Quantum Information and Computation, Vol. 11, No. 3&4 (2011) 0239–0252

NEW FAMILIES OF ASYMMETRIC QUANTUM BCH CODES

GIULIANO G. LA GUARDIA
Department of Mathematics and Statistics,
State University of Ponta Grossa – UEPG
84030-900, Ponta Grossa, PR, Brazil

Received March 31, 2010
Revised November 5, 2010

Several families of nonbinary asymmetric quantum Bose-Chaudhuri-Hocquenghem (BCH) codes are presented in this paper. These quantum codes have parameters better than the ones available in the literature. Additionally, such codes can be applied in quantum systems where the asymmetry between qudit-flip and phase-shift errors is large.

Keywords:
Communicated by: R Jozsa & B Terhal

1 Introduction

Since the last two decades, many authors have focused the attention in the construction of good quantum codes [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26]. Recently, some authors have constructed asymmetric quantum error-correcting codes (AQECC) [27, 28, 29, 16, 30, 31, 32, 33, 34], that are quantum codes defined over quantum channels where the probability of occurrence of qudit-flip errors may be different from the probability of occurrence of phase-shift errors. Actually, it is an extension of the theory of quantum error-correcting codes (QECC) for asymmetric quantum channels. Steane [35] was the first author who introduced the notion of asymmetric quantum errors. An asymmetric quantum code is denoted by $[[N, K, d_z/d_x]]_q$, where d_z is used to correct phase-shift errors and d_x is applied to correct qudit-flip errors. More precisely, the code can correct all qudit-flip errors up to $\lfloor (d_x - 1)/2 \rfloor$ and all phase-shift errors up to $\lfloor (d_z - 1)/2 \rfloor$.

In this paper, we propose the construction of several families of asymmetric q-ary (q is an odd prime power) quantum Bose-Chaudhuri-Hocquenghem (BCH) codes by means of the Calderbank-Shor-Steane (CSS) construction [4, 12, 36] applied to two distinct q-ary classical BCH codes (note that most authors of QECC's restrict themselves to binary codes, whereas in this work we deal with construction of q-ary codes, where q is an odd prime power). More precisely, we construct subclasses of (classical) BCH codes with great dimensions, computing lower-bounds to the corresponding minimum distances d_z and d_x by applying the well-known BCH bound. The proposed families have parameters better than the ones available in the literature in a certain sense specified in this section.

Briefly, the CSS construction consists of constructing a pair of linear codes (C_1, C_2) with $C_2^{\perp} \subset C_1$, where $C_2^{\perp}$ denotes the Euclidean dual of the code C_2 (see for example [12]). Note

that in some existing papers (see for example [4]) and also in this work, the code C_2 is replaced by $C_2^{\perp}$ so that the pair becomes $(C_1, C_2^{\perp})$ with $C_2 \subset C_1$ (the condition $C_2^{\perp} \subset C_1$ is equivalent to $C_1^{\perp} \subset C_2$). The class of CSS quantum error-correcting codes falls in the class of symplectic codes [4, 12, 1, 27, 2, 20].

Although in [26] families of quantum codes were constructed by applying similar technique, the parameters (dimension and minimum distances) of the proposed families are quite different from the ones shown in [26]. Additionally, the lower bounds for the minimum distances d_z and d_x of codes displayed in [26] are the same, whereas in the present paper we construct several families of asymmetric quantum codes where the lower bound for d_z is greater than the lower bound for d_x. In other words, the proposed codes have the property that d_z is large when compared to d_x, so such quantum codes are able to correct quantum errors with great asymmetry.

To compare the asymmetric quantum codes constructed in this paper with the ones shown in the literature we utilize the following criterion: for fixed values of the code-length n, and for fixed values of d_z and d_x, the asymmetric quantum BCH codes constructed here achieve greater values of the number of qudits than the ones available in the literature. This criterion is based on the evaluation of the pair of minimum distances d_z and d_x (see [12, 33, 31, 34]).

According to this criterion, the proposed families consist of quantum codes whose parameters are better than the ones available in the literature; the new code parameters are given by

i) $[[n, n - m(2c - l - 4) - 2, d_z \geq c/d_x \geq (c - l)]]_q$, $2 \leq c \leq q$ and $0 \leq l \leq c - 2$;

ii) $[[n, n - m(2c - l - 6) - 2, d_z \geq c/d_x \geq (c - l)]]_q$, $q + 2 < c \leq 2q$ and $0 \leq l \leq c - q - 3$;

iii) $[[n, n - m(4q - l - 5) - 1, d_z \geq (2q + 1)/d_x \geq (2q - l)]]_q$, $0 \leq l \leq q - 2$;

iv) $[[n, n - m(4q - l - 5) - 2, d_z \geq (2q + 2)/d_x \geq (2q - l)]]_q$, $0 \leq l \leq q - 2$,

where q is an odd prime power and $n = q^m - 1$.

On the other hand, it may be noted that such criterion is applicable only to CSS codes, whereas if it is adopted the fidelity (entanglement fidelity, or its variants) [36] as a measure of efficiency, one can compare any (binary or nonbinary) QECC's with any other (binary or nonbinary) QECC's. The quantum channels are usually (and also in this work) modeled as trace-preserving completely positive (TPCP) maps (see [36, 27, 16]), in which the measure is the fidelity [37, 38]. Such maps can be written in terms of Kraus operators A_i of the channel, where the action of the channel on a given input state ρ is described as $\rho \longmapsto \sum_i A_i \rho A_i^{\dagger}$, where the completeness relation $\sum_i A_i^{\dagger} A_i = I$ holds (here I denotes the identity map).

Constructive asymmetric CSS codes over arbitrarily (often memoryless) quantum channels (TPCP) have been presented with performance evaluation in the literature [16]. More specifically, if the probability of occurrence of qudit-flip error is p_x and that of phase-shift is p_z, then the CSS codes shown in [16] (one particular form in [39] is explicit) achieve the rate $1 - h(p_x) - h(p_z)$, where h denotes the binary entropy function. In this context, it seems that the quantum codes constructed in the present paper are not as good as the ones available in [16]. However, an advantage offered by the proposed quantum codes when compared to the ones shown in [16]: since the codes available in [16] are concatenated codes, the lengths of such codes might be very large as compared to the codes constructed in this work.

This paper is structured as follows. In Section 2, basic concepts on cyclic codes are reviewed. In Section 3 we recall the concept of error operators and asymmetric quantum codes. In Section 4, the quantum code construction generating several families of asymmetric quantum BCH codes is presented. In Section 5, examples of the constructed asymmetric codes are exhibited. In Section 6, the parameters of the constructed quantum codes are compared with the ones available in the literature and, in Section 7, the concluding remarks are drawn.

