Quantum Information Processing (2019) 18:366
https://doi.org/10.1007/s11128-019-2477-1

Three new classes of entanglement-assisted quantum MDS codes from generalized Reed–Solomon codes

Lanqiang Li[1] · Shixin Zhu[1] · Li Liu[1]

Received: 7 May 2019 / Accepted: 14 October 2019 / Published online: 28 October 2019

Abstract

Entanglement-assisted quantum error-correcting (EAQEC) codes can be obtained from arbitrary classical linear codes, based on the entanglement-assisted stabilizer formalism. However, how to determine the required number of shared pairs is challenging. In this paper, we first construct three classes of classical linear MDS codes over finite fields by considering generalized Reed–Solomon codes and calculate the dimension of their Hermitian hulls. By using these MDS codes, we then obtain three new classes of EAQEC codes and EAQEC MDS codes, whose maximally entangled states can take various values. Moreover, these EAQEC codes have more flexible lengths.

Keywords Entanglement-assisted quantum error-correcting (EAQEC)codes · MDS codes · Hermitian hull · Generalized Reed–Solomon (GRS)codes

1 Introduction

Quantum error-correcting codes play a key role in quantum information processing and quantum computation [1,2]. As we know, quantum error-correcting codes can be constructed from classical linear error-correcting codes with certain dual-containing

This research is supported in part by the Fundamental Research Funds for the Central Universities of China Under Grant No. PA2019GDZC0097 and the National Natural Science Foundation of China Under Grant Nos. 61772168, 61572168, 11871187.

✉ Shixin Zhu
zhushixinmath@hfut.edu.cn

Lanqiang Li
lilanqiang716@126.com

Li Liu
liuli-1128@163.com

[1] School of Mathematics, Hefei University of Technology, Hefei 230009, Anhui, People's Republic of China

properties [3]. In other words, a classical linear code without the dual-containing condition cannot be used to construct quantum error-correcting codes. For more details on the construction of quantum MDS codes, please refer to [4–8]. The development of EAQEC codes theory is a breakthrough in the area of quantum error correction. Hsieh et al. [9] proposed a more general framework called entanglement-assisted stabilizer formalism. The framework allows arbitrary classical linear error-correcting codes without the dual-containing constraint to transform into EAQEC codes if shared entanglement is available between the sender and receiver. For more details on EAQECCs, we refer the reader to [10–16]. Recently, using arbitrary classical linear codes without the dual-containing condition to construct EAQEC codes has become an important area of study [17–32]; more and more scholars have been encouraged to construct EAQEC codes with good parameters (much larger minimum distances or code rates).

However, it is challenging to determine the number of pre-shared maximally entangled states for constructing an EAQEC code. By using algebraical methods, many EAQEC codes with good parameters have been constructed in [17–19]. Fan et al. provided a construction of EAQEC MDS codes with a small number of pre-shared maximally entangled states in [20]. Li et al. proposed the concept of decomposition of the defining set of cyclic codes in [21,22]. According to the concept, they transformed the problem of calculating the number of share pairs to determine a special subset of the defining set of a cyclic code and then constructed some EAQEC codes with good parameters. Their method was generalized to apply in negacyclic codes and constacyclic codes and yielded many EAQEC codes with good parameters [23–28]. Li et al. [29] constructed some EAQEC MDS codes by using generalized Reed–Solomon codes. Guenda et al. [18] proved that the required number of shared pairs was related to the dimension of the hull of a classical linear code. Via following the fact, Luo et al. [30] and Luo and Cao [31] constructed several new infinite classes of EAQEC MDS codes by determining the Euclidean hull of (extended) GRS codes. Fang et al. [32] obtained several classes of EAQEC MDS codes by determining the Hermitian hull of (extended) GRS codes. These works showed that (extended) GRS codes are a good source for producing EAQEC MDS codes.

In this paper, we first construct some MDS codes from GRS codes and calculate the dimension of their Hermitian hulls and then obtain three new classes of q-ary EAQEC codes and EAQEC MDS codes with these constructed MDS codes as follows:

(1) Let q be a prime power. If $q+1 < n \leq 2(q-1)$ and $n-q < k \leq \lfloor \frac{n}{2} \rfloor$, then there exist $[[n, k-l, n-k+1; n-k-l]]_q$ EAQEC codes and $[[n, n-k-l, k+1; k-l]]_q$ EAQEC MDS codes, where $1 \leq l \leq k+q-n$.

(2) Let $q = p^m \geq 3$ be a prime power and e be a positive integer with $e|m$. Assume that $N = tp^{ez}$ with $1 \leq t \leq p^e$ and $1 \leq z \leq \frac{2m}{e} - 1$ and n is an integer such that $1 < n < N$. If $1 < k \leq \lfloor \frac{N+q-1}{q+1} \rfloor$ and $n+k > N+1$, then there exist $[[n, k-l, n-k+1; n-k-l]]_q$ EAQEC codes and $[[n, n-k-l, k+1; k-l]]_q$ EAQEC MDS codes, where $1 \leq l \leq n-N+k-1$.

(3) Let $q = p^m \geq 3$ be a prime power and $n^{'} = ml$ be some divisor of q^2-1 with $l|q+1$ and $\gcd(n^{'}, q-1) = m$. Assume that $N = tn^{'}$ with $1 \leq t \leq \frac{q-1}{m}$ and n is an integer such that $1 < n < N$. If $1 < k \leq \lfloor \frac{N+q}{q+1} \rfloor$ and $n+k > N+1$, then there

exist $[[n, k-l, n-k+1; n-k-l]]_q$ EAQEC codes and $[[n, n-k-l, k+1; k-l]]_q$ EAQEC MDS codes, where $1 \leq l \leq n - N + k - 1$.

Note that the above EAQEC codes are new in the sense that their parameters are different from all previously known ones. Moreover, the three classes of EAQEC codes and EAQEC MDS codes have more flexible parameters not only on shared pairs but also on lengths.

The manuscript is organized as follows: In Sect. 2, we review some basic notations and results on Hermitian hull, GRS codes and EAQEC codes. Section 3 constructs three new classes of EAQEC codes and EAQEC MDS codes with more flexible shared pairs and lengths by using GRS codes. Section 4 summarizes this paper.

2 Preliminaries

In this section, some basic notations and results on Hermitian hull, generalized Reed–Solomon codes and entanglement-assisted quantum error-correcting codes are reviewed, which will be frequently used later.

Let q be a prime power and F_{q^2} be the finite field with q^2 elements. For any $\alpha \in F_{q^2}$, we denote as $\overline{\alpha}$ the conjugation of α. Let $A = (a_{ij})_{k\times n}$ be some $k \times n$ matrix, where $a_{ij} \in F_{q^2}$. We denote the conjugation of the matrix $A = (a_{ij})_{k\times n}$ by $\overline{A} = (\overline{a}_{ij})_{k\times n}$ and the conjugate transpose of A over F_{q^2} by $A^{\dagger} = \overline{A}^{\top}$.

2.1 Hermitian hull

Any k-dimensional vector subspace of $F_{q^2}^n$ with minimum Hamming distance d is said to be an $[n, k, d]_{q^2}$ linear code C. Moreover, C is called a maximum distance separable (MDS) code, if its parameters attain the Singleton bound, i.e., $k = n-d+1$. The Euclidean dual code of C is defined as

$$C^{\perp E} = \{\mathbf{x} \in F_{q^2}^n : \langle \mathbf{x}, \mathbf{y}\rangle_E = 0, \forall\, \mathbf{y} \in C\},$$

where $\langle \mathbf{x}, \mathbf{y}\rangle_E = \sum_{i=1}^{n} x_i y_i$ is the Euclidean inner product of $\mathbf{x}$ and $\mathbf{y}$. The Euclidean hull of C is defined as $C \cap C^{\perp E}$, which was first proposed in [33]. Obviously, the Euclidean hull of a linear code C is also a linear code.

