On Classical and Quantum MDS-Convolutional BCH Codes

Giuliano Gadioli La Guardia

***Abstract*— Several new families of multi-memory classical convolutional Bose-Chaudhuri-Hocquenghem codes as well as families of unit-memory quantum convolutional codes are constructed in this paper. Our unit-memory classical and quantum convolutional codes are optimal in the sense that they attain the classical (quantum) generalized Singleton bound. The constructions presented in this paper are performed algebraically and not by computational search.**

***Index Terms*— Convolutional codes, cyclic codes, MDS codes, quantum convolutional codes.**

I. Introduction

Several works available in the literature deal with constructions of quantum error-correcting codes (QECC) [4]–[9], [13], [17], [21], [22], [24], [33], [41], [42]. In contrast with this subject of research one has the theory of quantum convolutional codes [1]–[3], [12], [14]–[16], [34], [35], [43]–[45]. Ollivier and Tillich [34], [35] were the first to develop the stabilizer structure for these codes. Almeida and Palazzo Jr. construct an $[(4, 1, 3)]$ (memory $m = 3$) quantum convolutional code [1]. Grassl and Rötteler [14]–[16] constructed quantum convolutional codes as well as they provide algorithms to obtain non-catastrophic encoders. Forney, in a joint work with Guha and Grassl, constructed rate $(n-2)/n$ quantum convolutional codes. Wilde and Brun [44], [45] constructed entanglement-assisted quantum convolutional coding and Tan and Li [43] constructed quantum convolutional codes derived from LDPC codes.

Constructions of (classical) convolutional codes and their corresponding properties as well as constructions of optimal convolutional codes (in the sense that they attain the generalized Singleton bound [38]) have been also presented in the literature [11], [18], [25], [28], [29], [36], [38]–[40]. In particular, in the paper by Rosenthal and York [39], the authors obtained some of the matrices of the state-space realization of the convolutional codes in the same way as the parity check matrix of a BCH block code, generating convolutional codes with different structures of (classical block) BCH codes. As it is well known, the generalized (classical) Singleton bound [38] (see also [40]) appears recently in the literature. In the paper by Piret [37] and even in the handbook [36], the concept of MDS convolutional codes was addressed, but in a different context that the previously mentioned. In this paper we use the notion of MDS convolutional codes according to Smarandache and Rosenthal [40].

Keeping these facts in mind, in this paper we propose constructions of new families of quantum and classical convolutional codes by applying the famous method proposed by Piret [36] and recently generalized by Aly *et al.* [2], which consists in the construction of (classical) convolutional codes derived from block codes. More precisely, we first construct new families of classical maximum-distance-separable (MDS) convolutional codes (in the sense that they attain the generalized Singleton bound [38, Theorem 2.2]) as well as new families of multi-memory convolutional codes. After these constructions, we apply the well known technique by Aly *et al.* [2, Proposition 2] in order to construct new MDS convolutional stabilizer codes (in the sense that they attain the quantum generalized Singleton bound [3, Theorem 7]) derived from their classical counterparts.

An advantage of our techniques of construction lie in the fact that all new (classical and quantum) convolutional codes are generated algebraically and not by computational search. Therefore, new families of classical and quantum optimal convolutional codes are constructed, not only specific codes, in contrast with many works where only exhaustively computational search or even specific codes are constructed.

The constructions proposed here deal with suitable properties of cyclotomic cosets, that will be specified throughout this paper. These nice properties hold when considering classical convolutional codes of length $n = q + 1$ over the field F_q for all prime power q, or even quantum convolutional codes of length $n = q^2 + 1$ over F_{q^2}, where $q = 2^t$, $t \geq 3$ is an integer. In the quantum case, the corresponding classical codes are endowed with the Hermitian inner product.

The new families of classical convolutional MDS codes constructed have parameters

- $(n, n - 2i, 2; 1, 2i + 3)_q$, where $1 \leq i \leq \frac{q}{2} - 1$, $q = 2^t$, $t \geq 3$ is an integer, $n = q+1$ is the code length, $k = n-2i$ is the code dimension, $\gamma = 2$ is the degree of the code, $m = 1$ is the memory and $d_f = 2i+3$ is the free distance of the code;
- $(n, n - 2i + 1, 2; 1, 2i + 2)_q$, where $q = p^t$, $t \geq 2$ is an integer, p is an odd prime number, $n = q + 1$ and $2 \leq i \leq \frac{n}{2} - 1$.

The multi-memory (classical) convolutional codes constructed here have parameters

Manuscript received July 12, 2011; revised August 21, 2012 and July 23, 2013; accepted August 1, 2013. Date of publication October 31, 2013; date of current version December 20, 2013. This work was supported in part by the Brazilian Agencies CAPES and in part by CNPq.

The author is with the Department of Mathematics and Statistics, State University of Ponta Grossa, Ponta Grossa 84030-900, Brazil (e-mail: gguardia@uepg.br).

Communicated by A. Ashikhmin, Associate Editor for Coding Techniques.
Digital Object Identifier 10.1109/TIT.2013.2287693

- $(n, 2r+1, 2m; m, d_f \geq n-2[r+m])_q$, where $q = p^t$, $t \geq 2$ is an integer, p is an odd prime number, $n = q+1$, r, m are integers with $r \geq 1$, $m \geq 2$ and $3 \leq r+m \leq \frac{n}{2}-1$.

The new convolutional stabilizer MDS codes have parameters

- $[(n, n-4i, 1; 2, 2i+3)]_q$, where $2 \leq i \leq \frac{q}{2}-2$, $q = 2^t$, $t \geq 3$ is an integer and $n = q^2+1$. Here, n is the frame size, $k = n-4i$ is the number of logical qudits per frame, $m = 1$ is the memory, $\gamma = 2$ is the degree and $d_f = 2i+3$ is the free distance of the code.

Note that the order between the degree and the memory are changed when comparing the parameters of classical and quantum convolutional codes. This notation is adopted to keep the same notation utilized in [2].

Let us now give the structure of the paper. In Section II, we review basic concepts on cyclic codes. In Section III, a review of concepts concerning classical and quantum convolutional codes is given. In Section IV, we propose constructions of new families of classical MDS convolutional codes as well as families of multi-memory convolutional codes. In Section V we construct new optimal (MDS) quantum convolutional codes and, in Section VI, a brief summary of this work is described.

II. Review of Cyclic Codes

Notation: Throughout this paper, p denotes a prime number, q is a prime power and F_q is a finite field with q elements. The code length is denoted by n. In this paper we always assume that gcd $(n, q) = 1$. As usual, the multiplicative order of q modulo n is given by $l = ord_n(q)$, α denotes a primitive n-th root of unity, and the minimal polynomial (over F_q) of an element $\alpha^j \in F_{q^m}$ is denoted by $M^{(j)}(x)$.

The notation $\mathcal{C}_s$ is utilized to denote a cyclotomic coset containing s, the code $C^{\perp}$ denotes the Euclidean dual and the code $C^{\perp_h}$ denotes the Hermitian dual of a given code C.

Let C be a cyclic code of length n over F_q. Then there exists only one monic polynomial $g(x)$ with minimal degree in C. Moreover, $C = \langle g(x) \rangle$, i. e., $g(x)$ is a generator polynomial of C and $g(x)$ is a factor of $x^n - 1$. The dimension of C equals $n - r$, where $r = \deg g(x)$.