2 Review of Cyclic Codes

Notation. Throughout this paper, we always assume that q is an odd prime power, $n = q^m - 1$ is the code length, F_q denotes a finite field with q elements, α denotes a primitive element of F_{q^m}, $M^{(j)}(x)$ denotes the minimal polynomial of $\alpha^j \in F_{q^m}$, the congruence $\equiv$ is considered modulo n (mod n), $\mathrm{CSS}(C_1, C_2)$ denotes the asymmetric CSS code derived from two distinct classical linear codes C_1 and C_2, $C^{\perp}$ denotes the Euclidean dual code of a code C and $\mathbb{C}_{[a]}$ denotes the cyclotomic coset containing a, where a is not necessarily the smallest number in the coset $\mathbb{C}_{[a]}$.

Let us recall some basic concepts on cyclic codes, necessary for the development of the proposed code construction. For more details, we refer to [40, 41].

Definition 1 *[40, pg. 99] The minimal polynomial of $\beta \in F_{q^m}$ over F_q, is the monic polynomial of smallest degree, $M(x)$, with coefficients from F_q such that $M(\beta) = 0$. If $\beta = \alpha^j$ for the primitive element α, the minimal polynomial of $\beta = \alpha^j$ is denoted by $M^{(j)}(x)$.*

Recall that irreducible polynomials can be derived in the following way: $x^{q^m} - x =$ product of all monic, irreducible polynomials over F_q, whose degree divides m. The concept of cyclotomic cosets will be extensively used in this paper:

Definition 2 *[40, pg. 197] The cyclotomic coset modulo n over F_q which contains s is given by $\mathbb{C}_s = \{s, sq, sq^2, sq^3, \ldots, sq^{m_s-1}\}$, where m_s is the smallest positive integer such that $sq^{m_s} \equiv s \bmod n$. If s is the smallest number in a coset, this coset is denoted by $\mathbb{C}_s$.*

The following result also will be applied in our construction:

Theorem 1 *[40, pg. 197]* $x^n - 1 = \prod_j M^{(j)}(x)$, *where $M^{(j)}(x)$ denotes the minimal polynomial of $\alpha^j \in F_{q^m}$ and j runs through the coset representatives mod n.*

Let C be a cyclic code of length n with generator polynomial $g(x)$. Then $g(x)$ is a factor of $x^n - 1$. The dimension of C equals $n - r$, where $r = \partial(g(x))$ denotes the degree of $g(x)$. The dual code $C^{\perp}$ is cyclic and has generator polynomial $g^{\perp}(x) = x^{\partial h(x)} h(x^{-1})$, where $h(x) = (x^n - 1)/g(x)$. Let us recall the concept of equivalence of codes:

Definition 3 *[41, pg. 45] Two codes C and C^* are called equivalent if they differ only in the arrangement of symbols. More precisely, if C is the row space of a matrix G, then C^* is a code equivalent to C if and only if C^* is the row space of a matrix G^* that is obtained from G by rearranging columns.*

The code having generator polynomial $h(x)$ is equivalent to the dual code $C^{\perp}$. Let us next recall the well-known BCH bound Theorem:

Theorem 2 *[40, pg. 201] (The BCH bound Theorem) Let C be a cyclic code with gener-*

ator polynomial $g(x)$ such that, for some integers $b \geq 0$ and $\delta \geq 1$, one has

$$g(\alpha^b) = g(\alpha^{b+1}) = \ldots = g(\alpha^{b+\delta-2}) = 0,$$

that is, C has a sequence of $\delta - 1$ consecutive powers of α as zeros. Then the minimum distance of C is, at least, δ.

Definition 4 *[40, pg. 202] A cyclic code of length n over F_q is a BCH code of designed distance δ if, for some integer $b \geq 0$, one has*

$$g(x) = l.c.m.\{M^{(b)}(x), M^{(b+1)}(x), \ldots, M^{(b+\delta-2)}(x)\},$$

that is, $g(x)$ is the monic polynomial of smallest degree over F_q having $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$ as zeros.

From the BCH bound theorem, the minimum distance of a BCH code is greater than or equal to its designed distance δ. The following lemma will be applied in the proposed construction:

Lemma 1 *[15, Lemmas 8 and 9] Let $n \geq 1$ be an integer and q be a power of a prime such that* $\gcd(n, q) = 1$ *and $q^{\lfloor m/2 \rfloor} < n \leq q^m - 1$, where $m =$ $ord_n(q)$ denotes the* multiplicative order *of q* modulo *n. Then the cyclotomic coset $\mathbb{C}_x = \{xq^j \ mod \ n \mid 0 \leq j < m\}$ has cardinality m for all x in the range $1 \leq x \leq nq^{\lceil m/2 \rceil}/(q^m - 1)$. Moreover, if x and y are distinct integers in the range $1 \leq x, y \leq \min\{\lfloor nq^{\lceil m/2 \rceil}/(q^m - 1) - 1 \rfloor, n - 1\}$ such that the congruence $x, y \equiv 0$ mod q does not hold, then the q-ary cyclotomic cosets of x and y modulo n are distinct.*

3 Error Model and Asymmetric Codes

In this section we recall an appropriate error model to measure the performance of a code [4, 20].

Let $\mathcal{H}$ be the Hilbert space $\mathcal{H} = \mathcal{C}^{q^n} = \mathcal{C}^q \otimes \ldots \otimes \mathcal{C}^q$, where $\mathcal{C}^q$ denotes a q-dimensional complex vector space representing the states of a quantum mechanical system. Let $|x\rangle$ be the vectors of an orthonormal basis of $\mathcal{C}^q$, where the labels x are elements of F_q.

Consider $a, b \in F_q$; the unitary operators $X(a)$ and $Z(b)$ on $\mathcal{C}^q$ are defined by $X(a)|x\rangle = |x + a\rangle$ and $Z(b)|x\rangle = w^{tr(bx)}|x\rangle$, respectively, where $w = \exp(2\pi i/p)$ is a primitive pth root of unity and tr is the trace map from F_q to the prime field F_p.

