On optimal constacyclic codes

Giuliano G. La Guardia *

November 12, 2013

Abstract

In this paper we investigate the class of constacyclic codes, which is a natural generalization of the class of cyclic and negacyclic codes. This class of codes is interesting in the sense that it contains codes with good or even optimal parameters. In this light, we propose constructions of families of classical block and convolutional maximum-distance-separable (MDS) constacyclic codes, as well as families of asymmetric quantum MDS codes derived from (classical-block) constacyclic codes. These results are mainly derived from the investigation of suitable properties on cyclotomic cosets of these corresponding codes.

1 Introduction

The class of constacyclic codes [3–6, 8, 15] has been investigated in the literature. This class of codes contains the well-known class of cyclic and negacyclic codes [5, 12, 24]. Although the theory of cyclic codes is more investigated in the literature, one can also obtain codes with good or even optimal parameters when considering constacyclic codes not equivalent to the cyclic ones. The structure of constacyclic codes is in a certain sense similar to cyclic codes, since they are principal ideals in the corresponding quotient rings.

On the other hand, much investigation has been done concerning the theory of convolutional codes with their corresponding properties, as well as constructions of codes with good parameters or even maximum-distance-separable (MDS) codes (i.e., codes attaining the generalized Singleton bound [27, Theorem 2.2]) [11, 16, 17, 19–21, 26–28, 30].

In the last two decades, many researches have focussed the attention in the investigation of properties of asymmetric quantum error-correcting codes (AQECC) [7, 18, 22, 29, 31, 32], as well as constructions of AQECC with good or optimal parameters (optimal in the sense that the code parameters attain the quantum version of Singleton bound [29, Lemma 3.2] with equality; these codes are called maximum-distance-separable or MDS).

*Giuliano Gadioli La Guardia is with Department of Mathematics and Statistics, State University of Ponta Grossa (UEPG), 84030-900, Ponta Grossa, PR, Brazil.
It is well-known that the searching for codes with good (or optimal) parameters always received much attention in the literature. In order to contribute with this topic of research, we propose constructions of new families of optimal convolutional codes as well as new families of optimal asymmetric quantum codes. To be more specific, in this paper we utilize the families of classical constacyclic MDS codes constructed here in order to obtain optimal convolutional codes. Further, we construct two families of almost MDS codes of length $n = 2q + 2$ over $\mathbb{F}_q$, after deriving the corresponding almost MDS convolutional codes. Additionally, we also utilize these classical MDS codes constructed here to derive families of asymmetric quantum MDS codes. To construct our MDS constacyclic codes, we will compute and characterize all cyclotomic cosets of these codes. 

This paper is arranged as follows. In Section 2 we give the necessary background for the development of this work: Section 2.1 establishes known results on constacyclic codes and Section 2.2 presents a brief review of convolutional codes. Section 3 presents constructions of classical MDS constacyclic codes over $\mathbb{F}_q$ of length $n = q + 1$ and $n = \frac{(q + 1)}{2}$, where $q$ is a prime power; see Lemmas 3.1 to 3.4). These codes are obtained mainly by investigating the structure of the corresponding cosets. In Section 4 we construct new families of optimal convolutional codes, and in Section 5, we propose constructions of new families of optimal asymmetric quantum codes. Finally, in Section 6, we give a brief summary of this paper.

2 Preliminaries

In this section we present preliminary results for the development of this paper. We begin with a review of constacyclic codes, after giving a brief review of convolutional codes.

2.1 Constacyclic codes

Throughout this paper, we always assume that $q$ is a prime power, $\mathbb{F}_q$ is a finite field with $q$ elements, $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ is the (cyclic) multiplicative group of $\mathbb{F}_q$. The order of an element $\alpha \in \mathbb{F}_q^*$ denoted by $\text{ord}(\alpha)$, is the smallest positive integer $t$ such that $\alpha^t = 1$. We always consider that $n$ (the code length) is a positive integer with $\gcd(n, q) = 1$. As usual, we utilize the notation $[n, k, d]_q$ to denote the parameters of a classical linear code of length $n$, dimension $k$ and minimum distance $d$.

Let $r$ be a positive integer with $r|(q - 1)$, $rk = q - 1$, and consider that $\beta$ is a primitive $rn$-th root of unity in $\mathbb{F}_{q^m}$, where $m = \text{ord}_{rn}(q)$ denotes the multiplicative order of $q$ (mod $rn$), (i.e, $m$ is the smallest positive integer such that $rn|(q^m - 1)$). Thus $\xi = \beta^r \in \mathbb{F}_{q^m}$ is a primitive $m$-th root of unity. Moreover $[\beta^n]^r = 1 \implies [\beta^{nr}]^k = 1 \implies [\beta^n]^{(q-1)} = 1 \implies [\beta^n]^q = \beta^n$. Hence, it follows that $\beta^n \in \mathbb{F}_q$. Since $\alpha = \beta^n \neq 0$ then $\alpha \in \mathbb{F}_q^*$ is an element of order $r$. Thus, if we consider the quotient ring $R_n = \mathbb{F}_q/(x^n - \alpha)$,
an $\alpha$-constacyclic code $C$ of length $n$ is a principal ideal of $R_n$ under the usual correspondence $c = (c_0, c_1, \ldots, c_{n-1}) \mapsto c_0 + c_1 x + \ldots + c_{n-1} x^{n-1} \pmod{(x^n - \alpha)}$. The generator polynomial $g(x)$ of $C$ satisfies $g(x)|(x^n - \alpha)$. The roots of $x^n - \alpha$ are given by $\beta^{1+ri}$ for all $0 \leq i \leq n-1$. Let us consider the set $\mathbb{O}_{rn} = \{1 + ri, 0 \leq i \leq n - 1\}$; the defining set of $C$ is given by $Z = \{j \in \mathbb{O}_{rn}|\beta^j \text{ is root of } g(x)\}$. The defining set is a union of $q$-ary cyclotomic cosets given by $C_s = \{s, sq^2, \ldots, sq^{2(m_s-1)}\}$, where $m_s$ is the smallest positive integer such that $sq^{(m_s)} \equiv s \pmod{rn}$. The minimal polynomial (over $\mathbb{F}_q$) of $\beta^j \in \mathbb{F}_{q^n}$ is denoted by $M^{(j)}(x)$ and it is given by $M^{(j)}(x) = \prod_{j \in C_i} (x - \beta^j)$.

The dimension of $C$ is given by $n - |Z|$. Let us recall the concept of $\alpha$-constacyclic BCH codes:

**Definition 2.1 (Constacyclic BCH codes)** Let $q$ be a prime power with $\gcd(n, q) = 1$. Let $\beta$ be a primitive $rn$-th root of unity in $\mathbb{F}_{q^n}$. A $\alpha$-constacyclic code $C$ of length $n$ over $\mathbb{F}_q$ is a BCH code with designed distance $\delta$ if, for some $b = 1 + ri$ we have $g(x) = \lcm\{M^{(b)}(x), M^{(b+i)}(x), \ldots, M^{(b+(d-2))}(x)\}$, i.e., $g(x)$ is the monic polynomial of smallest degree over $\mathbb{F}_q$ having $\alpha^b, \alpha^{b+r}, \ldots, \alpha^{b+(d-2)}$ as zeros. Therefore, $c \in C$ if and only if $c(\alpha^b) = c(\alpha^{(b+r)}) = \ldots = c(\alpha^{(b+\gamma(d-2))}) = 0$. Thus the code has a string of $\delta - 1$ consecutive $r$ powers of $\beta$ as zeros.

