

On Negacyclic MDS-Convolutional Codes

Giuliano G. La Guardia *

January 30, 2014

Abstract

New families of classical and quantum optimal negacyclic convolutional codes are constructed in this paper. This optimality is 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.

1 Introduction

Much effort have been paid in order to construct good quantum error-correcting codes (QECC) [4, 9, 22, 24, 25, 36, 44] as well as quantum convolutional codes with good parameters [1–3, 13–16, 27, 37, 38]. On the other hand, the investigation of the class of (classical) convolutional codes and their corresponding properties as well as constructions of maximum-distance-separable (MDS) convolutional codes (i.e., codes attaining the generalized Singleton bound [41]) have also been presented in the literature [11, 12, 17, 26–34, 39, 41–43].

In this paper, we utilize the class of negacyclic codes [5–8, 10, 23] in order to construct classical and quantum MDS convolutional codes. More precisely, we apply the famous method proposed by Piret [39] (generalized recently by Aly *et al.* [2]), which consists in the construction of (classical) convolutional codes derived from block codes. 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, in contrast with many works where only exhaustively computational search or even specific codes are constructed.

Our classical convolutional MDS codes constructed here have parameters

- $(n, n - 2i + 1, 2; 1, 2i + 2)_{q^2}$, where $q \equiv 1 \pmod{4}$ is a power of an odd prime, $n = q^2 + 1$ and $2 \leq i \leq n/2 - 1$;
- $(n, n - 2i + 2, 2; 1, 2i + 1)_{q^2}$, where q is a power of an odd prime, $n = (q^2 + 1)/2$ and $2 \leq i \leq (n - 1)/2$;

*Giuliano Gadioli La Guardia is with Department of Mathematics and Statistics, State University of Ponta Grossa (UEPG), 84030-900, Ponta Grossa, PR, Brazil.

- $(n, n - 2i + 1, 2; 1, 2i + 2)_{q^2}$, where $q \geq 5$ is a power of an odd prime, $n = (q^2 + 1)/2$ and $2 \leq i \leq (n - 1)/2 - 1$.

The new convolutional stabilizer MDS codes have parameters

- $[(n, n - 4i + 2, 1; 2, 2i + 2)]_q$, where $q \equiv 1 \pmod{4}$ is a power of an odd prime, $n = q^2 + 1$ and $2 \leq i \leq (q - 1)/2$;
- $[(n, n - 4i + 4, 1; 2, 2i + 1)]_q$, where $q \geq 7$ is a power of an odd prime, $n = (q^2 + 1)/2$ and $2 \leq i \leq (q - 1)/2$.

We observe that the order between the degree and the memory are changed when comparing the parameters of classical and quantum convolutional codes. We adopt this notation to keep the same notation utilized in [2].

The paper is organized as follows. In Sections 2 we review basic concepts on negacyclic codes. In Sections 3 and 4, we review of concepts concerning classical and quantum convolutional codes, respectively. In Section 5, we propose constructions of new families of classical MDS convolutional derived from negacyclic codes. In Section 6 we construct new optimal (MDS) quantum convolutional codes and, in Section 7, a brief summary of this work is described.

2 Negacyclic codes

The class of negacyclic codes [5–8, 10, 21, 23] have been studied in the literature. This class of codes are a particular class of a more general class of constacyclic codes [8]. In this section we review the basic concepts of these codes.

Throughout this paper, we always assume that q is a power of an odd prime, \mathbb{F}_q is a finite field with q elements and n is a positive integer with $\gcd(n, q) = 1$. Analogously to cyclic codes, if we consider the quotient ring $R_n = \mathbb{F}_q/(x^n + 1)$, then a negacyclic code is a principal ideal of R_n under the usual correspondence $\mathbf{c} = (c_0, c_1, \dots, c_{n-1}) \longrightarrow c_0 + c_1x + \dots + c_{n-1}x^{n-1} \pmod{(x^n + 1)}$. The generator polynomial $g(x)$ of a negacyclic code C satisfies $g(x)|(x^n + 1)$. The roots of $(x^n + 1)$ are the roots of $(x^{2n} - 1)$ which are not roots of $(x^n - 1)$ in some extension field of \mathbb{F}_{q^2} (since we will work with codes endowed with the Hermitian inner product).

Consider that $m = \text{ord}_{2n}(q^2)$ and let β be a primitive $2n$ th root of unity in $\mathbb{F}_{q^{2m}}$ (so $\alpha = \beta^2 \in \mathbb{F}_{q^{2m}}$ is a primitive n th root of unity). Then the roots of $x^n + 1$ are given by β^{2i+1} $0 \leq i \leq n - 1$. Put $\mathbb{O}_{2n} = \{1, 3, \dots, 2n - 1\}$; the defining set of a negacyclic code C of length n generated by $g(x)$ is given by $\mathcal{Z} = \{i \in \mathbb{O}_{2n} | \beta^i \text{ is root of } g(x)\}$. The defining set is a union of q^2 -ary cyclotomic cosets given by $\mathcal{C}_i = \{i, iq^2, \dots, iq^{2(m_i-1)}\}$, where m_i is the smallest positive integer such that $iq^{2(m_i)} \equiv i \pmod{2n}$. The minimal polynomial (over \mathbb{F}_{q^2}) of $\beta^j \in \mathbb{F}_{q^{2m}}$ is denoted by $M^{(j)}(x)$ and it is given by $M^{(j)}(x) = \prod_{j \in \mathcal{C}_i} (x - \beta^j)$.

