mid \mathbf{b} \in \mathbf{F}_q^n, c \in \mathbf{F}_p\}. \quad (14)$$

Hence the total error group

$$\begin{aligned} G &= \{\mathbf{G}_x, \mathbf{G}_z\} \\ &= \left\{ \omega^c \bigotimes_{i=1}^n X(a_i), \omega^c \bigotimes_{i=1}^n Z(b_i) \mid a_i, b_i \in \mathbf{F}_q \right\} \end{aligned} \quad (15)$$

Many constructed quantum codes assume that the quantum errors resulted from decoherence and noise have equal probabilities,  $\Pr X = \Pr Z$ . We show a family of asymmetric quantum error control codes that differentiate between these two kinds of errors  $\Pr Z > \Pr X$ .

**Definition 3:** 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  $\mathcal{C}^{q^n}$  and can control all bit-flip errors up to  $\lfloor \frac{d_x-1}{2} \rfloor$  and all phase-flip errors up to  $\lfloor \frac{d_z-1}{2} \rfloor$ .

We use different notation from the one given in [37]. 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  $\rho$  and dimension  $k$  of the quantum code.

**Connection to Classical 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  $H_i$  is  $k_i$ . If  $C_i^\perp \subset C_{1+(i \bmod 2)}$ , then  $C_{1+(i \bmod 2)}^\perp \subset C_i$ . So, the rows of  $H_i$  which form a basis for  $C_i^\perp$  can be

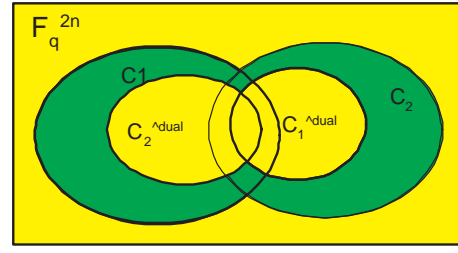


Fig. 1. Constructions of asymmetric quantum codes based on two classical codes  $C_1$  and  $C_2$ . AQEC has parameters  $[[n, k_1 + k_2 - n, d_z/d_x]]_q$

extended to form a basis for  $C_{1+(i \bmod 2)}$  by adding some vectors. Also, if  $g_i(x)$  is the generator polynomial of a cyclic code  $C_i$  then  $k_i = n - \deg(g_i(x))$ .

The error groups  $\mathbf{G}_z$  and  $\mathbf{G}_x$  can be mapped, respectively, to two classical codes  $C_1$  and  $C_2$  in a similar manner as in QEC. This connection is well-known, see for example [31], [88], [92]. Let  $C_i$  be a classical code such that  $C_{1+(i \bmod 2)}^\perp \subset C_i$  for  $i \in \{1, 2\}$ , then we have a symmetric quantum control code 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  $C_i^\perp \subset C_{1+(i \bmod 2)}$  for  $i \in \{1, 2\}$ , and  $d_x = \min\{\text{wt}(C_1 \setminus C_2^\perp), \text{wt}(C_2 \setminus C_1^\perp)\}$ , and  $d_z = \max\{\text{wt}(C_1 \setminus C_2^\perp), \text{wt}(C_2 \setminus C_1^\perp)\}$ . Then there is asymmetric quantum code with parameters  $[[n, k_1 + k_2 - n, d_z/d_x]]_q$ .

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

We keep the definitions of BCH codes to a minimal since they have been well-known, see of example [14] or any textbook on classical coding theory [79], [58], [55]. 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

$$S_x = \{xq^i \bmod n \mid i \in \mathbf{Z}, i \geq 0\}. \quad (16)$$

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

$$g(x) = \prod_{i=1}^{\delta-1} (x - \alpha^i). \quad (17)$$

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

be defined as

$$H_{bch} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{\delta-1} & \alpha^{2(\delta-1)} & \dots & \alpha^{(\delta-1)(n-1)} \end{bmatrix}. \quad (18)$$

In fact, we show the dimension of nonprimitive BCH codes over  $\mathbf{F}_q$ .

**Theorem 6 (Dimension BCH Codes):** Let  $q$  be a prime power and  $\gcd(n, q) = 1$ , with  $\text{ord}_n(q) = m$ . 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  $\delta$  in the range  $2 \leq \delta \leq \delta_{\max} = \min\{\lfloor nq^{\lfloor m/2 \rfloor} / (q^m - 1) \rfloor, n\}$ , has dimension of

$$k = n - m\lceil(\delta - 1)(1 - 1/q)\rceil. \quad (19)$$

*Proof:* See [14, Theorem 10]. ■

In [18], [14], 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 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.

**Theorem 7:** Let  $m = \text{ord}_n(q)$  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

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

then there exists a quantum code with parameters

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

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

### A. AQEC-BCH

Fortunately, the mathematical structure of BCH codes always us easily to show the nest 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  $\alpha^2, \alpha^3, \dots, \alpha^{\delta-1}$  over  $\mathbf{F}_q$ . We know that the generator polynomial has degree  $m\lceil(1 - 1/\delta)\rceil$  if  $\delta \leq \delta_{\max}$ . Therefore the dimension is given by  $k = n - \text{deg}(g(x))$ . Hence, the nested structure of BCH codes is obvious and can be described as follows. Let

