Int J Theor Phys (2015) 54:198–209
DOI 10.1007/s10773-014-2214-6

Nonbinary Quantum Convolutional Codes Derived from Negacyclic Codes

Jianzhang Chen · Jianping Li · Fan Yang · Yuanyuan Huang

Received: 13 December 2013 / Accepted: 27 May 2014 / Published online: 13 June 2014
© Springer Science+Business Media New York 2014

Abstract In this paper, some families of nonbinary quantum convolutional codes are constructed by using negacyclic codes. These nonbinary quantum convolutional codes are different from quantum convolutional codes in the literature. Moreover, we construct a family of optimal quantum convolutional codes.

Keywords Quantum convolutional codes · Quantum codes · Negacyclic codes

1 Introduction

Recently, many researchers studied quantum convolutional codes by using different methods. Ollivier and Tillich developed the stabilizer structure for quantum convolutional codes firstly in [1, 2]. In [3], Almeida and Palazzo Jr. studied the [(4, 1, 3)] quantum convolutional code. Grassl and Rötteler constructed some new quantum convolutional codes and presented their relative algorithms to get non-catastrophic encoders for these quantum convolutional codes in [4–6]. Forney et al. studied convolutional and tail-biting quantum codes in [7]. Wilde and Brun constructed entanglement assisted quantum convolutional codes in [8, 9]. Tan and Li constructed quantum convolutional codes by using LDPC codes in [10]. Aly et al. constructed quantum convolutional codes by using BCH codes in [11]. Recently, G. G.

J. Chen (✉) · J. Li · F. Yang
School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
e-mail: chenyouqing66@gmail.com

Y. Huang
Department of Network Engineering, Chengdu University of Information Technology, Chengdu 610225, China

La Guardia [12, 13] constructed some quantum convolutional codes derived from BCH codes and obtained some new MDS quantum convolutional codes. In [14], G. G. La Guardia also used negacyclic codes to construct some new families of MDS quantum convolutional codes. In this paper, we will use negacyclic codes constructed in [15] to study unite-memory quantum convolutional codes and multi-memory quantum convolutional codes. Here, we use the algebraic method to construct quantum convolutional codes. Moreover, the new constructed quantum convolutional codes are different from quantum convolutional codes available in the literature.

The organization of this paper is as follows: In Section 2, we present some definitions and basic results of negacyclic codes. In Section 3, we state some basic concepts and results of classical and quantum convolutional codes. In section 4, some families of quantum convolutional codes are derived from negacyclic codes.

2 Review of Negacyclic Codes

In this section, we recall some basic results about negacyclic codes in [15–19].

Throughout this paper, let p be an odd prime number, q be a power of p, and F_{q^2} be the finite field with q^2 elements. Let $a^q = (a_0^q, a_1^q, \cdots, a_{n-1}^q)$ denotes the conjugation of the vector $a = (a_0, a_1, \cdots, a_{n-1})$. For $u = (u_0, u_1, \cdots, u_{n-1})$, $v = (v_0, v_1, \cdots, v_{n-1}) \in F_{q^2}^n$, we can define the Hermitian inner product as follows:

$$\langle u, v\rangle_h = u_0 v_0^q + u_1 v_1^q + \cdots + u_{n-1} v_{n-1}^q.$$

If $\mathcal{C}$ is a k-free submodule with length n, then $\mathcal{C}$ is said to be an $[n, k]$-linear code. The number of nonzero components of $c \in \mathcal{C}$ is said to be the weight $wt(c)$ of the codeword c. The minimum nonzero weight d of all codewords in $\mathcal{C}$ is said to be the minimum weight of $\mathcal{C}$.

If a q^2-ary linear code $\mathcal{C}$ of length n is invariant under the permuation of F_{q^2}, i.e.,

$$(c_0, c_1, \cdots, c_{n-1}) \rightarrow (ac_{n-1}, c_0, c_1, \cdots, c_{n-2}),$$

then $\mathcal{C}$ is constacyclic code. If $a = 1$, then $\mathcal{C}$ is said to be a cyclic code. If $a = -1$, then $\mathcal{C}$ is called a negacyclic code.

We can see that $xc(x)$ corresponds to a negacyclic shift of $c(x)$ in the quotient ring $F_{q^2}[x]/\langle x^n+1\rangle$. Then, a q^2-ary negacyclic code $\mathcal{C}$ of length n is an ideal of $F_{q^2}[x]/\langle x^n+1\rangle$ and $\mathcal{C}$ can be generated by a monic polynomial $g(x)$ of $x^n + 1$.

Let $gcd(n, q) = 1$. Then $x^n + 1$ doesn't have multiple roots. Let m be the multiplicative order of q^2 modulo $2n$. Let δ be primitive $2n$th root of unity in $F_{q^{2m}}$ and $\alpha = \delta^2 \in F_{q^{2m}}$. Then, α is a primitive nth root of unity. Hence,

$$x^n + 1 = \Pi_{i=0}^{n-1}(x - \delta\alpha^i) = \Pi_{i=0}^{n-1}(x - \delta^{2i+1}).$$

The q^2-cyclotomic coset module $2n$ containing i is defined by C_i, $C_i = \{i, iq^2, iq^4, \cdots, iq^{2(m_i-1)}\}$, where m_i is the smallest positive integer such that $iq^{2m_i} \equiv i \ mod\ 2n$.

For a q^2-ary linear code $\mathcal{C}$ of length n, the Hermitian dual code of $\mathcal{C}$ can be defined as follows:

$$\mathcal{C}^{\perp_h} = \{u \in F_{q^2}^n \mid \langle u, v\rangle_h = 0 \ for\ all\ v \in \mathcal{C}\}.$$

A q^2-ary linear code $\mathcal{C}$ of length n is called Hermitian self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^{\perp_h}$.

