New constructions of quantum MDS convolutional codes derived from generalized Reed-Solomon codes [*]

Baokun Ding [†]   Tao Zhang [‡]   Gennian Ge [§]

Abstract

Quantum convolutional codes can be used to protect a sequence of qubits of arbitrary length against decoherence. In this paper, we give two new constructions of quantum MDS convolutional codes derived from generalized Reed-Solomon codes and obtain eighteen new classes of quantum MDS convolutional codes. Most of them are new in the sense that the parameters of the codes are different from all the previously known ones.

Key words: Quantum MDS convolutional codes, classical convolutional codes, generalized Reed-Solomon codes.

1 Introduction

In recent years, there has been tremendous interest in constructing quantum block codes, which is an important subject in quantum information and quantum computing. Quantum convolutional codes give quantum block codes an alternative to protect quantum information for reliable quantum communication over noisy quantum channels. And quantum convolutional codes can also be used to protect a sequence of qubits of arbitrary length against decoherence. Therefore, constructing good quantum convolutional codes has been an important research problem.

The original definition of quantum convolutional codes appeared in [3]. Afterwards, Ollivier and Tillich [16, 17] presented the fundamentals of quantum convolutional codes and explained how to encode a stream of qubits efficiently. Quantum convolutional codes obtained from classical convolutional

[†]B. Ding is with the School of Mathematical Sciences, Zhejiang University, Hangzhou 310027, China (e-mail: bkding@zju.edu.cn).

[‡]T. Zhang is with the School of Mathematical Sciences, Zhejiang University, Hangzhou 310027, China (e-mail: tzh@zju.edu.cn).

[§]G. Ge is with the School of Mathematical Sciences, Capital Normal University, Beijing 100048, China. He is also with Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing 100048, China (e-mail: gnge@zju.edu.cn).

codes are provided in [7, 15]. Tan and Li [19] proposed five systematic constructions by using LDPC and LDPC-convolutional codes. La Guardia constructed several new families of quantum negacyclic MDS convolutional codes in [14] and unit-memory quantum convolutional BCH codes in [13]. Some new nonbinary quantum convolution codes are also obtained in [4, 22] by using constacyclic codes. Further results about quantum convolutional codes can be found in [5, 8, 9, 10, 18, 20, 21].

Generalized Reed-Solomon codes (GRS codes) are an important group of error correcting codes. They are MDS (maximum distance separable) codes as their parameters meet the Singleton bound. Recently, they were applied to construct quantum codes. In [12], Jin et al. used GRS codes and algebraic geometry codes to construct quantum MDS codes. In [2], Aly et al. presented some quantum MDS convolutional codes from GRS codes based on limit constructions. Some pure asymmetric quantum MDS codes from GRS codes were given in [6]. By using GRS codes, Zhang et al. [23] obtained some new constructions of q-ary quantum MDS codes. It seems that GRS codes are a rich source of constructing quantum MDS codes with good parameters.

In this paper, we present two new constructions of quantum MDS convolutional codes by using GRS codes. Consequently, we obtain eighteen new classes of quantum MDS convolutional codes. Most of them are new in the sense that the parameters of the codes are different from the ones available in the literature.

This paper is organized as follows. In Section 2, we recall some preliminary concepts and results about classical convolutional codes, quantum convolutional codes and GRS codes. In Section 3, we propose new constructions of quantum MDS convolution codes derived from GRS codes. Section 4 concludes the paper.

2 Preliminaries

In this section, we recall some basic notations and necessary facts which are important to our constructions. Throughout this paper, we always assume that q is a prime power and $\mathbb{F}_q$ is the field with q elements if not specified.

A linear $[n, k]$ code $\mathcal{C}$ over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. The weight $\mathrm{wt}(x)$ of a codeword $x \in \mathcal{C}$ is the number of nonzero components of x. The distance of two codewords $x, y \in \mathcal{C}$ is $d(x, y) = \mathrm{wt}(x - y)$. The minimum distance d of $\mathcal{C}$ is the minimum distance between any two distinct codewords of $\mathcal{C}$. An $[n, k, d]_q$ code is an $[n, k]$ code over $\mathbb{F}_q$ with the minimum distance d.

Given two vectors $x = (x_0, x_1, \cdots, x_{n-1})$, $y = (y_0, y_1, \cdots, y_{n-1}) \in \mathbb{F}_q^n$. We define the Euclidean inner product as $\langle x, y \rangle_E = \sum_{i=0}^{n-1} x_i y_i$. When $q = l^2$, where l is a prime power, we also consider the Hermitian inner product which is defined by $\langle x, y \rangle_H = \sum_{i=0}^{n-1} x_i y_i^l$. We define the Euclidean dual code of $\mathcal{C}$ as

$$\mathcal{C}^{\perp E} = \{x \in \mathbb{F}_q^n | \langle x, y \rangle_E = 0 \text{ for all } y \in \mathcal{C}\}.$$

Similarly, the Hermitian dual code of $\mathcal{C}$ is defined as

$$\mathcal{C}^{\perp H} = \{x \in \mathbb{F}_q^n | \langle x, y \rangle_H = 0 \text{ for all } y \in \mathcal{C}\}.$$

A linear code $\mathcal{C}$ is called Euclidean (Hermitian) dual-containg if $\mathcal{C}^{\perp E} \subseteq \mathcal{C}$ ($\mathcal{C}^{\perp H} \subseteq \mathcal{C}$, respectively). The following theorem gives a bound on the minimum distance of a linear code.