Consider that $\mathbf{a} = (a_1, \ldots, a_n) \in F_q^n$ and $\mathbf{b} = (b_1, \ldots, b_n) \in F_q^n$. Denote by $X(\mathbf{a}) = X(a_1) \otimes \ldots \otimes X(a_n)$ and $Z(\mathbf{b}) = Z(b_1) \otimes \ldots \otimes Z(b_n)$ the tensor products of n error operators. The set $\mathbf{E}_n = \{X(\mathbf{a})Z(\mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in F_q^n\}$ is a *error basis* on the complex vector space $\mathcal{C}^{q^n}$ and the set $\mathbf{G}_n = \{w^c X(\mathbf{a})Z(\mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in F_q^n, c \in F_p\}$ is the *error group* associated with $\mathbf{E}_n$. For a quantum error $\mathbf{e} = w^c X(\mathbf{a})Z(\mathbf{b}) \in \mathbf{G}_n$ the *quantum weight* $w_Q(\mathbf{e})$ of $\mathbf{e}$ is defined as $w_Q(\mathbf{e}) = \#\{i : 1 \leq i \leq n, (a_i, b_i) \neq (0, 0)\}$; the X-*weight* $w_X(\mathbf{e})$ of $\mathbf{e}$ is defined by $w_X(\mathbf{e}) = \#\{i : 1 \leq i \leq n, a_i \neq 0\}$ and the Z-*weight* $w_Z(\mathbf{e})$ of $\mathbf{e}$ by $w_Z(\mathbf{e}) = \#\{i : 1 \leq i \leq n, b_i \neq 0\}$.

In this paper we deal with the construction of several families of asymmetric quantum codes in which $p_z > p_x$, where p_x if the probability of occurrence of qudit-flip error and p_z is the probability of occurrence of phase-shift error, so $d_z > d_x$.

Definition 5 *[4, 20, 33, 34] (AQECC) A q-ary asymmetric quantum code C, denoted by $[[n, k, d_z/d_x]]_q$, is a q^k-dimensional subspace of the Hilbert space $\mathcal{C}^{q^n}$ and corrects all qudit-flip errors up to $\lfloor \frac{(d_x-1)}{2} \rfloor$ and all phase-shift errors up to $\lfloor \frac{(d_z-1)}{2} \rfloor$.*

Let us recall the well-known CSS quantum code construction:

Theorem 3 *[36, 12, 4, 20](CSS codes) Let C_1 and C_2 denote two classical linear codes with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$, respectively, and $d_x = \min\{wt(C_1 \backslash C_2), wt(C_2^{\perp} \backslash C_1^{\perp})\}$ and $d_z = \max\{wt(C_1 \backslash C_2), wt(C_2^{\perp} \backslash C_1^{\perp})\}$. If $C_2 \subset C_1$, then there exists an AQECC with parameters $[[n, K = k_1 - k_2, d_z/d_x]]_q$.*

4 Code Constructions

In this section we present the contributions of this paper. The main results are Theorems 4 and 5 and Corollary 1. They provide several families of nonbinary asymmetric quantum BCH codes. Roughly speaking, the main idea applied in Theorem 4 is as follows: the smaller the cardinality of the defining set is, the greater is its dimension. According to this idea, we need to show there exist distinct and specific singleton cyclotomic cosets contained in the defining sets of codes C_1 and C, where C is the code equivalent to the code $C_2^{\perp}$. Additionally, we need to find the cardinality of their defining sets and also we have to show that they are disjoint themselves. All these results will be shown from Lemma 2 to Lemma 7. They enable us to compute the exact dimension of the corresponding quantum code, which is a hard task, since the dimension of BCH codes are not known. In our construction we always assume that the code C_1 is used to correct phase-shift errors and the code $C_2^{\perp}$ is used to correct qudit-flip errors.

Let us recall the following lemmas shown in [26].

Lemma 2 *Let $n = q^m - 1$, where $q \geq 3$ is an odd prime power and $m \geq 3$ is an integer. Then,*

i) The cyclotomic coset $\mathbb{C}_{[\frac{q^m-1}{2}]}$ contains only one element;

ii) The coset $\mathbb{C}_{[\frac{q^m-1}{2}-1]}$ contains the element $\frac{q^m-1}{2} - q$;

iii) The coset $\mathbb{C}_{[\frac{q^m-1}{2}+1]}$ contains the element $\frac{q^m-1}{2} + q$.

Proof See [26, Lemma 3.1]. □

Lemma 3 *If $n = q^m - 1$, where $q \geq 3$ is an odd prime power and $m \geq 3$ is an integer, then the q-ary cyclotomic cosets $\mathbb{C}_1, \mathbb{C}_2, \ldots, \mathbb{C}_{q-1}, \mathbb{C}_{q+1}, \ldots, \mathbb{C}_{2q-1}$ (modulo n) are disjoint and each of them has m elements.*

Proof See [26, Lemma 3.2]. □

Lemma 4 *If $n = q^m - 1$, where $q \geq 3$ is an odd prime power and $m \geq 3$ is an integer (if $q = 3$, $m \geq 4$) then the q-ary cyclotomic cosets*

$$\mathbb{C}_0, \mathbb{C}_1, \mathbb{C}_2, \ldots, \mathbb{C}_{q-1}, \mathbb{C}_{q+1}, \ldots, \mathbb{C}_{2q-1}$$

are distinct from the q-ary cosets $\mathbb{C}_{[\frac{q^m-1}{2}+k]}$, where $k = 0, 1, \ldots, q-1$.

Proof See [26, Lemma 3.3]. □

Lemma 5 *If $n = q^m - 1$, where $q \geq 3$ is an odd prime power and $m \geq 3$ is an integer (if $q = 3$, $m \geq 4$), then the q-ary cyclotomic cosets*

$$\mathbb{C}_0, \mathbb{C}_1, \mathbb{C}_2, \ldots, \mathbb{C}_{q-1}, \mathbb{C}_{q+1}, \ldots, \mathbb{C}_{2q-1}$$

are distinct from the q-ary cosets $\mathbb{C}_{[\frac{q^m-1}{2}-k]}$, where $k = 1, \ldots, q-1$.

Proof See [26, Lemma 3.4]. □

Lemma 6 *Let $n = q^m - 1$, where $q \geq 3$ is an odd prime power and $m \geq 3$ is an integer.*

i) Each one of the q-ary cosets $\mathbb{C}_{[\frac{q^m-1}{2}+k]}$ is distinct, where $k = 1, \ldots, q-1$;

ii) Each one of the q-ary cosets $\mathbb{C}_{[\frac{q^m-1}{2}-k]}$ is distinct, where $k = 1, \ldots, q-1$;

iii) The cosets of the form $\mathbb{C}_{[\frac{q^m-1}{2}+i]}$ are distinct from each one of the cosets of the form $\mathbb{C}_{[\frac{q^m-1}{2}-j]}$, where $1 \leq i, j \leq q-1$.

