

Duality and decoding of linearized Algebraic Geometry codes

Elena Berardini¹, Xavier Caruso², and Fabrice Drain³

¹*CNRS, Mathematical Institute of Bordeaux, University of Bordeaux, France**

²*CNRS, Mathematical Institute of Bordeaux, University of Bordeaux, France[†]*

³*Mathematical Institute of Bordeaux, University of Bordeaux, France[‡]*

March 2026

Abstract

We design a polynomial time decoding algorithm for linearized Algebraic Geometry codes with unramified evaluation places, a family of sum-rank metric evaluation codes on division algebras over function fields introduced in [BC24]. By establishing a Serre duality and a Riemann–Roch theorem for these algebras, we prove that the dual codes of such linearized Algebraic Geometry codes, that we term linearized Differential codes, coincide with the linearized Algebraic Geometry codes themselves over the adjoint algebra, and that our decoding algorithm is correct.

Contents

1	Riemann–Roch theorem on division algebras	3
1.1	The case of numerical divisors	4
1.2	Riemann theorem for extended divisors	7
1.3	Differentials and residues	10
1.4	Serre duality and Riemann–Roch Theorem	12
2	Application to linearized Algebraic Geometry codes	14
2.1	Duality	15
2.2	Decoding	16
A	SageMath implementation of the decoding algorithm	20

*elena.berardini@math.u-bordeaux.fr

†xavier.caruso@math.u-bordeaux.fr

‡fabrice.drain@math.u-bordeaux.fr

2020 *Mathematics Subject Classification*. Primary: 11R52,94B35; Secondary: 14A22,14R56

Keywords: algebraic curve, sum-rank metric, decoding, division algebra

Introduction

Sum-rank metric codes have seen a resurgence of interest in recent decades due to their broad applications in areas like network coding, distributed data storage, and code-based cryptography as described in [MPSK22]. Recent code constructions, such as the linearized Reed–Solomon codes introduced in [MP18b], achieve the sum-rank Singleton-type bound. Furthermore, linearized Algebraic Geometry (LAG) codes were introduced and studied by the first and second authors in [BC24], using Riemann–Roch spaces on some division algebras over function fields of curves. They generalize both Algebraic Geometry (AG) codes as described in [Sti93] and linearized Reed–Solomon codes. This lends them good properties in the sum-rank metric: they almost meet the sum-rank Singleton bound and their length is not limited by the size of the alphabet. We also mention that other algebraic constructions exist, such as linearized Reed–Muller codes, described in [BC25].

The main contributions of this paper are to study the duality properties of linearized AG codes and to design a decoding algorithm for them, under the hypothesis that the evaluation places used in their definition are unramified.

We briefly outline the construction of linearized AG codes (a more detailed presentation is given at the beginning of Section 2 of the present paper). Let $\mathbb{K}$ be a the function field of an algebraic curve defined over a field $\mathbb{F}$. We fix a cyclic extension $\mathbb{L}/\mathbb{K}$ of degree r and a generator θ of its Galois group. We let $\mathbb{L}[T; \theta]$ be the corresponding Ore polynomial ring. We set

$$\mathbb{D} := \frac{\mathbb{L}[T; \theta]}{T^r - x},$$

where $x \in \mathbb{K}$ is chosen so that $\mathbb{D}$ is a division algebra as in [BC24, Section IV A].

In [BC24], valuations on $\mathbb{D}$ (indexed by the places of $\mathbb{L}$) are introduced and used to define Riemann–Roch spaces $\Lambda_{\mathbb{D}}(A) \subset \mathbb{D}$ associated to certain rational divisors A of $\mathbb{L}$. Moreover, for any rational place P of $\mathbb{K}$ away from A (meaning that the support of A does not contain any place of $\mathbb{L}$ above P) and satisfying a certain hypothesis called **(H2- P_i)** in [BC24], an evaluation morphism $\bar{\varepsilon}_P : \Lambda_{\mathbb{D}}(A) \rightarrow \text{End}_{\mathbb{F}}(V_P)$ is constructed, where V_P is the residual algebra of $\mathbb{L}$ at P . Fixing a finite set $\{P_1, \dots, P_s\}$ of such places and writing $D = P_1 + \dots + P_s$, one can concatenate the $\bar{\varepsilon}_i$ to obtain a multievaluation morphism

