Quantum Information Processing (2019) 18:89
https://doi.org/10.1007/s11128-019-2207-8

Two new families of entanglement-assisted quantum MDS codes from generalized Reed–Solomon codes

Gaojun Luo[1] · **Xiwang Cao**[1,2]

Received: 18 July 2018 / Accepted: 1 February 2019 / Published online: 9 February 2019

Abstract
Entanglement-assisted quantum error-correcting codes (EAQECCs) make use of pre-existing entanglement between the sender and receiver to boost the rate of transmission. It is possible to construct an EAQECC by any classical linear code. In this paper, we propose two constructions of generalized Reed–Solomon codes and calculate the dimension of their hulls. With these generalized Reed–Solomon codes, we present two new infinite families of EAQECCs, which are optimal with respect to the Singleton bound for EAQECCs. Notably, the parameters of our EAQECCs are new and flexible.

Keywords Hull · Generalized Reed–Solomon code · Entanglement-assisted quantum error-correcting code (EAQECC)

1 Introduction

The theory of quantum error-correcting codes (QECCs) has been exhaustively investigated in the literature. As we all know, QECCs are a powerful tool for fighting against noise in quantum communication and quantum computation. Therefore, there are many recent contributions to this topic [1,5,8,11,14,15,22–24]. Recently, such theory has been extended to entanglement-assisted quantum error-correcting codes (EAQECCs). Customarily, an entanglement-assisted quantum error-correcting code

This work was supported by the National Natural Science Foundation of China (Grant Nos. 11771007 and 61572027) and the China Scholarship Council (201806830044).

✉ Gaojun Luo
gjluo1990@163.com

Xiwang Cao
xwcao@nuaa.edu.cn

1 Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 211100, China

2 State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

can be denoted as $[[n, k, d; c]]_q$, which encodes k information qubits into n channel qubits with the help of c pairs of maximally entangled states and corrects up to $\lfloor \frac{d-1}{2} \rfloor$ errors, where d is the minimum distance of the code. If $c = 0$, then it is called a q-ary standard $[[n, k, d]]_q$ quantum code. The net rate of an EAQECC is $\frac{k-c}{n}$ and the rate of an EAQECC is $\frac{k}{n}$.

The concept of an EAQECC was introduced by Brun et al. [3], which overcomes the barrier of the dual-containing condition in constructing standard quantum codes from classical codes. So, it is much easier to construct EAQECCs by classical codes. They proved that if the shared entanglement is available between the sender and receiver in advance, non-dual-containing classical quaternary codes can be used to construct EAQECCs. Afterward, many researchers presented some constructions of good EAQECCs [4,7,9,10,17–19,21,25].

For many purposes, the net rate is an important parameter of an EAQECC. In general, the net rate can be positive, negative, or zero. EAQECCs with negative net rates may actually have advantages in practice. One great advantage of shared entanglement as a resource is that it is independent of the message being sent, and can in principle be prepared well ahead of time. One natural application of EAQECCs would therefore be to a quantum network where usage varies at different times. EAQECCs with positive net rates can be employed in some other ways to improve the power and flexibility of quantum communications. Brun et al. [4] indicated that it is possible to construct catalytic codes if the net rate of an EAQECC is positive. Precisely speaking, any $[[n, k; c]]_q$ EAQECC with $k - c > 0$ can lead to an $[[n, k - c; c]]_q$ catalytic quantum error-correcting code. It is clear that the net rate of the EAQECC is the rate of the catalytic quantum error-correcting code. Generally, one would like to design a code with large rate to decrease the redundant date.

As Brun et al. pointed out in [4], there exists a practical advantage of EAQECCs over standard QECCs. In the protocol, the entanglement is a strictly weaker resource than quantum communication. Hence, the comparison of the net yield, $k - c$, between an $[[n, k, d; c]]_q$ EAQECC and an $[[n, k, d; 0]]_q$ QECC is not being entirely fair to former. Furthermore, one can obtain the pre-shared entanglement from a two-way entanglement distillation protocol that has higher rates than one-way schemes. At this point, a large value of c is favorable because it implies a higher qubit channel yield. Above all, the design of an EAQECC with a flexible value of c is significant.

Recently, Guenda et al. [12] constructed some EAQECCs with good parameters. Furthermore, they established a link between the number of maximally shared qubits required to construct an EAQECC from any classical linear code and the hull of the classical code. And they also provided methods for constructing EAQECCs requiring desirable amounts of entanglement.

The main goal of this paper is to construct MDS EAQECCs. Enlightened by the idea of [12], we propose two constructions of generalized Reed–Solomon codes and determine their hulls. Using these generalized Reed–Solomon codes, we obtain two new infinite families of MDS EAQECCs. Notably, the parameters of these MDS EAQECCs are new and flexible. For reference, we list the parameters of some known MDS EAQECCs and the new ones in Table 1.