Let $\mathcal{O}_{2n}$ be the set of all odd integers from 1 to $2n$. The defining set of a negacyclic code $\mathcal{C} = \langle g(x)\rangle$ of length n is the set $Z = \{i \in \mathcal{O}_{2n} \mid \delta^i\ is\ a\ root\ of\ g(x)\}$. Let $\mathcal{C}$ be an

$[n, k]$ negacyclic code over F_{q^2} with defining set Z. Then the Hermitian dual $\mathcal{C}^{\perp_h}$ is also negacyclic and has defining set $Z^{\perp_h} = \{z \in \mathcal{O}_{2n} | -qz(mod\ 2n) \notin Z\}$.

The following proposition in [16–18] plays an important role in constructing quantum convolutional codes.

Proposition 1 *(The BCH bound for negacyclic codes) Let $\mathcal{C}$ be a q^2-ary negacyclic code of length n. If the generator polynomial $g(x)$ of $\mathcal{C}$ has the elements $\{\delta^{1+2i} \mid 0 \le i \le d-2\}$ as the roots where δ is a primitive $2nth$ root of unity, then the minimum distance of $\mathcal{C}$ is at least d.*

3 Review of Classical Convolutional Codes and Quantum Convolutional Codes

In this section, we recall some definitions and some basic results about classical convolutional codes and quantum convoutional codes in [11–14] and [20–26].

A polynomial encoder matrix $G(D) \in F_q[D]^{k\times n}$ is called basic if $G(D)$ has a polynomial right inverse. If the overall constraint length $\gamma = \sum_{i=1}^{k} \gamma_i$ has the smallest value among all basic generator matrices of convolutional code $\mathcal{C}$, then the basic generator matrix of the convolutional code $\mathcal{C}$ is said to be reduced. For this case, the overall constraint length γ is called the degree of the convolutional code $\mathcal{C}$. The weight of an element $v(D) \in F_q[D]^n$ is defined as $wt(v(D)) = \sum_{i=1}^{n} wt(v_i(D))$, where $wt(v_i(D))$ is the number of nonzero coefficients of $v_i(D)$.

Definition 1 [11] A rate k/n convolutional code $\mathcal{C}$ with parameters $(n, k, \gamma;\ \mu, d_f)$ 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, $\mathcal{C} = \{u(D)G(D)|u(D) \in F_q[D]^k\}$, where n is the length, k is the dimension, $\gamma = \sum_{i=1}^{k} \gamma_i$ is the degree, where $\gamma_i = max_{1\le j\le n}\ \{deg\ g_{ij}\}$, $\mu = max_{1\le i\le k}\{\gamma_i\}$ is the memory and $d_f = wt(\mathcal{C}) = min\{wt(v(D))|\ v(D) \in \mathcal{C}, v(D) \ne 0\}$ is the free distance of the code.

For two n-tuples $u(D) = \sum_i u_i D^i$ and $v(D) = \sum_j u_j D^j$ in $F_q[D]^n$, the Euclidean inner product can be defined as $\langle u(D)|v(D)\rangle = \sum_i u_i v_i$. The Euclidean dual of convolutional code $\mathcal{C}$ is defined as $\mathcal{C}^{\perp} = \{u(D) \in F_q[D]^n | \langle u(D)|v(D)\rangle = 0\ for\ all\ v(D) \in \mathcal{C}\}$. The Hermitian inner product is defined as $\langle u(D)|v(D)\rangle_h = \sum_i u_i v_i^q$, where $u_i, v_i \in F_{q^2}^n$ and $v_i^q = (v_{1i}^q, v_{2i}^q, \cdots, v_{ni}^q)$. The Hermitian dual of convolutional code $\mathcal{C}$ is defined as $\mathcal{C}^{\perp_h} = \{u(D) \in F_{q^2}[D]^n | \langle u(D)|v(D)\rangle_h = 0\ for\ all\ v(D) \in \mathcal{C}\}$.

Now, we recall some results about classical convolutional codes available in [11–14].

Let $[n, k, d]_q$ be a block code with parity check matrix H, it can be partitioned into $\mu+1$ disjoint submatrices H_i such that $H = [H_0, H_1, \cdots H_\mu]^T$, where each H_i has n columns. Therefore, we have the polynomial matrix as following:

$$G(D) = \widetilde{H}_0 + \widetilde{H}_1 D + \widetilde{H}_2 D^2 + \cdots + \widetilde{H}_\mu D^\mu. \qquad (1)$$

The matrix $G(D)$ has κ rows and it can generate a convolutional code V, where κ is the maximum number of rows among the matrices H_i. The matrices $\widetilde{H}_i$ can be derived from the matrices H_i by adding zero-rows at the bottom such that the matrix $\widetilde{H}_i$ has κ rows in total.

Theorem 1 [11–14] *Let $\mathcal{C} \subseteq F_q^n$ is an $[n, k, d]_q$ code with parity check matrix $H \in F_q^{(n-k)\times n}$. Assume that H is partitioned into submatrices $H_0, H_1, \cdots, H_\mu$ as above such*

that $\kappa = rkH_0$ and $rkH_i \leq \kappa$ for $1 \leq i \leq \mu$. Consider the matrix $G(D)$ in (1). *Then we have:*
(a) The matrix $G(D)$ is a reduced basic generator matrix.
(b) If $\mathcal{C}^{\perp} \subset \mathcal{C}$(resp. $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$), then the convolutional code $V =+ \{v(D) = u(D)G(D)|u(G) \in F_q^{n-k}[D]\}$ satisfies $V \subset V^{\perp}$(resp.$V \subset V^{\perp_h}$).
(c) If d_f and $d_f^{\perp}$ denote the free distance of V and $V^{\perp}$, respectively, d_i denote the minimum distance of the code $\mathcal{C}_i = \{v \in F_q^n | v\widetilde{H}_i^t = 0\}$ and $d^{\perp}$ is the minimum distance of $\mathcal{C}^{\perp}$, then one has $min\{d_0 + d_{\mu}, d\} \leq d_f^{\perp} \leq d$ and $d_f \geq d^{\perp}$.

