MDS Codes With Galois Hulls of Arbitrary Dimensions and the Related Entanglement-Assisted Quantum Error Correction

Meng Cao

***Abstract*— Let $q = p^e$ be a prime power and ℓ be an integer with $0 \leq \ell \leq e-1$. The ℓ-Galois hull of classical linear codes is a generalization of the Euclidean hull and Hermitian hull. We provide a necessary and sufficient condition under which a codeword of a GRS code or an extended GRS code belongs to its ℓ-Galois dual code, generalizing both the Euclidean case and Hermitian case in the literature. By using four different tools: 1) the norm mapping from $\mathbb{F}_q^*$ to $\mathbb{F}_{p^\ell}^*$; 2) the direct product of two cyclic subgroups; 3) the coset decomposition of a cyclic group; 4) an additive subgroup of $\mathbb{F}_q$ and its cosets, we construct eleven families of q-ary MDS codes with ℓ-Galois hulls of arbitrary dimensions, and give the related eleven families of $[[n, k, d; c]]_q$ entanglement-assisted quantum error-correcting codes (EAQECCs) with relatively large minimum distance in the sense that $2d = n - k + 2 + c$. We show that developing the theory on ℓ-Galois hulls of q-ary MDS codes in this paper enables us to obtain new q-ary EAQECCs with different kinds of length sets via different ℓ, where $2\ell \mid e$.**

***Index Terms*— ℓ-Galois hull, MDS code, generalized Reed-Solomon (GRS) code, entanglement-assisted quantum error-correcting code (EAQECC).**

I. Introduction

QUANTUM error-correcting codes are essential to quantum computation and quantum communication due to their crucial role in dealing with the problem of quantum decoherence. In 1995, Shor [50] discovered the world's first quantum error-correcting code with parameters $[[9, 1, 3]]$ by using the quantum analog of the repetition code. Since then, the theory of quantum codes has achieved rapid development (e.g., see [1], [4], [5], [7], [8], [12], [21], [23], [25], [27], [28], [33], [35], [43], [44], [47], [48], [51]). As we know, the construction of quantum codes with good parameters is important in quantum information processing. However, it is very difficult to give a general method for acquiring more good quantum codes. In 1996, the famous CSS construction proposed by Calderbank and Shor [6] and Steane [52] offers us an effective way to construct quantum stabilizer codes from classical linear codes with certain self-orthogonality. By this method, a q-ary quantum stabilizer code can be derived from a q-ary self-orthogonal or dual-containing classical linear code.

Nevertheless, the CSS construction is inapplicable to general classical linear codes. In other words, a classical linear code which is neither self-orthogonal nor dual-containing can not generate a quantum stabilizer code by CSS construction. To avoid this problem, Brun et al. [2] proposed an interesting concept called entanglement-assisted quantum error-correcting codes (EAQECCs), which can be regarded as a generalization of the quantum stabilizer codes. According to their discovery, the EAQECCs can be generated by the classical linear codes without the restriction of self-orthogonality by utilizing the pre-shared entanglement between the sender and receiver. Usually, we denote by $[[n, k, d; c]]_q$ a q-ary EAQECC which encodes k logical qubits into n physical qubits by means of c copies of maximally entangled states (i.e., c ebits). To be specific, let $\mathcal{L}$ be the space of linear operators defined in the qubit Hilbert space $\mathcal{H}$. Let us consider the isometric operator $U : \mathcal{H}^{\otimes n_1} \to \mathcal{H}^{\otimes n_2}$ and its completely positive, trace preserving (CPTP) map $\hat{U} : \mathcal{L}^{\otimes n_1} \to \mathcal{L}^{\otimes n_2}$ defined by $\hat{U}(\chi) = U\chi U^\dagger$. As shown in [3], the quantum communication scenario involves two spatially separated parties, Alice and Bob, owning the following resources at their disposal:

- A noisy quantum channel defined by a CPTP map $\mathcal{N} : \mathcal{L}^{\otimes n} \to \mathcal{L}^{\otimes n}$ taking density operators on Alice's system to those on Bob's system;
- The c ebit state $|\Upsilon\rangle^{\otimes c}$ shared between Alice and Bob.

Through these resources, Alice wants to send k qubits to Bob perfectly. Then, an $[[n, k, d; c]]_q$ EAQECC is made up of

- An encoding operation $\mathcal{E} : \mathcal{L}^{\otimes k} \otimes \mathcal{L}^{\otimes c} \to \mathcal{L}^{\otimes n}$;
- A decoding operation $\mathcal{D} : \mathcal{L}^{\otimes n} \otimes \mathcal{L}^{\otimes c} \to \mathcal{L}^{\otimes k}$

with $\mathcal{D} \circ \mathcal{N} \circ \mathcal{E} \circ \hat{V} = \mathrm{id}^{\otimes k}$, where V appends the state $|\Upsilon\rangle^{\otimes c}$, namely, $V|\Xi\rangle = |\Xi\rangle|\Upsilon\rangle^{\otimes c}$, and id is the identity map on a single qubit from $\mathcal{L}$ to $\mathcal{L}$. The "entanglement-assisted" setting described above simplifies the theory of quantum channels and makes quantum error correction easier in a way, which helps us to create many different kinds of quantum codes in quantum communication. For example, Hsieh et al. [30] utilized classical quasi-cyclic low-density parity-check (LDPC) codes to obtain some entanglement-assisted quantum LDPC codes with good performance. In [54], Wilde and Brun developed a

Manuscript received September 4, 2020; revised July 24, 2021; accepted September 22, 2021. Date of publication October 5, 2021; date of current version November 22, 2021.

The author is with the Yau Mathematical Sciences Center, Tsinghua University, Beijing 100084, China, and also with the Yanqi Lake Beijing Institute of Mathematical Sciences and Applications, Beijing 101408, China (e-mail: mengcaomath@126.com).

Communicated by M. Wilde, Associate Editor for Quantum Information Theory.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIT.2021.3117562.

Digital Object Identifier 10.1109/TIT.2021.3117562

useful theory of entanglement-assisted quantum convolutional coding by exploiting pre-shared entanglement and a convolutional coding structure. They showed that a Calderbank-Shor-Steane (CSS) entanglement-assisted quantum convolutional code can be constructed by two arbitrary classical binary convolutional codes. In [56], Wilde et al. revealed that entanglement assistance can simplify the theory of quantum turbo codes in several important manners and they also examined the effect on the performance of these codes with the help of entanglement assistance. For more information about EAQECCs, we refer the reader to [17]–[20], [22], [24], [31], [32], [37]–[39], [55], [57].

In [3], Brun et al. showed that EAQECCs can be linked with the related idea of catalytic quantum error correction in quantum communication. More concretely, one can imagine that Alice and Bob are allowed to send c qubits error-free through a noiseless quantum channel that serves as a catalyst and is returned at the end of the protocol, apart from a noisy quantum channel $\mathcal{N}$. Then, the encoding operation $\mathcal{E}$ and decoding operation $\mathcal{D}$ mentioned above will define an $[[n, k-c, d; c]]_C$ catalytic quantum error-correcting code (CQECC), where $\mathcal{D} \circ (\mathcal{N} \otimes \mathrm{id}^{\otimes c}) \circ \mathcal{E} = \mathrm{id}^{\otimes k-c} \otimes \mathrm{id}^{\otimes c}$.

In [53], Wilde and Brun proposed a useful method for constructing EAQECCs from binary classical linear codes. In 2019, Galindo, Hernando, Matsumoto and Ruano [19] extended the binary case to the general one and obtained many important results on EAQECCs over arbitrary finite fields. By these results, an $[n, k, d]_q$ linear code with parity check matrix H produces an $[[n, 2k-n+c, d; c]]_q$ EAQECC with $c = \mathrm{rank}(HH^T)$. Denote by $Hull_E(\mathcal{C}) = \mathcal{C} \bigcap \mathcal{C}^{\perp_E}$ (resp. $Hull_H(\mathcal{C}) = \mathcal{C} \bigcap \mathcal{C}^{\perp_H}$) the Euclidean hull (resp. Hermitian hull) of a classical linear code $\mathcal{C}$, where $\mathcal{C}^{\perp_E}$ (resp. $\mathcal{C}^{\perp_H}$) is the Euclidean dual (resp. Hermitian dual) code of $\mathcal{C}$. Guenda et al. [29] proved that the parameter c of an $[[n, 2k-n+c, d; c]]_q$ EAQECC is related to the dimension of the Euclidean hull (or Hermitian hull) of an $[n, k, d]_q$ linear code. Based on these facts, Luo et al. [46] constructed several families of MDS codes with Euclidean hulls of arbitrary dimensions and obtained the corresponding EAQECCs with flexible parameters. Soon after, Fang et al. [16] presented several families of MDS codes with Euclidean hulls and Hermitian hulls of arbitrary dimensions, and then they also supplied the corresponding EAQECCs with flexible parameters. Note that the ℓ-Galois dual code $\mathcal{C}^{\perp_\ell}$ introduced by Fan and Zhang [14] generalizes both the Euclidean dual code $\mathcal{C}^{\perp_E}$ and the Hermitian dual code $\mathcal{C}^{\perp_H}$. Consequently, the ℓ-Galois hull of $\mathcal{C}$, denoted by $Hull_\ell(\mathcal{C}) = \mathcal{C} \bigcap \mathcal{C}^{\perp_\ell}$, is a generalization of the Euclidean hull and Hermitian hull of $\mathcal{C}$. Naturally, we may wonder how to construct MDS codes with ℓ-Galois hulls of arbitrary dimensions. Once such MDS codes are constructed, some new families of EAQECCs may be obtained subsequently.

In this paper, our goal is to construct q-ary MDS codes with ℓ-Galois hulls of arbitrary dimensions and obtain new $[[n, k, d; c]]_q$ EAQECCs with relatively large minimum distance in the sense that $2d = n-k+2+c$. Compared with [16] and [46], the research scope is extended from the Euclidean hulls and Hermitian hulls to the ℓ-Galois hulls. To achieve this goal, we first provide a necessary and sufficient condition under which a codeword of a GRS code or an extended GRS code belongs to its ℓ-Galois dual code (see Propositions II.1 and II.2), which generalizes both the Euclidean case in [9] and the Hermitian case in [15]. By utilizing this condition, we then construct eleven families of MDS codes with ℓ-Galois hulls of arbitrary dimensions by means of: (i) the norm mapping from $\mathbb{F}_q^*$ to $\mathbb{F}_{p^\ell}^*$ (see Theorems III.1-III.3); (ii) the direct product of two cyclic subgroups (see Theorems III.4-III.6); (iii) the coset decomposition of a cyclic group (see Theorems III.7-III.9); and (iv) an additive subgroup of $\mathbb{F}_q$ and its cosets (see Theorems III.10 and III.11). Using these MDS codes, we give eleven families of EAQECCs with relatively large minimum distance as follows.

Let $q = p^e$ with p being an odd prime number and let ℓ be an integer with $0 \le \ell \le e-1$. Let x_1 and x_2 be two positive integers. Then, there exists an $[[n, k-h, n-k+1; n-k-h]]_q$ EAQECC with relatively large minimum distance if one of the following eleven conditions holds:

(a) $n = \frac{t(q-1)}{p^\ell-1}$, $1 \le t \le p^\ell - 1$, $1 \le k \le \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$, $2\ell \mid e$ and $0 \le h \le k-1$ (see Theorem IV.1 (1));

(b) $n = \frac{t(q-1)}{p^\ell-1} + 1$, $1 \le t \le p^\ell - 1$, $1 \le k \le \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$, $2\ell \mid e$ and $0 \le h \le k$ (see Theorem IV.1 (2));

(c) $n = \frac{t(q-1)}{p^\ell-1} + 2$, $1 \le t \le p^\ell - 1$, $1 \le k \le \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$, $2\ell \mid e$ and $0 \le h \le k-1$ (see Theorem IV.1 (3));

(d) $n = \frac{r(q-1)}{\gcd(x_2, q-1)}$, $\frac{q-1}{p^\ell-1} \mid x_1$, $(q-1) \mid \mathrm{lcm}(x_1, x_2)$, $1 \le r \le \frac{q-1}{\gcd(x_1, q-1)}$, $1 \le k \le \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$, $2\ell \mid e$ and $0 \le h \le k-1$ (see Theorem IV.2 (1));

(e) $n = \frac{r(q-1)}{\gcd(x_2, q-1)} + 1$, $\frac{q-1}{p^\ell-1} \mid x_1$, $(q-1) \mid \mathrm{lcm}(x_1, x_2)$, $1 \le r \le \frac{q-1}{\gcd(x_1, q-1)}$, $1 \le k \le \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$, $2\ell \mid e$ and $0 \le h \le k$ (see Theorem IV.2 (2));

(f) $n = \frac{r(q-1)}{\gcd(x_2, q-1)} + 2$, $\frac{q-1}{p^\ell-1} \mid x_1$, $(q-1) \mid \mathrm{lcm}(x_1, x_2)$, $1 \le r \le \frac{q-1}{\gcd(x_1, q-1)}$, $1 \le k \le \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$, $2\ell \mid e$ and $0 \le h \le k-1$ (see Theorem IV.2 (3));

(g) $n = rm$, $m \mid (q-1)$, $1 \le r \le \frac{p^\ell-1}{m_1}$, $m_1 = \frac{m}{\gcd(m,y)}$, $y = \frac{q-1}{p^\ell-1}$, $1 \le k \le \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$, $2\ell \mid e$ and $0 \le h \le k-1$ (see Theorem IV.3 (1));

(h) $n = rm+1$, $m \mid (q-1)$, $1 \le r \le \frac{p^\ell-1}{m_1}$, $m_1 = \frac{m}{\gcd(m,y)}$, $y = \frac{q-1}{p^\ell-1}$, $1 \le k \le \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$, $2\ell \mid e$ and $0 \le h \le k$ (see Theorem IV.3 (2));

(i) $n = rm+2$, $m \mid (q-1)$, $1 \le r \le \frac{p^\ell-1}{m_1}$, $m_1 = \frac{m}{\gcd(m,y)}$, $y = \frac{q-1}{p^\ell-1}$, $1 \le k \le \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$, $2\ell \mid e$ and $0 \le h \le k-1$ (see Theorem IV.3 (3));

(j) $n = tp^{aw}$, $1 \le t \le p^a$, $1 \le w \le \frac{e}{a} - 1$, $1 \le k \le \lfloor \frac{p^\ell+n-1}{p^\ell+1} \rfloor$, $a \mid \ell$, $2\ell \mid e$ and $0 \le h \le k$ (see Theorem IV.4 (1));

(k) $n = tp^{aw} + 1$, $1 \le t \le p^a$, $1 \le w \le \frac{e}{a} - 1$, $1 \le k \le \lfloor \frac{p^\ell+n-1}{p^\ell+1} \rfloor$, $a \mid \ell$, $2\ell \mid e$ and $0 \le h \le k-1$ (see Theorem IV.4 (2)).

For each theorem of Theorems IV.1-IV.4, we show that the variables ℓ with $2\ell \mid e$ correspond to different kinds of EAQECCs in the sense that they have different kinds of length sets, by providing some examples and several tables for $\ell = 1, 2, 3$ (see Tables V and VIII) and $\ell = 1, 2$

(see Tables VI and VII). This is an important advantage of developing the theory on ℓ-Galois hulls of MDS codes in this paper. We also show that some lengths coming from the set of length n in Theorem IV.1 cannot be obtained by the set of length n in Theorem IV.2, and vice versa, by providing a table (see Table IX) for $p = 3$, $e = 8$ and $\ell = 2$.

The remainder of this paper is organized as follows. In Sect. II, we recall and give some results about ℓ-Galois dual codes, GRS codes and extended GRS codes. In Sect. III, we construct eleven families of q-ary MDS codes with ℓ-Galois hulls of arbitrary dimensions. In Sect. IV, by applying these MDS codes constructed in Sect. III we obtain eleven families of $[[n, k, d; c]]_q$ EAQECCs with relatively large minimum distance in the sense that $2d = n - k + 2 + c$. Sect. V makes a detailed discussion on the lengths of our EAQECCs for different variables ℓ. Finally, Sect. VI gives a summary of this paper and offers two open problems.

II. Preliminaries

Throughout this paper, we always assume that $q = p^e$ is a prime power, where p is a prime number and e is a positive integer. Denote $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$, where $\mathbb{F}_q$ is the finite field with q elements. For any finite set S, we denote by $|S|$ its *cardinality*, namely, the number of all the elements in S.

As usual, we denote by $[n, k, d]_q$ a classical linear code over $\mathbb{F}_q$ with length n, dimension k and minimum distance d. The minimum distance d of a linear code must satisfy the well-known Singleton bound $d \leq n + 1 - k$. If the minimum distance achieves the bound, i.e., $d = n + 1 - k$, then such a linear code is called a *maximum distance separable (MDS) code*.

We need to recall the following important concepts introduced by Fan and Zhang [14].

Definition II.1 ([14]): (1) Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n$. For each integer ℓ with $0 \leq \ell \leq e - 1$, the inner product

$$(\mathbf{x}, \mathbf{y})_\ell = \sum_{i=1}^{n} x_i y_i^{p^\ell}$$

is called the *ℓ-Galois inner product* (i.e., p^ℓ-inner product) of $\mathbf{x}$ and $\mathbf{y}$.

(2) Let $\mathcal{C}$ be a linear code with length n over $\mathbb{F}_q$. For each integer ℓ with $0 \leq \ell \leq e - 1$, the code

$$\mathcal{C}^{\perp_\ell} = \{\mathbf{x} \in \mathbb{F}_q^n | (\mathbf{y}, \mathbf{x})_\ell = 0 \text{ for each } \mathbf{y} \in \mathcal{C}\}$$

is called the *ℓ-Galois dual code* (i.e., p^ℓ-dual code) of $\mathcal{C}$.

In particular, in the above definition,

- If $\ell = 0$, then $(\mathbf{x}, \mathbf{y})_0$ is just the Euclidean inner product of $\mathbf{x}$ and $\mathbf{y}$. Besides, $\mathcal{C}^{\perp_0}$ is the Euclidean dual code of $\mathcal{C}$.
- If e is even and $\ell = \frac{e}{2}$, then $(\mathbf{x}, \mathbf{y})_{\frac{e}{2}}$ is just the Hermitian inner product of $\mathbf{x}$ and $\mathbf{y}$. Besides, $\mathcal{C}^{\perp_{\frac{e}{2}}}$ is the Hermitian dual code of $\mathcal{C}$.

As usual, we use the notations $\mathcal{C}^{\perp_E}$ and $\mathcal{C}^{\perp_H}$ to denote $\mathcal{C}^{\perp_0}$ and $\mathcal{C}^{\perp_{\frac{e}{2}}}$ (if e is even), respectively. Further, for each integer ℓ with $0 \leq \ell \leq e - 1$, we call $Hull_\ell(\mathcal{C}) := \mathcal{C} \bigcap \mathcal{C}^{\perp_\ell}$ the *ℓ-Galois hull* of $\mathcal{C}$. Naturally, the concept of the ℓ-Galois hull is a generalization of the Euclidean hull and Hermitian hull.

For a vector $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_q^n$, we define $\mathbf{v}^a = (v_1^a, v_2^a, \ldots, v_n^a)$ for any integer a. Let M be a subset of $\mathbb{F}_q^n$, then M^a is defined as the set $\{\mathbf{v}^a | \mathbf{v} \in M\}$.

The following useful lemma given by Liu et al. characterizes the ℓ-Galois dual code of a linear code.

Lemma II.1 ([41]): For an $[n, k, d]_q$ linear code $\mathcal{C}$, we have $\mathcal{C}^{\perp_\ell} = (\mathcal{C}^{p^{e-\ell}})^{\perp_E}$ for $0 \leq \ell \leq e - 1$.

Now let us recall and study the generalized Reed-Solomon (GRS) codes and the extended GRS codes. Take $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ with $a_1, a_2, \ldots, a_n$ being distinct elements in $\mathbb{F}_q$, and put $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ with $v_1, v_2, \ldots, v_n \in \mathbb{F}_q^*$. Suppose $k \leq n \leq q$, then the k-dimensional GRS code with respect to $\mathbf{a}$ and $\mathbf{v}$ is defined as

$$GRS_k(\mathbf{a}, \mathbf{v}) = \{(v_1 f(a_1), v_2 f(a_2), \ldots, v_n f(a_n)) | f(x) \in \mathbb{F}_q[x], \deg(f(x)) \leq k - 1\}.$$

It is an $[n, k, n-k+1]_q$ MDS code whose generator matrix is

$$G_k(\mathbf{a}, \mathbf{v}) = \begin{bmatrix} v_1 & v_2 & \cdots & v_n \\ v_1 a_1 & v_2 a_2 & \cdots & v_n a_n \\ \vdots & \vdots & \ddots & \vdots \\ v_1 a_1^{k-1} & v_2 a_2^{k-1} & \cdots & v_n a_n^{k-1} \end{bmatrix}. \quad (1)$$

Moreover, the k-dimensional extended GRS code with respect to $\mathbf{a}$ and $\mathbf{v}$ is defined as

$$GRS_k(\mathbf{a}, \mathbf{v}, \infty) = \{(v_1 f(a_1), \ldots, v_n f(a_n), f_{k-1}) | f(x) \in \mathbb{F}_q[x], \deg(f(x)) \leq k - 1\},$$

where f_{k-1} denotes the coefficient of x^{k-1} in $f(x)$. It is not difficult to verify that $GRS_k(\mathbf{a}, \mathbf{v}, \infty)$ is an $[n+1, k, n-k+2]_q$ MDS code whose generator matrix is

$$G_k(\mathbf{a}, \mathbf{v}, \infty) = \begin{bmatrix} v_1 & v_2 & \cdots & v_n & 0 \\ v_1 a_1 & v_2 a_2 & \cdots & v_n a_n & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ v_1 a_1^{k-2} & v_2 a_2^{k-2} & \cdots & v_n a_n^{k-2} & 0 \\ v_1 a_1^{k-1} & v_2 a_2^{k-1} & \cdots & v_n a_n^{k-1} & 1 \end{bmatrix}. \quad (2)$$

From now on, for each $i = 1, 2, \ldots, n$, we shall denote by

$$u_i = \prod_{1 \leq j \leq n, j \neq i} (a_i - a_j)^{-1}. \quad (3)$$

Let $\mathbf{1} = (1, 1, \ldots, 1)$ be the all one vector. By the above basics, the Euclidean dual codes $GRS_k(\mathbf{a}, \mathbf{1})^{\perp_E}$ and $GRS_k(\mathbf{a}, \mathbf{1}, \infty)^{\perp_E}$ can be expressed as follows.

Lemma II.2 ([34]): Let $\mathbf{u} = (u_1, u_2, \ldots, u_n)$, where each u_i is defined by Eq. (3). Then,

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

Lemma II.3 ([15]):

$$GRS_k(\mathbf{a}, \mathbf{1}, \infty)^{\perp_E} = \{(u_1 g(a_1), \ldots, u_n g(a_n), -g_{n-k}) | g(x) \in \mathbb{F}_q[x], \deg(g(x)) \leq n - k\},$$

where g_{n-k} denotes the coefficient of x^{n-k} in $g(x)$.

Based on Lemma II.2, the following proposition provides a necessary and sufficient condition under which a codeword $\mathbf{c}$ of $GRS_k(\mathbf{a},\mathbf{v})$ belongs to $GRS_k(\mathbf{a},\mathbf{v})^{\perp_\ell}$.