Theorem 2.1 (The BCH bound) [32, pg. 201]: Let α be a primitive n-th root of unity. Let C be a cyclic code with generator polynomial $g(x)$ such that, for some integers $b \geq 0$ and $\delta \geq 1$, and for $\alpha \in F_q$, we have $g(\alpha^b) = g(\alpha^{b+1}) = \ldots = g(\alpha^{b+\delta-2}) = 0$, that is, the code has a sequence of $\delta - 1$ consecutive powers of α as zeros. Then the minimum distance of C is, at least, δ.

Definition 2.1 [32, pg. 202]: Let α be a primitive n-th root of unity and gcd $(q, n) = 1$. A cyclic code C of length n over F_q is a BCH code with designed distance δ if, for some integer $b \geq 0$, we have

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

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. Therefore, $c \in C$ if and only if $c(\alpha^b) = c(\alpha^{b+1}) = \ldots = c(\alpha^{b+\delta-2}) = 0$. Thus the code has a string of $\delta - 1$ consecutive powers of α as zeros. A parity check matrix for C is given by

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

where each entry is replaced by the corresponding column of l elements from F_q, where $l = ord_n(q)$, and then removing any linearly dependent rows. The rows of the resulting matrix over F_q are the parity checks satisfied by C.

Let $\mathcal{B} = \{b_1, \ldots, b_l\}$ be a basis of F_{q^l} over F_q. If $u = (u_1, \ldots, u_n) \in F_{q^l}^n$ then one can write the vectors u_i, $1 \leq i \leq n$, as linear combinations of the elements of $\mathcal{B}$, that is, $u_i = u_{i1}b_1 + \ldots + u_{il}b_l$. Consider that $u^{(j)} = (u_{1j}, \ldots, u_{nj})$ are vectors in F_q^n with $1 \leq j \leq l$. Then, if $v \in F_q^n$, one has $v \cdot u = 0$ if and only if $v \cdot u^{(j)} = 0$ for all $1 \leq j \leq l$.

From the BCH bound, the minimum distance of a BCH code is greater than or equal to its designed distance δ. If $n = q^l - 1$ then the BCH code is called primitive and if $b = 1$ it is called narrow-sense.

III. Review of Convolutional Codes

In this section we present a brief review of classical and quantum convolutional codes. For more details we refer the reader to [2], [3], [11], [19], [20], [36]. The following results can be found in [2], [3], [19], [20].

Recall that a polynomial encoder matrix $G(D) \in F_q[D]^{k \times n}$ is called *basic* if $G(D)$ has a polynomial right inverse. A basic generator matrix is called *reduced* (or minimal [19], [29], [40]) if the overall constraint length $\gamma = \sum_{i=1}^{k} \gamma_i$ has the smallest value among all basic generator matrices (in this case the overall constraint length γ will be called the *degree* of the resulting code).

Definition 3.1 [3]: A rate k/n *convolutional code* C with parameters $(n, k, \gamma; m, d_f)_q$ is a submodule of $F_q[D]^n$ generated by a reduced basic matrix $G(D) = (g_{ij}) \in F_q[D]^{k \times n}$, that is, $C = \{\mathbf{u}(D)G(D) | \mathbf{u}(D) \in F_q[D]^k\}$, where n is the length, k is the dimension, $\gamma = \sum_{i=1}^{k} \gamma_i$ is the *degree*, where $\gamma_i = \max_{1 \leq j \leq n}\{\deg g_{ij}\}$, $m = \max_{1 \leq i \leq k}\{\gamma_i\}$ is the *memory* and $d_f = \mathrm{wt}(C) = \min\{wt(\mathbf{v}(D)) \mid \mathbf{v}(D) \in C, \mathbf{v}(D) \neq 0\}$ is the *free distance* of the code.

In the above definition, the *weight* of an element $\mathbf{v}(D) \in F_q[D]^n$ is defined as $\mathrm{wt}(\mathbf{v}(D)) = \sum_{i=1}^{n} \mathrm{wt}(v_i(D))$, where $\mathrm{wt}(v_i(D))$ is the number of nonzero coefficients of $v_i(D)$.

If one considers the field of Laurent series $F_q((D))$ whose elements are given by $\mathbf{u}(D) = \sum_i u_i D^i$, where $u_i \in F_q$ and $u_i = 0$ for $i \leq r$, for some $r \in \mathbb{Z}$, we define the weight of $\mathbf{u}(D)$ as $\mathrm{wt}(\mathbf{u}(D)) = \sum_{\mathbb{Z}} \mathrm{wt}(u_i)$. A generator matrix $G(D)$ is called *catastrophic* if there exists a $\mathbf{u}(D)^k \in F_q((D))^k$ of infinite Hamming weight such that $\mathbf{u}(D)^k G(D)$ has finite

Hamming weight. Since a basic generator matrix is non-catastrophic, all the classical (quantum) convolutional codes constructed in this paper have non catastrophic generator matrices.

Let us recall that the Euclidean inner product of two n-tuples $\mathbf{u}(D) = \sum_i \mathbf{u}_i D^i$ and $\mathbf{v}(D) = \sum_j \mathbf{u}_j D^j$ in $F_q[D]^n$ is defined as $\langle \mathbf{u}(D) \mid \mathbf{v}(D) \rangle = \sum_i \mathbf{u}_i \cdot \mathbf{v}_i$. If C is a convolutional code then the code $C^{\perp} = \{\mathbf{u}(D) \in F_q[D]^n \mid \langle \mathbf{u}(D) \mid \mathbf{v}(D) \rangle = 0$ for all $\mathbf{v}(D) \in C\}$ denotes its Euclidean dual.

Similarly, the Hermitian inner product is defined as $\langle \mathbf{u}(D) \mid \mathbf{v}(D) \rangle_h = \sum_i \mathbf{u}_i \cdot \mathbf{v}_i^q$, where $\mathbf{u}_i, \mathbf{v}_i \in F_{q^2}^n$ and $\mathbf{v}_i^q = (v_{1i}^q, \ldots, v_{ni}^q)$. The Hermitian dual of the code C is defined by $C^{\perp_h} = \{\mathbf{u}(D) \in F_{q^2}[D]^n \mid \langle \mathbf{u}(D) \mid \mathbf{v}(D) \rangle_h = 0$ for all $\mathbf{v}(D) \in C\}$.

A. Convolutional Codes Derived from Block Codes

In this subsection we recall some results shown in [2] that will be utilized in the proposed constructions.

We consider that $[n, k, d]_q$ is a block code with parity check matrix H and then we split H into $m + 1$ disjoint submatrices H_i such that

$$H = \begin{bmatrix} H_0 \\ H_1 \\ \vdots \\ H_m \end{bmatrix}, \tag{1}$$

where each H_i has n columns, obtaining the polynomial matrix

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

where the matrices $\tilde{H}_i$, for all $1 \leq i \leq m$, are derived from the respective matrices H_i by adding zero-rows at the bottom in such a way that the matrix $\tilde{H}_i$ has κ rows in total, where κ is the maximal number of rows among the matrices H_i. As it is well known, the matrix $G(D)$ generates a convolutional code with κ rows. Note that m is the memory of the resulting convolutional code generated by the matrix $G(D)$.