Here, we recall some basic results of quantum convolutional code in [2, 7, 11, 12, 27]. The stabilizer can be given by a matrix of the form

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

which satisfies $X(D)Z(1/D)^t - Z(D)X(1/D)^t = 0$. Now, we can consider a quantum convolutional code $\mathcal{C}$ defined by the the full-rank stabilizer matrix $S(D)$ given above. Then $\mathcal{C}$ is a rate k/n quantum convolutional code with parameters with $[(n, k, \mu; \gamma, d_f)]_q$, where n is called the frame size, k is the number of logical qudits per frame. The memory of the quantum convolutional codes is $\mu = max_{1\leq i\leq n-k, 1\leq j\leq n}\{max\{degX_{ij}(D), degZ_{ij}(D)\}\}$, d_f is the free distance and γ is the degree of the code. We also can define the constraint lengths of quantum convolutional codes as $\gamma_i = max_{1\leq j\leq n}\{max\{degX_{ij}(D), degZ_{ij}(D)\}\}$. Then, the overall constraint length is defined as $\gamma = \sum_{i=1}^{n-k} \gamma_i$. For more details about quantum convolutional codes, readers can consult [12–14].

The following theorem shows how to construct quantum convolutional stabilizer codes by using classical convolutional codes:

Theorem 2 [11] *Let $\mathcal{C}$ be an $(n, (n-k)/2, \gamma; \mu)_{q^2}$ convolutional code such that $\mathcal{C} \subseteq \mathcal{C}^{\perp_h}$. Then there exists an $[(n, k, \mu; \gamma, d_f)]_q$ convolutional stabilizer code, where $d_f = wt$ $(\mathcal{C}^{\perp_h} \setminus \mathcal{C})$.*

4 Constructions of Quantum Convolutional Codes

4.1 Code Construction I

In this subsection, we will use negacyclic codes with length $n = q^{2m} + 1$ to construct quantum convolutional codes. Now, we recall the following lemma in [15].

Lemma 1 [15] *Assume that $q \equiv 1(mod\ 4)$. Let $n = q^{2m} + 1$, where $m \geq 2$, and $s = n/2$. If $\mathcal{C}$ is a negacyclic code over F_{q^2} of length n with defining set $Z = C_{s-2l} \cup \cdots \cup C_{s-2} \cup C_s$ for $1 \leq l \leq q^2 - 1$. Then $\mathcal{C}$ contains its Hermitian dual code.*

Theorem 3 *Assume that $q \equiv 1(mod\ 4)$. Let $n = q^{2m}+1$, where $m \geq 2$, and $s = n/2$. Then there exist quantum convolutional codes with parameters $[(n, n-4ml+4m-2, 1; 2m, d_f \geq 2l + 2)]_q$, where $2 \leq l \leq q^2 - 1$.*

Proof Consider $\mathcal{C}$ is a negacyclic code over F_{q^2} of length n and the defining set of $\mathcal{C}$ is given by $Z = C_s \cup C_{s-2} \cup \cdots \cup C_{s-2l}$, where $2 \le l \le q^2 - 1$. Let

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

Since $2m = ord_{2n}(q^2)$, from Lemma 4 in [18], the parity check matrix H of $\mathcal{C}$ can be obtained from the matrix $H_{2l+2,s+2l}$ by expanding each entry as a column vector over some F_{q^2}-basis of $F_{q^{4m}}$ and then removing any linearly dependent rows. From Proposition 1, we can see that $\mathcal{C}$ is a negacyclic code with parameters $[n, n-2ml-1, d \ge 2l+2]_{q^2}$, where $2 \le l \le q^2 - 1$. □

Similarly, consider $\mathcal{C}_0$ is a negacyclic code over F_{q^2} of length n and the defining set of $\mathcal{C}_0$ is given by $Z_0 = C_s \cup C_{s-2} \cup \cdots \cup C_{s-2l+2}$. Let

$$H_{2l,s+2l-2} = \begin{bmatrix} 1 & \delta^{s} & \delta^{2s} & \cdots & \delta^{(n-1)s} \\ 1 & \delta^{s+2} & \delta^{2(s+2)} & \cdots & \delta^{(n-1)(s+2)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \delta^{s+2l-4} & \delta^{2(s+2l-4)} & \cdots & \delta^{(n-1)(s+2l-4)} \\ 1 & \delta^{s+2l-2} & \delta^{2(s+2l-2)} & \cdots & \delta^{(n-1)(s+2l-2)} \end{bmatrix}.$$

From Lemma 4 in [18], the parity check matrix H_0 of $\mathcal{C}_0$ can be obtained from the matrix $H_{2l,s+2l-2}$ by expanding each entry as a column vector over some F_{q^2}-basis of $F_{q^{4m}}$ and then removing any linearly dependent rows. From Proposition 1, we can see that $\mathcal{C}_0$ is a negacyclic code with parameters $[n, n-2ml+2m-1, d \ge 2l]_{q^2}$

Now, we can assume that $\mathcal{C}_1$ is is a negacyclic code over F_{q^2} of length n and the defining set of $\mathcal{C}_1$ is given by $Z_1 = C_{s-2l}$. Let

$$H_{2,s+2l} = \begin{bmatrix} 1 & \delta^{s+2l} & \delta^{2(s+2l)} & \cdots & \delta^{(n-1)(s+2l)} \end{bmatrix}.$$

From Lemma 4 in [18], the parity check matrix H_1 of $\mathcal{C}_1$ can be obtained from the matrix $H_{2,s+2l}$ by expanding each entry as a column vector over some F_{q^2}-basis of $F_{q^{4m}}$ and then removing any linearly dependent rows. From Proposition 1, we can see that $\mathcal{C}_1$ is a negacyclic code with parameters $[n, n-2m, d \ge 2]_{q^2}$.

