

A representation of Galois dual codes of algebraic geometry codes via Weil differentials

Jiaqi Li¹, and Liming Ma² 

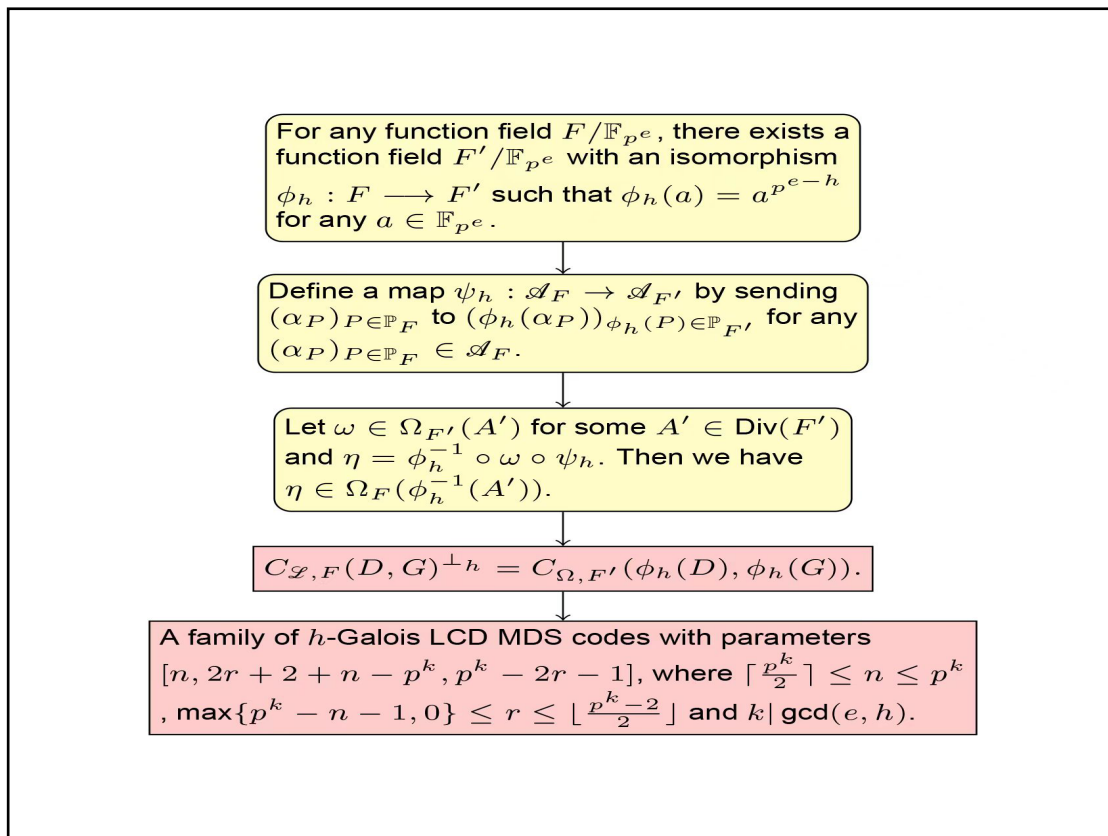
¹School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, China;

²Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, China

Correspondence: Liming Ma, E-mail: lmma20@ustc.edu.cn

© 2023 The Author(s). This is an open access article under the CC BY-NC-ND 4.0 license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

Graphical abstract



The process of representing $C_{L,F}(D, G)^{\perp_h}$ as an algebraic geometry code and constructing h -Galois LCD MDS codes.

Public summary

- For any function field $F/\mathbb{F}_{p^e}$, there exists a function field $F'/\mathbb{F}_{p^e}$ with an isomorphism $\phi_h : F \rightarrow F'$ satisfying $\phi_h(a) = a^{p^{e-h}}$ for all $a \in \mathbb{F}_{p^e}$.
- We showed that the h -Galois dual code of algebraic geometry code $C_{L,F}(D, G)$ can be represented as $C_{\Omega, F'}(\phi_h(D), \phi_h(G))$.
- As an application of the above result, we constructed a class of h -Galois LCD MDS codes.

A representation of Galois dual codes of algebraic geometry codes via Weil differentials

Jiaqi Li¹, and Liming Ma² 

¹School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, China;

²Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, China

 Correspondence: Liming Ma, E-mail: lmma20@ustc.edu.cn

© 2023 The Author(s). This is an open access article under the CC BY-NC-ND 4.0 license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).



Cite This: *JUSTC*, 2023, 53(12): 1208 (6pp)



Read Online

Abstract: Galois dual codes are a generalization of Euclidean dual codes and Hermitian dual codes. We show that the h -Galois dual code of an algebraic geometry code $C_{L,F}(D, G)$ from function field $F/\mathbb{F}_{p^r}$ can be represented as an algebraic geometry code $C_{\Omega,F'}(\phi_h(D), \phi_h(G))$ from an associated function field $F'/\mathbb{F}_{p^r}$ with an isomorphism $\phi_h: F \rightarrow F'$ satisfying $\phi_h(a) = a^{p^{r-h}}$ for all $a \in \mathbb{F}_{p^r}$. As an application of this result, we construct a family of h -Galois linear complementary dual maximum distance separable codes (h -Galois LCD MDS codes).

Keywords: algebraic geometry codes; Galois dual codes; Galois LCD codes; MDS codes

CLC number: O236.2

Document code: A

2020 Mathematics Subject Classification: 94B27; 14G50

1 Introduction

Goppa^[1] introduced a class of linear codes from algebraic curves over a finite field, which are called algebraic geometry codes. Algebraic geometry codes are a generalization of Reed–Solomon codes. A notable property of algebraic geometry codes is that there exist sequences of algebraic geometry codes exceeding the Gilbert–Varshamov bound^[2]. Algebraic geometry codes have many applications in constructing good codes, such as linear complementary dual codes^[3], self-dual near maximal distance separable codes^[4], and optimal locally repairable codes^[5–7].