Proof See [26, Lemma 3.5]. □

Lemma 7 *Let $n = q^m - 1$, where $q \geq 3$ is an odd prime power and $m \geq 3$ is an integer (if $q = 3$, $m \geq 4$). Then, each one of the q-ary cosets $\mathbb{C}_{[\frac{q^m-1}{2}+i]}$ and $\mathbb{C}_{[\frac{q^m-1}{2}-j]}$, where $1 \leq i, j \leq q-1$ has m elements.*

Proof See [26, Lemma 3.6]. □

Let us now show Theorem 4:

Theorem 4 *Let $n = q^m - 1$, where q is an odd prime power and $m \geq 3$ is an integer (if $q = 3$, $m \geq 4$). Then there exist quantum codes with parameters*

$$[[n, n - m(4q-5) - 2, d_z \geq (2q+2)/d_x \geq 2q]]_q.$$

Proof Let $C_1 = [n, k_1]_q$ be the classical BCH code generated by the product of the minimal polynomials

$$g_1(x) = M^{(0)}(x)M^{(1)}(x)\ldots M^{(q-1)}(x)M^{(q+1)}(x)\ldots M^{(2q-1)}(x),$$

and $C_2 = [n, k_2]_q$ be the cyclic code generated by the product of the minimal polynomials

$$g_2(x) = \prod_i M^{(i)}(x),$$

where each $M^{(i)}(x)$ is the minimal polynomial of α^i such that

$$i \notin \{a-q+2, \ldots, a-1, a, a+1, \ldots, a+q-1\},$$

$a = \frac{q^m-1}{2}$ and i runs through the coset representatives mod $n = q^m - 1$.

We next construct asymmetric quantum BCH codes derived from codes C_1 and C_2 by applying the CSS construction. From the BCH bound one has $d_1 \geq 2q+2$, where d_1 is the minimum distance of C_1, since the defining set of C_1 contains the sequence of $2q+1$ consecutive integers given by $0, 1, \ldots, 2q$. Similarly, the defining set of the code C generated by the polynomial $h_2(x) = (x^n - 1)/g_2(x)$ contains a sequence of $2q-1$ consecutive integers given by $a-q+2, \ldots, a-1, a, a+1, \ldots, a+q$, since, from Lemma 2, the coset $\mathbb{C}_{[\frac{q^m-1}{2}+1]}$ contains the element $\frac{q^m-1}{2}+q$. Thus, from the BCH bound, C has minimum distance greater than or equal to $2q$. Since C is equivalent to $C_2^{\perp}$, it follows that $C_2^{\perp}$ also has minimum distance greater than or equal to $2q$. Therefore, the resulting asymmetric quantum code has minimum distances $d_z \geq 2q+2$ and $d_x \geq 2q$. Furthermore, from Lemmas 4 and 5 and by construction, one has $C_2 \subsetneq C_1$.

Next, let us compute the dimension of the proposed families of CSS codes. From Lemma 3, the $(2q-2)$ q-ary cyclotomic cosets

$$\mathbb{C}_1, \mathbb{C}_2, \ldots, \mathbb{C}_{q-1}, \mathbb{C}_{q+1}, \ldots, \mathbb{C}_{2q-1}$$

(modulo n) are disjoint and each of them has m elements. Since $\mathbb{C}_0$ has only one element, the defining set of code C_1 has $2m(q-1)+1$ elements. We know that, if $i \in \mathbb{C}_s$ then one has

$$M^{(i)}(x) = \prod_{j \in \mathbb{C}_s} (x - \alpha^j), \tag{1}$$

where α is a primitive element of F_{q^m} and $M^{(i)}(x)$ denotes the minimal polynomial of the element $\alpha^i \in F_{q^m}$.

Equation (1) means that the degree of the polynomial $M^{(i)}(x)$ equals the cardinality of the coset C_s, and so the degree of the generator polynomial of a cyclic code equals the cardinality of its defining set. Hence, the dimension k_1 of code C_1 equals $k_1 = n - \partial g_1(x) = n - 2m(q-1) - 1$.

From Lemma 2, the coset $\mathbb{C}_{[\frac{q^m-1}{2}]}$ contains only one element. From Lemmas 6 and 7 the $(2q-2)$ q-ary cosets $\mathbb{C}_{[\frac{q^m-1}{2}+j]}$ and $\mathbb{C}_{[\frac{q^m-1}{2}-i]}$, where $1 \leq i, j \leq q-1$, are disjoint and each of them has m elements. Since the coset $\mathbb{C}_{[\frac{q^m-1}{2}]}$ has only one element and each one of the cosets $\mathbb{C}_{[\frac{q^m-1}{2}+j]}$ and $\mathbb{C}_{[\frac{q^m-1}{2}-i]}$, $1 \leq i, j \leq q-1$, has m elements, $m \geq 3$ ($m \geq 4$ if $q = 3$), we conclude that the coset $\mathbb{C}_{[\frac{q^m-1}{2}]}$ is disjoint of the cosets $\mathbb{C}_{[\frac{q^m-1}{2}+j]}$ and $\mathbb{C}_{[\frac{q^m-1}{2}-i]}$, $1 \leq i, j \leq q-1$. Therefore, the dimension of C_2 is given by

$$k_2 = n - \partial g_2(x) = n - [n - m(2q-3) - 1] = m(2q-3) + 1,$$

and so, the dimension of the corresponding asymmetric quantum code equals

$$k_1 - k_2 = n - 2m(q-1) - 1 - m(2q-3) - 1 = n - m(4q-5) - 2,$$

where $n = q^m - 1$.

Applying the CSS construction to C_1 and C_2 one obtains asymmetric quantum BCH codes with parameters

$$[[n, n - m(4q-5) - 2, d_z \geq (2q+2)/d_x \geq 2q]]_q,$$

as desired. □

Theorem 5 is a generalization of Theorem 4. It is one of the main results of this paper:

Theorem 5 *Let $n = q^m - 1$, where q is an odd prime power and $m \geq 3$ is an integer (if $q = 3$, $m \geq 4$). Then there exist quantum codes with parameters*

$$[[n, n - m(4q-c-5) - 2, d_z \geq (2q+2)/d_x \geq (2q-c)]]_q,$$

where $0 \leq c \leq q-2$.