From the above discussion, we can see that $rkH_0 > rkH_1$. Therefore, the convolutional code V generated by the matrix $G(D) = \widetilde{H}_0 + \widetilde{H}_1 D$ has parameters $(n, 2ml-2m+1, 2m; 1, d_f^*)_{q^2}$, where $\widetilde{H}_0 = H_0$, $\widetilde{H}_1$ can be obtained from H_1 by adding zero-rows at the bottom such that $\widetilde{H}_1$ has the number of rows of H_0. Since $wt(V^{\perp}) = wt(V^{\perp_h})$, then we can see that $d_f^{\perp_h} \ge 2l+2$ from Theorem 1. From Theorem 1 and Lemma 1, one has $V \subset V^{\perp_h}$. Then, there exist convolutional codes with parameters $[(n, n-4ml+4m-2, 1; 2m, d_f \ge 2l+2)]_q$ from Theorem 2, where $2 \le l \le q^2 - 1$.

Example 1 Let $q = 5$ and $m = 2$, then $n = 626$ and $s = 313$. Let $\mathcal{C}$ be a negacyclic code over F_{25} of length 626 and the defining set of $\mathcal{C}$ is given by $Z = C_{313} \cup C_{311} \cup \cdots \cup C_{301}$. Then $\mathcal{C}$ is a negacyclic code with parameters $[626, 601, d \ge 14]_{25}$. Now, let $\mathcal{C}_0$ be a negacyclic code over F_{25} of length 626 with defining set $Z_0 = C_{313} \cup C_{311} \cup \cdots \cup C_{303}$. Then $\mathcal{C}_0$ is a negacyclic code with parameters $[626, 605, d \ge 12]_{25}$. Let $\mathcal{C}_1$ be a negacyclic

Table 1 Some quantum convolutional codes constructed from Theorem 3

$[(n, n-4ml+4m-2, 1; 2m, d_f \geq 2l+2)]_q$,
$[(626, 616, 1; 4, d_f \geq 6)]_5$
$[(626, 608, 1; 4, d_f \geq 8)]_5$
$[(626, 600, 1; 4, d_f \geq 10)]_5$
$[(626, 592, 1; 4, d_f \geq 12)]_5$
$[(6562, 6552, 1; 4, d_f \geq 6)]_9$
$[(6562, 6544, 1; 4, d_f \geq 8)]_9$
$[(6562, 6536, 1; 4, d_f \geq 10)]_9$
$[(6562, 6528, 1; 4, d_f \geq 12)]_9$
$[(6562, 6520, 1; 4, d_f \geq 14)]_9$
$[(6562, 6512, 1; 4, d_f \geq 16)]_9$

code over F_{25} of length 626 with defining set $Z_1 = C_{301}$. Then $\mathcal{C}_1$ is a negacyclic code with parameters $[626, 622, d \geq 2]_{25}$. Applying Theorem 3, we can obtain quantum convolutional code with parameters $[(626, 584, 1; 4, d_f \geq 14)]_5$. In Table 1, some quantum convolutional codes with lengths 626 and 6562 are listed respectively. These quantum convolutional codes are different from the ones available in [11–14].

Let us now present the construction of multi-memory quantum convolutional codes.

Theorem 4 *Assume that $q \equiv 1(mod\, 4)$. Let $n = q^{2m}+1$, where $m \geq 2$, and $s = n/2$. Then there exist convolutional codes with parameters $[(n, n-4ml+4\mu m-2, \mu; 2\mu m, d_f \geq 2l+4-2\mu)]_q$, where $2 \leq \mu < l \leq q^2-1$.*

Proof Consider $\mathcal{C}$ is a negacyclic code over F_{q^2} of length n and the defining set of $\mathcal{C}$ is given by $Z = C_s \cup C_{s-2} \cup \cdots \cup C_{s-2l+2} \cup C_{s-2l}$, where $2 < l \leq q^2-1$. The parity matrix of $\mathcal{C}$ is denoted by H, where H can be obtained from the matrix $H_{2l+2,s+2l}$ of Theorem 3 by expanding each entry as a column vector over some F_{q^2}-basis of $F_{q^{4m}}$ and then removing any linear dependent rows. From Proposition 1, we can see that $\mathcal{C}$ is a negacyclic code with parameters $[n, n-2ml-1, d \geq 2l+2]_{q^2}$. □

Similarly, consider $\mathcal{C}_0$ is a negacyclic code over F_{q^2} of length n and the defining set of $\mathcal{C}_0$ is given by $Z_0 = C_s \cup C_{s-2} \cup \cdots \cup C_{s-2(l-\mu)}$, where $2 \leq \mu < l \leq q^2-1$. The parity matrix of $\mathcal{C}_0$ is denoted by H_0, where H_0 can be obtained from the matrix

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

by expanding each entry in matrix as a column vector over some F_{q^2}-basis of $F_{q^{4m}}$ and then removing any linear dependent rows. From Proposition 1, we can see that $\mathcal{C}_0$ is a negacyclic code with parameters $[n, n-2ml+2\mu m-1, d \geq 2l+2-2\mu]_{q^2}$.