Linear complementary dual codes (LCD codes) are linear codes intersecting trivially with their Euclidean dual codes. Massey^[8] first proposed LCD codes. LCD codes with large minimum distances have applications in dealing with side-channel attacks^[9] and constructing entanglement-assisted quantum error correcting codes^[10]. Therefore, linear complementary dual maximum distance separable codes (LCD MDS codes) have attracted much attention from researchers. Carlet et al.^[11] proved that there exist q -ary LCD MDS codes with parameters $[n, k, d]$ for $q > 3$, $0 \leq k \leq n \leq q + 1$, and $q = 2^m$, $n = q + 2$, $k = 3$ or $q - 1$. Many classes of LCD MDS codes were produced via generalized Reed–Solomon codes^[12–16]. Mesnager et al.^[3] provided a sufficient condition for algebraic geometry codes to be LCD codes and constructed several classes of LCD MDS codes via algebraic geometry codes.

As a generalization of the Euclidean dual codes and Hermitian dual codes, the h -Galois dual codes were first introduced by Fan and Zhang^[17]. Liu et al.^[18] introduced h -Galois

LCD codes, which are linear codes intersecting trivially with their h -Galois dual codes and hence a generalization of LCD codes. Moreover, a criterion for linear codes to be the h -Galois LCD codes was given, and two classes of h -Galois LCD MDS codes were constructed^[18]. More generally, the h -Galois hull of a linear code C is defined as the intersection of C and its h -Galois dual code. Galois hulls of MDS codes were studied and many classes of MDS codes with Galois hulls of arbitrary dimensions were constructed^[19–23]. By taking the dimensions of Galois hulls to be zero, the h -Galois LCD MDS codes can be obtained.

Let $F/\mathbb{F}_{p^r}$ be a function field with the full constant field $\mathbb{F}_{p^r}$. Let D and G be two divisors of F . The usual Euclidean dual code of the algebraic geometry code $C_{L,F}(D, G)$ is the algebraic geometry code $C_{\Omega,F}(D, G)$. By Lemma 2.3 in Ref. [18], the h -Galois dual code of $C_{L,F}(D, G)$ is the code $C_{\Omega,F}(D, G)^{p^{r-h}}$. However, the code $C_{\Omega,F}(D, G)^{p^{r-h}}$ is not in the form of algebraic geometry codes. In this article, we are interested in representing $C_{\Omega,F}(D, G)^{p^{r-h}}$ as an algebraic geometry code. In particular, we show that the Galois dual code of $C_{L,F}(D, G)$ can be represented as $C_{\Omega,F'}(\phi_h(D), \phi_h(G))$ for some function field $F'/\mathbb{F}_{p^r}$ with an isomorphism $\phi_h: F \rightarrow F'$ satisfying $\phi_h(a) = a^{p^{r-h}}$ for all $a \in \mathbb{F}_{p^r}$. As an application of this result, we provide a sufficient condition for algebraic geometry codes to be the h -Galois LCD codes and produce a class of h -Galois LCD MDS codes.

The rest of this paper is organized as follows. In Section 2, we collect some basic definitions and results on algebraic function fields over finite fields, algebraic geometry codes, and Galois inner products. In Section 3, we study the Galois

dual codes of algebraic geometry codes. In Section 4, we provide a sufficient condition on the function field F such that the Galois dual codes of algebraic geometry codes from F are algebraic geometry codes from F as well. As an application of this result, we construct a family of Galois LCD MDS codes. In Section 5, we conclude this work.

2 Preliminaries

In this section, we introduce some basic definitions and results of algebraic function fields, algebraic geometry codes and Galois inner products.

2.1 Algebraic function fields

Throughout this article, let p be a prime, e be a positive integer, $q = p^e$ be a prime power, and $\mathbb{F}_q$ be the finite field with q elements.

Let F be an algebraic function field of one variable over the full constant field $\mathbb{F}_q$, which is denoted by $F/\mathbb{F}_q$. The set of all places of $F/\mathbb{F}_q$ is denoted by $\mathbb{P}_F$. Let $\mathcal{O}_P$ be the valuation ring of a place P . The degree of P is given by $\deg(P) := [\mathcal{O}_P : \mathbb{F}_q]$. Any place of degree one is called rational.

A divisor G of $F/\mathbb{F}_q$ is a formal sum $\sum_{P \in \mathbb{P}_F} n_P P$, where almost all n_P are zero. The degree of G is defined as $\deg(G) := \sum_{P \in \mathbb{P}_F} n_P \deg(P)$. For any $x \in F \setminus \{0\}$, the principal divisor of x is defined as $(x) := \sum_{P \in \mathbb{P}_F} v_P(x) P$, where v_P is the discrete valuation of F corresponding to P . Let g be the genus of F and $\text{Div}(F)$ be the divisor group of F . For any $G \in \text{Div}(F)$, the Riemann–Roch space of G defined by

$$\mathcal{L}(G) := \{x \in F^* \mid (x) \geq -G\} \cup \{0\} \quad (1)$$

is a finite-dimensional vector space over $\mathbb{F}_q$ with dimension $\ell(G) \geq \deg(G) - g + 1$.

An adele of $F/\mathbb{F}_q$ is an element $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ in the direct product $\prod_{P \in \mathbb{P}_F} F$ such that $v_P(\alpha_P) \geq 0$ for almost all $P \in \mathbb{P}_F$. The set of all adeles is denoted by $\mathcal{A}_F$. For any divisor A , let $\mathcal{A}_F(A) = \{\alpha \in \mathcal{A}_F \mid v_P(\alpha_P) \geq -v_P(A)\}$. A Weil differential of $F/\mathbb{F}_q$ is an $\mathbb{F}_q$ -linear map $\omega : \mathcal{A}_F \rightarrow \mathbb{F}_q$ vanishing on $\mathcal{A}_F(A) + F$ for some divisor A . The set of all Weil differentials of $F/\mathbb{F}_q$ is denoted by Ω_F . For $A \in \text{Div}(F)$, let $\Omega_F(A) = \{\omega \in \Omega_F \mid \omega \text{ vanishes on } \mathcal{A}_F(A) + F\}$. For any $\omega \in \Omega_F \setminus \{0\}$, there exists a unique maximal divisor W such that $\omega \in \Omega_F(W)$ which is called the divisor of ω and denoted by (ω) . We end this subsection with the famous Riemann–Roch theorem (Theorem 1.5.15 in Ref. [24]).

Lemma 2.1. Let W be a canonical divisor of $F/\mathbb{F}_q$. Then, for each divisor $A \in \text{Div}(F)$,

$$\ell(A) = \deg(A) + 1 - g + \ell(W - A). \quad (2)$$

If $\deg(A) \geq 2g - 1$, then $\ell(A) = \deg(A) - g + 1$.