The BCH bound for Constacyclic codes (see [3, 15] for instance) establishes that if $C$ is an $\alpha$-constacyclic code of length $n$ over $\mathbb{F}_q$ with generator polynomial $g(x)$ and if $g(x)$ has the elements $\{\beta^{1+ri}|0 \leq i \leq d-2\}$ as roots, ($\beta$ is a primitive $rn$-th root of unity), then the minimum distance $d_C$ of $C$ satisfies $d_C \geq d$. Recall that given an arbitrary $[n, k, d]_q$ linear code $C$, the Singleton bound asserts that $d \leq n - k + 1$. If the parameters of $C$ satisfy $d = n - k + 1$, the code is called maximum-distance-separable (MDS) or optimal.

### 2.2 Convolutional Codes

The class of convolutional codes is a well-studied class of codes [1, 11–13, 26]. We assume the reader is familiar with the theory of convolutional codes. For more details, see [13]. Recall that a polynomial encoder matrix $G(D) \in \mathbb{F}_q[D]^{k \times n}$ is called basic if $G(D)$ has a polynomial right inverse. A basic generator matrix is called reduced (or minimal [12, 13]) 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 $\gamma$ will be called the degree of the resulting code).

**Definition 2.2** [13] A rate $k/n$ convolutional code $C$ with parameters $(n, k; \gamma; m, d_f)_q$ 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, $C = \{u(D)G(D)|u(D) \in \mathbb{F}_q[D]^k\}$, where $n$ is the length, $k$ is the dimension, $\gamma = \sum_{i=1}^k \gamma_i$ is the degree, where $\gamma_i = \max_{1 \leq j \leq n}\{\deg g_{ij}\}$. 

3
\[ m = \max_{1 \leq i \leq k} \{ \gamma_i \} \text{ is the memory and } d_f = \text{wt}(C) = \min\{\text{wt}(v(D)) \mid v(D) \in C, v(D) \neq 0\} \text{ is the free distance of the code.} \]

Recall that if \([n, k, d]_q\) denotes the parameters of a block code with parity check matrix \(H\), then we split \(H\) into \(m + 1\) disjoint submatrices \(H_i\) such that

\[
H = \begin{bmatrix}
H_0 \\
H_1 \\
\vdots \\
H_m
\end{bmatrix}, \text{ where each } H_i \text{ has } n \text{ columns, obtaining the polynomial matrix}
\]

\[
G(D) = \tilde{H}_0 + \tilde{H}_1 D + \tilde{H}_2 D^2 + \ldots + \tilde{H}_m D^m, \tag{1}
\]

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 \(H_i\) has \(\kappa\) rows in total, where \(\kappa\) 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 \(\kappa\) rows. Note that \(m\) is the memory of the resulting convolutional code generated by the matrix \(G(D)\).

**Theorem 2.1** [1, 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 of \(C\) 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 \(d_f\) and \(d_f^\perp\) denote the free distances of \(V\) and \(V^\perp\), respectively, \(d_i\) denote the minimum distance of the code \(C_i = \{ v \in \mathbb{F}_q^n \mid v\tilde{H}_i = 0 \}\) 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 \(d_f \geq d_f^\perp\).

## 3 Classical MDS Codes

In this section we propose the construction of optimal \(\alpha\)-constacyclic codes. It is well known that an \([n, k, d]_q\) \(\alpha\)-constacyclic MDS code of length \(n = q + 1\) over \(\mathbb{F}_q\) exists for \(k\) odd if \(\alpha\) is a quadratic residue in \(\mathbb{F}_q\) and for \(k\) even if \(\alpha\) is not a quadratic residue in \(\mathbb{F}_q\) (see [15]). However, the constructions presented here differs from the ones shown in the literature since they consider properties of \(q\)-ary cyclotomic cosets \((\mod rn)\). In order to proceed further, we will show some useful lemmas that will be utilized in our constructions. Lemmas 3.1 to 3.4 presented here are generalizations of Lemmas 4.1 and 4.4 in [14].

**Lemma 3.1** Let \(q\) be a power of an odd prime and \(n = q + 1\). Assume that \(\alpha \in \mathbb{F}_q^*\) is an element of order \(r \geq 2\), where \(q - 1 = rk\), \(k\) even. Put \(s = n/2\).

Then the following hold:

(a) The unique \(q\)-ary cosets \((\mod rn)\) with only one element are the cosets \(C_s = \{s\}\) and \(C_{s+(r+1)s} = \{(r+1)s\}\);
b) All the remaining $q$-ary cosets \( (\text{mod } rn) \) are given by \( C_{(s-ri)} = \{s-ri, s+ri\} \), where \( 1 \leq i \leq s-1 \).

**Proof:** Notice that \( \gcd(q,n) = 1 \) and \( \text{ord}_{rn}(q) = 2 \) are true.

a) Let us consider \( c = k/2 \). Then we have \( sq = \frac{n}{2}(q-1) + \frac{n}{2} = \frac{nq}{2} + \frac{n}{2} = cnr + \frac{n}{2} \equiv s \pmod{(rn)} \). On the other hand, \((r+1)sq = rsq + sq \equiv rs + s = (r+1)s \pmod{(rn)} \).

b) We have: \((s + ri)q \equiv s + rqi = s + r(q+1)i - ri \equiv s - ri \pmod{(rn)} \). Since \( s = 1 + r\frac{q}{2} \), it follows that \( s \in \mathbb{O}_{rn} \). Therefore, the elements \( s - ri, s + ri \in \mathbb{O}_{rn} \) for all \( 1 \leq i \leq s-1 \). Moreover, it is easy to see that these cosets are mutually disjoint. Further, with exception of the cosets \( C_s = \{s\} \) and \( C_{(r+1)s} = \{(r+1)s\} \), all the remaining cosets have two elements. The union of all cosets have \( 2(s-1) + 2 = n \) elements, hence the result follows. \( \square \)

**Lemma 3.2** Let \( q \) be a power of an odd prime and \( n = q + 1 \). Assume that \( \alpha \in \mathbb{F}_q^* \) is an element of order \( r \geq 2 \), where \( q - 1 = rk \), \( k \) odd. Then the following hold:

a) If \( t = (n + r)/2 \) then the \( q \)-ary coset \( \pmod{(rn)} \) containing \( t \) is of the form \( C_t = \{t, t-r\} \);

b) All the remaining \( q \)-ary cosets \( \pmod{(rn)} \) are of the form \( C_{(t+ri)} = \{t + ri, t - ri - r\} \), where \( 1 \leq i \leq n/2 - 1 \).

