AIMS Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 9(6): 13553–13569.
DOI: 10.3934/math.2024661
Received: 15 February 2024
Revised: 16 March 2024
Accepted: 01 April 2024
Published: 12 April 2024

Research article

Dimensions of the hull of generalized Reed-Solomon codes

Jing Huang[1,*], **Jingge Liu**[2] **and Dong Yu**[2]

[1] School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China

[2] School of Mathematics, South China University of Technology, Guangzhou 510641, China

* **Correspondence:** Email: jhuangmath@foxmail.com.

Abstract: Let $\mathrm{GRS}_k(\boldsymbol{\alpha}, \boldsymbol{v})$ be a k-dimensional generalized Reed-Solomon (GRS) code over $\mathbb{F}_q$ associated with $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\boldsymbol{v} = (v_1, \ldots, v_n)$. In this paper, we determined the dimension of the Euclidean hull $\mathrm{GRS}_k(\boldsymbol{\alpha}, \boldsymbol{v}) \cap \mathrm{GRS}_k(\boldsymbol{\alpha}, \boldsymbol{v})^{\perp}$, which addresses an open problem posed in [Chen et al., IEEE-TIT, 2023]. We also presentd a new approach to generating all self-dual RS codes.

Keywords: hull of a code; generalized Reed-Solomon code; algebraic geometry code
Mathematics Subject Classification: 94B05, 94B50

1. Introduction

In recent years, determining the dimensions of the hulls of generalized Reed-Solomon (GRS) codes has become a hot research topic. One of the principal reasons is that the hulls of linear codes play an important role in the so-called entanglement-assisted quantum error-correcting codes (EAQECCs). For a linear code C, let $C^{\perp}$ be the dual code of C with respect to some inner product. The *hull* of C is defined as $C \bigcap C^{\perp}$.

Luo et al. [1] presented several classes of GRS codes, extended GRS codes with Euclidean hulls of arbitrary dimensions, and constructed some families of maximum distance separable (MDS) EAQECCs. Fang et al. [2] obtained several new families of MDS EAQECCs with flexible parameters from GRS codes and extended GRS codes, where they can determine the dimensions of their Euclidean hulls or Hermitian hulls. Fang et al. [3] constructed MDS codes with Euclidean hulls of arbitrary dimensions from self-orthogonal codes. Cao [4] gave 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; eleven families of MDS codes with ℓ-Galois hulls of arbitrary dimensions were constructed explicitly. Some problems relating hulls of linear codes were also considered; see [5–7]. Very recently, Chen et al. [8] determined the dimensions of the hulls of all RS codes via an algebraic geometry approach. The paper concludes with a problem of how to extend the main result of [8] to all GRS codes.

The purpose of this paper is to address the aforementioned problem posed in [8]. By further exploring the methods in Luo et al. [1] and Chen et al. [8], we manage to find the dimensions of the hulls of all GRS codes under the Euclidean inner product. Consequently, our results contain the main result of [8]. As a corollary, we also give a new approach to generate all self-dual RS codes. More explicitly, we obtain the following result.

Theorem 1.1. *Assume that* $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})$ *is a k-dimensional GRS code over* $\mathbb{F}_q$ *asscociated with* $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$ *and* $\boldsymbol{v} = (v_1, \dots, v_n)$. *Let*

$$h = \prod_{i=1}^{n}(z - \alpha_i)$$

and let h' *denote the derivative of* h. *Let* $u(z) \in \mathbb{F}_q[z]$ *be a polynomial satisfying* $u(\alpha_i) = v_i (1 \le i \le n)$ *and* $\deg u(z) = n$. *By polynomial long division,*

$$u^2 h' = Q_0 h + R_0$$

with $\deg R_0 < n$. *Using polynomial long division repeatedly,*

$$h = Q_1 R_0 + R_1$$

with $\deg R_1 < \deg R_0$, *and*

$$R_i = Q_{i+2} R_{i+1} + R_{i+2}$$

with $\deg R_{i+2} < \deg R_{i+1}$ *for* $i \ge 0$, *we have*

$$\dim\left(\mathrm{GRS}_k(\boldsymbol{\alpha}, \boldsymbol{v}) \bigcap \mathrm{GRS}_k(\boldsymbol{\alpha}, \boldsymbol{v})^{\perp}\right) = \begin{cases} \min\{k, n-k-\deg R_0\}, & \text{if } \deg R_0 \le n-k, \\ \min\{s_{a-1}, n-k-\deg R_a\}, & \text{if } a \ge 1 \text{ is the smallest integer} \\ \text{satisfying } \deg R_a \le n-k \text{ and } & \deg R_{a-1} = n-k+s_{a-1} > n-k. \end{cases}$$

This paper is organized as follows. Definitions and preliminary facts about rational function fields and algebraic geometry codes are reviewed in Section 2. In Section 3, we present a proof for Theorem 1.1, which is broken into a series of lemmas. In Section 4, we derive some corollaries of Theorem 1.1. Lastly, Section 5 concludes this paper.

2. Preliminaries

In this section, after reviewing some basic facts about rational function fields and algebraic geometry codes, we restate that GRS codes can be viewed as a particular subclass of algebraic geometry codes. For the details or the general theory of algebraic function fields and algebraic geometry codes, interested readers may refer to [9] for the details.

Throughout this paper, let $\mathbb{F}_q$ be the finite field of order q and let z be a transcendental element over $\mathbb{F}_q$. Let $\mathbb{F}_q[z]$ be the polynomial ring in variable z over $\mathbb{F}_q$. The extension field $\mathbb{F}_q(z)/\mathbb{F}_q$ is called a rational function field, where $\mathbb{F}_q(z)$ denotes the set of all rational functions, i.e.,

$$\mathbb{F}_q(z) = \left\{ \frac{f(z)}{g(z)} \,\middle|\, f(z), g(z) \in \mathbb{F}_q[z],\ g(z) \ne 0 \right\}.$$

In this paper, we always use F to denote $\mathbb{F}_q(z)$. A *valuation ring* of $F/\mathbb{F}_q$ is a ring $\mathcal{O}$ satisfying

$$\mathbb{F}_q \subsetneq \mathcal{O} \subsetneq F$$

and, for any $x \in F$, either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$. It turns out that $\mathcal{O}$ is a local ring, i.e., $\mathcal{O}$ has a unique maximal ideal (see [9, Proposition 1.1.5]). A *place* P of the rational function field $F/\mathbb{F}_q$ is the maximal ideal of some valuation ring $\mathcal{O}$ of $F/\mathbb{F}_q$. The set of all places of $F/\mathbb{F}_q$ is denoted by $\mathbb{P}_F$. By [9, Theorem 1.2.2], one has

$$\mathbb{P}_F = \left\{P_{p(z)} \,\middle|\, p(z) \text{ is a monic irreducible polynomial over } \mathbb{F}_q\right\} \bigcup \{P_\infty\},$$

where $P_{p(z)}$ and P_∞ are defined in [9]. The degree of the monic irreducible polynomial $p(z)$ is equal to the degree of the place $P_{p(z)}$, and the degree of P_∞ is equal to 1 (for the definition of the degree of a place, see [9, Definition 1.1.14]). For each $\alpha \in \mathbb{F}_q$, the places $P_{z-\alpha}$ (P_α for short) and P_∞ are called rational places of $F/\mathbb{F}_q$. A divisor G of $F/\mathbb{F}_q$ is a formal sum

$$G = \sum_{P \in \mathbb{P}_F} v_P(G) P$$

with $v_P(G)$ being integers and only finitely many $v_P(G)$ being nonzero when P runs over $\mathbb{P}_F$. The support of G is a subset of $\mathbb{P}_F$ defined as

$$\operatorname{supp}(G) = \left\{P \in \mathbb{P}_F \,\middle|\, v_P(G) \neq 0\right\}.$$