The dimension of C is given by $n - |\mathcal{Z}|$. The BCH bound for Constacyclic codes (see [5, 23]) asserts that C is a q^2 -ary negacyclic code of length n with

generator polynomial $g(x)$ and if $g(x)$ has the elements $\{\beta^{2i+1} | 0 \leq i \leq d-2\}$ as roots, where β is a primitive $2n$ th root of unity, then the minimum distance d_C of C satisfies $d_C \geq d$.

3 Classical Convolutional Codes

The class of (classical) convolutional codes is a well-studied class of codes [2, 3, 12, 18, 19, 39]. We assume the reader is familiar with the theory of convolutional codes. For more details, see [19]. Recall that a polynomial encoder matrix $G(D) = (g_{ij}) \in \mathbb{F}_q[D]^{k \times n}$ is called *basic* if $G(D)$ has a polynomial right inverse. A basic generator matrix is called *reduced* (or minimal [18, 32, 43]) if the overall constraint length $\gamma = \sum_{i=1}^k \gamma_i$, where $\gamma_i = \max_{1 \leq j \leq n} \{\deg g_{ij}\}$, 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 $(n, k, \gamma; \mu, d_f)_q$ is a submodule of $\mathbb{F}_q[D]^n$ generated by a reduced basic matrix $G(D) = (g_{ij}) \in \mathbb{F}_q[D]^{k \times n}$, that is, $C = \{\mathbf{u}(D)G(D) | \mathbf{u}(D) \in \mathbb{F}_q[D]^k\}$, where n is the length, k is the dimension, $\gamma = \sum_{i=1}^k \gamma_i$ is the degree, $\mu = \max_{1 \leq i \leq k} \{\gamma_i\}$ is the memory and $d_f = wt(C) = \min\{wt(\mathbf{v}(D)) | \mathbf{v}(D) \in C, \mathbf{v}(D) \neq 0\}$ is the free distance of the code.*

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

Let C an $[n, k, d]_q$ block code with parity check matrix H . We split H into

$\mu + 1$ disjoint submatrices H_i such that $H = \begin{bmatrix} H_0 \\ H_1 \\ \vdots \\ H_\mu \end{bmatrix}$, where each H_i has n

columns, obtaining the polynomial matrix $G(D) = \tilde{H}_0 + \tilde{H}_1 D + \tilde{H}_2 D^2 + \dots + \tilde{H}_\mu D^\mu$, where the matrices \tilde{H}_i , for all $1 \leq i \leq \mu$, 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. Note that μ is the memory of the resulting convolutional code generated by the matrix $G(D)$.

Theorem 3.1 [2, Theorem 3] *Let $C \subseteq \mathbb{F}_q^n$ be a linear code with parameters $[n, k, d]_q$ and assume also that $H \in \mathbb{F}_q^{(n-k) \times n}$ is a parity check matrix for C partitioned into submatrices H_0, H_1, \dots, H_μ as above such that $\kappa = rkH_0$ and*

$rkH_i \leq \kappa$ for $1 \leq i \leq \mu$ and consider the polynomial matrix $G(D)$ as given above. 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 $V = \{\mathbf{v}(D) = \mathbf{u}(D)G(D) \mid \mathbf{u}(D) \in \mathbb{F}_q^{n-k}[D]\}$ 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 $C_i = \{\mathbf{v} \in \mathbb{F}_q^n \mid \mathbf{v}\tilde{H}_i^t = 0\}$ and d^\perp is the minimum distance of C^\perp , then one has $\min\{d_0 + d_\mu, d\} \leq d_f^\perp \leq d$ and $d_f \geq d^\perp$.

Recall that the (classical) generalized Singleton bound [41, Theorem 2.2] of an $(n, k, \gamma; \mu, d_f)_q$ convolutional code is given by

$$d_f \leq (n - k)[\lceil \gamma/k \rceil + 1] + \gamma + 1 \quad (1)$$

If the parameters of a convolutional code C satisfies (1) with equality then C is said maximum-distance-separable (MDS).

4 Quantum Convolutional Codes

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

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

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 $[(n, k, \mu; \gamma, d_f)]_q$, where n is the frame size, k is the number of logical qudits per frame, $\mu = \max_{1 \leq i \leq n-k, 1 \leq j \leq n} \{\max\{\deg X_{ij}(D), \deg Z_{ij}(D)\}\}$ 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

$$\gamma = \sum_{i=1}^{n-k} \gamma_i.$$

Next, let $\mathbb{H} = \mathbb{C}^{q^n} = \mathbb{C}^q \otimes \dots \otimes \mathbb{C}^q$ 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 \mathbb{F}_q . Consider $a, b \in \mathbb{F}_q$ 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 \mathbb{F}_q and tr is the trace map from \mathbb{F}_q to \mathbb{F}_p . Considering the *error basis* $\mathbb{E} = \{X(a), Z(b) \mid a, b \in \mathbb{F}_q\}$, 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 code C is *pure* if does not exist errors of weight less than d_f in the stabilizer of C .

