

On MDS Codes With Galois Hulls of Arbitrary Dimensions

Yang Li^a, Shixin Zhu^{a,*}, Ping Li^a

^a*School of Mathematics, HeFei University of Technology, Hefei 230601, China*

Abstract

The Galois hulls of linear codes are a generalization of the Euclidean and Hermitian hulls of linear codes. In this paper, we study the Galois hulls of (extended) GRS codes and present several new constructions of MDS codes with Galois hulls of arbitrary dimensions via (extended) GRS codes. Two general methods of constructing MDS codes with Galois hulls of arbitrary dimensions by Hermitian or general Galois self-orthogonal (extended) GRS codes are given. Using these methods, some MDS codes with larger dimensions and Galois hulls of arbitrary dimensions can be obtained and relatively strict conditions can also lead to many new classes of MDS codes with Galois hulls of arbitrary dimensions.

Keywords: Generalized Reed-Solomon codes, Galois hulls, Hermitian self-orthogonal, Galois self-orthogonal

2010 MSC: 12E20, 81p70

1. Introduction

Throughout this paper, let $q = p^h$, where p is a prime and h is a positive integer. Let \mathbb{F}_q be the finite field with q elements. Let $\mathbf{c}_1 = (c_{11}, c_{12}, \dots, c_{1n})$ and $\mathbf{c}_2 = (c_{21}, c_{22}, \dots, c_{2n}) \in \mathbb{F}_q^n$. The e -Galois inner product of \mathbf{c}_1 and \mathbf{c}_2 is defined by $(\mathbf{c}_1, \mathbf{c}_2)_e = c_{11}c_{21}^{p^e} + c_{12}c_{22}^{p^e} + \dots + c_{1n}c_{2n}^{p^e}$, where $0 \leq e \leq h-1$, which was first introduced by Fan et al. [10]. In particular, if $e = 0$, the e -Galois inner product coincides with the usual Euclidean inner product. Moreover, if h is even and $e = h/2$, the e -Galois inner product coincides with the Hermitian inner product.

An $[n, k, d]_q$ linear code \mathcal{C} is a k -dimensional subspace of \mathbb{F}_q^n with minimum distance d . Its e -Galois dual code, denoted by \mathcal{C}^{\perp_e} , is defined by $\mathcal{C}^{\perp_e} = \{\mathbf{c}_1 \in \mathbb{F}_q^n : (\mathbf{c}_1, \mathbf{c}_2)_e = 0, \text{ for all } \mathbf{c}_2 \in \mathcal{C}\}$. The e -Galois hull of the code \mathcal{C} is defined by $\text{Hull}_e(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^{\perp_e}$. If $e = 0$, $\text{Hull}_e(\mathcal{C})$ is called the Euclidean hull of \mathcal{C} . If h is even and $e = h/2$, $\text{Hull}_e(\mathcal{C})$ is called the Hermitian hull of \mathcal{C} . Hence, e -Galois hulls of linear codes are a generalization of the Euclidean and Hermitian hulls of linear codes.

For the Euclidean hull of linear codes, it was first introduced by Assmus [1] to classify finite projective planes. It had been shown that the hull of linear codes plays an important role in many other aspects of coding theory, such as determining the complexity of algorithms for checking the

*This research was supported by the National Natural Science Foundation of China under Grant Nos.U21A20428 and 12171134.

*Corresponding author

Email addresses: yanglimath@163.com (Yang Li), zhushixinmath@hfut.edu.cn (Shixin Zhu), lpmath@126.com (Ping Li)

permutation equivalence of two linear codes, computing the automorphism group of a linear code and increasing a security level against side channel attacks and fault injection attacks [4, 27, 28, 35, 36]. They usually work very well when the dimension of the Euclidean hull of a linear code is small.

With the development of quantum computation and quantum communication, how to construct quantum codes to counteract the noise in quantum channels becomes an important and difficult problem in quantum information theory. In 1996, an explicit method, called CSS construction, proposed by Calderbank et al. [3] and Steane [33], makes it possible to construct quantum stabilizer codes from certain self-orthogonal or dual containing codes. However, the self-orthogonality is often difficult to obtain. About ten years later, Brun et al. [2] introduced entanglement-assisted quantum error-correction codes (EAQECCs). In their constructions, an EAQECC can be derived from any classical linear codes with the help of pre-shared entanglement between the encoder and decoder. However, the determination of the number of shared pairs that required is usually difficult. Fortunately, one found certain relationships between this number and the dimension of the hull of a linear code. Specifically, we refer to [16] for the usual Euclidean and classical Hermitian cases, and [29] for the general Galois case. Based on these outstanding results, a large number of MDS codes (i.e., $d = n - k + 1$) with Euclidean hulls and Hermitian hulls of arbitrary dimensions were constructed and so many EAQECCs were given in [7, 12, 17, 23, 24, 26, 30, 39] and references therein.

However, up to the authors' knowledge, there seems to be little research on MDS codes with Galois hulls of arbitrary dimensions. About only twenty classes were constructed by Qian et al., Cao and Fang et al. in [5, 8, 32]. Very recently, Wu et al. [40] studied the Galois hulls of generalized Reed-Solomon (GRS) codes. They proved that the Galois hulls of some GRS codes are still GRS codes when $\mathfrak{L} = \mathfrak{L}^{p^{h-e}}$ in terms of Goppa codes. In their conditions, the dimensions of Galois hulls are also relatively flexible. Considering the excellent properties of the hull of linear codes and its important applications in coding theory, as well as relatively little research under Galois inner product, it is necessary to study and construct linear codes with Galois hulls of arbitrary dimensions, especially MDS codes with Galois hulls of arbitrary dimensions.

In this paper, we study the Galois hulls of (extended) GRS codes and present some new constructions of MDS codes with Galois hulls of arbitrary dimensions via (extended) GRS codes. For reference, we list the parameters of all known MDS codes with Galois hulls of arbitrary dimensions in Table 1 and the new ones in Table 2.

The rest of this paper is organized as follows. Some basic knowledge about (extended) GRS codes are introduced in Section 2. The six new constructions of MDS codes with Galois hulls of arbitrary dimensions are discussed in Section 3. And finally, Section 4 concludes this paper.

2. Preliminary

Let \mathcal{C} be an $[n, k, d]_q$ linear code. Then \mathcal{C} is called an MDS code if $d = n - k + 1$. Let's now introduce an important class of MDS codes.

Table 1: Known constructions on MDS codes with Galois hulls of arbitrary dimensions

Class	q -Ary	Code length n	Dimension k	Ref.
1	$q = p^h$ is even	$n \leq q, \frac{m}{\gcd(e,m)}$ and $m > 1$	$1 \leq k \leq \lfloor \frac{p^e+n-1}{p^e+1} \rfloor$	[32]
2	$q = p^h > 3$	$n \leq r, r = p^m$ with $m \mid h$ and $(p^e + 1) \mid \frac{q-1}{r-1}$	$1 \leq k \leq \lfloor \frac{p^e+n-1}{p^e+1} \rfloor$	[32]
3	$q = p^h > 3$	$n \mid q$	$1 \leq k \leq \lfloor \frac{p^e+n-1}{p^e+1} \rfloor$	[32]
4	$q = p^h > 3$	$(n-1) \mid (q-1)$	$1 \leq k \leq \lfloor \frac{p^e+n-1}{p^e+1} \rfloor$	[32]
5	$q = p^h > 3$	$n \mid (q-1)$	$1 \leq k \leq \lfloor \frac{p^e+n-1}{p^e+1} \rfloor$	[32]
6	$q = p^h$ is odd, $2e \mid h$	$n = \frac{r(q-1)}{\gcd(x_2, q-1)}, 1 \leq r \leq \frac{q-1}{\gcd(x_1, q-1)},$ $(q-1) \mid \text{lcm}(x_1, x_2)$ and $\frac{q-1}{p^e-1} \mid x_1$	$1 \leq k \leq \lfloor \frac{p^e+n}{p^e+1} \rfloor$	[5]
7	$q = p^h$ is odd, $2e \mid h$	$n = \frac{r(q-1)}{\gcd(x_2, q-1)} + 1, 1 \leq r \leq \frac{q-1}{\gcd(x_1, q-1)},$ $(q-1) \mid \text{lcm}(x_1, x_2)$ and $\frac{q-1}{p^e-1} \mid x_1$	$1 \leq k \leq \lfloor \frac{p^e+n}{p^e+1} \rfloor$	[5]
8	$q = p^h$ is odd, $2e \mid h$	$n = \frac{r(q-1)}{\gcd(x_2, q-1)} + 2, 1 \leq r \leq \frac{q-1}{\gcd(x_1, q-1)},$ $(q-1) \mid \text{lcm}(x_1, x_2)$ and $\frac{q-1}{p^e-1} \mid x_1$	$1 \leq k \leq \lfloor \frac{p^e+n}{p^e+1} \rfloor$	[5]
9	$q = p^h$ is odd, $2e \mid h$	$n = rm, 1 \leq r \leq \frac{p^e-1}{m_1},$ $m_1 = \frac{m}{\gcd(m, y)}, m \mid (q-1)$ and $y = \frac{q-1}{p^e-1}$	$1 \leq k \leq \lfloor \frac{p^e+n}{p^e+1} \rfloor$	[5]
10	$q = p^h$ is odd, $2e \mid h$	$n = rm + 1, 1 \leq r \leq \frac{p^e-1}{m_1},$ $m_1 = \frac{m}{\gcd(m, y)}, m \mid (q-1)$ and $y = \frac{q-1}{p^e-1}$	$1 \leq k \leq \lfloor \frac{p^e+n}{p^e+1} \rfloor$	[5]
11	$q = p^h$ is odd, $2e \mid h$	$n = rm + 2, 1 \leq r \leq \frac{p^e-1}{m_1},$ $m_1 = \frac{m}{\gcd(m, y)}, m \mid (q-1)$ and $y = \frac{q-1}{p^e-1}$	$1 \leq k \leq \lfloor \frac{p^e+n}{p^e+1} \rfloor$	[5]
12	$q = p^h$ is odd, $2e \mid h$	$n = tp^{aw}, 1 \leq t \leq p^a, 1 \leq w \leq \frac{h}{a} - 1, a \mid e$	$1 \leq k \leq \lfloor \frac{p^e+n-1}{p^e+1} \rfloor$	[5]
13	$q = p^h$ is odd, $2e \mid h$	$n = tp^{aw} + 1, 1 \leq t \leq p^a, 1 \leq w \leq \frac{h}{a} - 1, a \mid e$	$1 \leq k \leq \lfloor \frac{p^e+n-1}{p^e+1} \rfloor$	[5]
14	$q = p^h$ is odd, $2e \mid h$	$n = \frac{t(q-1)}{p^e-1}, 1 \leq t \leq p^e - 1$	$1 \leq k \leq \lfloor \frac{p^e+n}{p^e+1} \rfloor$	[5]
15	$q = p^h$ is odd, $2e \mid h$	$n = \frac{t(q-1)}{p^e-1} + 1, 1 \leq t \leq p^e - 1$	$1 \leq k \leq \lfloor \frac{p^e+n}{p^e+1} \rfloor$	[5]
16	$q = p^h$ is odd, $2e \mid h$	$n = \frac{t(q-1)}{p^e-1} + 2, 1 \leq t \leq p^e - 1$	$1 \leq k \leq \lfloor \frac{p^e+n}{p^e+1} \rfloor$	[5]
17	$q = p^{em}$ is odd, m is even	$n = tp^{er}, t \mid (p^e - 1), r \leq m - 1$	$1 \leq k \leq \lfloor \frac{p^e+n-1}{p^e+1} \rfloor$	[8]
18	$q = p^h$ is odd, $2e \mid h$	$n = tp^{h-e}, 1 \leq t \leq p^e$	$1 \leq k \leq \lfloor \frac{p^e+n-1}{p^e+1} \rfloor$	[8]
19	$q = p^h$ is odd	$1 \leq m \leq \lfloor \frac{n}{2} \rfloor, \frac{h}{e}$ is odd, $\text{GRS}_m(\mathbf{a}, \mathbf{v})^{\perp_0} = \text{GRS}_{n-m}(\mathbf{a}, \mathbf{v})$	$1 \leq k \leq \lfloor \frac{p^e+n-1}{p^e+1} \rfloor$	[8]
20	$q = p^h$ is odd	$1 \leq m \leq \lfloor \frac{n+1}{2} \rfloor, \frac{h}{e}$ is odd, $\text{GRS}_m(\mathbf{a}, \mathbf{v}, \infty)^{\perp_0} = \text{GRS}_{n-m}(\mathbf{a}, \mathbf{v}, \infty)$	$1 \leq k \leq \lfloor \frac{p^e+n-1}{p^e+1} \rfloor$	[8]

