arXiv:quant-ph/0703113v2 9 Apr 2007

Quantum Convolutional BCH Codes

Salah A. Aly[1], Markus Grassl[2], Andreas Klappenecker[1], Martin Rötteler[3], Pradeep Kiran Sarvepalli[1]
[1]Department of Computer Science, Texas A&M University, College Station, TX 77843-3112, USA
[2]Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe (TH), D-76128 Karlsruhe, Germany
[3]NEC Laboratories America, Inc., 4 Independence Way, Suite 200, Princeton, NJ 08540, USA

***Abstract*— Quantum convolutional codes can be used to protect a sequence of qubits of arbitrary length against decoherence. We introduce two new families of quantum convolutional codes. Our construction is based on an algebraic method which allows to construct classical convolutional codes from block codes, in particular BCH codes. These codes have the property that they contain their Euclidean, respectively Hermitian, dual codes. Hence, they can be used to define quantum convolutional codes by the stabilizer code construction. We compute BCH-like bounds on the free distances which can be controlled as in the case of block codes, and establish that the codes have non-catastrophic encoders.**

I. Introduction

Quantum convolutional codes provide an alternative to quantum block codes to protect quantum information for reliable quantum communication. Ollivier and Tillich launched the stabilizer framework for quantum convolutional codes [11]. Using this stabilizer framework Forney *et al.* constructed rate $(n-2)/n$ quantum convolutional codes [3]. Recently, two of us constructed quantum convolutional codes from product codes [5] and derived an algorithm to construct non-catastrophic encoders and encoder inverses [6]. In [1], a generalized Singleton bound for a class of quantum convolutional codes has been established, together with a family of codes based on generalized Reed-Solomon codes meeting this bound.

Unit memory convolutional codes are an important class of codes that appeared in a paper by Lee [10]. He also showed that these codes have large free distance d_f among other codes (multi-memory) with the same rate. Convolutional codes are often designed heuristically. However, classes of unit memory codes were constructed algebraically by Piret based on Reed-Solomon codes [12] and by Hole based on BCH codes [8]. In a recent paper, doubly-cyclic convolutional codes are investigated which include codes derived from Reed-Solomon and BCH codes [4]. These codes are related, but not identical to the codes defined in this paper.

The main results of this paper are: (a) a method to construct convolutional codes from block codes (b) a new class of convolutional stabilizer codes based on BCH codes. These codes have non-catastrophic dual encoders making it possible to derive non-catastrophic encoders for the quantum convolutional codes.

II. Background

A. Convolutional Codes

We briefly recall the basic facts about classical convolutional codes relevant for our discussion. Let $\mathbf{F}_q$ be a finite field with q elements. A *convolutional code* C of length n and dimension k over $\mathbf{F}_q$ is a free module of rank k that is a direct summand of $\mathbf{F}_q[D]^n$. A matrix G in $\mathbf{F}_q[D]^{k\times n}$ such that $C = \operatorname{im} G = \{\mathbf{u}G \mid \mathbf{u} \in \mathbf{F}_q[D]^k\}$ is called a *basic generator matrix* of C, and a matrix $H \in \mathbf{F}_q[D]^{(n-k)\times n}$ such that $C = \ker H^t = \{\mathbf{v} \mid \mathbf{v} \in \mathbf{F}_q[D]^n, \mathbf{v}H^t = 0\}$ is called a *basic parity check matrix* of C.

The existence of a convolutional code C is equivalent to the existence of four matrices $G \in \mathbf{F}_q[D]^{k\times n}$, $H \in \mathbf{F}_q[D]^{(n-k)\times n}$, $K \in \mathbf{F}_q[D]^{n\times k}$, and $L \in \mathbf{F}_q[D]^{n\times(n-k)}$ such that $C = \operatorname{im} G = \ker H^t$, $GK = 1_{\mathbf{F}_q[D]^k}$, and $L^tH^t = 1_{\mathbf{F}_q[D]^{n-k}} = HL$.

Let ν_i denote the maximum of the degrees among the polynomials in the ith row of a basic generator matrix G, and let the *memory* m be the maximal value of ν_i. A basic generator matrix of a convolutional code C is called *reduced* if the *overall constraint length* $\nu = \nu_1 + \cdots + \nu_k$ has the smallest value among all basic generator matrices of C. It is often convenient to express the generator matrix as $G = G_0 + G_1D + \cdots + G_mD^m$, where $G_i \in \mathbf{F}_q^{k\times n}$.