$$\delta_{i+1} > \delta_i > \delta_{i-1} \geq \dots \geq 2, \quad (20)$$

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

$$C_{i+1} \subset C_i \subset C_{i-1} \subset \dots \quad (21)$$

We need to ensure that  $\delta_i$  and  $\delta_{i+1}$  away of each other, so the elements (roots)  $2, \dots, \delta_i - 1$  and  $2, \dots, \delta_{i+1} - 1$  are different. This means that the cyclotomic cosets generated by  $\delta_i$  and  $\delta_{i+1}$  are not the same,  $S_1 \cup \dots \cup S_{\delta_i-1} \neq S_1 \cup \dots \cup S_{\delta_{i+1}-1}$ . 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:** Let  $q$  be a prime power and  $\gcd(n, q) = 1$ , with  $\text{ord}_n(q) = m$ . 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  $\delta_1$  and  $\delta_2$  in the range  $2 \leq \delta_1, \delta_2 \leq \delta_{\max} = \min\{\lfloor nq^{\lfloor m/2 \rfloor} / (q^m - 1) \rfloor, n\}$  and  $\delta_1 < \delta_2^\perp \leq \delta_2 < \delta_1^\perp$ .

Assume  $S_1 \cup \dots \cup S_{\delta_1-1} \neq S_1 \cup \dots \cup S_{\delta_2-1}$ , then there exists an asymmetric quantum error control code with parameters  $[[n, n - m\lceil(\delta_1 - 1)(1 - 1/q)\rceil - m\lceil(\delta_2 - 1)(1 - 1/q)\rceil, \geq d_z/d_x]]_q$ , where  $d_z = \text{wt}(C_2 \setminus C_1^\perp) > d_x = \text{wt}(C_1 \setminus C_2^\perp)$ .

*Proof:* From the nest structure of BCH codes, we know that if  $\delta_1 < \delta_2^\perp$ , then  $C_2^\perp \subset C_1$ , similarly if  $\delta_2 < \delta_1^\perp$ , then  $C_1^\perp \subset C_2$ . By Lemma 6, we have  $k_i = n - m\lceil(\delta_i - 1)(1 - 1/q)\rceil$  for  $i = \{1, 2\}$ . Since  $S_1 \cup \dots \cup S_{\delta_1-1} \neq S_1 \cup \dots \cup S_{\delta_2-1}$ , this means that  $\text{deg}(g_1(x)) < \text{deg}(g_2(x))$ , hence  $k_2 < k_1$ . Furthermore  $k_1^\perp < k_2^\perp$ .

By Lemma 4 and we assume  $d_x = \text{wt}(C_1 \setminus C_2^\perp) \geq \delta_1$  and  $d_z = \text{wt}(C_2 \setminus C_1^\perp) \geq \delta_2$  such that  $d_z > d_x$  otherwise we exchange the rules of  $d_z$  and  $d_x$ . Therefore, there exists AQEC with parameters  $[[n, k_1 + k_2 - n, \geq d_z/d_x]]_q$ . ■

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.

The condition regarding the designed distances  $\delta_1$  and  $\delta_2$  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  $n = q^m - 1$  for some integers  $m$ . 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  $S_1 \cup \dots \cup S_{\delta_1-1} \neq S_1 \cup \dots \cup S_{\delta_2-1}$ , then there exists an asymmetric quantum error control code with parameters  $[[n, k_1 + k_2 - n, \geq d_z/d_x]]_q$ , where  $d_z = \text{wt}(C_1 \setminus C_2^\perp) = \delta_2 > d_x = \text{wt}(C_2 \setminus C_1^\perp) = \delta_1$ .

In fact the previous theorem can be used to derive any asymmetric cyclic quantum control codes. We can also show it for RS codes as an example.

### B. RS Codes

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

$$g(x) = \prod_{i=1}^{d-1} (x - \alpha^i). \quad (22)$$

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  $d_1 < d_2 < d_1^\perp$ . Then there exists AQEC code with parameters  $[[n, n - d_1 - d_1 + 2, d_z/d_x]]_q$ , where  $d_x = d_1 < d_z = d_2$ .

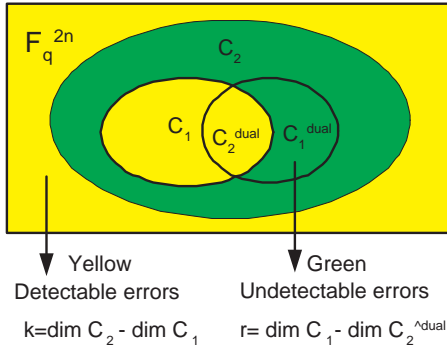


Fig. 2. A quantum code  $Q$  is decomposed into two subsystem  $A$  (info) and  $B$  (gauge)

*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  $d_z = \text{wt}(C_2 \setminus C_1^\perp) = d_2$  and  $d_x = \text{wt}(C_1 \setminus C_2^\perp) = d_1$ . Therefore there must exist AQEC with parameters  $[[n, n - d_1 - d_1 + 2, d_z/d_x]]_q$ . ■

One can also derive asymmetric quantum RS codes based on RS codes over  $\mathbb{F}_{q^2}$ .