Table 2: The new constructions of MDS codes with Galois hulls of arbitrary dimensions

Class	q -Ary	Code length n	Dimension k	Ref.
1	$q = p^h \geq 5$	$\gcd(e', h) = e, \frac{h}{e} \text{ is even,}$ $\text{GRS}_m(\mathbf{a}, \mathbf{v}) \subseteq \text{GRS}_m(\mathbf{a}, \mathbf{v})^{\perp_e}$	$1 \leq k \leq \lfloor \frac{p^{e'} + n - 1 - \deg(h(x))}{p^{e'} + 1} \rfloor,$ $\deg(h(x)) \leq n - m - 1$	Theorem 5 1)
2	$q = p^h \geq 5$	$\gcd(e', h) = e, \frac{h}{e} \text{ is even, } m \geq 2,$ $\text{GRS}_m(\mathbf{a}, \mathbf{v}, \infty) \subseteq \text{GRS}_m(\mathbf{a}, \mathbf{v}, \infty)^{\perp_e}$	$1 \leq k \leq \lfloor \frac{p^{e'} + n - 1 - \deg(h(x))}{p^{e'} + 1} \rfloor,$ $\deg(h(x)) \leq n - m - 1$	Theorem 5 2)
3	$q = p^h \text{ is odd, } h \text{ is even}$	$\frac{h}{\gcd(e', h)} \text{ is odd,}$ $\text{GRS}_m(\mathbf{a}, \mathbf{v}) \subseteq \text{GRS}_m(\mathbf{a}, \mathbf{v})^{\perp_{\frac{h}{2}}}$	$1 \leq k \leq \lfloor \frac{p^{e'} + n - 1 - \deg(h(x))}{p^{e'} + 1} \rfloor,$ $\deg(h(x)) \leq n - m - 1$	Theorem 8 1)
4	$q = p^h \text{ is odd, } h \text{ is even}$	$\frac{h}{\gcd(e', h)} \text{ is odd, } m \geq 2,$ $\text{GRS}_m(\mathbf{a}, \mathbf{v}, \infty) \subseteq \text{GRS}_m(\mathbf{a}, \mathbf{v}, \infty)^{\perp_{\frac{h}{2}}}$	$1 \leq k \leq \lfloor \frac{p^{e'} + n - 1 - \deg(h(x))}{p^{e'} + 1} \rfloor,$ $\deg(h(x)) \leq n - m - 1$	Theorem 8 2)
5	$q = p^h \text{ is odd,}$ $2^t \mid \frac{h}{m}, 2^t = p^e + 1$	$n = wp^{mz}, 1 \leq w \leq p^m, 1 \leq z \leq \frac{h}{m} - 1$	$1 \leq k \leq \lfloor \frac{p^e + n - 1}{p^e + 1} \rfloor$	Theorem 15 1)
6	$q = p^h \text{ is odd,}$ $2^t \mid \frac{h}{m}, 2^t = p^e + 1$	$n = wp^{mz} + 1, 1 \leq w \leq p^m, 1 \leq z \leq \frac{h}{m} - 1$	$1 \leq k \leq \lfloor \frac{p^e + n - 1}{p^e + 1} \rfloor$	Theorem 15 2)

Suppose that $\{a_1, a_2, \dots, a_n\}$ are n distinct elements of \mathbb{F}_q and $\mathbf{a} = (a_1, a_2, \dots, a_n)$. Let $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. For a vector $\mathbf{v} = (v_1, v_2, \dots, v_n) \in (\mathbb{F}_q^*)^n$ and an integer $k \geq 0$, we define a generalized Reed-Solomon (GRS) code as

$$\text{GRS}_k(\mathbf{a}, \mathbf{v}) = \{(v_1 f(a_1), v_2 f(a_2), \dots, v_n f(a_n)) : f(x) \in \mathbb{F}_q[x], \deg(f(x)) \leq k - 1\}.$$

It is well known that $\text{GRS}_k(\mathbf{a}, \mathbf{v})$ is an $[n, k, n - k + 1]_q$ MDS code. Usually, we call the elements a_1, a_2, \dots, a_n the *code locators* of $\text{GRS}_k(\mathbf{a}, \mathbf{v})$ and the elements v_1, v_2, \dots, v_n the *column multipliers* of $\text{GRS}_k(\mathbf{a}, \mathbf{v})$. Moreover, an extended GRS code, denoted by $\text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)$, is defined by

$$\text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty) = \{(v_1 f(a_1), v_2 f(a_2), \dots, v_n f(a_n), f_{k-1}) : f(x) \in \mathbb{F}_q[x], \deg(f(x)) \leq k - 1\},$$

where f_{k-1} is the coefficient of x^{k-1} in $f(x)$. It is easy to show that $\text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)$ is an $[n + 1, k, n - k + 2]_q$ MDS code.

Recall the definitions of e -Galois self-orthogonal GRS and extended GRS codes. Let $\text{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp_e}$ (resp. $\text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)^{\perp_e}$) be the e -Galois dual code of $\text{GRS}_k(\mathbf{a}, \mathbf{v})$ (resp. $\text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)$). Then $\text{GRS}_k(\mathbf{a}, \mathbf{v})$ (resp. $\text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)$) is e -Galois self-orthogonal if $\text{GRS}_k(\mathbf{a}, \mathbf{v}) \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp_e}$ (resp. $\text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty) \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)^{\perp_e}$). Equivalently, we can also say $\text{GRS}_k(\mathbf{a}, \mathbf{v})$ (resp. $\text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)$) is e -Galois self-orthogonal if $\text{Hull}_e(\text{GRS}_k(\mathbf{a}, \mathbf{v})) = \text{GRS}_k(\mathbf{a}, \mathbf{v})$ (resp. $\text{Hull}_e(\text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)) = \text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)$).

We now consider the e -Galois hulls of the GRS codes and extended GRS codes further. To this end,

for $1 \leq i \leq n$, let

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

which will be need in the sequel. In addition, we need the following important results.

Lemma 1. ([5], Propositions II.1 and II.2) *Let notations be the same as before.*

- 1) *Let $\mathbf{c} = (v_1 f(a_1), v_2 f(a_2), \dots, v_n f(a_n)) \in \text{GRS}_k(\mathbf{a}, \mathbf{v})$, then $\mathbf{c} \in \text{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp_e}$ if and only if there exists a polynomial $g(x) \in \mathbb{F}_q[x]$ with $\deg(g(x)) \leq n - k - 1$ such that*

$$(v_1^{p^e+1} f^{p^e}(a_1), v_2^{p^e+1} f^{p^e}(a_2), \dots, v_n^{p^e+1} f^{p^e}(a_n)) = (u_1 g(a_1), u_2 g(a_2), \dots, u_n g(a_n)).$$

- 2) *Let $\mathbf{c} = (v_1 f(a_1), v_2 f(a_2), \dots, v_n f(a_n), f_{k-1}) \in \text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)$, then $\mathbf{c} \in \text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)^{\perp_e}$ if and only if there exists a polynomial $g(x) \in \mathbb{F}_q[x]$ with $\deg(g(x)) \leq n - k$ such that*

$$(v_1^{p^e+1} f^{p^e}(a_1), v_2^{p^e+1} f^{p^e}(a_2), \dots, v_n^{p^e+1} f^{p^e}(a_n), f_{k-1}^{p^e}) = (u_1 g(a_1), u_2 g(a_2), \dots, u_n g(a_n), -g_{n-k}),$$

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

Lemma 2. ([22], Lemma 3) *Let $s \geq 1$ and $p > 1$ be two integers. Then*

$$\gcd(p^r + 1, p^s - 1) = \begin{cases} 1 & \text{if } \frac{s}{\gcd(r,s)} \text{ is odd and } p \text{ is even,} \\ 2 & \text{if } \frac{s}{\gcd(r,s)} \text{ is odd and } p \text{ is odd,} \\ p^{\gcd(r,s)} + 1 & \text{if } \frac{s}{\gcd(r,s)} \text{ is even.} \end{cases} \quad (2)$$

3. Constructions

In this section, we construct several classes of MDS codes with Galois hulls of arbitrary dimensions via (extended) GRS codes. We also give two general methods to construct MDS codes with Galois hulls of arbitrary dimensions from Hermitian or general Galois self-orthogonal (extended) GRS codes. Some MDS codes with Galois hulls of arbitrary dimensions constructed from Hermitian self-orthogonal (extended) GRS codes have larger dimensions.

3.1. MDS codes with Galois hulls of arbitrary dimensions from Galois self-orthogonal (extended) GRS codes

In this subsection, we use Galois self-orthogonal (extended) GRS codes to construct MDS codes with Galois hulls of arbitrary dimensions. We begin with the following lemmas, which give some necessary conditions for Galois self-orthogonal (extended) GRS codes.

Lemma 3. *If $\text{GRS}_k(\mathbf{a}, \mathbf{v}) \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp_e}$, then there exists a monic polynomial $h(x) \in \mathbb{F}_q[x]$ with $\deg(h(x)) \leq n - k - 1$ such that*

$$\lambda u_i h(a_i) = v_i^{p^e+1}, \quad 1 \leq i \leq n, \quad (3)$$

where $\lambda \in \mathbb{F}_q^*$.