Now, we can assume that $\mathcal{C}_j$ is a negacyclic code over F_{q^2} of length n and the defining set of $\mathcal{C}_j$ is given by $Z_j = C_{s-2(l-\mu+j)}$, where $j = 1, \cdots, \mu$. The parity matrix of $\mathcal{C}_j$ is denoted by H_j, where H_j can be obtained from the matrix

$$H_{2,s+2l-2\mu+2j} = \left[\, 1 \;\; \delta^{s+2l-2\mu+2j} \;\; \delta^{2(s+2l-2\mu+2j)} \;\; \ldots \;\; \delta^{(n-1)(s+2l-2\mu+2j)} \,\right]$$

by expanding each entry as a column vector over some F_{q^2}-basis of $F_{q^{4m}}$ and then removing any linear dependent rows. From Proposition 1, we can see that $\mathcal{C}_j$ is a negacyclic code with parameters $[n, n-2m, d \geq 2]_{q^2}$.

From the above discussion, we can see that $rkH_0 > rkH_j$, where $j = 1, \cdots, \mu$. Therefore, the convolutional code V generated by the matrix $G(D) = \widetilde{H}_0 + \widetilde{H}_1 D + \cdots + \widetilde{H}_\mu D^\mu$ has parameters $(n, 2ml - 2\mu m + 1, 2m\mu; \mu, d_f^*)_{q^2}$. Since $wt(V^\perp) = wt(V^{\perp_h})$, then we can see that $d_f^{\perp_h} \geq 2l + 4 - 2\mu$ from Theorem 1. From Theorem 1 and Lemma 1, one has $V \subset V^{\perp_h}$. Then, we can obtain quantum convolutional code with parameters $[(n, n - 4ml + 4\mu m - 2, \mu; 2\mu m, d_f \geq 2l + 4 - 2\mu)]_q$ from Theorem 2, where $2 \leq \mu < l \leq q^2 - 1$.

4.2 Code Construction II

In [12, 13], G. G. La Guardia constructed quantum convolutional codes by using BCH cyclic codes. In this subsection, we will use negacyclic codes of length $n = \frac{q^{2m}+1}{2}$ to construct a family of quantum convolutional codes. The following lemma in [15] will play an important role in the construction of quantum convolutional codes.

Lemma 2 [15] *Let $n = \frac{q^{2m}+1}{2}$, where $m \geq 2$ is a positive integer. If $\mathcal{C}$ is a negacyclic code over F_{q^2} of length n with defining set $Z = C_1 \cup C_3 \cup \cdots \cup C_{2l-1}$, where $1 \leq l \leq \frac{q-1}{2}$. Then, $\mathcal{C}$ contains its Hermitian dual code.*

Theorem 5 *Let $n = \frac{q^{2m}+1}{2}$, where $m \geq 2$ is a positive integer. Then there exist convolutional codes with parameters $[(n, n - 4ml + 4m, 1; 2m, d_f \geq 2l + 1)]_q$, where $2 \leq l \leq (q-1)/2$.*

Proof Consider $\mathcal{C}$ is a negacyclic code over F_{q^2} of length n and the defining set of $\mathcal{C}$ is given by $Z = C_1 \cup C_3 \cup \cdots \cup C_{2l-3} \cup C_{2l-1}$, where $2 \leq l \leq (q-1)/2$. The parity matrix of negacyclic code $\mathcal{C}$ is denoted by H, where H can be obtained from the matrix

$$H_{2l+1,2l-1} = \begin{bmatrix} 1 & \delta & \delta^2 & \ldots & \delta^{(n-1)} \\ 1 & \delta^3 & \delta^6 & \ldots & \delta^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \delta^{2l-3} & \delta^{2(2l-3)} & \ldots & \delta^{(n-1)(2l-3)} \\ 1 & \delta^{2l-1} & \delta^{2(2l-1)} & \ldots & \delta^{(n-1)(2l-1)} \end{bmatrix}$$

by expanding each entry as a column vector over some F_{q^2}-basis of $F_{q^{4m}}$ and then removing any linear dependent rows. From Proposition 1, we can see that $\mathcal{C}$ is a negacyclic code with parameters $[n, n - 2ml, d \geq 2l + 1]_{q^2}$. □

Similarly, consider $\mathcal{C}_0$ is a negacyclic code over F_{q^2} of length n and the defining set of $\mathcal{C}_0$ is given by $Z_0 = C_1 \cup C_3 \cup \cdots \cup C_{2l-3}$. The parity matrix of negacyclic code $\mathcal{C}_0$ is denoted by H_0, where H_0 can be obtained from the matrix

$$H_{2l-1,2l-3} = \begin{bmatrix} 1 & \delta & \delta^2 & \cdots & \delta^{(n-1)} \\ 1 & \delta^3 & \delta^6 & \cdots & \delta^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \delta^{2l-3} & \delta^{2(2l-3)} & \cdots & \delta^{(n-1)(2l-3)} \end{bmatrix}$$

by expanding each entry as a column vector over some F_{q^2}-basis of $F_{q^{4m}}$ and then removing any linear dependent rows. From Proposition 1, we can see that $\mathcal{C}_0$ is a negacyclic code with parameters $[n, n-2ml+2m, d \geq 2l-1]_{q^2}$.

Now, we can assume that $\mathcal{C}_1$ is is a negacyclic code over F_{q^2} of length n with defining set $Z_1 = C_{2l-1}$. The parity matrix of negacyclic code $\mathcal{C}_1$ is denoted by H_1, where H_1 can be obtained from the matrix

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

by expanding each entry as a column vector over some F_{q^2}-basis of $F_{q^{4m}}$ and then removing any linear dependent rows. From Proposition 1, we can see that $\mathcal{C}_1$ is a negacyclic code with parameters $[n, n-2m, d \geq 2]_{q^2}$.