Theorem 3.1 [2, Theorem 3]: Suppose that $C \subseteq F_q^n$ is a linear code with parameters $[n, k, d]_q$ and assume also that $H \in F_q^{(n-k)\times n}$ is a parity check matrix for C partitioned into submatrices $H_0, H_1, \ldots, H_m$ as in eq. (1) such that $\kappa = \text{rk} H_0$ and $\text{rk} H_i \leq \kappa$ for $1 \leq i \leq m$ and consider the polynomial matrix $G(D)$ as in eq. (2). Then we have:
(a) The matrix $G(D)$ is a reduced basic generator matrix;
(b) If $C^{\perp} \subset C$ (resp. $C^{\perp_h} \subset C$), then the convolutional code $V = \{\mathbf{v}(D) = \mathbf{u}(D)G(D) \mid \mathbf{u}(D) \in F_q^{n-k}[D]\}$ satisfies $V \subset V^{\perp}$ (resp. $V \subset V^{\perp_h}$);
(c) If d_f and $d_f^{\perp}$ denote the free distances of V and $V^{\perp}$, respectively, d_i denote the minimum distance of the code $C_i = \{\mathbf{v} \in F_q^n \mid \mathbf{v}\tilde{H}_i^t = 0\}$ and $d^{\perp}$ is the minimum distance of $C^{\perp}$, then one has $\min\{d_0 + d_m, d\} \leq d_f^{\perp} \leq d$ and $d_f \geq d^{\perp}$.

B. Review of Quantum Convolutional Codes

We begin this subsection by describing briefly the concept of quantum convolutional codes. For more details the reader can consult [35].

A quantum convolutional code is defined by means of its stabilizer which is a subgroup of the infinite version of the Pauli group, consisting of tensor products of generalized Pauli matrices acting on a semi-infinite stream of qudits. The stabilizer can be defined by a stabilizer matrix of the form

$$S(D) = (X(D) \mid Z(D)) \in F_q[D]^{(n-k)\times 2n}$$

satisfying $X(D)Z(1/D)^t - Z(D)X(1/D)^t = 0$ (symplectic orthogonality). More precisely, consider a quantum convolutional code C defined by a full-rank stabilizer matrix $S(D)$ given above. Then C is a rate k/n code with parameters $[(n, k, m; \gamma, d_f)]_q$, where n is the frame size, k is the number of logical qudits per frame, $m = \max_{1\leq i\leq n-k, 1\leq j\leq n}\{\max\{\deg X_{ij}(D), \deg Z_{ij}(D)\}\}$ is the memory, d_f is the free distance and γ is the degree of the code. Similarly as in the classical case, the constraint lengths are defined as $\gamma_i = \max_{1\leq j\leq n}\{\max\{\deg X_{ij}(D), \deg Z_{ij}(D)\}\}$, and the overall constraint length is defined as $\gamma = \sum_{i=1}^{n-k} \gamma_i$.

On the other hand, a quantum convolutional code can also be described in terms of a semi-infinite stabilizer matrix S with entries in $F_q \times F_q$ in the following way. If $S(D) = \sum_{i=0}^{m} G_i D^i$, where each matrix G_i for all $i = 0, \ldots, m$, is a matrix of size $(n-k) \times n$, then the semi-infinite matrix is defined as

$$S = \begin{bmatrix} G_0 & G_1 & \ldots & G_m & 0 & \ldots & \ldots & \ldots \\ 0 & G_0 & G_1 & \ldots & G_m & 0 & \ldots & \ldots \\ 0 & 0 & G_0 & G_1 & \ldots & G_m & 0 & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix}.$$

Next, let $\mathbb{H} = \mathbb{C}^{q^n} = \mathbb{C}^q \otimes \ldots \otimes \mathbb{C}^q$ be the Hilbert space and $|x\rangle$ be the vectors of an orthonormal basis of $\mathbb{C}^q$, where the labels x are elements of F_q. Consider $a, b \in F_q$ and take the unitary operators $X(a)$ and $Z(b)$ in $\mathbb{C}^q$ 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 p-th root of unity, p is the characteristic of F_q and tr is the trace map from F_q to F_p. Considering the *error basis* $\mathbb{E} = \{X(a), Z(b) | a, b \in F_q\}$, one defines the set P_∞ (according to [3]) as the set of all infinite tensor products of matrices $N \in \langle M \mid M \in \mathbb{E}\rangle$, in which all but finitely many tensor components are equal to I, where I is the $q \times q$ identity matrix. Then one defines the *weight* wt of $A \in P_\infty$ as its (finite) number of nonidentity tensor components. In this context, one says that a quantum convolutional code has free distance d_f if and only if it can detect all errors of weight less than d_f, but cannot detect some error of weight d_f.

The following lemma deals with the existence of convolutional stabilizer codes derived from classical convolutional codes:

Lemma 3.2 [2, Proposition 2]: Let C be an $(n, (n-k)/2, \gamma; m)_{q^2}$ convolutional code such that $C \subseteq C^{\perp_h}$. Then there exists an $[(n, k, m; \gamma, d_f)]_q$ convolutional stabilizer code, where $d_f = \text{wt}(C^{\perp_h} \backslash C)$.

In [3], the authors derived the quantum *Singleton* bound for quantum convolutional codes as it is shown in the next theorem. Let C be an $[(n, k, m; \gamma, d_f)]_q$ quantum convolutional code. Recall that C is a *pure* code if does not exist errors of weight less than d_f in the stabilizer of C.

Theorem 3.3 (Quantum Singleton bound): The free distance of an $[(n, k, m; \gamma, d_f)]_q$ F_{q^2}-linear pure convolutional stabilizer code is bounded by

$$d_f \leq \frac{n-k}{2}\left(\left\lfloor \frac{2\gamma}{n+k} \right\rfloor + 1\right) + \gamma + 1.$$

Remark 3.4: When Klappenecker *et al.* introduced the generalized quantum Singleton bound (GQSB) (see [3]) they developed an approach to convolutional stabilizer codes based on direct limit constructions. It seems that the direct limit structure behaves well with respect to the trace-alternant form. In this context they derived the GQSB. It is interesting to note that this is one of few bounds presenting in the literature concerning quantum convolutional codes.

IV. New Classical MDS-Convolutional Codes

Constructions of classical convolutional codes with good or even optimal parameters (where the latter class of codes is known as maximum-distance-separable or MDS codes, i.e., codes attaining the generalized Singleton bound according to [38]) is a difficult task [10], [18], [26]–[31], [36], [38], [40]. Due to this difficulty, most of methods available in the literature are based on computational search. Keeping in mind the discussion above, our purpose is to construct new families of classical and quantum MDS convolutional codes by applying algebraic methods.

The main results of this section are Theorem 4.2 and Theorem 4.6. They generate new families of optimal (in the sense that the codes attain the generalized Singleton bound [38]) convolutional codes of length $n = q + 1$, over F_q for all prime power q. Before proceeding further, recall the well known result from [32]:

Lemma 4.1 [32, Theorem 9, Chapter 11]: Suppose that $q = 2^t$, where $t \geq 2$ is an integer, $n = q + 1$ and consider that $a = \frac{q}{2}$. Then one has:

i) With exception of coset $\mathcal{C}_0 = \{0\}$, each one of the other q-ary cyclotomic cosets is of the form $\mathcal{C}_{a-i} = \{a-i, a+i+1\}$, where $0 \leq i \leq a-1$;

ii) The q-ary cosets $\mathcal{C}_{a-i} = \{a-i, a+i+1\}$, where $0 \leq i \leq a-1$, are mutually disjoint.

We are now able to show one of the main results of this section:

Theorem 4.2 Assume that $q = 2^t$, where $t \geq 3$ is an integer, $n = q + 1$ and consider that $a = \frac{q}{2}$. Then there exist classical MDS convolutional codes with parameters $(n, n - 2i, 2; 1, 2i + 3)_q$, where $2 \leq i \leq a - 1$.