Proof Let $C_1 = [n, k_1]_q$ be the BCH code generated by the product of the minimal polynomials

$$g_1(x) = M^{(0)}(x)M^{(1)}(x)\ldots M^{(q-1)}(x)M^{(q+1)}(x)\ldots M^{(2q-1)}(x),$$

and $C_2 = [n, k_2]_q$ be the cyclic code generated by the product of the minimal polynomials

$$g_2(x) = \prod_i M^{(i)}(x),$$

where each $M^{(i)}(x)$ is the minimal polynomial of α^i such that

$$i \notin \{a - q + 2 + c, \ldots, a, a + 1, \ldots, a + q - 1\},$$

$a = \frac{q^m - 1}{2}$, i runs through the coset representatives mod $n = q^m - 1$ and $0 \leq c \leq q - 2$.

By applying the BCH bound as in the proof of Theorem 4 one concludes that $d_z \geq 2q + 2$ and $d_x \geq 2q - c$ hold.

Let us now compute the dimension k_1 of C_1 and k_2 of C_2. By applying the same method shown in the proof of Theorem 4, it can be easily seen that

$$k_1 = n - 2m(q - 1) - 1$$

and

$$k_2 = n - [n - m(q - 1) - 1 - m(q - 2 - c)] = m(2q - c - 3) + 1,$$

so

$$k_1 - k_2 = n - 2m(q - 1) - 1 - m(2q - c - 3) - 1 = n - m(4q - c - 5) - 2.$$

Therefore, asymmetric quantum codes with parameters

$$[[n, n - m(4q - c - 5) - 2, d_z \geq (2q + 2)/d_x \geq (2q - c)]]_q$$

can be constructed. □

Corollary 1 *Let $n = q^m - 1$, q is an odd prime power and $m \geq 3$ is an integer. Then we have:*

i) There exist quantum codes with parameters

$$[[n, n - m(2c - l - 4) - 2, d_z \geq c/d_x \geq (c - l)]]_q,$$

where $2 \leq c \leq q$ and $0 \leq l \leq c - 2$;

ii) There exist quantum codes with parameters

$$[[n, n - m(2c - l - 6) - 2, d_z \geq c/d_x \geq (c - l)]]_q,$$

where $q + 2 < c \leq 2q$ and $0 \leq l \leq c - q - 3$;

iii) There exist quantum codes with parameters

$$[[n, n - m(4q - l - 5) - 1, d_z \geq (2q + 1)/d_x \geq (2q - l)]]_q,$$

where $0 \leq l \leq q - 2$.

Proof

Consider that $n = q^m - 1$, where n is the code-length, q is an odd prime power and $m \geq 3$ is an integer.

i) It suffices to consider C_1 as the BCH code generated by the product of the minimal polynomials

$$g_1(x) = M^{(0)}(x)M^{(1)}(x)\dots M^{(c-2)}(x),$$

and C_2 be the cyclic code generated by the product of the minimal polynomials

$$g_2(x) = \prod_i M^{(i)}(x),$$

where each $M^{(i)}(x)$ is the minimal polynomial of α^i such that $i \notin \{a, \dots, a+c-2-l\}$, $a = \frac{q^m-1}{2}$ and i runs through the coset representatives mod q^m-1. Proceeding similarly as in the proof of Theorem 4 the result follows.

ii) Let C_1 be the BCH code generated by the product of the minimal polynomials

$$g_1(x) = M^{(0)}(x)M^{(1)}(x)\dots M^{(q-1)}(x)M^{(q+1)}(x)\dots M^{(c-2)}(x),$$

and C_2 be the cyclic code generated by the product of the minimal polynomials

$$g_2(x) = \prod_i M^{(i)}(x),$$

where each $M^{(i)}(x)$ is the minimal polynomial of α^i such that $i \notin \{a-r+l, \dots, a-1, a, a+1, \dots, a+q-1\}$, $a = \frac{q^m-1}{2}$, r is an integer such that $r = c-2-q$, $0 \leq l \leq c-q-3$ and i runs through the coset representatives mod q^m-1. Proceeding similarly as in the proof of Theorem 4 the result follows.

iii) Let C_1 be the BCH code generated by the product of the minimal polynomials

$$g_1(x) = M^{(1)}(x)\dots M^{(q-1)}(x)M^{(q+1)}(x)\dots M^{(2q-1)}(x),$$

and C_2 be the cyclic code generated by the product of the minimal polynomials

$$g_2(x) = \prod_i M^{(i)}(x),$$

where each $M^{(i)}(x)$ is the minimal polynomial of α^i such that $i \notin \{a-q+2+l, \dots, a, a+1, \dots, a+q-1\}$, $a = \frac{q^m-1}{2}$ and i runs through the coset representatives mod q^m-1. Applying the CSS construction to codes C_1 and C_2 and proceeding similarly as in the proof of Theorem 4 the result follows.

□

From now on we investigate the case $m = 3$ and $q = 3$. For $q = 3$ and $n = 3^3 - 1 = 26$ the cyclotomic cosets are given by $\mathbb{C}_0 = \{0\}, \mathbb{C}_1 = \{1, 3, 9\}, \mathbb{C}_2 = \{2, 6, 18\}, \mathbb{C}_4 = \{4, 12, 10\}, \mathbb{C}_5 = \{5, 15, 19\}$, $\mathbb{C}_7 = \{7, 21, 11\}, \mathbb{C}_8 = \{8, 24, 20\}$,
$\mathbb{C}_{13} = \{13\}, \mathbb{C}_{14} = \{14, 16, 22\}, \mathbb{C}_{17} = \{17, 25, 23\}$.

Corollary 2 *There exist quantum codes with parameters*

$$[[26, 13, d_z \geq 5/d_x \geq 4]]_3,$$

$$[[26, 15, d_z \geq 5/d_x \geq 3]]_3,$$

$$[[26, 16, d_z \geq 4/d_x \geq 3]]_3.$$

Proof Consider $C_1 = [n, k_1]_3$ be the BCH code generated by the product of the minimal polynomials

$$C_1 = \langle g_1(x) \rangle = \langle M^{(0)}(x) M^{(1)}(x) M^{(2)}(x) \rangle$$

and let $C_2 = [n, k_2]_3$ be the cyclic code generated by

$$\prod_i M^{(i)}(x),$$

where each $M^{(i)}(x)$ is the minimal polynomial of α^i such that $i \notin \{5, 14\}$, and i runs through the coset representatives mod 26.