Table 1 Some known classes of MDS EAQECCs with parameters $[[n, k, d, c]]_q$ for an odd prime power q

Parameters $[[n, k, d, c]]_q$	Constraints	References
$[[\frac{q^2-1}{5}, \frac{q^2-5q+4-20t}{5}, \frac{q+5+4t}{2}; 4]]_q$	$q = 20m + 3$ or $q = 20m + 7$ and $m \leq t \leq \frac{q-3}{4}$, where $m > 0$ is an integer	[9]
$[[q^2 + 1, q^2 + 5 - 2q - 4t, q + 2t + 1; 4]]_q$	$q \geq 5$ such that $q \equiv 1 \pmod 4$ and $2 \leq t \leq \frac{q-1}{2}$	[7]
$[[\frac{q^2+1}{2}, \frac{q^2+1}{2} - 2q - 4t + 5, q + 2t + 1; 5]]_q$	$q > 7$ and $2 \leq t \leq \frac{q-1}{2}$	[7]
$[[\lambda(q + 1), \lambda(q - 1) - 2t - q + 5, \frac{q+1}{2} + t + \lambda; 4]]_q$	$q \geq 7$, $\lambda \geq 3$ with $\lambda \mid (q - 1)$ and $\frac{q+3}{2} \leq t \leq \frac{q-1}{2} + \lambda$	[7]
$[[2\lambda(q + 1), 2\lambda(q - 1) - 2t - q + 5, \frac{q+1}{2} + t + 2\lambda; 4]]_q$	$q \geq 13$ such that $q \equiv 1 \pmod 4$, $\lambda \geq 3$ with $\lambda \mid (q - 1)$ and $\frac{q+3}{2} \leq t \leq \frac{q-1}{2} + 2\lambda$	[7]
$[[q^2 + 1, q^2 - 2d + 7, d; 4]]_q$	d is even such that $q + 3 \leq d \leq 3q - 1$	[18]
$[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - 2d + 3, d; 1]]_q$	$q = 10m + 3$ and d is even such that $2 \leq d \leq 6m + 2$, where $m > 0$ is an integer	[18]
$[[\frac{q^2+1}{10}, \frac{q^2+1}{10} - 2d + 3, d; 1]]_q$	$q = 10m + 7$ and d is even such that $2 \leq d \leq 6m + 4$, where $m > 0$ is an integer	[18]
$[[\frac{q^2-1}{h}, \frac{q^2-1}{h} - 2d + 3, d; 1]]_q$	$h \in \{3, 5, 7\}$ is a divisor of $q + 1$ and d is even such that $\frac{q+1}{h} \leq d \leq \frac{(q+1)(h+3)}{2h} - 1$	[18]
$[[q^2 + 1, q^2 - 2t, 2t + 2; 2t + 1]]_q$	$0 \leq t \leq \frac{(r-1)(q^2-1)}{2r}$, where $r \mid (q - 1)$ and $r \nmid (q + 1)$	[21]
$[[n, n - k - h, k + 1; k - h]]_q$	$q > 3$, $m > 1$ is an integer such that $m \mid q$, $1 < k \leq \lfloor \frac{n}{2} \rfloor$, $n + k > m + 1$, $1 < n < m$ and $1 \leq h \leq n - m + k - 1$	Theorem 3.3
$[[n, n - k - h, k + 1; k - h]]_q$	$q > 3$, $m > 1$ is an integer such that $m \mid q$, $1 < k < \lfloor \frac{n}{2} \rfloor$, $2n - k - 1 < m \leq 2n - 2$, $1 < n < m$ and $1 \leq h \leq 2n - m - 1$	Theorem 3.4

This paper is organized as follows. In Sect. 2, some basic background and results about generalized Reed–Solomon codes and EAQECCs are reviewed. In Sect. 3, we construct two infinite classes of MDS EAQECCs. Section 4 concludes the paper.

2 Preliminaries

In this section, we recall some basic definitions and results about generalized Reed–Solomon codes and entanglement-assisted quantum error-correcting codes.

2.1 Generalized Reed–Solomon codes

Let q be a power of a prime and $\mathbb{F}_q$ denote the finite field with q elements. We write $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. An $[n, k, d]$ linear code over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d. Let $\mathbb{F}_q^n$ stand for the vector space with dimension n over $\mathbb{F}_q$. An $[n, k, d]$ code $\mathcal{C}$ is called an MDS code if $n = k + d - 1$. For any two vectors, $\mathbf{x} = (x_1, x_2, \ldots, x_n)^t$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)^t$ of $\mathbb{F}_q^n$, their Euclidean inner product is defined as

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i.$$

The dual of the code $\mathcal{C}$ is defined by the set

$$\mathcal{C}^{\perp} = \{\mathbf{x} \in \mathbb{F}_q^n : \mathbf{x} \cdot \mathbf{y} = 0 \quad \text{for all } \mathbf{y} \in \mathcal{C}\}.$$

The hull of $\mathcal{C}$ is the code $\mathcal{C} \bigcap \mathcal{C}^{\perp}$, denoted by $\mathrm{Hull}(\mathcal{C})$, in the terminology that was introduced in [2].