Proposition II.1: For $\mathbf{c} = (v_1 f(a_1), v_2 f(a_2), \ldots, v_n f(a_n)) \in GRS_k(\mathbf{a},\mathbf{v})$, we have $\mathbf{c} \in GRS_k(\mathbf{a},\mathbf{v})^{\perp_\ell}$ if and only if there exists a polynomial $g(x) \in \mathbb{F}_q[x]$ with $\deg(g(x)) \le n-k-1$ such that

$$\begin{aligned}(v_1^{p^\ell+1} f^{p^\ell}(a_1), v_2^{p^\ell+1} f^{p^\ell}(a_2), \ldots, v_n^{p^\ell+1} f^{p^\ell}(a_n)) \\ = (u_1 g(a_1), u_2 g(a_2), \ldots, u_n g(a_n)).\end{aligned} \tag{4}$$

Proof: By Eq. (1), we know that

$$G_k(\mathbf{a},\mathbf{v}) = G_k(\mathbf{a},\mathbf{1})D,$$

where $D = \mathrm{diag}(v_1, v_2, \ldots, v_n)$. Then, by Lemmas II.1 and II.2, we have that

$$\begin{aligned}\mathbf{c} \in GRS_k(\mathbf{a},\mathbf{v})^{\perp_\ell} &\Leftrightarrow \mathbf{c} \in (GRS_k(\mathbf{a},\mathbf{v})^{\perp_E})^{p^{e-\ell}} \\ &\Leftrightarrow \mathbf{c}^{p^\ell} \in GRS_k(\mathbf{a},\mathbf{v})^{\perp_E} \\ &\Leftrightarrow G_k(\mathbf{a},\mathbf{v})(\mathbf{c}^{p^\ell})^T = 0 \\ &\Leftrightarrow G_k(\mathbf{a},\mathbf{1})D(\mathbf{c}^{p^\ell})^T = 0 \\ &\Leftrightarrow \mathbf{c}^{p^\ell} D \in GRS_k(\mathbf{a},\mathbf{1})^{\perp_E} \\ &\Leftrightarrow \mathbf{c}^{p^\ell} D \in GRS_{n-k}(\mathbf{a},\mathbf{u}).\end{aligned}$$

Thus, the proof is completed. ∎

Remark II.1: Proposition II.1 generalizes both the Euclidean case (i.e., $\ell = 0$) in [9, Lemma 2] and the Hermitian case (i.e., $\ell = \frac{e}{2}$ for even e) in [15, Lemma 6].

For the extended GRS code $GRS_k(\mathbf{a},\mathbf{v},\infty)$, we give the following proposition by using Lemma II.3.

Proposition II.2: For $\mathbf{c} = (v_1 f(a_1), v_2 f(a_2), \ldots, v_n f(a_n), f_{k-1}) \in GRS_k(\mathbf{a},\mathbf{v},\infty)$, we have $\mathbf{c} \in GRS_k(\mathbf{a},\mathbf{v},\infty)^{\perp_\ell}$ if and only if there exists a polynomial $g(x) \in \mathbb{F}_q[x]$ with $\deg(g(x)) \le n-k$ such that

$$\begin{aligned}(v_1^{p^\ell+1} f^{p^\ell}(a_1), \ldots, v_n^{p^\ell+1} f^{p^\ell}(a_n), f_{k-1}^{p^\ell}) \\ = (u_1 g(a_1), \ldots, u_n g(a_n), -g_{n-k}).\end{aligned} \tag{5}$$

Proof: According to Eq. (2), we have that

$$G_k(\mathbf{a},\mathbf{v},\infty) = G_k(\mathbf{a},\mathbf{1},\infty)\widetilde{D},$$

where $\widetilde{D} = \mathrm{diag}(v_1, \ldots, v_n, 1)$. Then, by Lemma II.1, we have that

$$\begin{aligned}\mathbf{c} \in GRS_k(\mathbf{a},\mathbf{v},\infty)^{\perp_\ell} &\Leftrightarrow \mathbf{c} \in (GRS_k(\mathbf{a},\mathbf{v},\infty)^{\perp_E})^{p^{e-\ell}} \\ &\Leftrightarrow \mathbf{c}^{p^\ell} \in GRS_k(\mathbf{a},\mathbf{v},\infty)^{\perp_E} \\ &\Leftrightarrow G_k(\mathbf{a},\mathbf{v},\infty)(\mathbf{c}^{p^\ell})^T = 0 \\ &\Leftrightarrow G_k(\mathbf{a},\mathbf{1},\infty)\widetilde{D}(\mathbf{c}^{p^\ell})^T = 0 \\ &\Leftrightarrow \mathbf{c}^{p^\ell}\widetilde{D} \in GRS_k(\mathbf{a},\mathbf{1},\infty)^{\perp_E}.\end{aligned}$$

Applying Lemma II.3, we finish the proof. ∎

Remark II.2: Proposition II.2 generalizes both the Euclidean case (i.e., $\ell = 0$) in [9, Lemma 3] and the Hermitian case (i.e., $\ell = \frac{e}{2}$ for even e) in [15, Lemma 7].

Propositions II.1 and II.2 provide us with an effective method for deriving the expression of the polynomial $f(x)$. By virtue of them, in the next section, we can determine the dimensions of the ℓ-Galois hulls of some GRS codes and extended GRS codes in a convenient way.

III. Constructions of MDS Codes With ℓ-Galois Hulls of Arbitrary Dimensions

In this section, we will construct several families of MDS codes with ℓ-Galois hulls of arbitrary dimensions. The phrase 'arbitrary dimensions' appeared previously in [16] and [46] when describing the MDS codes with Euclidean hulls and Hermitian hulls therein. Here, it represents that the ℓ-Galois hulls of our MDS codes can take all or almost all possible dimensions. More precisely, the dimensions of the ℓ-Galois hulls in this section run through the integers from 0 to k, or $k-1$ (in fact, $0 \le \dim(Hull_\ell(\mathcal{C})) \le k$), where k is the dimension of the MDS code $\mathcal{C}$.

As can be seen in Propositions II.1 and II.2, an important point of our constructions is to take n suitable distinct elements $a_1, a_2, \ldots, a_n$ as the coordinates of the vector $\mathbf{a}$ in $GRS_k(\mathbf{a},\mathbf{v})$ or $GRS_k(\mathbf{a},\mathbf{v},\infty)$. Further, for the convenience of calculating the values of $u_1, u_2, \ldots, u_n$ (see Eq. (3)), we find several kinds of suitable elements $a_1, a_2, \ldots, a_n$ related to (i) the norm mapping from $\mathbb{F}_q^*$ to $\mathbb{F}_{p^\ell}^*$ (see Theorems III.1-III.3); (ii) the direct product of two cyclic subgroups (see Theorems III.4-III.6); (iii) the coset decomposition of a cyclic group (see Theorems III.7-III.9); and (iv) an additive subgroup of $\mathbb{F}_q$ and its cosets (see Theorems III.10 and III.11). By utilizing these tools, we present eleven families of MDS codes with ℓ-Galois hulls of arbitrary dimensions in the following four subsections.

A. MDS Codes Related to the Norm Mapping From $\mathbb{F}_q^*$ to $\mathbb{F}_{p^\ell}^*$

Let $q = p^e$ with p being a prime number, $0 \le \ell \le e-1$. Assume that $\ell \mid e$. Consider the following surjective homomorphism called the *norm mapping*:

$$\begin{aligned}\mathrm{Norm} : \mathbb{F}_q^* &\to \mathbb{F}_{p^\ell}^* \\ x &\mapsto \prod_{i=0}^{\frac{e}{\ell}-1} x^{p^{i\ell}} = x^{\frac{q-1}{p^\ell-1}}.\end{aligned}$$

Denote by $\mathbb{F}_{p^\ell}^* = \{b_1, b_2, \ldots, b_{p^\ell-1}\}$. For each $b_i \in \mathbb{F}_{p^\ell}^*$, $i = 1, 2, \ldots, p^\ell - 1$, define

$$N_i = \{x \in \mathbb{F}_q^* |\ \mathrm{Norm}(x) = b_i\}.$$

Then $N_i = \beta_i \mathrm{Ker}(\mathrm{Norm})$, where $\mathrm{Norm}(\beta_i) = b_i$ holds for some $\beta_i \in \mathbb{F}_q^*$ since Norm is surjective, and $\mathrm{Ker}(\mathrm{Norm}) = \{x \in \mathbb{F}_q^* |\ \mathrm{Norm}(x) = 1\}$ is the kernel of Norm. This yields that $|N_i| = \big|\mathrm{Ker}(\mathrm{Norm})\big|$. On the one hand, by the fundamental homomorphism theorem, we have that

$$\mathbb{F}_q^*/\mathrm{Ker}(\mathrm{Norm}) \cong \mathrm{Im}(\mathrm{Norm}) \le \mathbb{F}_{p^\ell}^*,$$

where $\mathrm{Im}(\mathrm{Norm})$ is the image of Norm. Then, we have $\big|\mathbb{F}_q^*/\mathrm{Ker}(\mathrm{Norm})\big| \le p^\ell - 1$. On the other hand, since $\big|\mathrm{Ker}(\mathrm{Norm})\big| \le \frac{q-1}{p^\ell-1}$, we know that $\big|\mathbb{F}_q^*/\mathrm{Ker}(\mathrm{Norm})\big| \ge p^\ell - 1$. Hence, $\big|\mathbb{F}_q^*/\mathrm{Ker}(\mathrm{Norm})\big| = p^\ell - 1$, i.e., $\big|\mathrm{Ker}(\mathrm{Norm})\big| = \frac{q-1}{p^\ell-1}$. Therefore, $|N_i| = \frac{q-1}{p^\ell-1}$.

Now, denote by

$$\mathcal{N} = \bigcup_{i=1}^{t} N_i = \{a_1, a_2, \ldots, a_n\}, \tag{6}$$

where $1 \le t \le p^\ell - 1$. Then, $n = \frac{t(q-1)}{p^\ell - 1}$ for $1 \le t \le p^\ell - 1$, and $N_i \cap N_j = \emptyset$ hold for all $i \ne j$. Therefore, we have the following lemma.

Lemma III.1: Let a_i and u_i be defined as in Eqs. (6) and (3), respectively. Assume that $\ell \mid e$. Then, $a_i^{-1}u_i \in \mathbb{F}_{p^\ell}^*$ holds for each $i = 1, 2, \ldots, n$.

Proof: For any $a_i \in \mathcal{N}$, $i = 1, 2, \ldots, n$, we may assume $a_i \in N_s$ for some $1 \le s \le t$. Then $\mathrm{Norm}(a_i) = b_s = a_i^{\frac{q-1}{p^\ell - 1}}$. By Eq. (3), we see that

$$u_i = \prod_{c_j \in N_s, c_j \ne a_i} (a_i - c_j)^{-1} \cdot \prod_{1 \le s' \le t, s' \ne s} \prod_{d_{j'} \in N_{s'}} (a_i - d_{j'})^{-1}. \tag{7}$$

Let $u(x) = \prod_{c_j \in N_s}(x - c_j)$, then $u(x) = \mathrm{Norm}(x) - b_s = x^{\frac{q-1}{p^\ell - 1}} - b_s$. Since $a_i \in N_s$, then

$$\prod_{c_j \in N_s, c_j \ne a_i} (a_i - c_j) = u'(a_i) = \frac{q-1}{p^\ell - 1} a_i^{\frac{q-1}{p^\ell - 1} - 1}.$$

Noticing that $\frac{q-1}{p^\ell - 1} \equiv 1 \mod p$, we obtain

$$\prod_{c_j \in N_s, c_j \ne a_i} (a_i - c_j)^{-1} = a_i^{1 - \frac{q-1}{p^\ell - 1}}.$$

Hence,

$$a_i^{-1} \prod_{c_j \in N_s, c_j \ne a_i} (a_i - c_j)^{-1} = a_i^{-\frac{q-1}{p^\ell - 1}} \in \mathbb{F}_{p^\ell}^*. \tag{8}$$

By $\prod_{d_{j'} \in N_{s'}}(x - d_{j'}) = \mathrm{Norm}(x) - b_{s'}$, we have that

$$\begin{aligned} &\prod_{1 \le s' \le t, s' \ne s} \prod_{d_{j'} \in N_{s'}} (a_i - d_{j'})^{-1} \\ &= \prod_{1 \le s' \le t, s' \ne s} \left(\mathrm{Norm}(a_i) - b_{s'}\right)^{-1} \\ &= \prod_{1 \le s' \le t, s' \ne s} (b_s - b_{s'})^{-1} \in \mathbb{F}_{p^\ell}^*. \end{aligned} \tag{9}$$

It follows from Eqs. (7)-(9) that $a_i^{-1}u_i \in \mathbb{F}_{p^\ell}^*$. Therefore, the proof is completed. ∎

As shown in Lemma III.1, $a_i^{-1}u_i \in \mathbb{F}_{p^\ell}^*$ holds under some suitable conditions. Now, for any $u \in \mathbb{F}_{p^\ell}^*$, observing Eq. (4) in Proposition II.1 and Eq. (5) in Proposition II.2, we wonder if there exists $v \in \mathbb{F}_q^*$ such that $v^{p^\ell + 1} = u$. If such a relation exists, then it will help us to explore the structure of the polynomial $f(x)$ in Propositions II.1 and II.2, which makes it easy to determine the dimensions of the ℓ-Galois hulls of some GRS codes and extended GRS codes.

In the following lemma, we give a necessary and sufficient condition under which the relation $v^{p^\ell + 1} = u$ holds.

Lemma III.2: Let $q = p^e$ with p being an odd prime number and let $0 \le \ell \le e - 1$. Then, for any $u \in \mathbb{F}_{p^\ell}^*$, there exists $v \in \mathbb{F}_q^*$ such that $v^{p^\ell + 1} = u$ if and only if $2\ell \mid e$.

Proof: First of all, as $\mathbb{F}_{p^\ell}$ is required to be a subfield of $\mathbb{F}_q$, we immediately obtain $\ell \mid e$. Let $e = \ell\ell'$ for some integer ℓ'. Assume $\mathbb{F}_q^* = \langle \varepsilon \rangle$, then $\mathrm{ord}(\varepsilon^{p^\ell + 1}) = \frac{q-1}{\gcd(q-1, p^\ell + 1)}$. Denote by

$$H := \{x^{p^\ell + 1} | x \in \mathbb{F}_q^*\},$$

then H is a subgroup of $\mathbb{F}_q^*$ with $\mathrm{ord}(H) = \frac{q-1}{\gcd(q-1, p^\ell + 1)}$. Besides, $\mathbb{F}_{p^\ell}^*$ is a subgroup of $\mathbb{F}_q^*$ with $\mathrm{ord}(\mathbb{F}_{p^\ell}^*) = p^\ell - 1$. Therefore, we have that

$$\begin{aligned} \mathbb{F}_{p^\ell}^* \subseteq H &\Leftrightarrow (p^\ell - 1) \,\Big|\, \frac{q-1}{\gcd(q-1, p^\ell + 1)} \\ &\Leftrightarrow (p^\ell - 1) \cdot \gcd(q-1, p^\ell + 1) \mid (q-1). \end{aligned}$$

Note that

$$\begin{aligned} \gcd(q-1, p^\ell + 1) &= \gcd(((p^\ell + 1) - 1)^{\ell'} - 1, p^\ell + 1) \\ &= \gcd((-1)^{\ell'} - 1, p^\ell + 1) \\ &= \begin{cases} 2, & \text{if } \ell' \text{ is odd;} \\ p^\ell + 1, & \text{if } \ell' \text{ is even.} \end{cases} \end{aligned}$$

Case (i): If ℓ' is odd, then $(p^\ell - 1) \cdot \gcd(q-1, p^\ell + 1) = 2(p^\ell - 1)$. Besides, we know that $q - 1 = p^{\ell\ell'} - 1 = (p^\ell - 1)\sum_{i=0}^{\ell'-1} p^{\ell i}$. Observing that $\sum_{i=0}^{\ell'-1} p^{\ell i}$ is odd, we obtain that

$$(p^\ell - 1) \cdot \gcd(q-1, p^\ell + 1) \nmid (q-1).$$

Case (ii): If ℓ' is even, assume $\ell' = 2\ell''$ for some integer ℓ''. Then $q - 1 = p^{\ell\ell'} - 1 = p^{2\ell\ell''} - 1$. Combining this with the fact $(p^\ell - 1) \cdot \gcd(q-1, p^\ell + 1) = p^{2\ell} - 1$, we obtain that

$$(p^\ell - 1) \cdot \gcd(q-1, p^\ell + 1) \mid (q-1).$$

Thus, we conclude that $\mathbb{F}_{p^\ell}^* \subseteq H \Leftrightarrow 2\ell \mid e$, which completes the proof. ∎

By using the previous lemmas, we give the following $[n, k]_q$ MDS codes with ℓ-Galois hulls of arbitrary dimensions.

Theorem III.1: Let $q = p^e$ with p being an odd prime number. Assume $2\ell \mid e$. Let $n = \frac{t(q-1)}{p^\ell - 1}$ for each $1 \le t \le p^\ell - 1$. Then, for any $1 \le k \le \lfloor \frac{p^\ell + n}{p^\ell + 1} \rfloor$ and $0 \le h \le k - 1$, there exists an $[n, k]_q$ MDS code with h-dimensional ℓ-Galois hull.

Proof: Let $a_1, a_2, \ldots, a_n$ be defined by Eq. (6). For each $1 \le i \le n$, by Lemma III.1, we have $a_i^{-1}u_i \in \mathbb{F}_{p^\ell}^*$. Further, in terms of Lemma III.2, there exists $v_i \in \mathbb{F}_q^*$ such that $v_i^{p^\ell + 1} = a_i^{-1}u_i$. Set $z := k - 1 - h$ and take $\beta \in \mathbb{F}_q^*$ such that $\gamma := \beta^{p^\ell + 1} \ne 1$. Put $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{v} = (\beta v_1, \ldots, \beta v_z, v_{z+1}, \ldots, v_n)$. Consider the ℓ-Galois hull of the $[n, k]_q$ MDS code $\mathcal{C} := GRS_k(\mathbf{a}, \mathbf{v})$. Then for any $\mathbf{c} = (\beta v_1 f(a_1), \ldots, \beta v_z f(a_z), v_{z+1} f(a_{z+1}), \ldots, v_n f(a_n)) \in Hull_\ell(\mathcal{C})$ with $\deg(f(x)) \le k-1$, in terms of Proposition II.1, there exists a polynomial $g(x) \in \mathbb{F}_q[x]$ with $\deg(g(x)) \le n - k - 1$ such that

$$\begin{aligned} &(\beta^{p^\ell + 1} v_1^{p^\ell + 1} f^{p^\ell}(a_1), \ldots, \beta^{p^\ell + 1} v_z^{p^\ell + 1} f^{p^\ell}(a_z), v_{z+1}^{p^\ell + 1} f^{p^\ell}(a_{z+1}), \\ &\qquad \ldots, v_n^{p^\ell + 1} f^{p^\ell}(a_n)) = (u_1 g(a_1), u_2 g(a_2), \ldots, u_n g(a_n)). \end{aligned}$$

That is,

$$(\gamma a_1^{-1}u_1 f^{p^\ell}(a_1),\ldots,\gamma a_z^{-1}u_z f^{p^\ell}(a_z), a_{z+1}^{-1}u_{z+1}f^{p^\ell}(a_{z+1}),\ldots,a_n^{-1}u_n f^{p^\ell}(a_n)) = (u_1 g(a_1), u_2 g(a_2),\ldots,u_n g(a_n)). \tag{10}$$

Comparing the last $n-z$ coordinates of Eq. (10), we have $a_i^{-1}u_i f^{p^\ell}(a_i) = u_i g(a_i)$, i.e., $f^{p^\ell}(a_i) = a_i g(a_i)$ for $i = z+1,\ldots,n$. Hence the number of the distinct roots of $f^{p^\ell}(x) - xg(x)$ is at least $n-z \geq n-k+1$. Since $k \leq \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$, we have $\deg(f^{p^\ell}(x)) \leq p^\ell(k-1) \leq n-k$, which, together with $\deg(xg(x)) \leq n-k$, derives that $\deg(f^{p^\ell}(x) - xg(x)) \leq n-k$. This implies that $f^{p^\ell}(x) = xg(x)$ and hence $x \mid f(x)$.

Observing the first z coordinates of Eq. (10), we know that

$$\gamma a_i^{-1}u_i f^{p^\ell}(a_i) = u_i g(a_i) = u_i a_i^{-1} f^{p^\ell}(a_i)$$

for $i = 1,\ldots,z$. Hence $f^{p^\ell}(a_i) = 0$, i.e., $f(a_i) = 0$ for $i = 1,\ldots,z$. Then we can express $f(x)$ as

$$f(x) = xc(x)\prod_{i=1}^{z}(x-a_i)$$

for some $c(x) \in \mathbb{F}_q[x]$ with $\deg(c(x)) \leq k-z-2$. Thus, $\dim(Hull_\ell(\mathcal{C})) \leq k-z-1$.

Conversely, let $f(x) = xc(x)\prod_{i=1}^{z}(x-a_i)$, where $c(x) \in \mathbb{F}_q[x]$ with $\deg(c(x)) \leq k-z-2$. Taking $g(x) = x^{-1}f^{p^\ell}(x)$, then $\deg(g(x)) \leq p^\ell(k-1)-1 \leq n-k-1$ and Eq. (10) holds. By Proposition II.1, we have $(\beta v_1 f(a_1),\ldots,\beta v_z f(a_z), v_{z+1}f(a_{z+1}),\ldots,v_n f(a_n)) \in Hull_\ell(\mathcal{C})$, which means that $\dim(Hull_\ell(\mathcal{C})) \geq k-z-1$.

Therefore, we obtain $\dim(Hull_\ell(\mathcal{C})) = k-z-1 = h$, which completes the proof. ∎

Next, based on Theorem III.1, we proceed to construct a family of MDS codes of length $n+1$ from GRS codes with ℓ-Galois hulls of arbitrary dimensions as follows.

Theorem III.2: Let $q = p^e$ with p being an odd prime number. Assume $2\ell \mid e$. Let $n = \frac{t(q-1)}{p^\ell-1}$ for each $1 \leq t \leq p^\ell - 1$. Then, for any $1 \leq k \leq \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$ and $0 \leq h \leq k$, there exists an $[n+1,k]_q$ MDS code with h-dimensional ℓ-Galois hull.

