Quantum Information Review
An International Journal

http://dx.doi.org/10.12785/qir/030201

New Families of Quantum Cyclic and Subsystem Codes for Asymmetric Quantum Channels

Salah A. Aly Ahmed[1,2,*] *and Alexei Ashikhmin*[3]

[1] Department of Applied Mathematics, Zewail University of Science and Technology, Egypt
[2] Department of Mathematics and Computer Science, Faculty of Science, Fayoum University, Egypt
[3] Bell Labs, Murray Hill , New Jersey, USA

Received: 15 Feb. 2015, Revised: 15 Apr. 2015, Accepted: 3 May 2015
Published online: 1 Jul. 2015

Abstract: A quantum computer exploits the rules of quantum mechanics to speed up computations. However, one has to mitigate noise and decoherence to avoid computational errors in order to successfully build quantum computers.
Recently the theory of quantum error control codes has been extended to the case of asymmetric quantum channels — qubit-flip and phase-shift errors may have equal or different probabilities. In this paper, we further develop this theory and establish the connection between asymmetric quantum codes and subsystem codes. We present families of subsystem and asymmetric quantum codes obtained from classical BCH and RS codes.

Keywords: Quantum Error-correcting Codes (QEC), Subsystem Codes (SSC), Error-Correcting Codes, Asymmetric Quantum Channels

1 Introduction

Quantum computers theoretically are able to solve certain problems more quickly than any deterministic or probabilistic computers. An example of such problems is the factorization of large integers in polynomial time. The novel idea is that a quantum computer exploits the rules of quantum mechanics to speed up computations. However, one has to mitigate noise and decoherence to avoid computational errors in order to successfully build quantum computers. Recently, the theory of quantum codes is extended to include construction of asymmetric quantum error-correcting codes (AQEC) for correcting error in channels with qubit-flip error probability $\Pr X$ different from the phase-shift error probability $\Pr Z$. Typically $\Pr Z \geq \Pr X$. First constructions of AQEC appeared in [11, 17, 28]. In [1] two families of asymmetric CSS quantum codes were constructed on the base on classical BCH codes. For an introduction into CSS codes see for example [8, 10, 23–26].

Note that several attempts to characterize noise error models in quantum systems were made in [19, 25]. Recently, quantum error correction has been extended over amplitude-damping channels [13], which is an example of asymmetric quantum channel.

The asymmetric quantum cyclic codes that we construct in this work have simple encoding and decoding circuits that can be implemented using shift-registers with feedback connections. Also, their algebraic structure simplifies the problem their parameters estimation. Furthermore, their stabilizers can be easily found from generator polynomials of the corresponding classical codes.

In this paper, we construct quantum error-correcting codes (QEC) that correct quantum errors that may destroy quantum information with different probabilities. We propose two generic methods that can be applied to any classical cyclic codes in order of obtaining asymmetric quantum cyclic codes. We use these methods to construct asymmetric quantum BCH, RM, RS codes, and further families of asymmetric subsystem codes (ASSC). Note that several classes of AQECs are also presented in [1, 7, 17, 22].

Notation: Let q be a power of a prime p. We denote by $\mathbf{F}_q$ the finite field with q elements. Let C be an additive code over $\mathbb{F}_{q^2}$ of length n (note that C is linear over $\mathbb{F}_p$).

* Corresponding author e-mail: sahmed@zewailcity.edu.eg

If C has minimum distance d and size $(q^2)^k$ we will say that it is an $[n,k,d]_{q^2}$ code. We define the Euclidean inner product for vectors $\mathbf{x},\mathbf{y}\in\mathbb{F}_q^n$ by $\langle x|y\rangle=\sum_{i=1}^n x_iy_i$ and the Euclidean dual code of C as

$$C^{\perp}=\{x\in\mathbf{F}_{q^2}^n \mid \langle x|y\rangle=0 \text{ for all } y\in C\}.$$

We define the Hermitian inner product for vectors $x,y\in\mathbf{F}_{q^2}^n$ as $\langle x|y\rangle_h=\sum_{i=1}^n x_i^q y_i$ and the Hermitian dual of C as

$$C^{\perp_h}=\{x\in\mathbf{F}_{q^2}^n \mid \langle x|y\rangle_h=0 \text{ for all } y\in C\}.$$

If C is an $[n,(n-k)/2]_{q^2}$ self-orthogonal code, i.e., $C\subseteq C^{\perp_h}$, then it defines a q-ary quantum stabilizer code Q that encodes k logical qubits into n qubits with minimum distance $d=\min_{c\in C^{\perp_h}\setminus C}\mathrm{wt}(c)$, for details see [10], [25], [8]. We will say that Q is an $[[n,k,d]]_q$ stabilizer code. The

A special family of stabilizer code are CSS codes. In this case a self orthogonal code over $\mathbf{F}_{q^2}$ is constructed from one or two codes over $\mathbf{F}_q$ and it is further used to construct a quantum stabilizer code. Omitting details, we describe CSS codes as follows. If C is an $[n,k,d]_q$ classical additive code such that $C\subseteq C^{\perp}$, that is C is self-orthogonal with respect to the Euclidean inner product, then it can be used to construct an $[[n,n-2k,d]]_q$ stabilizer code. Also recall that if C is an $[n,k,d]_q$ classical additive dual-containing code, $C^{\perp}\subseteq C$, respect to the Euclidean inner product, then there exists an $[[n,2k-n,d]]_q$ stabilizer code. More generally, if C_1 and C_2 are $[n,k_1,d_1]_q$ and $[n,k_2,d_2]_q$ two classical codes such that $C_1\subseteq C_2$, then there exists a $[[n,k_2-k_1,d]]_q$ stabilizer code.