5 The New Convolutional MDS Codes

In this section we propose the construction of new classical convolutional codes. In order to proceed further, let us recall some results shown in the literature:

Lemma 5.1 [20, Lemma 4.1] *Let $n = q^2 + 1$, where $q \equiv 1 \pmod{4}$ is a power of an odd prime and suppose that $s = n/2$. Then the q^2 -ary cosets modulo $2n$ are given by: $C_s = \{s\}$, $C_{3s} = \{3s\}$ and $C_{s-2i} = \{s - 2i, s + 2i\}$, where $1 \leq i \leq s - 1$.*

Lemma 5.2 [20, Lemma 4.4] *Let $n = (q^2 + 1)/2$, where q is a power of an odd prime. Then the q^2 -ary cosets modulo $2n$ containing all odd integers from 1 to $2n - 1$ are given by: $C_n = \{n\}$, and $C_{2i-1} = \{2i - 1, 1 - 2i\}$, where $1 \leq i \leq (n - 1)/2$.*

Recall the concept of negacyclic BCH codes:

Definition 5.1 (Negacyclic BCH codes) *Let q be a power of an odd prime with $\gcd(n, q) = 1$. Let β be a primitive $2n$ th root of unity in \mathbb{F}_{q^m} . A negacyclic code C of length n over \mathbb{F}_q is a BCH code with designed distance δ if, for some odd integer $b \geq 1$, we have*

$$g(x) = \text{lcm}\{M^{(b)}(x), M^{(b+2)}(x), \dots, M^{[b+2(\delta-2)]}(x)\},$$

i.e., $g(x)$ is the monic polynomial of smallest degree over \mathbb{F}_q having $\alpha^b, \alpha^{b+2}, \dots, \alpha^{[b+2(\delta-2)]}$ as zeros. Therefore, $c \in C$ if and only if $c(\alpha^b) = c(\alpha^{b+2}) = \dots = c(\alpha^{[b+2(\delta-2)]}) = 0$. Thus the code has a string of $\delta - 1$ consecutive odd powers of β as zeros.

Remark 5.3 *Let $\mathcal{B} = \{b_1, \dots, b_l\}$ be a basis of \mathbb{F}_{q^l} over \mathbb{F}_q . If $u = (u_1, \dots, u_n) \in \mathbb{F}_{q^l}^n$ then one can write the vectors u_i , $1 \leq i \leq n$, as linear combinations of the elements of \mathcal{B} , that is, $u_i = u_{i1}b_1 + \dots + u_{il}b_l$. Consider that $u^{(j)} = (u_{1j}, \dots, u_{nj})$ are vectors in \mathbb{F}_q^n with $1 \leq j \leq l$. Then, if $v \in \mathbb{F}_q^n$, one has $v \cdot u = 0$ if and only if $v \cdot u^{(j)} = 0$ for all $1 \leq j \leq l$.*

In the following theorem we construct a parity-check matrix for negacyclic codes:

Theorem 5.4 *Assume that q is a power of an odd prime, $\gcd(n, q) = 1$, and $m = \text{ord}_{2n}(q)$. Let β be a primitive $2n$ th root of unity in \mathbb{F}_{q^m} . Let b be an odd positive integer with $1 \leq b \leq 2n - 1$. Then a parity-check matrix for the*

BCH negacyclic code C of length n and designed distance δ , generated by the polynomial $g(x) = \text{lcm}\{M^{(b)}(x), M^{(b+2)}(x), \dots, M^{[b+2(\delta-2)]}(x)\}$, is the matrix

$$H_{\delta,b} = \begin{bmatrix} 1 & \beta^b & \beta^{2b} & \dots & \beta^{(n-1)b} \\ 1 & \beta^{(b+2)} & \beta^{2(b+2)} & \dots & \beta^{(n-1)(b+2)} \\ 1 & \beta^{(b+4)} & \beta^{2(b+4)} & \dots & \beta^{(n-1)(b+4)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \beta^{[b+2(\delta-2)]} & \beta^{2[b+2(\delta-2)]} & \dots & \beta^{(n-1)[b+2(\delta-2)]} \end{bmatrix},$$

where each entry is replaced by the corresponding column of m elements from \mathbb{F}_q and then removing any linearly dependent rows.