Proof: We first note that $\gcd(n, q) = 1$ and $ord_n(q) = 2$. The proof consists of two steps. The first one is the construction of suitable BCH (block) codes and the second step is the construction of convolutional BCH codes derived from the BCH (block) codes generated in the first step.

Let us begin the first step. Let C_2 be the BCH code of length n over F_q generated by the product of the minimal polynomials

$$\begin{aligned} C_2 &= \langle g_2(x) \rangle \\ &= \langle M^{(a-i)}(x) M^{(a-i+1)}(x) \cdots M^{(a-1)}(x) M^{(a)}(x) \rangle. \end{aligned}$$

A parity check matrix of C_2 is obtained from the matrix

$$H_{2i+3,a-i} = \begin{bmatrix} 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \cdots & \alpha^{(n-1)(a-i)} \\ 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \cdots & \alpha^{(n-1)(a-i+1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ 1 & \alpha^{a} & \cdots & \cdots & \alpha^{(n-1)a} \end{bmatrix}$$

by expanding each entry as a column vector (containing 2 rows) with respect to some F_q−basis β of F_{q^2} and then removing any linearly dependent rows. This new matrix H_{C_2} is a parity check matrix of C_2 and it has $2i + 2$ rows. Since the dimension of C_2 is equal to $n - 2(i + 1)$ (as proved in the paragraph below), so there is no linearly dependent rows in H_{C_2}.

From Lemma 4.1, each one of the q-ary cyclotomic cosets $\mathcal{C}_{a-i}$, where $0 \leq i \leq a - 1$ (corresponding to the minimal polynomials $M^{(a-i)}(x)$), has two elements and they are mutually disjoint. Since the degree of the generator polynomial $g_2(x)$ of the code C_2 equals the cardinality of its defining set, then one has $\deg(g_2(x)) = 2(i + 1)$, so the dimension k_{C_2} of C_2 equals $k_{C_2} = n - \deg(g_2(x)) = n-2(i+1)$. Moreover, the defining set of the code C_2 consists of the sequence $\{a-i, a-i+1, \ldots, a, a+1, \ldots, a+i+1\}$ of $2i + 2$ consecutive integers, so, from the BCH bound, the minimum distance d_{C_2} of C_2 satisfies $d_{C_2} \geq 2i+3$. Thus, C_2 is a MDS code with parameters $[n, n-2i-2, 2i+3]_q$ and, consequently, its (Euclidean) dual code has dimension $2i+2$.

We next consider that C_1 is the BCH code of length n over F_q generated by the product of the minimal polynomials

$$\begin{aligned} C_1 &= \langle g_1(x) \rangle \\ &= \langle M^{(a-i+1)}(x) M^{(a-i+2)}(x) \cdots M^{(a-1)}(x) M^{(a)}(x) \rangle. \end{aligned}$$

Similarly, C_1 has a parity check matrix derived from the matrix

$$H_{2i+1,a-i+1} = \begin{bmatrix} 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \cdots & \alpha^{(n-1)(a-i+1)} \\ 1 & \alpha^{(a-i+2)} & \alpha^{2(a-i+2)} & \cdots & \alpha^{(n-1)(a-i+2)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ 1 & \alpha^{a} & \cdots & \cdots & \alpha^{(n-1)a} \end{bmatrix}$$

by expanding each entry as a column vector (containing 2 rows) with respect to β (already done, since $H_{2i+1,a-i+1}$ is a submatrix of $H_{2i+3,a-i}$). After performing the expansion to all entries, such new matrix is denoted by H_{C_1} (H_{C_1} is a submatrix of H_{C_2}). Applying again Lemma 4.1 and proceeding similarly as above, it follows that C_1 is a MDS code with parameters $[n, n-2i, 2i+1]_q$.

To finish the first step, consider C be the BCH code of length n over F_q generated by the minimal polynomial $M^{(a-i)}(x)$, that is,

$$C = \langle M^{(a-i)}(x) \rangle.$$

C has parameters $[n, n-2, d \geq 2]_q$. A parity check matrix H_C of C is given by expanding each entry of the matrix

$$H_{2,a-i} = \left[\, 1 \ \alpha^{(a-i)} \ \alpha^{2(a-i)} \ \cdots \ \alpha^{(n-1)(a-i)} \,\right]$$

with respect to β (already done, since $H_{2,a-i}$ is a submatrix of $H_{2i+3,a-i}$). Since C has dimension $n-2$, H_C has rank 2 (H_C is also a submatrix of H_{C_2}).

Next we describe the second step. We begin by rearranging the rows of H_{C_2} in the form

$$H = \begin{bmatrix} 1 & \alpha^{a} & \cdots & \cdots & \alpha^{(n-1)a} \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \cdots & \alpha^{(n-1)(a-i+1)} \\ 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \cdots & \alpha^{(n-1)(a-i)} \end{bmatrix},$$

(to simplify the notation we write H in terms of powers of α, although it is clear from the context that this matrix has entries in F_q, which are derived from expanding each entry with respect to the basis β already performed).

Then we split H into two disjoint submatrices H_0 and H_1 of the forms

$$H_0 = \begin{bmatrix} 1 & \alpha^{a} & \cdots & \cdots & \alpha^{(n-1)a} \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \cdots & \alpha^{(n-1)(a-i+1)} \end{bmatrix}$$

and

$$H_1 = \left[\, 1 \ \alpha^{(a-i)} \ \alpha^{2(a-i)} \ \cdots \ \alpha^{(n-1)(a-i)} \,\right],$$

respectively, where H_0 is obtained from the matrix H_{C_1} by rearranging rows and H_1 is derived from H_C also by rearranging rows. Hence it follows that $\mathrm{rk}H_0 \geq \mathrm{rk}H_1$.

Then we form the convolutional code V generated by the reduced basic (according to Theorem III-A Item (a)) generator matrix

$$G(D) = \tilde{H}_0 + \tilde{H}_1 D,$$

where $\tilde{H}_0 = H_0$ and $\tilde{H}_1$ is obtained from H_1 by adding zero-rows at the bottom such that $\tilde{H}_1$ has the number of rows of H_0 in total. By construction, V is a unit-memory convolutional code of dimension $2i$ and degree $\delta_V = 2$.

Consider next the Euclidean dual $V^{\perp}$ of the convolutional code V. We know that $V^{\perp}$ has dimension $n-2i$ and degree 2. Let us now compute the free distance $d_f^{\perp}$ of $V^{\perp}$. By Theorem 3.1 Item (c), the free distance of $V^{\perp}$ is bounded by $\min\{d_0 + d_1, d\} \leq d_f^{\perp} \leq d$, where d_i is the minimum distance of the code $C_i = \{\mathbf{v} \in F_q^n \mid \mathbf{v}\tilde{H}_i^t = 0\}$. From construction one has $d = 2i+3$, $d_0 = 2i+1$ and $d_1 \geq 2$, so $V^{\perp}$ has parameters $(n, n-2i, 2; 1, 2i+3)_q$.

Recall that the generalized (classical) Singleton bound [40] of an $(n, k, \gamma; m, d_f)_q$ convolutional code is given by

$$d_f \leq (n-k)[\lfloor \gamma/k \rfloor + 1] + \gamma + 1.$$

Replacing the values of the parameters of $V^{\perp}$ in the above inequality one concludes that $V^{\perp}$ is a MDS convolutional code and the proof is complete. ■

Remark 4.3 Note that the new codes have degree $\gamma = 2$. The reason for this is as follows: in order to obtain codes with maximum minimum distances we have to construct codes (the notation is the same utilized in Theorem 4.2) satisfying the inequalities $\min\{d_0 + d_1, d\} \leq d_f^{\perp} \leq d$. Therefore one designs the code C with parameters $[n, n-2, d_1 \geq 2]_q$. Now, it is easy to see that the corresponding convolutional code $V^{\perp}$ has degree 2.