Proof: Let $a_1, a_2, \ldots, a_n$ be defined as in Eq. (6) and let $a_{n+1} = 0$. For each $1 \leq i \leq n$, in view of Lemma III.1, we have that

$$\prod_{1\leq j\leq n+1, j\neq i}(a_i-a_j)^{-1} = a_i^{-1}\prod_{1\leq j\leq n, j\neq i}(a_i-a_j)^{-1} \in \mathbb{F}_{p^\ell}^*.$$

For $i = n+1$, we know that

$$\prod_{j=1}^{n}(a_{n+1}-a_j)^{-1} = (-1)^n\Big[\prod_{i=1}^{t}\Big(\prod_{a_j\in N_i} a_j\Big)\Big]^{-1}. \tag{11}$$

Let us compute $\prod_{a_j\in N_i} a_j$. Denote by

$$N_i = \Big\{a_{i,1}, a_{i,2},\ldots,a_{i,\frac{q-1}{p^\ell-1}}\Big\},$$

then for each $a_j \in N_i$, i.e., for each $a_{i,r} \in N_i$, where $r = 1,2,\ldots,\frac{q-1}{p^\ell-1}$, we have $\mathrm{Norm}(a_{i,r}) = b_i = a_{i,r}^{\frac{q-1}{p^\ell-1}}$, and thus

$$x^{\frac{q-1}{p^\ell-1}} - b_i = (x-a_{i,1})(x-a_{i,2})\cdots\Big(x-a_{i,\frac{q-1}{p^\ell-1}}\Big),$$

which implies that $\prod_{r=1}^{\frac{q-1}{p^\ell-1}} a_{i,r} = (-1)^{\frac{p^\ell-q}{p^\ell-1}}b_i$. Substituting this into Eq. (11), we obtain that

$$\prod_{j=1}^{n}(a_{n+1}-a_j)^{-1} = (-1)^n\Big[\prod_{i=1}^{t}(-1)^{\frac{p^\ell-q}{p^\ell-1}}b_i\Big]^{-1} = (-1)^{n+\frac{t(q-p^\ell)}{p^\ell-1}}\prod_{i=1}^{t}b_i^{-1} \in \mathbb{F}_{p^\ell}^*.$$

Denote $w_i = \prod_{1\leq j\leq n+1, j\neq i}(a_i-a_j)^{-1}, i = 1,\ldots,n+1$. Then, from Lemma III.2, there exists $v_i \in \mathbb{F}_q^*$ such that $v_i^{p^\ell+1} = w_i$ for $i = 1,\ldots,n+1$. Set $z := k-h$ and take $\beta \in \mathbb{F}_q^*$ such that $\gamma := \beta^{p^\ell+1} \neq 1$. Put $\mathbf{a} = (a_1, a_2, \ldots, a_{n+1})$ and $\mathbf{v} = (\beta v_1,\ldots,\beta v_z, v_{z+1},\ldots,v_{n+1})$. Consider the ℓ-Galois hull of the $[n+1,k]_q$ MDS code $\mathcal{C} := GRS_k(\mathbf{a},\mathbf{v})$. Then for any $\mathbf{c} = (\beta v_1 f(a_1),\ldots,\beta v_z f(a_z), v_{z+1}f(a_{z+1}),\ldots,v_{n+1}f(a_{n+1})) \in Hull_\ell(\mathcal{C})$ with $\deg(f(x)) \leq k-1$, by Proposition II.1, there exists a polynomial $g(x) \in \mathbb{F}_q[x]$ with $\deg(g(x)) \leq n-k$ such that

$$(\beta^{p^\ell+1}v_1^{p^\ell+1}f^{p^\ell}(a_1),\ldots,\beta^{p^\ell+1}v_z^{p^\ell+1}f^{p^\ell}(a_z), v_{z+1}^{p^\ell+1}f^{p^\ell}(a_{z+1}), \ldots, v_{n+1}^{p^\ell+1}f^{p^\ell}(a_{n+1})) = (w_1 g(a_1), w_2 g(a_2),\ldots,w_{n+1}g(a_{n+1})).$$

That is,

$$(\gamma w_1 f^{p^\ell}(a_1),\ldots,\gamma w_z f^{p^\ell}(a_z), w_{z+1}f^{p^\ell}(a_{z+1}),\ldots,w_{n+1}f^{p^\ell}(a_{n+1})) = (w_1 g(a_1), w_2 g(a_2),\ldots,w_{n+1}g(a_{n+1})). \tag{12}$$

From the last $n-z+1$ coordinates of Eq. (12), we have $w_i f^{p^\ell}(a_i) = w_i g(a_i)$, i.e., $f^{p^\ell}(a_i) = g(a_i)$ for $i = z+1,\ldots,n+1$. Hence the number of the distinct roots of $f^{p^\ell}(x) - g(x)$ is at least $n-z+1 \geq n-k+1$. Since $k \leq \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$, we have $\deg(f^{p^\ell}(x)) \leq p^\ell(k-1) \leq n-k$, which, together with $\deg(g(x)) \leq n-k$, derives that $\deg(f^{p^\ell}(x) - g(x)) \leq n-k$. Hence $f^{p^\ell}(x) = g(x)$.

Observing the first z coordinates of Eq. (12), we have that

$$\gamma w_i f^{p^\ell}(a_i) = w_i g(a_i) = w_i f^{p^\ell}(a_i)$$

for $i = 1,\ldots,z$. Hence $f^{p^\ell}(a_i) = 0$, i.e., $f(a_i) = 0$ for $i = 1,\ldots,z$. Then we can write $f(x)$ as

$$f(x) = c(x)\prod_{i=1}^{z}(x-a_i)$$

for some $c(x) \in \mathbb{F}_q[x]$ with $\deg(c(x)) \leq k-z-1$. Thus $\dim(Hull_\ell(\mathcal{C})) \leq k-z$.

Conversely, similar to the proof of Theorem III.1, we have $\dim(Hull_\ell(\mathcal{C})) \geq k-z$.

Therefore, $\dim(Hull_\ell(\mathcal{C})) = k-z = h$, which completes the proof. ∎

Now, if we consider the extended GRS code $GRS_k(\mathbf{a},\mathbf{v},\infty)$ of length $n+2$ with $\mathbf{a}$ and $\mathbf{v}$ being defined as in the proof of Theorem III.2, then a new family of MDS codes with ℓ-Galois hulls of arbitrary dimensions can be yielded as follows.

Theorem III.3: Let $q = p^e$ with p being an odd prime number. Assume $2\ell \mid e$. Let $n = \frac{t(q-1)}{p^\ell-1}$ for each $1 \leq t \leq$

$p^\ell-1$. Then, for any $1 \le k \le \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$ and $0 \le h \le k-1$, there exists an $[n+2,k]_q$ MDS code with h-dimensional ℓ-Galois hull.

Proof: Set $z := k-1-h$ and take $\beta \in \mathbb{F}_q^*$ such that $\gamma := \beta^{p^\ell+1} \neq 1$. Let $\mathbf{a} = (a_1, a_2, \ldots, a_{n+1})$, $\mathbf{v} = (\beta v_1, \ldots, \beta v_z, v_{z+1}, \ldots, v_{n+1})$ and w_i be defined as in the proof of Theorem III.2. We can consider the ℓ-Galois hull of the $[n+2,k]_q$ MDS code $\mathcal{C} := GRS_k(\mathbf{a}, \mathbf{v}, \infty)$. Then for any $\mathbf{c} = (\beta v_1 f(a_1), \ldots, \beta v_z f(a_z), v_{z+1} f(a_{z+1}), \ldots, v_{n+1} f(a_{n+1}), f_{k-1}) \in Hull_\ell(\mathcal{C})$ with $\deg(f(x)) \le k-1$, by Proposition II.2, there exists a polynomial $g(x) \in \mathbb{F}_q[x]$ with $\deg(g(x)) \le n-k+1$ such that

$$\begin{aligned}&(\beta^{p^\ell+1} v_1^{p^\ell+1} f^{p^\ell}(a_1), \ldots, \beta^{p^\ell+1} v_z^{p^\ell+1} f^{p^\ell}(a_z),\\ &\quad v_{z+1}^{p^\ell+1} f^{p^\ell}(a_{z+1}), \ldots, v_{n+1}^{p^\ell+1} f^{p^\ell}(a_{n+1}), f_{k-1}^{p^\ell})\\ &= (w_1 g(a_1), \ldots, w_{n+1} g(a_{n+1}), -g_{n-k+1}).\end{aligned}$$

That is,

$$\begin{aligned}&(\gamma w_1 f^{p^\ell}(a_1), \ldots, \gamma w_z f^{p^\ell}(a_z), w_{z+1} f^{p^\ell}(a_{z+1}),\\ &\qquad \ldots, w_{n+1} f^{p^\ell}(a_{n+1}), f_{k-1}^{p^\ell})\\ &= (w_1 g(a_1), \ldots, w_{n+1} g(a_{n+1}), -g_{n-k+1}). \qquad (13)\end{aligned}$$

For $i = z+1, \ldots, n+1$, by comparing the i-th coordinate of Eq. (13), we have $w_i f^{p^\ell}(a_i) = w_i g(a_i)$, i.e., $f^{p^\ell}(a_i) = g(a_i)$. Hence the number of the distinct roots of $f^{p^\ell}(x) - g(x)$ is at least $n-z+1 \ge n-k+2$. Since $k \le \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$, we have $\deg(f^{p^\ell}(x)) \le p^\ell(k-1) \le n-k$, which, together with $\deg(g(x)) \le n-k+1$ derives that $\deg(f^{p^\ell}(x) - g(x)) \le n-k+1$. Hence $f^{p^\ell}(x) = g(x)$.

Moreover, we have $f_{k-1}^{p^\ell} = -g_{n-k+1}$ from Eq. (13). Assume that $f_{k-1} \neq 0$. By $\deg(f^{p^\ell}(x)) = \deg(g(x))$, we have $p^\ell(k-1) = n-k+1$, which yields a contradiction since $p^\ell(k-1) \le n-k$. Hence, $f_{k-1} = 0$, implying that $\deg(f(x)) \le k-2$.

According to the first z coordinates of Eq. (13), we have that

$$\gamma w_i f^{p^\ell}(a_i) = w_i g(a_i) = w_i f^{p^\ell}(a_i)$$

for $i = 1, \ldots, z$. Hence $f^{p^\ell}(a_i) = 0$, i.e., $f(a_i) = 0$ for $i = 1, \ldots, z$. Then $f(x)$ can be written as

$$f(x) = c(x) \prod_{i=1}^{z} (x - a_i)$$

for some $c(x) \in \mathbb{F}_q[x]$ with $\deg(c(x)) \le k-2-z$. Thus $\dim(Hull_\ell(\mathcal{C})) \le k-1-z$.

Conversely, similar to the proofs of Theorems III.1 and III.2, we get $\dim(Hull_\ell(\mathcal{C})) \ge k-1-z$.

Therefore, $\dim(Hull_\ell(\mathcal{C})) = k-1-z = h$, which completes the proof. ∎

Remark III.1: Note that the lengths n of the MDS codes in Theorems III.1, III.2 and III.3 are $\frac{q-1}{p^\ell-1}, \frac{2(q-1)}{p^\ell-1}, \ldots, \frac{(p^\ell-2)(q-1)}{p^\ell-1}, q-1$, which are related to ℓ except the last one. Substituting these lengths $n = \frac{t(q-1)}{p^\ell-1}$ into the upper bound $\frac{p^\ell+n}{p^\ell+1}$ of the dimension k gives rise to $\frac{p^\ell+n}{p^\ell+1} = \frac{p^\ell+\frac{t(q-1)}{p^\ell-1}}{p^\ell+1} = \frac{p^{2\ell}-p^\ell+t(q-1)}{p^{2\ell}-1}$. Then, for a fixed t (there always exist some fixed t for different ℓ_1 and ℓ_2, for example, take $t = 1, 2$), the derivative $(\frac{p^{2\ell}-p^\ell+t(q-1)}{p^{2\ell}-1})' = \frac{p^{2\ell}[p^\ell-2t(q-1)]\ln p+(p^\ell-2p^{2\ell})\ln p}{(p^{2\ell}-1)^2} < 0$. This together with the condition $2\ell \mid e$ (means $1 \le \ell \le \frac{e}{2}$) reveals that the range of the dimension k for any $1 \le \ell < \frac{e}{2}$ with $2\ell \mid e$ is wider than the range of the dimension k for the Hermitian case $\ell = \frac{e}{2}$. Therefore, the $[n,k]_q$, $[n+1,k]_q$ and $[n+2,k]_q$ MDS codes in Theorems III.1, III.2 and III.3 with dimension k satisfying $\lfloor \frac{p^{\frac{e}{2}}+n}{p^{\frac{e}{2}}+1} \rfloor + 1 \le k \le \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$ for any $1 \le \ell < \frac{e}{2}$ with $2\ell \mid e$ cannot be obtained by the Hermitian case $\ell = \frac{e}{2}$. For example, take $p=5$, $e=4$, $\ell=1$ and $t=1$ in Theorems III.1, III.2 and III.3, then $n=156$, and hence $\lfloor \frac{5^1+156}{5^1+1} \rfloor = 26$ and $\lfloor \frac{5^2+156}{5^2+1} \rfloor = 6$. Therefore, we can obtain $[156,k]_{5^4}$, $[157,k]_{5^4}$ and $[158,k]_{5^4}$ MDS codes for each $1 \le k \le 26$, while for the same length, MDS codes with dimension k satisfying $7 \le k \le 26$ cannot be produced from those by considering the Hermitian case $\ell = 2$.

B. MDS Codes Related to the Direct Product of Two Cyclic Subgroups

In this subsection, we will present another three families of MDS codes with ℓ-Galois hulls of arbitrary dimensions. The coordinates of the vector $\mathbf{a}$ in $GRS_k(\mathbf{a}, \mathbf{v})$ or $GRS_k(\mathbf{a}, \mathbf{v}, \infty)$ are obtained via the direct product of two cyclic subgroups.

First, let us give the following lemma, which is useful for constructing the coordinates of the vector $\mathbf{a}$ in $GRS_k(\mathbf{a}, \mathbf{v})$.

Lemma III.3: Let x_1 and x_2 be two positive integers. Denote by $\xi_1 = \alpha^{x_1}$ and $\xi_2 = \alpha^{x_2}$, where α is a primitive element of $\mathbb{F}_q$. Then,

$$\gcd(\mathrm{ord}(\xi_1), \mathrm{ord}(\xi_2)) = 1 \Leftrightarrow (q-1) \mid \mathrm{lcm}(x_1, x_2),$$

where $\mathrm{ord}(x)$ denotes the order of the element x in $\mathbb{F}_q^*$.

Proof: Since $\mathrm{ord}(\xi_1) = \frac{q-1}{\gcd(x_1, q-1)}$ and $\mathrm{ord}(\xi_2) = \frac{q-1}{\gcd(x_2, q-1)}$, then $\gcd(\mathrm{ord}(\xi_1), \mathrm{ord}(\xi_2)) = 1$ if and only if

$$\gcd\left(\frac{q-1}{\gcd(x_1, q-1)}, \frac{q-1}{\gcd(x_2, q-1)} \right) = 1. \qquad (14)$$

Let S be the set consisting of all the prime divisors of $q-1$, x_1 and x_2. Assume $q-1 = \prod_{p_i \in S} p_i^{\alpha_i}$, $x_1 = \prod_{p_i \in S} p_i^{\beta_i}$ and $x_2 = \prod_{p_i \in S} p_i^{\gamma_i}$, where $\alpha_i, \beta_i, \gamma_i \in \mathbb{N}$, then we have that

$$\gcd(x_1, q-1) = \prod_{p_i \in S} p_i^{\min(\alpha_i, \beta_i)},$$

which implies that

$$\frac{q-1}{\gcd(x_1, q-1)} = \prod_{p_i \in S} p_i^{\alpha_i - \min(\alpha_i, \beta_i)}.$$

Hence, Eq. (14) holds if and only if for each i,

$$\begin{aligned}0 &= \min(\alpha_i - \min(\alpha_i, \beta_i), \alpha_i - \min(\alpha_i, \gamma_i))\\ &= \alpha_i - \max(\min(\alpha_i, \beta_i), \min(\alpha_i, \gamma_i)).\end{aligned}$$

That is,

$$\begin{aligned}&\alpha_i = \max(\min(\alpha_i,\beta_i),\min(\alpha_i,\gamma_i))\\ &\Leftrightarrow \alpha_i = \min(\alpha_i,\beta_i) \text{ or } \alpha_i = \min(\alpha_i,\gamma_i)\\ &\Leftrightarrow \alpha_i \le \beta_i \text{ or } \alpha_i \le \gamma_i\\ &\Leftrightarrow \alpha_i \le \max(\beta_i,\gamma_i)\\ &\Leftrightarrow (q-1) \mid \mathrm{lcm}(x_1,x_2).\end{aligned}$$

This completes the proof. ∎

Remark III.2: By Lemma III.3, we know that for two positive integers x_1 and x_2, the group $\langle\xi_1\rangle\otimes\langle\xi_2\rangle$ for $\xi_1=\alpha^{x_1}$ and $\xi_2=\alpha^{x_2}$ is a subgroup of $\mathbb{F}_q^*$ with order $\mathrm{ord}(\xi_1)\cdot\mathrm{ord}(\xi_2)$ if $(q-1)\mid \mathrm{lcm}(x_1,x_2)$. This implies that the elements $\xi_1^{i_1}\xi_2^{j_1}\neq \xi_1^{i_2}\xi_2^{j_2}$ for any $(i_1,j_1)\neq(i_2,j_2)$, where $1\le i_1,i_2\le \mathrm{ord}(\xi_1)$ and $1\le j_1,j_2\le \mathrm{ord}(\xi_2)$. Therefore, these elements can be taken as the coordinates of the vector $\mathbf{a}$ in $GRS_k(\mathbf{a},\mathbf{v})$ or $GRS_k(\mathbf{a},\mathbf{v},\infty)$.

Let α be a primitive element of $\mathbb{F}_q$. Consider $\xi_1=\alpha^{x_1}$ and $\xi_2=\alpha^{x_2}$ for two positive integers x_1 and x_2. Let $n=r_1r_2$, where $1\le r_1\le \mathrm{ord}(\xi_1)$, $r_2=\mathrm{ord}(\xi_2)$. Denote by

$$\mathcal{R}=\bigcup_{i=1}^{r_1} R_i=\{a_1,a_2,\ldots,a_n\}, \tag{15}$$

where $R_i=\{\xi_1^i\xi_2^j | j=1,2,\ldots,r_2\}$ for $i=1,2,\ldots,r_1$. Then by Lemma III.3 and Remark III.2, we derive the following lemma.

Lemma III.4: Let a_i and u_i be defined as in Eqs. (15) and (3), respectively. Assume that $(q-1)\mid \mathrm{lcm}(x_1,x_2)$ and $\gcd(x_2,q-1)\mid x_1(p^\ell-1)$ for two positive integers x_1 and x_2. Then, $a_i^{-1}u_i\in\mathbb{F}_{p^\ell}^*$ holds for each $i=1,2,\ldots,n$.

Proof: For $(q-1)\mid \mathrm{lcm}(x_1,x_2)$, it follows from Lemma III.3 and Remark III.2 that $a_i\neq a_j$ for any $1\le i\neq j\le n$. For any $i=1,2,\ldots,n$, we may assume $a_i\in R_s$ for some $1\le s\le r_1$. Then there exists $t\in\{1,2,\ldots,r_2\}$ such that $a_i=\xi_1^s\xi_2^t$.

By Eq. (3), we see that

$$u_i=\prod_{a_j\in R_s, a_i\neq a_j}(a_i-a_j)^{-1}\cdot\prod_{1\le s'\le r_1, s'\neq s}\prod_{a_{j'}\in R_{s'}}(a_i-a_{j'})^{-1}. \tag{16}$$

Note that $\prod_{1\le t'\le r_2-1}(x-\xi_2^{t'})=\sum_{i=0}^{r_2-1}x^i$, then

$$\begin{aligned}\prod_{a_j\in R_s,a_i\neq a_j}(a_i-a_j)&=\prod_{1\le t'\le r_2, t'\neq t}(\xi_1^s\xi_2^t-\xi_1^s\xi_2^{t'})\\ &=(\xi_1^s\xi_2^t)^{r_2-1}\prod_{1\le t'\le r_2-1}(1-\xi_2^{t'})\\ &=a_i^{-1}\xi_1^{sr_2}r_2.\end{aligned} \tag{17}$$

Besides, in light of $\prod_{1\le t'\le r_2}(x-b\xi_2^{t'})=x^{r_2}-b^{r_2}$, we have that

$$\prod_{a_{j'}\in R_{s'}}(a_i-a_{j'})=\prod_{1\le t'\le r_2}(\xi_1^s\xi_2^t-\xi_1^{s'}\xi_2^{t'})=\xi_1^{sr_2}-\xi_1^{s'r_2}. \tag{18}$$

Substituting Eqs. (17) and (18) into Eq. (16), we obtain that

$$u_i=a_i\xi_1^{-sr_2}r_2^{-1}\prod_{1\le s'\le r_1, s'\neq s}(\xi_1^{sr_2}-\xi_1^{s'r_2})^{-1}. \tag{19}$$

Further, since $\gcd(x_2,q-1)\mid x_1(p^\ell-1)$, it is easy to check that $\xi_1^{r_2}\in\mathbb{F}_{p^\ell}^*$. From this and Eq. (19), the desired result follows. ∎

We notice that for $\ell\mid e$, the condition $(q-1)\mid\mathrm{lcm}(x_1,x_2)$ and $\gcd(x_2,q-1)\mid x_1(p^\ell-1)$ in Lemma III.4 is equivalent to a simpler form as follows.

Lemma III.5: Let $q=p^e$ with p being a prime number and let $\ell\mid e$. Then, for any two positive integers x_1 and x_2, the following statements are equivalent:

(1) $(q-1)\mid\mathrm{lcm}(x_1,x_2)$, $\gcd(x_2,q-1)\mid x_1(p^\ell-1)$;

(2) $(q-1)\mid\mathrm{lcm}(x_1,x_2)$, $\frac{q-1}{p^\ell-1}\mid x_1$.

Proof: (2)⇒(1): When $\frac{q-1}{p^\ell-1}\mid x_1$, we have that $(q-1)\mid x_1(p^\ell-1)$, which immediately yields that $\gcd(x_2,q-1)\mid x_1(p^\ell-1)$.

(1)⇒(2): Note that for any $a,b,c\in\mathbb{N}$, we have the fact

$$a\mid\mathrm{lcm}(b,c)\Leftrightarrow a\mid\mathrm{lcm}(b,\gcd(a,c)).$$

Now, for $(q-1)\mid\mathrm{lcm}(x_1,x_2)$, we have that

$$(q-1)\mid\mathrm{lcm}(x_1,\gcd(x_2,q-1)). \tag{20}$$

Besides, it follows from the condition $\gcd(x_2,q-1)\mid x_1(p^\ell-1)$ that

$$\mathrm{lcm}(x_1,\gcd(x_2,q-1))\mid\mathrm{lcm}(x_1,x_1(p^\ell-1)).$$

That is,

$$\mathrm{lcm}(x_1,\gcd(x_2,q-1))\mid x_1(p^\ell-1). \tag{21}$$

Combining Eq. (20) with Eq. (21), we obtain $(q-1)\mid x_1(p^\ell-1)$, i.e., $\frac{q-1}{p^\ell-1}\mid x_1$. This completes the proof. ∎

By using the previous lemmas, we give the following $[n,k]_q$ MDS codes with ℓ-Galois hulls of arbitrary dimensions.

Theorem III.4: Let $q=p^e$ with p being an odd prime number. Assume $2\ell\mid e$, $(q-1)\mid\mathrm{lcm}(x_1,x_2)$ and $\frac{q-1}{p^\ell-1}\mid x_1$ for two positive integers x_1 and x_2. Let $n=\frac{r(q-1)}{\gcd(x_2,q-1)}$ for each $1\le r\le\frac{q-1}{\gcd(x_1,q-1)}$. Then, for any $1\le k\le\lfloor\frac{p^\ell+n}{p^\ell+1}\rfloor$ and $0\le h\le k-1$, there exists an $[n,k]_q$ MDS code with h-dimensional ℓ-Galois hull.

Proof: Let $a_1,a_2,\ldots,a_n$ be defined by Eq. (15). For each $1\le i\le n$, by Lemmas III.4 and III.5, we have $a_i^{-1}u_i\in\mathbb{F}_{p^\ell}^*$. Further, in terms of Lemma III.2, there exists $v_i\in\mathbb{F}_q^*$ such that $v_i^{p^\ell+1}=a_i^{-1}u_i$. Set $z:=k-1-h$ and take $\beta\in\mathbb{F}_q^*$ such that $\gamma:=\beta^{p^\ell+1}\neq 1$. Put $\mathbf{a}=(a_1,a_2,\ldots,a_n)$ and $\mathbf{v}=(\beta v_1,\ldots,\beta v_z,v_{z+1},\ldots,v_n)$. Consider the ℓ-Galois hull of the $[n,k]_q$ MDS code $\mathcal{C}:=GRS_k(\mathbf{a},\mathbf{v})$. Then, working in a similar manner as in Theorem III.1, the desired result follows. ∎

Next, based on Theorem III.4, we proceed to construct a family of MDS codes of length $n+1$ from GRS codes with ℓ-Galois hulls of arbitrary dimensions as follows.