Similarly, the Hermitian dual code of C is defined as

$$C^{\perp H} = \{\mathbf{x} \in F_{q^2}^n : \langle \mathbf{x}, \mathbf{y}\rangle_H = 0, \forall\, \mathbf{y} \in C\},$$

where$\langle \mathbf{x}, \mathbf{y}\rangle_H = \sum_{i=1}^{n} x_i y_i^q$ is the Hermitian product of $\mathbf{x}$ and $\mathbf{y}$. The Hermitian hull of a linear code C over F_{q^2} is $C \cap C^{\perp H}$, denoted by $\mathrm{Hull}_h(C)$. It is obvious that $Hull_h(C)$ is also a linear code over F_{q^2}.

2.2 Generalized Reed–Solomon codes

Let $F_{q^2}[x]_k = \{f(x) \in F_{q^2}[x] | \deg(f(x)) \leq k-1\}$, $\mathbf{a} = (\alpha_1, \alpha_2, \dots, \alpha_n) \in F_{q^2}^n$ and $\mathbf{v} = (\upsilon_1, \upsilon_2, \dots, \upsilon_n) \in (F_{q^2}^*)^n$, where $\alpha_1, \alpha_2, \dots, \alpha_n \in F_{q^2}$ are distinct, $\upsilon_1, \upsilon_2, \dots, \upsilon_n \in F_{q^2}^*$ may not be distinct and $k \leq n \leq q^2$. Then, the GRS code over F_{q^2} associated with $\mathbf{a}$ and $\mathbf{v}$ can be defined as:

$$GRS_k(\mathbf{a}, \mathbf{v}) = \{(\upsilon_1 f(\alpha_1), \upsilon_2 f(\alpha_2), \dots, \upsilon_n f(\alpha_n)) : f(x) \in F_{q^2}[x]_k\}.$$

The GRS code $GRS_k(\mathbf{a}, \mathbf{v})$ above is an $[n, k, n-k+1]$ linear MDS code over F_{q^2}. The generator matrix G of $GRS_k(\mathbf{a}, \mathbf{v})$ is given as follows:

$$G = \begin{pmatrix} \upsilon_1\alpha_1^0 & \upsilon_2\alpha_2^0 & \cdots & \upsilon_n\alpha_n^0 \\ \upsilon_1\alpha_1^1 & \upsilon_2\alpha_2^1 & \cdots & \upsilon_n\alpha_n^1 \\ \vdots & \vdots & \ddots & \vdots \\ \upsilon_1\alpha_1^{k-1} & \upsilon_2\alpha_2^{k-1} & \cdots & \upsilon_n\alpha_n^{k-1} \end{pmatrix}.$$

It is well known that the Euclidean dual of $GRS_k(\mathbf{a}, \mathbf{v})$ is also a GRS code and can be denoted as $GRS_{n-k}(\mathbf{a}, \mathbf{v}^{'})$ for some $\mathbf{v}^{'} = (\upsilon_1^{'}, \upsilon_2^{'}, \dots, \upsilon_n^{'}) \in (F_{q^2}^*)^n$ (see [34]). Denote the all-one vector of length n by $\mathbf{1}$=(1, 1, ..., 1), then we have that $GRS_k(\mathbf{a}, \mathbf{1})^{\perp E} = GRS_{n-k}(\mathbf{a}, \mathbf{u})$, where $\mathbf{u} = (u_1, u_2, \dots, u_n)$ with $u_i = \prod_{1 \leq j \leq n, j \neq i}(\alpha_i - \alpha_j)^{-1}$ for all $1 \leq i \leq n$ (see [35]). Recently, Luo and Cao [31] proposed that $GRS_k(\mathbf{a}, \mathbf{v})^{\perp} = GRS_{n-k}(\mathbf{a}, \mathbf{w})$, where $\mathbf{w} = (\omega_1, \omega_2, \dots, \omega_n)$ with $\omega_i = \upsilon_i^{-1}u_i$ for any $1 \leq i \leq n$. Notice that $C^{\perp H} = \overline{C}^{\perp E}$ for any linear code C. For the Hermitian dual of $GRS_k(\mathbf{a}, \mathbf{v})$, we have the following lemma.

Lemma 2.1 *Let the notations be defined as above. Then, the Hermitian dual of $GRS_k(\mathbf{a}, \mathbf{v})$ is $GRS_{n-k}(\overline{\mathbf{a}}, \overline{\mathbf{w}})$, where $\overline{\mathbf{w}} = (\overline{\omega_1}, \overline{\omega_2}, \dots, \overline{\omega_n})$ with $\omega_i = \upsilon_i^{-1} \prod_{1 \leq j \leq n, j \neq i}(\alpha_i - \alpha_j)^{-1}$ for all $1 \leq i \leq n$. In particular, we have $GRS_k(\mathbf{a}, \mathbf{1})^{\perp H} = GRS_{n-k}(\overline{\mathbf{a}}, \overline{\mathbf{u}})$, where $\mathbf{u} = (u_1, u_2, \dots, u_n)$ with $u_i = \prod_{1 \leq j \leq n, j \neq i}(\alpha_i - \alpha_j)^{-1}$ for all $1 \leq i \leq n$.*

Proof Let σ be the mapping $\sigma(\alpha) = \overline{\alpha}$ for any $\alpha \in F_{q^2}$. From [36], σ is an automorphism of F_{q^2}. Then, we have

$$\begin{aligned} \overline{GRS_k(\mathbf{a}, \mathbf{v})} &= \{(\overline{\upsilon_1}\overline{f}(\overline{\alpha_2}), \overline{\upsilon_1}\overline{f}(\overline{\alpha_2}), \dots, \overline{\upsilon_n}\overline{f}(\overline{\alpha_n})) : f(x) \in F_{q^2}[x]_k\} \\ &= \{(\overline{\upsilon_1} f(\overline{\alpha_2}), \overline{\upsilon_1} f(\overline{\alpha_2}), \dots, \overline{\upsilon_n} f(\overline{\alpha_n})) : f(x) \in F_{q^2}[x]_k\} \\ &= GRS_k(\overline{\mathbf{a}}, \overline{\mathbf{v}}). \end{aligned}$$

Therefore, the Hermitian dual of $GRS_k(\mathbf{a}, \mathbf{v})$ is

$$GRS_k(\mathbf{a}, \mathbf{v})^{\perp H} = GRS_k(\overline{\mathbf{a}}, \overline{\mathbf{v}})^{\perp E} = GRS_{n-k}(\overline{\mathbf{a}}, \overline{\mathbf{w}}),$$

where $\overline{\mathbf{w}} = (\overline{\omega_1}, \overline{\omega_2}, \ldots, \overline{\omega_n})$ with $\omega_i = \upsilon_i^{-1} \prod_{1 \leq j \leq n, j \neq i} (\alpha_i - \alpha_j)^{-1}$ for all $1 \leq i \leq n$. □

The following lemma provides a sufficient and necessary condition of $\mathbf{c} \in GRS_k(\mathbf{a}, \mathbf{v}) \cap GRS(\mathbf{a}, \mathbf{v})^{\perp H}$ and will be used frequently for determining the Hermitian hull of a GRS code.

Lemma 2.2 *Suppose that* $GRS_k(\mathbf{a}, \mathbf{v})$ *is the GRS code associated with* $\mathbf{a}$ *and* $\mathbf{v}$ *defined as above. For any codeword* $\mathbf{c} = (\upsilon_1 f(\alpha_1), \upsilon_2 f(\alpha_2), \ldots, \upsilon_n f(\alpha_n)) \in GRS_k(\mathbf{a}, \mathbf{v})$, $\mathbf{c} \in GRS(\mathbf{a}, \mathbf{v})^{\perp H}$ *if and only if there exists a polynomial* $g(x)$ *with deg*$(g(x)) \leq n - k - 1$ *such that*

$$\begin{aligned}
&(\upsilon_1^{q+1} f(\alpha_1), \upsilon_2^{q+1} f(\alpha_2), \ldots, \upsilon_n^{q+1} f(\alpha_n)) \\
&\quad = (\overline{u_1} g(\overline{\alpha_1}), \overline{u_2} g(\overline{\alpha_2}), \ldots, \overline{u_n} g(\overline{\alpha_n})) \\
&\quad = (\overline{u_1} g'^{q}(\alpha_1), \overline{u_2} g'^{q}(\alpha_2), \ldots, \overline{u_n} g'^{q}(\alpha_n)),
\end{aligned}$$

where $g'^{q}(\alpha_i) = g(\overline{\alpha_i})$ *and* $\overline{u_i} = \prod_{1 \leq j \leq n, j \neq i} (\overline{\alpha_i} - \overline{\alpha_j})^{-1}$ *for all* $1 \leq i \leq n$.