TABLE I  
FAMILIES OF ASYMMETRIC QUANTUM BCH CODES [26]

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]	$[[31, 11, 7/3]]_2$
2	[31, 26, 3]	[31, 16, 7]	$[[31, 10, 8/3]]_2$
2	[31, 26, 3]	[31, 11, 11]	$[[31, 6, 11/3]]_2$
2	[31, 26, 3]	[31, 6, 15]	$[[31, 1, 15/3]]_2$
2	[127, 113, 5]	[127, 78, 15]	$[[127, 64, 15/5]]_2$
2	[127, 106, 7]	[127, 77, 27]	$[[127, 56, 25/7]]_2$

#### IV. AQEC AND CONNECTION WITH SUBSYSTEM CODES

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  $QA \otimes B$ , see Fig.2, as follows

**Definition 11:** 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  $\mathbb{F}_q$  and  $\mathbb{F}_{q^2}$ . Such codes do not need the classical codes to be self-orthogonal (or dual-containing) as shown in the following theorem.

We gave general constructions of subsystem codes in [16] known as CSS and Hermitian Constructions. We provide a proof for the following special case of our previous constructions.

**Lemma 12 (SSC Euclidean Construction):** If  $C$  is a  $k'$ -dimensional  $\mathbb{F}_q$ -linear code of length  $n$  that has a  $k''$ -dimensional subcode  $D = C \cap C^\perp$  and  $k' + k'' < n$ , then there exists an

$$[[n, n - (k' + k''), k' - k'', \text{wt}(D^\perp \setminus C)]]_q$$

subsystem code.

*Proof:* Let us define the code  $X = C \times C \subseteq \mathbb{F}_q^{2n}$ , therefore  $X^{\perp_s} = (C \times C)^{\perp_s} = C^{\perp_s} \times C^{\perp_s}$ . Hence  $Y = X \cap X^{\perp_s} = (C \times C) \cap (C^{\perp_s} \times C^{\perp_s}) = D \times D$ . Thus,  $\dim_{\mathbb{F}_q} Y = 2k''$ . Hence  $|X||Y| = q^{2(k'+k'')}$  and  $|X|/|Y| = q^{2(k'-k'')}$ . By Theorem [16, 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)  $d = \text{swt}(Y^{\perp_s} \setminus X) = \text{wt}(D^\perp \setminus C)$ .

Subsystem codes require the code  $D$  to be self-orthogonal,  $D \subseteq D^\perp$ . From this result, we can see that any two classical codes, in which they can be used to construct a subsystem code, can be also used to construct AQEC. AQEC subsystem codes are much larger class of subsystem codes. AQEC does not require the intersection code to be self-orthogonal.

We have shown in [13], [8] that All stabilizer codes (pure and impure) can be reduced to subsystem codes as shown in the following result.

**Theorem 13:** Let  $q$  be a power of a prime  $p$ . If there exists an  $\mathbb{F}_q$ -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  $\mathbb{F}_q$ -linear  $[[n, k - 1, r + 1, \geq d]]_q$  subsystem code that is pure to  $\min\{d, d'\}$ . If a pure ( $\mathbb{F}_q$ -linear)  $[[n, k, r, d]]_q$  subsystem code exists, then a pure ( $\mathbb{F}_q$ -linear)  $[[n, k + r, d]]_q$  stabilizer code exists.

We have shown in [14], [18] that narrow sense BCH codes, primitive and non-primitive, with length  $n$  and designed distance  $\delta$  are Euclidean dual-containing codes if and only if  $2 \leq \delta \leq \delta_{\max} = \frac{n}{q^m - 1} (q^{\lceil m/2 \rceil} - 1 - (q - 2)[m \text{ odd}])$ . We use this result and [13, Theorem 2] to derive primitive subsystem BCH codes from classical BCH codes over  $\mathbb{F}_q$  and  $\mathbb{F}_{q^2}$  [16], [18].

For simplicity, we will proceed our work for primitive narrow sense BCH codes, however, the generalization for non-primitive BCH codes is a straightforward.

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

*Proof:* We know that if  $2 \leq \delta \leq q^{\lceil m/2 \rceil} - 1 - (q - 2)[m \text{ odd}]$ , then there exists a stabilizer code with parameters  $[[q^m - 1, n - 2m \lceil (\delta - 1)(1 - 1/q) \rceil, \geq \delta]]_q$ . Let  $r$  be an integer in the range  $0 \leq r < n - 2m \lceil (\delta - 1)(1 - 1/q) \rceil$ . From [13, Theorem 2], then there must exist a subsystem BCH code with parameters  $[[q^m - 1, n - 2m \lceil (\delta - 1)(1 - 1/q) \rceil - r, r, \geq \delta]]_q$ . ■

We can also construct subsystem BCH codes from stabilizer codes using the Hermitian constructions.

**Lemma 15:** If  $q$  is a power of a prime,  $m$  is a positive integer, and  $\delta$  is an integer in the range  $2 \leq \delta \leq \delta_{\max} = q^{m+[m \text{ even}]} - 1 - (q^2 - 2)[m \text{ even}]$ , then there exists a subsystem code  $Q$  with parameters

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

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

*Proof:* If  $2 \leq \delta \leq \delta_{\max} = q^{m+[m \text{ even}]} - 1 - (q^2 - 2)[m \text{ even}]$ , then exists a classical BCH code with parameters  $[q^m - 1, q^m - 1 - m\lceil(\delta - 1)(1 - 1/q)\rceil, \geq \delta]_q$  which contains its dual code. From [13, Theorem 2], then there must exist a subsystem code with the given parameters. ■

If fact we can look at subsystem codes as asymmetric quantum control codes, by just omitting the self-orthogonality condition of the code  $D = C \cap C^\perp$ . This is obviously not a necessary condition on AQEC construction.