Let A_i and $A_i^{\perp},i=1,\ldots,n$, be the number of vectors of weight i in codes C and $C^{\perp_h}$ respectively. Since $C\subseteq C^{\perp_h}$ we have $A_i^{\perp}\geq A_i$. Let d_Q be the first integer such that $A_{d_Q}^{\perp}>A_{d_Q}$. Then d_Q is the minimum distance of Q and we will say that Q is an $[[n,k,d_Q]]_q$ quantum stabilizer code. Further if the minimum distance of $C^{\perp_h}$ is d_Q (potentially it could be smaller than d_Q) we will say that Q is a *pure* quantum code. Details on the connection between quantum stabilizer codes and classical self-orthogonal codes can be found in [10], [25], [8].

The following theorem establishes the connection between two classical codes and QECs (Quantum Error-correcting Codes), AQECs, SSCs (Subsystem Codes), ASSCs (Asymmetric Subsystem Codes).

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*

$$d_x=\min\{\mathrm{wt}(C_1\backslash C_2^{\perp}),\mathrm{wt}(C_2\backslash C_1^{\perp})\},\ \textit{and}$$
$$d_z=\max\{\mathrm{wt}(C_1\backslash C_2^{\perp}),\mathrm{wt}(C_2\backslash C_1^{\perp})\}.$$

i) If $C_2^{\perp}\subseteq C_1$, then there exists an AQEC with parameters

$$[[n,\dim C_1-\dim C_2^{\perp},\mathrm{wt}(C_2\backslash C_1^{\perp})/\mathrm{wt}(C_1\backslash C_2^{\perp})]]_q$$
$$=[[n,k_1+k_2-n,d_z/d_x]]_q.$$

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 $[[n,k_1+k_2-n-r,r,d_x]]_q$, $0\leq r<k_1+k_2-n$.

iii) If $C_2^{\perp}=C_1\cap C_1^{\perp}\subseteq C_2$, then there exist ASSCs 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 the above codes are pure to their minimum distances.

The paper is organized as follows. Sections 2, 3, and 6 are devoted to two families of AQECs, namely BCH AQECs and RS AQECs. Sections 4 and 7 consider the problem of construction of asymmetric subsystem codes and their relation to AQECs. We show the tradeoff between subsystem codes and AQECs. Section 7 presents the bound on AQEC and ASSC parameters. Finally, the paper is concluded with a discussion in Section 8.

2 Asymmetric Quantum Codes

Let $\mathscr{H}$ be the Hilbert space $\mathscr{H}=\mathbb{C}^{q^n}=\mathbb{C}^q\otimes\mathbb{C}^q\otimes\ldots\otimes\mathbb{C}^q$. Let vectors $|x\rangle,x\in\mathbb{F}_q$, for an orthonormal basis of $\mathbb{C}^q$, assuming $q=p^2$. For $a,b\in\mathbb{F}_q$ we define the unitary operators $X(a)$ and $Z(b)$ that act in $\mathbb{C}^q$ as

$$X(a)|x\rangle=|x+a\rangle,\qquad Z(b)|x\rangle=\omega^{\mathrm{tr}(bx)}|x\rangle, \tag{1}$$

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 $\mathbf{b}=(b_1,\ldots,b_n)\in\mathbf{F}_q^n$, and further

$$X(a)|x\rangle=|x+a\rangle,\qquad Z(b)|x\rangle=\omega^{\mathrm{tr}(bx)}|x\rangle, \tag{2}$$

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

$$X(\mathbf{a})=X(a_1)\otimes\cdots\otimes X(a_n),\ \text{and}$$
$$Z(\mathbf{b})=Z(b_1)\otimes\cdots\otimes Z(b_n) \tag{3}$$

the tensor products of n error operators and further

$$\mathbf{E}_x=\{X(\mathbf{a})|\mathbf{a}\in\mathbf{F}_q^n\},\ \mathbf{E}_z=\{Z(\mathbf{b})|\mathbf{b}\in\mathbf{F}_q^n\} \tag{4}$$

We define the error groups $\mathbf{G}_x$ and $\mathbf{G}_z$ by

$$\mathbf{G}_x=\{\omega^c\mathbf{E}_x|c\in\mathbf{F}_p\}=\{\omega^cX(\mathbf{a})\,|\,\mathbf{a}\in\mathbf{F}_q^n,c\in\mathbf{F}_p\},$$
$$\mathbf{G}_z=\{\omega^c\mathbf{E}_z|c\in\mathbf{F}_p\}=\{\omega^cZ(\mathbf{b})\,|\,\mathbf{b}\in\mathbf{F}_q^n,c\in\mathbf{F}_p\}. \tag{5}$$

We will say that $\mathbf{G}_x$ and $\mathbf{G}_z$ represent the qubit-flip and phase-shift errors, respectively. The entire error group is defined by

$$\mathbf{G} = \langle \mathbf{G}_x, \mathbf{G}_z \rangle = \left\{ \omega^c X(\mathbf{a}) Z(\mathbf{b}) | c \in \mathbf{F}_p, \mathbf{a}, \mathbf{b} \in \mathbf{F}_q^n \right\} \quad (6)$$

The error operators from $\mathbf{G}_x$ and $\mathbf{G}_z$ represent the qubit-flip and phase-shift errors respectively.