Proof: Assume that $\mathbf{c} = (c_0, c_1, \dots, c_{n-1}) \in C$. Thus we have $\mathbf{c}(\beta^b) = \mathbf{c}(\beta^{b+2}) = \mathbf{c}(\beta^{b+4}) = \dots = \mathbf{c}(\beta^{[b+2(\delta-2)]}) = 0$, hence

$$\begin{bmatrix} 1 & \beta^b & \beta^{2b} & \dots & \beta^{(n-1)b} \\ 1 & \beta^{(b+2)} & \beta^{2(b+2)} & \dots & \beta^{(n-1)(b+2)} \\ 1 & \beta^{(b+4)} & \beta^{2(b+4)} & \dots & \beta^{(n-1)(b+4)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \beta^{[b+2(\delta-2)]} & \beta^{2[b+2(\delta-2)]} & \dots & \beta^{(n-1)[b+2(\delta-2)]} \end{bmatrix} \cdot \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}_{(\delta-1,1)}.$$

From Remark 5.3 and from the definition of BCH negacyclic codes, the result follows. \square

Now we are ready to show one of the main results of this section:

Theorem 5.5 *Let $n = q^2 + 1$, where $q \equiv 1 \pmod{4}$ is a power of an odd prime and suppose that $s = n/2$. Then there exist MDS convolutional codes with parameters $(n, n - 2i + 1, 2; 1, 2i + 2)_{q^2}$, where $2 \leq i \leq n/2 - 1$.*

Proof: First, note that $\text{gcd}(n, q) = 1$ and $\text{ord}_{2n}(q^2) = 2$. Let β be a primitive $2n$ th root of unity in $\mathbb{F}_{q^{2m}}$. Consider that C_2 is the negacyclic BCH code of length n over \mathbb{F}_{q^2} generated by the product of the minimal polynomials

$$C_2 = \langle g_2(x) \rangle = \langle M^{(s)}(x)M^{(s+2)}(x) \cdot \dots \cdot M^{(s+2i)}(x) \rangle,$$

where $2 \leq i \leq s - 1$.

By Theorem 5.4, a parity check matrix of C_2 is obtained from the matrix

$$H_2 = \begin{bmatrix} 1 & \beta^s & \beta^{2s} & \dots & \beta^{(n-1)s} \\ 1 & \beta^{(s+2)} & \beta^{2(s+2)} & \dots & \beta^{(n-1)(s+2)} \\ 1 & \beta^{(s+4)} & \beta^{2(s+4)} & \dots & \beta^{(n-1)(s+4)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \beta^{(s+2i)} & \beta^{2(s+2i)} & \dots & \beta^{(n-1)(s+2i)} \end{bmatrix}$$

by expanding each entry as a column vector (containing 2 rows) with respect to some \mathbb{F}_{q^2} -basis β of \mathbb{F}_{q^4} and then removing one linearly dependent row. From Lemma 5.1, this new matrix H_{C_2} has rank $2i + 1$, so C_2 has dimension $n - 2i - 1$. From the BCH bound for negacyclic codes it follows that the minimum distance d_2 of C_2 satisfies $d_2 \geq 2i + 2$. Thus, from the (classical) Singleton bound, one concludes that C_2 is a MDS code with parameters $[n, n - 2i - 1, 2i + 2]_{q^2}$ and, consequently, its Hermitian dual code has dimension $2i + 1$.

Next we assume that C_1 is the negacyclic BCH code of length n over \mathbb{F}_{q^2} generated by the product of the minimal polynomials

$$C_1 = \langle g_1(x) \rangle = \langle M^{(s)}(x)M^{(s+2)}(x) \cdots M^{[s+2(i-1)]}(x) \rangle,$$

Similarly, by Theorem 5.4, C_1 has a parity check matrix derived from the matrix

$$H_1 = \begin{bmatrix} 1 & \beta^s & \beta^{2s} & \cdots & \beta^{(n-1)s} \\ 1 & \beta^{(s+2)} & \beta^{2(s+2)} & \cdots & \beta^{(n-1)(s+2)} \\ 1 & \beta^{(s+4)} & \beta^{2(s+4)} & \cdots & \beta^{(n-1)(s+4)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \beta^{[s+2(i-1)]} & \beta^{2[s+2(i-1)]} & \cdots & \beta^{(n-1)[s+2(i-1)]} \end{bmatrix}$$

by expanding each entry as a column vector with respect to some \mathbb{F}_{q^2} -basis β of \mathbb{F}_{q^4} (already done, since H_1 is a submatrix of H_2) and then removing one linearly dependent row. From Lemma 5.1, this new matrix H_{C_1} has rank $2i - 1$, so C_1 has dimension $n - 2i + 1$. From the BCH bound for negacyclic codes, the minimum distance d_1 of C_1 satisfies $d_1 \geq 2i$, so C_1 is an $[n, n - 2i + 1, 2i]_{q^2}$ MDS code. Thus, its Hermitian dual code has dimension $2i - 1$.

Now, let C_0 be the negacyclic BCH code of length n over \mathbb{F}_{q^2} generated by the minimal polynomial $M^{(s+2i)}(x)$. Then C_0 has parameters $[n, n - 2, d_0 \geq 2]_{q^2}$. A parity check matrix H_{C_0} of C_0 is given by expanding the entries of the matrix

$$H_0 = [1 \quad \alpha^{(s+2i)} \quad \alpha^{2(s+2i)} \quad \cdots \quad \alpha^{(n-1)(s+2i)}]$$

with respect to β (already done, since H_0 is a submatrix of H_2).