Assume that $\alpha_1, \alpha_2, \ldots, \alpha_n$ are n distinct elements of $\mathbb{F}_q$, where $1 < n \leq q$. For n nonzero fixed elements $v_1, v_2, \ldots, v_n$ of $\mathbb{F}_q$ (v_i may not be distinct), the generalized Reed–Solomon code (GRS code for short) [20] associated with $\mathbf{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ is defined as follows:

$$\begin{aligned} GRS_k(\mathbf{a}, \mathbf{v}) = \{&(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)) : f(x) \in \mathbb{F}_q[x], \\ &\deg(f(x)) \leq k - 1\}. \end{aligned} \tag{1}$$

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

$$G = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ v_1\alpha_1^2 & v_2\alpha_2^2 & \cdots & v_n\alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \cdots & v_n\alpha_n^{k-1} \end{pmatrix}.$$

It is well known that the code $GRS_k(\mathbf{a}, \mathbf{v})$ is a q-ary $[n, k, n-k+1]$-MDS code [20, Th. 9.1.4] and the dual of a GRS code is again a GRS code. More specifically,

$$GRS_k(\mathbf{a}, \mathbf{v})^{\perp} = GRS_{n-k}(\mathbf{a}, \mathbf{v}')$$

for some $\mathbf{v}' = (v_1', v_2', \cdots, v_n')$ such that $v_i' \neq 0$ for any $1 \leq i \leq n$. Furthermore, Jin [13] indicated that

$$GRS_k(\mathbf{a}, \mathbf{1})^{\perp} = GRS_{n-k}(\mathbf{a}, \mathbf{u}),$$

where $\mathbf{1}$ stands for the all-one row vector of length n and $\mathbf{u} = \{u_1, u_2, \ldots, u_n\}$ with $u_i = \prod_{1 \leq j \leq n, j \neq i} (\alpha_i - \alpha_j)^{-1}$ for $1 \leq i \leq n$. By this fact, we have following lemma.

Lemma 2.1 *Let the symbols be the same as above. Then the dual code of $GRS_k(\mathbf{a}, \mathbf{v})$ is $GRS_{n-k}(\mathbf{a}, \mathbf{w})$, where $\mathbf{w} = \{\omega_1, \omega_2, \ldots, \omega_n\}$ with $\omega_i = v_i^{-1} u_i$ for $1 \leq i \leq n$.*

proof Thanks to $GRS_k(\mathbf{a}, \mathbf{1})^{\perp} = GRS_{n-k}(\mathbf{a}, \mathbf{u})$, we get that $\sum_{i=1}^{n} f(\alpha_i)(u_i g(\alpha_i)) = 0$ for any two polynomials $f(x), g(x) \in \mathbb{F}_q[x]$ such that $\deg(f(x)) \leq k-1$ and $\deg(g(x)) \leq n-k-1$. Note that $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ and $v_1, v_2, \cdots, v_n$ are nonzero elements of $\mathbb{F}_q$. Then we deduce that

$$\sum_{i=1}^{n} v_i f(\alpha_i)(v_i^{-1} u_i g(\alpha_i)) = 0,$$

for any two polynomials $f(x), g(x) \in \mathbb{F}_q[x]$ such that $\deg(f(x)) \leq k-1$ and $\deg(g(x)) \leq n-k-1$. Assume that $\mathbf{w} = \{\omega_1, \omega_2, \ldots, \omega_n\}$ with $\omega_i = v_i^{-1} u_i$ for $1 \leq i \leq n$. Hence, $GRS_{n-k}(\mathbf{a}, \mathbf{w})$ is orthogonal to $GRS_k(\mathbf{a}, \mathbf{v})$. The lemma follows immediately from the fact that

$$\dim(GRS_k(\mathbf{a}, \mathbf{v})) + \dim(GRS_{n-k}(\mathbf{a}, \mathbf{w})) = k + n - k = n.$$

□

The following result provides a method for determining the hull of a GRS code.

Lemma 2.2 *Let $GRS_k(a, v)$ be the generalized Reed–Solomon code associated with $\mathbf{a}$ and $\mathbf{v}$. For a codeword $\mathbf{c} = (v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n))$ of $GRS_k(\mathbf{a}, \mathbf{v})$, $\mathbf{c}$ is contained in $GRS_k(\mathbf{a}, \mathbf{v})^{\perp}$ if and only if there is a polynomial $g(x) \in \mathbb{F}_q[x]$ with $deg(g(x)) \leq n-k-1$ such that*

$$(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)) = (v_1^{-1} u_1 g(\alpha_1), v_2^{-1} u_2 g(\alpha_2), \ldots, v_n^{-1} u_n g(\alpha_n)),$$

where $u_i = \prod_{1 \leq j \leq n, j \neq i} (\alpha_i - \alpha_j)^{-1}$ for $1 \leq i \leq n$.

Lemma 2.2 is now a direct consequence of Lemma 2.1. In fact, Lemma 2.2 is another form of [6, Lemma III.1], and we have given a different proof of it.