The sequence $0, 1, 2, 3$ belongs to the defining set of C_1 so, from the BCH bound, one has $d_1 \geq 5$, where d_1 is the minimum distance of C_1. Moreover, it follows that $K_1 = 19$. The sequence $14, 15, 16$ belongs to the defining set of code C which is generated by the polynomial $h_2(x) = (x^n - 1)/g_2(x)$. Since C is equivalent to $C_2^{\perp}$, by applying the BCH bound, $C_2^{\perp}$ has minimum distance $d_2^{\perp} \geq 4$. Moreover, C_2 has dimension $k_2 = 6$. Therefore, an $[[26, 13, d_z \geq 5/d_x \geq 4]]_3$ asymmetric quantum code can be constructed.

Analogously, if

$$C_1 = \langle g_1(x) \rangle = \langle M^{(0)}(x) M^{(1)}(x) M^{(2)}(x) \rangle$$

and if C_2 is the cyclic code generated by $\prod_i M^{(i)}(x)$, where each $M^{(i)}(x)$ is the minimal polynomial of α^i such that $i \notin \{13, 14\}$, and i runs through the coset representatives mod 26, an $[[26, 15, d_z \geq 5/d_x \geq 3]]_3$ asymmetric quantum BCH code is constructed.

Furthermore, if $C_1 = \langle g_1(x) \rangle = \langle M^{(1)}(x) M^{(2)}(x) \rangle$ and if C_2 is the cyclic code generated by $\prod_i M^{(i)}(x)$, where each $M^{(i)}(x)$ is the minimal polynomial of α^i such that $i \notin \{13, 14\}$, and i runs through the coset representatives mod 26, then an $[[26, 16, d_z \geq 4/d_x \geq 3]]_3$ code is generated. □

5 Examples

In this section we present illustrative examples to show how the proposed construction works.

Example **5.1** *Let C_1 be the BCH code and C_2 be the cyclic code both of length 80 over F_3, generated, respectively, by the polynomials*

$$g_1 = M^{(0)}(x) M^{(1)}(x) M^{(2)}(x) M^{(4)}(x) M^{(5)}(x),$$

and

$$g_2(x) = \prod_i M^{(i)}(x),$$

where each $M^{(i)}(x)$ is the minimal polynomial of α^i such that $i \notin \{14, 40, 41\}$, and i runs through the coset representatives mod 80.

We know that the sequence $0, 1, 2, 3, 4, 5, 6$ belongs to the defining set of C_1 so, from the BCH bound, one obtains $d_1 \geq 8$, where d_1 is the minimum distance of C_1. Analogously, the sequence $40, 41, 42, 43$ belongs to the defining set of code C which is generated by the polynomial $h_2(x) = (x^n - 1)/g_2(x)$. Since C is equivalent to $C_2^{\perp}$, from the BCH bound, $C_2^{\perp}$ has minimum distance greater than or equal to 5. The cosets of C_1 are $\mathbb{C}_0 = \{0\}, \mathbb{C}_1 = \{1, 3, 9, 27\}, \mathbb{C}_2 =$

$\{2,6,18,54\}, \mathbb{C}_4 = \{4,12,36,28\}, \mathbb{C}_5 = \{5,15,45,55\}$, *and the cosets of* C_2 *are all cyclotomic cosets except the cosets* $\mathbb{C}_{14} = \{14,42,46,58\}, \mathbb{C}_{40} = \{40\}, \mathbb{C}_{41} = \{41,43,49,67\}$.

Therefore C_1 *has dimension* $k_1 = 80-17 = 63$ *and* C_2 *has dimension* $k_2 = 80-(80-9) = 9$ *so, the dimension of this asymmetric quantum code is equal to* $k_1-k_2 = 63-9 = 54$. *Therefore, an* $[[80, 54, d_z \geq 8/d_x \geq 5]]_3$ *asymmetric quantum BCH code is constructed. Similarly, an* $[[80, 58, d_z \geq 6/d_x \geq 5]]_3$ *quantum code can be constructed, and so on.*

Example **5.2** *Let* C_1 *be the BCH code and let* C_2 *be the cyclic code, both of length* 124 *over* F_5, *generated, respectively, by the polynomials*

$$g_1(x) = M^{(0)}(x)M^{(1)}(x)M^{(2)}(x)M^{(3)}(x),$$

and

$$g_2(x) = \prod_i M^{(i)}(x),$$

where each $M^{(i)}(x)$ *is the minimal polynomial of* α^i *such that* $i \notin \{62,63,64\}$, *and* i *runs through the coset representatives mod* $n = 124$. *Proceeding similarly as above, an* $[[124, 107, d_z \geq 5/d_x \geq 4]]_5$ *asymmetric quantum code can be obtained. Analogously, an* $[[124, 110, d_z \geq 5/d_x \geq 3]]_5$ *quantum code can be constructed, and so on.*

6 Code Comparisons

In this section we compare the parameters of the asymmetric CSS codes constructed in this paper with the best asymmetric CSS codes available in [31]. For, let us recall a result shown in [31]:

Theorem 6 *[31, Theorem 8] Let* q *be a prime power and* $\gcd(q,n) = 1$, *with* $ord_n(q) = m$. *Let* C_1 *and* C_2 *be two narrow-sense BCH codes of length* $q^{\lfloor m/2 \rfloor} < n \leq q^m - 1$ *over* F_q *with designed distances* δ_1 *and* δ_2 *in the range* $2 \leq \delta_1, \delta_2 \leq \delta_{max} = \min\{\lfloor nq^{\lceil m/2 \rceil}/(q^m-1) \rfloor, n\}$ *and* $\delta_1 < \delta_2^{\perp} \leq \delta_2 < \delta_1^{\perp}$. *Assume* $S_1 \cup \ldots \cup S_{\delta_1 - 1} \neq S_1 \cup \ldots \cup S_{\delta_2 - 1}$, *then there exists an asymmetric quantum error control code with parameters*

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

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

In Table 1, the parameters of asymmetric quantum BCH codes shown in [31] are given by

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

where $d_z^* = wt(C_2 \backslash C_1^{\perp}) \geq \delta_2 > d_x^* = wt(C_1 \backslash C_2^{\perp}) \geq \delta_1$. Here, $n = q^m - 1$ is the code length, (q is an odd prime power), k^* is the code dimension and d_z^*/d_x^* are the corresponding minimum distances with respect to phase-shift and qudit-flip errors, respectively.