Theorem III.5: Let $q=p^e$ with p being an odd prime number. Assume $2\ell\mid e$, $(q-1)\mid\mathrm{lcm}(x_1,x_2)$ and $\frac{q-1}{p^\ell-1}\mid x_1$ for two positive integers x_1 and x_2. Let $n=\frac{r(q-1)}{\gcd(x_2,q-1)}$ for each $1\le r\le\frac{q-1}{\gcd(x_1,q-1)}$. Then, for any $1\le k\le\lfloor\frac{p^\ell+n}{p^\ell+1}\rfloor$ and $0\le h\le k$, there exists an $[n+1,k]_q$ MDS code with h-dimensional ℓ-Galois hull.

Proof: Let $a_1, a_2, \ldots, a_n$ be defined as in Eq. (15) and let $a_{n+1} = 0$. For each $1 \le i \le n$, in view of Lemma III.4, we have that

$$\prod_{1\le j\le n+1, j\neq i} (a_i - a_j)^{-1} = a_i^{-1} \prod_{1\le j\le n, j\neq i} (a_i - a_j)^{-1} \in \mathbb{F}_{p^\ell}^*.$$

For $i = n+1$, a direct calculation derives that

$$\begin{aligned}\prod_{j=1}^{n}(a_{n+1} - a_j)^{-1} &= (-1)^n \Big[\prod_{j=1}^{r_2}\Big(\prod_{i=1}^{r_1}\xi_1^i\xi_2^j\Big)\Big]^{-1} \\ &= (-1)^n \xi_1^{-\frac{r_1(r_1+1)r_2}{2}} \xi_2^{-\frac{r_2(r_2+1)r_1}{2}} \\ &\in \mathbb{F}_{p^\ell}^*.\end{aligned}$$

Denote $w_i = \prod_{1\le j\le n+1, j\neq i}(a_i - a_j)^{-1}, i = 1, \ldots, n+1$. Then, from Lemma III.2, there exists $v_i \in \mathbb{F}_q^*$ such that $v_i^{p^\ell+1} = w_i$ for $i = 1, \ldots, n+1$. Set $z := k - h$ and take $\beta \in \mathbb{F}_q^*$ such that $\gamma := \beta^{p^\ell+1} \neq 1$. Put $\mathbf{a} = (a_1, a_2, \ldots, a_{n+1})$, $\mathbf{v} = (\beta v_1, \ldots, \beta v_z, v_{z+1}, \ldots, v_{n+1})$ and consider the ℓ-Galois hull of the $[n+1, k]_q$ MDS code $\mathcal{C} := GRS_k(\mathbf{a}, \mathbf{v})$. Similar to the proof of Theorem III.2, the desired result follows. ∎

Now, if we consider the extended GRS code $GRS_k(\mathbf{a}, \mathbf{v}, \infty)$ of length $n+2$ with $\mathbf{a}$ and $\mathbf{v}$ being defined as in the proof of Theorem III.5, then a new family of MDS codes with ℓ-Galois hulls of arbitrary dimensions can be yielded as follows.

Theorem III.6: Let $q = p^e$ with p being an odd prime number. Assume $2\ell \mid e$, $(q-1) \mid \mathrm{lcm}(x_1, x_2)$ and $\frac{q-1}{p^\ell-1} \mid x_1$ for two positive integers x_1 and x_2. Let $n = \frac{r(q-1)}{\gcd(x_2, q-1)}$ for each $1 \le r \le \frac{q-1}{\gcd(x_1, q-1)}$. Then, for any $1 \le k \le \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$ and $0 \le h \le k-1$, there exists an $[n+2, k]_q$ MDS code with h-dimensional ℓ-Galois hull.

Proof: Set $z := k - 1 - h$ and take $\beta \in \mathbb{F}_q^*$ such that $\gamma := \beta^{p^\ell+1} \neq 1$. Let $\mathbf{a} = (a_1, a_2, \ldots, a_{n+1})$, $\mathbf{v} = (\beta v_1, \ldots, \beta v_z, v_{z+1}, \ldots, v_{n+1})$ and w_i be defined as in the proof of Theorem III.5. We can consider the ℓ-Galois hull of the $[n+2, k]_q$ MDS code $\mathcal{C} := GRS_k(\mathbf{a}, \mathbf{v}, \infty)$. Then, working in a similar manner as in Theorem III.3, the desired result follows. ∎

Remark III.3: For the MDS codes in Theorems III.4, III.5 and III.6, we can verify that the value of the length n is related to ℓ (namely, depends on ℓ), for example, we may take $x_2 = p^\ell - 1$, then $(q-1) \mid \mathrm{lcm}(x_1, p^\ell - 1)$ and $\frac{q-1}{p^\ell-1} \mid x_1$. In this case, one easily finds that there always exists $x_1 = \frac{q-1}{p^\ell-1}s$ for some positive integer s such that $(q-1) \mid \mathrm{lcm}\big(\frac{q-1}{p^\ell-1}s, p^\ell - 1\big)$, then the length n can be written as $n = \frac{r(q-1)}{p^\ell-1}$, where $1 \le r \le \frac{q-1}{\gcd\left(\frac{q-1}{p^\ell-1}s, q-1\right)} = \frac{p^\ell-1}{\gcd(s, p^\ell-1)}$. Hence, the upper bound $\frac{p^\ell+n}{p^\ell+1}$ of the dimension k is $\frac{p^\ell + \frac{r(q-1)}{p^\ell-1}}{p^\ell+1} = \frac{p^{2\ell}-p^\ell+r(q-1)}{p^{2\ell}-1}$. Then, for a fixed r (there always exist some fixed r for different ℓ_1 and ℓ_2, for example, take $r = 1$), the derivative $(\frac{p^{2\ell}-p^\ell+r(q-1)}{p^{2\ell}-1})' = \frac{p^{2\ell}[p^\ell - 2r(q-1)]\ln p + (p^\ell - 2p^{2\ell})\ln p}{(p^{2\ell}-1)^2} < 0$. This together with the condition $2\ell \mid e$ (means $1 \le \ell \le \frac{e}{2}$) reveals that the range of the dimension k for any $1 \le \ell < \frac{e}{2}$ with $2\ell \mid e$ is wider than the range of the dimension k for the Hermitian case $\ell = \frac{e}{2}$. Therefore, the $[n, k]_q$, $[n+1, k]_q$ and $[n+2, k]_q$ MDS codes in Theorems III.4, III.5 and III.6 with dimension k satisfying $\lfloor \frac{p^{\frac{e}{2}}+n}{p^{\frac{e}{2}}+1} \rfloor + 1 \le k \le \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$ for any $1 \le \ell < \frac{e}{2}$ with $2\ell \mid e$ cannot be obtained by the Hermitian case $\ell = \frac{e}{2}$. For example, take $p = 7$, $e = 4$, $\ell = 1$, $x_1 = 2400$, $x_2 = 6$ and $r = 1$ in Theorems III.4, III.5 and III.6, then $n = 400$, and hence $\lfloor \frac{7^1+400}{7^1+1} \rfloor = 50$ and $\lfloor \frac{7^2+400}{7^2+1} \rfloor = 8$. Therefore, we can obtain $[400, k]_{7^4}$, $[401, k]_{7^4}$ and $[402, k]_{7^4}$ MDS codes for each $1 \le k \le 50$, while for the same length, MDS codes with dimension k satisfying $9 \le k \le 50$ cannot be produced from those by considering the Hermitian case $\ell = 2$.

C. MDS Codes Related to the Coset Decomposition of a Cyclic Group

In this subsection, we will construct another three families of MDS codes with ℓ-Galois hulls of arbitrary dimensions. The coordinates of the vector $\mathbf{a}$ in $GRS_k(\mathbf{a}, \mathbf{v})$ or $GRS_k(\mathbf{a}, \mathbf{v}, \infty)$ are obtained via the coset decomposition of a cyclic group.

Let $q = p^e$ with p being a prime number. Assume $\ell \mid e$ and set $y := \frac{q-1}{p^\ell-1}$. Let $m \mid (q-1)$. We know m can be labeled as $m = m_1 m_2$, where $m_1 = \frac{m}{\gcd(m,y)}$ and $m_2 = \gcd(m, y)$. Let $\mathbb{F}_q^* = \langle\alpha\rangle$. Denote $H = \langle\vartheta_1\rangle$ and $G = \langle\vartheta_2\rangle$, where $\vartheta_1 := \alpha^{\frac{q-1}{m}}$ and $\vartheta_2 = \alpha^{\frac{y}{m_2}}$. Then we have $\mathrm{ord}(H) = m$ and $\mathrm{ord}(G) = (p^\ell - 1)m_2$.

Next, it follows from $m_2 = \gcd(m, y)$ that $\gcd(m_1, \frac{y}{m_2}) = 1$. Combining it with $m_1 \mid \frac{q-1}{m_2}$, we obtain $m_1 \mid (p^\ell - 1)$, which implies that H is a subgroup of G. Thus the left coset decomposition of G with respect to H can be written as $G = \bigcup_{i=1}^{\frac{p^\ell-1}{m_1}} \eta_i H$, where η_i is the left coset representative of G/H for $i = 1, 2, \ldots, \frac{p^\ell-1}{m_1}$.

Let $n = rm$, where $1 \le r \le \frac{p^\ell-1}{m_1}$. Denote

$$\mathcal{H} = \bigcup_{i=1}^{r} \eta_i H = \{a_1, a_2, \ldots, a_n\}. \tag{22}$$

We give the following lemma.

Lemma III.6: Let a_i and u_i be defined by Eqs. (22) and (3), respectively. Assume $\ell \mid e$ and $m \mid (q-1)$. Then, $a_i^{-1}u_i \in \mathbb{F}_{p^\ell}^*$ holds for each $i = 1, 2, \ldots, n$.

Proof: For any $i = 1, 2, \ldots, n$, there exists $s \in \{1, 2, \ldots, r\}$ such that $a_i \in \eta_s H$. Then $a_i = \eta_s \vartheta_1^t$ for some $1 \le t \le m$. By Eq. (3), we know that

$$u_i = \prod_{a_j \in \eta_s H, a_i \neq a_j} (a_i - a_j)^{-1} \cdot \prod_{1\le s'\le r, s'\neq s} \prod_{a_{j'} \in \eta_{s'} H} (a_i - a_{j'})^{-1}.$$

First, we have that

$$\begin{aligned}\prod_{a_j \in \eta_s H, a_i \neq a_j} (a_i - a_j) &= \prod_{1\le t'\le m, t'\neq t} (\eta_s\vartheta_1^t - \eta_s\vartheta_1^{t'}) \\ &= (\eta_s\vartheta_1^t)^{m-1} \prod_{1\le t'\le m-1} (1 - \vartheta_1^{t'}) \\ &= a_i^{-1}\eta_s^m m.\end{aligned}$$

Besides, we obtain that

$$\prod_{a_{j'} \in \eta_{s'} H} (a_i - a_{j'}) = \prod_{1\le t'\le m} (\eta_s\vartheta_1^t - \eta_{s'}\vartheta_1^{t'}) = \eta_s^m - \eta_{s'}^m.$$

Thus, we get that

$$u_i = a_i \eta_s^{-m} m^{-1} \prod_{1 \le s' \le r, s' \ne s} (\eta_s^m - \eta_{s'}^m)^{-1}.$$

For any $1 \le i \le r$, we know that $\eta_i = \vartheta_2^j$ holds for some $1 \le j \le (p^\ell - 1)m_2$. Then, $\eta_i^m = \alpha^{jm_1 y} \in \mathbb{F}_{p^\ell}^*$, which derives that $a_i^{-1} u_i \in \mathbb{F}_{p^\ell}^*$. This completes the proof. ∎

Now, by applying the above lemma, we obtain a new family of MDS codes of length n with ℓ-Galois hulls of arbitrary dimensions as follows.

Theorem III.7: Let $q = p^e$ with p being an odd prime number. Assume $2\ell \mid e$ and $m \mid (q-1)$. Let $n = rm$ for each $1 \le r \le \frac{p^\ell - 1}{m_1}$ with $m_1 = \frac{m}{\gcd(m,y)}$ for $y = \frac{q-1}{p^\ell - 1}$. Then, for any $1 \le k \le \lfloor \frac{p^\ell + n}{p^\ell + 1} \rfloor$ and $0 \le h \le k-1$, there exists an $[n,k]_q$ MDS code with h-dimensional ℓ-Galois hull.

Proof: Let $a_1, a_2, \ldots, a_n$ be defined by Eq. (22). For each $1 \le i \le n$, by Lemma III.6, we have $a_i^{-1} u_i \in \mathbb{F}_{p^\ell}^*$. Further, in terms of Lemma III.2, there exists $v_i \in \mathbb{F}_q^*$ such that $v_i^{p^\ell + 1} = a_i^{-1} u_i$. Set $z := k - 1 - h$ and take $\beta \in \mathbb{F}_q^*$ such that $\beta^{p^\ell + 1} \ne 1$. We can consider the ℓ-Galois hull of the $[n,k]_q$ MDS code $\mathcal{C} := GRS_k(\mathbf{a}, \mathbf{v})$, where $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{v} = (\beta v_1, \ldots, \beta v_z, v_{z+1}, \ldots, v_n)$. Similar to the proof of Theorem III.1, we can obtain $\dim(Hull_\ell(\mathcal{C})) = k - z - 1 = h$. From this, the desired result follows immediately. ∎

Next, based on Theorem III.7, we proceed to construct a family of MDS codes of length $n+1$ from GRS codes with ℓ-Galois hulls of arbitrary dimensions as follows.

Theorem III.8: Let $q = p^e$ with p being an odd prime number. Assume $2\ell \mid e$ and $m \mid (q-1)$. Let $n = rm$ for each $1 \le r \le \frac{p^\ell - 1}{m_1}$ with $m_1 = \frac{m}{\gcd(m,y)}$ for $y = \frac{q-1}{p^\ell - 1}$. Then, for any $1 \le k \le \lfloor \frac{p^\ell + n}{p^\ell + 1} \rfloor$ and $0 \le h \le k$, there exists an $[n+1,k]_q$ MDS code with h-dimensional ℓ-Galois hull.

Proof: Let $a_1, a_2, \ldots, a_n$ be defined by Eq. (22) and let $a_{n+1} = 0$. For each $1 \le i \le n$, it follows from Lemma III.6 that

$$\prod_{1 \le j \le n+1, j \ne i} (a_i - a_j)^{-1} = a_i^{-1} \prod_{1 \le j \le n, j \ne i} (a_i - a_j)^{-1} \in \mathbb{F}_{p^\ell}^*.$$

For $i = n+1$, a direct calculation derives that

$$\prod_{i=1}^{n} (a_{n+1} - a_i)^{-1} = (-1)^n \Big[\prod_{i=1}^{r} \Big(\prod_{j=1}^{m} \eta_i \vartheta_1^j \Big) \Big]^{-1} = (-1)^n \vartheta_1^{-\frac{rm(m+1)}{2}} \prod_{i=1}^{r} \eta_i^{-m} \in \mathbb{F}_{p^\ell}^*.$$

Further, we write $w_i = \prod_{1 \le j \le n+1, j \ne i} (a_i - a_j)^{-1}, i = 1, \ldots, n+1$. In light of Lemma III.2, there exists $v_i \in \mathbb{F}_q^*$ such that $v_i^{p^\ell + 1} = w_i$ for $i = 1, \ldots, n+1$.

Next, we set $z := k - h$ and take $\beta \in \mathbb{F}_q^*$ such that $\beta^{p^l + 1} \ne 1$. We can consider the ℓ-Galois hull of the $[n+1,k]_q$ MDS code $\mathcal{C} := GRS_k(\mathbf{a}, \mathbf{v})$, where $\mathbf{a} = (a_1, a_2, \ldots, a_{n+1})$ and $\mathbf{v} = (\beta v_1, \ldots, \beta v_z, v_{z+1}, \ldots, v_{n+1})$. Working in a similar way to the proof of Theorem III.2, we can deduce that $\dim(Hull_\ell(\mathcal{C})) = k - z = h$. Therefore, the desired result follows. ∎

Now, if we consider the extended GRS code $GRS_k(\mathbf{a}, \mathbf{v}, \infty)$ of length $n+2$ with $\mathbf{a}$ and $\mathbf{v}$ being defined as in the proof of Theorem III.8, then a family of MDS codes with ℓ-Galois hulls of arbitrary dimensions can be yielded as follows.

Theorem III.9: Let $q = p^e$ with p being an odd prime number. Assume $2\ell \mid e$ and $m \mid (q-1)$. Let $n = rm$ for each $1 \le r \le \frac{p^\ell - 1}{m_1}$ with $m_1 = \frac{m}{\gcd(m,y)}$ for $y = \frac{q-1}{p^\ell - 1}$. Then, for any $1 \le k \le \lfloor \frac{p^\ell + n}{p^\ell + 1} \rfloor$ and $0 \le h \le k-1$, there exists an $[n+2,k]_q$ MDS code with h-dimensional ℓ-Galois hull.

Proof: Let $a_1, a_2, \ldots, a_n$ be defined by Eq. (22) and let $a_{n+1} = 0$. For each $1 \le i \le n+1$, write $w_i = \prod_{1 \le j \le n+1, j \ne i} (a_i - a_j)^{-1}$. Then $w_i \in \mathbb{F}_{p^\ell}^*$. By Lemma III.2, there exists $v_i \in \mathbb{F}_q^*$ such that $v_i^{p^\ell + 1} = w_i$ for $i = 1, \ldots, n+1$.

Next, we set $z := k - h - 1$ and take $\beta \in \mathbb{F}_q^*$ such that $\beta^{p^\ell + 1} \ne 1$. Put $\mathbf{a} = (a_1, a_2, \ldots, a_{n+1})$ and $\mathbf{v} = (\beta v_1, \ldots, \beta v_z, v_{z+1}, \ldots, v_{n+1})$. We can consider the ℓ-Galois hull of the $[n+2,k]_q$ MDS code $\mathcal{C} := GRS_k(\mathbf{a}, \mathbf{v}, \infty)$. Similar to the proof of Theorem III.3, we deduce that $\dim(Hull_\ell(\mathcal{C})) = k - 1 - z = h$, completing the proof. ∎

Remark III.4: Note that when e is even, the MDS codes in Theorems III.7, III.8 and III.9 generalize those in [16, Theorems 3.8-3.10] which consider the Hermitian case (i.e., $\ell = \frac{e}{2}$). More importantly, observing the condition $2\ell \mid e$ (as shown in Lemma III.2, this condition is necessary since it enables us to find a $v_i \in \mathbb{F}_q^*$ such that $v_i^{p^\ell + 1} = u_i$ holds for any $u_i \in \mathbb{F}_{p^\ell}^*$, which means that $1 \le \ell \le \frac{e}{2}$) and using the fact $(\frac{p^\ell + n}{p^\ell + 1})' = \frac{(1-n)p^\ell \ln p}{(p^\ell + 1)^2} < 0$ for $n \ge 2$, we know that when n is fixed (for example, take $r = 1$, then $n = m$ is fixed), the range of the dimension of the MDS codes in Theorems III.7, III.8 and III.9 for any $1 \le \ell < \frac{e}{2}$ with $2\ell \mid e$ is wider than the range of the dimension of those in [16, Theorems 3.8-3.10]. In other words, for the same length n, the $[n,k]_q$, $[n+1,k]_q$ and $[n+2,k]_q$ MDS codes in Theorems III.7, III.8 and III.9 with dimension k satisfying $\lfloor \frac{p^{\frac{e}{2}} + n}{p^{\frac{e}{2}} + 1} \rfloor + 1 \le k \le \lfloor \frac{p^\ell + n}{p^\ell + 1} \rfloor$ for any $1 \le \ell < \frac{e}{2}$ with $2\ell \mid e$ cannot be obtained by the Hermitian case $\ell = \frac{e}{2}$ considered in [16, Theorems 3.8-3.10]. For example, take $p = 5$, $e = 6$, $\ell = 1$, $m = 126$ and $r = 1$ in Theorems III.7, III.8 and III.9, then $n = 126$ and $\lfloor \frac{5^1 + 126}{5^1 + 1} \rfloor = 21$. Hence, we can obtain $[126,k]_{5^6}$, $[127,k]_{5^6}$ and $[128,k]_{5^6}$ MDS codes for each $1 \le k \le 21$, while for the same lengths, Theorems 3.8-3.10 of [16] only produce $[126,1]_{5^6}$, $[127,1]_{5^6}$ and $[128,1]_{5^6}$ MDS codes since $\lfloor \frac{5^3 + 126}{5^3 + 1} \rfloor = 1$.

D. MDS Codes Related to an Additive Subgroup of $\mathbb{F}_q$ and Its Cosets

We will construct another two families of MDS codes with ℓ-Galois hulls of arbitrary dimensions. The coordinates of the vector $\mathbf{a}$ in $GRS_k(\mathbf{a}, \mathbf{v})$ or $GRS_k(\mathbf{a}, \mathbf{v}, \infty)$ are related to an additive subgroup of $\mathbb{F}_q$ and its cosets.

Let $q = p^e$ with p being an odd prime number. Let $a \mid e$ and K be a $\mathbb{F}_{p^a}$-subspace of $\mathbb{F}_q$ of dimension w satisfying $\{0\} \subsetneq K \subsetneq \mathbb{F}_q$. Then, $1 \le w \le \frac{e}{a} - 1$. Take $\eta \in \mathbb{F}_q \backslash K$ and put $\mathbb{F}_{p^a} = \{\beta_1, \beta_2, \ldots, \beta_{p^a}\}$. For $1 \le i \le p^a$, denote by

$K_i = K + \beta_i\eta$. For $1 \le t \le p^a$, denote by

$$\bigcup_{i=1}^{t} K_i = \{a_1, a_2, \ldots, a_n\}.$$

Then, we have $n = tp^{aw}$. By [16, Lemma 3.1], there exists $\varepsilon \in \mathbb{F}_q^*$ such that $\varepsilon u_i \in \mathbb{F}_{p^a}^*$ for each i. Let $a \mid \ell$ and $2\ell \mid e$. Then, we have $\varepsilon u_i \in \mathbb{F}_{p^\ell}^*$. According to Lemma III.2, there exists $v_i \in \mathbb{F}_q^*$ such that $\varepsilon u_i = v_i^{p^\ell+1}$.

Based on the above analysis, we are able to give another two families of MDS codes with ℓ-Galois hulls of arbitrary dimensions in the following two theorems. Since their construction procedures are similar to those of Theorems III.1-III.9, we omit the proofs.

Theorem III.10: Let $q = p^e$ with p being an odd prime number. Assume $2\ell \mid e$ and $a \mid \ell$. Let $n = tp^{aw}$ for each $1 \le t \le p^a$ and each $1 \le w \le \frac{e}{a} - 1$. Then, for any $1 \le k \le \lfloor \frac{p^\ell+n-1}{p^\ell+1} \rfloor$ and $0 \le h \le k$, there exists an $[n, k]_q$ MDS code with h-dimensional ℓ-Galois hull.