Let us now give an illustrative example.

Example 4.1: According to Theorem 4.2, let $q = 16$, $n = q+1 = 17$ and $a = 8$. Assume C_2 is an $[17, 11, 7]_{16}$ (cyclic) MDS code generated by the product of the minimal polynomials $M^{(8)}(x)M^{(7)}(x)M^{(6)}(x)$. The corresponding cyclotomic cosets of C_2 are $\{8, 9\}$, $\{7, 10\}$ and $\{6, 11\}$. Consider C_1 be the (cyclic) MDS code generated by the product of the minimal polynomials $M^{(8)}(x)M^{(7)}(x)$; C_1 has parameters $[17, 13, 5]_{16}$. Finally, suppose C is the cyclic code generated by $M^{(6)}(x)$, where C has parameters $[17, 15, d \geq 2]_{16}$. In this case we have $i = 2$. Then we can form the convolutional code V with reduced basic generator matrix $G(D) = \tilde{H}_0 + \tilde{H}_1 D$, where $\tilde{H}_0 = H_0$ and $\tilde{H}_1$ is obtained from H_1 by adding zero-rows at the bottom such that $\tilde{H}_1$ has the number of rows of H_0 in total. The matrix H_0 is the parity check matrix of C_1 (up to permutation of rows) and H_1 is the parity check matrix of C. V has parameters $(17, 4, 2; 1, d_f)_{16}$. The Euclidean dual $V^{\perp}$ has parameters $(17, 13, 2; 1, d_f^{\perp})_{16}$, where $\min\{d_0 + d_1, d\} \leq d_f^{\perp} \leq d$, where $d_0 = 5$, $d_1 \geq 2$ and $d = 7$. Therefore $V^{\perp}$ has parameters $(17, 13, 2; 1, 7)_{16}$. Applying the generalized Singleton bound one has $7 = 4(\lfloor 2/13 \rfloor + 1) + 2 + 1$, so $V^{\perp}$ is MDS.

It is well known (see for example [38]) that if a convolutional code C is MDS then one can not guarantee that its dual also is MDS. Unfortunately in the above construction, although the codes $V^{\perp}$ are MDS, there is no guarantee that their duals V are MDS:

Corollary 4.4: Assume $q = 2^t$, where $t \geq 3$ is an integer, $n = q+1$ and consider that $a = \frac{q}{2}$. Then there exist classical convolutional codes with parameters $(n, 2i, 2; 1, d_f)_q$, where $1 \leq i \leq a-1$ and $d_f \geq n - 2i - 1$.

Proof: Consider the same construction and notation used in Theorem 4.2. We know that V has parameters $(n, 2i, 2; 1, d_f)_q$. Let us compute d_f. From Theorem 3.1 Item (b), $d_f \geq d^{\perp}$. We know that the matrix H is obtained by rearranging the rows of H_{C_2} and the code $C_2^{\perp}$ is a MDS code with parameters $[n, 2i+2, n-2i-1]_q$. Thus $d_f \geq n - 2i - 1$ and V has parameters $(n, 2i, 2; 1, d_f)_q$, where $d_f \geq n - 2i - 1$. ■

Theorem 4.6, given in the sequence, is the second main result of this section. More precisely, in such theorem, we construct new families of (classical) MDS convolutional codes over F_q for all $q = p^t$, where $t \geq 2$ and p is an odd prime number. In order to prove it, we need the following well known result:

Lemma 4.5 [32, Theorem 9, Chapter 11]: Suppose that $q = p^t$, where $t \geq 2$ is an integer and p is an odd prime number. Let $n = q + 1$ and consider that $a = \frac{n}{2}$. Then one has:

i) The q-ary coset $\mathcal{C}_a$ has only one element, i.e., $\mathcal{C}_a = \{a\}$;
ii) With exception of cosets $\mathcal{C}_0 = \{0\}$ and $\mathcal{C}_a$, each one of the other q-ary cyclotomic cosets is of the form $\mathcal{C}_{a-i} = \{a-i, a+i\}$, where $1 \leq i \leq a-1$;
iii) The q-ary cosets $\mathcal{C}_{a-i} = \{a-i, a+i\}$, where $1 \leq i \leq a-1$, are mutually disjoint and have two elements.

Let us now prove Theorem 4.6. Since its proof is analogous to that of Theorem 4.2, we only give a sketch of it.

Theorem 4.6: Assume that $q = p^t$, where $t \geq 2$ is an integer and p is an odd prime number. Consider that $n = q + 1$ and $a = \frac{n}{2}$. Then there exist classical MDS convolutional codes with parameters $(n, n-2i+1, 2; 1, 2i+2)_q$, where $2 \leq i \leq a-1$.

Proof: Let C_2 be the BCH code of length n over F_q generated by the product of the minimal polynomials

$$\begin{aligned} C_2 &= \langle g_2(x)\rangle \\ &= \langle M^{(a-i)}(x)M^{(a-i+1)}(x)\cdots M^{(a-1)}(x)M^{(a)}(x)\rangle. \end{aligned}$$

whose parity check matrix H_{C_2} is obtained from the matrix

$$H_{2i+2,a-i} = \begin{bmatrix} 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \cdots & \alpha^{(n-1)(a-i)} \\ 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \cdots & \alpha^{(n-1)(a-i+1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ 1 & \alpha^{a} & \cdots & \cdots & \alpha^{(n-1)a} \end{bmatrix}$$

by expanding each entry as a column vector over some F_q−basis β of F_{q^2} and removing one linearly dependent row, because H_{C_2} has rank $2i+1$ (computed below).

From Lemma 4.5, each one of the q-ary cyclotomic cosets $\mathcal{C}_{a-i}$, where $2 \leq i \leq a-1$, has two elements, they are mutually disjoint and the coset $\mathcal{C}_a$ has only one element. Thus the dimension k_{C_2} of C_2 equals $k_{C_2} = n - \deg(g_2(x)) = n-2i-1$. Moreover, since the defining set of the code C_2 consists of the sequence $\{a-i, a-i+1, \ldots, a, a+1, \ldots, a+i\}$ of $2i+1$ consecutive integers then the minimum distance d_{C_2} of C_2 satisfies $d_{C_2} \geq 2i+2$. Hence, C_2 is a MDS code with parameters $[n, n-2i-1, 2i+2]_q$.

We next consider C_1 as the BCH code of length n over F_q generated by the product of the minimal polynomials

$$\begin{aligned} C_1 &= \langle g_1(x)\rangle \\ &= \langle M^{(a-i+1)}(x)M^{(a-i+2)}(x)\cdots M^{(a-1)}(x)M^{(a)}(x)\rangle. \end{aligned}$$

whose parity check matrix H_{C_1} is derived from the matrix

$$H_{2i,a-i+1} = \begin{bmatrix} 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \cdots & \alpha^{(n-1)(a-i+1)} \\ 1 & \alpha^{(a-i+2)} & \alpha^{2(a-i+2)} & \cdots & \alpha^{(n-1)(a-i+2)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ 1 & \alpha^{a} & \cdots & \cdots & \alpha^{(n-1)a} \end{bmatrix}$$

by expanding each entry as a column vector with respect to β of F_{q^2}. Then it follows that C_1 is a MDS code with parameters $[n, n-2i+1, 2i]_q$ and H_{C_1} has rank $2i-1$.