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

In [12] we give a method to derive subsystem codes from classical BCH codes directly as shown in the following results.

**Lemma 16:** If  $q$  is a power of a prime,  $m$  is a positive integer, and  $2 \leq \delta \leq q^{\lceil m/2 \rceil} - 1 - (q - 2)[m \text{ odd}]$ . Let  $D$  be a BCH code with length  $n = q^m - 1$  and defining set  $T_D = \{C_0, C_1, \dots, C_{n-\delta}\}$ , such that  $\gcd(n, q) = 1$ . Let  $T \subseteq \{0\} \cup \{C_\delta, \dots, C_{n-\delta}\}$  be a nonempty set. Assume  $C \subseteq \mathbf{F}_q^n$  be a BCH code with the defining set  $T_C = \{C_0, C_1, \dots, C_{n-\delta}\} \setminus (T \cup T^{-1})$  where  $T^{-1} = \{-t \bmod n \mid t \in T\}$ . Then there exists a subsystem BCH code with the parameters  $[[n, n - 2k - r, r, \geq \delta]]_q$ , where  $k = m\lceil(\delta - 1)(1 - 1/q)\rceil$  and  $r = |T \cup T^{-1}|$ .

*Proof:* See [12]. ■

## 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  $d_x = \text{wt}(C_1 \setminus C_2^\perp) = 3$  and  $d_z = \text{wt}(C_2 \setminus C_1^\perp) = 5$ . 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 the quantum codes encoded three qubits into 15 qubits, which is superior than the code  $[[9, 1, 3]]_2$  or  $[[7, 1, 3]]_2$ . We leave it as open issue to design a fault tolerant circuit for this code. We ensure that many other quantum BCH can be constructed using the approach given in this paper.

**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  $d = \text{wt}(C_1 \setminus C_2) = 3$ . Therefore, there exists a subsystem code with parameters  $[[15, 4, 3, 3]]_2$ .

**Remark 17:** Comparing with the Steane code  $[[7, 1, 4/3]]_2$ , AQEC might not be interesting because it can detect 3 shift-errors and detect 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 than 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 parameters would also apply for AQEC parameters. We can show that AQECs obey the Singleton bound.

### A. Singleton Bound

**Theorem 18:** 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  $C_2^\perp \subset C_1$  and  $C_1^\perp \subset C_2$ . furthermore  $d_x = C_1 \setminus C_2^\perp$  and  $d_z = C_2 \setminus C_1^\perp$ . 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.

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

**Lemma 19:** Asymmetric subsystem codes with parameters  $[[n, k, r, d_z/d_x]]_q$  for  $0 \leq r < k$  satisfy

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

### 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  $C_i^\perp \subset C_{1+(i \bmod 2)}$ , for  $i \in \{1, 2\}$  and  $C_2 = C_1 \cap C_1^\perp$ . Furthermore, the more general theory of QEC would be asymmetric quantum codes.

**Lemma 20:** 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. But this obeys the quantum Hamming bound [40]. Therefore it follows that

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

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 21:** 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,  $d_z > d_x$ .

## 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 codes. 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 [8].

## ACKNOWLEDGMENTS.

I thank Andreas 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. ©.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.

- i) The first work to utilize classical BCH codes in quantum codes was done by Steane in [100], [102], in which a class of binary quantum BCH codes is derived using the CSS construction.
- ii) In [48], a family of quantum BCH codes is shown and tables of the best known codes.
- iii) In [18], [14], two families of quantum BCH codes are given using the Euclidean and Hermitian constructions of BCH codes. Furthermore, formulas of the explicit dimensions and bounds on the minimum distance of these codes are proved for designed distance  $\delta \leq \delta_{\max}$
- iv) In [11], two families of quantum convolutional codes are driven using the stabilizer convolutional constructions. It is proved that these codes have non-catastrophic encoders.
- v) In [28], families of entangled-assisted quantum codes are derived using the primitive BCH codes.
- vi) In [13], [12], two classes of subsystem BCH codes are constructed using the defining sets of nonprimitive BCH codes.
- vii) In this paper, we give a family of asymmetric quantum BCH codes over finite fields.

### B. Symmetric Quantum Code Constructions

The first quantum code was introduced by Shor as an impure quantum code with parameters  $[[9, 1, 3]]_2$  in a landmark paper in 1995 [97]. The second code with parameters  $[[7, 1, 3]]_2$  was introduced by Steane [100], [99]. The idea was to protect one qubit against qubit-flip and phase-shift errors into nine or seven qubits for quantum channels that treat errors with equal probabilities. Calderbank and Shor extended the theory to codes over  $\mathbb{F}_4$  and introduced the CSS construction independently with Steane [25], [31], [32], [100]. Shortly, the stabilizer codes, quantum encoding circuits, and fault-tolerant quantum computing (FTCE) were introduced in [36], [71], [43], [44], [74], [87], [88], [98], [101]. The quantum code  $Q$  can be defined as follows.

**Definition 22 (Symmetric Channel QEC):** A  $q$ -ary quantum control code  $Q$ , denoted by  $[[n, k, d]]_q$ , over symmetric quantum channel is a  $q^k$  dimensional subspace of the Hilbert space  $\mathbb{C}^{q^n}$  and can correct all errors up to  $\lfloor \frac{d-1}{2} \rfloor$  and detect  $d-1$  errors.