2.2 Algebraic geometry codes

A linear code C is a vector subspace of $\mathbb{F}_q^n$. The integer n is called the length of C and the dimension of the vector subspace C over $\mathbb{F}_q$ is called the dimension of the code C . For a

vector $\mathbf{a} = (a_1, \dots, a_n)$ in $\mathbb{F}_q^n$, we define its Hamming weight $\text{wt}(\mathbf{a})$ to be the size of $\{1 \leq i \leq n \mid a_i \neq 0\}$. Denote by $\mathbf{0}$ the zero vector $(0, \dots, 0)$ in $\mathbb{F}_q^n$. The minimum distance of C is defined as

$$d(C) := \min\{\text{wt}(\mathbf{a}) \mid \mathbf{a} \in C \setminus \{\mathbf{0}\}\}. \quad (3)$$

The dual code of a linear code C is defined by

$$C^\perp := \{\mathbf{c} \in \mathbb{F}_q^n \mid \langle \mathbf{a}, \mathbf{c} \rangle = 0 \text{ for any } \mathbf{a} \in C\}. \quad (4)$$

A linear code C with length n , dimension k , and minimum distance d is denoted as an $[n, k, d]$ -linear code. For an $[n, k, d]$ -linear code C , we have the Singleton bound

$$k + d \leq n + 1. \quad (5)$$

If the above equality is achieved, then code C is called a maximum distance separable code (MDS code).

Let $F/\mathbb{F}_q$ be a function field over the full constant field $\mathbb{F}_q$. Let $P_1, P_2, \dots, P_n$ be distinct rational places of F and $D = \sum_{i=1}^n P_i$. Let G be a divisor of F satisfying $\text{supp}(G) \cap \{P_1, \dots, P_n\} = \emptyset$. The algebraic geometry code associated with D and G is defined by

$$C_{\mathcal{L},F}(D, G) := \{(f(P_1), \dots, f(P_n)) \mid f \in \mathcal{L}(G)\}. \quad (6)$$

Lemma 2.2. (Theorem 2.2.2 in Ref. [24]) If $0 \leq \deg(G) < n$, then $C_{\mathcal{L},F}(D, G)$ is an $[n, k, d]$ -linear code with

$$k = \ell(G) \geq \deg(G) - g + 1 \text{ and } d \geq n - \deg(G). \quad (7)$$

There is another way of defining algebraic geometry codes via Weil differentials. For any $P \in \mathbb{P}_F$, we define a map $\iota_P : F \rightarrow \mathcal{A}_F$ as follows: for any $x \in F$, $\iota_P(x)$ is the adele whose P -component is x and all other components are 0. For any $\omega \in \Omega_F$, we define its local component at P as $\omega_P := \omega \circ \iota_P$. The algebraic geometry code associated with D and G via Weil differentials can be defined by

$$C_{\Omega,F}(D, G) := \{(\omega_{P_1}(1), \dots, \omega_{P_n}(1)) \mid \omega \in \Omega_F(G - D)\}. \quad (8)$$

Lemma 2.3. (Theorem 2.2.7 in Ref. [24]) Let $i(A) := \ell(A) - \deg(A) + g - 1$ be the index of speciality of divisor A of $F/\mathbb{F}_q$. Then $C_{\Omega,F}(D, G)$ is an $[n, k', d']$ -linear code with

$$k' = i(G - D) - i(G) \text{ and } d' \geq \deg(G) - 2g + 2. \quad (9)$$

Lemma 2.4. (Proposition 2.2.10 in Ref. [24]) Let η be a Weil differential such that $\eta_{P_i}(1) = 1, v_{P_i}(\eta) = -1$ for any $1 \leq i \leq n$. Then

$$C_{\mathcal{L},F}(D, G)^\perp = C_{\Omega,F}(D, G) = C_{\mathcal{L},F}(D, D - G + (\eta)). \quad (10)$$

2.3 Galois inner products

Let h be a positive integer with $1 \leq h \leq e$ throughout this article. The h -Galois inner product on $\mathbb{F}_q^n$ is defined as

$$\langle \mathbf{a}, \mathbf{b} \rangle_h := \sum_{i=1}^n a_i b_i^{p^h}, \quad (11)$$

where $\mathbf{a} = (a_1, \dots, a_n), \mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$. For a linear code C , its h -Galois dual code is defined to be the linear code

$$C^{\perp_h} := \{c \in \mathbb{F}_q^n \mid \langle \mathbf{a}, c \rangle_h = 0 \text{ for any } \mathbf{a} \in C\}. \quad (12)$$

If $C \cap C^{\perp_h} = \{\mathbf{0}\}$, then C is called an h -Galois linear complementary dual code (h -Galois LCD code). By Remark 4.2 in Ref. [17], we have $(C^{\perp_h})^{\perp_{p^h-h}} = C$ and $\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(C^{\perp_h}) = n$. For any $\mathbf{a} = (a_1, \dots, a_n) \in C$, let $\mathbf{a}^{p^h} = (a_1^{p^h}, \dots, a_n^{p^h})$ and $C^{p^h} = \{\mathbf{a}^{p^h} \mid \mathbf{a} \in C\}$. From Lemma 2.3 in Ref. [18], we have the following result.

Lemma 2.5. For a linear code C , we have $C^{\perp_h} = (C^{\perp})^{p^{p^h-h}}$.

3 Galois dual codes of algebraic geometry codes

In this section, we investigate the h -Galois dual codes of algebraic geometry codes. In particular, we shall show that the h -Galois dual code of an algebraic geometry code from function field $F/\mathbb{F}_q$ can be obtained as an algebraic geometry code from an associated function field $F'/\mathbb{F}_q$. The following proposition gives the existence of such a function field $F'/\mathbb{F}_q$ for any function field $F/\mathbb{F}_q$.

Proposition 3.1. Let $F/\mathbb{F}_q$ be a function field. Then, there exists an associated function field $F'/\mathbb{F}_q$ with an isomorphism ϕ_h from F onto F' such that $\phi_h(a) = a^{p^{p^h-h}}$ for any $a \in \mathbb{F}_q$.