Lemma 2.1. [11] *Every linear $[n, k, d]_q$ code $\mathcal{C}$ satisfies the Singleton bound*

$$d \leq n - k + 1.$$

A code achieving this bound is called an MDS code.

2.1 Classical Convolution Codes

Recall that a convolutional code $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_{q^2}$ is a free module of rank k that is a direct summand of $\mathbb{F}_{q^2}[D]^n$ and a polynomial encoder matrix $G(D) = (g_{ij}) \in \mathbb{F}_{q^2}[D]^{k \times n}$ is called basic if it has a polynomial right inverse. A basic generator matrix is called reduced (or minimal [11]) if the overall constraint length $\gamma = \Sigma_{i=1}^k \gamma_i$ has the smallest value among all basic generator matrices, where $\gamma_i = \max_{1 \leq j \leq n}\{\deg g_{ij}\}$; in this case the overall constraint length γ will be called the degree of the code.

Definition 2.1. [2] *A convolutional code V with parameters $(n, k, \gamma; \mu, d_f)_{q^2}$ is a submodule of $\mathbb{F}_{q^2}[D]^n$ generated by a reduced basic matrix $G(D) = (g_{ij}) \in \mathbb{F}_{q^2}[D]^{k \times n}$, $V = \{\mathbf{u}(D)G(D)|\mathbf{u}(D) \in \mathbb{F}_{q^2}[D]^k\}$, where n is the length, k is the dimension, $\gamma = \Sigma_{i=1}^k \gamma_i$ is the degree, $\mu = \max_{1 \leq i \leq k}\{\gamma_i\}$ is the memory and $d_f = wt(V) = \min\{wt(\mathbf{v}(D))|\mathbf{v}(D) \in V, \mathbf{v}(D) \neq 0\}$ is the free distance of the code. Here, $wt(\mathbf{v}(D)) = \Sigma_{i=1}^n wt(v_i(D))$, where $wt(v_i(D))$ is the number of nonzero coefficients of $v_i(D)$.*

We define the Hermitian inner product on $\mathbb{F}_{q^2}[D]^n$ as $\langle \mathbf{u}(D), \mathbf{v}(D) \rangle_H = \Sigma_i \mathbf{u}_i \cdot \mathbf{v}_i^q$, where $\mathbf{u}_i, \mathbf{v}_i \in \mathbb{F}_{q^2}^n$, $\mathbf{v}_i = (v_{1i}, v_{2i}, \cdots, v_{ni})$ and $\mathbf{v}_i^q = (v_{1i}^q, v_{2i}^q, \cdots, v_{ni}^q)$. The Hermitian dual of the code V is defined by

$$V^{\perp_H} = \{\mathbf{u}(D) \in \mathbb{F}_{q^2}[D]^n | \langle \mathbf{u}(D), \mathbf{v}(D) \rangle_H = 0 \text{ for all } \mathbf{v}(D) \in V\}.$$

Let $\mathcal{C}$ be an $[n, k, d]_{q^2}$ linear code with parity check matrix H. Split H into $\mu + 1$ disjoint submatrices H_i such that

$$H = \begin{pmatrix} H_0 \\ H_1 \\ \vdots \\ H_\mu \end{pmatrix}, \tag{1}$$

where each H_i has n columns. Then we obtain the polynomial matrix

$$G(D) = \tilde{H}_0 + \tilde{H}_1 D + \cdots + \tilde{H}_\mu D^\mu, \tag{2}$$

where the matrices $\tilde{H}_i$ are derived from the respective matrices H_i by adding zero-rows at the bottom to ensure that the matrix $\tilde{H}_i$ has κ rows for all $1 \leq i \leq \mu$, and here κ denotes the maximal number of rows among the matrices H_i, for $1 \leq i \leq \mu$. Then the matrix $G(D)$ with κ rows generates a convolutional code and μ is the memory of the code.

Theorem 2.2. [1] *Suppose that $\mathcal{C}$ is a linear code over $\mathbb{F}_{q^2}$ with parameters $[n, k, d]_{q^2}$ and assume also that $H \in \mathbb{F}_{q^2}^{(n-k) \times n}$ is a parity check matrix for $\mathcal{C}$ partitioned into submatrices $H_0, H_1, \cdots, H_\mu$ as in (1) such that $\kappa = rank(H_0)$ and $rank(H_i) \leq \kappa$ for $1 \leq i \leq \mu$ and consider the polynomial matrix $G(D)$ as in (2). Then we have:*

(a) The matrix $G(D)$ is a reduced basic generator matrix.

(b) If $\mathcal{C}^{\perp H} \subseteq \mathcal{C}$, then the convolutional code $V = \{\mathbf{u}(D)G(D) | \mathbf{u}(D) \in \mathbb{F}_{q^2}[D]^{n-k}\}$ satisfies $V \subseteq V^{\perp H}$.

(c) If d_f and $d_f^{\perp H}$ denote the free distances of V and $V^{\perp H}$ respectively, d_i denotes the minimum distance of the code $\mathcal{C}_i = \{\mathbf{v} \in \mathbb{F}_{q^2}^n | \mathbf{v} \tilde{H}_i^t = 0\}$ and $d^{\perp H}$ is the minimum distance of $\mathcal{C}^{\perp H}$, then one has $\min\{d_0 + d_\mu\} \leq d_f^{\perp H} \leq d$ and $d_f \geq d^{\perp H}$.