Proof From Lemma 2.1, we have

$$(\upsilon_1^{q+1} f(\alpha_1), \upsilon_2^{q+1} f(\alpha_2), \ldots, \upsilon_n^{q+1} f(\alpha_n)) = (\overline{u_1} g(\overline{\alpha_1}), \overline{u_2} g(\overline{\alpha_2}), \ldots, \overline{u_n} g(\overline{\alpha_n})),$$

where $\deg(g(x)) \leq n - k - 1$ and $u_i = \prod_{1 \leq j \leq n, j \neq i} (\alpha_i - \alpha_j)^{-1}$ for all $1 \leq i \leq n$. According to the definition of σ, there exists a polynomial $g'(x) = \sigma^{-1}(g(\overline{x}))$ such that

$$(\overline{u_1} g(\overline{\alpha_1}), \overline{u_2} g(\overline{\alpha_2}), \ldots, \overline{u_n} g(\overline{\alpha_n})) = (\overline{u_1} g'^{q}(\alpha_1), \overline{u_2} g'^{q}(\alpha_2), \ldots, \overline{u_n} g'^{q}(\alpha_n)).$$

This completes the proof. □

Note that $\deg(g'(x)) = \deg(g(x)) \leq n - k - 1$ and the existence of $g(x)$ depends on the existence of $g'(x)$.

2.3 Entanglement-assisted quantum error-correcting codes

In the following, we recall some basic notations and results of entanglement-assisted quantum error-correcting codes. EAQEC codes are a generalization of standard stabilizer quantum codes that can be constructed via arbitrary classical linear codes (not necessarily dual-containing). A $q-ary$ EAQEC code 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. For an $[[n, k, d; c]]_q$ EAQEC code, the performance is determined by its rate k/n and net rate $(k - c)/n$. Brun et al. [14] proved that one can obtain catalytic codes if the net rate is positive. The parameters n, k, d and c of an EAQEC code have many constraints; one of the most important bounds on EAQEC codes is the EA-quantum Singleton bound as follows.

Lemma 2.3 [9,16] *For any EAQEC code $[[n, k, d; c]]_q$, if $d \leq \frac{n+2}{2}$, its parameters must satisfy*

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

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

An EAQEC code $[[n, k, d; c]]_q$ is called an EAQEC MDS code if its parameters achieve the EA-quantum Singleton bound. In recent years, more and more EAQEC codes have been constructed by using classical linear code over finite fields. One of the most frequently used constructions is given as below.

Theorem 2.4 [11,14] *Let H be the parity check matrix of an $[n, k, d]$ classical linear code over $\mathbb{F}_{q^2}$. Then, there exists an EAQEC code with parameters $[[n, 2k - n + c, d; c]]_q$, where $c = rank(HH^\dagger)$ is the required number of maximally entangled states and $H^\dagger$ is the conjugate transpose of H over F_{q^2}.*

Let C be an $[n, k]$ classical linear code with parity check matrix H. Guenda et al. [18] proved that $rank(HH^\dagger) = n - k - \dim(Hull_H(\mathcal{C})) = n - k - \dim(Hull_H(\mathcal{C}^{\perp_H}))$, which establishes the relation between the value of $rank(HH^\dagger)$ and the dimension of the Hermitian hull of C. Based on the fact, Guenda et al. provided the following construction, by considering linear code C and its dual code.

Lemma 2.5 [18] *Let C be an $[n, k, d]_{q^2}$ classical linear code and $C^\perp$ be its Euclidean dual code with parameters $[n, n - k, d^\perp]_{q^2}$. Then there exist $[[n, k - dim(Hull_h(C)), d; n-k-dim(Hull_h(C))]]_q$ and $[[n, n-k-dim(Hull_h(C)), d^\perp; k-dim(Hull_h(C))]]_q$ EAQEC codes. Furthermore, if C is MDS, then one of the two EAQEC codes must be MDS.*

3 Constructions of EAQEC MDS codes from GRS codes

In this section, by considering generalized Reed–Solomon codes over F_{q^2}, we first construct three classes of q^2-ary MDS codes and calculate the dimension of their Hermitian hulls. Let ω be a primitive element of F_{q^2}. It is easy to know that $F_q^* = \langle \omega^{q+1} \rangle$ is a cyclic subgroup of the multiplicative group $F_{q^2}^*$. This shows that $\alpha^{q+1} \in F_q$ for any $\alpha \in F_{q^2}$, and there must exist some element $\alpha \in F_{q^2}$ such that $\beta = \alpha^{q+1}$ for any $\beta \in F_q$.

Theorem 3.1 *Let q be a prime power. If $q + 1 \leq n \leq 2(q - 1)$ and $n - q < k \leq \lfloor \frac{n}{2} \rfloor$, then there exists a q^2-ary $[n, k]$ MDS code with l-dimensional Hermitian hull, where $1 \leq l \leq k + q - n$.*

Proof If s is even and $n - s \leq q$, we let $\alpha_1, \alpha_1^q, \ldots, \alpha_{\frac{s}{2}}, \alpha_{\frac{s}{2}}^q \in F_{q^2} \setminus F_q$ and $\beta_{s+1}, \ldots, \beta_n \in F_q$. Note that $(\alpha + \alpha^q) \in F_q$ for any $\alpha \in F_{q^2}$. For any $\beta \in F_q$ and $\alpha \in F_{q^2} \setminus F_q$, we have $(\beta - \alpha)(\beta - \alpha^q) = \beta^2 - (\alpha + \alpha^q)\beta + \alpha^{q+1} \in F_q^* = \langle \omega^{q+1} \rangle$. Let

$u_i = \prod_{s+1\le j\le n, j\ne i}(\beta_i-\beta_j)^{-1}\cdot\prod_{1\le j\le \frac{s}{2}}(\beta_i-\alpha_j)^{-1}(\beta_i-\alpha_j^q)^{-1}$ for $s+1\le i\le n$. It is clear that $u_i\in F_q^*$, i.e., $\overline{u_i}\in F_q^*=\langle\omega^{q+1}\rangle$. Then there exists a element $\upsilon_i\in F_{q^2}$ such that $\upsilon_i^{q+1}=\overline{u_i}$ for any $s+1\le i\le n$. When $1\le i\le s$, we let $u_i=(\alpha_{\frac{i+1}{2}}-\alpha^q_{\frac{i+1}{2}})^{-1}\prod_{1\le j\le\frac{s}{2}, j\ne\frac{i+1}{2}}(\alpha_{\frac{i+1}{2}}-\alpha_j)^{-1}(\alpha_{\frac{i+1}{2}}-\alpha_j^q)^{-1}\prod_{s+1\le j\le n}(\alpha_{\frac{i+1}{2}}-\beta_j)^{-1}$ for odd i and $u_i=(\alpha^q_{\frac{i}{2}}-\alpha_i)^{-1}\prod_{1\le j\le\frac{s}{2}, j\ne i}(\alpha^q_{\frac{i}{2}}-\alpha_j)^{-1}(\alpha^q_{\frac{i}{2}}-\alpha^q_j)^{-1}\prod_{s+1\le j\le n}(\alpha^q_{\frac{i}{2}}-\beta_j)^{-1}$ for even i. Take $\mathbf{a}=(\alpha_1,\alpha_1^q,\ldots,\alpha_{\frac{s}{2}},\alpha^q_{\frac{s}{2}},\beta_{s+1},\ldots,\beta_n)$ and $\mathbf{v}=(b_1,b_2,\ldots,b_s,\upsilon_{s+1},\ldots,\upsilon_n)$, where b_i for odd i satisfies $b_i^{q+1}\ne\overline{u_iu_{i+1}}$ and $b_i=1$ for even i. Then, we have

$$\begin{aligned}GRS_k(\mathbf{a},\mathbf{v})=\{&(b_1f(\alpha_1), f(\alpha_1^q),\ldots,b_{s-1}f(\alpha_{\frac{s}{2}}), f(\alpha^q_{\frac{s}{2}}),\\ &\upsilon_{s+1}f(\beta_{s+1}),\ldots,\upsilon_nf(\beta_n)) : f(x)\in F_{q^2}[x]_k\}.\end{aligned}$$