Theorem III.11: Let $q = p^e$ with p being an odd prime number. Assume $2\ell \mid e$ and $a \mid \ell$. Let $n = tp^{aw}$ for each $1 \le t \le p^a$ and each $1 \le w \le \frac{e}{a} - 1$. Then, for any $1 \le k \le \lfloor \frac{p^\ell+n-1}{p^\ell+1} \rfloor$ and $0 \le h \le k-1$, there exists an $[n+1, k]_q$ MDS code with h-dimensional ℓ-Galois hull.

Remark III.5: Note that when e is even, the MDS codes in Theorems III.10 and III.11 generalize those in [16, Theorem 3.6] which consider the Hermitian case (i.e., $\ell = \frac{e}{2}$). What's more, the condition $2\ell \mid e$ (this means that $1 \le \ell \le \frac{e}{2}$) and the fact $(\frac{p^\ell+n-1}{p^\ell+1})' = \frac{(2-n)p^\ell \ln p}{(p^\ell+1)^2} < 0$ for $n \ge 3$ imply that when n is fixed, the range of the dimension k of the MDS codes in Theorems III.10 and III.11 for any $1 \le \ell < \frac{e}{2}$ with $2\ell \mid e$ is wider than the range of the dimension k of those in [16, Theorem 3.6]. Hence, for the same length n, the $[n, k]_q$ and $[n+1, k]_q$ MDS codes in Theorems III.10 and III.11 with dimension k satisfying $\lfloor \frac{p^{\frac{e}{2}}+n-1}{p^{\frac{e}{2}}+1} \rfloor + 1 \le k \le \lfloor \frac{p^\ell+n-1}{p^\ell+1} \rfloor$ for any $1 \le \ell < \frac{e}{2}$ with $2\ell \mid e$ cannot be produced by [16, Theorem 3.6]. For example, take $p = 3$, $a = 2$, $e = 8$, $\ell = 2$, $w = 2$ and $t = 2$ in Theorems III.10 and III.11, then $n = 162$, and hence we can obtain $[162, k]_{3^8}$ and $[163, k]_{3^8}$ MDS codes for each $1 \le k \le 17$. Since $\lfloor \frac{3^4+161}{3^4+1} \rfloor = 2$, these k-dimensional MDS codes of the same length with $3 \le k \le 17$ cannot be produced by considering the Hermitian case, i.e., $\ell = 4$, in [16, Theorem 3.6].

IV. Constructions of EAQECCs With Relatively Large Minimum Distance

As the applications of the q-ary MDS codes constructed in Section III, this section aims to provide several families of $[[n, k, d; c]]_q$ entanglement-assisted quantum error-correcting codes (EAQECCs) with relatively large minimum distance in the sense that $2d = n - k + 2 + c$.

First, let us review some basic concepts and notations about quantum codes. For the complex field $\mathbb{C}$, let $\mathbb{C}^q$ denote the q-dimensional complex Hilbert space over $\mathbb{C}$. For a pure n-qudit state, it can be written as $|\mathbf{v}\rangle = \sum_{\mathbf{a}\in\mathbb{F}_q^n} v_{\mathbf{a}}|\mathbf{a}\rangle$, where $v_{\mathbf{a}} \in \mathbb{C}$ with $\sum_{\mathbf{a}\in\mathbb{F}_q^n} |v_{\mathbf{a}}|^2 = 1$ and $\{|\mathbf{a}\rangle = |a_1\rangle \otimes \cdots \otimes |a_n\rangle : (a_1, \ldots, a_n) \in \mathbb{F}_q^n\}$ being a basis of $\mathbb{C}^{q^n}$. Let γ be a complex primitive p-th root of unity. For $\mathbf{a} = (a_1, \ldots, a_n)$, $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$, let $T(\mathbf{a}) = T(a_1) \otimes \cdots \otimes T(a_n)$ and $R(\mathbf{a}) = R(a_1) \otimes \cdots \otimes R(a_n)$ be the tensor products of n error operators, where $T(a_i)$ and $R(a_i)$ are defined as $T(a_i)|x\rangle = |x + a_i\rangle$ and $R(a_i)|x\rangle = \gamma^{\mathrm{Tr}(a_i x)}|x\rangle$, respectively, in which $\mathrm{Tr}(x) := \sum_{i=0}^{e-1} x^{p^i}$ is the trace function from $\mathbb{F}_q$ ($q = p^e$) to $\mathbb{F}_p$. Then, $T(\mathbf{a})$ and $R(\mathbf{a})$ satisfy $T(\mathbf{a})|\mathbf{x}\rangle = |\mathbf{x} + \mathbf{a}\rangle$ and $R(\mathbf{a})|\mathbf{x}\rangle = \gamma^{\mathrm{Tr}((\mathbf{a},\mathbf{x})_E)}|\mathbf{x}\rangle$, respectively. Therefore, the error set

$$E_n = \{\gamma^i T(\mathbf{a})R(\mathbf{b}) | 0 \le i \le p-1, \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n\}$$

forms an error group. For any error $\mathbf{e} = \gamma^i T(\mathbf{a})R(\mathbf{b}) \in E_n$, its quantum weight is defined by $w_Q(\mathbf{e}) = \sharp\{i | (a_i, b_i) \ne (0, 0)\}$. Denote $E_n(i) = \{\mathbf{e} \in E_n | w_Q(\mathbf{e}) \le i\}$. For a q-ary quantum code Q, if d is the largest positive integer such that $\langle \mathbf{x}|\mathbf{e}|\mathbf{y}\rangle = \mathbf{0}$ holds for any $|\mathbf{x}\rangle, |\mathbf{y}\rangle \in Q$ with $\langle \mathbf{x}|\mathbf{y}\rangle = \mathbf{0}$ and $\mathbf{e} \in E_n(d-1)$, then Q has minimum distance d.

Usually, we use the notation $[[n, k, d]]_q$ to denote a q-ary quantum code of length n, dimension q^k and minimum distance d. It has the abilities to detect up to $d-1$ quantum errors and correct up to $\lfloor \frac{d-1}{2} \rfloor$ quantum errors. The minimum distance d of a quantum code must satisfy the *quantum Singleton bound*, i.e., $2d \le n + 2 - k$. Further, if $2d = n + 2 - k$, then such a quantum code is called a *quantum MDS code*.

In 2006, Brun et al. [2] introduced an interesting concept called entanglement-assisted quantum error-correcting codes (EAQECCs), which turns out to be significant progress in the field of quantum error correction. These codes can be regarded as a generalization of the quantum stabilizer codes generated by CSS construction. As shown in [2], we can obtain EAQECCs from any classical linear codes with the help of the pre-shared entanglement between the sender and receiver. Furthermore, we denote by $[[n, k, d; c]]_q$ a q-ary EAQECC which encodes k logical qubits into n physical qubits by means of c copies of maximally entangled states (i.e., c ebits). When $c = 0$, the EAQECCs are just the standard quantum stabilizer codes.

For an $[[n, k, d; c]]_2$ EAQECC, the authors in [3] gave the following Singleton bound on its parameters:

$$2d \le n - k + 2 + c.$$

It is very exciting to know that Grassl [24] presented a new entanglement-assisted quantum communication scheme with parameters violating this bound in certain ranges. The scheme in [24] shows better parameters than the one proposed in [2] in some range. For more information on the counter examples of quantum Singleton bound, we refer the reader to the latest results obtained by Grassl, Huber and Winter in [26]. Considering these facts, from now on, if an $[[n, k, d; c]]_q$ EAQECC satisfies $2d = n - k + 2 + c$, then we call it an *EAQECC with relatively large minimum distance* rather than a MDS EAQECC.

The following lemmas tell us how to construct EAQECCs from the classical linear codes.

Lemma IV.1 ([19], [53]): Let $\mathcal{C}_1 : [n, k_1, d_1]_q$ and $\mathcal{C}_2 : [n, k_2, d_2]_q$ be two linear codes with parity check matrices H_1

and H_2, respectively. Then, there exists an $[[n, k_1+k_2-n+c, \min\{d_1, d_2\}; c]]_q$ EAQECC, where $c = \mathrm{rank}(H_1 H_2^T)$ is the required number of maximally entangled states.

Lemma IV.2 ([19]): Let $\mathcal{C}_1 : [n, k_1, d_1]_{q^2}$ and $\mathcal{C}_2 : [n, k_2, d_2]_{q^2}$ be two linear codes with parity check matrices H_1 and H_2, respectively. Then, there exists an $[[n, k_1+k_2-n+c, \min\{d_1, d_2\}; c]]_q$ EAQECC, where $c = \mathrm{rank}(H_1 H_2^\dagger)$ is the required number of maximally entangled states with $H^\dagger := (h_{ji}^q)$ for $H = (h_{ij})$.

Remark IV.1: The binary case for the EAQECCs in Lemma IV.1 was given by Wilde and Brun [53] in 2008. In 2019, Galindo, Hernando, Matsumoto and Ruano [19] extended the binary case to the general one and they also obtained several important results on EAQECCs.

For a matrix $A = (a_{ij})$ over $\mathbb{F}_q$, we define $A^{(p^{e-\ell})} = (a_{ij}^{p^{e-\ell}})$ and denote $A^\ddagger = [A^{(p^{e-\ell})}]^T$. Then, we have the following useful lemma.

Lemma IV.3 ([41]): If $\mathcal{C}$ is an $[n, k, d]_q$ linear code with parity-check matrix H, then

$$\mathrm{rank}(HH^\ddagger) = n - k - \dim(Hull_\ell(\mathcal{C})).$$

Based on the above facts, we obtain the following proposition.

Proposition IV.1: If $\mathcal{C}$ is an $[n, k, d]_q$ linear code, then there exists an $[[n, k-\dim(Hull_\ell(\mathcal{C})), d; n-k-\dim(Hull_\ell(\mathcal{C}))]]_q$ EAQECC.

Proof: Taking $\mathcal{C}_1 = \mathcal{C}$ and $\mathcal{C}_2 = \mathcal{C}^{p^{e-\ell}}$ in Lemma IV.1, we obtain an $[[n, 2k-n+c, d; c]]_q$ EAQECC, where $c = \mathrm{rank}(H(H^{(p^{e-\ell})})^T)$. By Lemma IV.3, we know that

$$c = \mathrm{rank}(HH^\ddagger) = n - k - \dim(Hull_\ell(C)),$$

which completes the proof. ∎

By Proposition IV.1, we immediately obtain the following corollary.

Corollary IV.1: If $\mathcal{C}$ is an $[n, k]_q$ MDS code, then exists an $[[n, k-\dim(Hull_\ell(\mathcal{C})), n-k+1; n-k-\dim(Hull_\ell(\mathcal{C}))]]_q$ EAQECC.

Remark IV.2: Given an $[n, k]_q$ ($q = p^e$) MDS code $\mathcal{C}$. If e is even, then $\mathcal{C}^{\perp_H}$ (i.e., $\mathcal{C}^{\perp_{\frac{e}{2}}}$) is an $[n, n-k]_q$ MDS code. Hence, it follows from Lemma IV.2 and Corollary IV.1 that there exist $[[n, k-\dim(Hull_H(\mathcal{C})), n-k+1; n-k-\dim(Hull_H(\mathcal{C}))]]_{\sqrt{q}}$ and $[[n, n-k-\dim(Hull_H(\mathcal{C})), k+1; k-\dim(Hull_H(\mathcal{C}))]]_{\sqrt{q}}$ EAQECCs.

Generally speaking, the comparison of the QECCs (including the EAQECCs) over different fields makes no sense. Therefore, from now on, when we compare the EAQECCs for different ℓ, the EAQECCs for the Hermitian case $\ell = \frac{e}{2}$ refer to the q-ary EAQECCs produced by the q-ary MDS codes (see Corollary IV.1) rather than the $\sqrt{q}$-ary EAQECCs produced by the q-ary MDS codes (see Remark IV.2).

By combining Theorems III.1-III.3 with Corollary IV.1, we can construct the following three families of EAQECCs with relatively large minimum distance.

Theorem IV.1: Let $q = p^e$ with p being an odd prime number. Assume $2\ell \mid e$. Let $n = \frac{t(q-1)}{p^\ell - 1}$ for each $1 \le t \le p^\ell - 1$. Then, for any $1 \le k \le \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$,

(1) there exists an $[[n, k-h, n-k+1; n-k-h]]_q$ EAQECC with relatively large minimum distance for any $0 \le h \le k-1$;

(2) there exists an $[[n+1, k-h, n-k+2; n-k-h+1]]_q$ EAQECC with relatively large minimum distance for any $0 \le h \le k$;

(3) there exists an $[[n+2, k-h, n-k+3; n-k-h+2]]_q$ EAQECC with relatively large minimum distance for any $0 \le h \le k-1$.

Remark IV.3: By Remark III.1, we know that the $[[n, k, n-k+1; n-k]]_q$, $[[n+1, k, n-k+2; n-k+1]]_q$ and $[[n+2, k, n-k+3; n-k+2]]_q$ EAQECCs (take $h = 0$) in Theorem IV.1 with dimension q^k satisfying $\lfloor \frac{p^{\frac{e}{2}}+n}{p^{\frac{e}{2}}+1} \rfloor + 1 \le k \le \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$ for any $1 \le \ell < \frac{e}{2}$ with $2\ell \mid e$ ecannot be obtained by considering the Hermitian case. For example, as shown in Remark III.1, by taking $p = 5$, $e = 4$, $\ell = 1$ and $t = 1$ in Theorem IV.1 we know that the $[[156, k, 157-k; 156-k]]_{5^4}$, $[[157, k, 158-k; 157-k]]_{5^4}$ and $[[158, k, 159-k; 158-k]]_{5^4}$ EAQECCs for each $7 \le k \le 26$ derived from Theorem IV.1 cannot be produced by considering the Hermitian case $\ell = 2$. Note that if e is even in Theorem IV.1, then by Remark IV.2, there exist $[[n+n', k-h, n-k+n'+1; n-k-h+n']]_{\sqrt{q}}$ and $[[n+n', n-k-h+n', k+1; k-h]]_{\sqrt{q}}$ EAQECCs for $n = t(\sqrt{q}+1)$ and $n' = 0, 1, 2$, where $1 \le t \le \sqrt{q}-1$ and $1 \le k \le \lfloor \frac{\sqrt{q}+n}{\sqrt{q}+1} \rfloor$.

Next, in terms of Theorems III.4-III.6 and Corollary IV.1, we obtain three families of EAQECCs with relatively large minimum distance in the following theorem.

Theorem IV.2: Let $q = p^e$ with p being an odd prime number. Assume $2\ell \mid e$, $(q-1) \mid \mathrm{lcm}(x_1, x_2)$ and $\frac{q-1}{p^\ell-1} \mid x_1$ for two positive integers x_1 and x_2. Let $n = \frac{r(q-1)}{\gcd(x_2, q-1)}$ for each $1 \le r \le \frac{q-1}{\gcd(x_1, q-1)}$. Then, for any $1 \le k \le \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$,

(1) there exists an $[[n, k-h, n-k+1; n-k-h]]_q$ EAQECC with relatively large minimum distance for any $0 \le h \le k-1$;

(2) there exists an $[[n+1, k-h, n-k+2; n-k-h+1]]_q$ EAQECC with relatively large minimum distance for any $0 \le h \le k$;

(3) there exists an $[[n+2, k-h, n-k+3; n-k-h+2]]_q$ EAQECC with relatively large minimum distance for any $0 \le h \le k-1$.

Remark IV.4: By Remark III.3, we know that the $[[n, k, n-k+1; n-k]]_q$, $[[n+1, k, n-k+2; n-k+1]]_q$ and $[[n+2, k, n-k+3; n-k+2]]_q$ EAQECCs (take $h = 0$) in Theorem IV.2 with dimension q^k satisfying $\lfloor \frac{p^{\frac{e}{2}}+n}{p^{\frac{e}{2}}+1} \rfloor + 1 \le k \le \lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$ for any $1 \le \ell < \frac{e}{2}$ with $2\ell \mid e$ cannot be obtained by considering the Hermitian case. For example, as shown in Remark III.3, by taking $p = 7$, $e = 4$, $\ell = 1$, $x_1 = 2400$, $x_2 = 6$ and $r = 1$ in Theorem IV.2 we know that the $[[400, k, 401-k; 400-k]]_{7^4}$, $[[401, k, 402-k; 401-k]]_{7^4}$ and $[[402, k, 403-k; 402-k]]_{7^4}$ EAQECCs for each $9 \le k \le 50$ derived from Theorem IV.2 cannot be produced by considering the Hermitian case $\ell = 2$. Note that if e is even in Theorem IV.2, then by Remark IV.2, there exist $[[n+n', k-h, n-k+n'+1; n-k-h+n']]_{\sqrt{q}}$ and $[[n+n', n-k-h+n', k+1; k-h]]_{\sqrt{q}}$ EAQECCs for

$n = \frac{r(q-1)}{\gcd(x_2,q-1)}$ and $n' = 0, 1, 2$, where $1 \le k \le \lfloor \frac{\sqrt{q}+n}{\sqrt{q}+1} \rfloor$, $1 \le r \le \frac{q-1}{\gcd(x_1,q-1)}$, $(q-1) \mid \mathrm{lcm}(x_1, x_2)$ and $(\sqrt{q}+1) \mid x_1$.

Now, by Theorems III.7-III.9 and Corollary IV.1, we have the following three families of EAQECCs with relatively large minimum distance.

Theorem IV.3: Let $q = p^e$ with p being an odd prime number. Assume $2\ell \mid e$ and $m \mid (q-1)$. Let $n = rm$ for each $1 \le r \le \frac{p^\ell - 1}{m_1}$ with $m_1 = \frac{m}{\gcd(m,y)}$ for $y = \frac{q-1}{p^\ell - 1}$. Then, for any $1 \le k \le \lfloor \frac{p^\ell + n}{p^\ell + 1} \rfloor$,

(1) there exists an $[[n, k-h, n-k+1; n-k-h]]_q$ EAQECC with relatively large minimum distance for any $0 \le h \le k-1$;

(2) there exists an $[[n+1, k-h, n-k+2; n-k-h+1]]_q$ EAQECC with relatively large minimum distance for any $0 \le h \le k$;

(3) there exists an $[[n+2, k-h, n-k+3; n-k-h+2]]_q$ EAQECC with relatively large minimum distance for any $0 \le h \le k-1$.

Remark IV.5: By Remark III.4, for the same length n, the $[[n, k, n-k+1; n-k]]_q$, $[[n+1, k, n-k+2; n-k+1]]_q$ and $[[n+2, k, n-k+3; n-k+2]]_q$ EAQECCs (take $h = 0$) in Theorem IV.3 with dimension q^k satisfying $\lfloor \frac{p^{\frac{e}{2}} + n}{p^{\frac{e}{2}} + 1} \rfloor + 1 \le k \le \lfloor \frac{p^\ell + n}{p^\ell + 1} \rfloor$ for any $1 \le \ell < \frac{e}{2}$ with $2\ell \,|\, e$ cannot be produced by the Hermitian case. For example, as shown in Remark III.4, by taking $p = 5$, $e = 6$, $\ell = 1$, $m = 126$ and $r = 1$ in Theorem IV.3 we know that the $[[126, k, 127-k; 126-k]]_{5^6}$, $[[127, k, 128-k; 127-k]]_{5^6}$ and $[[128, k, 129-k; 128-k]]_{5^6}$ EAQECCs for $2 \le k \le 21$ derived from Theorem IV.3 cannot be produced by the Hermitian case $\ell = 3$. Note that if e is even in Theorem IV.3, then by Remark IV.2, there exist $[[n+n', k-h, n-k+n'+1; n-k-h+n']]_{\sqrt{q}}$ and $[[n+n', n-k-h+n', k+1; k-h]]_{\sqrt{q}}$ EAQECCs for $n = rm$ and $n' = 0, 1, 2$, where $1 \le k \le \lfloor \frac{\sqrt{q}+n}{\sqrt{q}+1} \rfloor$, $m \mid (q-1)$ and $1 \le r \le \frac{\sqrt{q}-1}{m_1}$ with $m_1 = \frac{m}{\gcd(m,\sqrt{q}+1)}$. The latter $\sqrt{q}$-ary EAQECCs are identical to those shown in [16, Theorem 4.9].

Finally, by Theorems III.10-III.11 and Corollary IV.1, we obtain the following two families of EAQECCs with relatively large minimum distance.

Theorem IV.4: Let $q = p^e$ with p being an odd prime number. Assume $2\ell \mid e$ and $a \mid \ell$. Let $n = tp^{aw}$ for each $1 \le t \le p^a$ and each $1 \le w \le \frac{e}{a} - 1$. Then, for any $1 \le k \le \lfloor \frac{p^\ell + n - 1}{p^\ell + 1} \rfloor$,

(1) there exists an $[[n, k-h, n-k+1; n-k-h]]_q$ EAQECC with relatively large minimum distance for any $0 \le h \le k$;

(2) there exists an $[[n+1, k-h, n-k+2; n-k-h+1]]_q$ EAQECC with relatively large minimum distance for any $0 \le h \le k-1$.

Remark IV.6: By Remark III.5, for the same length n, the $[[n, k, n-k+1; n-k]]_q$ and $[[n+1, k, n-k+2; n-k+1]]_q$ EAQECCs in Theorem IV.4 with dimension q^k satisfying $\lfloor \frac{p^{\frac{e}{2}} + n - 1}{p^{\frac{e}{2}} + 1} \rfloor + 1 \le k \le \lfloor \frac{p^\ell + n - 1}{p^\ell + 1} \rfloor$ for any $1 \le \ell < \frac{e}{2}$ with $2\ell \,|\, e$ cannot be obtained by the Hermitian case. For example, as shown in Remark III.5, by taking $p = 3$, $a = 2$, $e = 8$, $\ell = 2$, $w = 2$ and $t = 2$ in Theorem IV.4 we know that Theorem IV.4 can produce $[[162, k, 163-k; 162-k]]_{3^8}$ and $[[163, k, 164-k; 163-k]]_{3^8}$ EAQECCs for each $1 \le k \le 17$, while for the same lengths, these EAQECCs with $3 \le k \le 17$ cannot be obtained by the Hermitian case $\ell = 4$. Note that if e is even in Theorem IV.4, then by Remark IV.2, there exist $[[n+n', k-h, n-k+n'+1; n-k-h+n']]_{\sqrt{q}}$ and $[[n+n', n-k-h+n', k+1; k-h]]_{\sqrt{q}}$ EAQECCs for $n = tp^{aw}$ and $n' = 0, 1$, where $1 \le k \le \lfloor \frac{\sqrt{q}+n-1}{\sqrt{q}+1} \rfloor$, $1 \le t \le p^a$, $a \mid \frac{e}{2}$ and $1 \le w \le \frac{e}{a} - 1$. The latter $\sqrt{q}$-ary EAQECCs are identical to those shown in [16, Theorem 4.8].