The new code parameters are denoted by $[[n, k, d_z \geq d/d_x \geq (d-c)]]_q$ and are given by:

- $[[n, n - m(2c - l - 4) - 2, d_z \geq c/d_x \geq (c - l)]]_q$, where $2 \leq c \leq q$ and $0 \leq l \leq c - 2$;
- $[[n, n - m(2c - l - 6) - 2, d_z \geq c/d_x \geq (c - l)]]_q$, where $q + 2 < c \leq 2q$ and $0 \leq l \leq c - q - 3$;
- $[[n, n - m(4q - l - 5) - 1, d_z \geq (2q + 1)/d_x \geq (2q - l)]]_q$, where $0 \leq l \leq q - 2$;

- $[[n, n-m(4q-l-5)-2, d_z \geq (2q+2)/d_x \geq (2q-l)]]_q$, where $0 \leq l \leq q-2$.

Here, $n = q^m - 1$ is the code length, where q is an odd prime power, k is the code dimension and d_z/d_x are the corresponding minimum distances with respect to phase-shift and qudit-flip errors, respectively.

Table 1. Quantum Code Comparison.

New asymmetric codes	Asymmetric codes shown in [31]
$[[n, k, d_z \geq d/d_x \geq (d-c)]]_q$	$[[n, k^*, d_{z^*}/d_{x^*}]]_q$
$[[26, 16, d_z \geq 4/d_x \geq 3]]_3$	$[[26, 14, d_{z^*} \geq 4/d_{x^*} \geq 3]]_3$
$[[26, 15, d_z \geq 5/d_x \geq 3]]_3$	$[[26, 11, d_{z^*} \geq 5/d_{x^*} \geq 3]]_3$
$[[26, 13, d_z \geq 5/d_x \geq 4]]_3$	$[[26, 11, d_{z^*} \geq 5/d_{x^*} \geq 4]]_3$
$[[80, 58, d_z \geq 6/d_x \geq 5]]_3$	$[[80, 52, d_{z^*} \geq 6/d_{x^*} \geq 5]]_3$
$[[80, 54, d_z \geq 8/d_x \geq 5]]_3$	$[[80, 48, d_{z^*} \geq 8/d_{x^*} \geq 5]]_3$
$[[242, 210, d_z \geq 8/d_x \geq 5]]_3$	$[[242, 202, d_{z^*} \geq 8/d_{x^*} \geq 5]]_3$
$[[242, 205, d_z \geq 8/d_x \geq 6]]_3$	$[[242, 197, d_{z^*} \geq 8/d_{x^*} \geq 6]]_3$
$[[728, 690, d_z \geq 8/d_x \geq 5]]_3$	$[[728, 680, d_{z^*} \geq 8/d_{x^*} \geq 5]]_3$
$[[728, 684, d_z \geq 8/d_x \geq 6]]_3$	$[[728, 674, d_{z^*} \geq 8/d_{x^*} \geq 6]]_3$
$[[728, 691, d_z \geq 7/d_x \geq 5]]_3$	$[[728, 686, d_{z^*} \geq 7/d_{x^*} \geq 5]]_3$
$[[124, 110, d_z \geq 5/d_x \geq 3]]_5$	$[[124, 106, d_{z^*} \geq 5/d_{x^*} \geq 3]]_5$
$[[124, 107, d_z \geq 5/d_x \geq 4]]_5$	$[[124, 103, d_{z^*} \geq 5/d_{x^*} \geq 4]]_5$
$[[124, 86, d_z \geq 10/d_x \geq 8]]_5$	$[[124, 82, d_{z^*} \geq 10/d_{x^*} \geq 8]]_5$
$[[124, 87, d_z \geq 11/d_x \geq 7]]_5$	$[[124, 85, d_{z^*} \geq 11/d_{x^*} \geq 7]]_5$
$[[124, 86, d_z \geq 12/d_x \geq 7]]_5$	$[[124, 82, d_{z^*} \geq 12/d_{x^*} \geq 7]]_5$
$[[124, 83, d_z \geq 12/d_x \geq 8]]_5$	$[[124, 79, d_{z^*} \geq 12/d_{x^*} \geq 8]]_5$
$[[124, 80, d_z \geq 12/d_x \geq 9]]_5$	$[[124, 76, d_{z^*} \geq 12/d_{x^*} \geq 9]]_5$
$[[124, 77, d_z \geq 12/d_x \geq 10]]_5$	$[[124, 73, d_{z^*} \geq 12/d_{x^*} \geq 10]]_5$
$[[624, 606, d_z \geq 5/d_x \geq 3]]_5$	$[[624, 600, d_{z^*} \geq 5/d_{x^*} \geq 3]]_5$
$[[624, 602, d_z \geq 5/d_x \geq 4]]_5$	$[[624, 596, d_{z^*} \geq 5/d_{x^*} \geq 4]]_5$
$[[624, 574, d_z \geq 10/d_x \geq 8]]_5$	$[[624, 568, d_{z^*} \geq 10/d_{x^*} \geq 8]]_5$
$[[624, 575, d_z \geq 11/d_x \geq 7]]_5$	$[[624, 572, d_{z^*} \geq 11/d_{x^*} \geq 7]]_5$
$[[624, 574, d_z \geq 12/d_x \geq 7]]_5$	$[[624, 568, d_{z^*} \geq 12/d_{x^*} \geq 7]]_5$
$[[624, 562, d_z \geq 12/d_x \geq 10]]_5$	$[[624, 556, d_{z^*} \geq 12/d_{x^*} \geq 10]]_5$
$[[342, 322, d_z \geq 7/d_x \geq 3]]_7$	$[[342, 318, d_{z^*} \geq 7/d_{x^*} \geq 3]]_7$
$[[342, 316, d_z \geq 7/d_x \geq 5]]_7$	$[[342, 312, d_{z^*} \geq 7/d_{x^*} \geq 5]]_7$
$[[342, 292, d_z \geq 12/d_x \geq 10]]_7$	$[[342, 288, d_{z^*} \geq 12/d_{x^*} \geq 10]]_7$
$[[342, 284, d_z \geq 15/d_x \geq 10]]_7$	$[[342, 282, d_{z^*} \geq 15/d_{x^*} \geq 10]]_7$
$[[342, 286, d_z \geq 16/d_x \geq 9]]_7$	$[[342, 282, d_{z^*} \geq 16/d_{x^*} \geq 9]]_7$

7 Final Remarks

We have constructed several families of asymmetric quantum BCH codes whose parameters are better than the ones available in the literature. Additionally, such codes can be applied in quantum systems where the asymmetry between qudit-flip and phase-shift errors is large.

Acknowledgment

We are indebted to the anonymous referees for their valuable comments and suggestions that helped to improve significantly the quality of this paper. We also thank one of the referees for drawing our attention to reference [27].