Let $\mathbf{F}_q((D))$ be the field of Laurent series consisting of elements of the form $v(D) = \sum_i v_iD^i$ for $v_i \in \mathbf{F}_q$ and $v_i = 0$ for $i \le r$ for some $r \in \mathbf{Z}$. We associate with a convolutional code C another module $C^\infty = \{\mathbf{u}(D)G \mid \mathbf{u}(D) \in \mathbf{F}_q((D))^k\}$, The entries of a generator matrix G of C^∞ might be rational functions. Let $\mathbf{v}(D) = (v_1(D), \ldots, v_n(D)) \in \mathbf{F}_q((D))^n$ where $v_i(D) = \sum_j v_{ij}D^j$. Then we can identify $\mathbf{v}(D)$ with an element in $\mathbf{F}_q^n((D))$ as $\sum_j \mathbf{v}_jD^j$, where $\mathbf{v}_j = (v_{1j}, \ldots, v_{nj}) \in \mathbf{F}_q^n$. We define the weight of $\mathbf{v}(D)$ as $\operatorname{wt}(\mathbf{v}(D)) = \sum_{i\in\mathbf{Z}} \operatorname{wt}(\mathbf{v}_i)$. A generator matrix G is called *catastrophic* if there exists a $\mathbf{u}(D) \in \mathbf{F}_q((D))^k$ of infinite Hamming weight such that $\mathbf{u}(D)G \in C^\infty$ has finite Hamming weight. The free distance d_f of C is defined as

$$d_f = \min\{\operatorname{wt}(\mathbf{v}(D)) \mid \mathbf{v}(D) \in C, \mathbf{v}(D) \neq 0\}. \tag{1}$$

A rate k/n convolutional code with memory m, overall constraint length ν, and free distance d_f is denoted by $(n, k, \nu; m, d_f)_q$. Sometimes a shorter notation $(n, k, \nu)_q$ is also used.

The *Euclidean inner product* of two n-tuples $\mathbf{u}(D) = \sum_i \mathbf{u}_iD^i$ and $\mathbf{v}(D) = \sum_j \mathbf{v}_iD^j$ in $\mathbf{F}_q[D]^n$ is defined as $\langle\mathbf{u}(D)|\mathbf{v}(D)\rangle = \sum_i \mathbf{u}_i \cdot \mathbf{v}_i$. The Euclidean dual of a convolutional code C is denoted by $C^\perp = \{\mathbf{u}(D) \in \mathbf{F}_q[D]^n \mid \langle\mathbf{u}(D)|\mathbf{v}(D)\rangle = 0 \text{ for all } \mathbf{v}(D) \in C\}$. Note that $H(D)$, the parity check matrix of C, *does not* generate the Euclidean dual in general. Instead, one has to reverse the order of

the coefficients of the polynomials in $H(D)$, *i.e.* consider the matrix $D^{m^\perp}H(1/D)$, where $m^\perp$ is the memory of the code generated by $H(D)$. For codes over $\mathbf{F}_{q^2}$, we define the Hermitian inner product as $\langle \mathbf{u}(D)|\mathbf{v}(D)\rangle_h = \sum_i \mathbf{u}_i \cdot \mathbf{v}_i^q$, where $\mathbf{u}_i, \mathbf{v}_i \in \mathbf{F}_{q^2}^n$ and $\mathbf{v}_i^q = (v_{1i}^q, \ldots, v_{ni}^q)$. The Hermitian dual of C is then $C^{\perp_h} = \{\mathbf{u}(D) \in \mathbf{F}_{q^2}[D]^n \mid \langle \mathbf{u}(D)|\mathbf{v}(D)\rangle_h = 0 \text{ for all } \mathbf{v}(D) \in C\}$.

B. Quantum Convolutional Codes

We briefly describe the stabilizer framework for quantum convolutional codes, see also [1], [7], [11]. The stabilizer is given by a matrix

$$S(D) = (X(D)|Z(D)) \in \mathbf{F}_q[D]^{(n-k)\times 2n}. \tag{2}$$

which satisfies the symplectic orthogonality condition $0 = X(D)Z(1/D)^t - Z(D)X(1/D)^t$. Let $\mathcal{C}$ be a quantum convolutional code defined by a stabilizer matrix as in eq. (2). Then n is called the frame size, k the number of logical qudits per frame, and k/n the rate of $\mathcal{C}$. It can be used to encode a sequence of blocks with k qudits in each block (that is, each element in the sequence consists of k quantum systems each of which is q-dimensional) into a sequence of blocks with n qudits.