TABLE I

NEW EAQECCS FROM THEOREM IV.1 FOR $p = 5$, $e = 4, \ell = 1$ AND $t = 2, 3$

New EAQECCs for $n = 312$	New EAQECCs for $n = 468$
$[[312, 13, 300; 299]]_{5^4}$	$[[468, 19, 450; 449]]_{5^4}$
$[[312, 14, 299; 298]]_{5^4}$	$[[468, 20, 449; 448]]_{5^4}$
$[[312, 15, 298; 297]]_{5^4}$	$[[468, 21, 448; 447]]_{5^4}$
$\vdots$	$\vdots$
$[[312, 51, 262; 261]]_{5^4}$	$[[468, 77, 392; 391]]_{5^4}$
$[[312, 52, 261; 260]]_{5^4}$	$[[468, 78, 391; 390]]_{5^4}$
$[[313, 13, 301; 300]]_{5^4}$	$[[469, 19, 451; 450]]_{5^4}$
$[[313, 14, 300; 299]]_{5^4}$	$[[469, 20, 450; 449]]_{5^4}$
$[[313, 15, 299; 298]]_{5^4}$	$[[469, 21, 449; 448]]_{5^4}$
$\vdots$	$\vdots$
$[[313, 51, 263; 262]]_{5^4}$	$[[469, 77, 393; 392]]_{5^4}$
$[[313, 52, 262; 261]]_{5^4}$	$[[469, 78, 392; 391]]_{5^4}$
$[[314, 13, 302; 301]]_{5^4}$	$[[470, 19, 452; 451]]_{5^4}$
$[[314, 14, 301; 300]]_{5^4}$	$[[470, 20, 451; 450]]_{5^4}$
$[[314, 15, 300; 299]]_{5^4}$	$[[470, 21, 450; 449]]_{5^4}$
$\vdots$	$\vdots$
$[[314, 51, 264; 263]]_{5^4}$	$[[470, 77, 394; 393]]_{5^4}$
$[[314, 52, 263; 262]]_{5^4}$	$[[470, 78, 393; 392]]_{5^4}$

Remark IV.7: As we know, it is not easy to construct an $[[n'', k'', d''; c'']]_q$ EAQECC with $2d'' = n'' - k'' + 2 + c''$ such that the value of the copies of maximally entangled states c'' is flexible. Note that the parameter c'' of many EAQECCs constructed in the literature is fixed (for example, see [10], [11], [13], [29], [36], [42], [45], [49]). Observing the EAQECCs in Theorems IV.1-IV.4, we know that their parameters are flexible. Besides, their relatively large minimum distance means that they have good error detection and error correction capabilities.

From Theorems IV.1-IV.4, we can expect a myriad of new EAQECCs with relatively large minimum distance. Here, we provide some examples of EAQECCs with flexible parameters in Tables I-IV. The relatively large minimum distance of these EAQECCs indicates that they have good error detection and error correction capabilities.

Apart from the example given in Remark IV.3, Table I gives some new EAQECCs from Theorem IV.1 for $p = 5, e = 4$, $\ell = 1$ and $t = 2, 3$.

Apart from the example given in Remark IV.4, Table II lists some new EAQECCs from Theorem IV.2 for $p = 3, e = 6$, $\ell = 1, x_1 = 364$, $x_2 = 24$ and $n = 91, 182$.

Apart from the example shown in Remark IV.5, Table III provides some new EAQECCs from Theorem IV.3 for $p = 5, e = 6, \ell = 1, m = 186, r = 1, n = 186$ and $p = 7, e = 4, \ell = 1, m = 50, r = 4, n = 200$, respectively.

TABLE II

NEW EAQECCS FROM THEOREM IV.2 FOR $p=3, e=6$, $\ell=1, x_1=364$ AND $x_2=24$

New EAQECCs for $n=91$	New EAQECCs for $n=182$
$[[91,5,87;86]]_{3^6}$	$[[182,8,175;174]]_{3^6}$
$[[91,6,86;85]]_{3^6}$	$[[182,9,174;173]]_{3^6}$
$[[91,7,85;84]]_{3^6}$	$[[182,10,173;172]]_{3^6}$
$\vdots$	$\vdots$
$[[91,22,70;69]]_{3^6}$	$[[182,45,138;137]]_{3^6}$
$[[91,23,69;68]]_{3^6}$	$[[182,46,137;136]]_{3^6}$
$[[92,5,88;87]]_{3^6}$	$[[183,8,176;175]]_{3^6}$
$[[92,6,87;86]]_{3^6}$	$[[183,9,175;174]]_{3^6}$
$[[92,7,86;85]]_{3^6}$	$[[183,10,174;173]]_{3^6}$
$\vdots$	$\vdots$
$[[92,22,71;70]]_{3^6}$	$[[183,45,139;138]]_{3^6}$
$[[92,23,70;69]]_{3^6}$	$[[183,46,138;137]]_{3^6}$
$[[93,5,89;88]]_{3^6}$	$[[184,8,177;176]]_{3^6}$
$[[93,6,88;87]]_{3^6}$	$[[184,9,176;175]]_{3^6}$
$[[93,7,87;86]]_{3^6}$	$[[184,10,175;174]]_{3^6}$
$\vdots$	$\vdots$
$[[93,22,72;71]]_{3^6}$	$[[184,45,140;139]]_{3^6}$
$[[93,23,71;70]]_{3^6}$	$[[184,46,139;138]]_{3^6}$

TABLE III

NEW EAQECCS FROM THEOREM IV.3 FOR $p=5, e=6, \ell=1$, $m=186, r=1$ AND $p=7, e=4, \ell=1, m=50, r=4$

New EAQECCs for $n=186$	New EAQECCs for $n=200$
$[[186,3,184;183]]_{5^6}$	$[[200,5,196;195]]_{7^4}$
$[[186,4,183;182]]_{5^6}$	$[[200,6,195;194]]_{7^4}$
$[[186,5,182;181]]_{5^6}$	$[[200,7,194;193]]_{7^4}$
$\vdots$	$\vdots$
$[[186,30,157;156]]_{5^6}$	$[[200,24,177;176]]_{7^4}$
$[[186,31,156;155]]_{5^6}$	$[[200,25,176;175]]_{7^4}$
$[[187,3,185;184]]_{5^6}$	$[[201,5,197;196]]_{7^4}$
$[[187,4,184;183]]_{5^6}$	$[[201,6,196;195]]_{7^4}$
$[[187,5,183;182]]_{5^6}$	$[[201,7,195;194]]_{7^4}$
$\vdots$	$\vdots$
$[[187,30,158;157]]_{5^6}$	$[[201,24,178;177]]_{7^4}$
$[[187,31,157;156]]_{5^6}$	$[[201,25,177;176]]_{7^4}$
$[[188,3,186;185]]_{5^6}$	$[[202,5,198;197]]_{7^4}$
$[[188,4,185;184]]_{5^6}$	$[[202,6,197;196]]_{7^4}$
$[[188,5,184;183]]_{5^6}$	$[[202,7,196;195]]_{7^4}$
$\vdots$	$\vdots$
$[[188,30,159;158]]_{5^6}$	$[[202,24,179;178]]_{7^4}$
$[[188,31,158;157]]_{5^6}$	$[[202,25,178;177]]_{7^4}$

Finally, apart from the example shown in Remark IV.6, Table IV also lists some new EAQECCs from Theorem IV.4 for $p=7, e=6, \ell=1, a=1, w=2, t=4, n=196$ and $p=13, e=4, \ell=1, a=1, w=2, t=2, n=338$, respectively.

TABLE IV

NEW EAQECCS FROM THEOREM IV.4 FOR $p=7, e=6, \ell=1$, $a=1, w=2, t=4$ AND $p=13, e=4, \ell=1, a=1, w=2, t=2$

New EAQECCs for $n=196$	New EAQECCs for $n=338$
$[[196,2,195;194]]_{7^6}$	$[[338,3,336;335]]_{13^4}$
$[[196,3,194;193]]_{7^6}$	$[[338,4,335;334]]_{13^4}$
$[[196,4,193;192]]_{7^6}$	$[[338,5,334;333]]_{13^4}$
$\vdots$	$\vdots$
$[[196,24,173;172]]_{7^6}$	$[[338,24,315;314]]_{13^4}$
$[[196,25,172;171]]_{7^6}$	$[[338,25,314;313]]_{13^4}$
$[[197,2,196;195]]_{7^6}$	$[[339,3,337;336]]_{13^4}$
$[[197,3,195;194]]_{7^6}$	$[[339,4,336;335]]_{13^4}$
$[[197,4,194;193]]_{7^6}$	$[[339,5,335;334]]_{13^4}$
$\vdots$	$\vdots$
$[[197,24,174;173]]_{7^6}$	$[[339,24,316;315]]_{13^4}$
$[[197,25,173;172]]_{7^6}$	$[[339,25,315;314]]_{13^4}$

V. DISCUSSION ON THE LENGTHS OF OUR EAQECCS IN THEOREMS IV.1-IV.4

Inspired by the reviewers' insightful comments, it is meaningful and necessary to make a detailed explanation for why we further develop the theory on ℓ-Galois hulls of MDS codes in the previous sections to construct new families of EAQECCs. To be specific, the main advantages of this work are reflected in the following two aspects:

Advantage 1: As revealed in Sections III and IV (e.g., see Remarks IV.3-IV.6), the range of the dimension q^k of the $[[n+\hat{a}, k, n-k+\hat{a}+1; n-k+\hat{a}]]_q$ ($\hat{a}=0,1,2$ and take $h=0$) EAQECCs in Theorems IV.1-IV.3 and the $[[n+\hat{b}, k, n-k+\hat{b}+1; n-k+\hat{b}]]_q$ ($\hat{b}=0,1$ and take $h=0$) EAQECCs in Theorem IV.4 for any $1 \leq \ell < \frac{e}{2}$ with $2\ell \mid e$ is wider than those for the Hermitian case $\ell=\frac{e}{2}$. In particular, when $\ell=1$, the upper bound $\lfloor \frac{p^\ell+n-1}{p^\ell+1} \rfloor$ or $\lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$ of k attains a maximum.

Advantage 2: For each theorem of Theorems IV.1-IV.4, the variables ℓ with $2\ell \mid e$ correspond to EAQECCs with different kinds of length sets because the length n therein is related to ℓ. This allows us to obtain different kinds of EAQECCs in each theorem of Theorems IV.1-IV.4 through different variables ℓ. More specifically, in each theorem of Theorems IV.1-IV.4:

(1) For each $\ell \neq 1, \frac{e}{2}$, the corresponding kind of EAQECCs has some EAQECCs whose lengths cannot be obtained by those derived from $\ell=1$;

(2) For certain $\ell=\ell_1 \neq 1, \frac{e}{2}$, the corresponding kind of EAQECCs has some EAQECCs whose lengths cannot be obtained by those derived from certain $\ell=\ell_2 \neq 1, \frac{e}{2}$, where $\ell_1 \neq \ell_2$.

To finish this section and verify our statement in **Advantage 2**, we will provide some examples and several tables (see Tables V, VI, VII and VIII) containing parameters of EAQECCs derived from Theorems IV.1-IV.4 that possess different kinds of length sets by considering $\ell=1,2,3$ (see Subsections V-A and V-D) and $\ell=1,2$ (see Subsections V-B and V-C), and have larger dimension that cannot be yielded from those by considering the Hermitian case.

It seems that the sets of length n in Theorems IV.1 and IV.2 are either identical, or, one of the two sets is contained in the other one. In fact, that is not the case. As a sample, for $p=3$, $e=8$ and $\ell=2$, Table IX will supply some lengths coming from the set of length n in Theorem IV.1 (resp. Theorem IV.2)

that cannot be obtained by the set of length n in Theorem IV.2 (resp. Theorem IV.1).

We need to fix some notations which will be used in the sequel. For any two integers x, y with $x < y$, denote by $[x, y]$ the set consisting of the integers $x, x+1, \ldots, y$. For any two sets A and B, define their *difference* by $A\backslash B = \{x | x \in A,\ x \notin B\}$. The symbol $A_1 \sqcup A_2 \sqcup \cdots \sqcup A_m$ represents the union of the mutually disjoint sets $A_1, A_2, \ldots, A_m$.

A. Length $n = \frac{t(q-1)}{p^\ell - 1}$ for $1 \le t \le p^\ell - 1$ and $2\ell \mid e$ in Theorem IV.1

In this subsection, let us consider $p = 5$, $e = 12$ and $\ell = \ell_i = i$ for $i = 1, 2, 3$ in Theorem IV.1. In this case, we have that $q - 1 = 5^{12} - 1 = 2^4 \cdot 3^2 \cdot 7 \cdot 13 \cdot 31 \cdot 601$. In what follows, let us compute the sets of length $n = \frac{t(q-1)}{p^\ell - 1}$ for the cases $\ell = \ell_i = i$, where $i = 1, 2, 3$. For convenience, we denote by $X_1(t)$, $X_2(t)$ and $X_3(t)$ the corresponding sets of length $n = \frac{t(q-1)}{p^\ell - 1}$ for $\ell = \ell_1 = 1$, $\ell = \ell_2 = 2$ and $\ell = \ell_3 = 3$, respectively.

1. For $\ell = \ell_1 = 1$, we have $n = t \cdot 2^2 \cdot 3^2 \cdot 7 \cdot 13 \cdot 31 \cdot 601$ for each $1 \le t \le 2^2$, then

$$X_1(t) = \{t \cdot 2^2 \cdot 3^2 \cdot 7 \cdot 13 \cdot 31 \cdot 601 | 1 \le t \le 2^2\}.$$

2. For $\ell = \ell_2 = 2$, we have $n = t \cdot 2 \cdot 3 \cdot 7 \cdot 13 \cdot 31 \cdot 601$ for each $1 \le t \le 2^3 \cdot 3$, then

$$X_2(t) = \{t \cdot 2 \cdot 3 \cdot 7 \cdot 13 \cdot 31 \cdot 601 | 1 \le t \le 2^3 \cdot 3\}.$$

3. For $\ell = \ell_3 = 3$, we have $n = t \cdot 2^2 \cdot 3^2 \cdot 7 \cdot 13 \cdot 601$ for each $1 \le t \le 2^2 \cdot 31$, then

$$X_3(t) = \{t \cdot 2^2 \cdot 3^2 \cdot 7 \cdot 13 \cdot 601 | 1 \le t \le 2^2 \cdot 31\}.$$

In order to determine the length set $X_i(t)\backslash X_j(t)$ for each $1 \le i \ne j \le 3$, we need to compute the sets $X_1(t) \cap X_2(t)$, $X_1(t) \cap X_3(t)$ and $X_2(t) \cap X_3(t)$. We first consider $X_1(t) \cap X_2(t)$. Suppose there exist $1 \le t_1 \le 2^2$ and $1 \le t_2 \le 2^3 \cdot 3$ such that $t_1 \cdot 2^2 \cdot 3^2 \cdot 7 \cdot 13 \cdot 31 \cdot 601 = t_2 \cdot 2 \cdot 3 \cdot 7 \cdot 13 \cdot 31 \cdot 601$, then $t_2 = 6t_1$, i.e., $(t_1, t_2) = (i, 6i)$ for $i = 1, 2, 3, 4$. Therefore, $X_1(t) \cap X_2(t) = X_1(t)$, which implies that $X_1(t) \subset X_2(t)$. Similarly, we obtain $X_1(t) \cap X_3(t) = X_1(t)$ and hence $X_1(t) \subset X_3(t)$.

Now, let us compute $X_2(t) \cap X_3(t)$. Suppose there exist $1 \le t_2 \le 2^3 \cdot 3$ and $1 \le t_3 \le 2^2 \cdot 31$ such that $t_2 \cdot 2 \cdot 3 \cdot 7 \cdot 13 \cdot 31 \cdot 601 = t_3 \cdot 2^2 \cdot 3^2 \cdot 7 \cdot 13 \cdot 601$, hence $31t_2 = 6t_3$, i.e., $(t_2, t_3) = (6i, 31i)$ for $i = 1, 2, 3, 4$ and therefore

$$\begin{aligned} X_2(t) \cap X_3(t) &= \{X_2(6), X_2(12), X_2(18), X_2(24)\} \\ &= \{X_3(31), X_3(62), X_3(93), X_3(124)\} \\ &= X_1(t). \end{aligned}$$

Remark V.1: For $\ell = 1, 2, 3$, Table V lists the corresponding $[[n, k, n-k+1; n-k]]_{5^{12}}$ EAQECCs derived from Theorem IV.1 with length sets $X_1(t)$, $X_2(t)$ and $X_3(t)$, respectively. Moreover, Table V also gives the corresponding $[[n, k, n-k+1; n-k]]_{5^{12}}$ EAQECCs of length n coming from $X_2(t)\backslash X_1(t)$, $X_2(t)\backslash X_3(t)$, $X_3(t)\backslash X_1(t)$ and $X_3(t)\backslash X_2(t)$, respectively, with dimension 5^{12k} satisfying $\left\lfloor \frac{5^6+n}{5^6+1} \right\rfloor + 1 \le k \le \left\lfloor \frac{25+n}{26} \right\rfloor$ or $\left\lfloor \frac{5^6+n}{5^6+1} \right\rfloor + 1 \le k \le \left\lfloor \frac{125+n}{126} \right\rfloor$ that cannot be obtained by the Hermitian case $\ell = 6$. From Table V, we see that 20 of the 24 kinds of lengths in $X_2(t)$ for $\ell = \ell_2 = 2$ cannot be produced by $X_1(t)$ for $\ell = \ell_1 = 1$, and 120 of the 124 kinds of lengths in $X_3(t)$ for $\ell = \ell_3 = 3$ cannot be produced by $X_1(t)$ for $\ell = \ell_1 = 1$. Moreover, 20 of the 24 kinds of lengths in $X_2(t)$ for $\ell = \ell_2 = 2$ cannot be produced by $X_3(t)$ for $\ell = \ell_3 = 3$, and 120 of the 124 kinds of lengths in $X_3(t)$ for $\ell = \ell_3 = 3$ cannot be produced by $X_2(t)$ for $\ell = \ell_2 = 2$.

B. Length $n = \frac{r(q-1)}{\gcd(x_2, q-1)}$ for $(q-1) \mid \mathrm{lcm}(x_1, x_2)$, $\frac{q-1}{p^\ell - 1} \mid x_1$, $1 \le r \le \frac{q-1}{\gcd(x_1, q-1)}$ and $2\ell \mid e$ in Theorem IV.2

Since $\frac{q-1}{p^\ell - 1} \mid x_1$, there exists a positive integer t_1 such that $x_1 = \frac{q-1}{p^\ell - 1} t_1$. Then, we obtain that $\gcd(x_1, q-1) = \frac{q-1}{p^\ell - 1} \gcd(t_1, p^\ell - 1)$. Hence, the upper bound $\frac{q-1}{\gcd(x_1, q-1)}$ of r becomes $\frac{p^\ell - 1}{\gcd(t_1, p^\ell - 1)}$. Therefore, the length n in Theorem IV.2 can be expressed as $n = \frac{r(q-1)}{\gcd(x_2, q-1)}$, where $(q-1) \mid \mathrm{lcm}(\frac{q-1}{p^\ell - 1} t_1, x_2)$ and $1 \le r \le \frac{p^\ell - 1}{\gcd(t_1, p^\ell - 1)}$.

In this subsection, let us consider $p = 3$, $e = 8$ and $\ell = \ell_i = i$ for $i = 1, 2$ in Theorem IV.2. In this case, we obtain $q - 1 = 3^8 - 1 = 2^5 \cdot 5 \cdot 41$. For convenience, we denote by Y_1 and Y_2 the corresponding sets of length $n = \frac{r(q-1)}{\gcd(x_2, q-1)}$ for $\ell = \ell_1 = 1$ and $\ell = \ell_2 = 2$, respectively.

1. For $\ell = \ell_1 = 1$, we have that

$$n = \frac{r \cdot 2^5 \cdot 5 \cdot 41}{\gcd(x_2, 2^5 \cdot 5 \cdot 41)},$$

where $2^5 \cdot 5 \cdot 41 \mid \mathrm{lcm}(2^4 \cdot 5 \cdot 41 \cdot t_1, x_2)$ and $1 \le r \le \frac{2}{\gcd(t_1, 2)}$.

Case (1.1): When $\gcd(t_1, 2) = 1$, we have $2^5 \mid x_2$. Write $x_2 = 2^5 x_2'$ for any positive integer x_2'. Then $n = \frac{r \cdot 5 \cdot 41}{\gcd(x_2', 5 \cdot 41)}$ for $1 \le r \le 2$, which implies that the set of length n, denoted by $Y_{1,1}$, is

$$Y_{1,1} = \{r \cdot 5^b \cdot 41^c | 1 \le r \le 2,\ 0 \le b, c \le 1\}. \tag{23}$$

Case (1.2): When $\gcd(t_1, 2) = 2$, we have $2 \mid t_1$, implying that x_2 can be taken as any positive integer. Then, the set of length n, denoted by $Y_{1,2}$, is

$$Y_{1,2} = \{2^a \cdot 5^b \cdot 41^c | 0 \le a \le 5,\ 0 \le b, c \le 1\}. \tag{24}$$

Combining Eq. (23) with Eq. (24), we know that the set of length n for $\ell = \ell_1 = 1$ is

$$Y_1 = Y_{1,1} \cup Y_{1,2} = Y_{1,2}.$$

2. For $\ell = \ell_2 = 2$, we have that

$$n = \frac{r \cdot 2^5 \cdot 5 \cdot 41}{\gcd(x_2, 2^5 \cdot 5 \cdot 41)},$$

where $2^5 \cdot 5 \cdot 41 \mid \mathrm{lcm}(2^2 \cdot 5 \cdot 41 \cdot t_1, x_2)$ and $1 \le r \le \frac{8}{\gcd(t_1, 8)}$.