Proof. Suppose that $\text{GRS}_k(\mathbf{a}, \mathbf{v}) \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp_e}$. Then, for any codeword

$$\mathbf{c} = (v_1 f(a_1), v_2 f(a_2), \dots, v_n f(a_n)) \in \text{GRS}_k(\mathbf{a}, \mathbf{v}),$$

we have $\mathbf{c} \in \text{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp_e}$. Specially, taking $f(x) = 1$, then $\mathbf{c} = (v_1, v_2, \dots, v_n)$. According to the result 1) of Lemma 1, there exists a polynomial $g(x) \in \mathbb{F}_q[x]$ with $\deg(g(x)) \leq n - k - 1$ such that $v_i^{p^e+1} f^{p^e}(a_i) = u_i g(a_i)$, i.e., $v_i^{p^e+1} = u_i g(a_i)$ for $1 \leq i \leq n$. It is clear that there exists a $\lambda^{-1} \in \mathbb{F}_q^*$ such that $h(x) = \lambda^{-1} g(x) \in \mathbb{F}_q[x]$ is a monic polynomial with $\deg(h(x)) = \deg(g(x)) \leq n - k - 1$. Note that $u_i g(a_i) = \lambda u_i h(a_i)$, hence $\lambda u_i h(a_i) = v_i^{p^e+1}$ for $1 \leq i \leq n$. This completes the proof. \square

Lemma 4. *If $\text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty) \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)^{\perp_e}$ with $k \geq 2$, then there exists a monic polynomial $h(x) \in \mathbb{F}_q[x]$ with $\deg(h(x)) \leq n - k - 1$ such that*

$$\lambda u_i h(a_i) = v_i^{p^e+1}, \quad 1 \leq i \leq n, \quad (4)$$

where $\lambda \in \mathbb{F}_q^*$.

Proof. Similar to the proof of Lemma 3, take $f(x) = 1$, then

$$\mathbf{c} = (v_1, v_2, \dots, v_n, 0) \in \text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty) \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)^{\perp_e}.$$

According to the result 2) of Lemma 1, there exists a polynomial $g(x) \in \mathbb{F}_q[x]$ with $\deg(g(x)) \leq n - k$ such that $v_i^{p^e+1} = u_i g(a_i)$ for $1 \leq i \leq n$ and $g_{n-k} = -f_{k-1}^{p^e} = 0$. It follows that $\deg(g(x)) \leq n - k - 1$. Clearly, there exists a $\lambda^{-1} \in \mathbb{F}_q^*$ such that $h(x) = \lambda^{-1} g(x) \in \mathbb{F}_q[x]$ is a monic polynomial with $\deg(h(x)) = \deg(g(x)) \leq n - k - 1$. Therefore, $v_i^{p^e+1} = u_i g(a_i) = \lambda u_i h(a_i)$ for $1 \leq i \leq n$. This completes the proof. \square

Remark 1. 1) *By the proofs of Lemmas 3 and 4, $h(x) = \lambda^{-1} g(x)$ and $g(a_i) = u_i^{-1} v_i^{p^e+1}$, $1 \leq i \leq n$ when $f(x) = 1$. Note that $g(x)$ is a polynomial with $\deg(g(x)) \leq n - k - 1$ and a_i , u_i and v_i are all known for $1 \leq i \leq n$ when a GRS code or extended GRS code is given. Hence, according to the existence and uniqueness of Lagrange Interpolation Formula, the interpolation polynomial obtained by using these n mutually different interpolation points $(a_1, u_1^{-1} v_1^{p^e+1})$, $(a_2, u_2^{-1} v_2^{p^e+1})$, \dots , $(a_n, u_n^{-1} v_n^{p^e+1})$ is actually $g(x)$ itself. Therefore the structure of $h(x)$ and $\deg(h(x))$ can be easily derived from $h(x) = \lambda^{-1} g(x)$.*

2) *In practical applications, there are many occasions where we don't even need to use Lagrange Interpolation Formula. Because in the constructions of many known self-orthogonal (extended) GRS codes, $g(x)$, as an important intermediate tool, was usually given directly (e.g., see [5, 8, 11, 12, 15, 23, 24, 37, 38] and references therein). Hence taking $f(x) = 1$, in these cases, the structure of $h(x)$ and $\deg(h(x))$ can be determined directly. Some specific examples will be given later.*

We now can start our constructions. It is worth noting that the polynomial $h(x)$ appearing in the constructions refers to $h(x)$ in Lemmas 3 and 4, i.e., Eqs. (3) and (4) hold. According to Remark 1, $\deg(h(x))$ can be easily determined.

Theorem 5. Let $q = p^h \geq 5$ be a prime power. Let $1 \leq e, e' \leq h - 1$ such that $e = \gcd(e', h)$ and $\frac{h}{e}$ is even. Then the following hold.

- 1) Suppose that $\text{GRS}_m(\mathbf{a}, \mathbf{v}) \subseteq \text{GRS}_m(\mathbf{a}, \mathbf{v})^{\perp_e}$, then for $1 \leq k \leq \lfloor \frac{p^{e'} + n - 1 - \deg(h(x))}{p^{e'} + 1} \rfloor$, there exists an $[n, k]_q$ MDS code \mathcal{C} with $\dim(\text{Hull}_{e'}(\mathcal{C})) = l$, where $0 \leq l \leq k$.
- 2) Suppose that $\text{GRS}_m(\mathbf{a}, \mathbf{v}, \infty) \subseteq \text{GRS}_m(\mathbf{a}, \mathbf{v}, \infty)^{\perp_e}$ with $m \geq 2$, then for $1 \leq k \leq \lfloor \frac{p^{e'} + n - 1 - \deg(h(x))}{p^{e'} + 1} \rfloor$, there exists an $[n + 1, k]_q$ MDS code \mathcal{C} with $\dim(\text{Hull}_{e'}(\mathcal{C})) = l$, where $0 \leq l \leq k - 1$.

Proof. 1) It follows from $\text{GRS}_m(\mathbf{a}, \mathbf{v}) \subseteq \text{GRS}_m(\mathbf{a}, \mathbf{v})^{\perp_e}$ and Lemma 3 that there exists a monic polynomial $h(x) \in \mathbb{F}_q[x]$ with $\deg(h(x)) \leq n - m - 1$ such that

$$\lambda u_i h(a_i) = v_i^{p^e + 1} \neq 0, \quad 1 \leq i \leq n, \quad (5)$$

where $\lambda \in \mathbb{F}_q^*$. Since $e = \gcd(e', h)$ and $\frac{h}{e}$ is even, by Lemma 2,

$$\gcd(p^{e'} + 1, p^h - 1) = p^{\gcd(e', h)} + 1 = p^e + 1.$$

Therefore, there exist two integers μ and ν such that $\mu(p^{e'} + 1) + \nu(p^h - 1) = p^e + 1$. Denote $v_i^\mu = v'_i$, then

$$v_i^{p^e + 1} = v_i^{\mu(p^{e'} + 1) + \nu(p^h - 1)} = (v_i^\mu)^{p^{e'} + 1} = (v'_i)^{p^{e'} + 1}. \quad (6)$$

Substituting Eq. (6) into Eq. (5), we have

$$\lambda u_i h(a_i) = (v'_i)^{p^{e'} + 1}, \quad 1 \leq i \leq n.$$

Since $(q - 1) \nmid (p^{e'} + 1)$, there is an $\alpha \in \mathbb{F}_q^*$ such that $\beta = \alpha^{p^{e'} + 1} \neq 1$. Let $\mathbf{a} = (a_1, a_2, \dots, a_n)$ be the same as before and $\mathbf{v}' = (\alpha v'_1, \dots, \alpha v'_s, v'_{s+1}, \dots, v'_n) \in (\mathbb{F}_q^*)^n$, where $s = k - l \leq k$. We now consider the e' -Galois hull of the $[n, k]_q$ MDS code $\mathcal{C} = \text{GRS}_k(\mathbf{a}, \mathbf{v}')$.

For any codeword

$$\mathbf{c} = (\alpha v'_1 f(a_1), \dots, \alpha v'_s f(a_s), v'_{s+1} f(a_{s+1}), \dots, v'_n f(a_n)) \in \text{Hull}_{e'}(\mathcal{C}),$$

where $f(x) \in \mathbb{F}_q[x]$ and $\deg(f(x)) \leq k - 1$. By the result 1) of Lemma 1, there exists a polynomial $g(x) \in \mathbb{F}_q[x]$ with $\deg(g(x)) \leq n - k - 1$ such that

$$\begin{aligned} & (\alpha^{p^{e'} + 1} (v'_1)^{p^{e'} + 1} f^{p^{e'}}(a_1), \dots, \alpha^{p^{e'} + 1} (v'_s)^{p^{e'} + 1} f^{p^{e'}}(a_s), (v'_{s+1})^{p^{e'} + 1} f^{p^{e'}}(a_{s+1}), \dots, (v'_n)^{p^{e'} + 1} f^{p^{e'}}(a_n)) \\ &= (u_1 g(a_1), \dots, u_s g(a_s), u_{s+1} g(a_{s+1}), \dots, u_n g(a_n)). \end{aligned}$$

Replacing $\alpha^{p^{e'} + 1}$ and $(v'_i)^{p^{e'} + 1}$ with β and $\lambda u_i h(a_i)$, respectively, we have

$$\begin{aligned} & (\beta \lambda u_1 h(a_1) f^{p^{e'}}(a_1), \dots, \beta \lambda u_s h(a_s) f^{p^{e'}}(a_s), \lambda u_{s+1} h(a_{s+1}) f^{p^{e'}}(a_{s+1}), \dots, \lambda u_n h(a_n) f^{p^{e'}}(a_n)) \\ &= (u_1 g(a_1), \dots, u_s g(a_s), u_{s+1} g(a_{s+1}), \dots, u_n g(a_n)). \end{aligned} \quad (7)$$

On one hand, from the last $n - s$ coordinates of Eq. (7), we have

$$\lambda u_i h(a_i) f^{p^{e'}}(a_i) = u_i g(a_i), \quad s + 1 \leq i \leq n,$$

i.e., $\lambda h(x)f^{p^{e'}}(x) = g(x)$ has at least $n - s$ distinct roots. Since $\deg(h(x)) \leq n - m - 1$ and $1 \leq k \leq \lfloor \frac{p^{e'} + n - 1 - \deg(h(x))}{p^{e'} + 1} \rfloor$,

$$\deg(h(x)f^{p^{e'}}(x)) \leq \deg(h(x)) + p^{e'}(k - 1) \leq n - k - 1,$$

$$\deg(g(x)) \leq n - k - 1.$$

Recall that $s = k - l \leq k$, then

$$\deg(\lambda h(x)f^{p^{e'}}(x) - g(x)) \leq n - k - 1 \leq n - s - 1 < n - s. \quad (8)$$

That is, $\lambda h(x)f^{p^{e'}}(x) = g(x)$.