2.2 Quantum Convolutional Codes

Quantum convolutional codes are defined as infinite versions of quantum stabilizer codes. The code is specified by its stabilizer which is a subgroup of the infinite version of the Pauli group that consists of tensor products of generalized Pauli matrices acting on a semi-infinite stream of qudits. The stabilizer can be described by a matrix with polynomial entries

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

satisfying $X(D)Z(1/D)^t - Z(D)X(1/D)^t = 0$. A full-rank stabilizer matrix $S(D)$ given above defines a quantum convolutional code $\mathcal{C}$ with parameters $[(n, k, \mu; \gamma, d')]_q$, where n is called the frame size, k is the number of logical qudits per frame and k/n is the rate of $\mathcal{C}$. It can be used to encode a sequence of blocks with k qudits in each block into a sequence of blocks with n qudits. The memory of the code is defined as $\mu = \max_{1 \leq i \leq n-k, 1 \leq j \leq n}\{\max\{\deg X_{ij}(D), \deg Z_{ij}(D)\}\}$. And d' denotes the free distance, γ denotes the degree.

In the sequel, we need the following result about how to construct quantum convolutional stabilizer codes by using classical convolutional codes.

Lemma 2.3. [1] *Let V be an $(n, (n-k)/2, \gamma; \mu)_{q^2}$ convolutional code satisfying $V \subseteq V^{\perp H}$. Then there exists an $[(n, k, \mu; \gamma, d')]_q$ convolutional stabilizer code whose free distance is given by $d' = wt(V^{\perp H} \backslash V)$, which is said to be pure if $d' = wt(V^{\perp H})$.*

Lemma 2.4. [2, 14] *The free distance of an $[(n, k, \mu; \gamma, d')]_q$, $\mathbb{F}_{q^2}$-linear pure convolutional stabilizer code is bounded by*

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

A quantum convolutional code achieving this bound is called a quantum MDS convolutional code.

2.3 Generalized Reed-Solomon codes

Now we recall the basics of GRS codes. Let n be any integer with $1 \leq n \leq q$. Choose $\mathbf{a} = (a_0, \cdots, a_{n-1})$ to be an n-tuple of distinct elements of $\mathbb{F}_q$, and $\mathbf{v} = (v_0, \cdots, v_{n-1})$ to be an n-tuple of nonzero elements

of $\mathbb{F}_q$. Let k be an integer with $1 \leq k \leq n$. Then the codes

$$GRS_k(\mathbf{a}, \mathbf{v}) = \{(v_0 f(a_0), v_1 f(a_1), \cdots, v_{n-1} f(a_{n-1})) | f \in \mathcal{P}_k\},$$

where $\mathcal{P}_k$ denote the set of polynomials of degree less than k in $\mathbb{F}_q[x]$, are the GRS codes. It is well known that a GRS code $GRS_k(\mathbf{a}, \mathbf{v})$ is an MDS code with parameters $[n, k, n-k+1]_q$.

A generator matrix of $GRS_k(\mathbf{a}, \mathbf{v})$ is

$$G = \begin{pmatrix} v_0 & v_1 & \cdots & v_{n-1} \\ v_0 a_0 & v_1 a_1 & \cdots & v_{n-1} a_{n-1} \\ v_0 a_0^2 & v_1 a_1^2 & \cdots & v_{n-1} a_{n-1}^2 \\ \vdots & \vdots & \vdots & \vdots \\ v_0 a_0^{k-1} & v_1 a_1^{k-1} & \cdots & v_{n-1} a_{n-1}^{k-1} \end{pmatrix}.$$

And a parity check matrix of $GRS_k(\mathbf{a}, \mathbf{v})$ is the generator matrix of $GRS_{n-k}(\mathbf{a}, \mathbf{w})$, where $\mathbf{w}$ is any nonzero codeword in the 1-dimensional code $GRS_{n-1}(\mathbf{a}, \mathbf{v})^{\perp_E}$ and satisfies

$$\sum_{i=0}^{n-1} w_i v_i h(a_i) = 0$$

for any polynomial $h \in \mathcal{P}_{n-1}$. Therefore a parity check matrix for $GRS_k(\mathbf{a}, \mathbf{v})$ is

$$H = \begin{pmatrix} w_0 & w_1 & \cdots & w_{n-1} \\ w_0 a_0 & w_1 a_1 & \cdots & w_{n-1} a_{n-1} \\ w_0 a_0^2 & w_1 a_1^2 & \cdots & w_{n-1} a_{n-1}^2 \\ \vdots & \vdots & \vdots & \vdots \\ w_0 a_0^{n-k-1} & w_1 a_1^{n-k-1} & \cdots & w_{n-1} a_{n-1}^{n-k-1} \end{pmatrix}.$$

In order to construct good quantum convolutional codes, we need the following two theorems which collect some known infinite families of Hermitian dual-containing GRS codes.