Further, let us construct the convolutional code V generated by the reduced basic (according to Theorem 3.1 Item (a)) generator matrix

$$G(D) = \tilde{H}_{C_1} + \tilde{H}_{C_0}D,$$

where $\tilde{H}_{C_1} = H_{C_1}$ and \tilde{H}_{C_0} is obtained from H_{C_0} by adding zero-rows at the bottom such that \tilde{H}_{C_0} has the number of rows of H_{C_1} in total. By construction, V is a unit-memory convolutional code of dimension $2i - 1$ and degree $\delta_V = 2$. We know that the Hermitian dual V^{\perp_h} of V has dimension $n - 2i + 1$ and degree 2. By Theorem 3.1 Item (c), the free distance of V^{\perp_h} is bounded by $\min\{d_0 + d_1, d_2\} \leq d_f^{\perp_h} \leq d_2$, where d_i is the minimum distance of the code $C_i = \{\mathbf{v} \in \mathbb{F}_q^n \mid \mathbf{v}\tilde{H}_{C_i}^t = 0\}$. From construction one has $d_2 = 2i + 2$, $d_1 = 2i$ and $d_0 \geq 2$, so V^{\perp_h} has parameters $(n, n - 2i + 1, 2; 1, 2i + 2)_{q^2}$. It is easy to see

that the parameters of $V^{\perp h}$ satisfies (1) with equality, so $V^{\perp h}$ is MDS. \square

Theorem 5.6 given in the following is the second main result of this section:

Theorem 5.6 *Let $n = (q^2 + 1)/2$, where q is a power of an odd prime. Then there exist MDS convolutional codes with parameters $(n, n - 2i + 2, 2; 1, 2i + 1)_{q^2}$, where $2 \leq i \leq (n - 1)/2$.*

Proof: It suffices to consider C_2 be the code generated by $\langle M^{(1)}(x)M^{(3)}(x) \cdots \cdots M^{(2i-1)}(x) \rangle$, where $2 \leq i \leq (n - 1)/2$, C_1 be the negacyclic BCH code generated by $\langle g_1(x) \rangle = \langle M^{(1)}(x)M^{(3)}(x) \cdots \cdots M^{(2i-3)}(x) \rangle$ and C_0 be the negacyclic BCH code generated by $M^{(2i-1)}(x)$. Proceeding similarly as in the proof of Theorem 5.5, the result follows. \square

Theorem 5.7 *Let $n = (q^2 + 1)/2$, where $q \geq 5$ is a power of an odd prime. Then there exist MDS convolutional codes with parameters $(n, n - 2i + 1, 2; 1, 2i + 2)_{q^2}$, where $2 \leq i \leq \frac{(n-1)}{2} - 1$.*

Proof: Consider that C_2 , C_1 and C_0 are negacyclic BCH codes of length n over \mathbb{F}_{q^2} generated, respectively by $\langle g_2(x) \rangle = \langle M^{(n)}(x)M^{(n+2)}(x) \cdots \cdots M^{(n+2i)}(x) \rangle$, $\langle g_1(x) \rangle = \langle M^{(n)}(x)M^{(n+2)}(x) \cdots \cdots M^{(n+2i-2)}(x) \rangle$, and $\langle g_0(x) \rangle = \langle M^{(n+2i)}(x) \rangle$. Applying the same procedure given in the proofs of Theorems 5.5 and 5.6, the result follows. \square

6 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, 13, 14, 16] but only in [3, 14] the constructions are made algebraically. Here, we propose the construction of MDS convolutional stabilizer codes derived from the convolutional codes constructed in Section 5. To proceed further, let us recall some results available in the literature:

Lemma 6.1 [2, Proposition 2] *Let C be an $(n, (n - k)/2, \gamma; \mu)_{q^2}$ convolutional code such that $C \subseteq C^{\perp h}$. Then there exists an $[(n, k, \mu; \gamma, d_f)]_q$ convolutional stabilizer code, where $d_f = wt(C^{\perp h} \setminus C)$.*

Theorem 6.2 [3] (Quantum Singleton bound) *The free distance of an $[(n, k, \mu; \gamma, d_f)]_q$ \mathbb{F}_{q^2} -linear pure convolutional stabilizer code is bounded by*

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

Lemma 6.3 [20] *Let $n = q^2 + 1$, where $q \equiv 1 \pmod{4}$ is a power of an odd prime and suppose that $s = n/2$. If C is a q^2 -ary negacyclic code of length n with defining set $\mathcal{Z} = \cup_{i=0}^{\delta} \mathcal{C}_{s-2i}$, where $0 \leq \delta \leq (q-1)/2$, then $C^{\perp h} \subseteq C$.*