The memory of the quantum convolutional code is defined as $m = \max_{1\le i\le n-k, 1\le j\le n}(\max(\deg X_{ij}(D), \deg Z_{ij}(D)))$. We use the notation $[(n,k,m)]_q$ to denote a quantum convolutional code with the above parameters. We can identify $S(D)$ with the generator matrix of a self-orthogonal classical convolutional code over $\mathbf{F}_q$ or $\mathbf{F}_{q^2}$, which gives us a means to construct convolutional stabilizer codes. Analogous to the classical codes we can define the free distance, d_f and the degree ν, prompting an extended notation $[(n,k,m;\nu,d_f)]_q$. All the parameters of the quantum convolutional code can be related to the associated classical code as the following propositions will show. For proof and further details see [1][1].

Proposition 1: Let $(n,(n-k)/2,\nu;m)_q$ be a convolutional code such that $C \le C^\perp$, where the dimension of $C^\perp$ is given by $(n+k)/2$. Then an $[(n,k,m;\nu,d_f)]_q$ convolutional stabilizer code exists whose free distance is given by $d_f = \mathrm{wt}(C^\perp \backslash C)$, which is said to be pure if $d_f = \mathrm{wt}(C^\perp)$.

Proposition 2: Let C be an $(n,(n-k)/2,\nu;m)_{q^2}$ convolutional code such that $C \subseteq C^{\perp_h}$. Then there exists an $[(n,k,m;\nu,d_f)]_q$ convolutional stabilizer code, where $d_f = \mathrm{wt}(C^{\perp_h} \setminus C)$.

III. A Construction of Convolutional Codes

In this section, we give a method to construct convolutional codes from block codes. This generalizes an earlier construction by Piret [13] to construct convolutional codes from block codes. One benefit of this method is that we can easily bound the free distance using the techniques for block codes. Another benefit is that we can derive non-catastrophic encoders.

[1]A small difference exists between the notion of memory defined here and the one used in [1].

A. Convolutional Codes from Block Codes

Given an $[n,k,d]_q$ block code with parity check matrix H, it is possible to split the matrix H into $m+1$ disjoint submatrices H_i, each of which has n columns, such that

$$H = \begin{bmatrix} H_0 \\ H_1 \\ \vdots \\ H_m \end{bmatrix}. \tag{3}$$

Then we can form the polynomial matrix

$$G(D) = \widetilde{H}_0 + \widetilde{H}_1 D + \widetilde{H}_2 D^2 + \ldots + \widetilde{H}_m D^m, \tag{4}$$

where the number of rows of $G(D)$ equals the maximal number κ of rows among the matrices H_i. The matrices $\widetilde{H}_i$ are obtained from the matrices H_i by adding zero-rows at the bottom such that the matrix $\widetilde{H}_i$ has κ rows in total. Then $G(D)$ generates a convolutional code. The fact that the H_i come from a common block code allows us to characterize the parameters of the convolutional code and its dual using the techniques of block codes. Our first result concerns a non-catastrophic encoder for the code generated by $G(D)$.

Theorem 3: Let $C \subseteq \mathbf{F}_q^n$ be an $[n,k,d]_q$ linear code with parity check matrix $H \in \mathbf{F}_q^{(n-k)\times n}$. Assume that H is partitioned into submatrices $H_0, H_1, \ldots, H_m$ as in eq. (3) such that $\kappa = \mathrm{rk}\, H_0$ and $\mathrm{rk}\, H_i \le \kappa$ for $1 \le i \le m$. Define the polynomial matrix $G(D)$ as in eq. (4). Then we have:

(a) The matrix $G(D)$ is a reduced basic generator matrix.
(b) If the code C contains its Euclidean dual $C^\perp$, respectively its Hermitian dual $C^{\perp_h}$, then the convolutional code $V = \{\mathbf{v}(D) = \mathbf{u}(D)G(D) \mid \mathbf{u}(D) \in \mathbf{F}_q^{n-k}[D]\}$ is contained in its dual $V^\perp$, respectively its Hermitian dual $V^{\perp_h}$.
(c) Let d_f and $d_f^\perp$ respectively denote the free distances of V and $V^\perp$. Let d_i be the minimum distance of the code $C_i = \{\mathbf{v} \in \mathbf{F}_q^n \mid \mathbf{v}\widetilde{H}_i^t = 0\}$, and let $d^\perp$ denote the minimum distance of $C^\perp$. Then the free distances are bounded by $\min\{d_0 + d_m, d\} \le d_f^\perp \le d$ and $d_f \ge d^\perp$.