For any $\mathbf{c}=(b_1f(\alpha_1), f(\alpha_1^q)\ldots,b_{s-1}f(\alpha_{\frac{s}{2}}), f(\alpha^q_{\frac{s}{2}}),\upsilon_{s+1}f(\beta_{s+1}),\ldots,\upsilon_nf(\beta_n))\in GRS_k(\mathbf{a},\mathbf{v})\cap GRS(\mathbf{a},\mathbf{v})^{\perp H}$, it follows from Lemma 2.2 that there exists $g(x)\in F_{q^2}[x]_{n-k}$ such that

$$\begin{aligned}&(b_1^{q+1}f(\alpha_1), f(\alpha_1^q)\ldots,b_{s-1}^{q+1}f(\alpha_{\frac{s}{2}}), f(\alpha^q_{\frac{s}{2}}),\upsilon_{s+1}^{q+1}f(\beta_{s+1}),\ldots,\upsilon_n^{q+1}f(\beta_n))\\ &\quad=(\overline{u_1}g(\alpha_1^q),\overline{u_2}g(\alpha_1),\ldots,\overline{u_{s-1}}g(\alpha^q_{\frac{s}{2}}),\overline{u_s}g(\alpha_{\frac{s}{2}}),\overline{u_{s+1}}g(\overline{\beta_{s+1}}),\ldots,\overline{u_n}g(\overline{\beta_n}))\qquad(1)\\ &\quad=(\overline{u_1}g(\alpha_1^q),\overline{u_2}g(\alpha_1),\ldots,\overline{u_{s-1}}g(\alpha^q_{\frac{s}{2}}),\overline{u_s}g(\alpha_{\frac{s}{2}}),\upsilon_{s+1}^{q+1}g(\beta_{s+1}),\ldots,\upsilon_n^{q+1}g(\beta_n)).\end{aligned}$$

Hence, we have $f(\beta_i)=g(\beta_i)$ for any $s+1\le i\le n$ and

$$\begin{cases}b_{2i-1}^{q+1}f(\alpha_i)=\overline{u_{2i-1}}g(\alpha_i^q),\\ f(\alpha_i^q)=\overline{u_{2i}}g(\alpha_i),\end{cases}\qquad(2)$$

for any $1\le i\le\frac{s}{2}$. Note that $\deg(f(x))\le k-1\le n-k-1$ and $\deg(g(x))\le n-k-1$. Since $n-k-1<n-s$, we have $f(x)=g(x)$ for any $x\in F_{q^2}$. Then (2) becomes

$$\begin{cases}b_{2i-1}^{q+1}g(\alpha_i)=\overline{u_{2i-1}}g(\alpha_i^q),\\ g(\alpha_i^q)=\overline{u_{2i}}g(\alpha_i),\end{cases}\qquad(3)$$

Combine (3) and the definition of b_i, we have $g(\alpha_i)=g(\alpha_i^q)=0$ for any $1\le i\le\frac{s}{2}$. Thus, we can obtain $f(x)=g(x)=h(x)\prod_{i=1}^{\frac{s}{2}}(x-\alpha_i)(x-\alpha_i^q)$, where $\deg(h(x))\le k-1-s$. In addition, if s is odd and $n-s<q$, we take $\mathbf{a}=(\alpha_1,\alpha_1^q,\ldots,\alpha_{\frac{s-1}{2}},\alpha^q_{\frac{s-1}{2}},\alpha_s,\beta_{s+1},\ldots,\beta_n)$ and $\mathbf{v}=(b_1,b_2,\ldots,b_{s-1},b_s\nu_s,\nu_{s+1},\ldots,\nu_n)$, where b_i for odd i satisfies $b_i^{q+1}\ne\overline{u_iu_{i+1}}$

and $b_i = 1$ for even i. Similarly, we can obtain $f(x) = g(x) = xh(x)\prod_{i=1}^{\frac{s-1}{2}}(x - \alpha_i)(x - \alpha_i^q)$, where $\deg(h(x)) \leq k - 1 - s$. These demonstrate the results. □

Let $q = p^m$ and e be a positive integer such that $e|m$. Notice that F_{q^2} can be regarded as a $\frac{2m}{e}$-dimensional vector space over F_{p^e}. For any integer z with $1 \leq z < \frac{2m}{e} - 1$, let A be an z-dimensional vector subspace over F_{p^e} of F_{q^2}. We denote the elements of F_{p^e} by $\alpha_1 = 0, \alpha_2, \ldots, \alpha_{p^e}$. For $1 \leq t \leq p^e$ and $1 \leq j \leq t$, we denote $A_j = \{x + \alpha_j \eta : x \in A\}$, where $\eta \in F_{q^2} \setminus F_{p^e}$ is some fixed element. Let $N = tp^{ez}$ be an integer with $1 \leq t \leq p^e$ and $1 \leq z < \frac{2m}{e} - 1$. Assume that $\cup_{i=1}^{t} A_i = \{\alpha_1, \alpha_2, \ldots, \alpha_N\}$ and $U_i = \prod_{1 \leq j \leq N, j \neq i}(\alpha_i - \alpha_j)^{-1}$ for any $1 \leq i \leq N$. If $\alpha_i \in A_h$ for some $1 \leq h \leq t$, it follows from Lemma 5 in [32] that

$$U_i = \left(\prod_{\alpha \neq 0 \in A} \alpha^{-1}\right)\left(\prod_{\beta \in A}(\eta - \beta)\right)^{1-t}\left(\prod_{1 \leq j \leq t, j \neq h}(\alpha_h - \alpha_j)^{-1}\right).$$

Moreover, let $\delta = (\prod_{\alpha \neq 0 \in A} \alpha)(\prod_{\beta \in A}(\eta - \beta))^{t-1}$, we have $\delta U_i \in F_{p^e} \subset F_q$ as $\alpha_1, \alpha_2, \ldots, \alpha_t \in F_{p^e}$. By using GRS codes, we construct the following MDS codes of length n over F_{q^2} and determine their Hermitian hulls.

Theorem 3.2 *Let $q = p^m \geq 3$ be a prime power and e be a positive integer with $e|m$. Let $N = tp^{ez}$ be an integer, where $1 \leq t \leq p^e$ and $1 \leq z \leq \frac{2m}{e} - 1$. Assume that n is an integer such that $1 < n < N$. For any $1 < k \leq \lfloor \frac{N+q-1}{q+1} \rfloor$ and $n + k > N + 1$, then there exists a q^2-ary $[n, k]$ MDS code with l-dimensional Hermitian hull for any $1 \leq l \leq n - N + k - 1$.*

Proof Let the notations be defined as above. Take $\mathbf{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Since $1 \leq t \leq p^e \leq q$ and $N = tp^{ez}$, we have $1 < k \leq \lfloor \frac{N+q-1}{q+1} \rfloor \leq p^{ez} = |A|$. It follows from $n + k > N + 1$ that $N - n < k - 1 \leq p^{ez} - 1 < |A|$. Then for any $1 \leq i \leq n$, we have

$$\begin{aligned} u_i &= \prod_{1 \leq j \leq n, j \neq i}(\alpha_i - \alpha_j)^{-1} \\ &= \prod_{1 \leq j \leq N, j \neq i}(\alpha_i - \alpha_j)^{-1}) \prod_{j=n+1}^{N}(\alpha_i - \alpha_j) \\ &= U_i \prod_{j=n+1}^{N}(\alpha_i - \alpha_j). \end{aligned}$$

Since $\delta U_i \in F_q$, there exist $\upsilon_1, \upsilon_2, \ldots, \upsilon_n \in F_{q^2}$ such that $\upsilon_i^{q+1} = \delta U_i$ for any $1 \leq i \leq n$. Furthermore, we take $\mathbf{v} = (b\upsilon_1, b\upsilon_2, \ldots, b\upsilon_s, \upsilon_{s+1}, \ldots, \upsilon_n)$ with $1 \leq s \leq n + k - N - 1$, where $b^{q+1} \neq 1$ and $\upsilon_i \in F_{q^2}^*$ with $\upsilon_i^{q+1} = \delta U_i$ for all $1 \leq i \leq n$.