Lemma 6.4 [20] *Let $n = (q^2 + 1)/2$, where q is a power of an odd prime. If C is a q^2 -ary negacyclic code of length n with defining set $\mathcal{Z} = \cup_{i=1}^{\delta} \mathcal{C}_{2i-1}$, where $1 \leq \delta \leq (q-1)/2$, then $C^{\perp h} \subseteq C$.*

Now, we are able to show the following two results, in which new families of quantum convolutional MDS codes are constructed:

Theorem 6.5 *Let $n = q^2 + 1$, where $q \equiv 1 \pmod{4}$ is a power of an odd prime and suppose that $s = n/2$. Then there exist quantum MDS convolutional codes with parameters $[(n, n - 4i + 2, 1; 2, 2i + 2)]_q$, where $2 \leq i \leq (q-1)/2$.*

Proof: We consider the same notation utilized in Theorem 5.5. From Theorem 5.5, there exists a classical convolutional MDS code $V^{\perp h}$ with parameters $(n, n - 2i + 1, 2; 1, 2i + 2)_{q^2}$, for each $2 \leq i \leq n/2 - 1$. This code is the Hermitian dual of the code V with parameters $(n, 2i - 1, 2; 1, d_f)_{q^2}$. From Lemma 6.3 and from Theorem 3.1 Item (b), one has $V \subset V^{\perp h}$. Applying Lemma 6.1, there exists an $[(n, n - 4i + 2, 1; 2, d_f \geq 2i + 2)]_q$ convolutional stabilizer code \mathcal{Q} , for each $2 \leq i \leq (q-1)/2$. Replacing the parameters of \mathcal{Q} in Theorem 6.2, the result follows. \square

Theorem 6.6 *Let $n = (q^2 + 1)/2$, where $q \geq 7$ is a power of an odd prime. Then there exist quantum MDS convolutional codes with parameters $[(n, n - 4i + 4, 1; 2, 2i + 1)]_q$, where $2 \leq i \leq (q-1)/2$.*

Proof: From Theorem 5.6, there exists a classical convolutional MDS code $V^{\perp h}$ with parameters $(n, n - 2i + 2, 2; 1, 2i + 1)_{q^2}$, for each $2 \leq i \leq (n-1)/2$. This code is the Hermitian dual of the code V with parameters $(n, 2i - 2, 2; 1, d_f)_{q^2}$. From Lemma 6.4 and from Theorem 3.1 Item (b), one has $V \subset V^{\perp h}$. Applying Lemma 6.1, there exists a convolutional stabilizer code \mathcal{Q} with parameters $[(n, n - 4i + 4, 1; 2, d_f \geq 2i + 1)]_q$, for each $2 \leq i \leq (q-1)/2$. Replacing the parameters of \mathcal{Q} in Theorem 6.2, the result follows. \square

In the following we present Tables 1 and 2, containing the parameters of some new convolutional codes and some new quantum convolutional codes, respectively, constructed in this paper. Recall the these codes are optimal in the sense they attain the classical (quantum) generalized Singleton bound.

7 Summary

In this paper we have constructed new families of classical and quantum MDS-convolutional codes derived from negacyclic codes. All the constructions presented here are performed algebraically and not by exhaustively computational

Table 1: Classical MDS

New convolutional codes	
$(n, n - 2i + 1, 2; 1, 2i + 2)_{q^2}$, $q \equiv 1 \pmod{4}$, $n = q^2 + 1$, $2 \leq i \leq n/2 - 1$	
	$(26, 23, 2; 1, 6)_{25}$
	$(26, 21, 2; 1, 8)_{25}$
	$(26, 19, 2; 1, 10)_{25}$
	$(26, 9, 2; 1, 20)_{25}$
	$(26, 7, 2; 1, 22)_{25}$
	$(26, 5, 2; 1, 24)_{25}$
	$(82, 63, 2; 1, 22)_{81}$
	$(82, 53, 2; 1, 32)_{81}$
	$(82, 43, 2; 1, 42)_{81}$
	$(82, 23, 2; 1, 62)_{81}$
	$(82, 13, 2; 1, 72)_{81}$
$(n, n - 2i + 2, 2; 1, 2i + 1)_{q^2}$, $n = (q^2 + 1)/2$, $2 \leq i \leq (n - 1)/2$	
	$(5, 3, 2; 1, 5)_9$
	$(25, 23, 2; 1, 5)_{49}$
	$(25, 21, 2; 1, 7)_{49}$
	$(25, 19, 2; 1, 9)_{49}$
	$(25, 17, 2; 1, 11)_{49}$
	$(25, 15, 2; 1, 13)_{49}$
	$(25, 13, 2; 1, 15)_{49}$
	$(25, 11, 2; 1, 17)_{49}$
	$(25, 7, 2; 1, 21)_{49}$
$(n, n - 2i + 1, 2; 1, 2i + 2)_{q^2}$, $q \geq 5$, $n = (q^2 + 1)/2$, $2 \leq i \leq (n - 1)/2 - 1$	
	$(13, 10, 2; 1, 6)_{25}$
	$(13, 8, 2; 1, 8)_{25}$
	$(13, 6, 2; 1, 10)_{25}$
	$(13, 4, 2; 1, 12)_{25}$
	$(25, 16, 2; 1, 12)_{49}$
	$(25, 10, 2; 1, 18)_{49}$
	$(25, 4, 2; 1, 24)_{49}$
	$(41, 38, 2; 1, 6)_{81}$
	$(41, 32, 2; 1, 12)_{81}$
	$(41, 24, 2; 1, 20)_{81}$
	$(41, 4, 2; 1, 40)_{81}$
	$(61, 32, 2; 1, 32)_{121}$
	$(61, 22, 2; 1, 42)_{121}$
	$(61, 4, 2; 1, 60)_{121}$