From the above discussion, we can see that $rkH_0 \geq rkH_1$. Therefore, the convolutional code V generated by the matrix $G(D) = \widetilde{H}_0 + \widetilde{H}_1 D$ has parameters $(n, 2ml - 2m, 2m; 1, d_f^*)_{q^2}$, where $\widetilde{H}_0 = H_0$ and $\widetilde{H}_1$ can be obtain from H_1 by adding zero-rows at the bottom such that $\widetilde{H}_1$ has the number of H_0 in total. Since $wt(V^{\perp}) = wt(V^{\perp_h})$, then we can see that $d_f^{\perp_h} \geq 2l+1$ from Theorem 1. From Theorem 1 and Lemma 2, one has $V \subset V^{\perp_h}$. Then, we can obtain the convolutional code with parameters $[(n, n-4ml+4m, 1; 2m, d_f \geq 2l+1)]_q$ from Theorem 2, where $2 \leq l \leq (q-1)/2$.

Example 2 Let $q = 5$ and $m = 2$, then $n = 313$. Let $\mathcal{C}$ be a negacyclic code over F_{25} of length 313 and the defining set of $\mathcal{C}$ is given by $Z = C_1 \cup C_3$. Then $\mathcal{C}$ is a negacyclic code with parameters $[313, 305, d \geq 5]_{25}$. Now, let $\mathcal{C}_0$ be a negacyclic code over F_{25} of length 313 and the defining set of $\mathcal{C}_0$ is given by $Z_0 = C_1$. Then $\mathcal{C}_0$ is a negacyclic code with parameters $[313, 309, d \geq 3]_{25}$. Let $\mathcal{C}_1$ be a negacyclic code over F_{25} of length 313 and the defining set of $\mathcal{C}_1$ is given by $Z_1 = C_3$. Then $\mathcal{C}_1$ is a negacyclic code with parameters $[313, 309, d \geq 2]_{25}$. Applying Theorem 5, we can obtain quantum convolutional code with parameters $[(313, 305, 1; 4, d_f \geq 5)]_5$. In Table 2, some quantum convolutional codes are listed. These quantum convolutional codes are different from the ones available in [11–14].

Let us now construct a family of multi-memory quantum convolutional codes.

Theorem 6 *Let* $n = \frac{q^{2m}+1}{2}$, *where* $m \geq 2$ *is a positive integer. Then there exist convolutional codes with parameters* $[(n, n-4ml+4m, \mu; 2\mu m, d_f \geq 2l+3-2\mu)]_q$, *where* $2 \leq \mu < l \leq (q-1)/2$.

Proof The proof presented here use the same ideal of Theorem 4. We present its proof here for completeness. Consider $\mathcal{C}$ is a negacyclic code over F_{q^2} of length n and the defining set of $\mathcal{C}$ is given by $Z = C_1 \cup C_3 \cup \cdots \cup C_{2l-3} \cup C_{2l-1}$. The parity matrix of negacyclic code $\mathcal{C}$ is denoted by H, H can be obtained from the matrix $H_{2l+1,2l-1}$ of Theorem 5 by expanding the each entry as a column vector over some F_{q^2}-basis of $F_{q^{4m}}$ and the removing

Table 2 Some quantum convolutional codes derived from Theorem 5

$[(n, n-4ml+4m, 1; 2m, d_f \geq 2l+1)]_q$
$[(1201, 1193, 1; 4, d_f \geq 5)]_7$
$[(1201, 1185, 1; 4, d_f \geq 7)]_7$
$[(3281, 3273, 1; 4, d_f \geq 5)]_9$
$[(3281, 3265, 1; 4, d_f \geq 7)]_9$
$[(3281, 3257, 1; 4, d_f \geq 9)]_9$
$[(7321, 7313, 1; 4, d_f \geq 5)]_{11}$
$[(7321, 7305, 1; 4, d_f \geq 7)]_{11}$
$[(7321, 7297, 1; 4, d_f \geq 9)]_{11}$
$[(7321, 7289, 1; 4, d_f \geq 11)]_{11}$

any linear dependent rows. From Proposition 1, we can see that $\mathcal{C}$ is a negacyclic code with parameters $[n, n-2ml, d \geq 2l+1]_{q^2}$ □

Similarly, consider $\mathcal{C}_0$ is a negacyclic code over F_{q^2} of length n and the defining set of $\mathcal{C}_0$ is given by $Z_0 = C_1 \cup C_3 \cup \cdots \cup C_{2(l-\mu)-1}$, where $2 \leq \mu < l < (q-1)/2$. The parity matrix of negacyclic code $\mathcal{C}_0$ is denoted by H_0, where H_0 can be obtained from the matrix

$$H_{2l-2\mu+1,2l-2\mu-1} = \begin{bmatrix} 1 & \delta & \delta^2 & \cdots & \delta^{(n-1)} \\ 1 & \delta^3 & \delta^6 & \cdots & \delta^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \delta^{2l-2\mu-3} & \delta^{2(2l-2\mu-3)} & \cdots & \delta^{(n-1)(2l-2\mu-3)} \\ 1 & \delta^{2l-2\mu-1} & \delta^{2(2l-2\mu-1)} & \cdots & \delta^{(n-1)(2l-2\mu-1)} \end{bmatrix}$$

by expanding each entry as a column vector over some F_{q^2}-basis of $F_{q^{4m}}$ and then removing any linear dependent rows. From Proposition 1, we can see that $\mathcal{C}_0$ is a negacyclic code with parameters $[n, n-2ml+2\mu m, d \geq 2l+1-2\mu]_{q^2}$.