Theorem 2.5. [23]

(1) *Let q be an odd prime power with the form $2am + 1$. Then for each $1 \leq b \leq 2a$, there exists a $[\frac{b(q^2-1)}{2a}, \frac{b(q^2-1)}{2a} - s, s+1]_{q^2}$ Hermitian dual-containing GRS code, where $1 \leq s \leq (a+1)m$.*

(2) *Let q be an odd prime power with the form $2am + 1$. Then for integers b, c such that $b, c \geq 0$ and $1 \leq b + c \leq 2a$, there exists a $[\frac{b(q^2-1)}{2a} + c(\frac{q^2-1}{2a} - q - 1), \frac{b(q^2-1)}{2a} + c(\frac{q^2-1}{2a} - q - 1) - s, s+1]_{q^2}$ Hermitian dual-containing GRS code, where $1 \leq s \leq (a+1)m - 1$.*

5

(3) Let q be an odd prime power with the form $2am - 1$. Then for each $1 \leq b \leq 2a$, there exists a $[\frac{b(q^2-1)}{2a}, \frac{b(q^2-1)}{2a} - s, s + 1]_{q^2}$ Hermitian dual-containing GRS code, where $1 \leq s \leq (a+1)m - 2$.

(4) Let q be an odd prime power with the form $2am - 1$. Then for integers b, c such that $b, c \geq 0$ and $1 \leq b + c \leq 2a$, there exists a $[\frac{b(q^2-1)}{2a} + c(\frac{q^2-1}{2a} - q + 1), \frac{b(q^2-1)}{2a} + c(\frac{q^2-1}{2a} - q + 1) - s, s + 1]_{q^2}$ Hermitian dual-containing GRS code, where $1 \leq s \leq (a+1)m - 3$.

(5) Let q be an odd prime power with the form $2am - 1$ where a is an odd integer. Then for integers c_1, c_2, c_3 such that $c_1, c_2, c_3 \geq 0$, $0 \leq c_1 + c_2 \leq a$, $0 \leq c_1 + c_3 \leq a$ and $c_1 + c_2 + c_3 \geq 1$, there exists a $[\frac{(c_2+c_3)(q^2-1)}{2a} + c_1(\frac{q^2-1}{a} - q + 1), \frac{(c_2+c_3)(q^2-1)}{2a} + c_1(\frac{q^2-1}{a} - q + 1) - s, s + 1]_{q^2}$ Hermitian dual-containing GRS code, where $1 \leq s \leq (a+1)m - 2$.

(6) Let q be an odd prime power with the form $q = 2ab - 1$, where $\gcd(a, b) = 1$ and a, b are odd. Then for integer c such that $1 \leq c \leq 2(a + b - 1)$, there exists a $[c(q - 1), c(q - 1) - s, s + 1]_{q^2}$ Hermitian dual-containing GRS code, where $1 \leq s \leq ab + c_1 - 2$,

$$c_1 = \begin{cases} c; & \text{if } 1 \leq c \leq a + b - 1, \\ \lfloor \frac{c}{2} \rfloor; & \text{if } a + b \leq c \leq 2(a + b - 1). \end{cases}$$

(7) Let q be an odd prime power with the form $q = 2ab + 1$, where $\gcd(a, b) = 1$ and a, b are odd. Then for integer c such that $1 \leq c \leq 2(a + b - 1)$, there exists a $[c(q + 1), c(q + 1) - s, s + 1]_{q^2}$ Hermitian dual-containing GRS code, where $1 \leq s \leq ab + c_1$,

$$c_1 = \begin{cases} c; & \text{if } 1 \leq c \leq a + b - 1, \\ \lfloor \frac{c}{2} \rfloor; & \text{if } a + b \leq c \leq 2(a + b - 1). \end{cases}$$

Theorem 2.6. [12]

(1) Let t be a divisor of $q^2 - 1$. Then, for any $r \leq (q^2 - 1)/t$ and $s \leq (t - 1)/(q + 1)$, there exists an $[n, n - s, s + 1]_{q^2}$ Hermitian dual-containing GRS code for both $n = rt$ and $rt + 1$.

(2) For any $2 \leq n \leq q^2$, we write $n = n_1 + \cdots + n_t$ with $1 \leq t \leq q$ and $2 \leq n_i \leq q$ for all i. Let $1 \leq s \leq \min\{n_1, \cdots, n_t\}/2$. Then there exists an $[n, n - s, s + 1]_{q^2}$ Hermitian dual-containing GRS code.

3 Constructions

It is well known that a suitable submatrix of the parity check matrix of a GRS code still corresponds to a GRS code and there are many available choices for such submatrices. Because of this nice property, we are able to construct quantum MDS convolutional codes from GRS codes. We propose two new constructions of quantum MDS convolutional codes in this section.