The code  $Q$  is able to encode  $k$  logical qubits into  $n$  physical qubits with a minimum distance of at least  $d$  between any two codewords. The  $Q$  can be constructed based on two classical codes  $C_1$  and  $C_2$  such that  $C_2^\perp \leq C_1$  as follows.

**Fact 23 (CSS Code Construction):** Let  $C_1$  and  $C_2$  denote two classical linear codes with parameters  $[n, k_1, d_1]_q$  and  $[n, k_2, d_2]_q$  such that  $C_2^\perp \leq C_1$ . Then there exists a  $[[n, k_1 + k_2 - n, d]]_q$  stabilizer code with minimum distance  $d = \min\{\text{wt}(c) \mid c \in (C_1 \setminus C_2^\perp) \cup (C_2 \setminus C_1^\perp)\} \geq \min\{d_1, d_2\}$ .

Constructing a quantum code  $Q$  reduces to constructing a self-orthogonal (or dual-containing) classical code  $C$  defined over  $\mathbb{F}_q$  or  $\mathbb{F}_{q^2}$  as follows.

**Fact 24:** If there exists an  $\mathbb{F}_q$ -linear  $[n, k, d]_q$  classical code  $C$  containing its dual,  $C^\perp \subseteq C$ , then there exists an  $[[n, 2k - n, \geq d]]_q$  quantum stabilizer code that is pure to  $d$ .

**Fact 25:** If there exists an  $\mathbb{F}_{q^2}$ -linear  $[n, k, d]_{q^2}$  classical code  $C$  such that  $C^{\perp_h} \subseteq C$ , then there exists an  $[[n, 2k - n, \geq d]]_q$  quantum stabilizer code that is pure to  $d$ .

One can construct convolutional stabilizer codes from self-orthogonal (or dual-containing) classical convolutional codes over  $\mathbb{F}_q$  (cf. [17, Corollary 6]) and  $\mathbb{F}_{q^2}$  (see [17, Theorem 5]) as stated in the following theorem.

**Fact 26 (QCC construction):** An  $[(n, k, nm; \nu, d_f)]_q$  convolutional stabilizer code exists if and only if there exists an  $(n, (n-k)/2, m; \nu)_q$  convolutional code such that  $C \leq C^\perp$  where the dimension of  $C^\perp$  is given by  $(n+k)/2$  and  $d_f = \text{wt}(C^\perp \setminus C)$ .

We will take a quick short review for the most known quantum paradigms. The construction aspects of quantum control codes for symmetric quantum channels can be classified briefly as follows <sup>1</sup>

#### i) Stabilizer code constructions (QEC):

Quantum codes appeared in a series of papers in mid '90 [32], [30], [70], [35]. There have been many families of stabilizer codes based on binary classical codes, see [25], [31], [80], [46], [47], [48], [63], [88], [95], [102], [53]. These classes of codes are derived from BCH, RS, LDPC, algebraic geometry codes in addition to codes over graphs. The theory has been generalized to finite fields, see [21], [38], [34], [39], [45], [64], [88], [89], [94], [27], [106]. Recently, bounds, encoding circuits, and new families have been investigated, see [18], [14], [15], [6], [20], [22], [40], [53], [38], [76], [62], [89], [93], [92]. The literature is rich with many other quantum code constructions, the reader might look into the references for further families. These classes of codes are mainly additive codes.

#### ii) Subsystem codes (SSC):

Subsystem codes are a generalization of the theory of quantum error correction and decoherence free subspaces. For a group representation of operator quantum codes, see [66], [69], [84]. For subsystem code constructions, see [7], [13], [16], [23], [24] and references therein.

#### iii) Quantum convolutional code constructions (QCC):

The theory of online encoding and decoding is developed according to the block stabilizer codes. There have not been many bounds on QCC code parameters except the Singleton bounds shown in [17]. The work on QCC developed mainly for symmetric quantum channels. There have been examples of quantum convolutional codes in the literature; the most notable being are [83], [81], [82], [42], [41], [50], families of QCC are derived in [17], [11], [7], [51], and the decoding aspects of these codes are shown [86], [85], [52].

#### iv) Entangled-assisted QEC and QCC:

Some progress in this theory and constructing quantum codes using entanglement are shown in [56], [28], [105], [29], [25], [72].

#### v) Decoherence free spaces:

The features of decoherence free subspaces [77], noiseless

<sup>1</sup>This is from a computer science and EE prospective. We do not consider the physical phenomena behind these constructions.

subsystems [107] are that they aim to correct passive errors, see [77], [96], [1].

vi) **Progress in quantum LDPC codes:**

Modern coding theory including all varieties of Low-density Parity Check (LDPC) codes have been also used to construct quantum codes. Quantum LDPC codes have been constructed using random and algebraic constructions including quantum LDPC derived from finite geometries, BCH, RM codes [10], [8], [9], [78], [54], [33], [57].

vii) **Nonadditive codes.** The recent progress in nonadditive quantum code constructions is shown in [60], [49], [91], [75], [19], [71], [90]. There have not been many families QEC in this direction.

viii) **Fault tolerant quantum computing:**

The research directions in fault tolerant quantum computing promise to speed up the process of building quantum computers under a certain threshold value, known as threshold theorem, see for example [2], [5], [68], [103], [23], [65], [61], [73], [45], [87], [45], [103], [4], [3], and references therein.

This was a quick overview of the quantum code constructions and their encoding and decoding aspects over symmetric quantum channels. Asymmetric quantum code constructions are recently shown in [37], [104] and the early code constructions by Steane [100], [99]. The rest of this paper is devoted for subsystem code and asymmetric quantum codes.