**Proof:** Note that \( t = (n + r)/2 = 1 + r \left\lfloor \frac{(k+1)}{2} \right\rfloor \), so the element \( t = (n + r)/2 \) is of the form \( 1 + ri \). Thus the elements \( t + ri, t - ri - r \) also belong to \( \mathbb{O}_{rn} \) for all \( 1 \leq i \leq n/2 - 1 \).

a) Consider that \( c = (k+1)/2 \). Then one has: \( tq = \frac{(n+r)}{2}q = \frac{r(k+1)+2}{2}q = (rc+1)q = (rc+1)(q+1) - rc - 1 = q - rc = q - r \left\lfloor \frac{(k+1)}{2} \right\rfloor = \frac{q+1-r}{2} = \frac{n-r}{2} = n+1 - r = t - r \pmod{(rn)} \).

b) We have: \((t+ri)q \equiv t - r + rqi = t - r + ri(q+1) - ri \equiv t - r - ri \pmod{(rn)} \). Similarly to the proof of Lemma 3.1, it is easy to see that these cosets are mutually disjoint and the union of them has \( n \) elements. \( \square \)

**Lemma 3.3** Let \( q \equiv 1 \pmod{4} \) be a power of an odd prime, \( n = (q+1)/2 \) and \( \alpha \in \mathbb{F}_q^* \) such that \( \text{ord}(\alpha) = r \geq 2 \), where \( q - 1 = rk \), \( k \) even. Then the following hold:

a) One has \( C_n = \{n\} \pmod{(rn)} \); 

b) All the remaining cosets are of the form \( C_{(n-ri)} = \{n-ri, n+ri\} \pmod{(rn)} \), where \( 1 \leq i \leq (n-1)/2 \).

**Proof:** Since \( k \) is even then \( n = 1 + r\frac{k}{2} \in \mathbb{O}_{rn} \). Items a) and b) follow by straightforward computation (note that, from hypothesis, \( n \) is odd). \( \square \)
Lemma 3.4 Let \( q \equiv 3 \pmod{4} \) be a power of an odd prime, \( n = (q + 1)/2 \) and \( \alpha \in \mathbb{F}_q^* \) such that \( \text{ord}(\alpha) = r \geq 2 \), where \( q - 1 = rk \), \( k \) even. Then the following hold:

a) The unitary cosets are \( C_n = \{n\} \) and \( C_{(r+2)n/2} = \left\{ \frac{(r+2)n}{2} \right\} \pmod{rn} \);

b) \( C_{(n-r)} = \{n - ri, n + ri\} \pmod{rn} \), where \( 1 \leq i \leq n/2 - 1 \).

Proof: Note that in this case \( n \) is even. \( \square \)

Remark 3.5 It is interesting to observe that in Lemmas 3.1 to 3.4 we have assumed \( r \geq 2 \) to avoid the case when \( \alpha = 1 \), i.e., cyclic codes.

Lemma 3.6 Let \( q = 2^l \), where \( t \geq 2 \), and \( n = q + 1 \). Assume that \( \alpha \in \mathbb{F}_q^* \) is such that \( \text{ord}(\alpha) = r \), where \( q - 1 = rk \). Suppose also that \( t_0 = \frac{(k-1)}{2} \), \( s = 1 + ri_0 \) and \( t = s + r(1 + \frac{2}{2}) \) (\( t \) is considered \( \pmod{rn} \)). Then the following hold:

a) \( C_s = \{s, s + r\} \) and \( C_t = \{t\} \pmod{rn} \);

b) \( C_{(s-ri)} = \{s - ri, s + ri\} \pmod{rn} \), where \( 1 \leq i \leq q/2 - 1 \).

Proof: We only show Item a): \( sq = \left[ 1 + r\frac{(k-1)}{2} \right] q = q + r(q + 1)\frac{(k-1)}{2} - r\frac{(k-1)}{2} \equiv rk + 1 + r\frac{(k-1)}{2} + r \pmod{rn} \). On the other hand, \( tq \equiv s + r + rq + rq\frac{2}{2} = s + r + rq + r(q + 1)\frac{2}{2} - r\frac{2}{2} \equiv s + r + r\frac{2}{2} = t \pmod{rn} \). \( \square \)

Until now we deal with properties and characterizations of cyclotomic cosets. In the following theorems, we utilize the previous results concerning cosets for the construction of optimal constacyclic codes. As we will see in the following sections, these codes will be utilized in order to construct families of optimal convolutional codes and also to derive families of optimal asymmetric quantum codes.

Theorem 3.7 Assume that all hypothesis of Lemma 3.1 hold. Then there exist MDS constacyclic codes with parameters \( [n, n - 2i - 1, 2i + 2]_q \), for every \( 0 \leq i \leq \frac{q}{2} - 1 \).

Proof: We adopt the same notation of Lemma 3.1. Let us consider the \( \alpha \)-constacyclic code with defining set \( Z = \bigcup_{l=0}^{n} C_{(s+rl)} \), where \( C_s = \{s\} \) and \( C_{(s-ri)} = \{s - ri, s + ri\} \), for every \( 0 \leq i \leq n/2 - 1 \). It is easy to see that \( C \) has dimension \( k = n - 2i - 1 \). From the BCH bound for constacyclic codes and from construction, \( C \) has minimum distance \( d \geq 2i + 2 \). By applying the Singleton bound, it follows that \( d = 2i + 2 \), hence there exists an \( [n, n - 2i - 1, 2i + 2]_q \) MDS code, for every \( 0 \leq i \leq n/2 - 1 \). \( \square \)
Theorem 3.8 Assume that all hypothesis of Lemma 3.2 hold. Then there exist MDS constacyclic codes with parameters \([n, n - 2i - 2, 2i + 3]_q\), for every \(0 \leq i \leq \frac{n}{2} - 2\).

Proof: Let \(C\) be the \(\alpha\)-constacyclic code with defining set \(Z = \bigcup_{l=0}^{i} C_{(s+rl)}\), \(0 \leq i \leq n/2 - 2\). It is easy to see that \(C\) has dimension \(k = n - 2i - 2\). From the BCH bound, from construction and by applying the Singleton bound, one concludes that \(C\) is an \([n, n - 2i - 2, 2i + 3]_q\) MDS code, for every \(0 \leq i \leq n/2 - 2\). □

Theorem 3.9 Assume that all hypothesis of Lemma 3.3 hold. Then there exist MDS constacyclic codes with parameters \([n, n - 2i - 1, 2i + 2]_q\), for every \(0 \leq i \leq (\frac{n-1}{2}) - 1\).

Proof: Let \(C\) be the \(\alpha\)-constacyclic code with defining set \(Z = \bigcup_{l=0}^{i} C_{(n-rl)}\). It is easy to see that \(C\) has dimension \(k = n - 2i - 1\). From the BCH bound, from construction and by applying the Singleton bound, one concludes that \(C\) is an \([n, n - 2i - 1, 2i + 2]_q\) MDS code. □

Remark 3.10 Applying Lemma 3.4 one can get analogous results to that of Theorem 3.9.

Theorem 3.11 Assume all hypothesis of Lemma 3.6 hold. Then there exist MDS constacyclic codes with parameters \([n, n - 2i - 2, 2i + 3]_q\), for every \(0 \leq i \leq \frac{(n-1)}{2} - 2\).

Proof: Let \(C\) be the \(\alpha\)-constacyclic code with defining set \(Z = \bigcup_{l=0}^{i} C_{(s-rl)}\), \(0 \leq i \leq \frac{(n-1)}{2} - 2\). It is easy to see that \(C\) has dimension \(k = n - 2i - 2\). From the BCH bound, from construction and by applying the Singleton bound the result follows. □

Theorem 3.12 Assume all hypothesis of Lemma 3.6 hold. Then there exist MDS constacyclic codes with parameters \([n, n - 2i - 1, 2i + 2]_q\), for every \(0 \leq i \leq \frac{(n-1)}{2} - 1\).