Proof: To prove the claim (a), it suffices to show that (i) $G(0)$ has full rank κ, (ii) $(\mathrm{coeff}(G(D)_{ij}, D^{\nu_i}))_{1\le i\le\kappa, 1\le j\le n}$, has full rank κ, where for $f(D) = \sum_{i\ge 0} a_i D^i$ we define $\mathrm{coeff}(f(D), D^i) = a_i$, and (iii) $G(D)$ is non-catastrophic; cf. [12, Theorem 2.16 and Theorem 2.24].

By definition, $G(0) = \widetilde{H}_0$ has rank κ, so (i) is satisfied. Condition (ii) is satisfied, since the rows of H are linearly independent; thus, the rows of the highest degree coefficient matrix are independent as well.

It remains to prove (iii). Seeking a contradiction, we assume that the generator matrix $G(D)$ is catastrophic. Then there exists an input sequence $\mathbf{u}(D) = \sum_i \mathbf{u}_i D^i \in \mathbf{F}_q((D))^\kappa$ with infinite Hamming weight that is mapped to an output sequence $\mathbf{v}(D) = \mathbf{u}(D)G = \sum_i \mathbf{v}_i D^i \in \mathbf{F}_q((D))^n$ with finite Hamming weight, *i.e.* $\mathbf{v}_i = 0$ for all $i \ge i_0$. We have

$$\mathbf{v}_{i+m} = \mathbf{u}_{i+m}\widetilde{H}_0 + \mathbf{u}_{i+m-1}\widetilde{H}_1 + \ldots + \mathbf{u}_i \widetilde{H}_m, \tag{5}$$

where $\mathbf{v}_{i+m} \in \mathbf{F}_q^n$ and $\mathbf{u}_j \in \mathbf{F}_q^\kappa$. By construction, the vector spaces generated by the rows of the matrices H_i intersect

trivially. Hence $\mathbf{v}_i = 0$ for $i \geq i_0$ implies that $\mathbf{u}_{i-j}\widetilde{H}_j = 0$ for $j = 0, \ldots, m$. The matrix $\widetilde{H}_0$ has full rank. This implies that $\mathbf{u}_i = 0$ for $i \geq i_0$, contradicting the fact that $\mathbf{u}(D)$ has infinite Hamming weight; thus, the claim (a) holds.

To prove the claim (b), let $\mathbf{v}(D) = \sum_i \mathbf{v}_i D^i$, $\mathbf{w}(D) = \sum_i \mathbf{w}_i D^i$ be any two codewords in $V \subseteq \mathbf{F}_q^n[D]$. Then from eq. (5), we see that $\mathbf{v}_i$ and $\mathbf{w}_j$ are in the rowspan of H *i.e.* they are elements of $C^\perp$, for any $i, j \in \mathbf{Z}$. Since $C^\perp \subseteq C = (C^\perp)^\perp$, it follows that $\mathbf{v}_i \cdot \mathbf{w}_j = 0$, for any $i, j \in \mathbf{Z}$ which implies that $\langle \mathbf{v}(D) | \mathbf{w}(D) \rangle = \sum_{i \in \mathbf{Z}} \mathbf{v}_i \cdot \mathbf{w}_i = 0$. Hence $V \subseteq V^\perp$. Similarly, we can show that if $C^{\perp_h} \subseteq C$, then $V \subseteq V^{\perp_h}$.

For the claim (c), without loss of generality assume that the codeword $\mathbf{c}(D) = \sum_{i=0}^{\ell} \mathbf{c}_i D^i$ is in $V^\perp$, with $\mathbf{c}_0 \neq 0 \neq \mathbf{c}_\ell$.