Proof. Let $F' = F^{p^{p^h-h}}$ and $\phi_h : F \rightarrow F'$ be the map defined by $\phi_h(z) = z^{p^{p^h-h}}$ for any $z \in F$. From the theory of purely inseparable extensions (Proposition 3.10.2 in Ref. [24]), the map ϕ_h is an isomorphism from F onto F' with $\phi_h(a) = a^{p^{p^h-h}}$ for any $a \in \mathbb{F}_q$.

Remark 3.1. The associated function field $F'/\mathbb{F}_q$ satisfying the property of Proposition 3.1 may be not unique. Let F be the rational function field $\mathbb{F}_q(x)$. It is easy to see that the map $\phi_h : F \rightarrow F$ determined by $\phi_h(x) = x$ and $\phi_h(a) = a^{p^{p^h-h}}$ for any $a \in \mathbb{F}_q$ is an automorphism of F .

Proposition 3.2. Let $F/\mathbb{F}_q$ be a function field. Let $F'/\mathbb{F}_q$ be any function field such that there exists an isomorphism ϕ_h from F onto F' satisfying $\phi_h(a) = a^{p^{p^h-h}}$ for any $a \in \mathbb{F}_q$. Then the following statements hold true:

① $\phi_h(P) \in \mathbb{P}_{F'}$ and $\deg(\phi_h(P)) = \deg(P)$ for any place $P \in \mathbb{P}_F$;

② $v_{\phi_h(P)}(\phi_h(x)) = v_P(x)$ for any $x \in F$ and $P \in \mathbb{P}_F$.

Proof. ① Let $\mathcal{O}$ be the valuation ring of F corresponding to place P . Then $\phi_h(\mathcal{O})$ is a subring of F' satisfying $\mathbb{F}_q \subseteq \phi_h(\mathcal{O}) \subseteq F'$. For any $y \in F' \setminus \{0\}$, we have $\phi_h^{-1}(y) \in \mathcal{O}$ or $\phi_h^{-1}(y^{-1}) = (\phi_h^{-1}(y))^{-1} \in \mathcal{O}$, i.e., $y \in \phi_h(\mathcal{O})$ or $y^{-1} \in \phi_h(\mathcal{O})$. By definition, $\phi_h(\mathcal{O})$ is a valuation ring of $F'/\mathbb{F}_q$. Since P is the unique maximal ideal of $\mathcal{O}$, $\phi_h(P)$ is the unique maximal ideal of $\phi_h(\mathcal{O})$. Hence, $\phi_h(P)$ is a place of $F'/\mathbb{F}_q$. From the isomorphism $\mathcal{O}/P \cong \phi_h(\mathcal{O})/\phi_h(P)$, we have $\deg(\phi_h(P)) = \deg(P)$.

② Let $t \in F$ be a prime element of P . For any $x \in F \setminus \{0\}$, we have $x = t^s u$, where $s = v_P(x)$ and u is invertible in $\mathcal{O}$. Then, $\phi_h(x) = \phi_h(t)^s \phi_h(u)$. Since t is a prime element of P , we have $P = t\mathcal{O}$ and $\phi_h(P) = \phi_h(t)\phi_h(\mathcal{O})$. Thus, $\phi_h(t)$ is a prime

element of $\phi_h(P)$. Since u is invertible in $\mathcal{O}$, there exists $v \in \mathcal{O}$ such that $uv = 1$. Then, $\phi_h(u)\phi_h(v) = 1$, and $\phi_h(u)$ is invertible in $\phi_h(\mathcal{O})$. Hence, we have $v_{\phi_h(P)}(\phi_h(x)) = v_P(x) = s$.

Since $\phi_h : F \rightarrow F'$ is an isomorphism, it induces a bijection between $\mathbb{P}_F$ and $\mathbb{P}_{F'}$. This bijection induces a degree-preserving isomorphism from $\text{Div}(F)$ onto $\text{Div}(F')$, which is also denoted by ϕ_h .

Proposition 3.3. For any divisor $A \in \text{Div}(F)$, we have $\ell(\phi_h(A)) = \ell(A)$. Moreover, the function field $F'/\mathbb{F}_q$ has the same genus as $F/\mathbb{F}_q$.

Proof. Consider the following two maps:

$$\begin{aligned} f : \mathcal{L}(A) &\rightarrow \mathcal{L}(\phi_h(A)), \\ x &\mapsto \phi_h(x), \end{aligned} \quad (13)$$

and

$$\begin{aligned} g : \mathcal{L}(\phi_h(A)) &\rightarrow \mathcal{L}(A), \\ y &\mapsto \phi_h^{-1}(y). \end{aligned} \quad (14)$$

These maps are well-defined by Proposition 3.2 and we have

$$fg = id_{\mathcal{L}(\phi_h(A))} \quad \text{and} \quad gf = id_{\mathcal{L}(A)}. \quad (15)$$

Thus, $\mathcal{L}(A)$ and $\mathcal{L}(\phi_h(A))$ are isomorphic as $\mathbb{F}_p$ -vector spaces. Since they have the same cardinality, we have $\ell(\phi_h(A)) = \ell(A)$. By Lemma 2.1, the function field $F'/\mathbb{F}_q$ has the same genus as $F/\mathbb{F}_q$.

Define a map ψ_h from $\mathcal{A}_F$ to $\mathcal{A}_{F'}$:

$$\begin{aligned} \psi_h : \mathcal{A}_F &\rightarrow \mathcal{A}_{F'}, \\ (\alpha_P)_{P \in \mathbb{P}_F} &\mapsto (\phi_h(\alpha_P))_{\phi_h(P) \in \mathbb{P}_{F'}}. \end{aligned} \quad (16)$$

The map ψ_h is well defined. For any adele $(\alpha_P)_{P \in \mathbb{P}_F} \in \mathcal{A}_F$, we have $v_{\phi_h(P)}(\phi_h(\alpha_P)) = v_P(\alpha_P) \geq 0$ for almost all $P \in \mathbb{P}_F$ by Proposition 3.2. Hence, $(\phi_h(\alpha_P))_{\phi_h(P) \in \mathbb{P}_{F'}}$ is an adele of $F'/\mathbb{F}_q$.

Proposition 3.4. ① For any $\alpha, \beta \in \mathcal{A}_F$, we have $\psi_h(\alpha + \beta) = \psi_h(\alpha) + \psi_h(\beta)$.