Now, we can assume that $\mathcal{C}_j$ is a negacyclic code over F_{q^2} of length n with defining set $Z_j = C_{2(l-\mu+j)-1}$, where $j = 1, \cdots, \mu$. The parity matrix of negacyclic code $\mathcal{C}_j$ is denoted by H_j, where H_j can be obtained from the matrix

$$H_{2,2l-2\mu+2j-1} = \begin{bmatrix} 1 & \delta^{2l-2\mu+2j-1} & \delta^{2(2l-2\mu+2j-1)} & \cdots & \delta^{(n-1)(2l-2\mu+2j-1)} \end{bmatrix}$$

by expanding each entry as a column vector over some F_{q^2}-basis of $F_{q^{4m}}$ and then removing any linear dependent rows. From Proposition 1, we can see that $\mathcal{C}_j$ is a negacyclic code with parameters $[n, n-2m, d \geq 2]_{q^2}$.

From the above discussion, we can see that $rkH_0 \geq rkH_j$, where $j = 1, \cdots, \mu$. Therefore, the convolutional code V generated by the matrix $G(D) = \widetilde{H}_0 + \widetilde{H}_1 D + \cdots + \widetilde{H}_\mu D^\mu$ has parameters $(n, 2ml-2\mu m, 2m\mu; \mu, d_f^*)_{q^2}$. Since $wt(V^\perp) = wt(V^{\perp_h})$, then we can see that $d_f^{\perp_h} \geq 2l+3-2\mu$ from Theorem 1. From Theorem 1 and Lemma 2, one has $V \subset V^{\perp_h}$. Then we can obtain quantum convolutional code with parameters $[(n, n-4ml+4\mu m, \mu; 2\mu m, d_f \geq 2l+3-2\mu)]_q$ from Theorem 2, where $2 \leq \mu < l \leq (q-1)/2$.

4.3 Code Construction III

In this subsection, we will use negacyclic codes to construct a family of optimal quantum convolutional codes. We can recall the following proposition in [27].

Proposition 2 [27]*(Quantum Singleton bound) The free distance of an* $[(n, k, \mu; \gamma, d_f)]_q$ F_{q^2}*-linear pure convolutional stabilizer code is bounded by*

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

We have the following lemma from [15, 28] plays an important role in the quantum construction.

Lemma 3 [15, 28]*Assume that* $q \equiv 1 \bmod 4$. *Let* l *be an odd divisor of* $q-1$ *or* $q+1$. *If* $\mathcal{C}$ *is a* q^2*-ary negacyclic code of length* $2l$ *with the defining set* $Z = \cup_{i=1}^{\tau} C_{2i-1}$, *where* $1 \leq \tau \leq l$, *then* $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}$.

Theorem 7 *Assume that* $q \equiv 1 \bmod 4$. *Let* l *be an odd divisor of* $q-1$ *or* $q+1$. *Then, there exist quantum convolutional codes with parameters* $[(2l, 2l-2\tau+2, 1; 1, \tau+1)]_q$, *where* $2 \leq \tau \leq l$.

Proof Consider the defining sets of $\mathcal{C}$, $\mathcal{C}_0$ and $\mathcal{C}_1$ of length $2l$ are given by

$$Z = C_1 \cup C_3 \cup \cdots \cup C_{2\tau-3} \cup C_{2\tau-1},$$
$$Z_0 = C_1 \cup C_3 \cup \cdots \cup C_{2\tau-3},$$

and

$$Z_1 = C_{2\tau-1},$$

respectively, where $2 \leq \tau \leq l$. □

Then, similar to Theorem 5, we can obtain quantum convolutional codes with parameters $[(2l, 2l-2\tau+2, 1; 1, d_f \geq \tau+1)]_q$, where $2 \leq \tau \leq l$. From Proposition 2, we know there exist optimal quantum convolutional codes with parameters $[(2l, 2l-2\tau+2, 1; 1, \tau+1)]_q$, where $2 \leq \tau \leq l$.

Example 3 Let $q = 9$ and $l = 5$. Applying Theorem 7, there exist some quantum MDS convolutional codes with parameters $[(10, 8, 1; 1, 3)]_9$, $[(10, 6, 1; 1, 4)]_9$, $[(10, 4, 1; 1, 5)]_9$ and $[(10, 2, 1; 1, 6)]_9$ respectively. These codes are different from the ones in [11–14].

In the next result, we construct multi-memory quantum convolutional codes.

Theorem 8 *Assume that* $q \equiv 1 \bmod 4$. *Let* l *be an odd divisor of* $q-1$ *or* $q+1$. *Then, there exist quantum convolutional codes with parameters* $[(2l, 2l-2\tau+2\mu, \mu; \mu, d_f \geq \tau+1)]_q$, *where* $2 \leq \mu < \tau \leq l$.

Proof Consider the defining sets of $\mathcal{C}$, $\mathcal{C}_0$ and $\mathcal{C}_1$ of length $2l$ are given by

$$Z = C_1 \cup C_3 \cup \cdots \cup C_{2\tau-3} \cup C_{2\tau-1},$$
$$Z_0 = C_1 \cup C_3 \cup \cdots \cup C_{2(\tau-\mu)-1},$$

and

$$Z_j = C_{2(\tau-\mu+j)-1},$$

respectively, where $2 \leq \mu < \tau \leq l$, and $j = 1, 2, \cdots, \mu$. □

Then, similar to Theorem 6, we know there exist quantum convolutional codes with parameters $[(2l, 2l+2\mu-2\tau, \mu; \mu, d_f \geq \tau+1)]_q$, where $2 \leq \mu < \tau \leq l$.

Remark 1 From the above discussion, if we consider $\mu > 1$, there is no guarantee that the corresponding quantum convolutional codes are MDS.