Table 2: Quantum MDS

New convolutional stabilizer codes	
$[[n, n - 4i + 2, 1; 2, 2i + 2]]_q$, $q \equiv 1 \pmod{4}$, $n = q^2 + 1$, $2 \leq i \leq (q - 1)/2$	
	$[(26, 20, 2; 1, 6)]_5$
	$[(82, 80, 2; 1, 4)]_9$
	$[(82, 76, 2; 1, 6)]_9$
	$[(82, 72, 2; 1, 8)]_9$
	$[(82, 68, 2; 1, 10)]_9$
	$[(170, 168, 2; 1, 4)]_{13}$
	$[(170, 164, 2; 1, 6)]_{13}$
	$[(170, 160, 2; 1, 8)]_{13}$
	$[(170, 156, 2; 1, 10)]_{13}$
	$[(170, 152, 2; 1, 12)]_{13}$
	$[(170, 148, 2; 1, 14)]_{13}$
$[[n, n - 4i + 4, 2; 1, 2i + 1]]_q$, $n = (q^2 + 1)/2$, $2 \leq i \leq (q - 1)/2$	
	$[(25, 21, 2; 1, 5)]_7$
	$[(25, 17, 2; 1, 7)]_7$
	$[(61, 57, 2; 1, 5)]_{11}$
	$[(61, 53, 2; 1, 7)]_{11}$
	$[(61, 49, 2; 1, 9)]_{11}$
	$[(61, 45, 2; 1, 11)]_{11}$
	$[(145, 141, 2; 1, 5)]_{17}$
	$[(145, 137, 2; 1, 7)]_{17}$
	$[(145, 133, 2; 1, 9)]_{17}$
	$[(145, 129, 2; 1, 11)]_{17}$
	$[(145, 125, 2; 1, 13)]_{17}$
	$[(145, 121, 2; 1, 15)]_{17}$
	$[(145, 117, 2; 1, 17)]_{17}$

search. The results obtained in this paper show that the class of negacyclic codes is also a good source in the search for optimal codes.

Acknowledgment

This research has been partially supported by the Brazilian Agencies CAPES and CNPq.

References

- [1] A. C. A. de Almeida and R. Palazzo Jr.. A concatenated $[[4, 1, 3]]$ quantum convolutional code. In *Proc. IEEE Inform. Theory Workshop (ITW)*, pp. 28–33, 2004.
- [2] S. A. Aly, M. Grassl, A. Klappenecker, M. Rötteler, P. K. Sarvepalli. Quantum convolutional BCH codes. e-print arXiv:quant-ph/0703113.
- [3] S. A. Aly, A. Klappenecker, P. K. Sarvepalli. Quantum convolutional codes derived from Reed-Solomon and Reed-Muller codes. e-print arXiv:quant-ph/0701037.
- [4] A. Ashikhmin and E. Knill. Non-binary quantum stabilizer codes. *IEEE Trans. Inform. Theory*, 47(7):3065–3072, November 2001.
- [5] N. Aydin, I. Siap, D. K. Ray-Chaudhuri. The Structure of 1-Generator Quasi-Twisted Codes and New Linear Codes. *Designs, Codes and Cryptography*, 24:313–326, 2001.
- [6] G. K. Bakshi and M. Raka. A class of constacyclic codes over a finite field. *Finite Fields Applic.*, 18:362–377, 2012.
- [7] E. R. Berlekamp. Negacyclic codes for the Lee metric. In *Symp. Combinatorial Math. Appl.*, pp. 1–27, 1967.
- [8] T. Blackford. Negacyclic duadic codes. *Finite Fields Appl.*, 14:930–943, 2008.
- [9] 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.
- [10] B. Chen, Y. Fan, L. Lin, and H. Liu. Constacyclic codes over finite fields. *Finite Fields Appl.*, 18:1217–1231, 2012.
- [11] J. J. Climent, V. Herranz, C. Perea. Linear system modelization of concatenated block and convolutional codes. *Linear Algebra Appl.*, 429(5-6):1191–1212, 2008.
- [12] G. D. Forney Jr. Convolutional codes I: algebraic structure. *IEEE Trans. Inform. Theory*, 16(6):720–738, November 1970.
- [13] G. D. Forney Jr., M. Grassl, S. Guha. Convolutional and tail-biting quantum error-correcting codes. *IEEE Trans. Inform. Theory*, 53(3):865–880, March 2007.
- [14] M. Grassl and M. Rötteler. Quantum block and convolutional codes from self-orthogonal product codes. In *Proc. Int. Symp. Inform. Theory (ISIT)*, pp. 1018–1022, 2005.