Typically quantum codes are constructed under the assumption that for any nonzero $a, b \in \mathbb{F}_q$ the error operators from $X(a)$ and $Z(b)$ have the same probabilities, i.e., $\Pr X(a) = \Pr Z(b)$. Physical experiments show that this assumption does not hold in reality [17, 28]. Below we derive families of asymmetric quantum error codes that are matched to quantum channels with $\Pr Z(b) > \Pr X(a)$.

Definition 1(AQEC). *A q-ary asymmetric quantum code Q, denoted by* $[[n,k,d_z/d_x]]_q$, *is a q-ary* $[[n,k]]$ *stabilizer code that can correct any* $\lfloor \frac{d_x-1}{2} \rfloor$ *flip errors and any* $\lfloor \frac{d_z-1}{2} \rfloor$ *phase-flip errors.*

The ratio $\rho = d_z/d_x$is used to compare d_z and d_x. Therefore, if $d_z > d_x$, then the AQEC has a ratio great than one and therefore the code is capable of correcting more phase-shift errors than qubit-flip errors. In our work, we would like to increase both the minimum distances d_z and d_x as well as dimension k of the quantum code.

Connection to Classical nonbinary Codes. Let C_1 and C_2 be $[n,k_1,d_1]_q$ and $[n,k_2,d_2]_q$ codes over $\mathbf{F}_q$ respectively. let $[n,k_1,d_1]_q$ and $[n,k_2,d_2]_q$ be their parameters. Denote by H_i a parity check matrix of code C_i for $i = 1,2$. 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. If now C_i are cyclic codes with generator polynomials $g_i(x)$ then $k_i = n - deg(g_i(x))$, see [16, 18]. The relation between codes C_1 and C_2 is shown in Fig.1.

Code vectors of C_1 and C_2 correspond to certain elements of the groups $\mathbf{G}_x$ and $\mathbf{G}_z$ respectively. This connection is well-know, see for example [10, 20, 21]. The following Lemmas shows that Asymmetric CSS quantum codes can be constructed from C_1 and C_2.

Lemma 1(CSS AQEC). *Let* $C_i, i = 1,2$ *be* $[n,k_i,d_i]_q$ *classical codes with the property that* $C_i^\perp \subseteq C_{1+(i \mod 2)}$. *Let* $d_x = \min\{\mathrm{wt}(C_1 \backslash C_2^\perp), \mathrm{wt}(C_2 \backslash C_1^\perp)\}$, *and* $d_z = \max\{\mathrm{wt}(C_1 \backslash C_2^\perp), \mathrm{wt}(C_2 \backslash C_1^\perp)\}$. *Then there exists an* $[[n, k_1+k_2-n, d_z/d_x]]_q$ *pure ACSS code.*

We use the same definition of pure code as stated in [10] [1]. Now we would like to find codes C_1 and C_2 that would give us large values for d_x and d_z for given n and k_1+k_2-n.

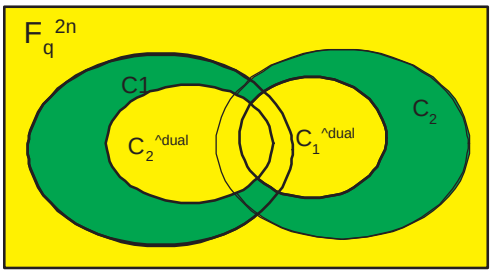

Fig. 1: Constructions of asymmetric quantum codes based on two classical codes C_1 and C_2 with parameters $[n,k_1]$ and $[n,d_2]$ such that $C_i \subseteq C_{1+(i \mod 2)}$ for $i = \{1,2\}$. AQEC has parameters $[[n, k_1+k_2-n, d_z/d_x]]_q$ where $d_x = \mathrm{wt}(C_1 \backslash C_2^\perp)$ and $d_z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

3 Asymmetric Quantum BCH and RS Codes

In this section we construct asymmetric CSS codes on the base of classical BCH and RS codes. We will restrict ourself to the Euclidean construction over $\mathbf{F}_q$, though the generalization to the Hermitian construction over $\mathbf{F}_{q^2}$ is straightforward.

BCH codes form a well known family of classical cyclic codes, see for example [15, 16, 18]. Below we remind their definition.

Let q be a power of a prime and n a positive integer such that $\gcd(q,n) = 1$. The *cyclotomic coset* S_x modulo n is defined by

$$S_x = \{xq^i \bmod n \mid i \in \mathbf{Z}, i \geq 0\}. \quad (7)$$

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

$$g(x) = \prod_{i \in S} (x - \alpha^i), \quad (8)$$

where $S = S_1 \cup S_2 \cup \ldots \cup S_{\delta-1}$. Thus, c is a codeword in $\mathscr{C}$ if and only if $c(\alpha) = c(\alpha^2) = \ldots = c(\alpha^{\delta-1}) = 0$. A parity check matrix of this code can be defined as

$$H_{bch} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{\delta-1} & \alpha^{2(\delta-1)} & \cdots & \alpha^{(\delta-1)(n-1)} \end{bmatrix}. \quad (9)$$

In general the dimensions and minimum distances of BCH codes are not known. However, lower bounds on these two parameters are given by $d \geq \delta$ and $k \geq n - m(\delta-1)$. Fortunately, in [4, 6] exact formulas for the dimensions and minimum distances are given under certain conditions. In particular, the following result hods.

Theorem 2(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*

$$k=n-m\lceil(\delta-1)(1-1/q)\rceil. \quad (10)$$

*Proof.*See [4, Theorem 10].