The degree of the divisor

$$G = \sum_{P \in \mathbb{P}_F} v_P(G) P,$$

denoted by $\deg G$ (or $\deg(G)$), is defined to be

$$\deg G = \sum_{P \in \mathbb{P}_F} v_P(G) \deg P,$$

where for a place $P \in \mathbb{P}_F$, $\deg P$ is the degree of P. Two divisors

$$G = \sum_{P \in \mathbb{P}_F} v_P(G) P \quad \text{and} \quad G' = \sum_{P \in \mathbb{P}_F} v_P(G') P$$

are added coefficient-wise

$$G + G' = \sum_{P \in \mathbb{P}_F} (v_P(G) + v_P(G')) P.$$

$$\operatorname{Div}(F) = \left\{G \,\middle|\, G \text{ is a divisor of } F/\mathbb{F}_q\right\}$$

is a group according to the above addition. A *partial ordering* on $\operatorname{Div}(F)$ is defined by

$$G_1 \le G_2 \iff v_P(G_1) \le v_P(G_2) \quad \text{for all} \quad P \in \mathbb{P}_F.$$

Let

$$G_1 = \sum_{P \in \mathbb{P}_F} v_P(G_1)P \quad \text{and} \quad G_2 = \sum_{P \in \mathbb{P}_F} v_P(G_2)P$$

be two divisors of $F/\mathbb{F}_q$. The intersection $G_1 \bigcap G_2$ of G_1 and G_2 is defined to be a divisor of $F/\mathbb{F}_q$ given by

$$G_1 \bigcap G_2 = \sum_{P \in \mathbb{P}_F} \min\{v_P(G_1), v_P(G_2)\} P.$$

The union $G_1 \bigcup G_2$ of G_1 and G_2 is defined to be

$$G_1 \bigcup G_2 = \sum_{P \in \mathbb{P}_F} \max\{v_P(G_1), v_P(G_2)\} P.$$

It is easily seen that

$$\deg(G_1 \bigcap G_2) + \deg(G_1 \bigcup G_2) = \deg(G_1) + \deg(G_2). \tag{2.1}$$

Suppose that a nonzero polynomial $f(z) \in \mathbb{F}_q[z]$ has the canonical irreducible factorization

$$f(z) = a \prod_{i=1}^{s} p_i(z)^{r_i}$$

with a being a nonzero element of $\mathbb{F}_q$, $r_i > 0$ being positive integers, and $p_i(z)$ being pairwise distinct monic irreducible polynomials over $\mathbb{F}_q$ for $1 \le i \le s$. The divisor

$$\sum_{i=1}^{s} r_i P_{p_i(z)} - (\deg f) P_\infty$$

of $F/\mathbb{F}_q$ is denoted by (f). Generally, for a nonzero rational function

$$h = \frac{f(z)}{g(z)} \in \mathbb{F}_q(z),$$

the *principal divisor* (h) is defined as (f)–(g); after combing like terms in (f)–(g), (h) can be uniquely written as

$$(h) = \sum_{P \in S} m_P P - \sum_{Q \in R} n_Q Q$$

with $m_P > 0$ for any $P \in S$ and $n_Q > 0$ for any $Q \in R$. The divisor $\sum_{P \in S} m_P P$ is called the *zero divisor* of h, which is denoted by $(h)_0$; the divisor $\sum_{Q \in R} n_Q Q$ is called the *pole divisor* of h, which is denoted by $(h)_\infty$. Using such terminologies, every principal divisor can be uniquely expressed as $(h) = (h)_0 - (h)_\infty$. It is well-known that $\deg(h)_0 = \deg(h)_\infty$ (see [9, Theorem 1.4.11]), and, particularly, all principal divisors have degree zero.

For a divisor G of $F/\mathbb{F}_q$, the *Riemann-Roch space* asscociated to G (denoted by $\mathscr{L}(G)$) is defined by

$$\mathscr{L}(G) = \left\{ h \in F \setminus \{0\} \,\middle|\, (h) + G \ge 0 \right\} \bigcup \{0\}.$$

For any divisor G, $\mathscr{L}(G)$ is a finite dimensional linear space over $\mathbb{F}_q$. The dimension of $\mathscr{L}(G)$ is denoted by $\ell(G)$ or $\dim(\mathscr{L}(G))$. We will frequently use the following lemmas.

Lemma 2.1. *([9, Corollary 1.4.12, Theorem 1.5.17]) Let* $G \in \mathrm{Div}(\mathbb{F}_q(z))$*. If* $\deg G \leq -1$*, then* $\ell(G) = 0$*. If* $\deg G \geq -1$*, then*

$$\ell(G) = \deg G + 1.$$

Lemma 2.2. *([10, Lemma 2.6]) Let* $G_1, G_2 \in \mathrm{Div}(\mathbb{F}_q(z))$*, then*

$$\mathscr{L}(G_1)\bigcap \mathscr{L}(G_2) = \mathscr{L}(G_1 \bigcap G_2).$$

Remark 2.3. *If* $\deg(G_1 \bigcap G_2) \leq -1,$ *then* $\mathscr{L}(G_1) + \mathscr{L}(G_2)$ *is a direct sum.*

Lemma 2.4. *([8, Lemma 7(1)]) Let* $G_1, G_2 \in \mathrm{Div}(\mathbb{F}_q(z))$*. If* $\deg(G_1 \bigcap G_2) \geq -1,$ *then*

$$\mathscr{L}(G_1) + \mathscr{L}(G_2) = \mathscr{L}(G_1 \bigcup G_2).$$

We are now ready to present the $\mathscr{L}$-construction of algebraic geometry codes.

Definition 2.5. *Let* $P_1, \ldots, P_n$ *be pairwise distinct rational places of* $F/\mathbb{F}_q$ *and let*

$$D = P_1 + \ldots + P_n.$$

Let G be a divisor of $F/\mathbb{F}_q$ *satisfying*

$$\mathrm{supp}(G)\bigcap \mathrm{supp}(D) = \emptyset.$$

The algebraic geometry code $C_{\mathscr{L}}(D, G)$ *associated with the divisors D and G is defined as the image of the evaluation map* $\mathrm{ev_D}$*:* $\mathscr{L}(G) \longrightarrow \mathbb{F}_q^n$ *given by*

$$\mathrm{ev_D}(f) = (f(P_1), \ldots, f(P_n)) \in \mathbb{F}_q^n \quad \textit{for any} \quad f \in \mathscr{L}(G),$$

namely,

$$C_{\mathscr{L}}(D, G) = \mathrm{ev_D}(\mathscr{L}(G)) = \left\{(f(P_1), \ldots, f(P_n)) \,\middle|\, f \in \mathscr{L}(G)\right\}.$$

The next lemma is useful in calculating the dimension of the Euclidean hull of $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})$.