## REFERENCES

- [1] *Decoherence Free Subspaces and Subsystems*, volume 622 of *Lecture Notes in Physics*, Berlin, 2003. Springer. eprint quant-ph/0301032.
- [2] D. Aharonov and M. Ben-Or. Fault tolerant computation with constant error. In *Proc. of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing (STOC97)*, pages 176–188, 1997.
- [3] P. Aliferis. *fault tolerance quantum computing*. PhD thesis, 2007.
- [4] P. Aliferis and A. W. Cross. Subsystem fault tolerance with the bacon-shor code. *Physical Review Letters*, 98(220502), 2007. quant-ph/0610063.
- [5] P. Aliferis, D. Gottesman, and J. Preskill. *Quant. Inf. Comp.*, 6(97), 2006.
- [6] S. A. Aly. A note on quantum hamming bound. *Technical Report, Department of Computer Science, Texas A&M University*, November 2007. arXiv:quant-ph/0711.4603.
- [7] S. A. Aly. *Quantum Error Control Codes*. PhD thesis, Texas A&M University, January 2008.
- [8] 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.
- [9] S. A. Aly. Families of quantum LDPC codes derived from Latin squares and combinatorial design. Technical report, Department of Computer Science, Texas A&M University, January 2008, cs.IT:arXiv:0802.4079.
- [10] 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.
- [11] 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.
- [12] S. A. Aly and A. Klappenecker. Structures and constructions of subsystem codes over finite fields. *Phys. Rev. A*, 2008. on submission.
- [13] S. A. Aly and A. Klappenecker. Subsystem code constructions. *Proc. 2008 IEEE International Symposium on Information Theory, Toronto, CA*, Submitted. arXiv:quant-ph:0712.4321v2.
- [14] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. On quantum and classical BCH codes. *IEEE Trans. Inform. Theory*, 53(3):1183–1188, 2007.
- [15] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. Remarkable degenerate quantum stabilizer codes derived from duadic codes. *Proc. 2006 IEEE International Symposium on Information Theory, Seattle, USA*, pages 1105–1108, July 2006.
- [16] 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.
- [17] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. Quantum convolutional codes derived from Reed-Solomon and Reed-Muller codes. In *Proc. 2007 IEEE International Symposium on Information Theory*, pages 821–825, June Nice, France, 2007. quant-ph/0701037v1.
- [18] 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.
- [19] V. Arvind, P. P. Kurur, and K. R. Parthasarathy. Nonstabilizer quantum codes from abelian subgroups of the error group. *Quantum Physics e-prints*, 2002. quant-ph/0210097.
- [20] A. E. Ashikhmin, A. M. Barg, E. Knill, and S. N. Litsyn. Quantum error detection II: Bounds. *IEEE Trans. Inform. Theory*, 46(3):789–800, 2000.
- [21] A. E. Ashikhmin and E. Knill. Nonbinary quantum stabilizer codes. *IEEE Trans. Inform. Theory*, 47(7):3065–3072, 2001.
- [22] A. E. Ashikhmin and S. Litsyn. Upper bounds on the size of quantum codes. *IEEE Trans. Inform. Theory*, 45(4):1206–1215, 1999.
- [23] D. Bacon. Operator quantum error correcting subsystems for self-correcting quantum memories. *Phys. Rev. A*, 73(012340), 2006.
- [24] 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.
- [25] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed state entanglement and quantum error correction. *Physical Review A*, 54:3824–3851, 1996.
- [26] W. Bosma, J.J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comp.*, 24:235–266, 1997.
- [27] S. B. Bravyi and A. Y. Kitaev. Quantum codes on a lattice with boundary. quant-ph/9810052, 1998.
- [28] T. Brun, I. Devetak, and M. Hsieh. Catalytic quantum error correction. 2006. arXiv:quant-ph-0608027v2.
- [29] T. Brun, I. Devetak, and M. Hsieh. Correcting quantum errors with entanglement. *Science*, 314(5798):436–439, 2006.
- [30] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 78(405), 19967.
- [31] 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.
- [32] A.R. Calderbank and P. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, 1996.
- [33] T. Camara, H. Ollivier, and J. P. Tillich. Constructions and performance of classes of quantum LDPC codes. 2005. quant-ph/00000.
- [34] H. Chen. Some good quantum error-correcting codes from algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 47, 2001.
- [35] R. Cleve. Quantum stabilizer codes and classical linear codes. *Phys. Rev. A*, 55(6):4054–4059, 1997.
- [36] R. Cleve and D. Gottesman. Efficient computations of encodings for quantum error correction. *Phys. Rev. A*, 56(1):76–82, 1997.
- [37] 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.
- [38] K. Feng. Quantum codes  $[[6, 2, 3]]_p$ ,  $[[7, 3, 3]]_p$  ( $p \geq 3$ ) exist. *IEEE Trans. Inform. Theory*, 48(8):2384–2391, 2002.
- [39] K. Feng. Quantum error-correcting codes. In *Coding Theory and Cryptology*, pages 91–142. Hackensack, NJ: World Scientific, 2002.
- [40] K. Feng and Z. Ma. A finite Gilbert-Varshamov bound for pure stabilizer quantum codes. *IEEE Trans. Inform. Theory*, 50(12):3323–3325, 2004.
- [41] 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.
- [42] G. D. Forney Jr. and S. Guha. Simple rate-1/3 convolutional and tail-biting quantum error-correcting codes. In *Proc. of 2005 IEEE Intl. Symposium on Information Theory*, pages 1028–1032, Adelaide, Australia, 2005.
- [43] D. Gottesman. A class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A*, 54:1862–1868, 1996.