Proof: It suffices to consider \(C\) be the \(\alpha\)-constacyclic code with defining set \(Z = C_1 \cup \bigcup_{l=1}^{i} C_{(t-rl)}\), \(1 \leq i \leq \frac{(n-1)}{2} - 1\). □

Recall the an \([n, k, d]_q\) linear code \(C\) is said almost MDS if it has Singleton defect 1, i.e., \(k = n - r - 1\) and \(d = r + 1\). In this context, we construct a simple family of almost MDS codes in the following theorem:

Theorem 3.13 Assume that \(q \equiv 3 \pmod{4}\) is a power of an odd prime and let \(n = 2q + 2\). Then there exist almost MDS codes with parameters \([n, n-4, d \geq 4]_q\).
Proof: It is easy to see that \( \gcd(q, n) = 1 \) and \( \text{ord}_n(q) = 2 \). We will construct a cyclic (\( \alpha = 1 \)) code having these parameters. Putting \( s = (q - 1)/2 \), we will verify that the \( q \)-ary coset containing \( s \) is given by \( C_s = \{ s, s + 2 \} \). In fact, since \( q = 4k + 3 \) for some \( k \in \mathbb{N} \), we have \( \frac{q - 1}{2} = 2k^2 + 10k + 3 \). Because \( 8k = n - 8 \), it follows that \( sq \equiv 2k + 3 = s + 2 \) (mod \( n \)). Further, the coset \( C_{s+1} \) have two elements and \( C_s \) and \( C_{s+1} \) are disjoint. Then the BCH code with defining set \( Z = C_s \cup C_{s+1} \) has parameters \([n, n - 4, d \geq 4]_q\), as desired. \( \square \)

**Theorem 3.14** Let \( q \) be a power of an odd prime and consider that \( n = 2q^2 - 2 \).

(a) If \( q \geq 5 \) then there exist almost MDS codes with parameters \([n, n - 4, d \geq 4]_q\).

(b) If \( q \geq 7 \) then there exist MDS codes with parameters \([n, n - 7, d \geq 6]_q\).

**Proof:** Note that the \( q \)-cosets \( C_s \) (mod \( n \)) for \( s \) even are singletons.

(a) Moreover the cosets \( C_3 \) has two elements. The BCH code with defining set \( Z = \bigcup_{i=2}^4 C_i \) has the specified parameters.

(b) Since the cosets \( C_1 \) and \( C_3 \) are disjoint and have two elements, the result follows by taking the BCH code with defining set \( Z = \bigcup_{i=0}^4 C_i \). \( \square \)

**Remark 3.15** Note that we have assumed that \( q \geq 7 \) in Item b) of Theorem 3.14 because for \( q = 5 \) one can get an \([8, 1, d \geq 7]_5\) code and not an \([8, 1, d \geq 6]_5\) as stated in such result.

**Theorem 3.16** Assume that \( q \equiv 1 \) (mod \( 4 \)) is a power of an odd prime and let \( n = 2q^2 \). Then there exist almost MDS codes with parameters \([n, n - 3, d \geq 3]_q\).

**Proof:** It is easy to see that the \( q \)-ary coset \( C_{(q+1)/2} \) is given by \( C_{(q+1)/2} = \left\{ \frac{(q+1)}{2} \right\} \) and the coset \( C_{[(q+1)/2] + 1} \) have two elements. Choosing the BCH (cyclic) code with defining set \( Z = C_{(q+1)/2} \cup C_{[(q+1)/2] + 1} \), the result follows. \( \square \)

**Remark 3.17** Let us recall the well-known MDS Conjecture: Let \( q \) be a prime power. If there exists a nontrivial classical \([n, k, d]_q\) MDS code, then \( n \leq q + 1 \), except when \( q \) is even and \( k = 3 \) or \( k = q - 1 \), and in this case one has \( n \leq q + 2 \).

Note that by applying Theorems 3.13, 3.11 and 3.16 one can derive codes with good parameters. In fact, if the MDS conjecture holds, those codes are the best ones known to exist.

### 4 New optimal convolutional codes

Recall that the generalized Singleton bound (see [27, Theorem 2.2]) of an \((n, k, \gamma; m, d_f)_q\) convolutional code is given by \( d_f \leq (n - k)[\lfloor \gamma/k \rfloor + 1] + \gamma + 1 \). If the parameters of a convolutional code \( C \) satisfies the generalized Singleton bound with equality then \( C \) is called maximum-distance-separable (MDS) or optimal code. In this section we shall construct new optimal convolutional
codes. To proceed further, it is necessary to construct a parity check matrix for
the (classical) constacyclic codes involved in the construction method proposed
here.

**Remark 4.1** Let \( \mathcal{B} = \{b_1, \ldots, b_l\} \) be a basis of \( F_q^n \) over \( F_q \). If \( u = (u_1, \ldots, u_n) \in F_q^n \) then one can write the vectors \( u_i, 1 \leq i \leq n \), as linear combinations of the
elements of \( \mathcal{B} \), that is, \( u_i = u_{i1} b_1 + \cdots + u_{il} b_l \). Consider that \( u^{(j)} = (u_{i1}, \ldots, u_{ij}) \) 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 \( 1 \leq j \leq l \).

The following result is a straightforward generalization of [19, Theorem 5.4]. Since we do not see an explicit proof of such result in the literature, we present
it here:

**Theorem 4.2** Assume that \( q \) is a prime power with \( \gcd(n, q) = 1 \), and \( m = \text{ord}_{n}(q) \). Let \( \beta \) be a primitive \( mn \)-th root of unity in \( F_{q^m} \), and \( b = 1 + ri, \) for
some \( 0 \leq i \leq n - 1 \). Then a parity-check matrix for a BCH constacyclic code \( C \) of length \( n \) and designed distance \( \delta \) is given by

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

where each entry is replaced by the corresponding column of \( m \) elements from
\( F_q \) and then removing any linearly dependent rows.

**Proof:** Assume that \( c = (c_0, c_1, \ldots, c_{n-1}) \in C \). Thus we have \( \begin{bmatrix} \beta^b \\ \beta^{(b+r)} \\ \beta^{(b+2r)} \\ \vdots \\ \beta^{[b+r(\delta-2)]} \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{n-1} \end{bmatrix} \) \( = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \). So it follows that

\[
\begin{bmatrix}
1 & \beta^b & \beta^{2b} & \cdots & \beta^{(n-1)b} \\
1 & \beta^{(b+r)} & \beta^{2(b+r)} & \cdots & \beta^{(n-1)(b+r)} \\
1 & \beta^{(b+2r)} & \beta^{2(b+2r)} & \cdots & \beta^{(n-1)(b+2r)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \beta^{[b+r(\delta-2)]} & \beta^{2[b+r(\delta-2)]} & \cdots & \beta^{[n-1][b+r(\delta-2)]}
\end{bmatrix} \begin{bmatrix}
c_0 \\
c_1 \\
c_2 \\
\vdots \\
c_{n-1}
\end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \text{.}
\]

From Remark 4.1 and from the definition of BCH constacyclic codes, the result
follows. \( \square \)

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

**Theorem 4.3** Assume that all hypothesis of Lemma 3.1 hold. Then there exist
MDS convolutional codes with parameters \( (n, n - 2i + 1, 2; 1, 2i + 2)_q \), where
\( 2 \leq i \leq n/2 - 2 \).
Proof: Let $C_2$ be the $\alpha$-constacyclic BCH code with parameters $[n, n - 2i - 1, 2i + 2]_q$ constructed in Theorem 3.7. By Theorem 4.2, a parity check matrix $H_{C_2}$ of $C_2$ is obtained from the matrix

\[
H_2 = \begin{bmatrix}
1 & \beta^s & \beta^{2s} & \ldots & \beta^{(n-1)s} \\
1 & \beta^{(s+r)} & \beta^{2(s+r)} & \ldots & \beta^{(n-1)(s+r)} \\
1 & \beta^{(s+2r)} & \beta^{2(s+2r)} & \ldots & \beta^{(n-1)(s+2r)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \beta^{(s+ri)} & \beta^{2(s+ri)} & \ldots & \beta^{(n-1)(s+ri)} \\
\end{bmatrix}
\]

by expanding each entry as a column vector (containing 2 rows) with respect to some $\mathbb{F}_q$-basis $\beta$ of $\mathbb{F}_q^2$ and then removing one linearly dependent row.