On the other hand, from the first s coordinates of Eq. (7), we have

$$\beta \lambda u_i h(a_i) f^{p^{e'}}(a_i) = u_i g(a_i) = \lambda u_i h(a_i) f^{p^{e'}}(a_i), \quad 1 \leq i \leq s.$$

Therefore, $f(a_i) = 0$ ($1 \leq i \leq s$) for $\beta \neq 1$ and $\lambda u_i h(a_i) \neq 0$. It follows that $f(x)$ can be written as

$$f(x) = r(x) \prod_{i=1}^s (x - a_i),$$

for some $r(x) \in \mathbb{F}_q[x]$ with $\deg(r(x)) \leq k - 1 - s = l - 1$. It deduces that $\dim(\text{Hull}_{e'}(\mathcal{C})) \leq l$.

Conversely, let $f(x) = r(x) \prod_{i=1}^s (x - a_i)$, where $r(x) \in \mathbb{F}_q[x]$ with $\deg(r(x)) \leq k - 1 - s = l - 1$. Take $g(x) = \lambda h(x)f^{p^{e'}}(x)$, then $\deg(g(x)) \leq \deg(h(x)) + p^{e'}(k - 1) \leq n - k - 1$ and

$$\begin{aligned} & (\alpha^{p^{e'}+1}(v'_1)^{p^{e'}+1}f^{p^{e'}}(a_1), \dots, \alpha^{p^{e'}+1}(v'_s)^{p^{e'}+1}f^{p^{e'}}(a_s), (v'_{s+1})^{p^{e'}+1}f^{p^{e'}}(a_{s+1}), \dots, (v'_n)^{p^{e'}+1}f^{p^{e'}}(a_n)) \\ & = (u_1 g(a_1), \dots, u_s g(a_s), u_{s+1} g(a_{s+1}), \dots, u_n g(a_n)). \end{aligned}$$

By the result 1) of Lemma 1, the vector

$$(\alpha v'_1 f(a_1), \dots, \alpha v'_s f(a_s), v'_{s+1} f(a_{s+1}), \dots, v'_n f(a_n)) \in \text{Hull}_{e'}(\mathcal{C}).$$

It deduces that $\dim(\text{Hull}_{e'}(\mathcal{C})) \geq l$.

Combining both aspects, we have $\dim(\text{Hull}_{e'}(\mathcal{C})) = l$, where $0 \leq l \leq k$. The desired result follows.

2) Since $\text{GRS}_m(\mathbf{a}, \mathbf{v}, \infty) \subseteq \text{GRS}_m(\mathbf{a}, \mathbf{v}, \infty)^{\perp_e}$ with $m \geq 2$ and by Lemma 4, there exists a monic polynomial $h(x) \in \mathbb{F}_q[x]$ with $\deg(h(x)) \leq n - m - 1$ such that $\lambda u_i h(a_i) = v_i^{p^e+1}$, $1 \leq i \leq n$. Similar to the result 1), it can be proved that there exists $v'_i \in \mathbb{F}_q^*$ such that

$$(v'_i)^{p^{e'}+1} = \lambda u_i h(a_i), \quad 1 \leq i \leq n.$$

Choose $\alpha \in \mathbb{F}_q^*$ satisfying $\beta = \alpha^{p^{e'}+1} \neq 1$ again. Let $\mathbf{a} = (a_1, a_2, \dots, a_n)$ be the same as before and $\mathbf{v}' = (\alpha v'_1, \dots, \alpha v'_s, v'_{s+1}, \dots, v'_n)$, where $s = k - l - 1 \leq k - 1$. We now consider the e' -Galois hull of the $[n + 1, k]_q$ MDS code $\mathcal{C} = \text{GRS}_k(\mathbf{a}, \mathbf{v}', \infty)$.

For any codeword

$$\mathbf{c} = (\alpha v'_1 f(a_1), \dots, \alpha v'_s f(a_s), v'_{s+1} f(a_{s+1}), \dots, v'_n f(a_n), f_{k-1}) \in \text{Hull}_{e'}(\mathcal{C}),$$

where $f(x) \in \mathbb{F}_q[x]$ and $\deg(f(x)) \leq k-1$. By the result 2) of Lemma 1, and replacing $\alpha^{p^{e'}+1}$ and $(v'_i)^{p^{e'}+1}$ with β and $\lambda u_i h(a_i)$, respectively, there exists a polynomial $g(x) \in \mathbb{F}_q[x]$ with $\deg(g(x)) \leq n-k$ such that

$$\begin{aligned} &(\beta \lambda u_1 h(a_1) f^{p^{e'}}(a_1), \dots, \beta \lambda u_s h(a_s) f^{p^{e'}}(a_s), \lambda u_{s+1} h(a_{s+1}) f^{p^{e'}}(a_{s+1}), \dots, \lambda u_n h(a_n) f^{p^{e'}}(a_n), \\ &f_{k-1}^{p^{e'}}) = (u_1 g(a_1), \dots, u_s g(a_s), u_{s+1} g(a_{s+1}), \dots, u_n g(a_n), -g_{n-k}). \end{aligned} \quad (9)$$

On one hand, from the last $n-s+1$ coordinates of Eq. (9), $\lambda u_i h(a_i) f^{p^{e'}}(a_i) = u_i g(a_i)$, for $s+1 \leq i \leq n$ and $f_{k-1}^{p^{e'}} = -g_{n-k}$. It follows from $\deg(h(x)) \leq n-m-1$, $1 \leq k \leq \lfloor \frac{p^{e'}+n-1-\deg(h(x))}{p^{e'}+1} \rfloor$ and $s = k-l-1 \leq k-1$ that $\lambda h(x) f^{p^{e'}}(x) = g(x)$. We now determine the value of f_{k-1} . If $f_{k-1} \neq 0$, then $\deg(h(x)) + p^{e'}(k-1) = n-k$, which contradicts to $1 \leq k \leq \lfloor \frac{p^{e'}+n-1-\deg(h(x))}{p^{e'}+1} \rfloor$. Therefore, $f_{k-1} = 0$ and $\deg(f(x)) \leq k-2$.

On the other hand, from the first s coordinates of Eq. (9), we have

$$\beta \lambda u_i h(a_i) f^{p^{e'}}(a_i) = u_i g(a_i) = \lambda u_i h(a_i) f^{p^{e'}}(a_i), \quad 1 \leq i \leq s.$$

Therefore, $f(a_i) = 0$ ($1 \leq i \leq s$) for $\beta \neq 0$ and $\lambda u_i h(a_i) \neq 0$. It follows that $f(x)$ can be written as

$$f(x) = r(x) \prod_{i=1}^s (x - a_i),$$

for some $r(x) \in \mathbb{F}_q[x]$ with $\deg(r(x)) \leq k-2-s = l-1$. It deduces that $\dim(\text{Hull}_{e'}(\mathcal{C})) \leq l$.

Conversely, let $f(x) = r(x) \prod_{i=1}^s (x - a_i)$, where $r(x) \in \mathbb{F}_q[x]$ with $\deg(r(x)) \leq k-2-s = l-1$. Take $g(x) = \lambda h(x) f^{p^{e'}}(x)$, then $\deg(g(x)) \leq \deg(h(x)) + p^{e'}(k-2) \leq n-k-1$ and

$$\begin{aligned} &(\alpha^{p^{e'}+1} (v'_1)^{p^{e'}+1} f^{p^{e'}}(a_1), \dots, \alpha^{p^{e'}+1} (v'_s)^{p^{e'}+1} f^{p^{e'}}(a_s), (v'_{s+1})^{p^{e'}+1} f^{p^{e'}}(a_{s+1}), \dots, (v'_n)^{p^{e'}+1} f^{p^{e'}}(a_n), 0) \\ &= (u_1 g(a_1), \dots, u_s g(a_s), u_{s+1} g(a_{s+1}), \dots, u_n g(a_n), 0). \end{aligned}$$

By the result 2) of Lemma 1, the vector

$$(\alpha v'_1 f(a_1), \dots, \alpha v'_s f(a_s), v'_{s+1} f(a_{s+1}), \dots, v'_n f(a_n), 0) \in \text{Hull}_{e'}(\mathcal{C}).$$

It deduces that $\dim(\text{Hull}_{e'}(\mathcal{C})) \geq l$

Combining both aspects, we have $\dim(\text{Hull}_{e'}(\mathcal{C})) = l$, where $0 \leq l \leq k-1$. The desired result follows. \square

Remark 2. 1) In the light of our present knowledge, there is relatively little work on general Galois self-orthogonal (extended) GRS codes. Classes 10, 12, 15 and 19 in Table 1 are some examples.
2) For the case $e = 0$, a similar result was given by Theorems 4.1 and 4.2 of [8]. We have list them as Classes 19 and 20 in Table 1.

Example 6. In Table 3, we give some examples satisfying the conditions that $e = \gcd(e', h)$ and $\frac{h}{e}$ is even. By Theorem 5, we can obtain more MDS codes with e' -Galois hulls of arbitrary dimensions from Classes 10, 12, 15 and 19. Taking Class 15 as an example, we show the specific steps as follows:

Table 3: Some examples satisfying the conditions that $\gcd(e', h) = e$ and $\frac{h}{e}$ is even

h	e	e'	h	e	e'
2	1	1	4	1	1, 3
4	2	2	6	1	1, 5
6	3	3	8	1	1, 3, 5, 7
8	2	2, 6	8	4	4
10	1	1, 3, 7, 9	10	5	5
12	1	1, 5, 7, 11	12	2	2, 10
12	3	3, 9	12	6	6

•**Step 1. Obtain e -Galois self-orthogonal codes.**

For example, taking $(p, h, t, e) = (3, 8, 2, 1)$ in Class 15 (i.e., Theorem III.2 of [5]), we know that $[6561, k]_{3^8}$ l -dim 1-Galois hull GRS codes exist, where $1 \leq k \leq 1640$ and $0 \leq l \leq k$. Take $l = k = 1640$, then $[6561, 1640]_{3^8}$ is a 1-Galois self-orthogonal GRS code.

•**Step 2. Determine $\deg(h(x))$.**

According to Remark 1, $h(x) = \lambda^{-1}g(x)$. Hence, we only need to determine the structure of $g(x)$. This is easy to do because, as the result 2) of Remark 1 said, $g(x) = f(x)^{p^e}$ was given explicitly in the proof of Theorem III.2 of [5]. Taking $f(x) = 1$ further, we have $g(x) = f(x)^{p^e} = 1$. Therefore, we can directly determine that $h(x) = \lambda^{-1}g(x) = 1$ and $\deg(h(x)) = 0$, where $\lambda = 1 \in \mathbb{F}_{3^8}^*$.