In [25, 27] Steane constructed first binary quantum BCH codes. In [14] Grassl *el. at.* proposed a family of quantum BCH codes and presented tables of best known BCH codes.

One of main challenges in [4, 6] were proofs of dual-containing conditions for BCH codes. We can avoid these problems by looking for BCH codes that are nested. The following result allows obtaining a family of quantum codes derived from nonprimitive narrow-sense BCH codes, see our initial results [7].

Theorem 3.*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*

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

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 [4, Theorem 19].

3.1 AQEC-BCH

Fortunately, the mathematical structure of BCH codes always us easily to show the nested required property needed in Lemma 1. Indeed, from Theorem 2 we know that the generator polynomial $g(x)$ has degree $m\lfloor(\delta-1)(1-1/\delta)\rfloor$ if $\delta\leq\delta_{max}$. Therefore the code dimension is equal to $k=n-deg(g(x))$. Hence, the nested structure of BCH codes is obvious and can be described as follows. Let

$$\delta_{i+1}>\delta_i>\delta_{i-1}\geq\ldots\geq 2, \quad (11)$$

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

$$C_{i+1}\subseteq C_i\subseteq C_{i-1}\subseteq\ldots \quad (12)$$

We need to ensure that $\delta_i\neq\delta_{i+1}$ and that the difference among them is large enough. Therefore the sets of roots $\{2,\ldots,\delta_i-1\}$ and $\{2,\ldots,\delta_{i+1}-1\}$ are distinct. 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 $\mathbf{F}_q$.

Table 1: Families of asymmetric quantum BCH codes [9]

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 4(AQEC-BCH). *Let $\gcd(n,q)=1$, with $ord_n(q)=m$. Let C_1 and C_2 be two narrow-sense BCH codes of length $q^{\lfloor m/2\rfloor}<n\leq q^m-1$ 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 $\delta_1<\delta_2^\perp\leq\delta_2<\delta_1^\perp$.*

If $S_1\cup\ldots\cup S_{\delta_1-1}\neq S_1\cup\ldots\cup S_{\delta_2-1}$, then there exists an asymmetric

$$[[n,n-m\lceil(\delta_1-1)(1-1/q)\rceil-m\lceil(\delta_2-1)(1-1/q)\rceil,\geq d_z/d_x]]_q$$

quantum code with $d_z=\mathrm{wt}(C_2\backslash C_1^\perp)\geq\delta_2>d_x=\mathrm{wt}(C_1\backslash C_2^\perp)\geq\delta_1$.

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 2, 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 $k_1^\perp<k_2^\perp$.

Let us denote $d_x=wt(C_1\backslash C_2^\perp)\geq\delta_1$ and $d_z=wt(C_2\backslash C_1^\perp)\geq\delta_2$ and assume that $d_z>d_x$. (If $d_x>d_z$ we interchange the roles of codes C_1 and C_2.) Then, by Lemma 1 and the assumptions there exists AQEC with parameters $[[n,k_1+k_2-n,\geq d_z/d_z]]_q$.

Usually the designed minimum distance gives only a lower bound on the true minimum distance of BCH codes. We argue that in our case the true minimum distances meet with the designed minimum distances for small values of designed distances. that are particularly interesting to us. One can also use the condition shown in [4, Corollary 11.] to ensure that the minimum distance meets the designed distance for certain bounds of the designed distance.

The condition on the designed distances δ_1 and δ_2, as shown in Theorem (4) and in [4, Corollary 11.], 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 2.*Let* $\gcd(m,q)=1$, *and* $n, q^{\lfloor m/2 \rfloor} < n \leq q^m - 1$, *is so that* $m = \mathrm{ord}_n(q)$. *Let* C_1 *and* C_2 *be* $[n,k_1,d_x \geq \delta_1]_q$ *and* $[n,k_2,d_z \geq \delta_2]_q$ *BCH codes respectively, such that* $\delta_1 < \delta_2^{\perp} \leq \delta_2 < \delta_1^{\perp}$, *and* $k_1+k_2 > n$. *If* $S_1 \cup \ldots \cup S_{\delta_1-1} \neq S_1 \cup \ldots \cup S_{\delta_2-1}$, *then there exists an asymmetric*

$$[[n, k_1+k_2-n, \geq d_z/d_x]]_q$$

quantum code with

$$d_z = \mathrm{wt}(C_1 \backslash C_2^{\perp}) = \delta_2 > d_x = \mathrm{wt}(C_2 \backslash C_1^{\perp}) = \delta_1.$$

This theorem can be used to construct any asymmetric cyclic quantum codes. Also, one can construct asymmetric quantum codes using codes over $\mathbf{F}_{q^2}$.

3.2 RS Codes

In this section we construct a family of asymmetric quantum codes based on classical Reed-Solomon codes. Recall that a RS code with length $n = q-1$ and designed distance δ over $\mathbf{F}_q$ is an $[[n, n-\delta+1, \delta]]_q$ cyclic code with the generator polynomial

$$g(x) = \prod_{i=1}^{d-1} (x - \alpha^i). \tag{13}$$

We use RS codes to construct an asymmetric quantum code as follows.

Theorem 5. *Let* $n = q-1$ *and* C_1 *and* C_2 *be* $[n, n-d_1+1, d_1]]_q$ *and* $[n, n-d_2+1, d_2]_q$ *RS codes respectively. Let further* $d_1 < d_2 < d_1^{\perp} = n - d_1$. *Then there exists an* $[[n, n-d_1-d_1+2, d_z/d_x]]_q$, *AQEC code with* $d_x = d_1 < d_z = d_2$.