We consider the following q^2-ary GRS code of length n,

$$\begin{aligned} GRS_k(\mathbf{a}, \mathbf{v}) = \{&(b\upsilon_1 f(\alpha_1), \ldots, b\upsilon_s f(\alpha_s), \upsilon_{s+1} f(\alpha_{s+1}),\\ &\ldots, \upsilon_n f(\alpha_n)) : f(x) \in F_{q^2}[x]_k\}. \end{aligned}$$

For any $\mathbf{c} = (b\upsilon_1 f(\alpha_1), \ldots, b\upsilon_s f(\alpha_s), \upsilon_{s+1} f(\alpha_{s+1}), \ldots, \upsilon_n f(\alpha_n)) \in GRS_k(\mathbf{a}, \mathbf{v})$ $\cap GRS(\mathbf{a}, \mathbf{v})^{\perp H}$. It follows from Lemma 2.2 that

$$\begin{aligned} &(b^{q+1}\upsilon_1^{q+1} f(\alpha_1), \ldots, b^{q+1}\upsilon_s^{q+1} f(\alpha_s), \upsilon_{s+1}^{q+1} f(\alpha_{s+1}), \ldots, \upsilon_n^{q+1} f(\alpha_n))\\ &\quad = (\overline{u_1} g(\alpha_1^q), \ldots, \overline{u_s} g(\alpha_s^q), \overline{u_{s+1}} g(\alpha_{s+1}^q), \ldots, \overline{u_n} g(\alpha_n^q)) \\ &\quad = (\overline{u_1} g^{'q}(\alpha_1), \ldots, \overline{u_s} g^{'q}(\alpha_s), \overline{u_{s+1}} g^{'q}(\alpha_{s+1}), \ldots, \overline{u_n} g^{'q}(\alpha_n)), \end{aligned} \tag{4}$$

where $g^{'}(x) \in F_{q^2}[x]_{n-k}$. For any $s+1 \leq i \leq n$, it follows from the last $n-s$ coordinates of (4) that $\upsilon_i^{q+1} f(\alpha_i) = \overline{u_i} g^{'q}(\alpha_i)$, i.e.,

$$\delta U_i f^q(\alpha_i) = u_i g^{'}(\alpha_i) = \left(U_i \prod_{n+1 \leq j \leq N} (\alpha_i - \alpha_j) \right) g^{'}(\alpha_i).$$

This shows that $\delta f^q(x) = (\prod_{n+1 \leq j \leq N}(x - \alpha_j))g^{'}(x)$ has at least $n-s$ distinct roots. It is clear that $\deg((\prod_{n+1 \leq j \leq N}(x - \alpha_j))g^{'}(x)) \leq N - n + n - k - 1 \leq N - k - 1$. Besides, it is easy to know that $\deg(\delta f^q(x)) \leq q(k-1) \leq N - k - 1$, due to $1 \leq k \leq \lfloor \frac{N+q-1}{q+1} \rfloor$. It follows from $1 \leq s \leq n + k - N - 1$ that $N - k - 1 < n - s$. Therefore, we have $\delta f^q(x) = (\prod_{n+1 \leq j \leq N}(x - \alpha_j))g^{'}(x)$ for any $x \in F_{q^2}$. According to the first s coordinates of (4), we have that $b^{q+1}\upsilon_i^{q+1} f(\alpha_i) = \overline{u_i} g^{'q}(\alpha_i)$, i.e.,

$$b^{q+1}\delta U_i f^q(\alpha_i) = u_i g^{'}(\alpha_i) = \left(U_i \prod_{n+1 \leq j \leq N} (\alpha_i - \alpha_j) \right) g^{'}(\alpha_i) = \delta U_i f^q(\alpha_i),$$

for any $1 \leq i \leq s$. As $b_i^{q+1} \neq 1$ for any $1 \leq i \leq s$, we can obtain $f(\alpha_i) = 0$ for any $1 \leq i \leq s$. Moreover, it follows from $\delta f^q(x) = (\prod_{n+1 \leq j \leq N}(x - \alpha_j))g^{'}(x)$ that $f(\alpha_i) = 0$ for any $n+1 \leq i \leq N$. Then we have that $f(x) = h(x)(\prod_{i=1}^{s}(x - \alpha_i))(\prod_{i=n+1}^{N}(x - \alpha_i))$, where $\deg(h(x)) \leq n - N + k - 1 - s$. Put $g^{'}(x) = \delta f^q(x) \prod_{i=n+1}^{N}(x - \alpha_i)^{-1} = \delta h^q(x)(\prod_{i=1}^{s}(x^q - \overline{\alpha_i}))(\prod_{i=n+1}^{N}(x - \alpha_i)^{q-1})$ and $g(x) = \delta^q h(x^q)(\prod_{i=1}^{s}(x^q - \alpha_i))(\prod_{i=n+1}^{N}(x - \alpha_i^q)^{q-1})$. For any $g(x), g^{'}(x) \in F_{q^2}[x]$ of the forms above, there is a $f(x) = h(x)(\prod_{i=1}^{s}(x - \alpha_i))(\prod_{i=n+1}^{N}(x - \alpha_i))$ such that

$$\begin{aligned}&(b^{q+1}\upsilon_1^{q+1}f(\alpha_1),\ldots,b^{q+1}\upsilon_s^{q+1}f(\alpha_s),\upsilon_{s+1}^{q+1}f(\alpha_{s+1}),\ldots,\upsilon_n^{q+1}f(\alpha_n))\\&=(\overline{u_1}g(\alpha_1^q),\ldots,\overline{u_s}g(\alpha_s^q),\overline{u_{s+1}}g(\alpha_{s+1}^q),\ldots,\overline{u_n}g(\alpha_n^q))\\&=(\overline{u_1}g^{\prime q}(\alpha_1),\ldots,\overline{u_s}g^{\prime q}(\alpha_s),\overline{u_{s+1}}g^{\prime q}(\alpha_{s+1}),\ldots,\overline{u_n}g^{\prime q}(\alpha_n)),\end{aligned}$$

which implies that

$$\begin{aligned}&(b\upsilon f(\alpha_1),\ldots,b\upsilon_s f(\alpha_s),\upsilon_{s+1}f(\alpha_{s+1}),\ldots,\upsilon_n f(\alpha_n))\\&\in GRS_k(\mathbf{a},\mathbf{v})\cap GRS_k(\mathbf{a},\mathbf{v})^{\perp H}.\end{aligned}$$

Therefore, $\dim(\mathrm{Hull}(GRS_k(\mathbf{a},\mathbf{v},\infty)))=n-N+k-s$, where $1\le s\le n+k-N-1$. This completes the proof. □

Let n' be some divisor of q^2-1. Denote $n_1=\dfrac{n'}{\gcd(n',q+1)}$ and $n_2=\gcd(n',q+1)$. Then $\gcd(n_1,q+1)=1$ and $n_1|q-1$. Let $G=\langle\omega^{\frac{q^2-1}{n'}}\rangle$ and $D=\langle\omega^{\frac{q+1}{n_2}}\rangle$. It is obvious that G and D are the multiplicative subgroups of $F_{q^2}^*$ of order $|G|=n'$ and $|D|=n_2(q-1)$, respectively. Due to $\frac{q+1}{n_2}|\frac{q^2-1}{n'}$, we have G as a subgroup of D. Then there are $\beta_1,\ldots,\beta_{\frac{q-1}{n_1}}\in D$ such that $D=\beta_1G\cup\beta_2G\cup\ldots\cup\beta_{(\frac{q-1}{n_1}-1)}G$. Let $1\le t\le\frac{q-1}{n_1}$ and $N=tn'$. For convenience, we denote $\cup_{i=1}^t\beta_iG=\{\alpha_1,\alpha_2,\ldots,\alpha_N\}$ and $U_i=\prod_{1\le j\le N,j\ne i}(\alpha_i-\alpha_j)^{-1}$ for any $1\le i\le N$. If $\alpha_i\in\beta_sG$ for some $1\le s\le t$, it follows from Lemma 7 of [32] that

$$U_i=\alpha_i n'^{-1}\beta_s^{-n'}\prod_{0\le h\le t-1,h\ne s}(\beta_s^{n'}-\beta_h^{n'})^{-1},$$

and $\varepsilon U_i=n'^{-1}\beta_s^{-n'}\prod_{0\le h\le t-1,h\ne s}(\beta_s^{n'}-\beta_h^{n'})^{-1}\in F_q^*$, where $\varepsilon=\alpha_i^{-1}$. Furthermore, we construct the following MDS codes and determine their Hermitian hulls.