•**Step 3. Derive new MDS codes with e' -Galois hulls of arbitrary dimensions.**

By the result 1) of Theorem 5 and Table 3, MDS codes with 1, 3, 5 and 7-Galois hulls of arbitrary dimensions can be derived as follows:

- $[6561, k_1]_{3^8}$ MDS code with l -dim 1-Galois hull for $1 \leq k_1 \leq 1640$, where $0 \leq l \leq k_1$;
- $[6561, k_3]_{3^8}$ MDS code with l -dim 3-Galois hull for $1 \leq k_3 \leq 235$, where $0 \leq l \leq k_3$;
- $[6561, k_5]_{3^8}$ MDS code with l -dim 5-Galois hull for $1 \leq k_5 \leq 27$, where $0 \leq l \leq k_5$;
- $[6561, k_7]_{3^8}$ MDS code with l -dim 7-Galois hull for $1 \leq k_7 \leq 3$, where $0 \leq l \leq k_7$;

Note that $2 \times 3 = 6$, $2 \times 5 = 10$, $2 \times 7 = 14$ are not divisors of $h = 8$, hence they cannot be constructed by Classes 10, 12, 15 and 19, which implies that all of these MDS codes with Galois hulls of arbitrary dimensions are new.

3.2. MDS codes with Galois hulls of arbitrary dimensions from Hermitian self-orthogonal (extended) GRS codes

Throughout this subsection, we take h as an even positive integer and $e = \frac{h}{2}$. For any prime p , let $q = p^h$, then \sqrt{q} is still a prime power. Since the Galois hull is a generalization of the Hermitian hull, we can conclude that $\text{GRS}_k(\mathbf{a}, \mathbf{v})$ (resp. $\text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)$) is Hermitian self-orthogonal if $\text{GRS}_k(\mathbf{a}, \mathbf{v}) \subseteq$

$\text{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp \frac{h}{2}}$ (resp. $\text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty) \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)^{\perp \frac{h}{2}}$). In this subsection, our main goal is to construct MDS codes with Galois hulls of arbitrary dimensions from Hermitian self-orthogonal (extended) GRS codes. To this end, we need the following lemma.

Lemma 7. *Let $q = p^h$, where p is a prime and h is an even positive integer.*

- 1) *If $\text{GRS}_k(\mathbf{a}, \mathbf{v}) \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp \frac{h}{2}}$, then there exists a monic polynomial $h(x) \in \mathbb{F}_q[x]$ with $\deg(h(x)) \leq n - k - 1$ such that $\lambda u_i h(a_i) = v_i^{\sqrt{q}+1}$, $1 \leq i \leq n$, where $\lambda \in \mathbb{F}_q^*$.*
- 2) *If $\text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty) \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)^{\perp \frac{h}{2}}$ with $k \geq 2$, then there exists a monic polynomial $h(x) \in \mathbb{F}_q[x]$ with $\deg(h(x)) \leq n - k - 1$ such that $\lambda u_i h(a_i) = v_i^{\sqrt{q}+1}$, $1 \leq i \leq n$, where $\lambda \in \mathbb{F}_q^*$.*

Proof. The proof of this lemma is similar to Lemma 3, so it is omitted. \square

Remark 3. *Similar to Remark 1, the structure and degree of $h(x)$ here can also be easily determined.*

Theorem 8. *Let $q = p^h$ be an odd prime power, where h is an even positive integer. Let $0 \leq e' \leq h - 1$ and such that $\frac{h}{\gcd(e', h)}$ is odd. Then the following hold.*

- 1) *Suppose $\text{GRS}_m(\mathbf{a}, \mathbf{v}) \subseteq \text{GRS}_m(\mathbf{a}, \mathbf{v})^{\perp \frac{h}{2}}$, then for $1 \leq k \leq \lfloor \frac{p^{e'} + n - 1 - \deg(h(x))}{p^{e'} + 1} \rfloor$, there exists an $[n, k]_q$ MDS code \mathcal{C} with $\dim(\text{Hull}_{e'}(\mathcal{C})) = l$, where $0 \leq l \leq k$.*
- 2) *Suppose $\text{GRS}_m(\mathbf{a}, \mathbf{v}, \infty) \subseteq \text{GRS}_m(\mathbf{a}, \mathbf{v}, \infty)^{\perp \frac{h}{2}}$ with $m \geq 2$, then for $1 \leq k \leq \lfloor \frac{p^{e'} + n - 1 - \deg(h(x))}{p^{e'} + 1} \rfloor$, there exists an $[n + 1, k]_q$ MDS code \mathcal{C} with $\dim(\text{Hull}_{e'}(\mathcal{C})) = l$, where $0 \leq l \leq k - 1$.*

Proof. 1) From $\text{GRS}_m(\mathbf{a}, \mathbf{v}) \subseteq \text{GRS}_m(\mathbf{a}, \mathbf{v})^{\perp \frac{h}{2}}$ and the result 1) of Lemma 7, there exists a monic polynomial $h(x) \in \mathbb{F}_q[x]$ with $\deg(h(x)) \leq n - m - 1$ such that

$$\lambda u_i h(a_i) = v_i^{\sqrt{q}+1} \neq 0, \quad 1 \leq i \leq n, \quad (10)$$

where $\lambda \in \mathbb{F}_q^*$. Note that $(v_i^{\sqrt{q}+1})^{\sqrt{q}} = v_i^{q-1+\sqrt{q}+1} = v_i^{\sqrt{q}+1}$, then $v_i^{\sqrt{q}+1} \in \mathbb{F}_{\sqrt{q}} \subseteq \mathbb{F}_q$ for $1 \leq i \leq n$. Hence there exists $v'_i \in \mathbb{F}_q^*$ such that

$$v_i^{\sqrt{q}+1} = v_i'^2, \quad 1 \leq i \leq n. \quad (11)$$

Since both $\frac{h}{\gcd(e', h)}$ and p are odd, by Lemma 2, $\gcd(p^{e'} + 1, p^h - 1) = 2$. Therefore, there exist two integers μ and ν such that $\mu(p^{e'} + 1) + \nu(p^h - 1) = 2$. Substituting it into Eqs. (10) and (11), we can get $(v'_i)^{\mu(p^{e'}+1)} = \lambda u_i h(a_i)$, $1 \leq i \leq n$. Denote $v''_i = (v'_i)^\mu$, $1 \leq i \leq n$, then

$$(v''_i)^{p^{e'}+1} = \lambda u_i h(a_i), \quad 1 \leq i \leq n.$$

Since $(q - 1) \nmid (p^{e'} + 1)$, there is an $\alpha \in \mathbb{F}_q^*$ such that $\beta = \alpha^{p^{e'}+1} \neq 1$. Let $\mathbf{a} = (a_1, a_2, \dots, a_n)$ be the same as before and $\mathbf{v}'' = (\alpha v''_1, \dots, \alpha v''_s, v''_{s+1}, \dots, v''_n)$, where $s = k - l \leq k$. We now consider the e' -Galois hull of the $[n, k]_q$ MDS code $\mathcal{C} = \text{GRS}_k(\mathbf{a}, \mathbf{v}'')$.

For any codeword

$$\mathbf{c} = (\alpha v''_1 f(a_1), \dots, \alpha v''_s f(a_s), v''_{s+1} f(a_{s+1}), \dots, v''_n f(a_n)) \in \text{Hull}_{e'}(\mathcal{C}),$$

where $f(x) \in \mathbb{F}_q[x]$ and $\deg(f(x)) \leq k-1$. Replace $\alpha^{p^{e'}+1}$ and $(v_i'')^{p^{e'}+1}$ with β and $\lambda u_i h(a_i)$, respectively. By the result 1) of Lemma 1, there exists a polynomial $g(x) \in \mathbb{F}_q[x]$ with $\deg(g(x)) \leq n-k-1$ such that

$$\begin{aligned} & (\beta \lambda u_1 h(a_1) f^{p^{e'}}(a_1), \dots, \beta \lambda u_s h(a_s) f^{p^{e'}}(a_s), \lambda u_{s+1} h(a_{s+1}) f^{p^{e'}}(a_{s+1}), \dots, \lambda u_n h(a_n) f^{p^{e'}}(a_n)) \\ &= (u_1 g(a_1), \dots, u_s g(a_s), u_{s+1} g(a_{s+1}), \dots, u_n g(a_n)). \end{aligned} \quad (12)$$

Similar to the result 1) of Theorem 5, we can deduce that $\lambda h(x) f^{p^{e'}}(x) = g(x)$ from the last $n-s$ coordinates of Eq. (12). Since $\beta \neq 1$ and $\lambda u_i h(a_i) \neq 0$, from the first s coordinates of Eq. (12), we can derive that $f(a_i) = 0$ for $1 \leq i \leq s$. Hence, $f(x)$ can be written as

$$f(x) = r(x) \prod_{i=1}^s (x - a_i)$$

for some $r(x) \in \mathbb{F}_q[x]$ with $\deg(r(x)) \leq k-1-s = l-1$. It deduces that $\dim(\text{Hull}_{e'}(\mathcal{C})) \leq l$.

Conversely, for any $f(x) = r(x) \prod_{i=1}^s (x - a_i)$, where $r(x) \in \mathbb{F}_q[x]$ with $\deg(r(x)) \leq k-1-s = l-1$. Let $g(x) = \lambda h(x) f^{p^{e'}}(x)$. Similar to the proof of the result 1) of Theorem 5 again, we can deduce that $\dim(\text{Hull}_{e'}(\mathcal{C})) \geq l$.

Combining both aspects, we have $\dim(\text{Hull}_{e'}(\mathcal{C})) = l$, where $0 \leq l \leq k$. The desired result follows.

2) Since $\text{GRS}_m(\mathbf{a}, \mathbf{v}, \infty) \subseteq \text{GRS}_m(\mathbf{a}, \mathbf{v}, \infty)^{\perp_{\frac{1}{2}}}$ with $m \geq 2$ and by the result 2) of Lemma 7, there exists a monic polynomial $h(x) \in \mathbb{F}_q[x]$ with $\deg(h(x)) \leq n-m-1$ such that $\lambda u_i h(a_i) = v_i^{\sqrt{q}+1}$, $1 \leq i \leq n$. For the same reason with 1) above, there exists $v_i' \in \mathbb{F}_q^*$ such that

$$(v_i')^{p^{e'}+1} = \lambda u_i h(a_i), \quad 1 \leq i \leq n.$$

Let $\alpha \in \mathbb{F}_q^*$ such that $\beta = \alpha^{p^{e'}+1} \neq 1$. Let $\mathbf{a} = (a_1, a_2, \dots, a_n)$ be the same as before and $\mathbf{v}' = (\alpha v_1', \dots, \alpha v_s', v_{s+1}', \dots, v_n')$, where $s = k-l-1 \leq k-1$. We now consider the e' -Galois hull of the $[n+1, k]_q$ MDS code $\mathcal{C} = \text{GRS}_k(\mathbf{a}, \mathbf{v}', \infty)$.