Lemma 2.6. *([9, Proposition 2.3.2] Let* $C_{\mathscr{L}}(D, G)$ *be a k-dimensional algebraic geometry code of length n over* $\mathbb{F}_q$*, as given in Definition 2.5, then* $k = n$ *if and only if* $\deg G \geq n - 1$*.*

For $1 \leq k \leq n$, the k-dimensional GRS code of length n associated with $\mathbf{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ is defined to be

$$GRS_k(\mathbf{a}, \mathbf{v}) = \left\{(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)) \,\middle|\, f(X) \in \mathbb{F}_q[X], \deg f(X) \leq k - 1\right\}.$$

The following result is useful in this paper, which represents the GRS codes in terms of the divisors of the rational function field $F/\mathbb{F}_q$.

Lemma 2.7. ([9, Propositions 2.2.10 and 2.3.5, Lemma 2.3.6]) *Consider the rational function field* $F/\mathbb{F}_q$ *and* $\alpha_1, \ldots, \alpha_n, \upsilon_1, \ldots, \upsilon_n \in \mathbb{F}_q$*, where* $\alpha_1, \ldots, \alpha_n$ *are pairwise distinct. Let*

$$h = \prod_{i=1}^{n}(z - \alpha_i) \quad \textit{and} \quad P_i = P_{z-\alpha_i}$$

be the places corresponding to the irreducible polynomials $z-\alpha_i$ *for* $1 \le i \le n$. *Let* $D = P_1+\ldots+P_n$. *For the k-dimensional GRS code* $\mathrm{GRS}_k(\boldsymbol{\alpha}, \boldsymbol{v})$ *associated with* $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ *and* $\boldsymbol{v} = (v_1, \ldots, v_n)$, *we have*

$$GRS_k(\boldsymbol{\alpha}, \boldsymbol{v}) = C_{\mathscr{L}}(D, (k-1)P_\infty - (u)),\ GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})^\perp = C_{\mathscr{L}}(D, (n-k-1)P_\infty + (u) + (h')),$$

where $h' \in \mathbb{F}_q[z]$ *is the derivative of the polynomial h and,* $u \in \mathbb{F}_q[z]$ *satisfies* $u(\alpha_i) = v_i$ $(1 \le i \le n)$, *and* $\deg u = n$.

From now on, we fix the notation and conditions in Lemma 2.7 and define

$$G_1 = (k-1)P_\infty - (u),\ G_2 = (n-k-1)P_\infty + (u) + (h'),\ \text{and } r = n - 1 - \deg h'.$$

3. Proof of Theorem 1.1

The main purpose of this section is to present a proof for Theorem 1.1. Our ultimate goal is to find the exact value of the dimension of

$$GRS_k(\boldsymbol{\alpha}, \boldsymbol{v}) \cap GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})^\perp.$$

By linear algebra, we have

$$\dim\left(GRS_k(\boldsymbol{\alpha}, \boldsymbol{v}) \cap GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})^\perp\right) = n - \dim\left(GRS_k(\boldsymbol{\alpha}, \boldsymbol{v}) + GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})^\perp\right). \tag{3.1}$$

We first need the next lemma.

Lemma 3.1. *Let the notations be the same as before, then* $\dim\left(GRS_k(\boldsymbol{\alpha}, \boldsymbol{v}) + GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})^\perp\right)$ *is equal to*

$$\dim\ (\mathscr{L}(G_1) + \mathscr{L}(G_2) + \mathscr{L}(G_1 \cup G_2 - D)) - \dim\ (\mathscr{L}(G_1 \cup G_2)) + \dim\ (C_{\mathscr{L}}(D, G_1 \cup G_2)).$$

Proof. Note that $G_i \le G_1 \cup G_2,\ i = 1, 2$, then

$$\mathscr{L}(G_i) \subseteq \mathscr{L}(G_1 \cup G_2),\ C_{\mathscr{L}}(D, G_i) \subseteq C_{\mathscr{L}}(D, G_1 \cup G_2),\ i = 1, 2,$$

and, thus,

$$\mathscr{L}(G_1) + \mathscr{L}(G_2) \subseteq \mathscr{L}(G_1 \bigcup G_2),\ C_{\mathscr{L}}(D, G_1) + C_{\mathscr{L}}(D, G_2) \subseteq C_{\mathscr{L}}(D, G_1 \cup G_2).$$

Consider the $\mathbb{F}_q$-linear map

$$\mathrm{ev_D} : \mathscr{L}(G_1 \cup G_2) \to \mathbb{F}_q^n,\ x \mapsto (x(P_1), \ldots, x(P_n)).$$

It is easily verified that

$$\mathrm{Ker}(\mathrm{ev_D}) = \mathscr{L}(G_1 \cup G_2 - D), \quad \mathrm{Im}(\mathrm{ev_D}) = C_{\mathscr{L}}(D, G_1 \cup G_2).$$

Hence, we have an $\mathbb{F}_q$-linear isomorphism,

$$\mathscr{L}(G_1 \cup G_2)/\mathscr{L}(G_1 \cup G_2 - D) \cong C_{\mathscr{L}}(D, G_1 \cup G_2),$$

which implies

$$\dim(\mathscr{L}(G_1 \cup G_2 - D)) = \dim(\mathscr{L}(G_1 \cup G_2)) - \dim(C_{\mathscr{L}}(D, G_1 \cup G_2)).$$

On the other hand, we have

$$\begin{aligned}\mathrm{ev_D}(\mathscr{L}(G_1) + \mathscr{L}(G_2) + \mathscr{L}(G_1 \cup G_2 - D)) &= \mathrm{ev_D}(\mathscr{L}(G_1)) + \mathrm{ev_D}(\mathscr{L}(G_2)) + \mathrm{ev_D}(\mathscr{L}(G_1 \cup G_2 - D)) \\ &= C_{\mathscr{L}}(D, G_1) + C_{\mathscr{L}}(D, G_2),\end{aligned}$$

which yields an $\mathbb{F}_q$-linear isomorphism,

$$\frac{\mathscr{L}(G_1) + \mathscr{L}(G_2) + \mathscr{L}(G_1 \cup G_2 - D)}{\mathscr{L}(G_1 \cup G_2 - D)} \cong C_{\mathscr{L}}(D, G_1) + C_{\mathscr{L}}(D, G_2). \tag{3.2}$$

Therefore, the dimension of $C_{\mathscr{L}}(D, G_1) + C_{\mathscr{L}}(D, G_2)$ is equal to

$$\dim(\mathscr{L}(G_1) + \mathscr{L}(G_2) + \mathscr{L}(G_1 \cup G_2 - D)) - \dim(\mathscr{L}(G_1 \cup G_2)) + \dim(C_{\mathscr{L}}(D, G_1 \cup G_2)).$$

Using Lemma 2.7, the proof is done. □

According to Eq (3.1) and Lemma 2.7, it is enough for us to determine

$$\dim(\mathscr{L}(G_1 \cup G_2)), \ \ \dim(C_{\mathscr{L}}(D, G_1 \cup G_2))$$

and

$$\dim(\mathscr{L}(G_1) + \mathscr{L}(G_2) + \mathscr{L}(G_1 \cup G_2 - D)).$$

It is easy to calculate $\dim(\mathscr{L}(G_1 \cup G_2))$ and $\dim(C_{\mathscr{L}}(D, G_1 \cup G_2))$. More explicitly, we have the following lemma.