② For any $k \in \mathbb{F}_q$ and $\alpha \in \mathcal{A}_F$, we have $\psi_h(k\alpha) = k^{p^{p^h-h}} \psi_h(\alpha)$.

③ Let $\omega \in \Omega_{F'}(A')$ for some $A' \in \text{Div}(F')$ and $\eta = \phi_h^{-1} \circ \omega \circ \psi_h$. Then we have $\eta \in \Omega_F(\phi_h^{-1}(A'))$.

Proof. ① Let $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}, \beta = (\beta_P)_{P \in \mathbb{P}_F} \in \mathcal{A}_F$. It is easy to verify that

$$\begin{aligned} \psi_h(\alpha + \beta) &= (\phi_h(\alpha_P + \beta_P))_{\phi_h(P) \in \mathbb{P}_{F'}} = \\ &= (\phi_h(\alpha_P))_{\phi_h(P) \in \mathbb{P}_{F'}} + (\phi_h(\beta_P))_{\phi_h(P) \in \mathbb{P}_{F'}} = \\ &= \psi_h(\alpha) + \psi_h(\beta). \end{aligned} \quad (17)$$

② Let $k \in \mathbb{F}_q$ and $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$. Then we have

$$\begin{aligned} \psi_h(k\alpha) &= (\phi_h(k\alpha_P))_{\phi_h(P) \in \mathbb{P}_{F'}} = \\ &= (k^{p^{p^h-h}} \phi_h(\alpha_P))_{\phi_h(P) \in \mathbb{P}_{F'}} = \\ &= k^{p^{p^h-h}} (\phi_h(\alpha_P))_{\phi_h(P) \in \mathbb{P}_{F'}} = k^{p^{p^h-h}} \psi_h(\alpha). \end{aligned} \quad (18)$$

③ It is easy to check that for any $\alpha, \beta \in \mathcal{A}_F$, $\eta(\alpha + \beta) = \eta(\alpha) + \eta(\beta)$. For any $k \in \mathbb{F}_q$ and $\alpha \in \mathcal{A}_F$, we have

$$\begin{aligned} \eta(k\alpha) &= \phi_h^{-1}(\omega(\psi_h(k\alpha))) = \phi_h^{-1}(\omega(k^{p^{p^h-h}} \psi_h(\alpha))) = \\ &= \phi_h^{-1}(k^{p^{p^h-h}} \omega(\psi_h(\alpha))) = \\ &= \phi_h^{-1}(k^{p^{p^h-h}} \phi_h^{-1}(\omega(\psi_h(\alpha)))) = k\eta(\alpha). \end{aligned} \quad (19)$$

Let $\alpha \in \mathcal{A}_F(\phi_h^{-1}(A'))$. For any $P \in \mathbb{P}_F$, we have

$$\begin{aligned} v_{\phi_h(P)}(\psi_h(\alpha)) &= v_{\phi_h(P)}(\phi_h(\alpha_P)) = v_P(\alpha_P) \geq \\ &= -v_P(\phi_h^{-1}(A')) = -v_{\phi_h(P)}(A'). \end{aligned} \quad (20)$$

Thus, $\psi_h(\alpha) \in \mathcal{A}_{F'}(A')$. Since ω vanishes on $\mathcal{A}_{F'}(A')$, we obtain $\eta \in \Omega_{F'}(\phi_h^{-1}(A'))$.

Theorem 3.1. Let $F/\mathbb{F}_q$ be a function field and $F'/\mathbb{F}_q$ be an associated function field with an isomorphism $\phi_h: F \rightarrow F'$ satisfying $\phi_h(a) = a^{p^{e-h}}$ for any $a \in \mathbb{F}_q$. Let $D = P_1 + \dots + P_n$, where $P_1, \dots, P_n$ are distinct rational places of F . Let G be a divisor of F such that $\text{supp}(G) \cap \text{supp}(D) = \emptyset$. Then the h -Galois dual code of $C_{\mathcal{L},F}(D, G)$ can be given by

$$C_{\mathcal{L},F}(D, G)^{\perp_h} = C_{\Omega, F'}(\phi_h(D), \phi_h(G)). \quad (21)$$

Proof. From Lemma 2.4 and Lemma 2.5, we have $C_{\mathcal{L},F}(D, G)^{\perp_h} = (C_{\mathcal{L},F}(D, G)^{\perp})^{p^{e-h}} = C_{\Omega, F}(D, G)^{p^{e-h}}$. Thus, it suffices to show that $C_{\Omega, F'}(\phi_h(D), \phi_h(G)) = C_{\Omega, F}(D, G)^{p^{e-h}}$. Let $\omega \in \Omega_{F'}(\phi_h(G - D))$ and $\eta = \phi_h^{-1} \circ \omega \circ \psi_h$. From Proposition 3.4, we have $\eta \in \Omega_F(G - D)$ and

$$\begin{aligned} (\omega_{\phi_h(P_i)}(1))^{p^h} &= \phi_h^{-1}(\omega(\iota_{\phi_h(P_i)}(1))) = \\ &= \phi_h^{-1}(\omega(\psi_h(\iota_{P_i}(1)))) = \eta(\iota_{P_i}(1)) = \eta_{P_i}(1) \end{aligned} \quad (22)$$

for $1 \leq i \leq n$, i.e., $(\omega_{\phi_h(P_1)}(1), \dots, \omega_{\phi_h(P_n)}(1)) = (\eta_{P_1}(1)^{p^{e-h}}, \dots, \eta_{P_n}(1)^{p^{e-h}})$. Hence, we have

$$C_{\Omega, F'}(\phi_h(D), \phi_h(G)) \subseteq C_{\Omega, F}(D, G)^{p^{e-h}}. \quad (23)$$

It remains to be shown that $\dim_{\mathbb{F}_q} C_{\Omega, F'}(\phi_h(D), \phi_h(G)) = i(G - D) - i(G)$. By Proposition 3.3, we have

$$\begin{aligned} i(\phi_h(G)) &= \ell(\phi_h(G)) - \deg(\phi_h(G)) + g - 1 = \\ &= \ell(G) - \deg(G) + g - 1 = i(G). \end{aligned} \quad (24)$$

Similarly, we have $i(\phi_h(G - D)) = i(G - D)$. Hence, $\dim_{\mathbb{F}_q} C_{\Omega, F'}(\phi_h(D), \phi_h(G)) = i(\phi_h(G - D)) - i(\phi_h(G)) = i(G - D) - i(G) = \dim_{\mathbb{F}_q} C_{\Omega, F}(D, G)$ from Lemma 2.3, i.e., $C_{\Omega, F'}(\phi_h(D), \phi_h(G)) = C_{\Omega, F}(D, G)^{p^{e-h}} = C_{\mathcal{L},F}(D, G)^{\perp_h}$.