References

1. A. Ashikhmin and E. Knill. Non-binary quantum stabilizer codes. *IEEE Trans. Inform. Theory*, 47(7):3065–3072, November 2001.
2. J. Bierbrauer and Y. Edel. Quantum twisted codes. *J. Comb. Designs*, 8:174–188, 2000.
3. A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 78(3):405–408, January 1997.
4. 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(4):1369–1387, July 1998.
5. G.D. Cohen, S.B. Encheva, and S. Litsyn. On binary constructions of quantum codes. *IEEE Trans. Inform. Theory*, 45(7):2495–2498, July 1999.
6. M. Grassl and T. Beth. Quantum BCH codes. In *Proc. X Int. Symp. Theor. Elec. Eng.*, pages 207–212, Magdeburg, Germany, 1999. e-print `arXiv:quant-ph/9910060`.
7. M. Grassl, T. Beth, and M. Rötteler. On optimal quantum codes. *Int. J. Quan. Inform.*, 2(1):757–766, 2004.
8. M. Grassl, W. Geiselmann, and T. Beth. Quantum Reed-Solomon codes. *AAECC-13*, 1709:231–244, 1999.
9. H. Chen, S. Ling, and C. P. Xing. Quantum codes from concatenated algebraic geometric codes. *IEEE. Trans. Inform. Theory*, 51(8):2915–2920, august 2005.
10. R. Li and X. Li. Binary construction of quantum codes of minimum distance three and four. *IEEE Trans. Inform. Theory*, 50:1331–1336, June 2004.
11. P. K. Sarvepalli and A. Klappenecker. Nonbinary quantum Reed-Muller codes. In *Proc. Int. Symp. Inform. Theory (ISIT)*, 2005.
12. A. Steane. Enlargement of Calderbank-Shor-Steane quantum codes. *IEEE Trans. Inform. Theory*, 45(7):2492–2495, November 1999.
13. Z. Ma, X. Lu, K. Feng, and D. Feng. On non-binary quantum BCH codes. In J.-Y. Cai, S. Cooper, and A. Li, editors, *Theory and Applications of Models of Computation*, volume 3959 of *Lecture Notes in Computer Science*, pages 675–683. Springer Berlin / Heidelberg, 2006.
14. S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. Primitive quantum BCH codes over finite fields. In *Proc. Int. Symp. Inform. Theory (ISIT)*, pages 1114–1118, 2006.
15. A. Salah, A. Klappenecker, and P.K. Sarvepalli. On quantum and classical BCH codes. *IEEE Trans. Inform. Theory*, 53(3):1183–1188, March 2007.
16. M. Hamada. Concatenated quantum codes constructible in polynomial time: efficient decoding and error correction. *IEEE Trans. Inform. Theory*, 54(12):5689–5704, December 2008.
17. B. Sundeep and A. Thangaraj. Self-orthogonality of q-ary images of q^m-ary codes and quantum code construction. *IEEE Trans. Inform. Theory*, 53(7):2492–2495, July 2007.
18. A. Thangaraj and S. McLaughlin. Quantum codes from cyclic codes over GF(4^m). *IEEE Trans. Inform. Theory*, 47(3):1176–1178, March 2001.
19. L. Xiaoyan. Quantum cyclic and constacyclic codes. *IEEE Trans. Inform. Theory*, 50(3):547–549, March 2004.
20. A. Ketkar, A. Klappenecker, S. Kumar, and P.K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, 52(11):4892–4914, November 2006.
21. L. Zhang and I. Fuss. Quantum Reed-Muller codes. Technical report, Defence Science and Technology Organisation, Australia, 1997.
22. V. D. Tonchev. Quantum codes from caps. *Discrete Math.*, 308(24):6368–6372, December 2008.
23. J.-L. Kim and J. Walker. Nonbinary quantum error-correcting codes from algebraic curves. *Discrete Math.*, 308(14):3115–3124, July 2008.
24. R. Li and X. Li. Binary construction of quantum codes of minimum distances five and six. *Discrete Mathematics*, 308:1603–1611, 2008.
25. G. G. La Guardia. Constructions of new families of nonbinary quantum codes. *Phys. Rev. A*, 80(4):042331(1–11), October 2009.
26. G. G. La Guardia and R. Palazzo Jr. Constructions of new families of nonbinary CSS codes. *Discrete Math.*, 310(21):2935–2945, November 2010.
27. M. Hamada. Lower bounds on the quantum capacity and highest error exponent of general

memoryless channels. *IEEE Trans. Inform. Theory*, 48(9):2547–2557, September 2002.
28. L. Ioffe and M. Mezard. Asymmetric quantum error-correcting codes. *Phys. Rev. A*, 75(3):032345(1–4), March 2007.
29. 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. Technical report, e-print `arXiv:quant-ph/0709.3875`, 2007.
30. A. M. Stephens, Z. W. E. Evans, S. J. Devitt, and L. C. L. Hollenberg. Asymmetric quantum error correction via code conversion. *Phys. Rev. A*, 77(6):062335(1–5), June 2008.
31. S. A. Aly. Asymmetric quantum BCH codes. In *Proc. IEEE Int. Conference on Comput. Engineering and Systems (ICCES08)*, pages 157–162, 2008.
32. P. K. Sarvepalli, A. Klappenecker, , and M. Rötteler. Asymmetric quantum LDPC codes. In *Proc. Int. Symp. Inform. Theory (ISIT)*, pages 305–309, 2008.
33. P. K. Sarvepalli, A. Klappenecker, and M. Rötteler. Asymmetric quantum codes: constructions, bounds and performance. In *Proc. of the Royal Society A*, pages 1645–1672, 2009.
34. S. A. Aly and A. Ashikhmin. Nonbinary quantum cyclic and subsystem codes over asymmetrically-decohered quantum channels. In *Proc. Int. Symp. Inform. Theory (ISIT)*, pages 157–162, 2010.
35. A. M. Steane. Simple quantum error correcting-codes. *Phys. Rev. A*, 54:4741–4751, 1996.
36. M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
37. M. Hamada. Quotient codes and their reliability. *IPSJ Digital Courier*, 1:450–460, 2005.
38. M. Hamada. Conjugate codes and applications to cryptography. Technical report, Tamagawa University Research Institute, 2006. `http://arxiv.org/abs/quant-ph/0610193`.
39. M. Hamada. Conjugate codes for secure and reliable information transmission. In *Proc. of 2006 IEEE. Inform. Workshop (ITW'06)*, pages 149–153, 2006.
40. F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.
41. W. W. Peterson and W. J. Weldon Jr. *Error-Correcting Codes*. MIT Press, 1972.