Theorem 3.3 *Let $q=p^m\ge 3$ be a prime power and $n'=n_1n_2$ be some divisor of q^2-1 with $n_1=\frac{n'}{gcd(n',q+1)}$ and $n_2=gcd(n',q+1)$. Suppose that $N=tn'$ with $1\le t\le\frac{q-1}{n_1}$ and n is an integer such that $1<n<N$. For any $1<k\le\lfloor\frac{N+q}{q+1}\rfloor$ and $n+k>N+1$, then there exists a q^2-ary $[n,k]$ MDS code with l-dimensional Hermitian hull for any $1\le l\le n-N+k-1$.*

Proof With the notations above, we take $\mathbf{a}=(\alpha_1,\alpha_2,\ldots,\alpha_n)$. Then we have

$$\begin{aligned}u_i&=\prod_{1\le j\le n,j\ne i}(\alpha_i-\alpha_j)^{-1}\\&=U_i\prod_{j=n+1}^{N}(\alpha_i-\alpha_j),\end{aligned}$$

for any $1 \le i \le n$. Since $\varepsilon U_i \in F_q^*$, there must exist $\upsilon_1, \upsilon_2, \ldots, \upsilon_n \in F_{q^2}$ such that $\upsilon_i^{q+1} = \varepsilon U_i$ for any $1 \le i \le n$. Let $b \in F_{q^2}^*$ and $b^{q+1} \neq 1$. Take $\mathbf{v} = (b\upsilon_1, b\upsilon_2, \ldots, b\upsilon_s, \upsilon_{s+1}, \ldots, \upsilon_n)$, where $1 \le s \le n+k-N-1$. Then we obtain the following q^2-ary GRS code of length n associated with $\mathbf{a}$ and $\mathbf{v}$,

$$\begin{aligned} GRS_k(\mathbf{a}, \mathbf{v}) = \{&(b\upsilon_1 f(\alpha_1), \ldots, b\upsilon_s f(\alpha_s), \upsilon_{s+1} f(\alpha_{s+1}), \\ &\ldots, \upsilon_n f(\alpha_n)) : f(x) \in F_{q^2}[x]_k\}. \end{aligned}$$

For any $\mathbf{c} = (b\upsilon_1 f(\alpha_1), \ldots, b\upsilon_s f(\alpha_s), \upsilon_{s+1} f(\alpha_{s+1}), \ldots, \upsilon_n f(\alpha_n)) \in GRS_k(\mathbf{a}, \mathbf{v})$ $\cap GRS(\mathbf{a}, \mathbf{v})^{\perp H}$. According to Lemma 2.2, we have

$$\begin{aligned} &(b^{q+1}\upsilon_1^{q+1} f(\alpha_1), \ldots, b^{q+1}\upsilon_s^{q+1} f(\alpha_s), \upsilon_{s+1}^{q+1} f(\alpha_{s+1}), \ldots, \upsilon_n^{q+1} f(\alpha_n)) \\ &\quad = (\overline{u_1} g(\alpha_1^q), \ldots, \overline{u_s} g(\alpha_s^q), \overline{u_{s+1}} g(\alpha_{s+1}^q), \ldots, \overline{u_n} g(\alpha_n^q)) \\ &\quad = (\overline{u_1} g^{'q}(\alpha_1), \ldots, \overline{u_s} g^{'q}(\alpha_s), \overline{u_{s+1}} g^{'q}(\alpha_{s+1}), \ldots, \overline{u_n} g^{'q}(\alpha_n)), \end{aligned} \tag{5}$$

where $g^{'}(x) \in F_{q^2}[x]_{n-k}$. For any $s+1 \le i \le n$, it follows from the last $n-s$ coordinates of (6) that $\upsilon_i^{q+1} f(\alpha_i) = \overline{u_i} g^{'q}(\alpha_i)$, i.e.,

$$\alpha_i^{-1} U_i f^q(\alpha_i) = u_i g^{'}(\alpha_i) = \left(U_i \prod_{j=n+1}^{N} (\alpha_i - \alpha_j) \right) g^{'}(\alpha_i).$$

Then the polynomial $f^q(x) = x(\prod_{j=n+1}^N (x-\alpha_j)) g^{'}(x)$ has at least $n-s$ distinct roots. It is clear that $\deg(x(\prod_{j=n+1}^N (x-\alpha_j)) g^{'}(x)) \le N-n+1+n-k-1 \le N-k$. Since $1 < k \le \lfloor \frac{N+q}{q+1} \rfloor$, $\deg(f^q(x)) \le q(k-1) \le N-k$. It follows from $1 \le s \le n+k-N-1$ that $N-k < n-s$. Therefore, we have $f^q(x) = x(\prod_{j=n+1}^N (x-\alpha_j)) g^{'}(x)$ for any $x \in F_{q^2}$. From the first s coordinates of (6), we have that $b^{q+1}\upsilon_i^{q+1} f(\alpha_i) = \overline{u_i} g^{'q}(\alpha_i)$, i.e.,

$$b^{q+1}\alpha_i^{-1} U_i f^q(\alpha_i) = u_i g^{'}(\alpha_i) = \left(U_i \prod_{j=n+1}^{N} (\alpha_i - \alpha_j) \right) g^{'}(\alpha_i),$$

for any $1 \le i \le s$. Then $b^{q+1} f^q(\alpha_i) = \alpha_i (\prod_{j=n+1}^N (\alpha_i - \alpha_j)) g^{'}(\alpha_i) = f^q(\alpha_i)$ for any $1 \le i \le s$. As $b_i^{q+1} \neq 1$ for any $1 \le i \le s$, we obtain $f(\alpha_i) = 0$ for any $1 \le i \le s$. In addition, it follows from $f^q(x) = x(\prod_{j=n+1}^N (x-\alpha_j)) g^{'}(x)$ that $f(0) = 0$ and $f(\alpha_i) = 0$ for any $n+1 \le i \le N$. Thus, we have that $f(x) = xh(x)(\prod_{i=1}^s (x-\alpha_i))(\prod_{i=n+1}^N (x-\alpha_i))$, where $\deg(h(x)) \le n-N+k-2-s$. Put $g^{'}(x) = x^{-1} f^q(x) \prod_{i=n+1}^N (x-\alpha_i)^{-1} = x^{q-1} h^q(x)(\prod_{i=1}^s (x^q - \overline{\alpha_i}))(\prod_{i=n+1}^N (x - \alpha_i)^{q-1})$ and $g(x) = x^{q-1} h(x^q)(\prod_{i=1}^s (x^q - \alpha_i))(\prod_{i=n+1}^N (x - \alpha_i^q)^{q-1})$. For any

Table 1 Sample parameters of EAQEC codes from Theorem 3.4 for $q = 9$ and $n = 11, 12$

k	l	$[[n, k_1, d_1; c_1]]_q$	$[[n, k_2, d_2; c_2]]_q$
3	1	$[[11, 2, 9; 7]]_9$	$[[11, 7, 4; 2]]_9$
4	1	$[[11, 3, 8; 6]]_9$	$[[11, 6, 5; 3]]_9$
4	2	$[[11, 2, 8; 5]]_9$	$[[11, 5, 5; 2]]_9$
5	1	$[[11, 4, 7; 5]]_9$	$[[11, 5, 6; 4]]_9$
5	2	$[[11, 3, 7; 4]]_9$	$[[11, 4, 6; 3]]_9$
5	3	$[[11, 2, 7; 3]]_9$	$[[11, 3, 6; 2]]_9$
4	1	$[[12, 3, 9; 7]]_9$	$[[12, 7, 5; 3]]_9$
5	1	$[[12, 4, 8; 6]]_9$	$[[12, 6, 6; 4]]_9$
5	2	$[[12, 3, 8; 5]]_9$	$[[12, 5, 6; 3]]_9$
6	1	$[[12, 5, 7; 5]]_9$	$[[12, 5, 7; 5]]_9$
6	2	$[[12, 4, 7; 4]]_9$	$[[12, 4, 7; 4]]_9$
6	3	$[[12, 3, 7; 3]]_9$	$[[12, 3, 7; 3]]_9$