4 Construction of a class of h -Galois LCD MDS codes

The code $C_{\mathcal{L},F}(D, G)$ and its h -Galois dual code $C_{\Omega, F'}(\phi_h(D), \phi_h(G))$ are algebraic geometry codes from function fields $F/\mathbb{F}_q$ and $F'/\mathbb{F}_q$, respectively. If the function field $F/\mathbb{F}_q$ admits an automorphism ϕ_h such that $\phi_h(a) = a^{p^{e-h}}$ for any $a \in \mathbb{F}_q$, then we have

$$C_{\mathcal{L},F}(D, G)^{\perp_h} = C_{\Omega, F'}(\phi_h(D), \phi_h(G)). \quad (25)$$

Both $C_{\mathcal{L},F}(D, G)$ and $C_{\Omega, F'}(\phi_h(D), \phi_h(G))$ are algebraic geometry codes from the same function field. In this section, we provide a sufficient condition on $F/\mathbb{F}_q$ such that F admits an automorphism ϕ_h satisfying $\phi_h(a) = a^{p^{e-h}}$ for any $a \in \mathbb{F}_q$. First, we need the following lemma from Theorem 5.2.8 in Ref. [25].

Lemma 4.1. Let k be a field, E be an algebraic extension of k , and $\sigma: k \rightarrow k^{ac}$ be an embedding of k into its algebraic closure k^{ac} . Then, there exists an extension of σ to an embedding of E into k^{ac} .

Proposition 4.1. Let $F/\mathbb{F}_q$ be a function field. If F is a finite and normal extension of $\mathbb{F}_{p^k}(z)$ for some $z \in F$ and $k | \gcd(e, h)$, then there exists an automorphism ϕ_h of F such that $\phi_h(a) = a^{p^{e-h}}$ for any $a \in \mathbb{F}_q$.

Proof. Let σ be the automorphism of $\mathbb{F}_q$ given by $\sigma(a) = a^{p^{e-h}}$ for any $a \in \mathbb{F}_q$. The automorphism σ induces an automorphism of $\mathbb{F}_q[z]$, which sends a polynomial $f(z) = \sum_{i=0}^n a_i z^i$ to $f^\sigma(z) = \sum_{i=0}^n \sigma(a_i) z^i$. This map induces an automorphism $\tilde{\sigma}$ of $\mathbb{F}_q(z)$ which sends $\frac{f(z)}{g(z)}$ to $\frac{f^\sigma(z)}{g^\sigma(z)}$, where $f(z), g(z) \in \mathbb{F}_q[z]$ and $g(z) \neq 0$. Regard the automorphism $\tilde{\sigma}$ as an embedding from $\mathbb{F}_q(z)$ into $\mathbb{F}_q(z)^{ac}$. The field extension $F/\mathbb{F}_q(z)$ is finite, hence there exists an embedding τ from F into $\mathbb{F}_q(z)^{ac}$ extending $\tilde{\sigma}$ by Lemma 4.1. Note that τ induces an identity on $\mathbb{F}_{p^k}(z)$ and $\mathbb{F}_q(z)^{ac} = \mathbb{F}_{p^k}(z)^{ac}$. Since $F/\mathbb{F}_{p^k}(z)$ is finite and normal, the embedding τ has image F . Therefore, τ is an automorphism of F that extends σ .

For any $G_1, G_2 \in \text{Div}(F)$, let

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

be the intersection of G_1, G_2 and

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

be the union of G_1, G_2 .

Theorem 4.1. Let $F/\mathbb{F}_q$ be a function field with an automorphism ϕ_h satisfying $\phi_h(a) = a^{p^{e-h}}$ for any $a \in \mathbb{F}_q$. Let

$D = \sum_{i=1}^n P_i$, where P_i are pairwise distinct ϕ_h -invariant rational places, i.e., $\phi_h(P_i) = P_i$ for $1 \leq i \leq n$. Let G be a divisor of $F/\mathbb{F}_q$ such that $\text{supp}(G) \cap \text{supp}(D) = \emptyset$ and $\phi_h(G) - G$ is principal. If there exists a Weil differential ω of F such that

- ① $\omega_{P_i}(1) = 1, v_{P_i}(\omega) = -1$ for any $1 \leq i \leq n$ and
- ② $G \wedge H$ is a nonspecial divisor of degree $g - 1$, where $H = D - \phi_h(G) + (\omega)$,

then $C_{\mathcal{L},F}(D, G)$ is an h -Galois LCD code.

Proof. By Theorem 3.1 and Lemma 2.4, we have

$$\begin{aligned} C_{\mathcal{L},F}(D, G)^{\perp_h} &= C_{\Omega, F'}(\phi_h(D), \phi_h(G)) = \\ &= C_{\mathcal{L},F}(D, D - \phi_h(G) + (\omega)) = C_{\mathcal{L},F}(D, H). \end{aligned}$$

It remains to be shown that $C_{\mathcal{L},F}(D, G) \cap C_{\mathcal{L},F}(D, H) = \{0\}$. Let $f \in \mathcal{L}(G)$ and $g \in \mathcal{L}(H)$ with $f(P_i) = g(P_i)$ for all $1 \leq i \leq n$. Denote by $h = f - g$. It is easy to see that $h \in \mathcal{L}(G \vee H - D)$. Note that $G \vee H + G \wedge H = G + H = D + G - \phi_h(G) + (\omega)$. From Lemma 2.1, the dimension of $\mathcal{L}(G \vee H - D)$ is

$$\begin{aligned} \ell(G \vee H - D) &= \ell((\omega) - G \wedge H + G - \phi_h(G)) = \\ &= \ell((\omega) - G \wedge H) = \\ &= \ell(G \wedge H) - \deg(G \wedge H) + g - 1 = 0. \end{aligned} \quad (26)$$

Therefore, we must have $h = 0$, i.e., $f = g \in \mathcal{L}(G \wedge H)$. Since $G \wedge H$ is nonspecial of degree $g - 1$, we have $\mathcal{L}(G \wedge H) = \{0\}$. It follows that $f = g = 0$, i.e., $C_{\mathcal{L},F}(D, G) \cap C_{\mathcal{L},F}(D, H) = \{0\}$.