Assume that C is the BCH code generated by the minimal polynomial $M^{(a-i)}(x)$. Then C has parameters $[n, n-2, d \geq 2]_q$. A parity check matrix H_C of C is given by expanding each entry of the matrix

$$H_{2,a-i} = \begin{bmatrix} 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \cdots & \alpha^{(n-1)(a-i)} \end{bmatrix}$$

with respect to β. H_C has rank 2.

Rearranging the rows of H_{C_2} we obtain the matrix

$$H = \begin{bmatrix} 1 & \alpha^{a} & \cdots & \cdots & \alpha^{(n-1)a} \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \cdots & \alpha^{(n-1)(a-i+1)} \\ 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \cdots & \alpha^{(n-1)(a-i)} \end{bmatrix},$$

where $a = \frac{n}{2}$. Next we split H into two disjoint submatrices H_0 and H_1 (as in Theorem IV) of the form

$$H_0 = \begin{bmatrix} 1 & \alpha^{a} & \cdots & \cdots & \alpha^{(n-1)a} \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \cdots & \alpha^{(n-1)(a-i+1)} \end{bmatrix}$$

and

$$H_1 = \begin{bmatrix} 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \cdots & \alpha^{(n-1)(a-i)} \end{bmatrix},$$

obtaining, in this way, the convolutional code V generated by the matrix

$$G(D) = \tilde{H}_0 + \tilde{H}_1 D$$

with parameters $(n, 2i-1, 2; 1, d_f)_q$. Proceeding similarly as in Theorem 4.2, one has a MDS convolutional code $V^{\perp}$ with parameters $(n, n-2i+1, 2; 1, 2i+2)_q$, for all $2 \leq i \leq a-1$. ∎

In the next result, we construct memory-two convolutional codes:

Theorem 4.7: Assume that $q = p^t$, where $t \geq 2$ is an integer and p is an odd prime number. Consider that $n = q+1$ and $a = \frac{n}{2}$. Then there exist convolutional codes with parameters $(n, 2i-3, 4; 2, d_f \geq n-2i)_q$, where $3 \leq i \leq a-1$.

Proof: Let C_3 be the BCH code of length n over F_q generated by the product of the minimal polynomials

$$\begin{aligned} C_3 = \langle g_3(x)\rangle = \langle M^{(a-i)}(x)M^{(a-i+1)}(x)M^{(a-i+2)}(x) \\ \cdots M^{(a-1)}(x)M^{(a)}(x)\rangle. \end{aligned}$$

whose parity check matrix H_{C_3} is obtained from the matrix

$$H_{2i+2,a-i} = \begin{bmatrix} 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \cdots & \alpha^{(n-1)(a-i)} \\ 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \cdots & \alpha^{(n-1)(a-i+1)} \\ 1 & \alpha^{(a-i+2)} & \alpha^{2(a-i+2)} & \cdots & \alpha^{(n-1)(a-i+2)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ 1 & \alpha^{a} & \cdots & \cdots & \alpha^{(n-1)a} \end{bmatrix}$$

by expanding each entry as a column vector over some F_q−basis β of F_{q^2}. We know that C_3 is a MDS code with parameters $[n, n-2i-1, 2i+2]_q$ and H_{C_3} has rank $2i+1$.

We next consider C_2 as the BCH code of length n over F_q generated by the product of the minimal polynomials

$$C_2 = \langle g_2(x) \rangle = \langle M^{(a-i+2)}(x) \cdots M^{(a-1)}(x) M^{(a)}(x) \rangle.$$

whose parity check matrix H_{C_2} is derived from the matrix

$$H_{2i-2,a-i+2} = \begin{bmatrix} 1 & \alpha^{(a-i+2)} & \alpha^{2(a-i+2)} & \cdots & \alpha^{(n-1)(a-i+2)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ 1 & \alpha^{a} & \cdots & \cdots & \alpha^{(n-1)a} \end{bmatrix}$$

by expanding each entry as a column vector with respect to β of F_{q^2}. Then it follows that C_2 is a code with parameters $[n, n-2i+3, 2i-2]_q$.

Let C_1 be the BCH code of length n over F_q generated by $M^{(a-i+1)}(x)$ whose parity check matrix H_{C_1} is given by expanding each entry of the matrix

$$H_{2,a-i+1} = \begin{bmatrix} 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \cdots & \alpha^{(n-1)(a-i+1)} \end{bmatrix}$$

with respect to β, and assume that C is the BCH code generated by the minimal polynomial $M^{(a-i)}(x)$ with parity check matrix H_C given by expanding each entry of the matrix

$$H_{2,a-i} = \begin{bmatrix} 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \cdots & \alpha^{(n-1)(a-i)} \end{bmatrix}$$

with respect to β. We know that C_1 and C has parameters $[n, n-2, d \geq 2]_q$.

Rearranging the rows of H_{C_3} we obtain the matrix

$$H = \begin{bmatrix} 1 & \alpha^{a} & \cdots & \cdots & \alpha^{(n-1)a} \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-i+2)} & \alpha^{2(a-i+2)} & \cdots & \alpha^{(n-1)(a-i+2)} \\ 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \cdots & \alpha^{(n-1)(a-i+1)} \\ 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \cdots & \alpha^{(n-1)(a-i)} \end{bmatrix}.$$

Next we split H into three disjoint submatrices H_0 and H_1 and H_2 (as in Theorem 4.2) of the form

$$H_0 = \begin{bmatrix} 1 & \alpha^{a} & \cdots & \cdots & \alpha^{(n-1)a} \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-i+2)} & \alpha^{2(a-i+2)} & \cdots & \alpha^{(n-1)(a-i+2)} \end{bmatrix},$$

$$H_1 = \begin{bmatrix} 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \cdots & \alpha^{(n-1)(a-i+1)} \end{bmatrix},$$

and

$$H_2 = \begin{bmatrix} 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \cdots & \alpha^{(n-1)(a-i)} \end{bmatrix},$$

obtaining, in this way, a memory-two convolutional code V generated by the matrix

$$G(D) = \tilde{H}_0 + \tilde{H}_1 D + \tilde{H}_2 D^2$$

with parameters $(n, 2i-3, 4; 2, d_f)_q$, where, from Item (c) of Theorem 3.1, one concludes that $d_f \geq d^{\perp} = n - 2i$. The proof is complete. ■

Theorem 4.7 can be easily generalized as one can see in the next result:

Theorem 4.8: Assume that $q = p^t$, where $t \geq 2$ is an integer and p is an odd prime number. Consider that $n = q + 1$, $a = \frac{n}{2}$ and let r, m integers with $r \geq 1$, $m \geq 2$ such that $3 \leq r + m \leq a - 1$. Then there exist convolutional codes with parameters $(n, 2r+1, 2m; m, d_f \geq n - 2[r+m])_q$.