It follows that $\langle D^i \mathbf{c}(D) | D^l G_j(D) \rangle = 0$ for $i, l \geq 0$, where $G_j(D)$ denotes the jth row of $G(D)$. In particular we have $\mathbf{c}_0 \widetilde{H}_m^t = 0$ and $\mathbf{c}_\ell \widetilde{H}_0^t = 0$. It follows that $\mathbf{c}_0 \in C_m$ and $\mathbf{c}_\ell \in C_0$. If $\ell > 0$, then $\mathrm{wt}(\mathbf{c}_0) \geq d_m$ and $\mathrm{wt}(\mathbf{c}_\ell) \geq d_0$ implying $\mathrm{wt}(\mathbf{c}(D)) \geq d_0 + d_m$. If $\ell = 0$, then $\langle D^i \mathbf{c}_0 | G_j(D) \rangle = 0$ implies $\mathbf{c}_0 \widetilde{H}_i^t = 0$ for $0 \leq i \leq m$, whence $\mathbf{c}_0 H^t = 0$ and $\mathbf{c}_0 \in C$, implying that $\mathrm{wt}(\mathbf{c}_0) \geq d$. It follows that $\mathrm{wt}(\mathbf{c}(D)) \geq \min\{d_0 + d_m, d\}$, giving the lower bound on $d_f^\perp$.

For the upper bound note that if $\mathbf{c}_0$ is a codeword of C, then $\mathbf{c}_0 H_i^t = 0$. From $\mathbf{c}_0$ we can construct a codeword $\mathbf{c}(D)$ by padding with zeros. Now, $\langle D^i \mathbf{c}(D) | D^l G_j(D) \rangle = 0$ and hence $\mathbf{c}(D) \in V^\perp$. Since $\mathrm{wt}(\mathbf{c}(D)) = \mathrm{wt}(\mathbf{c}_0)$ we obtain that $d_f^\perp \leq d$.

Finally, let $\mathbf{c}(D) = \sum_i \mathbf{c}_i D^i$ be a non-zero codeword in V. We saw earlier in the proof of (b) that every $\mathbf{c}_i$ is in $C^\perp$. Thus $d_f \geq \min\{\mathrm{wt}(\mathbf{c}_i) \mid \mathbf{c}_i \neq 0\} \geq d^\perp$. ∎

A special case of our claim (a) has been established by a different method in [8, Proposition 1].

IV. Convolutional BCH Codes

One of the attractive features of BCH codes is that they allow us to design codes with desired distance. There have been prior approaches to construct convolutional BCH codes, see [8], [14], and most notably [4], where one can control the free distance of the convolutional code. Here we focus on codes with unit memory. Our codes have better distance parameters as compared to Hole's construction [8] and are easier to construct compared to [14].

A. Unit Memory Convolutional BCH Codes

Let $\mathbf{F}_q$ be a finite field with q elements, n be a positive integer such that $\gcd(n, q) = 1$. Let α be a primitive nth root of unity. A BCH code C of designed distance δ and length n is a cyclic code with generator polynomial $g(x)$ in $\mathbf{F}_q[x]/\langle x^n - 1 \rangle$ whose defining set is given by $Z = C_b \cup C_{b+1} \cup \cdots \cup C_{b+\delta-2}$, where $C_x = \{xq^i \bmod n \mid i \in \mathbf{Z}, i \geq 0\}$. Let

$$H_{\delta,b} = \begin{bmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{b(n-1)} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(b+1)(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{(b+\delta-2)} & \alpha^{2(b+\delta-2)} & \cdots & \alpha^{(b+\delta-2)(n-1)} \end{bmatrix}.$$

Then $C = \{\mathbf{v} \in \mathbf{F}_q^n \mid \mathbf{v} H_{\delta,b}^t = 0\}$. If $r = \mathrm{ord}_n(q)$, then a parity check matrix H for C is given by writing every entry in the matrix $H_{\delta,b}$ as a column vector over some $\mathbf{F}_q$-basis of $\mathbf{F}_{q^r}$, and removing any dependent rows. Let $B = \{b_1, \ldots, b_r\}$ denote a basis of $\mathbf{F}_{q^r}$ over $\mathbf{F}_q$. Suppose that $\mathbf{w} = (w_1, \ldots, w_n)$ is a vector in $\mathbf{F}_{q^r}^n$, then we can write $w_j = w_{j,1} b_1 + \cdots + w_{j,r} b_r$ for $1 \leq j \leq n$. Let $\mathbf{w}^{(i)} = (w_{1,i}, \ldots, w_{n,i})$ be vectors in $\mathbf{F}_q^n$ with $1 \leq i \leq r$, For a vector $\mathbf{v}$ in $\mathbf{F}_q^n$, we have $\mathbf{v} \cdot \mathbf{w} = 0$ if and only if $\mathbf{v} \cdot \mathbf{w}^{(i)} = 0$ for all $1 \leq i \leq r$.