3.1 Quantum MDS convolutional codes with $\mu = 1$

Theorem 3.1. *Let $\mathcal{C}$ be a Hermitian dual-containing $[n, k, d]_{q^2}$ GRS code, $k \neq n/2$. Then there exist quantum MDS convolutional codes with parameters $[(n, n - 2t_0, 1; n - k - t_0, n - k + 1)]_q$, where $(n - k)/2 \leq t_0 < n - k$.*

Proof. Suppose H is the parity check matrix of $\mathcal{C}$ and split it into two disjoint submatrices such that

$$H = \begin{pmatrix} H_0 \\ H_1 \end{pmatrix},$$

where H_0 has t_0 rows and H_1 has $t_1 = n - k - t_0$ rows. Since $(n - k)/2 \leq t_0 < n - k$, we have $t_0 \geq t_1$. It is obvious that H_i is still a parity check matrix of an $[n, n - t_i, t_i + 1]_{q^2}$ GRS code, for $i = 0, 1$. According to Theorem 2.2, we obtain a convolutional code V that is generated by the reduced basic generator matrix

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

where $\tilde{H}_0 = H_0$ and $\tilde{H}_1$ is derived from H_1 by adding zero-rows at the bottom such that the number of rows of $\tilde{H}_1$ is exactly equal to the number of rows of $\tilde{H}_0$. It follows from Theorem 2.2 that V is a convolutional code of dimension t_0, degree $n - k - t_0$, memory 1 and free distance $\geq k + 1$. For the free distance of $V^{\perp_H}$, we have $\min\{t_0 + t_1 + 2, n - k + 1\} \leq d_f^{\perp_H} \leq n - k + 1$ which forces to $d_f^{\perp_H} = n - k + 1$.

Besides, we have $\mathcal{C}^{\perp_H} \subseteq \mathcal{C}$ which gives $V \subseteq V^{\perp_H}$ by Lemma 2.3. Thus we obtain an $[(n, n - 2t_0, 1; n - k - t_0, d')]_q$ quantum convolutional code W, where $d' = wt(V^{\perp_H} \backslash V)$. From Lemma 2.4, we have

$$
\begin{aligned}
d' &\leq \frac{n - k}{2}(\lfloor \frac{2\gamma}{n + k} \rfloor + 1) + \gamma + 1 \\
&\leq t_0(\lfloor \frac{n - k - t_0}{n - t_0} \rfloor + 1) + n - k - t_0 + 1 \\
&\leq n - k + 1.
\end{aligned}
$$

Because of the Hermitian dual-containing property of $\mathcal{C}$ and $k \neq n/2$, we have $d_f^{\perp_H} < d_f$. Thus, d' achieves the bound and W is a quantum MDS convolutional code. $\qquad\square$

It is easy to see that the theorem above is very powerful and can propose about $(n - k)/2$ quantum MDS convolutional codes from each $[n, k, d]_{q^2}$ Hermitian dual-containing GRS code. Combining Theorems 2.5, 2.6 and 3.1, we have the following nine new families of quantum MDS convolutional codes.

Theorem 3.2. *(1) Let q be an odd prime power with the form $2am + 1$. Then for each $1 \leq b \leq 2a$, there exists a $[(\frac{b(q^2 - 1)}{2a}, \frac{b(q^2 - 1)}{2a} - 2t_0, 1; s - t_0, s + 1)]_q$ quantum MDS convolutional code, where $1 \leq s \leq (a + 1)m$, $s/2 \leq t_0 < s$.*

(2) *Let q be an odd prime power with the form $2am+1$. Then for integers b,c such that $b,c \geq 0$ and $1 \leq b+c \leq 2a$, there exists a $[(\frac{b(q^2-1)}{2a}+c(\frac{q^2-1}{2a}-q-1), \frac{b(q^2-1)}{2a}+c(\frac{q^2-1}{2a}-q-1)-2t_0, 1; s-t_0, s+1)]_q$ quantum MDS convolutional code, where $1 \leq s \leq (a+1)m-1$, $s/2 \leq t_0 < s$.*

(3) *Let q be an odd prime power with the form $2am-1$. Then for each $1 \leq b \leq 2a$, there exists a $[(\frac{b(q^2-1)}{2a}, \frac{b(q^2-1)}{2a} - 2t_0, 1; s-t_0, s+1)]_q$ quantum MDS convolutional code, where $1 \leq s \leq (a+1)m-2$, $s/2 \leq t_0 < s$.*

(4) *Let q be an odd prime power with the form $2am-1$. Then for integers b,c such that $b,c \geq 0$ and $1 \leq b+c \leq 2a$, there exists a $[(\frac{b(q^2-1)}{2a}+c(\frac{q^2-1}{2a}-q+1), \frac{b(q^2-1)}{2a}+c(\frac{q^2-1}{2a}-q+1)-2t_0, 1; s-t_0, s+1)]_q$ quantum MDS convolutional code, where $1 \leq s \leq (a+1)m-3$, $s/2 \leq t_0 < s$.*

(5) *Let q be an odd prime power with the form $2am-1$ where a is an odd integer. Then for integers c_1, c_2, c_3 such that $c_1, c_2, c_3 \geq 0$, $0 \leq c_1+c_2 \leq a$, $0 \leq c_1+c_3 \leq a$ and $c_1+c_2+c_3 \geq 1$, there exists a $[(\frac{(c_2+c_3)(q^2-1)}{2a}+c_1(\frac{q^2-1}{a}-q+1), \frac{(c_2+c_3)(q^2-1)}{2a}+c_1(\frac{q^2-1}{a}-q+1)-2t_0, 1; s-t_0, s+1)]_q$ quantum MDS convolutional code, where $1 \leq s \leq (a+1)m-2$, $s/2 \leq t_0 < s$.*