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

It is obvious that the constructed code is a pure code. 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 $\mathbf{F}_q$.

4 AQEC and Connection with Subsystem Codes

In this section we consider a large class of quantum codes called asymmetric subsystem codes (ASSs). In particular, we construct families of subsystem BCH codes and subsystem cyclic codes over $\mathbf{F}_q$ In [2,3,7] we constructed other families of subsystem cyclic, BCH, RS and MDS codes over $\mathbf{F}_{q^2}$.

Subsystem quantum codes are a special class of quantum codes in which errors can be corrected as well as avoided (isolated).

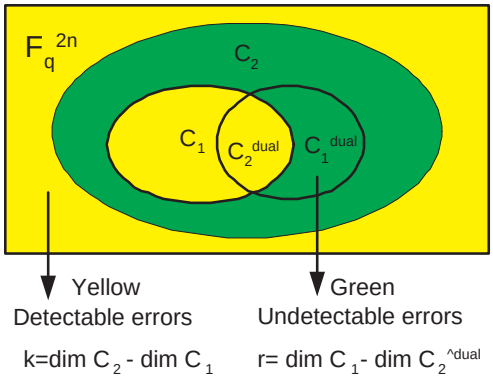

Fig. 2: A quantum code Q is decomposed into two subsystem A (info) and B (gauge)

Definition 2(Subsystem Codes). *An* $[[n,k,r,d]]_q$ *subsystem code is a subspace Q that a) can be represented as a tensor product of subspaces A and B, such that* $Q = A \otimes B$, *with* $\dim A = k$ *and* $\dim B = r$, *and b) all errors of weight less than d on subsystem A are detectable.*

Subsystem codes can be constructed from the classical codes over $\mathbf{F}_q$ and $\mathbf{F}_{q^2}$. The classical codes do not need to be self-orthogonal (or dual-containing) as shown in the Euclidean construction below. General constructions of subsystem codes, known as the subsystem CSS and Hermitian constructions, were proposed in [5]. Below we consider a special case of the subsystem CSS construction.

Lemma 3(SSC Based CSS 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. We remind that if $a,b,c,d \in \mathbf{F}_q^n$ then the symplectic inner product between vectors (a,b) and (c,d) is defined by

$$(a,b) * (c,d) = \langle a|d\rangle + \langle b|c\rangle$$

Further, the symplectic weight of a vector (a,b) is defined by

$$\mathrm{swt}((a,b)) = |\{(a_i,b_i) \neq (0,0)\}|.$$

For a linear code $C \subseteq \mathbf{F}_q^{2n}$ we define

$$\mathrm{swt}(C) = \min_{a \in C, a \neq 0} \mathrm{swt}(a).$$

The symplectic dual of C is defined by

$$C^{\perp_s} = \{b \in \mathbf{F}_q^{2n} : b *_s a = 0, \forall a \in C\}.$$

Let us now define the code $X = C_1 \times C_1 \subseteq \mathbf{F}_q^{2n}$, therefore $X^{\perp_s} = (C_1 \times C_1)^{\perp_s} = C_1^{\perp_s} \times ..$ 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 [5, 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 roles of C_1 and $C_1^{\perp}$, we obtain the other subsystem code.

Some particular construction of subsystem codes (SSC) requires that C_2 be self-orthogonal, $C_2 \subseteq C_2^{\perp}$, see [10]. However, both AQEC and SSC can be constructed from the pair-nested classical codes. Hence classical codes C_1 and C_2 with the property that $C_2 = C_1 \cap C_1^{\perp} \subseteq C_2^{\perp}$, can be used to construct a subsystem code and an asymmetric quantum code.

The construction in Lemma 3 can be generalized to asymmetric subsystem codes (ASSC) CSS construction in a similar way. This means that we can consider an $[[n,k,d_z/d_x]]_q$ AQEC as a $[[n,k,0,d_z/d_x]]_q$ subsystem code. Therefore all results obtained in [2, 3, 5] directly follow from this construction, by just fixing the minimum distance condition.

We have shown in [2, 3] that all stabilizer codes (pure and impure) can be reduced to subsystem codes. We say that a code is Co-SSC if it can be produced from SSC by reducing the dimension and increasing the minimum distance, as it is done in the following Theorem.

Theorem 6(Trading Dimensions of SSC and Co-SSC). *If there exists an $\mathbf{F}_q$-linear $[[n,k,r,d]]_q$ subsystem code with $k > 1$ that is pure up to d', then there exists an $\mathbf{F}_q$-linear $[[n,k-1,r+1,\geq d]]_q$ subsystem code that is pure up 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 [4, 6] 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

$$2 \leq \delta \leq \delta_{\max} = \frac{n}{q^m - 1}(q^{\lceil m/2 \rceil} - 1 - (q-2)), \qquad (14)$$

were m is odd.

We use this result and [3, Theorem 2] to obtain nonprimitive subsystem BCH codes from classical BCH codes over $\mathbf{F}_q$ and $\mathbf{F}_{q^2}$ [5, 6]. In [2] subsystem codes from primitive BCH codes were obtained.