- [15] M. Grassl and M. Rötteler. Non-catastrophic encoders and encoder inverses for quantum convolutional codes. In *Proc. Int. Symp. Inform. Theory (ISIT)*, pp. 1109-1113, 2006.
- [16] M. Grassl and M. Rötteler. Constructions of quantum convolutional codes. e-print arXiv:quant-ph/0703182.
- [17] K. J. Hole. On classes of convolutional codes that are not asymptotically catastrophic. *IEEE Trans. Inform. Theory*, 46(2):663–669, March 2000.
- [18] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. University Press, Cambridge, 2003.
- [19] R. Johannesson and K. S. Zigangirov. *Fundamentals of Convolutional Coding*. Digital and Mobile Communication, Wiley-IEEE Press, 1999.
- [20] X. Kai and S. Zhu. New Quantum MDS Codes From Negacyclic Codes. *IEEE Trans. Inform. Theory*, 59(2):1193–1197.
- [21] X. Kai and S. Zhu. Quantum Negacyclic Codes. *Phys. Rev. A*, 88(1):012326(1–5), 2013.
- [22] 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.
- [23] A. Krishna and D. V. Sarwate. Pseudocyclic maximum-distance-separable codes. *IEEE Trans. Inform. Theory*, 36(4):880-884, 1990.
- [24] G. G. La Guardia. Constructions of new families of nonbinary quantum codes. *Phys. Rev. A*, 80(4):042331(1–11), October 2009.
- [25] G. G. La Guardia. New quantum MDS codes. *IEEE Trans. Inform. Theory*, 57(8):5551–5554, August 2011.
- [26] G. G. La Guardia. Nonbinary convolutional codes derived from group character codes. *Discrete Math.*, 313:2730-2736, 2013.
- [27] G. G. La Guardia. On classical and quantum MDS-convolutional BCH codes. *IEEE Trans. Inform. Theory*, To appear.
- [28] L. N. Lee. Short unit-memory byte-oriented binary convolutional codes having maximum free distance. *IEEE Trans. Inform. Theory*, 22:349–352, May 1976.
- [29] H. Gluesing-Luerssen, J. Rosenthal and R. Smarandache. Strongly MDS convolutional codes. *IEEE Trans. Inform. Theory*, 52:584–598, 2006.
- [30] H. Gluesing-Luerssen, W. Schmale. Distance bounds for convolutional codes and some optimal codes. e-print arXiv:math/0305135.
- [31] H. Gluesing-Luerssen and W. Schmale. On doubly-cyclic convolutional codes. *Applicable Algebra in Eng. Comm. Comput.*, 17(2):151–170, 2006.
- [32] H. Gluesing-Luerssen and F-L Tsang. A matrix ring description for cyclic convolutional codes. *Advances in Math. Communications*, 2(1):55–81, 2008.
- [33] R. Hutchinson, J. Rosenthal and R. Smarandache. Convolutional codes with maximum distance profile. *Systems and Control Letters*, 54(1):53–63, 2005.
- [34] J. I. Iglesias-Curto. Generalized AG Convolutional Codes. *Advances in Mathematics of Communications*, 3(4):317–328, 2009.
- [35] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

- [36] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [37] H. Ollivier and J.-P. Tillich. Description of a quantum convolutional code. *Phys. Rev. Lett.*, 91(17):17790214, 2003.
- [38] H. Ollivier and J.-P. Tillich. Quantum convolutional codes: fundamentals. e-print arXiv:quant-ph/0401134.
- [39] Ph. Piret. *Convolutional Codes: An Algebraic Approach*. Cambridge, Massachusetts: The MIT Press, 1988.
- [40] Ph. Piret. A convolutional equivalent to Reed-Solomon codes. *Philips J. Res.*, 43:441–458, 1988.
- [41] J. Rosenthal and R. Smarandache. Maximum distance separable convolutional codes. *Applicable Algebra in Eng. Comm. Comput.*, 10:15–32, 1998.
- [42] J. Rosenthal and E. V. York. BCH convolutional codes. *IEEE Trans. Inform. Theory*, 45(6):1833-1844, 1999.
- [43] R. Smarandache, H. G.-Luerksen, J. Rosenthal. Constructions of MDS-convolutional codes. *IEEE Trans. Inform. Theory*, 47(5):2045–2049, July 2001.
- [44] A. Steane. Enlargement of Calderbank-Shor-Steane quantum codes. *IEEE Trans. Inform. Theory*, 45(7):2492–2495, November 1999.
- [45] S. Zhu and X. Kai. A class of constacyclic codes over \mathbb{Z}_p^m . *Finite Fields Appl.*, 16(4):243-254, 2010.

Giuliano G. 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), 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.