(6) *Let q be an odd prime power with the form $q = 2ab-1$, where $\gcd(a,b) = 1$ and a,b are odd. Then for integer c such that $1 \leq c \leq 2(a+b-1)$, there exists a $[(c(q-1), c(q-1)-2t_0, 1; s-t_0, s+1)]_q$ quantum MDS convolutional code, where $1 \leq s \leq ab+c_1-2$, $s/2 \leq t_0 < s$,*

$$c_1 = \begin{cases} c; & \text{if } 1 \leq c \leq a+b-1, \\ \lfloor \frac{c}{2} \rfloor; & \text{if } a+b \leq c \leq 2(a+b-1). \end{cases}$$

(7) *Let q be an odd prime power with the form $q = 2ab+1$, where $\gcd(a,b) = 1$ and a,b are odd. Then for integer c such that $1 \leq c \leq 2(a+b-1)$, there exists a $[(c(q+1), c(q+1)-2t_0, 1; s-t_0, s+1)]_q$ quantum MDS convolutional code, where $1 \leq s \leq ab+c_1$, $s/2 \leq t_0 < s$,*

$$c_1 = \begin{cases} c; & \text{if } 1 \leq c \leq a+b-1, \\ \lfloor \frac{c}{2} \rfloor; & \text{if } a+b \leq c \leq 2(a+b-1). \end{cases}$$

(8) *Let t be a divisor of q^2-1. Then, for any $r \leq (q^2-1)/t$ and $s \leq (t-1)/(q+1)$, there exists an $[(n, n-2t_0, 1; s-t_0, s+1)]_q$ quantum MDS convolutional code for both $n = rt$ and $rt+1$, where $s/2 \leq t_0 < s$.*

(9) *For any $2 \leq n \leq q^2$, we write $n = n_1 + \cdots + n_t$ with $1 \leq t \leq q$ and $2 \leq n_i \leq q$ for all i. Let $1 \leq s \leq \min\{n_1, \cdots, n_t\}/2$. Then there exists an $[(n, n - 2t_0, 1; s - t_0, s+1)]_q$ quantum MDS convolutional code, where $s/2 \leq t_0 < s$.*

Table 1 lists some quantum MDS convolutional codes obtained from Theorem 3.2.

8

Table 1: Quantum MDS Convolutional Codes

q	a	b	c	$[(n, k, \mu; \gamma, d')]_q$	s	t_0
17	1	2	$\diagdown$	$[(288, 288 - 2t_0, 1; s - t_0, s + 1)]_{17}$	$1 \leq s \leq 16$	$s/2 \leq t_0 < s$
17	2	2	1	$[(198, 198 - 2t_0, 1; s - t_0, s + 1)]_{17}$	$1 \leq s \leq 11$	$s/2 \leq t_0 < s$
11	2	4	$\diagdown$	$[(120, 120 - 2t_0, 1; s - t_0, s + 1)]_{11}$	$1 \leq s \leq 7$	$s/2 \leq t_0 < s$
23	3	3	2	$[(394, 394 - 2t_0, 1; s - t_0, s + 1)]_{23}$	$1 \leq s \leq 13$	$s/2 \leq t_0 < s$
29	3	5	10	$[(300, 300 - 2t_0, 1; s - t_0, s + 1)]_{29}$	$1 \leq s \leq 20$	$s/2 \leq t_0 < s$
31	3	5	10	$[(320, 320 - 2t_0, 1; s - t_0, s + 1)]_{31}$	$1 \leq s \leq 20$	$s/2 \leq t_0 < s$

3.2 Quantum MDS convolutional codes with $\mu = 2$

The following is a similar construction with memory and degree both equal two.

Theorem 3.3. *Let $\mathcal{C}$ be a Hermitian dual-containing $[n, k, d]_{q^2}$ GRS code, $n/2 < k < n - 2$. Then there exist a quantum MDS convolutional code with parameters $[(n, 2k - n + 4, 2; 2, n - k + 1)]_q$.*

Proof. Suppose H is the parity check matrix of $\mathcal{C}$ and split it into three disjoint submatrices such that

$$H = \begin{pmatrix} H_0 \\ H_1 \\ H_2 \end{pmatrix},$$

where H_0 has $t_0 = n - k - 2$ rows and both H_1 and H_2 have only one row. It is obvious to see that H_0 is the parity check matrix of an $[n, k + 2, n - k - 1]_{q^2}$ GRS code and H_i is the parity check matrix of an $[n, n - 1, 2]_{q^2}$ GRS code, for $i = 1, 2$. According to Theorem 2.2, we obtain a convolutional code V that is generated by the reduced basic generator matrix

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

where $\tilde{H}_0 = H_0$ and $\tilde{H}_1$ and $\tilde{H}_2$ are derived from H_1 and H_2 respectively, by adding zero-rows at the bottom such that the numbers of rows of $\tilde{H}_1$ and $\tilde{H}_2$ are exactly equal to the number of rows of $\tilde{H}_0$. It follows from Theorem 2.2 that V is a convolutional code of dimension t_0, degree 2, memory 2 and free distance $\geq k + 1$. For the free distance of $V^{\perp_H}$, we have $\min\{t_0 + t_2 + 2, n - k + 1\} \leq d_f^{\perp_H} \leq n - k + 1$ which forces to $d_f^{\perp_H} = n - k + 1$.