Lemma 3.2. *Let the notations be the same as before. We have*

$$\dim(\mathscr{L}(G_1 \cup G_2)) = 3n + k - r - 1, \quad \dim(C_{\mathscr{L}}(D, G_1 \cup G_2)) = n. \tag{3.3}$$

Proof. We note that $n + k - 1 > -n - k + r$, then

$$\begin{aligned}G_1 \cup G_2 &= (n + k - 1)P_\infty + (u)_0 + (h')_0 \\ &= (3n + k - r - 2)P_\infty + (u) + (h'),\end{aligned}$$

which implies

$$\deg(G_1 \cup G_2) = 3n + k - r - 2 \geq \max\{-1, \ n - 1\}.$$

According to Lemmas 2.1 and 2.6, we have

$$\dim(\mathscr{L}(G_1 \cup G_2)) = \deg(G_1 \cup G_2) + 1 = 3n + k - r - 1$$

and

$$\dim(C_{\mathscr{L}}(D, G_1 \cup G_2)) = n.$$

□

Now, we are going to determine $\dim(\mathscr{L}(G_1)+\mathscr{L}(G_2)+\mathscr{L}(G_1\cup G_2-D))$. To this end, we have to find an $\mathbb{F}_q$-basis of $\mathscr{L}(G_1)$, $\mathscr{L}(G_2)$, and $\mathscr{L}(G_1\cup G_2-D)$, respectively. Indeed, we have the next lemma.

Lemma 3.3. *With our notation, we have:*

1) The set $\left\{u, uz, \ldots, uz^{k-1}\right\}$ *is an* $\mathbb{F}_q$*-basis of* $\mathscr{L}(G_1)$*;*

2) The set $\left\{\frac{1}{uh'}, \frac{z}{uh'}, \ldots, \frac{z^{n-k-1}}{uh'}\right\}$ *is an* $\mathbb{F}_q$*-basis of* $\mathscr{L}(G_2)$*;*

3) The set $\left\{\frac{h}{uh'}, \frac{zh}{uh'}, \frac{z^2h}{uh'}, \ldots, \frac{z^{2n+k-r-2}h}{uh'}\right\}$ *is an* $\mathbb{F}_q$*-basis of* $\mathscr{L}(G_1\cup G_2-D)$*.*

Therefore, $\mathscr{L}(G_1)+\mathscr{L}(G_2)+\mathscr{L}(G_1\cup G_2-D)$ *is equal to the* $\mathbb{F}_q$*-linear space*

$$\left\langle u, uz, \ldots, uz^{k-1}, \frac{1}{uh'}, \frac{z}{uh'}, \ldots, \frac{z^{n-k-1}}{uh'}, \frac{h}{uh'}, \frac{zh}{uh'}, \frac{z^2h}{uh'}, \ldots, \frac{z^{2n+k-r-2}h}{uh'}\right\rangle.$$

Proof. (1) Recall that

$$G_1=(k-1)P_\infty-(u).$$

By

$$\deg G_1=k-1\geq -1$$

and Lemma 2.1,

$$\dim(\mathscr{L}(G_1))=\deg(G_1)+1=k.$$

It is easily seen that the set $\left\{u, uz, \ldots, uz^{k-1}\right\}$ is linearly independent over $\mathbb{F}_q$, so it is enough to show $uz^j\in\mathscr{L}(G_1)$, $j=0,1,\ldots,k-1$. Indeed, for any $0\leq j\leq k-1$,

$$\begin{aligned}(uz^j)+G_1&=(u)+j(z)+(k-1)P_\infty-(u)\\&=j(P_0-P_\infty)+(k-1)P_\infty\\&=jP_0+(k-1-j)P_\infty\geq 0.\end{aligned}$$

Hence, $uz^j\in\mathscr{L}(G_1)$, $j=0,1,\ldots,k-1$.

(2) Since

$$G_2=(n-k-1)P_\infty+(u)+(h').$$

Then by

$$\deg G_1=k-1\geq -1$$

and Lemma 2.1,

$$\dim(\mathscr{L}(G_2))=\deg(G_2)+1=n-k.$$

Obviously, the set $\left\{\frac{1}{uh'}, \frac{z}{uh'}, \ldots, \frac{z^{n-k-1}}{uh'}\right\}$ is linearly independent over $\mathbb{F}_q$. On the other hand, for any $0\leq j\leq n-k-1$, we have

$$\begin{aligned}(\tfrac{z^j}{uh'})+G_2&=j(z)-(u)-(h')+(n-k+1)P_\infty+(u)+(h')\\&=j(P_0-P_\infty)+(n-k-1)P_\infty\\&=jP_0+(n-k-1-j)P_\infty\\&\geq 0.\end{aligned}$$

Hence, $\frac{z^j}{uh'} \in \mathscr{L}(G_2),\ j = 0, 1, \ldots, n-k-1$. The proof of (2) is complete.

(3) Note that we have proved

$$\dim(\mathscr{L}(G_1 \cup G_2 - D)) = 2n + k - r - 1$$

in Lemma 3.2. Obviously, $\left\{\frac{h}{uh'}, \frac{zh}{uh'}, \frac{z^2h}{uh'}, \ldots, \frac{z^{2n+k-r-2}h}{uh'}\right\}$ is linearly independent over $\mathbb{F}_q$, so it is enough to show $\frac{z^jh}{uh'} \in \mathscr{L}(G_1 \cup G_2 - D)$, for any $0 \leq j \leq 2n + k - r - 2$. Since $n + k - 1 > -n - k + r$,

$$G_1 \cup G_2 = (n + k - 1)P_\infty + (u)_0 + (h')_0 = (3n + k - r - 2)P_\infty + (u) + (h').$$

Thus,

$$G_1 \cup G_2 - D = (3n + k - r - 2)P_\infty + (u) + (h') - (P_1 + \ldots + P_n).$$

For any $0 \leq j \leq 2n + k - r - 2$,

$$\begin{aligned}
(\tfrac{z^jh}{uh'}) + G_1 \cup G_2 - D &= j(z) + (h) - (u) - (h') + (3n + k - r - 2)P_\infty + (u) + (h') - (P_1 + \ldots + P_n) \\
&= j(P_0 - P_\infty) + (P_1 + \ldots + P_n) - nP_\infty + (3n + k - r - 2)P_\infty - (P_1 + \ldots + P_n) \\
&= jP_0 + (2n + k - r - 2 - j)P_\infty \\
&\geq 0.
\end{aligned}$$

Therefore, $\frac{z^jh}{uh'} \in \mathscr{L}(G_1 \cup G_2 - D)$ for any $0 \leq j \leq 2n + k - r - 2$. □

The next lemma determines $\dim(\mathscr{L}(G_1) + \mathscr{L}(G_2) + \mathscr{L}(G_1 \cup G_2 - D))$ completely.