Proof: Let C be the BCH code of length n over F_q generated by the product of the minimal polynomials

$$C = \langle g(x) \rangle = \langle M^{(a-[r+m])}(x) \cdots M^{(a-[r+1])}(x) \cdot M^{(a-r)}(x) \cdots M^{(a-1)}(x) M^{(a)}(x) \rangle.$$

whose parity check matrix H_C is obtained from the matrix

$$H_{2[r+m]+2,a-[r+m]} = \begin{bmatrix} 1 & \alpha^{(a-[r+m])} & \alpha^{2(a-[r+m])} & \cdots & \alpha^{(n-1)(a-[r+m])} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-[r+1])} & \alpha^{2(a-[r+1])} & \cdots & \alpha^{(n-1)(a-[r+1])} \\ 1 & \alpha^{(a-r)} & \alpha^{2(a-r)} & \cdots & \alpha^{(n-1)(a-r)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ 1 & \alpha^{a} & \cdots & \cdots & \alpha^{(n-1)a} \end{bmatrix}$$

by expanding each entry as a column vector over some F_q–basis β of F_{q^2}. We know that C is a MDS code with parameters $[n, n-2[r+m]-1, 2[r+m]+2]_q$

We next consider C_0 as the BCH code of length n over F_q generated by the product of the minimal polynomials

$$C_0 = \langle g_0(x) \rangle = \langle M^{(a-r)}(x) \cdots M^{(a-1)}(x) M^{(a)}(x) \rangle.$$

whose parity check matrix H_{C_0} is derived from the matrix

$$H_{2r+2,a-r} = \begin{bmatrix} 1 & \alpha^{(a-r)} & \alpha^{2(a-r)} & \cdots & \alpha^{(n-1)(a-r)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ 1 & \alpha^{a} & \cdots & \cdots & \alpha^{(n-1)a} \end{bmatrix}$$

by expanding each entry as a column vector with respect to β of F_{q^2}. We know that C_0 is a MDS code with parameters $[n, n-2r-1, 2r+2]_q$.

Let C_i for all $1 \leq i \leq m$, be the BCH code of length n over F_q generated by $M^{(a-[r+i])}(x)$ whose parity check matrix H_{C_i} is given by expanding each entry of the matrix

$$H_{2,a-[r+i]} = \begin{bmatrix} 1 & \alpha^{(a-[r+i])} & \alpha^{2(a-[r+i])} & \cdots & \alpha^{(n-1)(a-[r+i])} \end{bmatrix}$$

with respect to β. We know that C_i has parameters $[n, n-2, d \geq 2]_q$.

Proceeding similarly as in the proof of Theorem 4.7, one obtains a convolutional code V generated by the matrix

$$G(D) = \tilde{H}_0 + \tilde{H}_1 D + \tilde{H}_2 D^2 + \cdots + \tilde{H}_m D^m$$

with parameters $(n, 2r+1, 2m; m, d_f)_q$, where $d_f \geq n - 2[r+m]$. ■

Remark 4.9: It is important to observe that the procedure adopted in Theorem 4.8 has several variants and, therefore, several more new families can be constructed straightforwardly based on our method.

Remark 4.10: Unfortunately if one considers $m > 1$, there is no guarantee that the corresponding convolutional codes are MDS.

V. New Quantum MDS-Convolutional Codes

As in the classical case, the construction of MDS quantum convolutional codes is a difficult task. This task is performed in [3], [12], [14], [16] but only in [3], [14] the constructions are made algebraically. Based on this view point, we propose the construction of more MDS convolutional stabilizer codes.

It is well known that convolutional stabilizer codes can be constructed from classical convolutional codes (see for example [2, Proposition 1 and 2]). In the first construction, one utilizes convolutional codes endowed with the Euclidean inner product and in the second one, the codes are endowed with the Hermitian inner product. Considering the q-ary cosets modulo $n = q + 1$ as given in the previous section, it is easy to see that the dual-containing property with respect to the Euclidean inner product does not hold for (classical) convolutional codes derived from block codes with defining set of this type. However, when considering cyclic codes endowed with the Hermitian inner product one can show the existence of convolutional codes, derived from them, which are (Hermitian) self-orthogonal (see Lemma 5.1). This fact permits the construction of MDS quantum convolutional codes (in the sense that they attain the generalized quantum Singleton bound (Theorem 3.3) as it is shown in Theorem 5.2, given in the following. More precisely, we utilize the MDS-convolutional codes constructed in the previous section for constructing quantum MDS convolutional codes. Before proceeding further, we need the following result:

Lemma 5.1: Assume $q = 2^t$, where t is an integer such that $t \geq 1$, $n = q^2 + 1$ and let $a = \frac{q^2}{2}$. If C is the cyclic code whose defining set Z is given by $Z = \mathcal{C}_{a-i} \cup \ldots \cup \mathcal{C}_a$, where $0 \leq i \leq \frac{q}{2} - 1$, then C is Hermitian dual-containing.

Proof: See [23, Lemma 4.2]. ■

Although Theorem 5.2 is a Corollary of Theorem 4.2, we consider it as a theorem because the resulting quantum convolutional codes are MDS.

Theorem 5.2: Assume $q = 2^t$, where $t \geq 3$ is an integer, $n = q^2 + 1$ and consider that $a = \frac{q^2}{2}$. Then there exist quantum MDS convolutional codes with parameters $[(n, n - 4i, 1; 2, 2i + 3)]_q$, where $2 \leq i \leq \frac{q}{2} - 2$.

Proof: We consider the same notation utilized in Theorem 4.2. We know that $\gcd(n, q^2) = 1$. From Theorem 4.2, there exists a classical convolutional MDS code with parameters $(n, n - 2i, 2; 1, 2i + 3)_{q^2}$, for each $2 \leq i \leq \frac{q}{2} - 2$. This code is the Euclidean dual $V^{\perp}$ of the convolutional code V whose parameters are given by $(n, 2i, 2; 1, d_f)_{q^2}$. The codes $V^{\perp}$ and $V^{\perp_h}$ have the same degree as code (see the proof of Theorem 7 in [3]). Additionally, it is straightforward to check that wt($V^{\perp}$)=wt($V^{\perp_h}$), so $V^{\perp_h}$ has parameters $(n, n - 2i, 2; m^*, 2i + 3)_{q^2}$. From Lemma 5.1 and from Theorem 3.1 Item (b), one has $V \subset V^{\perp_h}$. Applying Lemma 3.2, there exists an $[(n, n - 4i, 1; 2, d_f \geq 2i + 3)]_q$ convolutional stabilizer code, for each $2 \leq i \leq \frac{q}{2} - 2$. Replacing the parameters of the previously constructed codes in the quantum generalized Singleton bound (Theorem 3.3) one has the equality $2i + 3 = 2i\left(\left\lfloor \frac{4}{2n-4i} \right\rfloor + 1\right) + 2 + 1$. Therefore, there exist MDS-convolutional stabilizer codes with parameters $[(n, n - 4i, 1; 2, 2i + 3)]_q$, for each $2 \leq i \leq \frac{q}{2} - 2$. ■

Example 5.1: To illustrate the previous construction, assume that $q = 8$, $n = 65$ and $i = 2$. Applying Theorem 5.2 there exists an $[(65, 57, 1; 2, 7)]_8$ convolutional stabilizer code that attains the generalized quantum Singleton bound.

Considering $q = 16$, $n = 257$ and $i = 2, 3, 4, 5$, one has quantum MDS codes with parameters $[(257, 249, 1; 2, 7)]_{16}$, $[(257, 245, 1; 2, 9)]_{16}$, $[(257, 241, 1; 2, 11)]_{16}$, $[(257, 237, 1; 2, 13)]_{16}$, respectively, and so on.

VI. Conclusion

In this paper we have constructed several new families of multi-memory classical convolutional BCH codes. The families of unit-memory codes are optimal in the sense that they attain the classical generalized Singleton bound. Moreover, we also have constructed families of unit-memory optimal quantum convolutional codes in the sense that these codes attain the quantum generalized Singleton bound. All the constructions presented here are performed algebraically and not by exhaustively computational search.