For a matrix M over $\mathbf{F}_{q^r}$, let $\mathrm{ex}_B(M)$ denote the matrix that is obtained by expanding each row into r rows over $\mathbf{F}_q$ with respect to the basis B, and deleting all but the first rows that generate the rowspan of the expanded matrix. Then $H = \mathrm{ex}_B(H_{\delta,b})$.

It is well known that the minimum distance of a BCH code is greater than or equal to its designed distance δ, which is very useful in constructing codes [9]. Before we can construct convolutional BCH codes we need the following result on the distance of cyclic codes.

Lemma 4: Let $\gcd(n, q) = 1$ and $2 \leq \alpha \leq \beta < n$. Let $C \subseteq \mathbf{F}_q^n$ be a cyclic code with defining set

$$Z = \{z \mid z \in C_x, \alpha \leq x \leq \beta, x \not\equiv 0 \bmod q\}. \tag{6}$$

The minimum distance $\Delta(\alpha, \beta)$ of C is lower bounded as

$$\Delta(\alpha, \beta) \geq \begin{cases} q + \lfloor (\beta - \alpha + 3)/q \rfloor - 2, & \text{if } \beta - \alpha \geq 2q - 3; \\ \lfloor (\beta - \alpha + 3)/2 \rfloor, & \text{otherwise.} \end{cases}$$

Proof: Our goal is to bound the distance of C using the Hartmann-Tzeng bound (for instance, see [9]). Suppose that there exists a such that $A = \{z, z+1, \ldots, z+a-2\} \subseteq Z$. Suppose further, that there exists b, where $\gcd(b, q) < a$ and $A + jb = \{z + jb, z + 1 + jb, \ldots, z + a - 2 + jb\} \subseteq Z$ for all $0 \leq j \leq s$. Then by [9, Theorem 4.5.6], the minimum distance of C is $\Delta(\alpha, \beta) \geq a + s$.

We choose $b = q$, so that $\gcd(n, q) = 1 < a$ is satisfied for any $a > 1$. Next we choose $A \subseteq Z$ such that $|A| = q - 1$ and $A + jb \subseteq Z$ for $0 \leq j \leq s$, with s as large as possible. Now two cases can arise. If $\beta - \alpha + 1 < 2q - 2$, then there *may not* always exist a set A such that $|A| = q - 1$. In this case we relax the constraint that $|A| = q - 1$ and choose A as the set of maximum number of consecutive elements. Then $|A| = a - 1 \geq \lfloor (\beta - \alpha + 1)/2 \rfloor$ and $s \geq 0$ giving the distance $\Delta(\alpha, \beta) \geq \lfloor (\beta - \alpha + 1)/2 \rfloor + 1 = \lfloor \beta - \alpha + 3)/2 \rfloor$.

If $(\beta - \alpha + 1) \geq 2q - 2$, then we can always choose a set $A \subseteq \{z \mid \alpha \leq z \leq \alpha + 2q - 3, z \not\equiv 0 \bmod q\}$ such that $|A| = q - 1$. As we want to make s as large as possible, the worst case arises when $A = \{\alpha + q - 1, \ldots, \alpha + 2q - 3\}$. Since $A + jb \subseteq Z$ holds for $0 \leq j \leq s$, it follows $\alpha + 2q - 3 + sq \leq \beta$. Thus $s \leq \lfloor (\beta - \alpha + 3)/q \rfloor - 2$. Thus the distance $\Delta(\alpha, \beta) \geq q + \lfloor (\alpha - \beta + 3)/q \rfloor - 2$. ∎

Theorem 5 (Convolutional BCH codes): Let n be a positive integer such that $\gcd(n, q) = 1$, $r = \mathrm{ord}_n(q)$ and $2 \leq 2\delta < \delta_{\max}$, where

$$\delta_{\max} = \left\lfloor \frac{n}{q^r - 1} (q^{\lceil r/2 \rceil} - 1 - (q - 2)[r \text{ odd}]) \right\rfloor.$$

Then there exists a unit memory rate k/n convolutional BCH code with free distance $d_f \geq \delta+1+\Delta(\delta+1, 2\delta)$ and $k = n-\kappa$, where $\kappa = r\lceil\delta(1-1/q)\rceil$. The free distance of the dual is $\geq \delta_{\max}+1$.