Lemma 3.4. *Let the notations be the same as before. By polynomial long division,*

$$u^2h' = Q_0h + R_0$$

with $\deg R_0 \leq n - 1$. *Using polynomial long division repeatedly,* $h = Q_1R_0 + R_1$ *with* $\deg R_1 < \deg R_0$, *and*

$$R_i = Q_{i+2}R_{i+1} + R_{i+2}$$

with $\deg R_{i+2} < \deg R_{i+1}$ *for* $i \geq 0$. *We have*

$$\begin{aligned}
&\dim(\mathscr{L}(G_1) + \mathscr{L}(G_2) + \mathscr{L}(G_1 \cup G_2 - D)) \\
&= \begin{cases}
\max\{3n - r - 1,\ 2n + 2k - r - 1 + \deg R_0\}, & \text{if } \deg R_0 \leq n - k, \\
\max\{3n + k - r - 1 - s_{a-1},\ 2n + 2k - r - 1 + \deg R_a\}, & \text{if } a \geq 1 \text{ is the smallest integer} \\
\text{satisfying } \deg R_a \leq n - k \text{ and } \deg R_{a-1} = n - k + s_{a-1} > n - k. &
\end{cases}
\end{aligned} \tag{3.4}$$

Proof. By Lemma 3.3, we have

$$\begin{aligned}
&\dim(\mathscr{L}(G_1) + \mathscr{L}(G_2) + \mathscr{L}(G_1 \cup G_2 - D)) \\
&= \dim\left\langle u, uz, \ldots, uz^{k-1}, \tfrac{1}{uh'}, \tfrac{z}{uh'}, \ldots, \tfrac{z^{n-k-1}}{uh'}, \tfrac{h}{uh'}, \tfrac{zh}{uh'}, \tfrac{z^2h}{uh'}, \ldots, \tfrac{z^{2n+k-r-2}h}{uh'}\right\rangle \\
&= \dim\left\langle u^2h', u^2h'z, \ldots, u^2h'z^{k-1}, 1, z, \ldots, z^{n-k-1}, h, zh, \ldots, z^{2n+k-r-2}h\right\rangle.
\end{aligned}$$

For convenience, we use V to denote the $\mathbb{F}_q$-linear space

$$\left\langle u^2h', u^2h'z, \ldots, u^2h'z^{k-1}, 1, z, \ldots, z^{n-k-1}, h, zh, \ldots, z^{2n+k-r-2}h \right\rangle.$$

By polynomial long division, $u^2h' = Q_0h + R_0$ with $\deg R_0 \leq n-1$. It is readily seen that

$$\begin{aligned} V &= \left\langle R_0, R_0z, \ldots, R_0z^{k-1}, 1, z, \ldots, z^{n-k-1}, h, zh, \ldots, z^{2n+k-r-2}h \right\rangle \\ &= \mathscr{L}((k-1)P_\infty - (R_0)) + \mathscr{L}((n-k-1)P_\infty) + \mathscr{L}((2n+k-r-2)P_\infty - (h)), \end{aligned}$$

where the first equality holds because

$$Q_0hz^j \in \left\langle h, zh, \ldots, z^{2n+k-r-2}h \right\rangle \quad \text{and} \quad u^2h'z^j = Q_0hz^j + R_0z^j, \ \forall\, 0 \leq j \leq k-1.$$

We distinguish the following cases:

(1) $\deg R_0 \leq n-k$.

In this case, we claim

$$\mathscr{L}((k-1)P_\infty - (R_0)) + \mathscr{L}((n-k-1)P_\infty) = \mathscr{L}(\max\{\deg R_0 + k - 1, n-k-1\} P_\infty).$$

Indeed,

$$(k-1)P_\infty - (R_0) = (\deg R_0 + k - 1)P_\infty - (R_0)_0$$

leading to

$$\begin{aligned} (n-k-1)P_\infty \cap ((k-1)P_\infty - (R_0)) &= \min\{n-k-1,\ \deg R_0 + k - 1\} P_\infty - (R_0)_0 \\ &= \min\{n-k-1-\deg R_0, k-1\} P_\infty - (R_0), \end{aligned}$$

and then by $\deg R_0 \leq n-k$,

$$\deg\left((n-k-1)P_\infty \bigcap ((k-1)P_\infty - (R_0))\right) = \min\{n-k-1-\deg R_0, k-1\} \geq -1.$$

By Lemma 2.4, we have

$$\begin{aligned} \mathscr{L}((k-1)P_\infty - (R_0)) + \mathscr{L}((n-k-1)P_\infty) &= \mathscr{L}(((k-1)P_\infty - (R_0)) \cup ((n-k-1)P_\infty)) \\ &= \mathscr{L}(\max\{\deg R_0 + k - 1, n-k-1\} P_\infty). \end{aligned}$$

On the other hand, we show that

$$\mathscr{L}(\max\{\deg R_0 + k - 1, n-k-1\} P_\infty) + \mathscr{L}((2n+k-r-2)P_\infty - (h))$$

is a direct sum. Indeed,

$$(2n+k-r-2)P_\infty - (h) = (3n+k-r-2)P_\infty - (h)_0 \ \text{ and } \ \max\{\deg R_0 + k - 1, n-k-1\} < 3n+k-r-2,$$

so,

$$\begin{aligned} &\max\{\deg R_0 + k - 1, n-k-1\} P_\infty \cap ((2n+k-r-2)P_\infty - (h)) \\ &= \max\{\deg R_0 + k - 1, n-k-1\} P_\infty - (h)_0 \end{aligned}$$

$$= \max\{\deg R_0 - n + k - 1, -k - 1\} P_\infty - (h),$$

and

$$\begin{aligned}
&\deg(\max\{\deg R_0 + k - 1, n - k - 1\}P_\infty \bigcap((2n + k - r - 2)P_\infty - (h))) \\
&= \max\{\deg R_0 - n + k - 1, -k - 1\} \\
&\leq -1.
\end{aligned}$$

By Remark 2.3, we arrive at the above direct sum. Therefore

$$\begin{aligned}
\dim V &= \dim(\mathscr{L}(\max\{\deg R_0 + k - 1, n - k - 1\} P_\infty)) + \dim(\mathscr{L}((2n + k - r - 2)P_\infty - (h))) \\
&= \max\{\deg R_0 + k, n - k\} + 2n + k - r - 1 \\
&= \max\{3n - r - 1,\ 2n + 2k + \deg R_0 - r - 1\}.
\end{aligned}$$

(2) $\deg R_0 > n - k$.