A completely similar argument to 1) above and Part 2) of Theorem 5 implies $\dim(\text{Hull}_{e'}(\mathcal{C})) = l$, where $0 \leq l \leq k-1$. This completes the proof. \square

Remark 4. 1) According to Theorem 8, we can construct MDS codes with Galois hulls of arbitrary dimensions via Hermitian self-orthogonal (extended) GRS codes. As we know, there are lots of Hermitian self-orthogonal (extended) GRS codes constructed in previous works.

2) Note that the conditions of Theorems 5 and 8 are different, so they can lead to different results in general. We list some examples satisfying the condition that $\frac{h}{\gcd(e', h)}$ is odd in Table 3. Then the following example allows us to intuitively see the difference between Theorems 5 and 8. Start from the Hermitian (i.e., 5-Galois) self-orthogonal (extended) GRS code over $\mathbb{F}_{p^{10}}$ with odd prime p . From Table 4, we can see that MDS codes with 0, 2, 4, 6 and 8-Galois hulls of arbitrary dimensions can be obtained by Theorem 8, while from Table 3, we can see that only MDS codes with 5-Galois hulls of arbitrary dimensions can be derived from Theorem 5. Clearly, they are totally different.

Table 4: Some examples satisfying the condition that $\frac{h}{\gcd(e', h)}$ is odd

h	e'	h	e'
4	0	6	0, 2, 4
8	0	10	0, 2, 4, 6, 8
12	0, 4, 8	14	0, 2, 4, 6, 8, 10, 12

Note that in some known constructions of Hermitian self-orthogonal (extended) GRS codes, the dimension k is usually roughly upper bounded by $\lfloor \frac{\sqrt{q}+n-1}{\sqrt{q}+1} \rfloor$ (e.g., see [11, 12, 15, 37, 38] and references therein), while the dimension k of our MDS codes with e' -Galois hulls of arbitrary dimensions constructed by Theorem 8 is upper bounded by $\lfloor \frac{p^{e'}+n-1-\deg(h(x))}{p^{e'}+1} \rfloor$. We compare the magnitude of these two bounds in the following theorem, and it turns out that in some cases the range of dimension of the new MDS codes with e' -Galois hulls of arbitrary dimensions will be wider.

Theorem 9. *Let $q = p^h$ be a prime power, where h is an even positive integer. Let $0 \leq e' < \frac{h}{2}$ be an integer and $\deg(h(x))$ be known. Then $\lfloor \frac{p^{e'}+n-1-\deg(h(x))}{p^{e'}+1} \rfloor > \lfloor \frac{\sqrt{q}+n-1}{\sqrt{q}+1} \rfloor$ if one of the following two conditions holds.*

- 1) $\deg(h(x)) = 0$ and $n \geq 3$;
- 2) $\deg(h(x)) > 0$, $0 \leq e' \leq \lfloor \log_p \frac{\sqrt{q}(n-3) - (\sqrt{q}+1)\deg(h(x)) - 1}{\sqrt{q}+n-1} \rfloor$ and $n \geq \lfloor \frac{4\sqrt{q} + (\sqrt{q}+1)\deg(h(x))}{\sqrt{q}-1} \rfloor$.

Proof. For the condition 1), we note that when $\deg(h(x)) = 0$, the new upper bound is $\lfloor \frac{p^{e'}+n-1}{p^{e'}+1} \rfloor$. Let $k(e') = \frac{p^{e'}+n-1}{p^{e'}+1}$ be a function of e' , where $0 \leq e' < \frac{h}{2}$. Easy to calculate, the first derivative of $k(e')$ is

$$k'(e') = \frac{(2-n)p^{e'} \ln p}{(p^{e'}+1)^2}, \quad 0 \leq e' < \frac{h}{2}.$$

It follows that $k(e')$ is monotonically decreasing for each $0 \leq e' < \frac{h}{2}$ from the fact $k'(e') < 0$ for $n \geq 3$. Since $0 \leq e' < \frac{h}{2}$ is an integer, we can easily conclude that the desired result holds.

For the condition 2), let $\Delta k = \frac{p^{e'}+n-1-\deg(h(x))}{p^{e'}+1} - \frac{\sqrt{q}+n-1}{\sqrt{q}+1}$. Then it is easy to verify that under the condition 2), we have

$$\begin{aligned} \Delta k &= \frac{(p^{e'}+n-1-\deg(h(x)))(\sqrt{q}+1) - (\sqrt{q}+n-1)(p^{e'}+1)}{(p^{e'}+1)(\sqrt{q}+1)} \\ &= \frac{(n-2)(\sqrt{q}-p^{e'}) - (\sqrt{q}+1)\deg(h(x))}{(p^{e'}+1)(\sqrt{q}+1)} \\ &\geq 1. \end{aligned}$$

It follows that $\lfloor \frac{p^{e'}+n-1-\deg(h(x))}{p^{e'}+1} \rfloor > \lfloor \frac{\sqrt{q}+n-1}{\sqrt{q}+1} \rfloor$. This completes the proof. \square

Remark 5. 1) We consider condition 1) and condition 2) separately in Theorem 9. On one hand, condition 1) is more explicit and has a weaker requirement for n than condition 2). Specifically, taking $\deg(h(x)) = 0$ in condition 2), it requires $n \geq \lfloor \frac{4\sqrt{q}}{\sqrt{q}-1} \rfloor = 4 + \lfloor \frac{4}{\sqrt{q}-1} \rfloor$, while $n \geq 3$ is required in condition 1). On the other hand, clearly, $\deg(h(x)) = 0$ is a relatively special situation.

- 2) According to Remarks 1 and 3, we can easily determine $h(x)$ and $\deg(h(x))$ when a Hermitian self-orthogonal (extended) GRS code is given. Hence, $\deg(h(x))$ in Theorem 9 is indeed known.

Example 10. We list some known Hermitian self-orthogonal (extended) GRS codes and further explain the role of Theorem 8.

- 1) From Theorems 2.3, 2.5 of [21] and Theorems 2, 3 of [15], there exists a q -ary Hermitian self-orthogonal GRS code of length n if any of the following conditions holds:
- $t \mid (q-1)$, $r \leq \frac{q-1}{t}$, $k \leq \frac{t-1}{\sqrt{q}+1}$, $n = rt$ or $n = rt + 1$;
 - $2 \leq n \leq q$, $n = n_1 + n_2 + \dots + n_t$ with $1 \leq t \leq \sqrt{q}$ and $2 \leq n_i \leq \sqrt{q}$ for all $1 \leq i \leq t$, $1 \leq k \leq \frac{\min\{n_1, \dots, n_t\}}{2}$;
 - $1 \leq m \leq \sqrt{q}$, $n = m(\sqrt{q} - 1)$ and $1 \leq k \leq \lfloor \frac{m\sqrt{q}-1}{\sqrt{q}+1} \rfloor$;
 - $1 \leq s \leq \sqrt{q} - 1$, $n = s(\sqrt{q} + 1)$ and $1 \leq k \leq s - 1$.
- 2) From Theorems 3.10, 3.11 of [14], Theorem 3.6 of [20], and Proposition 1 of [11], there exists a q -ary Hermitian self-dual or self-orthogonal extended GRS code of length $n + 1$ if any of the following conditions holds:
- $n = 2k - 1$, $n \leq \sqrt{q}$, $\mathbf{a} = (a_1, a_2, \dots, a_n) \in A_t^n$, where the definition of A_t^n see [14];
 - $n = 2k - 1$, $n \leq \sqrt{q}$, $\mathbf{a} = (a_1, a_2, \dots, a_n) \in A_{t,m}^n$, where the definition of $A_{t,m}^n$ see [14];
 - $n = q$, $0 \leq k \leq \sqrt{q}$;
 - $n = t(\sqrt{q} + 1) + 1$, $1 \leq t \leq \sqrt{q} - 1$ and $1 \leq k \leq t + 1$ with $(t, k) \neq (\sqrt{q} - 1, \sqrt{q} - 1)$.

According to Theorem 8 and Table 4, if $h = 6, 10, 14$, we can get twenty-four, forty and fifty-six classes of MDS codes with Galois hulls of arbitrary dimensions, respectively.

Example 11. Similar to Example 6, we show step by step how the new MDS codes with e' -Galois hulls of arbitrary dimensions are generated by known Hermitian self-orthogonal (extended) GRS codes.

- 1) New MDS codes with e' -Galois hulls of arbitrary dimensions can be derived from a Hermitian self-orthogonal GRS code as following steps:

•Step 1. Obtain Hermitian self-orthogonal GRS codes.

For example, taking $(q, m) = (3^6, 20)$, $h(x) = x^7 \in \mathbb{F}_{3^6}[x]$ and $\lambda = 26\omega^{76} \in \mathbb{F}_{3^6}^*$ in Theorem 2 of [15], we can get $[520, k]_{3^6}$ Hermitian self-orthogonal GRS codes for each $1 \leq k \leq 19$. Consider the $[520, 19]_{3^6}$ Hermitian self-orthogonal GRS code.

•Step 2. Determine $\deg(h(x))$.

Note that $\lambda u_i h(a_i) = v_i^{\sqrt{q}+1}$, $1 \leq i \leq 520$ for $h(x) = x^7$ and $\lambda = 26\omega^{76}$ in Theorem 2 of [15]. Therefore, according to Lemma 7 and Theorem 8, $h(x) = x^7$ is the $h(x)$ we are looking for. Hence, $\deg(h(x)) = 7$. (Note that we do not need to use the intermediate tool $g(x)$ at this time).

•Step 3. Derive new MDS codes with e' -Galois hulls of arbitrary dimensions.

By the result 1) of Theorem 8 and Table 4, we can obtain MDS codes with 0, 2 and 4-Galois hulls of arbitrary dimensions as follows:

- $[520, k_0]_{3^6}^{**}$ MDS code with l -dim 0-Galois hull for $1 \leq k_0 \leq 256$, where $0 \leq l \leq k_0$;
- $[520, k_2]_{3^6}^{**}$ MDS code with l -dim 2-Galois hull for $1 \leq k_2 \leq 52$, where $0 \leq l \leq k_2$;
- $[520, k_4]_{3^6}^{**}$ MDS code with l -dim 4-Galois hull for $1 \leq k_4 \leq 7$, where $0 \leq l \leq k_4$.

2) New MDS codes with e' -Galois hulls of arbitrary dimensions can be derived from a Hermitian self-orthogonal extended GRS code as following steps:

• **Step 1. Obtain Hermitian self-orthogonal extended GRS codes.**

For example, taking $q = 3^{10}$ and $(t, k) = (200, 100)$ in Proposition 1 of [11], we can get a $[48802, 100]_{3^{10}}$ Hermitian self-orthogonal extended GRS code.