Proof: Let $C \subseteq \mathbf{F}_q^n$ be a narrow-sense BCH code of designed distance $2\delta+1$ and let B a basis of $\mathbf{F}_{q^r}$ over $\mathbf{F}_q$. Recall that a parity check matrix for C is given by $H = \mathrm{ex}_B(H_{2\delta+1,1})$. Further, let $H_0 = \mathrm{ex}_B(H_{\delta+1,1})$, then from

$$H_{2\delta+1,1} = \begin{bmatrix} H_{\delta+1,1} \\ H_{\delta+1,\delta+1} \end{bmatrix}, \tag{7}$$

it follows that $H = [H_0^t, H_1^t]^t$, where H_1 is obtained from $\mathrm{ex}_B(H_{\delta+1,\delta+1})$ by removing all rows common to $\mathrm{ex}_B(H_{\delta+1,1})$. The code C_0 with parity check matrix $H_0 = \mathrm{ex}_B(H_{\delta+1,1})$ coincides with the narrow-sense BCH code of length n and designed distance $\delta+1$.

By [2, Theorem 10], we have $\dim C = n - r\lceil 2\delta(1-1/q)\rceil$ and $\dim C_0 = n - r\lceil\delta(1-1/q)\rceil$ which implies $\mathrm{rk}\, H = r\lceil 2\delta(1-1/q)\rceil$, $\mathrm{rk}\, H_0 = r\lceil\delta(1-1/q)\rceil$, and $\mathrm{rk}\, H_1 = \mathrm{rk}\, H - \mathrm{rk}\, H_0 = r\lceil 2\delta(1-1/q)\rceil - r\lceil\delta(1-1/q)\rceil$. For $x > 0$, we have $\lceil x\rceil \geq \lceil 2x\rceil - \lceil x\rceil$; therefore, $\kappa = \mathrm{rk}\, H_0 \geq \mathrm{rk}\, H_1$.

By Theorem 3(a), the matrix H defines a reduced basic generator matrix

$$G(D) = \widetilde{H}_0 + D\widetilde{H}_1 \tag{8}$$

of a convolutional code of dimension κ, while its dual which we refer to as a convolutional BCH code is of dimension $n-\kappa$.

Now H_1 is the parity check matrix of a cyclic code, C_1 of the form given in Lemma 4, *i.e.* the defining set of C_1 is Z_1 as defined in (6) with $\alpha = \delta+1$ and $\beta = 2\delta$. Since H_1 is linearly independent of H_0 we have $x \not\equiv 0 \bmod q$ in the definition of Z_1.

By Theorem 3(c), the free distance of the convolutional BCH code is bounded as $\min\{d_0 + d_1, d\} \leq d_f \leq d$. By Lemma 4, $d_1 \geq \Delta(\delta+1, 2\delta)$ and by the BCH bound $d_0 \geq \delta+1$. Thus $d_f \geq \delta+1+\Delta(\delta+1, 2\delta)$. The dual free distance also follows from Theorem 3(c) as $d_f^\perp \geq d^\perp$. But $d^\perp \geq \delta_{\max}+1$ by [2, Lemma 12]. ∎

V. Constructing Quantum Convolutional Codes

Under some restrictions on the designed free distance, we can use convolutional codes derived in the previous section to construct quantum convolutional codes.

Theorem 6: Assume the same notation as in Theorem 5. Then there exists a quantum convolutional code $\mathcal{C}$ with parameters $[(n, n-2\kappa, 1)]_q$, where $\kappa = r\lceil\delta(1-1/q)\rceil$. For the free distance of $\mathcal{C}$ the bound $d_f \geq \delta+1+\Delta(\delta+1, 2\delta)$ holds and it is pure to $d' \geq \delta_{\max}+1$.