By polynomial long division, $h = Q_1 R_0 + R_1$ with $\deg R_1 < \deg R_0$. For convenience, let $s_0 = \deg R_0 - (n - k)$, then $1 \leq s_0 < k$. It is easily seen that

$$V = \left\langle R_0, R_0 z, \ldots, R_0 z^{k-1}, 1, z, \ldots, z^{n-k-1}, h, zh, \ldots z^{s_0-1}h \right\rangle \oplus \left\langle z^{s_0}h, \ldots, z^{2n+k-r-2}h \right\rangle,$$

since

$$\deg R_0 z^i \leq n - k + s_0 + k - 1 = n + s_0 - 1 < \deg z^{s_0} h \quad (0 \leq i \leq k - 1)$$

and

$$\deg z^j h \leq \deg z^{s_0} h \ (0 \leq j \leq s_0 - 1).$$

Thus, we get

$$\dim V = \dim \left\langle R_0, R_0 z, \ldots, R_0 z^{k-1}, 1, z, \ldots, z^{n-k-1}, h, zh, \ldots z^{s_0-1}h \right\rangle + 2n + k - r - 1 - s_0.$$

On the other hand, for any $0 \leq j \leq s_0 - 1$, we have

$$z^j h = z^j Q_1 R_0 + z^j R_1 \quad \text{and} \quad \deg z^j Q_1 = j + k - s_0 \leq k - 1,$$

so

$$\begin{aligned}
&\left\langle R_0, R_0 z, \ldots, R_0 z^{k-1}, 1, z, \ldots, z^{n-k-1}, h, zh, \ldots z^{s_0-1}h \right\rangle \\
&= \left\langle R_0, R_0 z, \ldots, R_0 z^{k-1}, 1, z, \ldots, z^{n-k-1}, R_1, zR_1, \ldots z^{s_0-1}R_1 \right\rangle \\
&= \mathscr{L}((k - 1)P_\infty - (R_0)) + \mathscr{L}((n - k - 1)P_\infty) + \mathscr{L}((s_0 - 1)P_\infty - (R_1)).
\end{aligned}$$

Hence, it is enough to determine the dimension of the sum of the above Riemann-Roch spaces.

We still need to discuss the degree of R_1.

(a) $\deg R_1 \leq n - k$.

In this case, we claim:

$$\begin{aligned}
\mathscr{L}((n - k - 1)P_\infty) + \mathscr{L}((s_0 - 1)P_\infty - (R_1)) &= \mathscr{L}((n - k - 1)P_\infty \cup ((s_0 - 1)P_\infty - (R_1))) \\
&= \mathscr{L}(\max\{n - k - 1, s_0 - 1 + \deg R_1\} P_\infty).
\end{aligned}$$

By Lemma 2.4, we only need to show

$$\deg((n-k-1)P_\infty \cap ((s_0-1)P_\infty - (R_1))) \geq -1.$$

Indeed,

$$(s_0-1)P_\infty - (R_1) = (s_0 - 1 + \deg R_1)P_\infty - (R_1)_0,$$

so

$$\begin{aligned}(n-k-1)P_\infty \cap ((s_0-1)P_\infty - (R_1)) &= (n-k-1)P_\infty \cap ((s_0-1+\deg R_1)P_\infty - (R_1)_0)\\ &= \min\{n-k-1, s_0-1+\deg R_1\} P_\infty - (R_1)_0\\ &= \min\{n-k-1-\deg R_1, s_0-1\} P_\infty - (R_1),\end{aligned}$$

the degree of which is not less than -1.

On the other hand, we show that

$$\mathscr{L}((k-1)P_\infty - (R_0)) + \mathscr{L}(\max\{n-k-1, s_0-1+\deg R_1\} P_\infty)$$

is a direct sum. Indeed,

$$\deg R_0 > n-k, \;\; \deg R_1 \leq n-k \quad \text{and} \quad \deg R_0 = n-k+s_0,$$

so

$$n-k-1-\deg R_0 \leq -1 \quad \text{and} \quad s_0 - 1 + \deg R_1 - \deg R_0 = \deg R_1 - 1 - (n-k) \leq -1.$$

Therefore,

$$\begin{aligned}&\deg(((k-1)P_\infty - (R_0)) \cap (\max\{(n-k-1), s_0-1+\deg\ R_1\} P_\infty))\\ &= \deg(((k-1+\deg R_0)P_\infty - (R_0)_0) \cap (\max\{(n-k-1), s_0-1+\deg R_1\} P_\infty))\\ &= \deg(\min\{k-1+\deg R_0, \max\{(n-k-1), s_0-1+\deg R_1\}\} P_\infty - (R_0)_0)\\ &= \deg(\min\{k-1, \max\{n-k-1-\deg R_0, s_0-1+\deg R_1-\deg R_0\}\} P_\infty - (R_0))\\ &\leq -1,\end{aligned}$$

and, thus, we get the above direct sum by Remark 2.3. Hence, we have

$$\begin{aligned}&\dim(\mathscr{L}((k-1)P_\infty - (R_0)) + \mathscr{L}((n-k-1)P_\infty) + \mathscr{L}((s_0-1)P_\infty - (R_1)))\\ &= \dim(\mathscr{L}((k-1)P_\infty - (R_0)) \oplus \mathscr{L}(\max\{(n-k-1), s_0-1+\deg R_1\} P_\infty))\\ &= \dim(\mathscr{L}((k-1)P_\infty - (R_0))) + \dim(\mathscr{L}(\max\{(n-k-1), s_0-1+\deg R_1\} P_\infty))\\ &= k + \max\{n-k, s_0+\deg R_1\},\end{aligned}$$

which yields

$$\dim V = \max\{3n+k-r-1-s_0,\ 2n+2k-r-1+\deg R_1\}.$$

(b) $n-k < \deg R_1 < \deg R_0$.