Case (2.1): When $\gcd(t_1, 8) = 1$, we have $2^5 \mid x_2$. Write $x_2 = 2^5 x_2'$ for any positive integer x_2'. Then $n = \frac{r \cdot 5 \cdot 41}{\gcd(x_2', 5 \cdot 41)}$ for $1 \le r \le 8$. Thus, the set of the length n, denoted by $Y_{2,1}$, is

$$Y_{2,1} = \{r \cdot 5^b \cdot 41^c | 1 \le r \le 8,\ 0 \le b, c \le 1\}. \tag{25}$$

TABLE V
PARAMETERS OF THE $[[n, k, n-k+1; n-k]]_{5^{12}}$ EAQECCS IN THEOREM IV.1

ℓ	Length set	Cardinality	Length n	t	k
1	$X_1(t)$	4	$t \cdot 2^2 \cdot 3^2 \cdot 7 \cdot 13 \cdot 31 \cdot 601$	$[1, 4]$	$\left[1, \lfloor \frac{5+n}{6} \rfloor\right]$
2	$X_2(t)$	24	$t \cdot 2 \cdot 3 \cdot 7 \cdot 13 \cdot 31 \cdot 601$	$[1, 24]$	$\left[1, \lfloor \frac{25+n}{26} \rfloor\right]$
3	$X_3(t)$	124	$t \cdot 2^2 \cdot 3^2 \cdot 7 \cdot 13 \cdot 601$	$[1, 124]$	$\left[1, \lfloor \frac{125+n}{126} \rfloor\right]$
2	$X_2(t)\backslash X_1(t)$	20	$t \cdot 2 \cdot 3 \cdot 7 \cdot 13 \cdot 31 \cdot 601$	$[1, 23]\backslash\{6, 12, 18\}$	$\left[\lfloor \frac{5^6+n}{5^6+1} \rfloor + 1, \lfloor \frac{25+n}{26} \rfloor\right]$
2	$X_2(t)\backslash X_3(t)$	20	$t \cdot 2 \cdot 3 \cdot 7 \cdot 13 \cdot 31 \cdot 601$	$[1, 23]\backslash\{6, 12, 18\}$	$\left[\lfloor \frac{5^6+n}{5^6+1} \rfloor + 1, \lfloor \frac{25+n}{26} \rfloor\right]$
3	$X_3(t)\backslash X_1(t)$	120	$t \cdot 2^2 \cdot 3^2 \cdot 7 \cdot 13 \cdot 601$	$[1, 123]\backslash\{31, 62, 93\}$	$\left[\lfloor \frac{5^6+n}{5^6+1} \rfloor + 1, \lfloor \frac{125+n}{126} \rfloor\right]$
3	$X_3(t)\backslash X_2(t)$	120	$t \cdot 2^2 \cdot 3^2 \cdot 7 \cdot 13 \cdot 601$	$[1, 123]\backslash\{31, 62, 93\}$	$\left[\lfloor \frac{5^6+n}{5^6+1} \rfloor + 1, \lfloor \frac{125+n}{126} \rfloor\right]$

TABLE VI
PARAMETERS OF THE $[[n, k, n-k+1; n-k]]_{3^8}$ EAQECCS IN THEOREM IV.2

ℓ	Length set	Cardinality	Length n	a, b, c	k
1	Y_1	24	$2^a \cdot 5^b \cdot 41^c$	$a \in [0, 5]; b, c \in [0, 1]$	$\left[1, \lfloor \frac{3+n}{4} \rfloor\right]$
2	Y_2	38	$2^a \cdot 5^b \cdot 41^c$	$a \in [0, 5]; b, c \in [0, 1]$	$\left[1, \lfloor \frac{9+n}{10} \rfloor\right]$
			$3 \cdot 5^b \cdot 41^c$	$b, c \in [0, 1]$	$\left[1, \lfloor \frac{9+n}{10} \rfloor\right]$
			$5^2 \cdot 41^c$	$c \in [0, 1]$	$\left[1, \lfloor \frac{9+n}{10} \rfloor\right]$
			$6 \cdot 5^b \cdot 41^c$	$b, c \in [0, 1]$	$\left[1, \lfloor \frac{9+n}{10} \rfloor\right]$
			$7 \cdot 5^b \cdot 41^c$	$b, c \in [0, 1]$	$\left[1, \lfloor \frac{9+n}{10} \rfloor\right]$
2	$Y_2\backslash Y_1$	14	$3 \cdot 5^b \cdot 41^c$	$b, c \in [0, 1]$	$\left[1, \lfloor \frac{9+n}{10} \rfloor\right]$
			$5^2 \cdot 41^c$	$c \in [0, 1]$	$\left[1, \lfloor \frac{9+n}{10} \rfloor\right]$
			$6 \cdot 5^b \cdot 41^c$	$b, c \in [0, 1]$	$\left[1, \lfloor \frac{9+n}{10} \rfloor\right]$
			$7 \cdot 5^b \cdot 41^c$	$b, c \in [0, 1]$	$\left[1, \lfloor \frac{9+n}{10} \rfloor\right]$

Case (2.2): When $\gcd(t_1, 8) = 2$, we have $2 \mid t_1$ and $4 \nmid t_1$, and hence $2^5 \mid x_2$. Similarly, the set of length n, denoted by $Y_{2,2}$, is

$$Y_{2,2} = \{r \cdot 5^b \cdot 41^c | 1 \le r \le 4,\ 0 \le b, c \le 1\}. \tag{26}$$

Case (2.3): When $\gcd(t_1, 8) = 4$, we have $4 \mid t_1$ and $8 \nmid t_1$, and hence $2^5 \mid x_2$. Thus, the set of length n, denoted by $Y_{2,3}$, is

$$Y_{2,3} = \{r \cdot 5^b \cdot 41^c | 1 \le r \le 2,\ 0 \le b, c \le 1\}. \tag{27}$$

Case (2.4): When $\gcd(t_1, 8) = 8$, we have $8 \mid t_1$, implying that x_2 can be taken as any positive integer. Then the set of length n, denoted by $Y_{2,4}$, is

$$Y_{2,4} = \{2^a \cdot 5^b \cdot 41^c | 0 \le a \le 5,\ 0 \le b, c \le 1\}. \tag{28}$$

By Eqs. (25)-(28), we know that the set of length n for $\ell = \ell_2 = 2$ is

$$Y_2 = \cup_{i=1}^{4} Y_{2,i} = Y_{2,1} \cup Y_{2,4} = Y_{2,1} \cup Y_{1,2}.$$

Then, we know that $Y_1 \subset Y_2$. To determine $Y_2\backslash Y_1$, it suffices to compute $Y_{2,1} \cap Y_{1,2}$. Now, comparing the elements in sets $Y_{2,1}$ and $Y_{1,2}$ gives rise to

$$Y_{2,1} \cap Y_{1,2} = \{2^a \cdot 5^b \cdot 41^c | 0 \le a \le 3,\ 0 \le b, c \le 1\}.$$

Remark V.2: As is clear from above, one can verify that $|Y_{2,1}| = 30$, $|Y_{1,2}| = 24$ and $|Y_{2,1} \cap Y_{1,2}| = 16$. Hence, we deduce that 14 of the 38 kinds of lengths in Y_2 for $\ell = \ell_2 = 2$ cannot be produced by Y_1 for $\ell = \ell_1 = 1$. These 14 kinds of lengths are: (i) $n = 3 \cdot 5^b \cdot 41^c$ for each $0 \le b, c \le 1$ (take $r = 3$ in $Y_{2,1}$); (ii) $n = 5^2 \cdot 41^c$ for each $0 \le c \le 1$ (take $r = 5$ and $b = 1$ in $Y_{2,1}$); (iii) $n = 6 \cdot 5^b \cdot 41^c$ for each $0 \le b, c \le 1$ (take $r = 6$ in $Y_{2,1}$); (iv) $n = 7 \cdot 5^b \cdot 41^c$ for each $0 \le b, c \le 1$ (take $r = 7$ in $Y_{2,1}$). In Table VI, we list the corresponding $[[n, k, n-k+1; n-k]]_{3^8}$ EAQECCs for $\ell = 1, 2$ derived from Theorem IV.2 with length n coming from Y_1, Y_2 and $Y_2\backslash Y_1$, respectively. We note that all the EAQECCs of length n (except $n = 3, 6, 7$) taken from $Y_2\backslash Y_1$ with dimension 3^{8k} satisfying $\left\lfloor \frac{81+n}{82} \right\rfloor + 1 \le k \le \lfloor \frac{9+n}{10} \rfloor$ cannot be produced by considering the Hermitian case $\ell = 4$.

C. Length $n = rm$ for $1 \le r \le \frac{p^\ell - 1}{m_1}$, $m_1 = \frac{m}{\gcd(m, \frac{q-1}{p^\ell - 1})}$, $m \mid (q-1)$ and $2\ell \mid e$ in Theorem IV.3

First, we give the following lemma.

Lemma V.1: Let $q = p^e$ with p being a prime number. Assume that $\ell \mid e$. Define

$$F(\ell) = (p^\ell - 1)\gcd\Big(m, \frac{q-1}{p^\ell - 1}\Big),$$

where m is a fixed positive integer. For any two positive integers ℓ_1, ℓ_2 satisfying $\ell_1 \mid e$ and $\ell_2 \mid e$, if $\ell_1 \mid \ell_2$, then $F(\ell_1) \le F(\ell_2)$ holds.

Proof: Since $\ell_1 \mid e$, $\ell_2 \mid e$ and $\ell_1 \mid \ell_2$, we obtain that

$$\begin{aligned} F(\ell_1) &= (p^{\ell_1}-1)\mathrm{gcd}\Big(m, \frac{q-1}{p^{\ell_2}-1}\cdot\frac{p^{\ell_2}-1}{p^{\ell_1}-1}\Big) \\ &\le (p^{\ell_1}-1)\mathrm{gcd}\Big(m, \frac{q-1}{p^{\ell_2}-1}\Big)\cdot\frac{p^{\ell_2}-1}{p^{\ell_1}-1} \\ &= (p^{\ell_2}-1)\mathrm{gcd}\Big(m, \frac{q-1}{p^{\ell_2}-1}\Big) \\ &= F(\ell_2), \end{aligned}$$

which completes the proof. ∎

Observing the conditions in Theorem IV.3, we can rewrite the length as $n = rm$, where $1 \le r \le \frac{(p^{\ell}-1)\mathrm{gcd}\left(m, \frac{q-1}{p^{\ell}-1}\right)}{m}$, $m \mid (q-1)$ and $2\ell \mid e$. Hence, for a fixed m satisfying $m \mid (q-1)$ and for any two positive integers ℓ_1, ℓ_2 satisfying $2\ell_1 \mid e$, $2\ell_2 \mid e$ and $\ell_1 \mid \ell_2$, it follows from Lemma V.1 that the upper bound $\frac{(p^{\ell}-1)\mathrm{gcd}\left(m, \frac{q-1}{p^{\ell}-1}\right)}{m}$ of r for $\ell = \ell_2$ is wider than the one for $\ell = \ell_1$. Therefore, our EAQECCs with length $n = rm$ for $\frac{(p^{\ell_1}-1)\mathrm{gcd}\left(m, \frac{q-1}{p^{\ell_1}-1}\right)}{m} + 1 \le r \le \frac{(p^{\ell_2}-1)\mathrm{gcd}\left(m, \frac{q-1}{p^{\ell_2}-1}\right)}{m}$ coming from the case $\ell = \ell_2$ cannot be generated by the case $\ell = \ell_1$.

In this subsection, let us consider $p = 5$, $e = 8$ and $\ell = \ell_i = i$ for $i = 1, 2$ in Theorem IV.3. In this case, we know that $q - 1 = 5^8 - 1 = 2^5 \cdot 3 \cdot 13 \cdot 313$. For convenience, when fixing a positive integer m with $m \mid (5^8 - 1)$, we denote by $Z_1(r)$ and $Z_2(r)$ the corresponding sets of length $n = rm$ for $\ell = \ell_1 = 1$ and $\ell = \ell_2 = 2$, respectively. Hence, we obtain that

$$Z_1(r) = \left\{ n = rm \Big| 1 \le r \le \frac{4\mathrm{gcd}(m, 2^3 \cdot 3 \cdot 13 \cdot 313)}{m} \right\}$$

and

$$Z_2(r) = \left\{ n = rm \Big| 1 \le r \le \frac{24\mathrm{gcd}(m, 2^2 \cdot 13 \cdot 313)}{m} \right\}.$$

Remark V.3: By Lemma V.1, we know that $Z_1(r) \subset Z_2(r)$. For simplicity, we write $r_1 = \frac{4\mathrm{gcd}(m, 2^3 \cdot 3 \cdot 13 \cdot 313)}{m}$ and $r_2 = \frac{24\mathrm{gcd}(m, 2^2 \cdot 13 \cdot 313)}{m}$. Based on the previous analysis, for a fixed m with $m \mid (5^8 - 1)$, we deduce that $r_2 - r_1$ of the r_2 kinds of lengths in set $Z_2(r)$ for $\ell = \ell_2 = 2$ cannot be produced by $Z_1(r)$ for $\ell = \ell_1 = 1$. In Table VII, we list the corresponding $[[n, k, n-k+1; n-k]]_{5^8}$ EAQECCs for $\ell = 1, 2$ derived from Theorem IV.3 with length sets $Z_1(r)$ and $Z_2(r)$, respectively. Moreover, Table VII also gives the corresponding $[[n, k, n-k+1; n-k]]_{5^8}$ EAQECCs of length n coming from $Z_2(r) \backslash Z_1(r)$ with dimension 5^{8k} satisfying $\left\lfloor \frac{5^4+n}{5^4+1} \right\rfloor + 1 \le k \le \left\lfloor \frac{25+n}{26} \right\rfloor$ that cannot be obtained by the Hermitian case $\ell = 4$. In particular, for some different m with $m \mid (5^8 - 1)$, Table VII lists the corresponding $[[n, k, n-k+1; n-k]]_{5^8}$ EAQECCs with 82 kinds of lengths $n = rm$ coming from the set $Z_2(r) \backslash Z_1(r)$.

D. Length $n = tp^{aw}$ for $1 \le t \le p^a$, $1 \le w \le \frac{e}{a} - 1$, $a \mid \ell$ and $2\ell \mid e$ in Theorem IV.4

In this subsection, let us consider $p = 3$, $e = 12$ and $\ell = \ell_i = i$ for $i = 1, 2, 3$ in Theorem IV.4. For convenience, we denote by V_1, V_2 and V_3 the corresponding sets of length n in Theorem IV.4 for $\ell = \ell_1 = 1$, $\ell = \ell_2 = 2$ and $\ell = \ell_3 = 3$, respectively. Let

$$\begin{aligned} S_1 &= \{t \cdot 3^w | 1 \le t \le 3,\ 1 \le w \le 11\}, \\ S_2 &= \{t \cdot 3^{2w} | 1 \le t \le 3^2,\ 1 \le w \le 5\}, \\ S_3 &= \{t \cdot 3^{3w} | 1 \le t \le 3^3,\ 1 \le w \le 3\}. \end{aligned}$$

Though there are some repeated elements $t_i \cdot 3^{iw_i}$ in each set S_i $(i = 1, 2, 3)$ for some pairs of elements (t_i, w_i) with distinct t_is $(1 \le t_i \le 3^i)$ and distinct w_is $(1 \le w_i \le \frac{12}{i} - 1)$, one easily verifies that $|S_1| = 23$, $|S_2| = 41$ and $|S_3| = 79$. Besides, we note that

$$V_1 = S_1,\ V_2 = S_1 \cup S_2,\ V_3 = S_1 \cup S_3.$$

To determine which lengths in the set V_i are not contained in the set V_j for $i \ne j$, we need to compute the set $S_i \cap S_j$ for each $1 \le i \ne j \le 3$.

First, to determine $S_1 \cap S_2$, suppose there exist $1 \le t_1 \le 3$, $1 \le w_1 \le 11$, $1 \le t_2 \le 3^2$, $1 \le w_2 \le 5$ such that $t_1 \cdot 3^{w_1} = t_2 \cdot 3^{2w_2}$, i.e., $t_2 = 3^{w_1 - 2w_2} t_1$. Moreover, we have $w_1 - 2w_2 \in [-9, 9]$. Note that $1 \le t_1 \le 3$ and $1 \le t_2 \le 3^2$. This can be divided into four cases below.

(i): When $w_1 - 2w_2 = -1$, i.e., $(w_1, w_2) = (2i-1, i)$ for $i = 1, 2, \ldots, 5$, we have $t_1 = 3t_2$. Hence, $(t_1, t_2) = (3, 1)$. In this case, the intersection of S_1 and S_2, denoted by M_1, is

$$M_1 = \{3^{2i} | 1 \le i \le 5\}.$$

(ii): When $w_1 - 2w_2 = 0$, i.e., $(w_1, w_2) = (2i, i)$ for $i = 1, 2, \ldots, 5$, we have $t_1 = t_2$. Hence, $(t_1, t_2) = (i, i)$ for $i = 1, 2, 3$. In this case, the intersection of S_1 and S_2, denoted by M_2, is

$$M_2 = \{j \cdot 3^{2i} | 1 \le i \le 5, 1 \le j \le 3\}.$$

(iii): When $w_1 - 2w_2 = 1$, i.e., $(w_1, w_2) = (2i+1, i)$ for $i = 1, 2, \ldots, 5$, we have $t_2 = 3t_1$. Hence, $(t_1, t_2) = (i, 3i)$ for $i = 1, 2, 3$. In this case, the intersection of S_1 and S_2, denoted by M_3, is

$$M_3 = \{j \cdot 3^{2i+1} | 1 \le i \le 5, 1 \le j \le 3\}.$$

(iv): When $w_1 - 2w_2 = 2$, i.e., $(w_1, w_2) = (2i+1, i)$ for $i = 1, 2, 3, 4$, we have $t_2 = 9t_1$. Hence, $(t_1, t_2) = (1, 9)$. In this case, the intersection of S_1 and S_2, denoted by M_4, is

$$M_4 = \{3^{2i+2} | 1 \le i \le 4\}.$$

By the cases **(i)-(iv)**, we have that

$$\begin{aligned} S_1 \cap S_2 &= \cup_{i=1}^{4} M_i \\ &= \{3^i | 2 \le i \le 12\} \sqcup \{2 \cdot 3^i | 2 \le i \le 11\}. \end{aligned} \tag{29}$$

Hence, $|S_1 \cap S_2| = 21$. Since $V_2 \backslash V_1 = (S_1 \cup S_2) \backslash S_1 = S_2 \backslash S_1$, we know that

$$V_2 \backslash V_1 = \{j \cdot 3^{2i} | j = 4, 5, 7, 8,\ 1 \le i \le 5\}.$$

Hence, $|V_2 \backslash V_1| = 20$. Similar to the steps shown in the cases **(i)-(iv)**, we get that

$$S_1 \cap S_3 = \{3^i | 3 \le i \le 12\} \sqcup \{2 \cdot 3^i | 3 \le i \le 11\}. \tag{30}$$

TABLE VII
PARAMETERS OF THE $[[n, k, n-k+1; n-k]]_{5^8}$ EAQECCS IN THEOREM IV.3

ℓ	Length set	Cardinality	Length n	r	m (fixed value)	k
1	$Z_1(r)$	r_1	rm	$[1, r_1]$	$m \mid (5^8-1)$	$[1, \lfloor \frac{5+n}{6} \rfloor]$
2	$Z_2(r)$	r_2	rm	$[1, r_2]$	$m \mid (5^8-1)$	$[1, \lfloor \frac{25+n}{26} \rfloor]$
2	$Z_2(r)\backslash Z_1(r)$	r_2-r_1	rm	$[r_1+1, r_2]$	$m \mid (5^8-1)$	$[\lfloor \frac{5^4+n}{5^4+1} \rfloor + 1, \lfloor \frac{25+n}{26} \rfloor]$
2	$Z_2(r)\backslash Z_1(r)$	4	$r \cdot 2^4 \cdot 13$	$[3, 6]$	$2^4 \cdot 13$	$[\lfloor \frac{5^4+n}{5^4+1} \rfloor + 1, \lfloor \frac{25+n}{26} \rfloor]$
2	$Z_2(r)\backslash Z_1(r)$	20	$r \cdot 313$	$[5, 24]$	313	$[\lfloor \frac{5^4+n}{5^4+1} \rfloor + 1, \lfloor \frac{25+n}{26} \rfloor]$
2	$Z_2(r)\backslash Z_1(r)$	2	$r \cdot 2^5 \cdot 13$	$[2, 3]$	$2^5 \cdot 13$	$[\lfloor \frac{5^4+n}{5^4+1} \rfloor + 1, \lfloor \frac{25+n}{26} \rfloor]$
2	$Z_2(r)\backslash Z_1(r)$	20	$r \cdot 2 \cdot 313$	$[5, 24]$	$2 \cdot 313$	$[\lfloor \frac{5^4+n}{5^4+1} \rfloor + 1, \lfloor \frac{25+n}{26} \rfloor]$
2	$Z_2(r)\backslash Z_1(r)$	4	$r \cdot 3 \cdot 313$	$[5, 8]$	$3 \cdot 313$	$[\lfloor \frac{5^4+n}{5^4+1} \rfloor + 1, \lfloor \frac{25+n}{26} \rfloor]$
2	$Z_2(r)\backslash Z_1(r)$	20	$r \cdot 2^2 \cdot 313$	$[5, 24]$	$2^2 \cdot 313$	$[\lfloor \frac{5^4+n}{5^4+1} \rfloor + 1, \lfloor \frac{25+n}{26} \rfloor]$
2	$Z_2(r)\backslash Z_1(r)$	4	$r \cdot 2 \cdot 3 \cdot 313$	$[5, 8]$	$2 \cdot 3 \cdot 313$	$[\lfloor \frac{5^4+n}{5^4+1} \rfloor + 1, \lfloor \frac{25+n}{26} \rfloor]$
2	$Z_2(r)\backslash Z_1(r)$	8	$r \cdot 2^3 \cdot 313$	$[5, 12]$	$2^3 \cdot 313$	$[\lfloor \frac{5^4+n}{5^4+1} \rfloor + 1, \lfloor \frac{25+n}{26} \rfloor]$

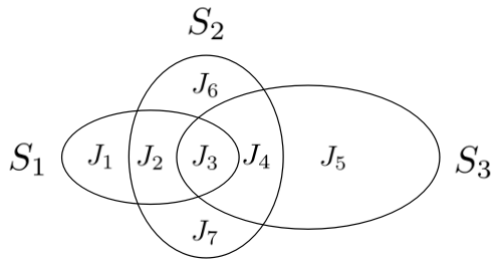

Fig. 1. Venn diagram of sets S_1, S_2 and S_3.

Then, $|S_1 \cap S_3| = 19$. Since $V_3\backslash V_1 = S_3\backslash S_1$, we obtain that

$$V_3\backslash V_1 = \{j \cdot 3^{3i} | j \in [4, 26],\ 3 \nmid j,\ 1 \le i \le 3\} \sqcup \{j \cdot 3^{3i+1} | j = 4, 5, 7, 8,\ 1 \le i \le 3\}.$$

Hence, $|V_3\backslash V_1| = 60$. In addition, we also compute that

$$S_2 \cap S_3 = \{3^i | 3 \le i \le 12\} \sqcup \{2 \cdot 3^i | i = 3, 8, 9\} \sqcup \{j \cdot 3^i | j = 2, 4, 5, 6, 7, 8,\ i = 4, 6, 10\}.$$

Then, $|S_2 \cap S_3| = 31$. Hence, we obtain that

$$S_2\backslash S_3 = \{3^2, 2 \cdot 3^2\} \sqcup \{j \cdot 3^i | j = 4, 5, 7, 8,\ i = 2, 8\}, \quad (31)$$

$$S_3\backslash S_2 = \{j \cdot 3^3 | j \in [4, 26], 3 \nmid j\} \sqcup \{j \cdot 3^6 | j \in [10, 26], 3 \nmid j\} \sqcup \{j \cdot 3^7 | j = 4, 5, 7, 8\} \sqcup \{j \cdot 3^9 | j \in [4, 26], 3 \nmid j\}. \quad (32)$$

We also notice that $S_1 \cap S_2 \cap S_3 = S_1 \cap S_3$. This means that $S_1 \cap S_3 \subset S_2$. Therefore, it will be convenient to determine the two sets $V_2\backslash V_3$ and $V_3\backslash V_2$ by using the Venn diagram of sets S_1, S_2 and S_3 (see Fig. 1, where the three ellipses represent the sets S_1, S_2 and S_3 in which, for convenience, they are divided into the disjoint subsets J_i for $i = 1, 2, \ldots, 7$ by using the relation $S_1 \cap S_3 \subset S_2$).

Based on Fig. 1, we know that $V_2\backslash V_3 = (S_1 \cup S_2)\backslash(S_1 \cup S_3) = J_6 \sqcup J_7$, $S_2\backslash S_3 = J_2 \sqcup J_6 \sqcup J_7$, $S_1 \cap S_2 = J_2 \sqcup J_3$ and $S_1 \cap S_3 = J_3$. Hence, we obtain that

$$V_2\backslash V_3 = S_2\backslash S_3 - J_2 = S_2\backslash S_3 - (S_1 \cap S_2 - S_1 \cap S_3),$$

which, together with Eqs. (29)-(31), gives rise to

$$V_2\backslash V_3 = \{j \cdot 3^i | j = 4, 5, 7, 8,\ i = 2, 8\}.$$

Hence, $|V_2\backslash V_3| = 8$. Finally, it follows from Fig. 1 that

$$V_3\backslash V_2 = (S_1 \cup S_3)\backslash(S_1 \cup S_2) = J_5 = S_3\backslash S_2,$$

as shown in Eq. (32). Hence, $|V_3\backslash V_2| = 48$.