Theorem 4.1 is a generalization of Theorem 4 in Ref. [3]. In the case of rational function fields, we have the following

result.

Corollary 4.1. Let $F = \mathbb{F}_q(x)$ be the rational function field over $\mathbb{F}_q$ and let ϕ_h be the automorphism of $\mathbb{F}_q(x)$ that fixes x and sends a to $a^{p^{e-h}}$ for any $a \in \mathbb{F}_q$. Let $D = \sum_{i=1}^n P_i$, where P_i

are distinct ϕ_h -invariant rational places of F . Let G be a divisor of F with $\text{supp}(G) \cap \text{supp}(D) = \emptyset$ and $0 \leq \deg(G) < n$. If there is a Weil differential ω of F such that

① $\omega_{P_i}(1) = 1, v_{P_i}(\omega) = -1$ for any $1 \leq i \leq n$ and

② $G \wedge H$ has degree -1 , where $H = D - \phi_h(G) + (\omega)$,

then $C_{L,F}(D, G)$ is an h -Galois LCD MDS code with parameters $[n, \deg(G) + 1, n - \deg(G)]$.

Proof. Since the genus of the rational function field is $g = 0$ and $\deg(G \wedge H) = -1 \geq 2g - 1$, we have

$$\ell(G \wedge H) = \deg(G \wedge H) - g + 1 = 0. \quad (27)$$

from Lemma 2.1, i.e., $G \wedge H$ is nonspecial. Since any divisor of F of degree 0 is principal from Riemann–Roch theorem, $\phi_h(G) - G$ is principal. From Theorem 4.1, the code $C_L(D, G)$ is an h -Galois LCD code. By Lemma 2.2, $C_L(D, G)$ is an $[n, \deg(G) + 1, n - \deg(G)]$ MDS code.

Theorem 4.2. Let $k | \gcd(h, e)$. For any $\lceil \frac{p^k}{2} \rceil \leq n \leq p^k$ and $\max\{p^k - n - 1, 0\} \leq r \leq \lfloor \frac{p^k - 2}{2} \rfloor$, there exists an h -Galois LCD MDS code with parameters $[n, 2r + 2 + n - p^k, p^k - 2r - 1]$.

Proof. Let F be the rational function field $\mathbb{F}_q(x)$ over $\mathbb{F}_q$. Let ϕ_h be the automorphism of F that fixes x and sends a to $a^{p^{e-h}}$ for any $a \in \mathbb{F}_q$. Let P_a be the zero of $x - a$ and P_∞ be the pole of x . It follows that $\phi_h(P_\infty) = P_\infty$ and $\phi_h(P_a) = P_{\phi_h(a)}$. Since $\phi_h(a) = a^{p^{e-h}} = a$ for any $a \in \mathbb{F}_{p^k}$, we have $\phi_h(P_a) = P_a$ for any $a \in \mathbb{F}_{p^k}$.

Let S be a subset of $\mathbb{F}_{p^k}$ of cardinality n and $T = \mathbb{F}_{p^k} \setminus S$. Let $D = \sum_{a \in S} P_a$ and $G = rP_\infty + \sum_{a \in T} m_a P_a$, where $\sum_{a \in T} m_a = r + 1 - |T|$ and $m_a \geq 0$ for any $a \in T$. Let $\omega = \frac{1}{x - x^{p^k}} dx$. Since the divisor of dx is $-2P_\infty$, we obtain

$$(\omega) = (p^k - 2)P_\infty - \sum_{a \in \mathbb{F}_{p^k}} P_a, \quad (28)$$

$$H = D - \phi_h(G) + (\omega) = (p^k - 2 - r)P_\infty - \sum_{a \in T} (m_a + 1)P_a, \quad (29)$$

$$G \wedge H = rP_\infty - \sum_{a \in T} (m_a + 1)P_a, \quad (30)$$

and $\omega_{P_a}(1) = 1$ for any $a \in \mathbb{F}_{p^k}$. Since the degree of G is $\deg(G) = 2r + 1 - |T|$, the algebraic geometry code $C_{L,F}(D, G)$ is an h -Galois LCD MDS code with parameters $[n, 2r + 2 + n - p^k, p^k - 2r - 1]$ from Corollary 4.1.

Remark 4.1. The parameters in Theorem 4.2 can also be obtained from Theorem 2.13 in Ref. [18] and Theorem 1 in Ref. [11] via generator matrices of MDS codes and generalized Reed–Solomon codes. To see this, let $k | \gcd(h, e)$ and $n \leq p^k$. If $p^k \leq 3$, then $n \leq 3$ and it is easy to construct q -ary h -Galois LCD MDS codes with parameters $[n, l, n - l + 1]$ for any $1 \leq l \leq n$.

If $p^k \geq 4$, set $s = \gcd(p^{e-h} + 1, p^e - 1)$ and $t = \frac{p^e - 1}{s}$. Then, we have

$$t \geq \frac{p^e - 1}{p^{e-h} + 1} \geq \frac{p^e - 1}{p^{e-k} + 1} = p^k - \frac{p^k + 1}{p^{e-k} + 1}. \quad (31)$$

Case 1: $k = e$. In this case, h -Galois LCD codes are Euclidean LCD codes. Since $p^k \geq 4$, we have $q \geq 4$. By Theorem 1 in Ref. [11], there exist q -ary Euclidean LCD MDS $[n, l, n - l + 1]$ codes for any $1 \leq l \leq n$.

Case 2: $k < e, t \geq n$. In this case, $\min\{t, n\} - 1 = n - 1$. By Theorem 2.13 in Ref. [18], there exist h -Galois LCD MDS $[n, l, n - l + 1]$ codes for any $1 \leq l \leq n$.

Case 3: $k < e, t < n$. Since $k < e$, we have $t \geq p^k - \frac{p^k + 1}{p^{e-k} + 1} \geq p^k - 1$. Since $t < n$, we have $e = 2h = 2k$, $n = p^k$ and $t = p^k - 1$. Since $p^k \geq 4$, we have $\frac{p^k}{2} \leq \min\{t, n\} - 1 = p^k - 2$. By Theorem 2.13 in Ref. [18], there exist h -Galois LCD MDS $[p^k, l, p^k - l + 1]$ codes for $1 \leq l \leq p^k$.