Using polynomial long division repeatedly (if necessary),

$$R_i = Q_{i+2}R_{i+1} + R_{i+2}$$

with

$$\deg R_{i+2} < \deg R_{i+1}, \quad i = 0, 1, 2, \ldots.$$

Let $a \geq 1$ be the smallest integer such that

$$R_{a-2} = Q_a R_{a-1} + R_a$$

with $\deg R_a \leq n - k$. Suppose that

$$s_b = \deg R_b - (n-k), \quad b = 0, 1, \ldots, a-1.$$

It is the same as in the cases (1) and (a). We obtain

$$\begin{aligned}
\dim V &= \dim \left\langle R_0, R_0 z, \ldots, R_0 z^{k-1}, 1, z, \ldots, z^{n-k-1}, R_1, zR_1, \ldots\ldots z^{s_0-1} R_1 \right\rangle + 2n + k - r - 2 - s_0 + 1 \\
&= \dim \left(\left\langle R_0, R_0 z, \ldots, R_0 z^{s_1-1}, 1, z, \ldots, z^{n-k-1}, R_1, zR_1, \ldots z^{s_0-1} R_1 \right\rangle \oplus \left\langle R_0 z^{s_1}, \ldots, R_0 z^{k-1} \right\rangle \right) \\
&\quad +2n + k - r - 1 - s_0 \\
&= \dim \left\langle R_0, R_0 z, \ldots, R_0 z^{s_1-1}, 1, z, \ldots, z^{n-k-1}, R_1, zR_1, \ldots z^{s_0-1} R_1 \right\rangle + (k - s_1) \\
&\quad +2n + k - r - 1 - s_0 \\
&= \dim \left\langle R_0, R_0 z, \ldots, R_0 z^{s_1-1}, 1, z, \ldots, z^{n-k-1}, R_1, zR_1, \ldots z^{s_0-1} R_1 \right\rangle + 2n + 2k - r - 1 - s_0 - s_1 \\
&= \dim \left\langle R_2, R_2 z, \ldots, R_2 z^{s_1-1}, 1, z, \ldots, z^{n-k-1}, R_1, zR_1, \ldots z^{s_0-1} R_1 \right\rangle + 2n + 2k - r - 1 - s_0 - s_1 \\
&= \dim \left(\left\langle R_2, R_2 z, \ldots, R_2 z^{s_1-1}, 1, z, \ldots, z^{n-k-1}, R_1, zR_1, \ldots z^{s_2-1} R_1 \right\rangle \oplus \left\langle z^{s_2} R_1, \ldots, z^{s_0-1} R_1 \right\rangle \right) \\
&\quad +2n + 2k - r - 1 - s_0 - s_1 \\
&= \dim \left\langle R_2, R_2 z, \ldots, R_2 z^{s_1-1}, 1, z, \ldots, z^{n-k-1}, R_1, zR_1, \ldots z^{s_2-1} R_1 \right\rangle + (s_0 - s_2) \\
&\quad +2n + 2k - r - 1 - s_0 - s_1 \\
&= \dim \left\langle R_2, R_2 z, \ldots, R_2 z^{s_1-1}, 1, z, \ldots, z^{n-k-1}, R_3, zR_3, \ldots z^{s_2-1} R_3 \right\rangle + 2n + 2k - r - 1 - s_1 - s_2 \\
&= \ldots \\
&= \dim \left\langle R_{a-1}, R_{a-1} z, \ldots, R_{a-1} z^{s_{a-2}-1}, 1, z, \ldots, z^{n-k-1}, R_a, zR_a, \ldots z^{s_{a-1}-1} R_a \right\rangle \\
&\quad +2n + 2k - r - 1 - s_{a-2} - s_{a-1} \\
&= \dim \left(\mathscr{L}((s_{a-2} - 1)P_\infty + (R_{a-1})) + \mathscr{L}((n-k-1)P_\infty) + \mathscr{L}((s_{a-1} - 1)P_\infty - (R_a)) \right) \\
&\quad +2n + 2k - r - 1 - s_{a-2} - s_{a-1} \\
&= \dim(\mathscr{L}((s_{a-2} - 1)P_\infty + (R_{a-1})) \oplus \mathscr{L}(\max\{n-k-1, s_{a-1} - 1 + \deg R_a\} P_\infty) \\
&\quad +2n + 2k - r - 1 - s_{a-2} - s_{a-1} \\
&= s_{a-2} + \max\{n-k, s_{a-1} + \deg R_a\} + 2n + 2k - r - 1 - s_{a-2} - s_{a-1} \\
&= \max\{3n + k - r - 1 - s_{a-1}, 2n + 2k - r - 1 + \deg R_a\}.
\end{aligned}$$

□

Combining the above lemmas, we have finished the proof of Thoerem 1.1.

4. Corollaries of Theorem 1.1

In this section, we derive several corollaries of Theorem 1.1. In [8], the authors considered a special class of GRS codes, i.e., $\boldsymbol{v} = (1, \ldots, 1) \in (\mathbb{F}_q^*)^n$. Let

$$u(z) = \prod_{i=1}^{n} (z - \alpha_i) + 1.$$

We have $R_0 = h'$ in the equation

$$u^2 h' = Q_0 h + R_0 \quad \text{with} \quad \deg R_0 \le n-1.$$

Thus we get the next corollary, which coincides with the main result in [8].

Corollary 4.1. *Let $RS_k(\boldsymbol{\alpha})$ be a k-dimensional RS code over $\mathbb{F}_q$ associated with $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$. Let*

$$h = \prod_{i=1}^{n} (z - \alpha_i)$$

and let h' denote the derivative of h. Let $u(z) = h(z) + 1$. Using polynomial long division repeatedly,

$$h = Q_1 h' + R_1 \quad \textit{with} \quad \deg R_1 < \deg h',$$

and

$$R_i = Q_{i+2} R_{i+1} + R_{i+2} \quad \textit{with} \quad \deg R_{i+2} < \deg R_{i+1} \; \textit{for } i \ge 0,$$

where $R_0 := h'$, we have

$$\dim(\mathrm{RS}_k(\boldsymbol{\alpha}) \bigcap \mathrm{RS}_k(\boldsymbol{\alpha})^{\perp}) = \begin{cases} \min\{k, n-k-\deg h'\}, & \textit{if} \deg h' \le n-k, \\ \min\{s_{a-1}, n-k-\deg R_a\}, & \textit{if } a \ge 1 \textit{ is the smallest integer} \\ \textit{satisfying} \deg R_a \le n-k \;\; \textit{and} \;\; \deg R_{a-1} = n-k+s_{a-1} > n-k. \end{cases}$$

In Theorem 1.1, if $\deg R_0 \le n - 2k$, then $\deg R_0 \le n-k$ and $k \le n-k-\deg R_0$. By the first case in Theorem 1.1, we have

$$\dim(GRS_k(\boldsymbol{\alpha}, \boldsymbol{v}) \cap GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})^{\perp}) = k,$$

which implies that $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})$ is self-orthogonal. Hence, we have the next corollary.

Corollary 4.2. *Let $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})$ be a k-dimensional GRS code over $\mathbb{F}_q$ associated with $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\boldsymbol{v} = (v_1, \ldots, v_n)$. Let*

$$h = \prod_{i=1}^{n} (z - \alpha_i)$$

and let h' denote the derivative of h. Let $u(z) \in \mathbb{F}_q[z]$ be a polynomial satisfying $u(\alpha_i) = v_i$ $(1 \le i \le n)$ and $\deg u(z) = n$. By polynomial long division, $u^2 h' = Q_0 h + R_0$ with $\deg R_0 < n$. Using polynomial long division repeatedly, $h = Q_1 R_0 + R_1$ with $\deg R_1 < \deg R_0$, and $R_i = Q_{i+2} R_{i+1} + R_{i+2}$ with $\deg R_{i+2} < \deg R_{i+1}$ for $i \ge 0$. If $\deg R_0 \le n-2k$, then $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})$ is self-orthogonal.