Lemma 4. *Let m be an odd positive integer such that $q^{\lfloor m/2 \rfloor} < n \leq q^m - 1$. Let $2 \leq \delta \leq \delta_{\max} = \frac{n}{q^m-1}(q^{\lceil m/2 \rceil} - 1 - (q-2))$. Then there exists an $[[n, n - 2m\lceil(\delta-1)(1-1/q)\rceil - r, r, \geq \delta]]_q$ subsystem BCH code with $0 \leq r < n - 2m\lceil(\delta-1)(1-1/q)\rceil$.*

Proof. We know that if $2 \leq \delta \leq \delta_{\max} = \frac{n}{q^m-1}(q^{\lceil m/2 \rceil} - 1 - (q-2))$, then the classical BCH codes contain their Euclidean dual codes, [4, Theorem 3.]. Therefore using [4, Theorem 19.], we obtain an $[[n, n - 2m\lceil(\delta-1)(1-1/q)\rceil, \geq \delta]]_q$ stabilizer code.

According to Theorem 6 any stabilizer code can be reduced to a subsystem code. Therefore for any r in the range $0 \leq r < n - 2m\lceil(\delta-1)(1-1/q)\rceil$ there exists 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 5. *Let $m = \mathrm{ord}_n(q^2)$. For any δ in the range $2 \leq \delta \leq \delta_{\max} = \lfloor n(q^m-1)/(q^{2m}-1)\rfloor$, there exists a subsystem*

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

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

Proof. According to [4, Theorem 14.] if $2 \leq \delta \leq \delta_{\max} = \lfloor n(q^m-1)/(q^{2m}-1)\rfloor$, then there exists a classical $[n, n - m\lceil(\delta-1)(1-1/q^2)\rceil, \geq \delta]_q$ BCH code that contains its Hermitian dual code. Hence, according to [4, Theorem 21.], the existence of a classical codes containing its Hermtian codes guarantees the existence of corresponding quantum codes. Now from [3, Theorem 2] we get that there exists an $[[n, n - 2m\lceil(\delta-1)(1-1/q^2)\rceil - r, r, d_Q \geq \delta]]_q$ subsystem code that is pure up to δ, for any $0 \leq r < n - 2m\lceil(\delta-1)(1-1/q^2)\rceil$.

Instead of constructing subsystem codes from stabilizer BCH codes as shown in Lemmas 4, 5, 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 $\{iq^j \bmod n \mid j \in \mathbf{Z}\}$. We will construct only SSC from nonprimitive BCH codes over $\mathbf{F}_q$ (for codes over $\mathbf{F}_{q^2}$ and further details see [2]).

Lemma 6. *Let $m = \mathrm{ord}_n(q)$ be an odd integer, and $2 \leq \delta \leq \delta_{\max} = \frac{n}{q^m-1}(q^{\lceil m/2 \rceil} - 1 - (q-2)$. Let C_2 be a BCH code with length $q^{\lfloor m/2 \rfloor} < n \leq q^m - 1, \gcd(n,q) = 1$, and the generator polynomial with roots from the set $T_{C_2} = \{S_0, S_1, \ldots, S_{n-\delta}\}$. Let $T \subseteq \{0\} \cup \{S_\delta, \ldots, S_{n-\delta}\}$.*

Table 2: 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

Let further $C_1 \subseteq \mathbf{F}_q^n$ be a BCH code with generator polynomial roots from the 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 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:

1. We know that $T_{C_2} = \{S_0, S_1, \ldots, S_{n-\delta}\}$ and $T \subseteq \{0\} \cup \{S_\delta, \ldots, S_{n-\delta}\}$ are nonempty sets. Hence $T_{C_2^\perp} = \{S_1, \ldots, S_{\delta-1}\}$. Further, if $2 \leq \delta \leq \delta_{\max} = \frac{n}{q^m-1}(q^{\lceil m/2\rceil} - 1 - (q-2))$, where m is odd, then $C_2 \subseteq C_2^\perp$. Now, if $k = m\lceil(\delta-1)(1-1/q)\rceil$, then $\dim C_2^\perp = n-k$ and $\dim C_2 = k$.
2. We know that $C_1 \in \mathbf{F}_q^n$ is a BCH code with generator polynomial roots from $T_{C_1} = T_{C_2} \setminus (T \cup T^{-1}) = \{S_0, S_1, \ldots, S_{n-\delta}\} \setminus (T \cup T^{-1})$ where $T^{-1} = \{-t \bmod n \mid t \in T\}$. Thus the generator polynomial roots of the dual code $C_1^\perp$ belong to the 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 $\dim C_1 = k+r$.
3. From step (i) and (ii), and for $0 \leq r < n-2k$, and by Lemma 3, 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 by using the distances d_x and d_z as shown in 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 straightforward and similar to our constructions in [2, 3].

5 Cyclic Subsystem Codes

Now, we will give a general construction of subsystem cyclic codes. Any cyclic codes, including BCH, RS, RM and duadic code, can be used in this construction. We show that if a classical cyclic code, say C_2 is self-orthogonal, i.e., $C_2 \subseteq C_2^\perp$, then one can use C_2 to construct cyclic subsystem codes. We will consider only codes over $\mathbf{F}_q$, and the case of $\mathbf{F}_{q^2}$ is considered in [2].

Theorem 7. *Let C_2 be a k-dimensional self-orthogonal cyclic code of length n over $\mathbf{F}_q$. Let sets of roots T_{C_2} and $T_{C_2^\perp}$ define codes C_2 and $C_2^\perp$ respectively. Let further T be a subset of $T_{C_2} \setminus T_{C_2^\perp}$ and C_1 be a cyclic code of length n over $\mathbf{F}_q$ with generator polynomial roots from $T_{C_1} = T_{C_2} \setminus (T \cup T^{-1})$. 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 [2] and S.Aly, 2008 Thesis, for details.