1. $k_1 = k - l, d_1 = n - k + 1, c_1 = n - k - l.$
2. $k_2 = n - k - l, d_2 = k + 1, c_2 = k - l$

$g(x), g^{'}(x) \in F_{q^2}[x]$ of the forms above, there exists a $f(x) = xh(x)(\prod_{i=1}^{s}(x - \alpha_i))(\prod_{i=n+1}^{N}(x - \alpha_i))$ such that

$$\begin{aligned}
&(b^{q+1}\upsilon_1^{q+1} f(\alpha_1), \ldots, b^{q+1}\upsilon_s^{q+1} f(\alpha_s), \upsilon_{s+1}^{q+1} f(\alpha_{s+1}), \ldots, \upsilon_n^{q+1} f(\alpha_n))\\
&\quad = (\overline{u_1} g(\alpha_1^q), \ldots, \overline{u_s} g(\alpha_s^q), \overline{u_{s+1}} g(\alpha_{s+1}^q), \ldots, \overline{u_n} g(\alpha_n^q))\\
&\quad = (\overline{u_1} g^{'q}(\alpha_1), \ldots, \overline{u_s} g^{'q}(\alpha_s), \overline{u_{s+1}} g^{'q}(\alpha_{s+1}), \ldots, \overline{u_n} g^{'q}(\alpha_n)),
\end{aligned}$$

which implies that

$$\begin{aligned}
&(b\upsilon f(\alpha_1), \ldots, b\upsilon_s f(\alpha_s), \upsilon_{s+1} f(\alpha_{s+1}), \ldots, \upsilon_n f(\alpha_n))\\
&\quad \in GRS_k(\mathbf{a}, \mathbf{v}) \cap GRS_k(\mathbf{a}, \mathbf{v})^{\perp H}.
\end{aligned}$$

Therefore, $\dim(\mathrm{Hull}(GRS_k(\mathbf{a}, \mathbf{v}, \infty))) = n - N + k - 1 - s$, where $1 \leq s \leq n + k - N - 1$. This completes the proof. □

In Theorems 3.1, 3.2 and 3.3, we constructed three classes of MDS codes by using GRS codes and completely determined their Hermitian hulls. Based on the results and Lemma 2.5, three classes of q-ary EAQEC codes and EAQEC MDS codes can be easily obtained as follows.

Theorem 3.4 *Let q be a prime power. If $q + 1 < n \leq 2(q - 1)$ and $n - q < k \leq \lfloor \frac{n}{2} \rfloor$, then there exist $[[n, k - l, n - k + 1; n - k - l]]_q$ EAQEC codes and $[[n, n - k - l, k + 1; k - l]]_q$ EAQEC MDS codes, where $1 \leq l \leq k + q - n$.*

Example 1 Let $q = 9$ and $n = 11, 12$ in Theorem 3.4. Then we can obtain some new EAQEC codes and EAQEC MDS codes, whose parameters are listed in Table 1.

Theorem 3.5 *Let $q = p^m \geq 3$ be a prime power and e be a positive integer with $e|m$. Assume that $N = tp^{ez}$ with $1 \leq t \leq p^e$ and $1 \leq z \leq \frac{2m}{e} - 1$ and n is an integer such that $1 < n < N$. If $1 < k \leq \lfloor \frac{N+q-1}{q+1} \rfloor$ and $n + k > N + 1$, then there exist $[[n, k - l, n - k + 1; n - k - l]]_q$ EAQEC codes and $[[n, n - k - l, k + 1; k - l]]_q$ EAQEC MDS codes, where $1 \leq l \leq n - N + k - 1$.*

Example 2 Let $p = 3$, $m = 2$ and $e = 2$ in Theorem 3.5, then $z = 1$. Take $N = 54$ and $n = 53$, then we can obtain some new EAQEC codes and EAQEC MDS codes, whose parameters are listed in Table 2.

Theorem 3.6 *Let $q = p^m \geq 3$ be a prime power and $n^{'} = n_1 n_2$ be some divisor of $q^2 - 1$ with $n_1 = \frac{n^{'}}{gcd(n^{'}, q+1)}$ and $n_2 = gcd(n^{'}, q + 1)$. Suppose that $N = tn^{'}$ with $1 \leq t \leq \frac{q-1}{n_1}$ and n is an integer such that $1 < n < N$. If $1 < k \leq \lfloor \frac{N+q}{q+1} \rfloor$ and $n + k > N + 1$, then there exist $[[n, k - l, n - k + 1; n - k - l]]_q$ EAQEC codes and $[[n, n - k - l, k + 1; k - l]]_q$ EAQEC MDS codes, where $1 \leq l \leq n - N + k - 1$.*

Example 3 Let $p = 5$ and $m = 2$ in Theorem 3.6. Take $N = tn^{'} = 2 \cdot 78 = 156$ and $n = 155$, then we can obtain some new EAQEC codes and EAQEC MDS codes, whose parameters are listed in Table 3.

Remark 1 (1) In [30,31], the authors constructed some EAQEC (MDS) codes of lengths $n \leq q$ and all EAQEC MDS codes of lengths $q + 1$. In [32], all q-ary EAQEC MDS codes of lengths $n \leq q$ are completely determined. So, we mainly consider the construction of EAQEC codes of length $n > q + 1$.

(2) Let $q > 3$ be a prime power. From Theorem 3.1, we know that Theorem 3.4 holds even for $n = q + 1$, i.e., we have EAQEC codes with parameters $[[q + 1, k - l, q - k + 2; q - k - l + 1]]_q$ and EAQEC MDS codes with parameters $[[q + 1, q - k - l + 1, k + 1; k - l]]_q$, where $1 < k \leq \lfloor \frac{q+1}{2} \rfloor$ and $1 \leq l \leq k - 1$. However, the EAQEC codes have been constructed in [30]. We do not consider the case with $n = q + 1$ in Theorem 3.4. Now, all the EAQEC codes in Theorem 3.4 are new in the sense that our parameters are not covered by the codes available in the literature.

(3) Notice that the required number of maximally entangled states and lengths of the EAQEC codes constructed by us can take various values. Comparing the parameters with all known ones in the literature, one can find that our EAQEC codes in Theorems 3.5 and 3.6 are new. Some examples are given in Tables 1, 2 and 3, which can be obtained by Theorems 3.4, 3.5 and 3.6, respectively. The parameters of our EAQEC codes are flexible not only on c but also on n.

4 Conclusions

In this paper, we first constructed three classes of MDS codes by considering GRS codes and determined their Hermitian hulls. Based on the constructed MDS codes, we obtained three new classes of q-ary EAQEC codes and EAQEC MDS codes,

Table 2 Sample parameters of EAQEC codes from Theorem 3.5 for $p = 9$, $N = 54$ and $n = 53$

k	l	$[[n, k_1, d_1; c_1]]_q$	$[[n, k_2, d_2; c_2]]_q$
3	1	$[[53, 2, 51; 49]]_9$	$[[53, 49, 4; 2]]_9$
4	1	$[[53, 3, 50; 48]]_9$	$[[53, 48, 5; 3]]_9$
4	2	$[[53, 2, 50; 47]]_9$	$[[53, 47, 5; 2]]_9$
5	1	$[[53, 4, 49; 47]]_9$	$[[53, 47, 6; 4]]_9$
5	2	$[[53, 3, 49; 46]]_9$	$[[53, 46, 6; 3]]_9$
5	3	$[[53, 2, 49; 45]]_9$	$[[53, 45, 6; 2]]_9$
6	1	$[[53, 5, 48; 46]]_9$	$[[53, 46, 7; 5]]_9$
6	2	$[[53, 4, 48; 45]]_9$	$[[53, 45, 7; 4]]_9$
6	3	$[[53, 3, 48; 44]]_9$	$[[53, 44, 7; 3]]_9$
6	4	$[[53, 2, 48; 43]]_9$	$[[53, 43, 7; 2]]_9$