Next we assume that $C_1$ is the $\alpha$-constacyclic BCH code of length $n$ over $\mathbb{F}_q$ generated by $(g_1(x)) = (\langle M^{(s)}(x)M^{(s+r)}(x)\ldots M^{(s+r(i-1))}(x) \rangle)$. Similarly, by Theorem 4.2, $C_1$ has a parity check matrix $H_{C_1}$ derived from the matrix

\[
H_1 = \begin{bmatrix}
1 & \beta^s & \beta^{2s} & \ldots & \beta^{(n-1)s} \\
1 & \beta^{(s+r)} & \beta^{2(s+r)} & \ldots & \beta^{(n-1)(s+r)} \\
1 & \beta^{(s+2r)} & \beta^{2(s+2r)} & \ldots & \beta^{(n-1)(s+2r)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \beta^{(s+r(i-1))} & \beta^{2(s+r(i-1))} & \ldots & \beta^{(n-1)(s+r(i-1))} \\
\end{bmatrix}
\]

by expanding each entry as a column vector with respect to $\beta$ (already done, since $H_1$ is a submatrix of $H_2$) and then removing the unique linearly dependent row. It is easy to see that $C_1$ is an $[n, n - 2i + 1, 2i]_q$ MDS code.

Now, consider $C_0$ be the $[n, n - 2, d_0 \geq 2]_q$ $\alpha$-constacyclic BCH code generated by $M^{(s+r(i))}(x)$. A parity check matrix $H_{C_0}$ of $C_0$ is given by expanding the entries of the matrix

\[
H_0 = \begin{bmatrix}
1 & \alpha^{(s+2i)} & \alpha^{2(s+2i)} & \ldots & \alpha^{(n-1)(s+2i)} \\
\end{bmatrix}
\]

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

Further, let us consider that $V$ is the convolutional code generated by the reduced basic (Theorem 2.1 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 $\delta_V = 2$. Thus the dual $V^\perp$ of the convolutional code $V$ has dimension $n - 2i + 1$ and degree 2. From Theorem 2.1 Item (b), the free distance of $V^\perp$ is bounded by $\min\{d_0 + d_1, d_2\} \leq d^f \leq d_2$. From construction one has $d_2 = 2i + 2, d_1 = 2i$ and $d_0 \geq 2$, so $V^\perp$ has parameters $(n, n - 2i + 1, 2i, 2i + 2)_q$. Applying the generalized Singleton bound we conclude that $V^\perp$ is MDS, as required. \qed
Theorem 4.4 Assume that all hypothesis of Lemma 3.2 hold. Then there exist MDS convolutional codes with parameters \((n, n - 2i, 2; 1, 2i + 3)_q\), where \(2 \leq i \leq n/2 - 2\).

Proof: We omit the proof since it follows the same line to that of Theorem 4.3. □

Theorem 4.5 Assume that all hypothesis of Lemma 3.3 hold. Then there exist MDS convolutional codes with parameters \((n, n - 2i + 1, 2; 1, 2i + 2)_q\), where \(2 \leq i \leq \left(\frac{n-1}{2}\right) - 1\).

Proof: Let \(C_2\), \(C_1\) and \(C_0\) be \(\alpha\)-constacyclic BCH codes of length \(n\) over \(\mathbb{F}_q\) generated, respectively, by the product of the minimal polynomials

\[
C_2 = \langle M^{(n)}(x)M^{(n+r)}(x)\cdots M^{(n+ri)}(x) \rangle,
\]

\[
C_1 = \langle M^{(n)}(x)M^{(n+r)}(x)\cdots M^{(n+ri-r)}(x) \rangle
\]

and

\[
C_0 = \langle M^{(n+ri)}(x) \rangle,
\]

where \(2 \leq i \leq \left(\frac{n-1}{2}\right) - 1\). Applying the same procedure shown in the proof of Theorem 4.3, the result follows. □

Remark 4.6 If we assume that all hypothesis of Lemma 3.4 hold then one can obtain more optimal convolutional codes.

Theorem 4.7 Assume all hypothesis of Theorem 3.11 hold, with \(t \geq 3\). Then there exist MDS convolutional codes with parameters \((n, n - 2i, 2; 1, 2i + 3)_q\), where \(2 \leq i \leq \left(\frac{n-1}{2}\right) - 2\).

Proof: It suffices to consider \(C_2\), \(C_1\) and \(C_0\) the \(\alpha\)-constacyclic BCH codes of length \(n\) over \(\mathbb{F}_q\) generated, respectively, by the product of the minimal polynomials

\[
C_2 = \langle M^{(s)}(x)M^{(s-r)}(x)\cdots M^{(s-ri)}(x) \rangle,
\]

\[
C_1 = \langle M^{(s)}(x)M^{(s-r)}(x)\cdots M^{(s-r[i-1])}(x) \rangle
\]

and

\[
C_0 = \langle M^{(s-ri)}(x) \rangle,
\]

where \(2 \leq i \leq \left(\frac{n-1}{2}\right) - 2\), after proceeding similarly as the proof of Theorem 4.3. □

Theorem 4.8 Assume all hypothesis of Theorem 3.12 hold, with \(t \geq 3\). Then there exist MDS convolutional codes with parameters \((n, n - 2i + 1, 2; 1, 2i + 2)_q\), where \(2 \leq i \leq \left(\frac{n-1}{2}\right) - 2\).
**Proof:** Similar to that of Theorem 4.7. □

**Remark 4.9** a) For every $q = p^t$, where $p$ is an odd prime and $t$ is an odd positive integer, the parameters of the convolutional codes constructed in Theorems 4.3, 4.4 and 4.5 are new; b) The parameters of the convolutional MDS codes constructed in Theorem 4.8 are new; c) Theorems 4.3, 4.4 and 4.5 are generalizations of the results shown in [19] (w.r.t. classical convolutional codes), in the sense that here we construct arbitrary $\alpha$-constacyclic code, whereas in [19], only negacyclic codes (i.e., $\alpha = -1$) are generated; d) In the same context, Theorem 4.7 is a generalization of the results shown in [17]; e) Codes constructed in Theorem 4.3 have the same parameters of the second family of codes shown in [17]. However, the codes constructed here are $\alpha$-constacyclic codes with $\mathrm{ord}(\alpha) \geq 2$ whereas in [17] only cyclic codes ($\alpha = 1$) are constructed; f) Summarizing: in general, several new families of MDS convolutional codes are constructed in this work.