2.2 Entanglement-assisted quantum error-correcting codes

By utilizing classical linear codes over finite fields, one can construct EAQECCs as follows.

Lemma 2.3 [25] *Suppose that H_1 and H_2 are parity check matrices of two q-ary linear codes $[n, k_1, d_1]$ and $[n, k_2, d_2]$, respectively. Then there exists an $[[n, k_1 + k_2 - n + c, \min\{d_1, d_2\}; c]]_q$ EAQECC, where $c = rank(H_1 H_2^t)$ is the required number of maximally entangled states.*

Between the parameters $n, k\, d$ and c of an EAQECC, there exists a trade-off, known as the Singleton bound [3,16].

Lemma 2.4 [3,16] *For any $[[n, k, d; c]]_q$ EAQECC with $d \leq \frac{n+2}{2}$, it satisfies*

$$n + c - k \geq 2(d - 1),$$

where $0 \leq c \leq n - 1$.

An EAQECC is called an MDS EAQECC if the parameters meet the Singleton bound. Guenda et al. [12] established a relation between the required number of maximally entangled states and the dimension of the hull of a classical code.

Lemma 2.5 [12] *Let $\mathcal{C}$ be a q-ary linear code with parameters $[n, k, d]$. Assume that H is a parity check matrix and G is a generator matrix of $\mathcal{C}$. Then we have*

$$rank(HH^t) = n - k - \dim(\mathrm{Hull}(\mathcal{C})) = n - k - \dim(\mathrm{Hull}(\mathcal{C}^{\perp})),$$

and

$$rank(GG^t) = k - \dim(\mathrm{Hull}(\mathcal{C})) = k - \dim(\mathrm{Hull}(\mathcal{C}^{\perp})).$$

As a direct consequence of Lemmas 2.3 and 2.5, one has the following lemma.

Lemma 2.6 [12] *Let $\mathcal{C}$ be an $[n, k, d]$ linear code over $\mathbb{F}_q$ and $\mathcal{C}^{\perp}$ its Euclidean dual with parameters $[n, n - k, d^{\perp}]$. Then there exist $[[n, k - \dim(\mathrm{Hull}(\mathcal{C})), d; n - k - \dim(\mathrm{Hull}(\mathcal{C}))]]_q$ and $[[n, n-k-\dim(\mathrm{Hull}(\mathcal{C})), d^{\perp}; k-\dim(\mathrm{Hull}(\mathcal{C}))]]_q$ EAQECCs.*

3 New MDS entanglement-assisted quantum error-correcting codes

In this section, using generalized Reed–Solomon codes, we present two infinite families of MDS EAQECCs. We begin with a construction of MDS linear codes over finite fields.

Theorem 3.1 *Let $q > 3$ be an odd prime power. Suppose that $m > 1$ is an integer with $m|q$ and n is a positive integer such that $1 < n < m$. If $1 < k \leq \lfloor \frac{n}{2} \rfloor$ and $n + k > m + 1$, then there exists a q-ary $[n, k]$ MDS linear code $\mathcal{C}$ with h-dimensional hull for any $1 \leq h \leq n - m + k - 1$.*

proof Due to $m|q$, $\mathbb{F}_m$ is the finite field with m elements and label the elements of

$$\mathbb{F}_m = \{\alpha_1, \ldots, \alpha_n, \alpha_{n+1}, \ldots, \alpha_m\}.$$

Assume that $u_i = \prod_{1\le j\le n, j\neq i}(\alpha_i - \alpha_j)^{-1}$ for $1 \le i \le n$. Let s be an integer such that $1 \le s \le n+k-m-1$. Put $\mathbf{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_s, \underbrace{1, \ldots, 1}_{n-s})$, where $v_i \in \mathbb{F}_q^*$ and $-v_i^2 \prod_{j=n+1}^{m}(\alpha_i - \alpha_j) \neq u_i$ for all $1 \le i \le s$. Then we obtain the q-ary GRS code $GRS_k(\mathbf{a}, \mathbf{v})$ of length n relative to $\mathbf{a}$ and $\mathbf{v}$ as follows:

$$GRS_k(\mathbf{a}, \mathbf{v}) = \{(v_1 f(\alpha_1), \ldots, v_s f(\alpha_s), f(\alpha_{s+1}), \ldots, f(\alpha_n)) : f(x) \in \mathbb{F}_q[x], \deg(f(x)) \le k-1\}.$$

Let $(v_1 f(\alpha_1), \ldots, v_s f(\alpha_s), f(\alpha_{s+1}), \ldots, f(\alpha_n)) \in GRS_k(\mathbf{a}, \mathbf{v}) \cap GRS_k(\mathbf{a}, \mathbf{v})^{\perp}$. It follows from Lemma 2.2 that there is a polynomial $g(x) \in \mathbb{F}_q[x]$ with $\deg(g(x)) \le n-k-1$ such that

$$(v_1 f(\alpha_1), \ldots, v_s f(\alpha_s), f(\alpha_{s+1}), \ldots, f(\alpha_n)) = (v_1^{-1} u_1 g(\alpha_1), \ldots, v_s^{-1} u_s g(\alpha_s), u_{s+1} g(\alpha_{s+1}), \ldots, u_n g(\alpha_n)). \tag{2}$$