5 Conclusion and Discussion

In this paper, we construct some families of quantum convolutional codes. These quantum codes are performed algebraically, and these codes are different from those codes available in the literature. In [13], G. G. La Guardia used cyclic codes to construct a family of quantum MDS-convolutional codes with parameters $[(q^2+1, q^2+1-4i, 1; 2, 2i+3)]_q$, where $2 \leq i \leq \frac{q}{2} - 2$, $q = 2^t$ and $t \geq 3$ is an integer. In [14], G. G. La Guardia used negecyclic codes to construct two families of quantum MDS-convolutional codes. The first family is quantum convolutional codes with parameters $[(q^2+1, q^2+3-4i, 1; 2, 2i+2)]_q$, where $q \equiv 1\ (mod\ 4)$ is a power of an odd prime and $2 \leq i \leq (q-1)/2$. The second one is quantum convolutional codes with parameters $[((q^2+1)/2, (q^2+1)/2+4-4i, 1; 2, 2i+1)]_q$, where $q \geq 7$ is a power of an odd prime and $2 \leq i \leq (q-1)/2$.

In this work, we construct a new family of quantum MDS-convolutional codes with parameters $[(2l, 2l-2\tau+2, 1; 1, \tau+1)]_q$, where $q \equiv 1\ mod\ 4$, l is an odd divisor of $q-1$ or $q+1$, and $2 \leq \tau \leq l$. However, the parameters of these quantum MDS-convolutional codes are not better than the ones in [13, 14]. Nevertheless, we can find some quantum convolutional codes in Theorem 5 have better parameters than the ones in [14]. For example, the new $[(1201, 1185, 1; 4, d_f \geq 7)]_7$ quantum convolutional code in Table 2 is better than the $[(25, 17, 1; 2, 7)]_7$ code constructed in [14]. From Theorem 3 in [12], there exist quantum convolutional codes with parameters $[(q^4-1, q^4-11, 1; 4, d_f \geq 6)]_q$, where $q \geq 3$ is a prime power. We can obtain quantum convolutional codes with parameters $[(q^4+1, q^4-9, 1; 4, d_f \geq 6)]_q$ from Theorem 3 in this paper, where $q \equiv 1 (mod\ 4)$ and q is a prime power. We can see that some quantum convolutional codes constructed by Theorem 3 in this paper have good parameters compared with some codes constructed from Theorem 3 in [12]. It is an interesting topic to consider the construction of quantum convolutional codes by using some other negacyclic codes. Also, in future research, negacyclic codes in this paper can be applied to derive quantum subsystem codes by using the method in [29].

Acknowledgments The research was supported by the National Science Foundation of China (No. 61370073) and National Science Foundation of China (No. 61202084).

References

1. Ollivier, H., Tillich, J.P.: Phys. Rev. Lett. **91**(17), 17790214 (2003)
2. Ollivier, H., Tillich, J.P.: arXiv:quant-ph/0401134 (2004)
3. Aido De Almeida, A.C., Reginaldo Palazzo Jr.: In: Proc. IEEE Inform. Theory Workshop (ITW), pp. 28–33 (2004)
4. Grassl, M., Rötteler, M.: In: Proc. Int. Symp. Inform. Theory (ISIT), pp. 1018–1022 (2005)
5. Grassl, M., Rötteler, M.: In: Proc. Int. Symp. Inform. Theory (ISIT), pp. 1109–1113 (2006)
6. Grassl, M., Rötteler, M.: arXiv:quant-ph/0703182 (2007)
7. Forney, G.D., Grassl, M., Guha, S.: IEEE Trans. Inform. Theory **53**(3), 865–880 (2007)
8. Wilde, M.M., Brun, T.A.: In: Proc. Int. Symp. Inf. Theory (ISIT), pp. 359–363 (2008)
9. Wilde, M.M., Brun, T.A.: Phys. Rev. A **81**(4), 042333 (2010)
10. Tan, P., Li, J.: IEEE Trans. Inform. Theory **56**(1), 476–491 (2010)
11. Aly, S.A., Grassl, M., Klappenecker, A., Rötteler, M., Sarvepalli, P.K.: arXiv:quant-ph/0703113 (2007)

12. La Guardia, G.G.: Quantum Inf. Comput. **12**(9–10), 820–842 (2012)
13. La Guardia, G.G.: IEEE Trans. Inf. Theory **60**(1), 304–312 (2014)
14. La Guardia, G.G.: arXiv:1310.3265 (2013)
15. Kai, X., Zhu, S., Tang, Y.: Phys. Rev. A **88**, 012326 (2013)
16. Berlekamp, E.R.: Algebraic Coding Theory. Aegean Park Press, California (1984)
17. Kai, X., Zhu, S.: IEEE Trans. Inf. Theory **59**(2), 1193–1197 (2013)
18. Krishna, A., Sarwate, D.V.: IEEE Trans. Inf. Theory **36**(4), 880–884 (1990)
19. Guenda, K.: Des. Codes Crypt. **62**(1), 31–42 (2012)
20. Forney, G. Jr.: IEEE Trans. Inform. Theory **16**(6), 720–738 (1970)
21. Rosenthal, J., Smarandache, R.: AAECC **10**, 15–32 (1998)
22. Rosenthal, J., York, E.: IEEE Trans. Inform. Theory **45**(6), 1833–1844 (1999)
23. Hole, K.J.: IEEE Trans. Inform. Theory **46**(2), 663–669 (2000)
24. Smarandache, R., Gluesing-Luerssen, H., Rosenthal, J.: IEEE Trans Inform. Theory **47**(5), 2045–2049 (2001)
25. Gluesing-Luerssen, H., Schmale, W.: AAECC **17**(2), 151–170 (2006)
26. Gluesing-Luerssen, H., Tsang, F.L.: Adv. Math. Commun. **2**(1), 55–81 (2008)
27. Aly, S.A., Klappenecker, A., Sarvepalli, P.K.: arXiv:quant-ph/0701037 (2007)
28. Kai, X., Zhu, S., Tang, Y.: Phys. Rev. A. **88**, 029907(E) (2013)
29. Qian, J., Zhang, L.: Discret. Math. **313**(21), 2451–2455 (2013)