Acknowledgment

I would like to thank the anonymous referees and the Associate Editor Prof. Dr. A. Ashikhmin for their valuable comments and suggestions that improve significantly the quality and the presentation of this paper.

References

[1] A. C. A. de Almeida and R. Palazzo, “A concatenated [(4, 1, 3)] quantum convolutional code,” in *Proc. IEEE ITW*, Oct. 2004, pp. 28–33.

[2] S. A. Aly, M. Grassl, A. Klappenecker, M. Rötteler, and P. K. Sarvepalli, “Quantum convolutional BCH codes,” in *Proc. IEEE 10th CWIT*, Apr. 2007, pp. 180–183.

[3] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, “Quantum convolutional codes derived from Reed-Solomon and Reed-Muller codes,” in *Proc. IEEE ISIT*, Jun. 2007, pp. 821–825.

[4] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, “On quantum and classical BCH codes,” *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1183–1188, Mar. 2007.

[5] A. Ashikhmin and E. Knill, “Non-binary quantum stabilizer codes,” *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3065–3072, Nov. 2001.

[6] J. Bierbrauer and Y. Edel, “Quantum twisted codes,” *J. Combinat. Designs*, vol. 8, pp. 174–188, May 2000.

[7] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, “Quantum error correction via codes over $GF(4)$,” *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.

[8] H. Chen, S. Ling, and C. P. Xing, “Quantum codes from concatenated algebraic geometric codes,” *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2915–2920, Aug. 2005.

[9] G. D. Cohen, S. B. Encheva, and S. Litsyn, “On binary constructions of quantum codes,” *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2495–2498, Jul. 1999.

[10] J. J. Climent, V. Herranz, and C. Perea, “Linear system modelization of concatenated block and convolutional codes,” *Linear Algebra Appl.*, vol. 429, nos. 5–6, pp. 1191–1212, 2008.

[11] G. D. Forney, “Convolutional codes I: Algebraic structure,” *IEEE Trans. Inf. Theory*, vol. 16, no. 6, pp. 720–738, Nov. 1970.

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

[13] M. Grassl, T. Beth, and M. Rötteler, “On optimal quantum codes,” *Int. J. Quantum Inf.*, vol. 2, no. 1, pp. 757–766, 2004.

[14] M. Grassl and M. Rötteler, "Quantum block and convolutional codes from self-orthogonal product codes," in *Proc. IEEE ISIT*, Sep. 2005, pp. 1018–1022.
[15] M. Grassl and M. Rötteler, "Non-catastrophic encoders and encoder inverses for quantum convolutional codes," in *Proc. IEEE ISIT*, Feb. 2006, pp. 1109–1113.
[16] M. Grassl and M. Rötteler, "Constructions of quantum convolutional codes," in *Proc. IEEE ISIT*, Jun. 2007, pp. 816–820.
[17] M. Hamada, "Concatenated quantum codes constructible in polynomial time: Efficient decoding and error correction," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5689–5704, Dec. 2008.
[18] K. J. Hole, "On classes of convolutional codes that are not asymptotically catastrophic," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 663–669, Mar. 2000.
[19] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.
[20] R. Johannesson and K. S. Zigangirov, *Fundamentals of Convolutional Coding*. New York, NY, USA: Wiley, 1999.
[21] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4892–4914, Nov. 2006.
[22] G. G. La Guardia, "Constructions of new families of nonbinary quantum codes," *Phys. Rev. A*, vol. 80, no. 4, pp. 042331-1–042331-11, Oct. 2009.
[23] G. G. La Guardia, "New quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5551–5554, Aug. 2011.
[24] G. G. La Guardia and R. Palazzo, "Constructions of new families of nonbinary CSS codes," *Discrete Math.*, vol. 310, no. 21, pp. 2935–2945, Nov. 2010.
[25] L. N. Lee, "Short unit-memory byte-oriented binary convolutional codes having maximum free distance," *IEEE Trans. Inf. Theory*, vol. 22, no. 3, pp. 349–352, May 1976.
[26] H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache, "Strongly-MDS convolutional codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 584–598, Feb. 2006.
[27] H. Gluesing-Luerssen and W. Schmale, "Distance bounds for convolutional codes and some optimal codes," Ph.D. dissertation, Dept. Math., Univ. Oldenburg, Oldenburg, Germany, May 2003.
[28] H. Gluesing-Luerssen and W. Schmale, "On doubly-cyclic convolutional codes," *Appl. Algebra Eng. Commun. Comput.*, vol. 17, no. 2, pp. 151–170, 2006.
[29] H. Gluesing-Luerssen and F.-L. Tsang, "A matrix ring description for cyclic convolutional codes," *Adv. Math. Commun.*, vol. 2, no. 1, pp. 55–81, 2008.
[30] R. Hutchinson, J. Rosenthal, and R. Smarandache, "Convolutional codes with maximum distance profile," *Syst. Control Lett.*, vol. 54, no. 1, pp. 53–63, 2005.
[31] J. I. Iglesias-Curto, "Generalized AG convolutional codes," *Adv. Math. Commun.*, vol. 3, no. 4, pp. 317–328, 2009.
[32] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.
[33] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.
[34] H. Ollivier and J.-P. Tillich, "Description of a quantum convolutional code," *Phys. Rev. Lett.*, vol. 91, no. 17, pp. 1779021–1–1779021-4, 2003.
[35] H. Ollivier and J.-P. Tillich, *Quantum Convolutional Codes: Fundamentals*. Ithaca, NY, USA: Cornell Univ. Press, Jan. 2004.
[36] P. Piret, *Convolutional Codes: An Algebraic Approach*. Cambridge, MA, USA: MIT Press, 1988.
[37] P. Piret, "A convolutional equivalent to Reed-Solomon codes," *Philips J. Res.*, vol. 43, nos. 3–4, pp. 441–458, 1988.
[38] J. Rosenthal and R. Smarandache, "Maximum distance separable convolutional codes," *Appl. Algebra Eng. Commun. Comput.*, vol. 10, no. 1, pp. 15–32, 1998.
[39] J. Rosenthal and E. V. York, "BCH convolutional codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1833–1844, Sep. 1999.
[40] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal, "Constructions of MDS-convolutional codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 5, pp. 2045–2049, Jul. 2001.
[41] P. K. Sarvepalli and A. Klappenecker, "Nonbinary quantum Reed-Muller codes," in *Proc. ISIT*, 2005, pp. 1023–1027.
[42] A. Steane, "Enlargement of calderbank-shor-steane quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2492–2495, Nov. 1999.
[43] P. Tan and J. Li, "Efficient quantum stabilizer codes: LDPC and LDPC-convolutional constructions," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 476–491, Jan. 2010.
[44] M. M. Wilde and T. A. Brun, "Unified quantum convolutional coding," in *Proc. ISIT*, 2008, pp. 359–363.
[45] M. M. Wilde and T. A. Brun, "Entanglement-assisted quantum convolutional coding," *Phys. Rev. A*, vol. 81, no. 4, pp. 042333-1–042333-21, Apr. 2010.

Giuliano Gadioli La Guardia received the M.S. degree in pure mathematics in 1998 and the Ph.D. degree in electrical engineering in 2008, both from the State University of Campinas (UNICAMP), São Paulo, Brazil. Since 1999, he has been with the Department of Mathematics and Statistics, State University of Ponta Grossa, where he is an Associate Professor. His research areas include theory of classical and quantum codes, matroid theory, and error analysis.