Note that $\prod_{1\le j\le m, j\neq i}(\alpha_i - \alpha_j)^{-1} = \prod_{x\in\mathbb{F}_m^*} x = -1$. It follows from the last $n-s$ coordinates of (2) that

$$f(\alpha_i) = u_i g(\alpha^i) = \prod_{1\le j\le n, j\neq i}(\alpha_i - \alpha_j)^{-1} g(\alpha^i) = -\prod_{j=n+1}^{m}(\alpha_i - \alpha_j) g(\alpha^i),$$

for any $s < i \le n$. Hence, $f(x) = -\prod_{j=n+1}^{m}(x - \alpha_j) g(x)$ has at least $n-s$ distinct roots. It follows from the definition of $f(x)$, $g(x)$ and $k \le \lfloor \frac{n}{2} \rfloor$ that

$$\deg(f(x)) \le k-1 \le n-k-1 < m-k-1,$$

$$\deg\left(\prod_{j=n+1}^{m}(x - \alpha_j) g(x)\right) \le m-n+n-k-1 = m-k-1.$$

Note that $1 \le s \le n+k-m-1$. We deduce that

$$n - s \ge n - (n+k-m-1) = m-k+1.$$

Since the degree of the polynomial $f(x) + \prod_{j=n+1}^{m}(x-\alpha_j) g(x)$ is less than $m-k-1$ and it has at least $n-s$ distinct roots, we have $f(x) = -\prod_{j=n+1}^{m}(x-\alpha_j) g(x)$ for any $x \in \mathbb{F}_q$. Considering the first s coordinates of (2), we have

$$v_i^2 f(\alpha_i) = u_i g(\alpha_i) = -v_i^2 \prod_{j=n+1}^{m}(\alpha_i - \alpha_j) g(\alpha_i),$$

for any $1 \le i \le s$. Since $-v_i^2 \prod_{j=n+1}^{m}(\alpha_i - \alpha_j) \ne u_i$ for all $1 \le i \le s$, $g(x)$ has at least s distinct roots $\alpha_1, \alpha_2, \ldots, \alpha_s$. Thanks to $f(x) = -\prod_{j=n+1}^{m}(x - \alpha_j)g(x)$, we obtain $\deg(f(x)) = \deg(g(x)) + m - n \le k - 1$, i.e., $\deg(g(x)) \le n - m + k - 1$. Therefore,

$$g(x) = h(x)\prod_{i=1}^{s}(x - \alpha^i), \quad h(x) \in \mathbb{F}_q[x], \quad \deg(h(x)) \le n - m + k - 1 - s.$$

For any $g(x) \in \mathbb{F}_q[x]$ of the form $g(x) = h(x)\prod_{i=1}^{s}(x - \alpha_i)$, where $\deg(h(x)) \le n - m + k - 1 - s$, there exists a polynomial $f(x) = -\prod_{j=n+1}^{m}(x - \alpha_j)g(x) = -h(x)\prod_{j=n+1}^{m}(x - \alpha_j)\prod_{i=1}^{s}(x - \alpha_i)$ such that

$$\begin{aligned}(v_1 f(\alpha_1), \ldots, v_s f(\alpha_s), f(\alpha_{s+1}), \ldots, f(\alpha_n)) = (v_1^{-1}u_1 g(\alpha_1), \ldots,\\ v_s^{-1}u_s g(\alpha_s), u_{s+1}g(\alpha_{s+1}), \ldots, u_n g(\alpha_n)),\end{aligned}$$

which implies that

$$(v_1 f(\alpha_1), \ldots, v_s f(\alpha_s), f(\alpha_{s+1}), \ldots, f(\alpha_n)) \in GRS_k(\mathbf{a}, \mathbf{v}) \cap GRS_k(\mathbf{a}, \mathbf{v})^{\perp}.$$

Therefore, $\dim(\mathrm{Hull}(GRS_k(\mathbf{a}, \mathbf{v}))) = n - m + k - 1 - s + 1 = n - m + k - s$, where $1 \le s \le n - m + k - 1$. □

Below, we provide another construction of MDS linear codes and determine their hulls.