Now, using Theorem 7, we can construct asymmetric cyclic subsystem codes with parameters $[[n, n-2k-r, r, d_z/d_x]]_q$ for all $0 \leq r < n-2k$ where $d_x = \min\{\mathrm{wt}(C_2^\perp \setminus C_1), \mathrm{wt}(C_2^\perp \setminus C_1^\perp)\}$ and $d_z = \max\{\mathrm{wt}(C_1^\perp \setminus C_2), \mathrm{wt}(C_1^\perp \setminus C_2)\}$.

6 Illustrative Example

In Section 3, we constructed a family of asymmetric quantum codes with large minimum distance for given length and code dimension. Below we present a simple example of the construction.

Let C_1 be the $[15, 11, 3]_2$ BCH code with generator matrix

$$\begin{bmatrix} 1000\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0 \\ 0100\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0 \\ 0010\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1 \\ 0001\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1 \\ 0000\,1\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0 \\ 0000\,0\,1\,0\,0\,0\,0\,0\,0\,1\,0\,1 \\ 0000\,0\,0\,1\,0\,0\,0\,0\,1\,1\,1\,0 \\ 0000\,0\,0\,0\,1\,0\,0\,0\,0\,1\,1\,1 \\ 0000\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,1 \\ 0000\,0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,1 \\ 0000\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,1 \end{bmatrix}. \quad (15)$$

Then $C_1^{\perp}$ is the $[15,4,8]_2$ code with generator matrix

$$\begin{bmatrix} 1000\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1 \\ 0100\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0 \\ 0010\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0 \\ 0001\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1 \end{bmatrix}. \quad (16)$$

Let now C_2 be the $[15,7,5]_2$ BCH code defined by generator matrix

$$\begin{bmatrix} 1000\,0\,0\,0\,1\,0\,0\,0\,1\,0\,1\,1 \\ 0100\,0\,0\,0\,1\,1\,0\,0\,1\,1\,1\,0 \\ 0010\,0\,0\,0\,0\,1\,1\,0\,0\,1\,1\,1 \\ 0001\,0\,0\,0\,1\,0\,1\,1\,1\,0\,0\,0 \\ 0000\,1\,0\,0\,0\,1\,0\,1\,1\,1\,0\,0 \\ 0000\,0\,1\,0\,0\,0\,1\,0\,1\,1\,1\,0 \\ 0000\,0\,0\,1\,0\,0\,0\,1\,0\,1\,1\,1 \end{bmatrix}. \quad (17)$$

Then $C_2^{\perp}$ is the $[15,8,4]_2$ code with generator matrix

$$\begin{bmatrix} 1000\,0\,0\,0\,0\,1\,1\,0\,1\,0\,0\,0 \\ 0100\,0\,0\,0\,0\,0\,1\,1\,0\,1\,0\,0 \\ 0010\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,0 \\ 0001\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1 \\ 0000\,1\,0\,0\,0\,1\,1\,0\,1\,1\,1\,0 \\ 0000\,0\,1\,0\,0\,0\,1\,1\,0\,1\,1\,1 \\ 0000\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,1 \\ 0000\,0\,0\,0\,1\,1\,0\,1\,0\,0\,0\,1 \end{bmatrix}. \quad (18)$$

AQEC. We assume that the code C_1 corrects the bit-flip errors such that $C_2^{\perp} \subset C_1$. Furthermore, $C_1^{\perp} \subset C_2$. Further $d_x = \mathrm{wt}(C_1 \backslash C_2^{\perp}) = 3$ and $d_z = \mathrm{wt}(C_2 \backslash C_1^{\perp}) = 5$. Hence, there must exist asymmetric quantum error control codes (AQEC) with parameters $[[n, k_1 + k_2 - n, d_z/d_x]]_2 = [[15,3,5/3]]_2$. This quantum code can detect 4 phase-shift errors and 2 bit-flip errors. Fault tolerant circuits for this code can be constructed similarly to the circuit presented for $[[9,1,3]]_2$ and $[[7,1,3]]_2$ codes.

SSC. We can also construct a subsystem code 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 $C_2^{\perp} \subset C_1$. Next, $k = \dim C_1 - \dim C_2 = 4$ and $r = \dim C_2 - \dim C_1^{\perp} = 3$, and $d = \mathrm{wt}(C_1 \backslash C_2) = 3$. Therefore, there exists a subsystem code (SSC) with parameters $[[15,4,3,3]]_2$, and an asymmetric subsystem code (ASSC) code with parameters $[[15,4,3,5/3]]_2$.

Remark. A natural question is to ask how we should choose distances d_z and d_x. A possible answer follows from real physical systems. Often, the time needed for a phase-shift error to occur is much less than the time needed for a qubit-flip error. Hence one has to design codes with d_z and d_x that fit a particular physical model.

7 Bounds on Asymmetric QEC and Subsystem Codes

In this section we generalize the Singleton bound for the asymmetric codes and asymmetric subsystem codes. We show in the asymmetric case dimensions and minimum distances can be trade off in a similar manner as shown in [2,3].

7.1 Asymmetric Singleton Bound

Theorem 8. *An $[[n,k,d_z/d_x]]_q$ asymmetric pure quantum code must have*

$$d_x \leq (n-k+2)/2,$$

and the bound

$$d_x + d_z \leq (n-k+2). \quad (19)$$

Proof. Existence of an $[[n,k,d_z/d_x]]_q$ asymmetric code 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 $d_x + d_z \leq n - (k_1 + k_2 - n) + 2 = n - k + 2$.