Besides, we have $\mathcal{C}^{\perp H} \subseteq \mathcal{C}$ which gives $V \subseteq V^{\perp H}$ by Lemma 2.3. Thus we obtain an $[(n, 2k - n + 4, 2; 2, d')]_q$ quantum convolutional code W, where $d' = wt(V^{\perp H} \setminus V)$. It follows from Lemma 2.4 that

$$
\begin{aligned}
d' &\leq \frac{n-k}{2}(\lfloor \frac{2\gamma}{n+k} \rfloor + 1) + \gamma + 1 \\
&\leq (n-k-2)(\lfloor \frac{4}{2k+4} \rfloor + 1) + 3 \\
&\leq n - k + 1.
\end{aligned}
$$

Because of the Hermitian dual-containing property of $\mathcal{C}$ and $k \neq n/2$, we have $d_f^{\perp H} < d_f$. Thus, d' achieves the bound and W is a quantum MDS convolutional code. $\square$

By Theorems 2.5, 2.6 and 3.3, we have the following nine new families of quantum MDS convolutional codes.

Theorem 3.4. *(1) Let q be an odd prime power with the form $2am + 1$. Then for each $1 \leq b \leq 2a$, there exists a $[(\frac{b(q^2-1)}{2a}, \frac{b(q^2-1)}{2a} - 2s + 4, 2; 2, s+1)]_q$ quantum MDS convolutional code, where $3 \leq s \leq (a+1)m$.*

(2) Let q be an odd prime power with the form $2am + 1$. Then for integers b, c such that $b, c \geq 0$ and $1 \leq b+c \leq 2a$, there exists a $[(\frac{b(q^2-1)}{2a} + c(\frac{q^2-1}{2a} - q - 1), \frac{b(q^2-1)}{2a} + c(\frac{q^2-1}{2a} - q - 1) - 2s + 4, 2; 2, s+1)]_q$ quantum MDS convolutional code, where $3 \leq s \leq (a+1)m - 1$.

(3) Let q be an odd prime power with the form $2am - 1$. Then for each $1 \leq b \leq 2a$, there exists a $[(\frac{b(q^2-1)}{2a}, \frac{b(q^2-1)}{2a} - 2s + 4, 2; 2, s+1)]_q$ quantum MDS convolutional code, where $3 \leq s \leq (a+1)m - 2$.

(4) Let q be an odd prime power with the form $2am - 1$. Then for integers b, c such that $b, c \geq 0$ and $1 \leq b+c \leq 2a$, there exists a $[(\frac{b(q^2-1)}{2a} + c(\frac{q^2-1}{2a} - q + 1), \frac{b(q^2-1)}{2a} + c(\frac{q^2-1}{2a} - q + 1) - 2s + 4, 2; 2, s+1)]_q$ quantum MDS convolutional code, where $3 \leq s \leq (a+1)m - 3$.

(5) Let q be an odd prime power with the form $2am - 1$ where a is an odd integer. Then for integers c_1, c_2, c_3 such that $c_1, c_2, c_3 \geq 0$, $0 \leq c_1 + c_2 \leq a$, $0 \leq c_1 + c_3 \leq a$ and $c_1 + c_2 + c_3 \geq 1$, there exists a $[(\frac{(c_2+c_3)(q^2-1)}{2a} + c_1(\frac{q^2-1}{a} - q + 1), \frac{(c_2+c_3)(q^2-1)}{2a} + c_1(\frac{q^2-1}{a} - q + 1) - 2s + 4, 2; 2, s+1)]_q$ quantum MDS convolutional code, where $3 \leq s \leq (a+1)m - 2$.

(6) Let q be an odd prime power with the form $q = 2ab - 1$, where $\gcd(a, b) = 1$ and a, b are odd. Then for integer c such that $1 \leq c \leq 2(a+b-1)$, there exists a $[(c(q-1), c(q-1) - 2s + 4, 2; 2, s+1)]_q$ quantum MDS convolutional code, where $3 \leq s \leq ab + c_1 - 2$,

$$
c_1 = \begin{cases} c; & \text{if } 1 \leq c \leq a + b - 1, \\ \lfloor \frac{c}{2} \rfloor; & \text{if } a + b \leq c \leq 2(a+b-1). \end{cases}
$$

Table 2: Quantum MDS Convolutional Codes

q	a	b	c	$[(n, k, \mu; \gamma, d')]_q$	s
17	1	2	$\diagdown$	$[(288, 292 - 2s, 2; 2, s+1)]_{17}$	$3 \leq s \leq 16$
17	2	2	1	$[(198, 202 - 2s, 2; 2, s+1)]_{17}$	$3 \leq s \leq 11$
11	2	4	$\diagdown$	$[(120, 124 - 2s, 2; 2, s+1)]_{11}$	$3 \leq s \leq 7$
23	3	3	2	$[(394, 398 - 2s, 2; 2, s+1)]_{23}$	$3 \leq s \leq 13$
29	3	5	10	$[(300, 304 - 2s, 2; 2, s+1)]_{29}$	$3 \leq s \leq 20$
31	3	5	10	$[(320, 324 - 2s, 2; 2, s+1)]_{31}$	$3 \leq s \leq 20$

(7) Let q be an odd prime power with the form $q = 2ab+1$, where $\gcd(a,b) = 1$ and a, b are odd. Then for integer c such that $1 \leq c \leq 2(a+b-1)$, there exists a $[(c(q+1), c(q+1) - 2s + 4, 2; 2, s+1)]_q$ quantum MDS convolutional code, where $3 \leq s \leq ab + c_1$,

$$c_1 = \begin{cases} c; & \text{if } 1 \leq c \leq a + b - 1, \\ \lfloor \frac{c}{2} \rfloor; & \text{if } a + b \leq c \leq 2(a+b-1). \end{cases}$$

(8) Let t be a divisor of $q^2 - 1$. Then, for any $r \leq (q^2 - 1)/t$ and $s \leq (t-1)/(q+1)$, there exists an $[(n, n - 2s + 4, 2; 2, s+1)]_q$ quantum MDS convolutional code for both $n = rt$ and $rt + 1$.