Theorem 3.2 *Let $q > 3$ be an odd prime power. Suppose that $m > 1$ is an integer with $m|q$ and n is a positive integer such that $1 < n < m$. If $1 < k < \lfloor \frac{n}{2} \rfloor$ and $2n - k - 1 < m \le 2n - 2$, then there exists a q-ary $[n, k]$ MDS linear code with h-dimensional hull for any $1 \le h \le 2n - m - 1$.*

proof According to $m|q$, we get that $\mathbb{F}_m$ is the finite field with m elements and label the elements of

$$\mathbb{F}_m = \{\alpha_1, \ldots, \alpha_n, \alpha_{n+1}, \ldots, \alpha_m\}.$$

Let s be an integer with $m - n - k + 1 \le s \le n - k - 1$. Take $\mathbf{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$, where $v_i = \prod_{j=1}^{s}(\alpha_i - \alpha_{n+j})$ for $1 \le i \le n$. Consider the GRS code $GRS_k(\mathbf{a}, \mathbf{v})$ of length n as follows:

$$GRS_k(\mathbf{a}, \mathbf{v}) = \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) : f(x) \in \mathbb{F}_q[x], \quad \deg(f(x)) \le k - 1\}.$$

For an arbitrary codeword $(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n))$ of $GRS_k(\mathbf{a}, \mathbf{v}) \cap GRS_k(\mathbf{a}, \mathbf{v})^{\perp}$, by Lemma 2.2, there exists a polynomial $g(x) \in \mathbb{F}_q[x]$ with $\deg(g(x)) \le n - k - 1$ such that

$$(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) = (v_1^{-1}u_1 g(\alpha_1), \ldots, v_n^{-1}u_n g(\alpha_n)),$$

where $u_i = \prod_{1\le j\le n, j\neq i}(\alpha_i - \alpha_j)^{-1}$ for $1 \le i \le n$, which implies that $v_i f(\alpha_i) = v_i^{-1} u_i g(\alpha_i)$ for $1 \le i \le n$. Since

$$v_i f(\alpha_i) = \prod_{j=1}^{s}(\alpha_i - \alpha_{n+j}) f(\alpha_i)$$

and

$$u_i g(\alpha_i) = \prod_{j=1}^{s}(\alpha_i - \alpha_{n+j})^{-1} \prod_{1\le j\le n, j\neq i}(\alpha_i - \alpha_j)^{-1} g(\alpha_i) = -\prod_{j=1}^{s}(\alpha_i - \alpha_{n+j})^{-1} \prod_{j=n+1}^{m}(\alpha_i - \alpha_j) g(\alpha_i),$$

we obtain

$$\prod_{j=1}^{s}(\alpha_i - \alpha_{n+j}) f(\alpha_i) = -\prod_{j=s+1}^{m-n}(\alpha_i - \alpha_{n+j}) g(\alpha_i),$$

for all $1 \le i \le n$. Note that

$$\deg\left(\prod_{j=1}^{s}(x - \alpha_{n+j}) f(x)\right) \le s + k - 1 \le n - 2$$

and

$$\begin{aligned}\deg\left(\prod_{j=s+1}^{m-n}(x - \alpha_{n+j}) g(x)\right) &\le m - n - s + n - k - 1\\ &= m - s - k - 1\\ &\le m - (m - n - k + 1) - k - 1\\ &= n - 2.\end{aligned}$$

Hence, we deduce that $\prod_{j=1}^{s}(x - \alpha_{n+j}) f(x) = -\prod_{j=s+1}^{m-n}(x - \alpha_{n+j}) g(x)$ for any $x \in \mathbb{F}_q$, which implies that

$$\prod_{j=s+1}^{m-n}(x - \alpha_{n+j}) \mid f(x).$$

Suppose that $f(x) = h(x)\prod_{j=s+1}^{m-n}(x - \alpha_{n+j})$, where $h(x) \in \mathbb{F}_q$ and $\deg(h(x)) \le n+s+k-m-1$. For any $f(x) \in \mathbb{F}_q[x]$ of the form $f(x) = h(x)\prod_{j=s+1}^{m-n}(x-\alpha_{n+j})$,

there exists a polynomial $g(x) = -h(x)\prod_{j=1}^{s}(x-\alpha_{n+j})$ such that

$$(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) = (v_1^{-1}u_1 g(\alpha_1), \ldots, v_n^{-1}u_n g(\alpha_n)),$$

which implies that

$$(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) \in GRS_k(\mathbf{a}, \mathbf{v}) \cap GRS_k(\mathbf{a}, \mathbf{v})^{\perp}.$$

Consequently, $\dim(\mathrm{Hull}(GRS_k(\mathbf{a}, \mathbf{v}))) = n + s + k - m - 1 + 1 = n + s + k - m$, where $m - n - k + 1 \le s \le n - k - 1$. □

Using Lemma 2.6, Theorems 3.1 and 3.2, we can easily obtain the following results.

Theorem 3.3 *Let $q > 3$ be an odd prime power. Assume that $m > 1$ is an integer such that $m|q$ and n is a positive integer with $1 < n < m$. If $1 < k \le \lfloor \frac{n}{2} \rfloor$ and $n + k > m + 1$, then there exist an $[[n, k-h, n-k+1; n-k-h]]_q$ EAQECC and an $[[n, n-k-h, k+1; k-h]]_q$ MDS EAQECC for any $1 \le h \le n - m + k - 1$.*

Example 1 Let $q = 13$, $m = 13$ and $n = 12$ in Theorem 3.3. Then we can obtain some new EAQECCs and MDS EAQECCs. Their parameters are listed in Table 2.