- [44] D. Gottesman. Stabilizer codes and quantum error correction. Caltech Ph. D. dissertation, eprint: quant-ph/9705052, 1997.
- [45] D. Gottesman. Fault-tolerant quantum computation with higher-dimensional systems. *Chaos, Solitons, Fractals*, 10(10):1749–1758, 1999.
- [46] M. Grassl and T. Beth. Cyclic quantum error-correcting codes and quantum shift registers. In *Proc. Royal Soc. London Series A*, volume 456, pages 2689–2706, 2000.
- [47] M. Grassl and T. Beth. Quantum BCH codes. In *Proc. X. Int'l. Symp. Theoretical Electrical Engineering*, pages 207–212, Magdeburg, 1999.
- [48] M. Grassl, W. Geiselmann, and T. Beth. Quantum Reed-Solomon codes. In *Applied Algebra, Algebraic Algorithms and Error-correcting Codes*, volume 1719 of *Honolulu, HI, Lecture Notes in Comput. Sci.*, pages 231–244. Springer, Berlin, 1999.
- [49] M. Grassl and M. Rötteler. Algorithmic aspects of error-correcting codes. In R. Brylinski and G. Chen, editors, *Proc. of the Mathematics of Quantum Computing*, pages 223–252. Boca Raton, FL: CRC Press, 2001.
- [50] M. Grassl and M. Rötteler. Quantum block and convolutional codes from self-orthogonal product codes. In *Proc. 2005 IEEE Intl. Symposium on Information Theory*, pages 1018–1022, Adelaide, Australia, 2005.
- [51] M. Grassl and M. Rötteler. Constructions of quantum convolutional codes. In *Proc. 2007 IEEE Intl. Symposium on Information Theory*, pages 816–820, Nice, France, 2007.
- [52] M. Grassl and M. Rötteler. Non-catastrophic encoders and encoder inverses for quantum convolutional codes. In *Proc. 2006 IEEE Intl. Symposium on Information Theory*, pages 1109–1113, Seattle, WA, USA, 2006.
- [53] M. Grassl, M. Rötteler, and T. Beth. Efficient quantum circuits for non-qubit quantum error-correcting codes. *Internat. J. Found. Comput. Sci.*, 14(5):757–775, 2003.
- [54] M. Hagiwara and H. Imai. Quantum quasi-cyclic LDPC codes. *Proc. 2007 IEEE International Symposium on Information Theory*, 2007. quant-ph/071020v1.
- [55] A. Hocquenghem. Codes correcteurs d'erreurs. *Chiffres*, 2:147–156, 1959.
- [56] M. H. Hsieh, I. Devetak, and T. A. Brun. General entanglement-assisted quantum error-correcting codes. 2007, arXiv:quant-ph-0708214v1.
- [57] M. H. Hsieh, I. Devetak, and T. A. Brun. Quantum quasi-cyclic low-density parity-check codes. March 2008. arXiv:quant-ph/arXiv:0803.0100.
- [58] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, Cambridge, 2003.
- [59] L. Ioffe and M. Marc Mzard. Asymmetric quantum error-correcting codes. *Phys. Rev. A*, 75(032345), 2007.
- [60] G. Smith J.A. Smolin and S. Wehner. A simple family of nonadditive quantum codes. 2007.
- [61] J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley. Theory of decoherence-free, fault-tolerant, universal quantum computation. *PRA*, 63:042307, 2001. quant-ph/0004064.
- [62] A. Ketkar, A. Klappenecker, S. Kumar, and P.K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, 52(11):4892 – 4914, 2006.
- [63] J.-L. Kim. New quantum-error-correcting codes from Hermitian self-orthogonal codes over GF(4). In *Proc. of the Sixth Intl. Conference on Finite Fields and Applications*, pages 209–213. Oaxaca, Mexico, Springer-Verlag, May 21-25, 2002.
- [64] J.-L. Kim and J. Walker. Nonbinary quantum error-correcting codes from algebraic curves. submitted to a special issue of Com<sup>2</sup>MaC Conference on Association Schemes, Codes and Designs in Discrete Math, 2004.
- [65] A. Kitaev. Topological quantum codes and anyons. In *Quantum Computation: A Grand Mathematical Challenge for the Twenty-first Century and the Millennium*, volume 58 of *Proc. Sympos. Appl. Math.*, pages 267–272. Amer. Math. Soc., Providence, RI, 2002.
- [66] A. Klappenecker and P.K. Sarvepalli. Clifford code constructions of operator quantum error correcting codes. arXiv:quant-ph/0604161, 2006.
- [67] E. Knill. Group representations, error bases and quantum codes. Los Alamos National Laboratory Report LAUR-96-2807, 1996.
- [68] E. Knill. Fault-tolerant postselected quantum computation: Threshold analysis. arXiv.org:quant-ph/0404104, 2004.
- [69] E. Knill. On protected realizations of quantum information. eprint: quant-ph/0603252, 2006.
- [70] E. Knill, R. Laflamme, and L. Viola. Theory of quantum error correction for general noise. *Phys. Rev. Lett.*, 84(002525), 2000.
- [71] E. Knill, R. Laflamme, and W. Zurek. Threshold accuracy for quantum computation. e-print quant-ph/9610011.