**Theorem 4.10** Let $q$ be a prime power such that $q - 1 = rn$ and let $\alpha \in \mathbb{F}_q^*$ be an element of order $r \geq 1$. Then there exist MDS convolutional codes with parameters $(n, n - c_1, c_2; 1, i + 2)_q$, where $0 \leq i \leq n - 2$ and $c_1, c_2$ are positive integers with $i + 1 = c_1 + c_2$ and $c_1 \geq c_2$.

**Proof:** Since $\mathrm{ord}_n(q) = 1$, then all the $q$-cosets $\mathbb{C}_{1+r_i}$ (mod $rn$) are singletons. Consider $C$ be the $\alpha$-constacyclic code with defining set $Z = \bigcup_{i=0}^{i} \mathbb{C}_{(1+r_i)}$, where $0 \leq i \leq n - 2$; $C$ has parameters $[n, n - i - 1, i + 2]_q$. We next construct a convolutional code $V$ with parameters $(n, c_1, c_2; 1, d_f)_q$. It is easy to see that its dual $V^\perp$ has parameters $(n, n - c_1, c_2; 1, i + 2)_q$ and its is a MDS code. Note that when $r = 1$, $C$ is a Reed-Solomon code over $\mathbb{F}_q$ (see [2]). □

**Theorem 4.11** Assume all the hypothesis of Theorem 3.13 hold. Then there exist almost MDS convolutional codes with parameters $(n, n - 2, 2; 1, 4)_q$.

**Proof:** It suffices to consider the codes constructed in Theorem 3.13, after proceeding similarly as in the proof of Theorem 4.3. □

**Remark 4.12** It is interesting to observe that the convolutional codes derived from Theorem 4.10 are almost MDS in the sense that their defects are $1$ with respect to the generalized Singleton bound. These codes seem to be new.

**Theorem 4.13** Assume all the hypothesis of Theorem 3.14 hold.

a) If $q \geq 5$, there exist almost MDS convolutional codes with parameters $(n, n - 4, 4; 1, 6)_q$. □
3, 1; 1, 4)q.
b) If \( q \geq 7 \), there exist convolutional codes with parameters \((n, n - 4, 3; 1, d_f \geq 6)_q\).

Proof: Similar to that of Theorem 4.3.

\[ \square \]

Remark 4.14 Note that the new convolutional codes derived from Theorem 4.13 - Item b), have Singleton defect at most 2, hence they are also good codes.

5 Asymmetric quantum codes

Asymmetric quantum error-correcting codes (AQECC) [18, 22, 29, 31] are quantum codes defined over quantum channels where the probability of occurrence of qudit-flip errors and phase-shift errors may be different. The combined amplitude damping and dephasing channel (specific to binary systems) is an example for a quantum channel where these probabilities are different.

The scenario is the Hilbert space \( \mathcal{H} = \mathbb{C}^q \otimes \mathbb{C}^q \otimes \ldots \otimes \mathbb{C}^q \) with a orthonormal basis consisting of vectors \( |x\rangle \), where the labels \( x \) are elements of \( \mathbb{F}_q \). The unitary operators \( X(a) \) and \( Z(b) \) for a, b \( \in \mathbb{F}_q \) are defined by \( X(a) |x\rangle = |x + a\rangle \) and \( Z(b) |x\rangle = w^{tr_{\pi/p}(bx)} |x\rangle \), respectively, where \( w = \exp(2\pi i/p) \) is a \( p \)-th root of unity. Assume that \( a = (a_1, \ldots, a_n) \) and \( b = (b_1, \ldots, b_n) \) are vectors in \( \mathbb{F}_q^n \) and consider \( X(a) = X(a_1) \otimes \ldots \otimes X(a_n) \) and \( Z(b) = Z(b_1) \otimes \ldots \otimes Z(b_n) \) be the tensor products of \( n \) error operators. The set \( \mathcal{E}_n = \{ X(a)Z(b) \mid a, b \in \mathbb{F}_q^n \} \) is the error basis on the complex vector space \( \mathbb{C}^q \) and the set \( G_n = \{ w^eX(a)Z(b) \mid a, b \in \mathbb{F}_q^n, c \in \mathbb{F}_p \} \) is the error group associated with \( \mathcal{E}_n \). For a quantum error \( e = w^eX(a)Z(b) \in G_n \), the X-weight is given by \( \text{wt}_X(e) = \# \{ i : 1 \leq i \leq n | a_i \neq 0 \} \); the Z-weight is defined as \( \text{wt}_Z(e) = \# \{ i : 1 \leq i \leq n | b_i \neq 0 \} \) and the symmetric (or quantum) weight \( \text{swt}(e) = \# \{ i : 1 \leq i \leq n | (a_i, b_i) \neq (0, 0) \} \).

An AQECC with parameters \((n, K, d_z/d_x)_q\) is an \( K \)-dimensional subspace of the Hilbert space \( \mathbb{C}^q \) and corrects all qudit-flip errors up to \( \lfloor \frac{d_z}{d_x} \rfloor \) and all phase-shift errors up to \( \lfloor \frac{d_x}{d_z} \rfloor \). An \((n, q^k, d_z/d_x)_q\) code is denoted by \([n, k, d_z/d_x]_q\).

Next we recall the well-known CSS construction:

Lemma 5.1 [7, 23, 25](CSS construction) Let \( C_1 \) and \( C_2 \) denote two classical linear codes with parameters \([n, k_1, d_1]_q\) and \([n, k_2, d_2]_q\), respectively. Assume that \( C_2^\perp \subset C_1 \). Then there exists an AQECC with parameters \([n, k_1 + k_2 - n, d_z/d_x]_q\), where \( d_z = \text{wt}(C_2 \setminus C_2^\perp) \) and \( d_x = \text{wt}(C_1 \setminus C_1^\perp) \). The resulting AQECC code is said pure if, in the above construction, \( d_z = \text{wt}(C_2) \) and \( d_x = \text{wt}(C_1) \).

The following result establishes the Singleton bound to AQECC, i.e., the asymmetric quantum Singleton bound (AQS):}

Lemma 5.2 [29, Lemma 3.2] A pure asymmetric \([n, k, d_z/d_x]_q\) CSS code satisfies \( k \leq n - d_x - d_z + 2 \).
If an AQECC $Q$ have parameters attaining the AQSB with equality we say that $Q$ is maximum-distance-separable (MDS) code. In the following results, new MDS AQECC are constructed.

**Theorem 5.3** Assume all the hypothesis of Lemma 3.1 hold. Then there exist asymmetric quantum MDS codes with parameters $[[n, 2(j-i), (n-2j)/(2i+2)]]_q$, for every $0 \leq i \leq j \leq n/2-2$.

**Proof:** Let $C_2^\perp$ be the $(\alpha$-constacyclic) code with defining set $Z = \bigcup_{i=0}^{j-1} C_{(s+rl)}$, where $C_s$ and $C_{(s-rl)}$ are given in Lemma 3.1. Then $C_2^\perp$ has parameters $[n, n-2j-1, 2j+2]_q$. Next, consider $C_1$ be the $(\alpha$-constacyclic) code with defining set $Z = \bigcup_{i=0}^{j-1} C_{(s+rl)}$, where $0 \leq i \leq j \leq n/2-2$; $C_1$ has parameters $[n, n-2i-1, 2i+2]_q$. From construction one has $C_2^\perp \subset C_1$; since $C_2^\perp$ is a MDS code then also is its (Euclidean) dual code, namely $C_2$, with parameters $[n, 2j+1, n-2j]_q$. The dimension of the resulting CSS codes equals $2(j-i)$. Applying the CSS construction, we obtain an AQECC with parameters $[[n, 2(j-i), (n-2j)/(2i+2)]]_q$. Finally, from the AQSB, we have an AQECC for every $0 \leq i \leq j \leq n/2-2$. Note that the parameters of these codes attain the AQSB with equality, hence they are MDS codes. □

**Theorem 5.4** Assume all the hypothesis of Lemma 3.2 hold. Then there exist asymmetric quantum MDS codes with parameters $[[n, 2(j-i), (n-2j-1)/(2i+3)]]_q$ for every $0 \leq i \leq j \leq n/2-2$.