Theorem 3.4 *Let $q > 3$ be an odd prime power. Let $m > 1$ be an integer with $m|q$ and n a positive integer such that $1 < n < m$. If $1 < k < \lfloor \frac{n}{2} \rfloor$ and $2n - k - 1 < m \le 2n - 2$, then there exist an $[[n, k-h, n-k+1; n-k-h]]_q$ EAQECC and an $[[n, n-k-h, k+1; k-h]]_q$ MDS EAQECC for any $1 \le h \le 2n - m - 1$.*

Example 2 Let $q = 27$, $m = 27$ and $n = 15$ in Theorem 3.4. Then some new EAQECCs and MDS EAQECCs with the parameters are listed in Table 3.

Table 2 Sample parameters of EAQECCs of Theorem 3.3 for $q = 13$, $m = 13$ and $n = 12$

k	h	$[[n, k_1, d_1; c_1]]_q^{\mathrm{a}}$	k	h	$[[n, k_2, d_2; c_2]]_q^{\mathrm{b}}$
3	1	$[[12, 2, 10; 8]]_{13}$	3	1	$[[12, 8, 4; 2]]_{13}$
4	1	$[[12, 3, 9; 7]]_{13}$	4	1	$[[12, 7, 5; 3]]_{13}$
4	2	$[[12, 2, 9; 6]]_{13}$	4	2	$[[12, 6, 5; 2]]_{13}$
5	1	$[[12, 4, 8; 6]]_{13}$	5	1	$[[12, 6, 6; 4]]_{13}$
5	2	$[[12, 3, 8; 5]]_{13}$	5	2	$[[12, 5, 6; 3]]_{13}$
5	3	$[[12, 2, 8; 4]]_{13}$	5	3	$[[12, 4, 6; 2]]_{13}$
6	1	$[[12, 5, 7; 5]]_{13}$	6	1	$[[12, 5, 7; 5]]_{13}$
6	2	$[[12, 4, 7; 4]]_{13}$	6	2	$[[12, 4, 7; 4]]_{13}$
6	3	$[[12, 3, 7; 3]]_{13}$	6	3	$[[12, 3, 7; 3]]_{13}$
6	4	$[[12, 2, 7; 2]]_{13}$	6	4	$[[12, 2, 7; 2]]_{13}$

[a] $k_1 = k - h, d_1 = n - k + 1, c_1 = n - k - h$
[b] $k_2 = n - k - h, d_2 = k + 1, c_2 = k - h$

Table 3 Sample parameters of EAQECCs of Theorem 3.4 for $q = 27$, $m = 27$ and $n = 15$

k	h	$[[n, k_1, d_1; c_1]]_q^{\mathrm{a}}$	k	h	$[[n, k_2, d_2; c_2]]_q^{\mathrm{b}}$
3	1	$[[15, 2, 13; 11]]_{27}$	3	1	$[[15, 11, 4; 2]]_{27}$
3	2	$[[15, 1, 13; 10]]_{27}$	3	2	$[[15, 10, 4; 1]]_{27}$
4	1	$[[15, 3, 12; 10]]_{27}$	4	1	$[[15, 10, 5; 3]]_{27}$
4	2	$[[15, 2, 12; 9]]_{27}$	4	2	$[[15, 9, 5; 2]]_{27}$
5	1	$[[15, 4, 11; 9]]_{27}$	5	1	$[[15, 9, 6; 4]]_{27}$
5	2	$[[15, 3, 11; 8]]_{27}$	5	2	$[[15, 8, 6; 3]]_{27}$
6	1	$[[15, 5, 10; 8]]_{27}$	6	1	$[[15, 8, 7; 5]]_{27}$
6	2	$[[15, 4, 10; 7]]_{27}$	6	2	$[[15, 7, 7; 4]]_{27}$

[a] $k_1 = k - h, d_1 = n - k + 1, c_1 = n - k - h$
[b] $k_2 = n - k - h, d_2 = k + 1, c_2 = k - h$

Remark 1 From Tables 2 and 3, we see that the required number of maximally entangled states of the MDS EAQECC obtained by Theorems 3.3 or 3.4 is very flexible while the required number of maximally entangled states of many known MDS EAQECCs reported in the literature (see Table 1) is a fixed number. For instance, the MDS EAQECCs constructed in [9] have parameters $\left[\left[\frac{q^2-1}{5}, \frac{q^2-5q+4-20t}{5}, \frac{q+5+4t}{2}; 4\right]\right]_q$ and its required number of maximally entangled states is always equal to 4. In fact, it is easy to check that the net rate $\frac{k-c}{n}$ of the MDS EAQECC derived from Theorems 3.3 or 3.4 is ranged from 0 to $\frac{n-4}{n}$. It is easier to obtain a large net rate of MDS EAQECCs from our constructions than those listed in Table 1. Above all, employing the MDS EAQECCs obtained by Theorems 3.3 and 3.4, one can obtain many catalytic quantum error correction codes with large rates and flexible parameters by the technique introduced in [4].