• **Step 2. Determine $\deg(h(x))$.**

Similar to Example 6, since $h(x) = \lambda^{-1}g(x)$, we only need to determine the structure of $g(x)$. According to the proof of Proposition 1 of [11], $g(x) = -m(x)^{\sqrt{q}+1}f^{\sqrt{q}}(x)$, where $m(x) \in \mathbb{F}_{3^{10}}[x]$ is a monic polynomial with $\deg(m(x)) = t + 1 - k = 101$. Taking $f(x) = 1$ and $\lambda = -1$ further, we have $h(x) = \lambda^{-1}g(x) = m(x)^{244}$. Hence, $\deg(h(x)) = 244 \times 101 = 24644$.

• **Step 3. Derive new MDS codes with e' -Galois hulls of arbitrary dimensions.**

By the result 2) of Theorem 8 and Table 4, we can obtain MDS codes with 0, 2, 4, 6 and 8-Galois hulls of arbitrary dimensions as follows:

- $[48802, k_0]_{3^{10}}^{**}$ MDS code with l -dim 0-Galois hull for $1 \leq k_0 \leq 12079$, where $0 \leq l \leq k_0 - 1$;
- $[48802, k_2]_{3^{10}}^{**}$ MDS code with l -dim 2-Galois hull for $1 \leq k_2 \leq 2416$, where $0 \leq l \leq k_2 - 1$;
- $[48802, k_4]_{3^{10}}^{**}$ MDS code with l -dim 4-Galois hull for $1 \leq k_4 \leq 295$, where $0 \leq l \leq k_4 - 1$;
- $[48802, k_6]_{3^{10}}^{**}$ MDS code with l -dim 6-Galois hull for $1 \leq k_6 \leq 34$, where $0 \leq l \leq k_6 - 1$;
- $[48802, k_8]_{3^{10}}^{**}$ MDS code with l -dim 8-Galois hull for $1 \leq k_8 \leq 4$, where $0 \leq l \leq k_8 - 1$.

Remark 6. We now discuss the dimensions of the new MDS codes with Galois hulls of arbitrary dimensions obtained in Example 11. Note that $\deg(h(x)) = 7$ in the result 1) of Example 11. Hence, by Theorems 8 and 9, we can obtain new MDS codes with larger dimensions and e' -Galois hulls of arbitrary dimensions when $0 \leq e' \leq \lfloor \log_p \frac{\sqrt{q}(n-3) - (\sqrt{q}+1)\deg(h(x)) - 1}{\sqrt{q}+n-1} \rfloor = \lfloor \log_3 \frac{27 \times (517) - (27+1) \times 7 - 1}{27+520-1} \rfloor = 2$. For the result 2) of Example 11, we note that $\deg(h(x)) = 24644$. Similarly, we can obtain new MDS codes with larger dimensions and e' -Galois hulls of arbitrary dimensions when $0 \leq e' \leq \lfloor \log_3 \frac{243 \times (48799) - (243+1) \times 24644 - 1}{243+48802-1} \rfloor = 4$. We have marked them in Example 11 with ******.

3.3. Some explicit constructions of MDS codes with Galois hulls of arbitrary dimensions

In this subsection, we construct two classes of MDS codes with Galois hulls of arbitrary dimensions. The conditions we use are relatively stringent. But applying Theorem 5, these newly obtained Galois self-orthogonal GRS codes will generate more MDS codes with Galois hulls of arbitrary dimensions. This means that, with the help of Theorem 5, many new MDS codes with Galois hulls of arbitrary dimensions can still be obtained by using stricter conditions. To this end, we need the following lemma.

Lemma 12. Let m, h be two positive integers and $m \mid h$. Suppose that there is a positive integer t such that $2^t \mid \frac{h}{m}$. Then for any element $x \in \mathbb{F}_{p^m}$, there exists $v \in \mathbb{F}_{p^h}$ such that $x = v^{2^t}$.

Proof. Since $2^t \mid \frac{h}{m}$, there exists a positive integer s such that $h = 2^t \cdot sm$. Then \mathbb{F}_{p^h} can be viewed as the $2^t \cdot s$ -th extension field of \mathbb{F}_{p^m} . It follows that any element $x \in \mathbb{F}_{p^m}$ can be written as $x = v^{2^t}$, where $v \in \mathbb{F}_{p^h}$. \square

Let notations be the same as before, we now consider the additive subgroup of \mathbb{F}_{p^h} and its cosets. We know that \mathbb{F}_{p^h} can be seen as a linear space over \mathbb{F}_{p^m} of dimension $\frac{h}{m}$. Suppose $1 \leq w \leq p^m$ and $1 \leq z \leq \frac{h}{m} - 1$. Let H be an \mathbb{F}_{p^m} -subspace of \mathbb{F}_{p^h} of dimension z . Choose $\eta \in \mathbb{F}_{p^h} \setminus H$. We label the elements of \mathbb{F}_{p^m} as $\beta_1 = 0, \beta_2, \dots, \beta_{p^m}$. For $1 \leq j \leq w$, define

$$H_j = H + \beta_j \eta = \{h + \beta_j \eta \mid h \in H\}.$$

Since $\beta_i \neq \beta_j$ for any $1 \leq i \neq j \leq n$, then $H_i \cap H_j = \emptyset$. Let $n = wp^{mz}$ and

$$\bigcup_{j=1}^w H_j = \{a_1, a_2, \dots, a_n\}. \quad (13)$$

Let a_i and u_i be defined as in Eqs. (13) and (1), we have the following lemma which has been shown in [12].

Lemma 13. ([12], Lemma 3.1) For a given $1 \leq i \leq n$, suppose $a_i \in H_b$ for some $1 \leq b \leq w$. Then

$$u_i = \left(\prod_{h \in H, h \neq 0} h^{-1} \right) \left(\prod_{g \in H} (\eta - g)^{1-w} \right) \left(\prod_{1 \leq j \leq t, j \neq b} (\beta_b - \beta_j)^{-1} \right).$$

In particular, let $\varepsilon = (\prod_{h \in H, h \neq 0} h) (\prod_{g \in H} (\eta - g)^{w-1})$, then $\varepsilon u_i \in \mathbb{F}_{p^m}^*$.

The following lemma can be derived directly by Lemmas 12 and 13.

Lemma 14. Let notations be the same as before, for any $\varepsilon u_i \in \mathbb{F}_{p^m}^*$, there exists $v_i \in \mathbb{F}_{p^h}^*$ such that

$$\varepsilon u_i = v_i^{2^t}. \quad (14)$$

Theorem 15. Let p be an odd prime. Let m, h be two positive integers with $m \mid h$ and $q = p^h$. Let $n = wp^{mz}$, where $1 \leq w \leq p^m$ and $1 \leq z \leq \frac{h}{m} - 1$. Suppose that t is a positive integer such that $2^t \mid \frac{h}{m}$ and $2^t = p^e + 1$ for some $0 \leq e \leq h - 1$. Then the following hold.

- 1) For $1 \leq k \leq \lfloor \frac{p^e + n - 1}{p^e + 1} \rfloor$, there exists an $[n, k]_q$ MDS code \mathcal{C} with $\dim(\text{Hull}_e(\mathcal{C})) = l$, where $0 \leq l \leq k$.
- 2) For $1 \leq k \leq \lfloor \frac{p^e + n - 1}{p^e + 1} \rfloor$, there exists an $[n + 1, k]_q$ MDS code \mathcal{C} with $\dim(\text{Hull}_e(\mathcal{C})) = l$, where $0 \leq l \leq k - 1$.

Proof. 1) Let notations be the same as before. By Lemma 14, there exists $v_i \in \mathbb{F}_{p^h}^*$ such that $\varepsilon u_i = v_i^{2^t}$ for $1 \leq i \leq n$. Since $(p^h - 1) \nmid (p^e + 1)$ for any $0 \leq e \leq h - 1$, there is an $\alpha \in \mathbb{F}_{p^h}^*$ such that $\beta = \alpha^{p^e + 1} \neq 1$. Let $\mathbf{a} = (a_1, a_2, \dots, a_n)$ and $\mathbf{v} = (\alpha v_1, \dots, \alpha v_s, v_{s+1}, \dots, v_n)$, where $s = k - l \leq k$. We now consider the q -ary MDS code $\mathcal{C} = \text{GRS}_k(\mathbf{a}, \mathbf{v})$.

Note that $2^t = p^e + 1$, similar to the proofs of the result 1) of Theorem 5 and the result 1) of Theorem 8, we can prove that $\dim(\text{Hull}_e(\mathcal{C})) = l$, where $0 \leq l \leq k$.

2) Let $s = k - l - 1 \leq k - 1$. We now consider the q -ary MDS code $\mathcal{C} = \text{GRS}_k(\mathbf{a}, \mathbf{v}, \infty)$. Taking a similar way as the result 2) of Theorem 5 and the result 2) of Theorem 8, we can also easily deduce that $\dim(\text{Hull}_e(\mathcal{C})) = l$, where $0 \leq l \leq k - 1$. \square

Table 5: Some examples satisfying the conditions $2^t = p^e + 1$ and $2^t \mid \frac{h}{m}$ for $e = 1$

p	t	m	h	q	p	t	m	h	q
3	2	1	4	81	3	2	2	8	6561
3	2	3	12	531441	3	2	4	16	43046721
3	2	5	20	3586784401	3	2	6	24	282429536481
3	2	7	28	22876792454961	3	2	8	32	1853020188851841
7	3	1	8	5764801	7	3	2	16	33232930569601
7	3	3	24	191581231380566414401	7	3	4	32	110442767424392064630529920

Example 16. In order to illustrate the practical significance of Theorem 15, we list some examples satisfying the condition $2^t = p^e + 1$ and $2^t \mid \frac{h}{m}$ for $e = 1$ in Table 5. We explain that our constructions are new and flexible by the following comparisons.