**Proof:** Let $C_2^+_{1}$ be the code with defining set $Z = \bigcup_{i=0}^{j-1} C_{(t+rl)}$, where $C_t$ and $C_{(t+rl)}$ are given in Lemma 3.2, and assume that $C_1$ is the code with defining set $Z = \bigcup_{i=0}^{j-1} C_{(t+rl)}$, with $0 \leq i \leq j \leq n/2-2$. Proceeding similarly as in the proof of Theorem 5.3, the result follows. □

**Theorem 5.5** Assume all the hypothesis of Lemma 3.3 hold. Then there exist asymmetric quantum MDS codes with parameters $[[n, 2(j-i), (n-2j)/(2i+2)]]_q$, for every $0 \leq i \leq j \leq \frac{(n-1)}{2} - 1$.

**Proof:** Let $C_2^+_{1}$ be the code with defining set $Z = \bigcup_{i=0}^{j-1} C_{(n+rl)}$, where $C_n$ and $C_{(n+rl)}$ are given in Lemma 3.3, and let $C_1$ be the code with defining set $Z = \bigcup_{i=0}^{j-1} C_{(n+rl)}$, where $0 \leq i \leq j \leq (n-1)/2-1$. Proceeding similarly as in the proof of Theorem 5.3, one can get these new codes. □

**Remark 5.6** It is important to observe that one can deduce an analogous of Theorem 4.10 to asymmetric quantum codes, generating in this way more optimal AQECC.
Theorem 5.7 Assume all the hypothesis of Theorem 3.11 hold, with \( t \geq 3 \). Then there exist asymmetric quantum MDS codes with parameters \([n, 2(j - i), (n - 2j - 1)/(2i + 3)]_q\) for every \( 0 \leq i \leq j \leq (n - 1)/2 - 2 \).

Proof: The proof is analogous of that Theorem 5.4. \(\Box\)

Remark 5.8 It is interesting to observe that if all hypothesis of Theorem 3.12 are true, more asymmetric quantum MDS codes can be constructed.

Remark 5.9 Note that (pure) asymmetric quantum MDS codes of lengths \( n = (q + 1)/2 \) and \( n = q + 1 \) over \( \mathbb{F}_q \) with the same parameters of our codes were constructed in [10]. However, those codes of length \( n = q + 1 \) are derived from (classical) extended generalized Reed-Solomon (GRS) codes and those of length \( n = (q + 1)/2 \) are derived from (classical) GRS codes. Additionally, with exception of the recent paper [9] (which deals with constructions of optimal negacyclic codes, i.e., \( \alpha = -1 \)), it seems that until now, none class of optimal asymmetric quantum constacyclic codes was presented in the literature (see [18]). Consequently, the optimal asymmetric quantum codes constructed in the present paper are new.

To illustrate the results shown in this paper, we present three tables containing the parameters of some codes constructed here. The meaning of the parameters are clear from the context, once we have explained it in each corresponding result in which the codes were derived.

6 Summary

In this paper we have constructed several families of constacyclic block and convolutional optimal codes. Further, we also have presented two families of almost MDS block and convolutional codes. Additionally, we also have constructed families of optimal asymmetric quantum codes derived from the classical MDS codes constructed here. These results show that the class of constacyclic codes is also a good resource in order to find codes with good or even optimal parameters.

Acknowledgment

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

References

[1] S. A. Aly, M. Grassl, A. Klappenecker, M. Rötteler, P. K. Sarvepalli. Quantum convolutional BCH codes. e-print arXiv:quant-ph/0703113.
Table 1: Convolutional MDS codes

| Parameters of the new codes | \((n, n - 2i + 1, 2; 1, 2i + 2)_q\), \(q\) odd prime power, \(q - 1 = rk\), \(k\) even, \(n = q + 1\), \(2 \leq i \leq n/2 - 2\) |
|-----------------------------|---------------------------------------------------------------------------------------------------------------|
| \((10, 7, 2; 1, 6)_9\), \((r = 4)\)                                       |                                                                                                               |
| \((10, 5, 2; 1, 8)_9\), \((r = 4)\)                                       |                                                                                                               |
| \((12, 9, 2; 1, 6)_{11}\), \((r = 5)\)                                    |                                                                                                               |
| \((12, 7, 2; 1, 8)_{11}\), \((r = 5)\)                                    |                                                                                                               |
| \((12, 5, 2; 1, 10)_{11}\), \((r = 5)\)                                   |                                                                                                               |
| \((26, 23, 2; 1, 6)_{25}\), \((r = 6)\)                                   |                                                                                                               |
| \((26, 17, 2; 1, 12)_{25}\), \((r = 6)\)                                   |                                                                                                               |
| \((26, 7, 2; 1, 22)_{25}\), \((r = 6)\)                                   |                                                                                                               |

| Parameters of the new codes | \((n, n - 2i, 2; 1, 2i + 3)_q\), \(q\) odd prime power, \(q - 1 = rk\), \(k\) odd, \(n = q + 1\), \(2 \leq i \leq n/2 - 2\) |
|-----------------------------|---------------------------------------------------------------------------------------------------------------|
| \((12, 8, 2; 1, 7)_{11}\), \((k = 5)\)                                       |                                                                                                               |
| \((12, 6, 2; 1, 9)_{11}\), \((k = 5)\)                                       |                                                                                                               |
| \((12, 4, 2; 1, 11)_{11}\), \((k = 5)\)                                     |                                                                                                               |
| \((20, 16, 2; 1, 7)_{19}\), \((k = 9)\)                                     |                                                                                                               |
| \((20, 14, 2; 1, 9)_{19}\), \((k = 9)\)                                     |                                                                                                               |
| \((20, 12, 2; 1, 11)_{19}\), \((k = 9)\)                                   |                                                                                                               |
| \((20, 10, 2; 1, 13)_{19}\), \((k = 9)\)                                   |                                                                                                               |
| \((20, 4, 2; 1, 19)_{19}\), \((k = 9)\)                                   |                                                                                                               |

| Parameters of the new codes | \((n, n - 2i + 1, 2; 1, 2i + 2)_q\), \(q\) odd prime power, \(q \equiv 1 \pmod{4}\), \(q - 1 = rk\), \(k\) even, \(n = (q + 1)/2\), \(2 \leq i \leq \frac{(n-1)}{2} - 1\) |
|-----------------------------|---------------------------------------------------------------------------------------------------------------|
| \((7, 4, 2; 1, 6)_{13}\), \((k = 2)\)                                         |                                                                                                               |
| \((9, 6, 2; 1, 6)_{17}\), \((k = 9)\)                                         |                                                                                                               |
| \((9, 4, 2; 1, 8)_{17}\), \((k = 9)\)                                         |                                                                                                               |
| \((15, 12, 2; 1, 6)_{29}\), \((k = 4; r = 7)\)                             |                                                                                                               |
| \((15, 10, 2; 1, 8)_{29}\), \((k = 4; r = 7)\)                             |                                                                                                               |
| \((15, 8, 2; 1, 10)_{29}\), \((k = 4; r = 7)\)                             |                                                                                                               |
| \((15, 6, 2; 1, 12)_{29}\), \((k = 4; r = 7)\)                             |                                                                                                               |
| \((15, 4, 2; 1, 14)_{29}\), \((k = 4; r = 7)\)                             |                                                                                                               |
Table 2: Asymmetric quantum MDS codes