1. $k_1 = k - l, d_1 = n - k + 1, c_1 = n - k - l.$
2. $k_2 = n - k - l, d_2 = k + 1, c_2 = k - l$

Table 3 Sample parameters of EAQEC codes from Theorem 3.6 for $q = 25$, $N = 156$ and $n = 155$

k	l	$[[n, k_1, d_1; c_1]]_q$	$[[n, k_2, d_2; c_2]]_q$
3	1	$[[155, 2, 153; 151]]_{25}$	$[[155, 151, 4; 2]]_{25}$
4	1	$[[155, 3, 152; 150]]_{25}$	$[[155, 150, 5; 3]]_{25}$
4	2	$[[155, 2, 152; 149]]_{25}$	$[[155, 149, 5; 2]]_{25}$
5	1	$[[155, 4, 151; 149]]_{25}$	$[[155, 149, 6; 4]]_{25}$
5	2	$[[155, 3, 151; 148]]_{25}$	$[[155, 148, 6; 3]]_{25}$
5	3	$[[155, 2, 151; 147]]_{25}$	$[[155, 147, 6; 2]]_{25}$
6	1	$[[155, 5, 150; 148]]_{25}$	$[[155, 148, 7; 5]]_{25}$
6	2	$[[155, 4, 150; 147]]_{25}$	$[[155, 147, 7; 4]]_{25}$
6	3	$[[155, 3, 150; 146]]_{25}$	$[[155, 146, 7; 3]]_{25}$
6	4	$[[155, 2, 150; 145]]_{25}$	$[[155, 145, 7; 2]]_{25}$

1. $k_1 = k - l, d_1 = n - k + 1, c_1 = n - k - l.$
2. $k_2 = n - k - l, d_2 = k + 1, c_2 = k - l$

whose maximally entangled states are closely related to the Hermitian hull and are flexible. Also, the three new classes of EAQEC codes and EAQEC MDS codes have more flexible lengths. Comparing with the parameters of all known EAQEC codes, all EAQEC codes obtained in this paper are new. The Hermitian hull of a linear code is a worthwhile problem for further study. It would be interesting to construct more EAQEC MDS codes by determining the Hermitian hulls of linear codes.

References

1. Shor, P.W.: Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A **52**(4), R2493 (1995)
2. Steane, A.: Multiple-particle interference and quantum error correction. Proc. R. Soc. Lond. Ser. A **452**(1954), 2551–2577 (1996)
3. 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)

4. Jin, L., Kan, H., Wen, J.: Quantum MDS codes with relatively large minimum distance from Hermitian self-orthogonal codes. Des. Codes Cryptogr. **84**(3), 463–471 (2017)
5. Zhang, T., Ge, G.: Quantum MDS codes with large minimum distance. Des. Codes Cryptogr. **83**(3), 503–517 (2017)
6. Shi, X., Yue, Q., Zhu, X.: Construction of some quantum MDS. Finite Fields Appl. **46**, 347–362 (2017)
7. Shi, X., Yue, Q., Chang, Y.: Some quantum MDS codes with large minimum distance from generalized Reed–Solomon codes. Cryptogr. Commun. **10**(6), 1165–1182 (2018)
8. Fang, W., Fu, F.: Two new classes of quantum MDS codes. Finite Fields Appl. **53**, 85–98 (2018)
9. Brun, T., Devetak, I., Hsieh, M.H.: Correcting quantum errors with entanglement. Science **314**(5798), 436–439 (2006)
10. Hsieh, M.H., Devetak, I., Brun, T.: General entanglement-assisted quantum error-correcting codes. Phys. Rev. A **76**, 062313 (2007)
11. Wilde, M., Brun, T.: Optimal entanglement formulas for entanglement-assisted quantum coding. Phys. Rev. A **77**, 064302 (2008)
12. Shin, J., Heo, J., Brun, T.: Entanglement-assisted codeword stabilized quantum codes. Phys. Rev. A, Gen. Phys. **84**, 062321 (2011)
13. Lai, C., Brun, T.: Entanglement increases the error-correcting ability of quantum error-correcting codes. Phys. Rev. A, Gen. Phys. **88**, 012320 (2013)
14. Brun, T.A., Devetak, I., Hsieh, M.H.: Catalytic quantum error correction. IEEE Trans. Inf. Theory **60**(6), 3073–3089 (2014)
15. Grassl, M.: Entanglement-assisted quantum communication beating the quantum singleton bound. In: AQIS, Taiwan (2016)
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. Qian, J., Zhang, L.: On MDS linear complementary dual codes and entanglement-assisted quantum codes. Des. Codes Cryptogr. **86**(7), 1565–1572 (2018)
18. Guenda, K., Jitman, S., Gulliver, T.A.: Constructions of good entanglement-assisted quantum error correcting codes. Des. Codes Cryptogr. **86**, 121–136 (2018)
19. Liu, X., Yu, L., Hu, P.: New entanglement-assisted quantum codes from k-Galois dual codes. Finite Fields Appl. **55**, 21–32 (2019)
20. Fan, J., Chen, H., Xu, J.: Construction of q-ary entanglement-assisted quantum MDS codes with minimum distance greater than $q+1$. Quantum Inf. Comput. **16**, 423–434 (2016)
21. Li, R., Zuo, F., Liu, Y.: A study of skew asymmetric q^2-cyclotomic coset and its application. J. Air Force Eng. Univ. (Nat. Sci. Ed.) **12**(1), 87–89 (2011). (in Chinese)
22. Lü, L.-D., Li, R.: Entanglement-assisted quantum codes constructed from primitive quaternary BCH codes. Int. J. Quantum Inf. **12**(03), 1450015 (2014)
23. Chen, J., Huang, Y., Feng, C., Chen, R.: Entanglement-assisted quantum MDS codes constructed from negacyclic codes. Quantum Inf. Process. **16**, 303 (2017)
24. Lu, L., Li, R., Guo, L., Ma, Y., Liu, Y.: Entanglement-assisted quantum MDS codes from negacyclic codes. Quantum Inf. Process. **17**, 69 (2018)
25. Chen, X., Zhu, S., Kai, X.: Entanglement-assisted quantum MDS codes constructed from constacyclic codes. Quantum Inf. Process. **17**, 273 (2018)
26. Lu, L., Ma, W., Li, R., Ma, Y., Liu, Y., Cao, H.: Entanglement-assisted quantum MDS codes from constacyclic codes with large minimum distance. Finite Fields Appl. **53**, 309–325 (2018)
27. Liu, Y., Li, R., Lv, L., Ma, Y.: Application of constacyclic codes to entanglement-assisted quantum maximum distance separable codes. Quantum Inf. Process. **17**, 210 (2018)
28. Koroglu, M.E.: New entanglement-assisted MDS quantum codes from constacyclic codes. Quantum Inf. Process. **18**, 44 (2019)
29. Li, L., Zhu, S., Liu, L., Kai, X.: Entanglement-assisted quantum MDS codes from generalized Reed–Solomon codes. Quantum Inf. Process. **18**, 153 (2019)
30. Luo, G., Cao, X., Chen, X.: MDS codes with hulls of arbitrary dimensions and their quantum error correction. IEEE Trans. Inf. Theory **65**(5), 2944–2952 (2019)
31. Luo, G., Cao, X.: Two new families of entanglement-assisted quantum MDS codes from generalized Reed–Solomon codes. Quantum Inf. Process. **18**, 89 (2019)
32. Fang, W., Fu, F., Li, L., Zhu, S.: Euclidean and Hermitian Hulls of MDS Codes and Their Applications to EAQECCs. arXiv:1812.09019 (2019)

33. Assmus Jr., E.F., Key, J.: Designs and Their Codes. Cambridge University Press, Cambridge (1992). (Cambridge Tracts in Mathematics, vol. 103 (Second printing with corrections, 1993))
34. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error Correcting Codes. North-Holland, The Netherlands (1977)
35. Jin, L., Xing, C.: New MDS self-dual codes from generalized Reed–Solomon codes. IEEE Trans. Inf. Theory **63**(3), 1434–1438 (2017)
36. Lidl, R., Niederreiter, H.: Finite Fields. Cambridge University Press, Cambridge (1977)