Proof: We construct a unit memory $(n, n-\kappa)_q$ classical convolutional BCH code as per Theorem 5. Its polynomial parity check matrix $G(D)$ is as given in eq. (8). Using the notation as in the proof of Theorem 5, we see that the code contains its dual if H is self-orthogonal. But given the restrictions on the designed distance, we know from [2, Theorem 3] that the BCH block code defined by H contains its dual. It follows from Theorem 3(b) that the convolutional BCH code contains its dual. From Proposition 1 we can conclude that there exists a convolutional code with the parameters $[(n, n-2\kappa, 1)]_q$. By Theorem 5 the free distance of the dual is $d' \geq \delta_{\max}+1$, also implying its purity. ∎

Another useful method to construct quantum codes makes use of codes over $\mathbf{F}_{q^2}$.

Theorem 7: Let $2 \leq 2\delta < \lfloor n(q^r-1)/(q^{2r}-1)\rfloor$, where and $r = \mathrm{ord}_n(q^2)$. Then there exist quantum convolutional codes with parameters $[(n, n-2\kappa, 1)]_q$ and free distance $d_f \geq \delta+1+\Delta(\delta+1, 2\delta)$, where $\kappa = r\lceil\delta(1-1/q^2)\rceil$.

Proof: By Theorem 5 there exists an $(n, n-\kappa, 1)_{q^2}$ convolutional BCH code with the polynomial parity check matrix as in eq. (8). The parent BCH code has design distance $2\delta+1$ and given the range of δ, we know by [2, Theorem 14] that it contains its Hermitian dual. By Theorem 3(b), the convolutional code also contains its Hermitian dual. By Proposition 2, we can conclude that there exists an $[(n, n-2\kappa, 1)]_q$ code with $d_f \geq \delta+1+\Delta(\delta+1, 2\delta)$. ∎

We conclude by noting that the convolutional codes in Theorems 6 and 7 have non-catastrophic encoders and encoder inverses. This follows directly from the fact that $G(D)$ in eq. (8) is a basic generator matrix (cf. [6], [7]).

Acknowledgment

We would like to thank one of the referees for drawing our attention to [4]. This research was supported by NSF CAREER award CCF 0347310, NSF grant CCF 0622201, and a Texas A&M TITF initiative.

References

[1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, "On quantum and classical BCH codes," in *Proc. 2007 IEEE Intl. Symp. Inform. Theory*, Nice, France, 2007, (to appear), quant-ph/701037v1.

[2] ——, "On quantum and classical BCH codes," *IEEE Trans. Inform. Theory*, vol. 53, no. 3, pp. 1183–1188, 2007.

[3] G. D. Forney, Jr., M. Grassl, and S. Guha, "Convolutional and tail-biting quantum error-correcting codes," *IEEE Trans. Inform. Theory*, vol. 53, no. 3, pp. 865–880, 2007.

[4] H. Gluesing-Luerssen and W. Schmale, "On doubly-cyclic convolutional codes," *Applicable Algebra in Engineering, Communication and Computing*, vol. 17, no. 2, pp. 151–170, 2006.

[5] M. Grassl and M. Rötteler, "Quantum block and convolutional codes from self-orthogonal product codes," in *Proc. 2005 IEEE Intl. Symp. Inform. Theory*, Adelaide, Australia, 2005, pp. 1018–1022.

[6] ——, "Non-catastrophic encoders and encoder inverses for quantum convolutional codes," in *Proc. 2006 IEEE Intl. Symp. Inform. Theory*, Seattle, USA, 2006, pp. 1109–1113.

[7] ——, "Constructions of quantum convolutional codes," in *Proc. 2007 IEEE Intl. Symp. Inform. Theory*, Nice, France, 2007, (to appear), quant-ph/0703182.

[8] K. J. Hole, "On classes of convolutional codes that are not aymptotically catastrophic," *IEEE Trans. Inform. Theory*, vol. 46, no. 2, pp. 663–669, 2000.

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

[10] L. Lee, "Short unit-memory byte-oriented binary convolutional codes having maximal free distance," *IEEE Trans. Inform. Theory*, vol. 22, no. 3, pp. 349–352, 1976.

[11] H. Ollivier and J.-P. Tillich, "Quantum convolutional codes: Fundamentals," 2004, quant-ph/0401134.

[12] P. Piret, *Convolutional Codes: An Algebraic Approach*. Cambridge, Massachusetts: The MIT Press, 1988.

[13] ——, "A convolutional equivalent to Reed-Solomon codes," *Philips J. Res.*, vol. 43, pp. 441–458, 1988.

[14] J. Rosenthal and E. York, "BCH convolutional codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 6, pp. 1833–1844, 1999.