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

Lemma 7. *Asymmetric subsystem codes with parameters $[[n,k,r,d_z/d_x]]_q$ for $0 \leq r < k$ satisfy*

$$k + r \leq n - d_x - d_z + 2. \quad (20)$$

Remark. In fact, the AQEC RS codes obtained in Section 3 are optimal in a sense that they meet the asymmetric Singleton bound with equality. Codes that meet Singleton bound are called maximum distance separable (MDS) codes. The conclusion is that MDS QECs are also MDS AQEC. Furthermore, MDS SSC are also MDS ASSC.

7.2 Asymmetric 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 $C_2 = C_1 \cap C_1^{\perp}$. We use this observation in the following theorem.

Lemma 8. *A pure* $((n,K,K',d_z/d_x))_q$ *asymmetric subsystem code satisfies*

$$\sum_{j=0}^{\lfloor\frac{d_x-1}{2}\rfloor}\binom{n}{j}(q^2-1)^j \leq q^n/KK'. \quad (21)$$

Proof. Considering an asymmetric code as a symmetric code we conclude that a pure $((n,K,K',d_z/d_x)))_q$ code implies the existence of a pure $((n,KK',d_x))_q$ code. The $((n,KK',d_x))_q$ code must obey the quantum Hamming bound [5, 12]. Therefore it follows that

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

It is easy to check that $\sum_{j=0}^{\lfloor\frac{d_z-1}{2}\rfloor}\binom{n}{j}(q^2-1)^j$ not necessarily less than or equal to q^n/KK'. As an example, consider the asymmetric subsystem codes $[[15,4,3,5/3]]_2$ and $[[15,6,1,5/3]]_2$, where $d_z=5$, in which

$$\sum_{j=0}^{\lfloor\frac{d_z-1}{2}\rfloor}\binom{n}{j}(q^2-1)^j \not\leq q^n/KK'. \quad (22)$$

8 Conclusion

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 $\mathbf{F}_q$.

Acknowledgments.

The authors would like to thank A. Klappenecker, A. Steane, L. Ioffe, A. Stephens, and the Q.O.I. at TAMU. Part of this research on SSC and QEC has been done at CS/TAMU and during a research visit to Bell-Labs & alcatel-Lucent and Princeton University, the generalization to ASSC is a consequence.
The authors are grateful to the anonymous referee for a careful checking of the details and for helpful comments that improved this paper.

References

[1] S. A Aly. Asymmetric quantum BCH codes. *Proc. IEEE International Conference on Computer Engineering & Systems (ICCES'08)*, pages 157–162, November 23-27, Cairo, EG, 2008. arXiv:quant-ph/0803.

[2] S. A. Aly and A. Klappenecker. Constructions of subsysem codes over finite fields. *International journal of quantum information*, 2009.

[3] S. A. Aly and A. Klappenecker. Subsysem code constructions. In *Proc. IEEE International Symposium on Information Theory (ISIT'08)*, pages 369–373, Toronto, Canada 2008. arXiv:0712.4321v3.

[4] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. On quantum and classical BCH codes. *IEEE Trans. Inform. Theory*, 53(3):1183–1188, 2007. arXiv:quant-ph/0604102v1.

[5] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. Subsystem codes. In *44th Annual Allerton Conference on Communication, Control, and Computing*, pages 528–535, Monticello, Illinois, September 2006. arXiv:quant-ph/0610153v1.

[6] 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.

[7] S. A. Aly and A. E. Ashikhmin. Nonbinary Quantum Cyclic and subsystem Codes Over Asymmetrically-decohered Quantum Channels. In *Proc. 2010 IEEE International Symposium on Information Theory*, Cairo, Egypt, january 2010.

[8] A. E. Ashikhmin and E. Knill. Nonbinary quantum stabilizer codes. *IEEE Trans. Inform. Theory*, 47(7):3065–3072, 2001.

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

[10] 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.

[11] 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. quant-ph://arXiv:0709.3875v1.

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

[13] A. S. Fletcher, P. W. Shor, and M. Z. Win. Channel-adapted quantum error correction for the amplitude damping channel. *IEEE Tran. on Info. Theory*, 54(12):5705–5718, 2008. quant-ph:arXiv0710.1052v1.

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

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

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

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

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

[19] M. Nielsen and I. Chang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

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

[21] 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.
[22] P. K. Sarvepalli, A. Klappenecker, and M. Roettler. Asymmetric quantum LDPC codes. In *Proc. IEEE ISIT*, July 6-11, 2008.
[23] P. W. Shor. Scheme for reducing decoherence in quantum memory. *Phys. Rev. A*, 2:2493–2496, 1995.
[24] A. M. Steane. Multiple-particle interference and quantum error correction. In *Proc. Roy. Soc., London A*, volume 452, pages 2551–2577, 1996.
[25] A. M. Steane. Simple quantum error correcting codes. *Phys. Rev. Lett.*, 77:793–797, 1996.
[26] A. M. Steane. Quantum Reed-Muller codes. *IEEE Trans. Inform. Theory*, 1997. quant-ph/9608026.
[27] A. M. Steane. Enlargement of Calderbank-Shor-Steane codes. *IEEE Trans. Inform. Theory*, 45(7):2492–2495, 1999.
[28] A. M. Stephens, Z. W. E. Evans, S. J. Devitt, and L. C. L. Hollenberg. Asymmetric quantum error correction via code conversion. *PRA*, 77(062335), 2008.