Remark V.4: For $\ell = 1, 2, 3$, Table VIII lists the corresponding $[[n, k, n-k+1; n-k]]_{3^{12}}$ EAQECCs derived from Theorem IV.4 with length sets V_1, V_2 and V_3, respectively. Moreover, Table VIII also gives the corresponding $[[n, k, n-k+1; n-k]]_{3^{12}}$ EAQECCs of length n coming from the sets $V_2\backslash V_1$, $V_2\backslash V_3$, $V_3\backslash V_1$ and $V_3\backslash V_2$, respectively, with dimension 3^{12k} satisfying $\lfloor \frac{3^6+n-1}{3^6+1} \rfloor + 1 \le k \le \lfloor \frac{8+n}{10} \rfloor$ or $\lfloor \frac{3^6+n-1}{3^6+1} \rfloor + 1 \le k \le \lfloor \frac{26+n}{28} \rfloor$ that cannot be obtained by the Hermitian case $\ell = 6$. From Table VIII, we see that 20 of the 43 kinds of lengths in V_2 for $\ell = \ell_2 = 2$ cannot be produced by V_1 for $\ell = \ell_1 = 1$, and 60 of the 83 kinds of lengths in V_3 for $\ell = \ell_3 = 3$ cannot be produced by V_1 for $\ell = \ell_1 = 1$. Moreover, 8 of the 43 kinds of lengths in V_2 for $\ell = \ell_2 = 2$ cannot be produced by V_3 for $\ell = \ell_3 = 3$, and 48 of the 83 kinds of lengths in V_3 for $\ell = \ell_3 = 3$ cannot be produced by V_2 for $\ell = \ell_2 = 2$.

E. Comparison of the Length Sets of the EAQECCs in Theorems IV.1 and IV.2 for $p = 3$, $e = 8$ and $\ell = 2$

It seems that the sets of length n in Theorems IV.1 and IV.2 are either identical, or, one of the two sets is contained in the other one. Fortunately, that is not the case. In fact, for the same ℓ, the corresponding set of length n in Theorem IV.1 (resp. Theorem IV.2) has some lengths that cannot be produced by the set of length n in Theorem IV.2 (resp. Theorem IV.1).

To verify this statement, let us consider an example for $p = 3$, $e = 8$ and $\ell = 2$ in Theorems IV.1 and IV.2.

TABLE VIII
PARAMETERS OF THE $[[n, k, n-k+1; n-k]]_{3^{12}}$ EAQECCS IN THEOREM IV.4

ℓ	Length set	Cardinality	Length n	j	i	k
1	V_1	23	$j \cdot 3^i$	$[1,3]$	$[1,11]$	$[1, \lfloor \frac{2+n}{4} \rfloor]$
2	V_2	43	$j \cdot 3^i$	$[1,3]$	$[1,11]$	$[1, \lfloor \frac{8+n}{10} \rfloor]$
			$j \cdot 3^{2i}$	$4,5,7,8$	$[1,5]$	$[1, \lfloor \frac{8+n}{10} \rfloor]$
3	V_3	83	$j \cdot 3^i$	$[1,3]$	$[1,11]$	$[1, \lfloor \frac{26+n}{28} \rfloor]$
			$j \cdot 3^{3i}$	$[4,26], 3 \nmid j$	$[1,3]$	$[1, \lfloor \frac{26+n}{28} \rfloor]$
			$j \cdot 3^{3i+1}$	$4,5,7,8$	$[1,3]$	$[1, \lfloor \frac{26+n}{28} \rfloor]$
2	$V_2 \backslash V_1$	20	$j \cdot 3^{2i}$	$4,5,7,8$	$[1,5]$	$[\lfloor \frac{3^6+n-1}{3^6+1} \rfloor + 1, \lfloor \frac{8+n}{10} \rfloor]$
2	$V_2 \backslash V_3$	8	$j \cdot 3^2$	$4,5,7,8$	–	$[\lfloor \frac{3^6+n-1}{3^6+1} \rfloor + 1, \lfloor \frac{8+n}{10} \rfloor]$
			$j \cdot 3^8$	$4,5,7,8$	–	$[\lfloor \frac{3^6+n-1}{3^6+1} \rfloor + 1, \lfloor \frac{8+n}{10} \rfloor]$
3	$V_3 \backslash V_1$	60	$j \cdot 3^{3i}$	$[4,26], 3 \nmid j$	$[1,3]$	$[\lfloor \frac{3^6+n-1}{3^6+1} \rfloor + 1, \lfloor \frac{26+n}{28} \rfloor]$
			$j \cdot 3^{3i+1}$	$4,5,7,8$	$[1,3]$	$[\lfloor \frac{3^6+n-1}{3^6+1} \rfloor + 1, \lfloor \frac{26+n}{28} \rfloor]$
3	$V_3 \backslash V_2$	48	$j \cdot 3^3$	$[4,26], 3 \nmid j$	–	$[\lfloor \frac{3^6+n-1}{3^6+1} \rfloor + 1, \lfloor \frac{26+n}{28} \rfloor]$
			$j \cdot 3^6$	$[10,26], 3 \nmid j$	–	$[\lfloor \frac{3^6+n-1}{3^6+1} \rfloor + 1, \lfloor \frac{26+n}{28} \rfloor]$
			$j \cdot 3^7$	$4,5,7,8$	–	$[\lfloor \frac{3^6+n-1}{3^6+1} \rfloor + 1, \lfloor \frac{26+n}{28} \rfloor]$
			$j \cdot 3^9$	$[4,26], 3 \nmid j$	–	$[\lfloor \frac{3^6+n-1}{3^6+1} \rfloor + 1, \lfloor \frac{26+n}{28} \rfloor]$

TABLE IX
COMPARISON OF THE LENGTH SETS OF THE EAQECCS IN THEOREMS IV.1 AND IV.2 FOR $p = 3$, $e = 8$ AND $\ell = 2$

Length set	Cardinality	Length n	t, a, b, c
$W_2(t)$	8	$t \cdot 2^2 \cdot 5 \cdot 41$	$t \in [1,8]$
Y_2	38	$2^a \cdot 5^b \cdot 41^c$	$a \in [0,5]; b, c \in [0,1]$
		$3 \cdot 5^b \cdot 41^c$	$b, c \in [0,1]$
		$5^2 \cdot 41^c$	$c \in [0,1]$
		$6 \cdot 5^b \cdot 41^c$	$b, c \in [0,1]$
		$7 \cdot 5^b \cdot 41^c$	$b, c \in [0,1]$
$W_2(t) \backslash Y_2$	4	$t \cdot 2^2 \cdot 5 \cdot 41$	$t \in \{3,5,6,7\}$
$Y_2 \backslash W_2(t)$	34	2^a	$a \in [0,5]$
		$2^a \cdot 5$	$a \in [0,5]$
		$2^a \cdot 41$	$a \in [0,5]$
		$2^a \cdot 5 \cdot 41$	$a \in [0,1]$
		$3 \cdot 5^b \cdot 41^c$	$b, c \in [0,1]$
		$5^2 \cdot 41^c$	$c \in [0,1]$
		$6 \cdot 5^b \cdot 41^c$	$b, c \in [0,1]$
		$7 \cdot 5^b \cdot 41^c$	$b, c \in [0,1]$

In this case, we denote by $W_2(t)$ the set of length n of the $[[n, k, n-k+1; n-k]]_{3^8}$ EAQECCs in Theorem IV.1. Then, we have that

$$W_2(t) = \{t \cdot 2^2 \cdot 5 \cdot 41 | 1 \leq t \leq 8\}.$$

As shown in Table VI (see also Table IX), the set of length n of the $[[n, k, n-k+1; n-k]]_{3^8}$ EAQECCs in Theorem IV.2 is Y_2 with cardinality $|Y_2| = 38$. One can check that $W_2(1), W_2(2), W_2(4), W_2(8) \in Y_2$ and $W_2(3), W_2(5), W_2(6), W_2(7) \notin Y_2$. Hence, we have $W_2(t) \cap Y_2 = \{W_2(1), W_2(2), W_2(4), W_2(8)\}$.

Remark V.5: Based on the above analysis, Table IX lists all the corresponding lengths coming from the sets $W_2(t)$, Y_2, $W_2(t) \backslash Y_2$ and $Y_2 \backslash W_2(t)$, respectively. As shown in Table IX, we know that 34 of the 38 kinds of lengths in the set Y_2 cannot be obtained by the set $W_2(t)$. At the same time, 4 of the 8 kinds of lengths in the set $W_2(t)$ cannot be yielded from the set Y_2.

VI. CONCLUSION

In this paper, by investigating the GRS codes and extended GRS codes, we constructed eleven families of MDS codes with ℓ-Galois hulls of arbitrary dimensions via four different tools, i.e., (i) the norm mapping from $\mathbb{F}_q^*$ to $\mathbb{F}_{p^\ell}^*$; (ii) the direct product of two cyclic subgroups; (iii) the coset decomposition of a cyclic group; and (iv) an additive subgroup of $\mathbb{F}_q$ and its cosets. Through these MDS codes, we presented eleven families of EAQECCs with flexible parameters in Theorems IV.1-IV.4.

Based on the analysis in Sections III, IV and V, let us make a summary on the parameters of our EAQECCs constructed in Theorems IV.1-IV.4.

- When ℓ increases, the range of the dimension q^k becomes smaller. It attains the maximum for $\ell = 1$ and the minimum for $\ell = \frac{e}{2}$ (Hermitian case).
- In general, when ℓ increases, the cardinality of the set of length n becomes larger. It attains the maximum for $\ell = \frac{e}{2}$ (Hermitian case) and the minimum for $\ell = 1$. Moreover, for certain $\ell = \ell_1 \neq 1, \frac{e}{2}$, the corresponding kind of EAQECCs has some EAQECCs whose lengths cannot be obtained by those derived from certain $\ell = \ell_2 \neq 1, \frac{e}{2}$, where $\ell_1 \neq \ell_2$.

All in all, we believe that the approaches shown in Sections II and III will be very useful for finding more new families of EAQECCs with flexible parameters.

Next, let us look at two problems. Since the dimension k of the MDS codes constructed in Theorems III.1-III.11 is bounded by $\lfloor \frac{p^\ell+n-1}{p^\ell+1} \rfloor$ or $\lfloor \frac{p^\ell+n}{p^\ell+1} \rfloor$, one has the following problem.

Problem VI.1: How to improve the bound of the dimension k of MDS codes in Theorems III.1-III.11 to a larger value such that $k > \lfloor \frac{p^l+n-1}{p^l+1} \rfloor$ or $k > \lfloor \frac{p^l+n}{p^l+1} \rfloor$?

If this problem is solved, then the dimensions of the corresponding EAQECCs in Theorems IV.1-IV.4 will have a broader range.

Note that the ℓ-Galois dual code $\mathcal{C}^{\perp_\ell}$ of an $[n,k]_q$ MDS code $\mathcal{C}$ is an $[n,n-k]_q$ MDS code (see [40]). So it follows from Corollary IV.1 that there also exists an

$$[[n, n-k-\dim(Hull_\ell(\mathcal{C}^{\perp_\ell})), k+1; k-\dim(Hull_\ell(\mathcal{C}^{\perp_\ell}))]]_q \tag{33}$$

EAQECC. For the Euclidean case (i.e., $\ell = 0$) and Hermitian case (i.e., $\ell = \frac{e}{2}$ for even e), we have $Hull_E(\mathcal{C}) = Hull_E(\mathcal{C}^{\perp_E})$ and $Hull_H(\mathcal{C}) = Hull_H(\mathcal{C}^{\perp_H})$ since $(\mathcal{C}^{\perp_E})^{\perp_E} = \mathcal{C}$ and $(\mathcal{C}^{\perp_H})^{\perp_H} = \mathcal{C}$. This implies that the parameters of the EAQECCs in Eq. (33) are determined by $\dim(Hull_E(\mathcal{C}))$ when $\ell = 0$ or determined by $\dim(Hull_H(\mathcal{C}))$ when $\ell = \frac{e}{2}$ (if e is even). However, we usually have $(\mathcal{C}^{\perp_\ell})^{\perp_\ell} \neq \mathcal{C}$ for $\ell \neq 0$ and $\ell \neq \frac{e}{2}$. Naturally, we give the following problem.

Problem VI.2: (1) How to determine the relationship between $Hull_\ell(\mathcal{C})$ and $Hull_\ell(\mathcal{C}^{\perp_\ell})$?

(2) Further, is there an equation to link $\dim(Hull_\ell(\mathcal{C}))$ with $\dim(Hull_\ell(\mathcal{C}^{\perp_\ell}))$?

If this problem is solved, then the parameters in Eq. (33) will be determined by $\dim(Hull_\ell(\mathcal{C}))$. As a consequence, we will obtain another eleven families of EAQECCs with flexible parameters apart from those shown in Theorems IV.1-IV.4. Then, in terms of [3], the EAQECCs with $2k < n$ in Eq. (33) will produce many catalytic quantum error-correcting codes (CQECCs) with flexible parameters determined by $\dim(Hull_\ell(\mathcal{C}))$.

ACKNOWLEDGMENT

The author would like to sincerely thank the two anonymous referees for their very careful reading and many constructive comments, corrections and suggestions which greatly improved the quality of this article. He would also like to thank an Associate Editor, Prof. Mark M. Wilde, for his helpful suggestions and excellent editorial job.

REFERENCES

[1] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3065–3072, Nov. 2001.

[2] T. A. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, no. 5798, pp. 436–439, Oct. 2006.

[3] T. A. Brun, I. Devetak, and M.-H. Hsieh, "Catalytic quantum error correction," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3073–3089, Jun. 2014.

[4] A. K. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 78, no. 3, pp. 405–408, 1997.

[5] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.

[6] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 2, pp. 1098–1105, Aug. 1996.

[7] M. Cao, "Quantum error-correcting codes from matrix-product codes related to quasi-orthogonal matrices and quasi-unitary matrices," 2020, *arXiv:2012.15691*. [Online]. Available: http://arxiv.org/abs/2012.15691

[8] M. Cao, H. Wang, and J. Cui, "Construction of quantum codes from matrix-product codes," *IEEE Commun. Lett.*, vol. 24, no. 4, pp. 706–710, Apr. 2020.

[9] B. Chen and H. Liu, "New constructions of MDS codes with complementary duals," *IEEE Trans. Inf. Theory*, vol. 64, no. 8, pp. 5776–5782, Aug. 2018.

[10] J. Chen, Y. Huang, C. Feng, and R. Chen, "Entanglement-assisted quantum MDS codes constructed from negacyclic codes," *Quantum Inf. Process.*, vol. 16, no. 12, pp. 1–22, Dec. 2017.

[11] X. Chen, S. Zhu, and X. Kai, "Entanglement-assisted quantum MDS codes constructed from constacyclic codes," *Quantum Inf. Process.*, vol. 17, no. 10, pp. 1–18, Oct. 2018.

[12] M.-D. Choi, D. W. Kribs, and K. Życzkowski, "Quantum error correcting codes from the compression formalism," *Rep. Math. Phys.*, vol. 58, no. 1, pp. 77–91, Aug. 2006.

[13] J. Fan, H. Chen, and J. Xu, "Constructions of q-ary entanglement-assisted quantum MDS codes with minimum distance greater than $q+1$," *Quantum Inf. Comput.*, vol. 16, nos. 5–6, pp. 423–434, 2016.

[14] Y. Fan and L. Zhang, "Galois self-dual constacyclic codes," *Des., Codes Cryptogr.*, vol. 84, no. 3, pp. 473–492, 2017.

[15] W. Fang and F.-W. Fu, "Two new classes of quantum MDS codes," *Finite Fields Appl.*, vol. 53, pp. 85–98, Sep. 2018.

[16] W. Fang, F.-W. Fu, L. Li, and S. Zhu, "Euclidean and Hermitian hulls of MDS codes and their applications to EAQECCs," *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3527–3537, Jun. 2020.

[17] Y. Fujiwara, D. Clark, P. Vandendriessche, M. De Boeck, and V. D. Tonchev, "Entanglement-assisted quantum low-density parity-check codes," *Phys. Rev. A, Gen. Phys.*, vol. 82, no. 4, pp. 1–19, Oct. 2010.

[18] Y. Fujiwara and V. D. Tonchev, "A characterization of entanglement-assisted quantum low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3347–3353, Jun. 2013.

[19] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano, "Entanglement-assisted quantum error-correcting codes over arbitrary finite fields," *Quantum Inf. Process.*, vol. 18, no. 4, pp. 1–18, Apr. 2019.

[20] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano, "Asymmetric entanglement-assisted quantum error-correcting codes and BCH codes," *IEEE Access*, vol. 8, pp. 18571–18579, 2020.

[21] C. Galindo, F. Hernando, and D. Ruano, "New quantum codes from evaluation and matrix-product codes," *Finite Fields Appl.*, vol. 36, pp. 98–120, Nov. 2015.

[22] C. Galindo, F. Hernando, and D. Ruano, "Entanglement-assisted quantum error-correcting codes from RS codes and BCH codes with extension degree 2," *Quantum Inf. Process.*, vol. 20, no. 5, pp. 1–26, May 2021.

[23] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A, Gen. Phys.*, vol. 54, pp. 1862–1868, Sep. 1996.

[24] M. Grassl, "Entanglement-assisted quantum communication beating the quantum singleton bound," *Phys. Rev. A, Gen. Phys.*, vol. 103, no. 2, Feb. 2021, Art. no. L020601.

[25] M. Grassl, T. Beth, and M. Rötteler, "On optimal quantum codes," *Int. J. Quantum Inf.*, vol. 2, no. 1, pp. 55–64, 2004.

[26] M. Grassl, F. Huber, and A. Winter, "Entropic proofs of singleton bounds for quantum error-correcting codes," 2020, *arXiv:2010.07902*. [Online]. Available: http://arxiv.org/abs/2010.07902

[27] M. Grassl and M. Rötteler, "Quantum MDS codes over small fields," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2015, pp. 1104–1108.

[28] M. Grassl, P. Shor, G. Smith, J. Smolin, and B. Zeng, "Generalized concatenated quantum codes," *Phys. Rev. A, Gen. Phys.*, vol. 79, no. 5, May 2009, Art. no. 050306.

[29] K. Guenda, S. Jitman, and T. A. Gulliver, "Constructions of good entanglement-assisted quantum error correcting codes," *Des., Codes Cryptogr.*, vol. 86, no. 1, pp. 121–136, Jan. 2018.

[30] M.-H. Hsieh, T. A. Brun, and I. Devetak, "Entanglement-assisted quantum quasicyclic low-density parity-check codes," *Phys. Rev. A, Gen. Phys.*, vol. 79, no. 3, Mar. 2009, Art. no. 032340.

[31] M.-H. Hsieh, I. Devetak, and T. Brun, "General entanglement-assisted quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 76, no. 6, Dec. 2007, Art. no. 062313.
[32] M.-H. Hsieh, W.-T. Yen, and L.-Y. Hsu, "High performance entanglement-assisted quantum LDPC codes need little entanglement," *IEEE Trans. Inf. Theory*, vol. 57, no. 3, pp. 1761–1769, Mar. 2011.
[33] F. Huber and M. Grassl, "Quantum codes of maximal distance and highly entangled subspaces," *Quantum*, vol. 4, no. 284, Jun. 2020.
[34] L. Jin and C. Xing, "A construction of new quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2921–2925, May 2014.
[35] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 55, no. 2, pp. 900–911, Feb. 1997.
[36] M. E. Koroglu, "New entanglement-assisted MDS quantum codes from constacyclic codes," *Quantum Inf. Process.*, vol. 18, no. 2, pp. 1–28, Feb. 2019.
[37] C.-Y. Lai and A. Ashikhmin, "Linear programming bounds for entanglement-assisted quantum error-correcting codes by split weight enumerators," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 622–639, Jan. 2018.
[38] C.-Y. Lai and T. A. Brun, "Entanglement-assisted quantum error-correcting codes with imperfect ebits," *Phys. Rev. A, Gen. Phys.*, vol. 86, no. 3, Sep. 2012, Art. no. 032319.
[39] C.-Y. Lai, T. A. Brun, and M. M. Wilde, "Duality in entanglement-assisted quantum error correction," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 4020–4024, Jun. 2013.
[40] X. Liu, Y. Fan, and H. Liu, "Galois LCD codes over finite fields," *Finite Fields Appl.*, vol. 49, pp. 227–242, Jan. 2018.
[41] X. Liu, H. Liu, and L. Yu, "New EAQEC codes constructed from Galois LCD codes," *Quantum Inf. Process.*, vol. 19, no. 1, pp. 1–15, Jan. 2020.
[42] Y. Liu, R. Li, L. Lü, and Y. Ma, "Application of constacyclic codes to entanglement-assisted quantum maximum distance separable codes," *Quantum Inf. Process.*, vol. 17, no. 8, pp. 1–19, 2018.
[43] S. Lloyd and J.-J. E. Slotine, "Analog quantum error correction," *Phys. Rev. Lett.*, vol. 80, no. 18, pp. 4088–4091, May 1998.
[44] S. Y. Looi, L. Yu, V. Gheorghiu, and R. B. Griffiths, "Quantum-error-correcting codes using qudit graph states," *Phys. Rev. A, Gen. Phys.*, vol. 78, no. 4, Oct. 2008, Art. no. 042303.
[45] L. Lu, R. Li, L. Guo, Y. Ma, and Y. Liu, "Entanglement-assisted quantum MDS codes from negacyclic codes," *Quantum Inf. Process.*, vol. 17, no. 3, pp. 1–23, Mar. 2018.
[46] G. Luo, X. Cao, and X. Chen, "MDS codes with hulls of arbitrary dimensions and their quantum error correction," *IEEE Trans. Inf. Theory*, vol. 65, no. 5, pp. 2944–2952, May 2019.
[47] C. Moore and M. Nilsson, "Parallel quantum computation and quantum codes," *SIAM J. Comput.*, vol. 31, no. 3, pp. 799–815, Jan. 2001.
[48] D. Poulin, "Stabilizer formalism for operator quantum error correction," *Phys. Rev. Lett.*, vol. 95, no. 23, Dec. 2005, Art. no. 230504.
[49] J. Qian and L. Zhang, "On MDS linear complementary dual codes and entanglement-assisted quantum codes," *Des., Codes Cryptogr.*, vol. 86, no. 7, pp. 1565–1572, 2018.
[50] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A, Gen. Phys.*, vol. 52, no. 4, pp. R2493–R2496, Oct. 1995.
[51] A. Steane, "Multiple-particle interference and quantum error correction," *Proc. Roy. Soc. London A, Math., Phys. Eng. Sci.*, vol. 452, pp. 2551–2577, Nov. 1996.
[52] A. M. Steane, "Simple quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 6, pp. 4741–4751, 1996.
[53] M. M. Wilde and T. A. Brun, "Optimal entanglement formulas for entanglement-assisted quantum coding," *Phys. Rev. A, Gen. Phys.*, vol. 77, no. 6, Jun. 2008, Art. no. 064302.
[54] M. M. Wilde and T. A. Brun, "Entanglement-assisted quantum convolutional coding," *Phys. Rev. A, Gen. Phys.*, vol. 81, no. 4, Apr. 2010, Art. no. 042333.
[55] M. M. Wilde and S. Guha, "Polar codes for degradable quantum channels," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4718–4729, Jul. 2013.
[56] M. M. Wilde, M.-H. Hsieh, and Z. Babar, "Entanglement-assisted quantum turbo codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1203–1222, Feb. 2014.
[57] M. M. Wilde and J. M. Renes, "Quantum polar codes for arbitrary channels," in *Proc. Int. Symp. Inf. Theory*, Cambridge, MA, USA, Jul. 2012, pp. 334–338.

Meng Cao received the Ph.D. degree in mathematics from Tsinghua University, Beijing, China, in 2020. He is currently a Post-Doctoral Researcher at the Yau Mathematical Sciences Center, Tsinghua University. He is also with the Yanqi Lake Beijing Institute of Mathematical Sciences and Applications, Beijing. His research interests include quantum information and coding theory.