The work [8, Corollary 19] gives a sufficient and necessary condition for an RS code to be a self-duality: Suppose $\mathrm{RS}_k(\boldsymbol{\alpha})$ is a k-dimensional RS code of length n over $\mathbb{F}_q$ associated with $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$. Let

$$h = \prod_{i=1}^{n} (z - \alpha_i)$$

and let h' be the derivative of h, then $\mathrm{RS}_k(\boldsymbol{\alpha})$ is self-dual if and only if $n = 2k$ and $\deg h' = 0$, or, equivalently, h' is a nonzero constant function. The following result suggests a new way to generate self-dual RS codes.

Corollary 4.3. *Let $\mathbb{F}_q$ be the finite field with characteristic p and let*

$$h = a_0 + a_1 x + b_1 x^p + b_2 x^{2p} + \ldots + b_m x^{mp}$$

be a polynomial over $\mathbb{F}_q$. Assume further that $\mathbb{F}_{q^\ell}$ is the splitting field of h with roots $\{\alpha_1, \ldots, \alpha_{pm}\}$. If pm is even, then $\mathrm{RS}_k(\boldsymbol{\alpha})$ is a self-dual RS code over $\mathbb{F}_{q^\ell}$, where $k = pm/2$ and $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{pm})$.

Example 4.4. Take $q = 9$ in Theorem 1.1 and let θ be a generator of $\mathbb{F}_9^*$ given by groups, algorithms and programming (GAP) [11]. Take $\boldsymbol{\alpha} = (\theta^1, \theta^2, \theta^3, \theta^4, \theta^5, \theta^6)$, $\boldsymbol{v} = (\theta, \theta, \theta, \theta, \theta, \theta)$, and $k = 4$ in Theorem 1.1, namely, we consider the GRS code $\mathrm{GRS}_4(\boldsymbol{\alpha}, \boldsymbol{v})$ of length 6 over $\mathbb{F}_9$. Using GAP directly, one has

$$\dim\left(\mathrm{GRS}_4(\boldsymbol{\alpha}, \boldsymbol{v}) \bigcap \mathrm{GRS}_4(\boldsymbol{\alpha}, \boldsymbol{v})^{\perp}\right) = 1.$$

On the other hand, Theorem 1.1 says that

$$\dim\left(\mathrm{GRS}_4(\boldsymbol{\alpha}, \boldsymbol{v}) \bigcap \mathrm{GRS}_4(\boldsymbol{\alpha}, \boldsymbol{v})^{\perp}\right) = 1.$$

5. Conclusions and future work

Let $\mathrm{GRS}_k(\boldsymbol{\alpha}, \boldsymbol{v})$ be a k-dimensional GRS code over $\mathbb{F}_q$ associated with $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\boldsymbol{v} = (v_1, \ldots, v_n)$. Let

$$h(z) = \prod_{i=1}^{n} (z - \alpha_i)$$

be a polynomial in variable z. In this paper, we determine the dimension of the Euclidean hull

$$GRS_k(\boldsymbol{\alpha}, \boldsymbol{v}) \ \cap GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})^{\perp}$$

in terms of the degree of the derivative of $h(z)$ and some relevant polynomials (see Theorem 1.1). The conclusion of our main result extends the main result of [8].

A possible direction for future work is to study the dimensions of the Hermitian hulls of GRS codes. It would also be interesting to find a new way to generate self-dual GRS codes.

Denote by $GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})$ a k-dimensional GRS code over $\mathbb{F}_q$ with parameters $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\boldsymbol{v} = (v_1, \ldots, v_n)$, and let

$$h(z) = \prod_{i=1}^{n} (z - \alpha_i)$$

represent a polynomial in z. This study focuses on determining the dimension of the intersection between the Euclidean hull

$$GRS_k(\boldsymbol{\alpha}, \boldsymbol{v}) \ \cap GRS_k(\boldsymbol{\alpha}, \boldsymbol{v})^{\perp}$$

based on the degree of the derivative of $h(z)$. The main result discussed in this paper builds upon the findings of [8].

A potential avenue for future research includes exploring the dimensions of the Hermitian hulls of GRS codes. Additionally, investigating novel methods for generating self-dual GRS codes could present an intriguing research direction.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

We sincerely thank the Associate Editor and the anonymous referees for their carefully reading and helpful suggestions that led to the improvement of the paper.

J. Huang was partially supported by the National Natural Science Foundation of China (Grant No. 12001202), the Guangdong Basic and Applied Basic Research Foundation (Grant No. 2023A1515010838) and the Guangzhou Basic and Applied Basic Research Foundation (Grant No. 2024A04J3328).

Conflict of interest

The authors declare no conflicts of interest.

References

1. G. Luo, X. Cao, X. Chen, MDS codes with hulls of arbitrary dimensions and their quantum error correction, *IEEE Trans. Inf. Theory*, **65** (2019), 2944–2952. https://doi.org/10.1109/TIT.2018.2874953
2. 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** (2020), 3527–3537. https://doi.org/10.1109/TIT.2019.2950245
3. X. Fang, M. Liu, J. Luo, On Euclidean hulls of MDS codes, *Cryptogr. Commun.*, **13** (2021), 1–14. https://doi.org/10.1007/s12095-020-00428-0
4. M. Cao, MDS codes with Galois hulls of arbitrary dimensions and the related entanglement-assisted quantum error correction, *IEEE Trans. Inf. Theory*, **67** (2021), 7964–7984. https://doi.org/10.1109/TIT.2021.3117562
5. S. Li, M. Shi, Characterization and classification of binary linear codes with various hull dimensions from an improved mass formula, *IEEE Trans. Inf. Theory*, 2023. https://doi.org/10.1109/TIT.2023.3298379
6. S. Li, M. Shi, J. Wang, An improved method for constructing formally self-dual codes with small hulls, *Designs Codes Cryptogr.*, **91** (2023), 2563–2583. https://doi.org/10.1007/s10623-023-01210-y
7. M. Shi, N. Liu, J. Kim, P. Solé, Additive complementary dual codes over $\mathbb{F}_4$, *Designs Codes Cryptogr.*, **91** (2023), 273–284. https://doi.org/10.1007/s10623-022-01106-3
8. B. Chen, S. Ling, H. Liu, Hulls of Reed-Solomon codes via algebraic geometry codes, *IEEE Trans. Inf. Theory*, **69** (2023), 1005–1014. https://doi.org/10.1109/TIT.2022.3211887

9. H. Stichtenoth, *Algebraic function fields and codes*, 2 Eds., Springer, 2009. https://doi.org/10.1007/978-3-540-76878-4

10. C. Munuera, R. Pellikaan, Equality of geometric Goppa codes and equivalence of divisors, *J. Pure Appl. Algebra*, **90** (1993), 229–252. https://doi.org/10.1016/0022-4049(93)90043-S

11. Groups, algorithms and programming (GAP), The GAP groups, algorithms and programming, Version 4.7.7. Available from: `http://www.gap-system.org,2015`.