5 Conclusions

In this work, we showed that the Galois dual code of $C_{L,F}(D, G)$ can be represented as $C_{Q,F'}(\phi_h(D), \phi_h(G))$ for some function field $F'/\mathbb{F}_q$ with an isomorphism $\phi_h : F \rightarrow F'$ satisfying $\phi_h(a) = a^{p^{e-h}}$ for all $a \in \mathbb{F}_q$. Then we provided a sufficient condition on the function field F such that Galois dual codes of algebraic geometry codes from F are algebraic geometry codes from F as well. Finally, we constructed a class of h -Galois LCD MDS codes. We extend the application of algebraic geometry codes in coding theory by showing that Galois LCD codes can be constructed from algebraic geometry codes. For the future research, we may consider constructing Galois LCD codes with good parameters via algebraic curves with genus larger than 0, such as elliptic curves, hyperelliptic curves, and Hermitian curve.

Acknowledgements

This work was supported by the National Key Research and Development Program of China (2022YFA1004900), the USTC Research Funds of the Double First-Class Initiative (YD0010002004), and the Fundamental Research Funds for the Central Universities (WK3470000020, WK0010000068).

Conflict of interest

The authors declare that they have no conflicts of interest.

Biographies

Jiaqi Li is currently a postgraduate student under the supervision of Prof. Xiaowu Chen at the University of Science and Technology of China. His research mainly focuses on coding theory.

Liming Ma is a Research Associate Professor with the School of Mathematical Sciences, University of Science and Technology of China. He received his Ph.D. degree in Mathematics from Nanyang Technological University, Singapore, in 2014. From April 2014 to May 2020, he was a Lecturer with the School of Mathematical Sciences, Yangzhou University, China. His research mainly focuses on algebraic function

fields over finite fields and coding theory.

References

- [1] Goppa V D. Codes on algebraic curves. *Soviet Mathematics Doklady*, **1981**, 24 (1): 170–172.
- [2] Tsfasman M A, Vlăduț S G, Zink T. Modular curves, Shimura curves, and Goppa codes, better than the Varshamov–Gilbert bound. *Mathematische Nachrichten*, **1982**, 109: 21–28.
- [3] Mesnager S, Tang C, Qi Y. Complementary dual algebraic geometry codes. *IEEE Transactions on Information Theory*, **2018**, 64 (4): 2390–2397.
- [4] Jin L, Kan H. Self-dual near MDS codes from elliptic curves. *IEEE Transactions on Information Theory*, **2019**, 65 (4): 2166–2170.
- [5] Barg A, Tamo I, Vlăduț S. Locally recoverable codes on algebraic curves. *IEEE Transactions on Information Theory*, **2017**, 63 (8): 4928–4939.
- [6] Li X, Ma L, Xing C. Optimal locally repairable codes via elliptic curves. *IEEE Transactions on Information Theory*, **2019**, 65 (1): 108–117.
- [7] Ma L, Xing C. The group structures of automorphism groups of elliptic curves over finite fields and their applications to optimal locally repairable codes. *Journal of Combinatorial Theory, Series A*, **2023**, 193: 105686.
- [8] Massey J L. Linear codes with complementary duals. *Discrete Mathematics*, **1992**, 106–107: 337–342.
- [9] Carlet C, Guilley S. Complementary dual codes for countermeasures to side-channel attacks. In: *Coding Theory and Applications*. Cham, Switzerland: Springer, **2015**.
- [10] Guenda K, Jitman S, Gulliver T A. Constructions of good entanglement-assisted quantum error correcting codes. *Designs, Codes and Cryptography*, **2018**, 86: 121–136.
- [11] Carlet C, Mesnager S, Tang C, et al. Euclidean and Hermitian LCD MDS codes. *Designs, Codes and Cryptography*, **2018**, 86: 2605–2618.
- [12] Chen B, Liu H. New constructions of MDS codes with complementary duals. *IEEE Transactions on Information Theory*, **2018**, 64 (8): 5776–5782.
- [13] Jin L. Construction of MDS codes with complementary duals. *IEEE Transactions on Information Theory*, **2017**, 63 (5): 2843–2847.
- [14] Beelen P, Jin L. Explicit MDS codes with complementary duals. *IEEE Transactions on Information Theory*, **2018**, 64 (11): 7188–7193.
- [15] Liu H, Liu S. Construction of MDS twisted Reed–Solomon codes and LCD MDS codes. *Designs, Codes and Cryptography*, **2021**, 89: 2051–2065.
- [16] Shi X, Yue Q, Yang S. New LCD MDS codes constructed from generalized Reed–Solomon codes. *Journal of Algebra and Its Applications*, **2018**, 18 (8): 1950150.
- [17] Fan Y, Zhang L. Galois self-dual constacyclic codes. *Designs, Codes and Cryptography*, **2017**, 84: 473–492.
- [18] Liu X, Fan Y, Liu H. Galois LCD codes over finite fields. *Finite Fields and Their Applications*, **2018**, 49: 227–242.
- [19] Cao M. MDS Codes with Galois hulls of arbitrary dimensions and the related entanglement-assisted quantum error correction. *IEEE Transactions on Information Theory*, **2021**, 67 (12): 7964–7984.
- [20] Cao M, Yang J. Intersections of linear codes and related MDS codes with new Galois hulls. arXiv: 2210.05551, **2022**.
- [21] Fang X, Jin R, Luo J, et al. New Galois hulls of GRS codes and application to EAQECCs. *Cryptography and Communications*, **2022**, 14: 145–159.
- [22] Li Y, Zhu S, Li P. On MDS codes with Galois hulls of arbitrary dimensions. *Cryptography and Communications*, **2023**, 15: 565–587.
- [23] Wu Y, Li C, Yang S. New Galois hulls of generalized Reed–Solomon codes. *Finite Fields and Their Applications*, **2022**, 83: 102084.
- [24] Stichtenoth H. *Algebraic Function Fields and Codes*. Berlin: Springer-Verlag, **2009**.
- [25] Lang S. *Algebra*. New York: Springer-Verlag, **2002**.