Parameters of the new codes

\[ [(n, 2(j - i), (n - 2j)/(2i + 2))]_q, \ q \text{ odd prime power, } q - 1 = rk, \ k \text{ even,} \]
\[ n = q + 1, \ 2 \leq i \leq j \leq n/2 - 2 \]

| [10, 6, 4/2]_9 | [10, 4, 4/4]_9 |
| [10, 2, 4/6]_9 |
| [18, 14, 4/2]_{17} |
| [18, 12, 4/4]_{17} |
| [18, 10, 4/6]_{17} |
| [18, 8, 4/8]_{17} |
| [18, 6, 4/10]_{17} |
| [18, 2, 4/14]_{17} |
| [18, 2, 14/4]_{17} |

Parameters of the new codes

\[ [(n, 2(j - i), (n - 2j - 1)/(2i + 3))]_q, \ q \text{ odd prime power, } q - 1 = rk, \ k \text{ odd,} \]
\[ n = q + 1, \ 2 \leq i \leq j \leq n/2 - 2 \]

| [12, 8, 3/3]_{11} |
| [12, 6, 3/5]_{11} |
| [12, 4, 3/7]_{11} |
| [12, 2, 3/9]_{11} |
| [12, 2, 9/3]_{11} |
| [12, 4, 7/3]_{11} |
| [14, 10, 3/3]_{13} (k = 3) |
| [14, 2, 3/11]_{13} (k = 3) |
| [14, 4, 7/5]_{13} (k = 3) |
| [14, 8, 3/5]_{13} (k = 3) |
| [14, 6, 3/7]_{13} (k = 3) |
Table 3: Asymmetric quantum MDS codes

Parameters of the new codes

\[ n, 2(j - i), (n - 2j)/(2i + 2) \]q, \( q \) odd prime power, \( q \equiv 1 \pmod{4}, \ q - 1 = rk, \kern.1em k \ \text{even}, \ n = (q + 1)/2, \ 2 \leq i \leq j \leq \frac{(n-1)}{2} - 1 \]

| Parameters | Codes |
|------------|-------|
| [9, 6, 3/2] | 17 |
| [9, 4, 3/4] | 17 |
| [9, 2, 3/6] | 17 |
| [9, 2, 7/2] | 17 |
| [9, 4, 5/2] | 17 |
| [15, 12, 3/2] | 29 |
| [15, 10, 3/4] | 29 |
| [15, 8, 3/6] | 29 |
| [15, 6, 3/8] | 29 |
| [15, 4, 3/10] | 29 |
| [15, 2, 3/12] | 29 |
| [15, 2, 13/2] | 29 |
| [15, 4, 11/2] | 29 |
| [15, 6, 9/2] | 29 |
| [15, 8, 7/2] | 29 |
| [15, 10, 5/2] | 29 |
| [15, 2, 5/10] | 29 |
| [15, 4, 9/4] | 29 |
[2] 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.

[3] 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.

[4] G. K. Bakshi and M. Raka. A class of constacyclic codes over a finite field. Finite Fields Appl., 18:362-377, 2012.

[5] E. R. Berlekamp. Negacyclic codes for the Lee metric. In Symp. Combinatorial Math. Appli., pp. 1–27, 1967.

[6] T. Blackford. Negacyclic duadic codes. Finite Fields Appl., 14:930-943, 2008.

[7] A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane. Quantum error correction via codes over GF(4). IEEE Trans. Inform. Theory, 44(4):1369–1387, 1998.

[8] B. Chen, Y. Fan, L. Lin, H. Liu. Constacyclic codes over finite fields. Finite Fields Appl., 18:12171231, 2012.

[9] J.-Z. Chen, J.-P. Li, J. Lin. New optimal asymmetric quantum codes derived from negacyclic codes. Int. J. Theor. Phys., doi: 10.1007/s10773-013-1784-z, 2013.

[10] M. F. Ezerman, S. Jitman, K. H. Mao, S. Ling. Pure asymmetric quantum MDS codes from CSS construction: a complete characterization. Int. J. Quantum Inform., 11:1350027-1–10, 2013.

[11] G. D. Forney Jr. Convolutional codes I: algebraic structure. IEEE Trans. Inform. Theory, 16(6):720–738, 1970.

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

[13] R. Johannesson and K. S. Zigangirov. Fundamentals of Convolutional Coding. Digital and Mobile Communication, Wiley-IEEE Press, 1999.

[14] X. Kai and S. Zhu. New Quantum MDS Codes From Negacyclic Codes. IEEE Trans. Inform. Theory, 59(2):1193–1197.

[15] A. Krishna and D. V. Sarwate. Pseudocyclic maximum-distance-separable codes. IEEE Trans. Inform. Theory, 36(4):880-884, 1990.

[16] G. G. La Guardia. Nonbinary convolutional codes derived from group character codes. Discrete Math., 313:2730-2736, 2013.

[17] G. G. La Guardia. On classical and quantum MDS-convolutional BCH codes. IEEE Trans. Inform. Theory, To appear.

[18] G. G. La Guardia. Asymmetric quantum codes: new codes from old. Quantum Inform. Processing, 12:2771-2790, 2013.

[19] G. G. La Guardia. On Negacyclic MDS-Convolutional Codes. e-print arXiv:quant-ph/1310.3265.

[20] L. N. Lee. Short unit-memory byte-oriented binary convolutional codes having maximum free distance. IEEE Trans. Inform. Theory, 22:349–352, 1976.

[21] H. Gluesing-Luerssen, J. Rosenthal, R. Smarandache. Strongly MDS convolutional codes. IEEE Trans. Inform. Theory, 52:584–598, 2006.
[22] L. Ioffe and M. Mezard. Asymmetric quantum error-correcting codes. *Phys. Rev. A*, 75:032345(1–4), 2007.

[23] A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, 52(11):4892–4914, 2006.

[24] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[25] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

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

[27] J. Rosenthal and R. Smarandache. Maximum distance separable convolutional codes. *Applicable Algebra in Eng. Comm. Comput.*, 10:15–32, 1998.

[28] J. Rosenthal and E. V. York. BCH convolutional codes. *IEEE Trans. Inform. Theory*, 45(6):1833-1844, 1999.

[29] P. K. Sarvepalli, A. Klappenecker, M. Rötteler. Asymmetric quantum codes: constructions, bounds and performance. In *Proc. of the Royal Society A*, pp. 1645–1672, 2009.

[30] R. Smarandache, H. G.-Luerssen, J. Rosenthal. Constructions of MDS-convolutional codes. *IEEE Trans. Inform. Theory*, 47(5):2045–2049, 2001.

[31] A. M. Steane. Simple quantum error correcting-codes. *Phys. Rev. A*, 54:4741–4751, 1996.

[32] A. Steane. Enlargement of Calderbank-Shor-Steane quantum codes. *IEEE Trans. Inform. Theory*, 45(7):2492–2495, 1999.