- 1) From Table 1, we can see that Classes 12, 13 and 17 have similar conditions with our results in Theorem 15. However, it is not difficult to find that $a \mid e$ (i.e., $m \mid e$) in Classes 12 and 13 or $t \mid (p^e - 1)$ (i.e., $w \mid (p^e - 1)$) in Class 17 do not need to be satisfied in our constructions. Hence our constructions will get some codes with new lengths. For example, taking $(p, t, m, h, e) = (7, 3, 2, 16, 1)$ in Theorem 15, we have $n = w \cdot 49^z$, where $1 \leq w \leq 49$, $1 \leq z \leq 7$. Then applying Theorem 15, we still can get many MDS codes with 1-Galois hulls of arbitrary dimensions, but Classes 12 and 13 will not be able to obtain these MDS codes because of $a \nmid e$ (since $a = 2$, $e = 1$ here, but $2 \nmid 1$). And Class 17 can only take $n = t \cdot 7^r$, where $t = 1, 2, 3, 6$ and $1 \leq r \leq 15$. Clearly, most code lengths in Theorem 15 are new.
- 2) Although we only list the case where $e = 1$ in Table 5, according to the result 1) of Theorem 5, we can get more new MDS codes with Galois hulls of arbitrary dimensions. For example, taking $(p, t, m, h, e) = (3, 2, 1, 8, 1)$, we can obtain $[w \cdot 3^z, k]_{3^8}$ 1-Galois self-orthogonal GRS codes (i.e., taking $l = k$ in the result 1) of Theorem 15), where $1 \leq w \leq 3$, $1 \leq z \leq 7$ and $1 \leq k \leq \lfloor \frac{w \cdot 3^z + 2}{4} \rfloor$. Similar to Example 6, one can easily determine that $h(x) = 1$ and $\deg(h(x)) = 0$. Then by the result 1) of Theorem 5 and Table 3, we can obtain $[w \cdot 3^z, k_1]_{3^8}$ MDS codes with 3-Galois hulls of arbitrary dimensions, $[w \cdot 3^z, k_2]_{3^8}$ MDS codes with 5-Galois hulls of arbitrary dimensions and $[w \cdot 3^z, k_3]_{3^8}$ MDS codes with 7-Galois hulls of arbitrary dimensions, where $1 \leq k_1 \leq \lfloor \frac{w \cdot 3^z + 26}{28} \rfloor$, $1 \leq k_2 \leq \lfloor \frac{w \cdot 3^z + 242}{244} \rfloor$ and $1 \leq k_3 \leq \lfloor \frac{w \cdot 3^z + 2186}{2188} \rfloor$. Finally, by Example 6 again, these codes are

also new. This fact shows that relatively strict conditions can also lead to many new classes of MDS codes with Galois hulls of arbitrary dimensions with the help of Theorem 5.

Remark 7. We further discuss the condition $2^t = p^e + 1$ when e takes different values.

- 1) Take $e = 0$, then $t \equiv 1$ and the results produced by the direct application of Theorem 15 are exactly the conclusions of Euclidean hull studied in the results (i) and (ii) of Theorem 3.3 of [12]. Hence, Theorem 15 is actually a generalization of [12].
- 2) Take $e = 1$, then $p = 2^t - 1$, which is the famous Mersenne prime. And t must be a prime in this case. As we know, there is a well known conjecture that the number of Mersenne primes is infinite.
- 3) Take $2 \leq e \leq h - 1$, then $p^e = 2^t - 1$, which implies that the odd prime p should be the unique prime factor of a Mersenne composite number. In fact, we can easily check that if e is even, there is no p satisfying the condition, but if e is odd, this maybe an open problem because of the difficulty of decomposition of Mersenne composite numbers.

For more information about Mersenne primes, we refer to [13, 18, 19, 31] and references therein.

4. Summary and concluding remarks

In this paper, three different methods are used to construct six new classes of MDS codes with Galois hulls of arbitrary dimensions (See Theorems 5, 8 and 15). Specifically, the first two general methods allow us to construct more MDS codes with Galois hulls of arbitrary dimensions from Hermitian self-orthogonal (extended) GRS codes and general Galois self-orthogonal (extended) GRS codes. As stated in Theorem 9, the new MDS codes with Galois hulls of arbitrary dimensions derived from Hermitian self-orthogonal (extended) GRS codes have larger dimensions in some cases.

In the third method, we use a relatively strict condition $2^t = p^e + 1$ to present two explicit constructions of MDS codes with Galois hulls of arbitrary dimensions. In particular, one of them can derive 1-Galois self-orthogonal GRS codes, and with the help of Theorem 5, more MDS codes with Galois hulls of arbitrary dimensions can be obtained from them directly (See Example 16). This fact shows that in our study, some relatively strict conditions can also lead to many new classes of MDS codes with Galois hulls of arbitrary dimensions.

As one can see, in our constructions, the determination of the dimensions of the new MDS codes with Galois hulls of arbitrary dimensions derived from known Galois or Hermitian self-orthogonal (extended) GRS codes depends on $\deg(h(x))$. Fortunately, according to Remarks 1 and 3, $\deg(h(x))$ is easy to be determined, whether it is calculated by Lagrange Interpolation Formula, or obtained directly from previous research results.

In conclusion, the methods proposed in this paper are convenient and efficient in constructing MDS codes with Galois hulls of arbitrary dimensions. For future research, it might be interesting to construct more Galois self-orthogonal (extended) GRS codes.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (Nos.U21A20428 and 12171134).

References

- [1] E.F. Assmus, J.D. Key, Designs and Their Codes, Cambridge Univ. Press. (1993),103.
- [2] T. Brun, I. Devetak, M. Hsieh, Correcting quantum errors with entanglement, Science. 314(5798) (2006),436-439.
- [3] A. Calderbank, P. Shor, Good quantum error-correcting codes exist, Phys. Rev. A. 54(2) (1996),1098-1105.
- [4] C. Carlet, S. Guilley, Complementary dual codes for counter-measures to side-channel attacks, Coding Theory and Applications, Springer, Cham. (2015),97-105.
- [5] M. Cao, MDS Codes With Galois Hulls of Arbitrary Dimensions and the Related Entanglement-Assisted Quantum Error Correction, IEEE Trans. Inf. Theory. 67(12) (2021),7964-7984.
- [6] H. Chen, New MDS Entanglement-Assisted Quantum Codes from MDS Hermitian Self-Orthogonal Codes, arXiv:2206.13995 [cs.IT]. (2022).
- [7] X. Chen, S. Zhu, X. Kai, Entanglement-assisted quantum MDS codes constructed from constacyclic codes, Quantum Inf. Process. 17(10) (2018),273.
- [8] X. Fang, R. Jin, J. Luo, W. M, New Galois Hulls of GRS Codes and Application to EAQECCs, Cryptogr. Commun. 14 (2022),145-159.
- [9] Y. Fu, H. Liu, Galois self-orthogonal constacyclic codes over finite fields, Des. Codes Cryptogr. (2021),1-31.
- [10] Y. Fan, L. Zhang, Galois self-dual constacyclic codes, Des. Codes Cryptogr. 84(3) (2017),473-492.
- [11] W. Fang, F. Fu, Two new classes of quantum MDS codes, Finite Fields Appl. 53 (2018),85-98.
- [12] W. Fang, F. Fu, L. Li, S. Zhu, Euclidean and hermitian hulls of mds codes and their applications to eaqeccs, IEEE Trans. Inf. Theory. 66(6) (2020),3527-3527.
- [13] D.B. Gillies, Three new Mersenne primes and a statistical theory, Math. Comput. 18(85) (1964),93-97.
- [14] G. Guo, R. Li, Hermitian Self-Dual GRS and Extended GRS Codes, IEEE Commun. Lett. 25(4) (2021),1062-1065.

- [15] G. Guo, R. Li, Y. Liu, Application of Hermitian self-orthogonal GRS codes to some quantum MDS codes, *Finite Fields Appl.* 76 (2021).
- [16] K. Guenda, S. Jitman, T. A. Gulliver, Constructions of good entanglement-assisted quantum error correcting codes, *Des. Codes Cryptogr.* 86 (2018),121-136.
- [17] N. Gao, J. Li, S. Huang, Hermitian Hulls of Constacyclic Codes and Their Applications to Quantum Codes, *Int. J. Theor. Phys.* 61(3) (2022),1-14.
- [18] R.K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Springer, New York. (2004).
- [19] G. H. JO, D. KIM, MERSENNE PRIME FACTOR AND SUM OF BINOMIAL COEFFICIENTS, *Journal of applied mathematics and informatics.* 40(1₂) (2022),61-68.
- [20] L. Jin, C. Xing, A Construction of New Quantum MDS Codes, *IEEE Trans. Inf. Theory.* 60(5) (2014),2921-2925.
- [21] L. Jin, S. Ling, J. Luo, C. Xing, Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes, *IEEE Trans. Inf. Theory.* 56(9) (2010),4735-4740.
- [22] C. Li, C. Ding, S. Li, LCD Cyclic Codes Over Finite Fields, *IEEE Trans. Inf. Theory.* 63(7) (2017),4344-4356.
- [23] G. Luo, X. Cao, Two new families of entanglement-assisted quantum MDS codes from generalized Reed-Solomon codes, *Quantum Inf. Process.* 18(3) (2019),89
- [24] G. Luo, X. Cao, X. Chen, MDS codes with hulls of arbitrary dimensions and their quantum error correction, *IEEE Trans. Inf. Theory.* 65(5) (2018),2944-2952.
- [25] H. Liu, P. Xu, Galois hulls of linear codes over finite fields, *Des. Codes Cryptogr.* 88 (2) (2020),241-255.
- [26] L. Li, S. Zhu, L. Liu, and X. Kai, Entanglement-assisted quantum MDS codes from generalized Reed-Solomon codes, *Quantum Inf. Process.* 18(5) (2019),153.
- [27] J. Leon, Computing automorphism groups of errorcorrecting codes, *IEEE Trans. Inf. Theory.* 28(3) (1982),496-511.
- [28] J.S. Leon, Permutation group algorithms based on partition, *Theory and algorithms. J. Symb. Comput.* 12 (1991),533-583.
- [29] X. Liu, H. Liu, L. Yu, New EAQEC codes constructed from Galois LCD codes, *Quantum Inf. Process.* 19(20) (2020).
- [30] Y. Liu, R. Li, L. Lv, and Y. Ma, Application of constacyclic codes to entanglement-assisted quantum maximum distance separable codes, *Quantum Inf. Process.* 17(8) (2018),210.

- [31] L. Murata, C. Pomerance, On the largest prime factor of a Mersenne number, *Number theory*. 36 (2004),209-218.
- [32] L. Qian, X. Cao, X. Wu, W. Lu, Entanglement-assisted quantum codes from 1-Galois hulls MDS codes of arbitrary dimensions, preprint. (2019).
- [33] A. M. Steane, Error correcting codes in quantum theory, *Phys. Rev. Lett.* 77(5) (1996),793-797.
- [34] A. Sharma, V. Chauhan, Skew multi-twisted codes over finite fields and their Galois duals, *Finite Fields Appl.* 59 (2019),297-334.
- [35] N. Sendrier, Finding the permutation between equivalent binary code, in *Proceedings of IEEE ISIT 1997*, Ulm, Germany. (1997),367.
- [36] N. Sendrier, Finding the permutation between equivalent codes: The support splitting algorithm, *IEEE Trans. Inf. Theory*. 46(4) (2000),1193-1203.
- [37] G. Wang, C. Tang, Some constructions of optimal subsystem codes derived GRS codes, *Quantum Inf. Process.* 21(8) (2022),1-16.
- [38] G. Wang, C. Tang, Some entanglement-assisted quantum MDS codes with large minimum distance, *Quantum Inf. Process.* 21(8) (2022),1-20.
- [39] L. Wang, S. Zhu, New quantum MDS codes derived from constacyclic codes, *Quantum Inf. Process.* 14(3) (2015),881-889.
- [40] Y. Wu, C. Li, S. Yang, New Galois hulls of generalized Reed-Solomon codes, *Finite Fields Appl.* 83 (2022),102084.