- [72] M. H. Kremsky, Hsieh and T. A. Brun. Classical enhancement of quantum error-correcting codes. submitted to PRA.
- [73] D. W. Kribs, R. Laflamme, and D. Poulin. Unified and generalized approach to quantum error correction. *Phys. Rev. Lett.*, 94(180501), 2005.
- [74] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek. Perfect quantum error correction code, 1996.
- [75] R. Lang and P.W. Shor. Nonadditive quantum error correcting codes adapted to the amplitude damping channel. *IEEE Trans. Inform. Theory*. arxiv: 0712.2586.
- [76] R. Li and X. Li. Binary construction of quantum codes of minimum distance three and four. *IEEE Trans. Inform. Theory*, 50(6):1331–1336, 2004.
- [77] D.A. Lidar, I.L. Chuang, and K.B. Whaley. Decoherence-free subspaces for quantum-computation. *Phys. Rev. Letters*, 81:2594–2597, 1998.
- [78] D. J. C. MacKay, G. Mitchison, and P. L. McFadden. Sparse-graph codes for quantum error correction. *IEEE Trans. Inform. Theory*, 50(10):2315–2330, 2004.
- [79] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.
- [80] M. Nielsen and I. Chang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.
- [81] H. Ollivier and J.-P. Tillich. Description of a quantum convolutional code. *Phys. Rev. Lett.*, 91(17):1779021–4, 2003.
- [82] H. Ollivier and J.-P. Tillich. Quantum convolutional codes: Fundamentals. ArXiv:quant-ph/0401134, 2004.
- [83] H. Ollivier and J.-P. Tillich. Interleaved serial concatenation of quantum convolutional codes: gate implementation and iterative error estimation algorithm. In *Proc. of the 26th Symposium on Information Theory in the Benelux*, page 149, Brussels, Belgium, 2005.
- [84] D. Poulin. Stabilizer formalism for operator quantum error correction. *Phys. Rev. Lett.*, 95(230504), 2005.
- [85] D. Poulin. Optimal and efficient decoding of concatenated quantum block codes. *Phys. Rev. A*, 2006.
- [86] D. Poulin, J.-P. Tillich, and H. Ollivier. Quantum serial turbo-codes. *Phys. Rev. A*, 2007.
- [87] J. Preskill. Reliable quantum computers. In *Proc. Roy. Soc.*, volume A 454, pages 385–410, 1998.
- [88] E.M. Rains. Nonbinary quantum codes. *IEEE Trans. Inform. Theory*, 45(6):1827–1832, 1999.
- [89] M. Rötteler, M. Grassl, and T. Beth. On quantum MDS codes. In *Proc. 2004 IEEE Intl. Symposium on Information Theory*, page 355, Chicago, USA, 2004.
- [90] V.P. Roychowdhury and F. Vatan. *Lecture Notes in Computer Science*, pages 325–336. New York: Springer, 1998.
- [91] C.H. Lai S. Yu, Q. Chen and C.H. Oh. Non-additive quantum error-correcting code. arxiv: 0704.2122.
- [92] 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.
- [93] P. K. Sarvepalli and A. Klappenecker. Quantum Reed-Muller codes. In *Proc. 2005 IEEE International Symposium on Information Theory*, Adelaide, Australia, 2005.
- [94] D. Schlingemann. Stabilizer codes can be realized as graph codes. *Quantum Inf. Comput.*, 2(4):307–323, 2002.
- [95] B. Schumacher. Quantum coding. *Phys. Rev. A*, 51, 1995.
- [96] A. Shabani and D. A. Lidar. Theory of initialization-free decoherence-free subspaces and subsystems. *PRA*, 72:042303, 2005.
- [97] P. W. Shor. Scheme for reducing decoherence in quantum memory. *Phys. Rev. A*, 2:2493–2496, 1995.
- [98] 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.
- [99] A. M. Steane. Multiple-particle interference and quantum error correction. In *Proc. Roy. Soc., London A*, volume 452, pages 2551–2577, 1996.
- [100] A. M. Steane. Simple quantum error correcting codes. *Phys. Rev. Lett.*, 77:793–797, 1996.
- [101] A. M. Steane. Quantum Reed-Muller codes. *IEEE Trans. Inform. Theory*, 1997. quant-ph/9608026.
- [102] A. M. Steane. Enlargement of Calderbank-Shor-Steane codes. *IEEE Trans. Inform. Theory*, 45(7):2492–2495, 1999.

- [103] A. M. Steane and B. Ibinson. Fault-tolerant logical gate networks for Calderbank-Shor-Steane codes. *Phys. Rev. A.*, 72(052335), 2005.
- [104] A. M. Stephens, Z. W. E. Evans, S. J. Devitt, and L. C. L. Hollenberg. Universal quantum computation under asymmetric quantum error correction, 2007.
- [105] T. A. Wilde, M. M. Brun. Entanglement-assisted quantum convolutional coding. *Submitted to IEEE Tran. on Info. Theory*, a2007, quant-ph:arXiv:0712.2223.
- [106] L. Xiaoyan. Quantum cyclic and constacyclic codes. *IEEE Trans. Inform. Theory*, 50(3):547, 2004.
- [107] P. Zanardi and M. Rasetti. Noiseless quantum codes. *Phys. Rev. Lett.*, 79:3306, 1997.