(9) For any $2 \leq n \leq q^2$, we write $n = n_1 + \cdots + n_t$ with $1 \leq t \leq q$ and $2 \leq n_i \leq q$ for all i. Let $1 \leq s \leq \min\{n_1, \cdots, n_t\}/2$. Then there exists an $[(n, n - 2s + 4, 2; 2, s+1)]_q$ quantum MDS convolutional code.

Table 2 lists some quantum MDS convolutional codes obtained from Theorem 3.4.

4 Conclusion

In this paper, we show that we can get quantum MDS convolutional codes from any GRS codes that are Hermitian dual-containing. In particular, we present two new constructions of quantum MDS convolutional codes and propose eighteen new classes of quantum MDS convolutional codes, providing a wide range of parameters.

References

[1] S. A. Aly, M. Grassl, A. Klappenecker, M. Rotteler, and P. K. Sarvepalli. Quantum convolutional BCH codes. In *Int. Symp. Inform. Theory, ISIT*, pages 180–183, 2007.

[2] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. Quantum convolutional codes derived from generalized Reed-Solomon codes. In *Int. Symp. Inform. Theory, ISIT*, pages 821–825, 2007.

[3] H. F. Chau. Quantum convolutional error-correcting codes. *Phys. Rev. A* (3), 58(2):905–909, 1998.

[4] J. Chen, J. Li, Y. Huang, and J. Lin. Some families of asymmetric quantum codes and quantum convolutional codes from constacyclic codes. *Linear Algebra Appl.*, 475:186–199, 2015.

[5] A. C. A. De Almeida and R. Palazzo Jr. A concatenated [(4, 1, 3)] quantum convolutional code. In *IEEE Inform.Theory Workshop (ITW)*, pages 28–33, 2004.

[6] M. F. Ezerman, S. Jitman, H. M. Kiah, and S. Ling. Pure asymmetric quantum MDS codes from CSS construction: a complete characterization. *Int. J. Quantum Inf.*, 11(3):1350027, 10, 2013.

[7] G. D. Forney, M. Grassl, and S. Guha. Convolutional and tail-biting quantum error-correcting codes. *IEEE Trans. Inform. Theory*, 53(3):865–880, 2007.

[8] M. Grassl and M. Rotteler. Non-catastrophic encoders and encoder inverses for quantum convolutional codes. In *Int. Symp. Inform. Theory, ISIT*, pages 1109–1113, 2006.

[9] M. Grassl and M. Rotteler. Constructions of quantum convolutional codes. In *Int. Symp. Inform. Theory, ISIT*, pages 816–820, 2007.

[10] M. Grassl and M. Rotteler. Quantum block and convolutional codes from self-orthogonal product codes. *Int. Symp. Inform. Theory, ISIT*, pages 1018–1022, 2007.

[11] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[12] L. Jin, S. Ling, J. Luo, and C. Xing. Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes. *IEEE Trans. Inform. Theory*, 56(9):4735–4740, 2010.

[13] G. G. La Guardia. On classical and quantum MDS-convolutional BCH codes. *IEEE Trans. Inform. Theory*, 60(1):304–312, 2014.

[14] G. G. La Guardia. On negacyclic MDS-convolutional codes. *Linear Algebra Appl.*, 448:85–96, 2014.

[15] D. A. Lidar and T. A. Brun. *Quantum error correction*. Cambridge University Press, 2013.

[16] H. Ollivier and J. P. Tillich. Description of a quantum convolutional code. *Phys. Rev. Lett.*, 91(17):177902, 2003.

[17] H. Ollivier and J. P. Tillich. Quantum convolutional codes: fundamentals. *HAL-INRIA*, 54(9):4053–4068, 2004.

[18] J. Qian and L. Zhang. Constructions of new quantum burst-correcting codes. *Internat. J. Theoret. Phys.*, 54(3):917–926, 2015.

[19] P. Tan and J. Li. Efficient quantum stabilizer codes: LDPC and LDPC-convolutional constructions. *IEEE Trans. Inform. Theory*, 56(1):476–491, 2010.

[20] M. M. Wilde and T. A. Brun. Entanglement-assisted quantum convolutional coding. *Phys. Rev. A (3)*, 81(4):042333, 21, 2010.

[21] M. M. Wilde, H. Krovi, and T. A. Brun. Convolutional entanglement distillation. In *Int. Symp. Inform. Theory, ISIT*, pages 2657–2661, 2010.

[22] G. Zhang, B. Chen, and L. Li. A construction of MDS quantum convolutional codes. *Internat. J. Theoret. Phys.*, 54(9):3182–3194, 2015.

[23] T. Zhang and G. Ge. Quantum MDS codes with large minimum distance. submitted.