4 Conclusion

In this paper, we presented two constructions of generalized Reed–Solomon codes and evaluated the dimensions of their hulls. Employing these generalized Reed–Solomon codes, we have constructed two families of MDS EAQECCs over the finite field $\mathbb{F}_q$, where $q > 3$ is an odd prime power. According to the entanglement-assisted quantum Singleton bound, the resulting EAQECCs are optimal. Notably, the parameters of our MDS EAQECCs are new and flexible. It would be interesting to construct optimal EAQECCs from other types of generalized Reed–Solomon codes.

Acknowledgments We are grateful to the anonymous referees and the associate editor for useful comments and suggestions that improved the presentation and quality of this paper.

References

1. Aly, S.A., Klappenecker, A., Sarvepalli, P.K.: On quantum and classical BCH codes. IEEE Trans. Inf. Theory **53**(3), 1183–1188 (2007)
2. Assmus, E.F., Key, J.: Designs and Their Codes. Cambridge Tracts in Mathematics, vol. 103. Cambridge University Press, Cambridge (1992). (Second printing with corrections, 1993)
3. Brun, T., Devetak, I., Hsieh, M.H.: Correcting quantum errors with entanglement. Science **314**, 436–439 (2006)
4. Brun, T., Devetak, I., Hsieh, M.H.: Catalytic quantum error correction. IEEE Trans. Inf. Theory **60**(6), 3073–3089 (2014)
5. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via codes over GF(4). IEEE Trans. Inf. Theory **44**(4), 1369–1387 (1998)
6. Chen, B., Liu, H.: New constructions of MDS codes with complementary duals. IEEE Trans. Inf. Theory **64**(8), 5776–5782 (2018)
7. Chen, J., Huang, Y., Feng, C., Chen, R.: Entanglement-assisted quantum MDS codes constructed from negacyclic codes. Quantum Inf. Process. **16**(12), 303 (2017)
8. Chen, X., Zhu, S., Kai, X.: Two classes of new optimal asymmetric quantum codes. Int. J. Theor. Phys. **57**(6), 1829–1838 (2018)
9. Chen, X., Zhu, S., Kai, X.: Entanglement-assisted quantum MDS codes constructed from constacyclic codes. Quantum Inf. Process. **17**, 273 (2018)
10. Grassl, M.: Entanglement-Assisted Quantum Communication Beating the Quantum Singleton Bound. AQIS, Taiwan (2016)
11. Grassl, M., Beth, T., Rötteler, M.: On optimal quantum codes. Int. J. Quantum Inf. **2**(1), 55–64 (2004)
12. Guenda, K., Jitman, S., Gulliver, T.A.: Constructions of good entanglement assisted quantum error correcting codes. Des. Codes Cryptogr. **86**, 121–136 (2018)
13. Jin, L.: Construction of MDS codes with complementary duals. IEEE Trans. Inf. Theory **63**(5), 2843–2847 (2017)
14. Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.K.: Nonbinary stabilizer codes over finite fields. IEEE Trans. Inf. Theory **52**(11), 4892–4914 (2006)
15. La Guardia, G.: New families of asymmetric quantum BCH codes. Quantum Inf. Comput. **11**, 239–252 (2011)
16. Lai, C.Y., Ashikhmin, A.: Linear programming bounds for entanglement-assisted quantum error-correcting codes by split weight enumerators. IEEE Trans. Inf. Theory **64**(1), 622–639 (2018)
17. Lai, C., Brun, T.: Entanglement increases the error-correcting ability of quantum error-correcting codes. Phys. Rev. A **88**, 012320 (2013)
18. Lu, L., Li, R., Ma, W., Li, R., Ma, Y., Liu, Y., Cao, H.: Entanglement-assisted quantum MDS codes from constacyclic codes with large minimum distance. arXiv:1803.04168
19. Lu, L., Li, R., Guo, L., Fu, Q.: Maximal entanglement-assisted quantum codes constructed from linear codes. Quantum Inf. Process. **14**(1), 165–182 (2015)
20. MacWilliams, F.J., Sloane, N.J.A.: The theory of Error-Correcting Codes. North-Holland, Amsterdam (1977)
21. Qian, J., Zhang, L.: On MDS linear complementary dual codes and entanglement-assisted quantum codes. Des. Codes Cryptogr. **86**(7), 1565–1572 (2018)
22. Shor, P.W.: Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A **52**(4), 2493–2496 (1995)
23. Steane, A.M.: Error correcting codes in quantum theory. Phys. Rev. Lett **77**, 793–797 (1996)
24. Wang, L., Feng, K.Q., Ling, S., Xing, C.P.: Asymmetric quantum codes: characterization and constructions. IEEE Trans. Inf. Theory **56**(6), 2938–2945 (2010)
25. Wilde, M., Brun, T.: Optimal entanglement formulas for entanglement-assisted quantum coding. Phys. Rev. A **77**, 064302 (2008)