$$\bar{\varepsilon}_D : \Lambda_{\mathbb{D}}(A) \rightarrow \prod_{i=1}^s \text{End}_{\mathbb{F}}(V_{P_i}) \simeq (\mathbb{F}^{r \times r})^s,$$

whose image is by definition the linearized AG code $\text{LAG}_{\mathbb{D}}(A, D)$. It is endowed with the sum-rank metric defined by the weight function $(M_1, \dots, M_s) \mapsto \sum_{i=1}^s \text{rank}(M_i)$.

Theorem 2 of [BC24] provides estimates on the parameters of the code $\text{LAG}_{\mathbb{D}}(A, D)$: assuming $\deg(A) < sr$, its minimum distance is at least $d^*(A) := sr - \deg A$, while its dimension is that of the Riemann–Roch space $\Lambda_{\mathbb{D}}(A)$, which is itself lower bounded by $r \deg(A) - r(g - 1)$, where g is given by an explicit formula (see Definition 1.1.7) and is called the *genus* of $\mathbb{D}$.

In this paper, we propose a decoding algorithm for linearized AG codes (see Algorithm 1) and prove the following theorem.

Theorem 1 (Theorem 2.2.13). *Let A be a divisor as above, and satisfying $2g - 2 < \deg A < sr$. We assume the existence of a non-split non-evaluation rational place of $\mathbb{K}$ (see Hypothesis 2.2.7). Set*

$$\rho_{\text{algo}} := \left\lfloor \frac{d^*(A) - g - 1}{2} \right\rfloor.$$

Then, our algorithm decodes any error relative to the code $\text{LAG}_{\mathbb{D}}(A, D)$ of sum-rank weight at most ρ_{algo} , with polynomial complexity in s and r .

Our decoding algorithm is the analogue in the sum-rank metric to the classical decoding algorithm for AG codes in the Hamming metric described in [Sti93, Section 8.5]. We express the received word m as the sum $m = c + e$ of the original codeword $c \in \text{LAG}_{\mathbb{D}}(A, D)$ and an error e of sum-rank weight at most ρ_{algo} . We first determine a space U localizing the error e with sufficient precision, *i.e.*, satisfying $\text{im}(e) \subset U$ and $\dim(U) < d^*(A)$. Then, we solve the syndrome equations for e restricted to the localizing space.

The fundamental theorem underlying our decoding algorithm is a Riemann–Roch Theorem on $\mathbb{D}$ for what we call *extended divisors*. Those are pairs composed of a divisor A away from D and a product of vector subspaces $W := \bigoplus_{i=1}^s W_i$, where $W_i \subset V_{P_i}$. To an extended divisor (A, W) , we associate its degree $\deg(A, W) = \deg A - \dim_{\mathbb{F}} W$ and the Riemann–Roch space

$$\Lambda_{\mathbb{D}}(A, W) := \{f \in \Lambda_{\mathbb{D}}(A) \mid \bar{\varepsilon}_i(f)|_{W_i} = 0 \quad \forall i \in \{1, \dots, s\}\}.$$

We denote its dimension by $\lambda_{\mathbb{D}}(A, W)$. Besides, we define a canonical divisor K related to $\mathbb{D}$, whose degree is $2g - 2$. Letting $\mathbb{D}^* = \frac{L[T; \theta]}{T^r - x^{-1}}$, our Riemann–Roch Theorem reads as follows.

Theorem 2 (Theorem 1.4.4). *Let (A, W) be an extended divisor. We have*

$$\lambda_{\mathbb{D}}(A, W) = r \deg(A, W) + r(1 - g) + \lambda_{\mathbb{D}^*}(K + \text{CoNr}(D) - A, W^{\perp})$$

where $\text{CoNr}(D) = \sum_{i=1}^s \sum_{Q|P_i} Q$ and $W^{\perp}$ is the orthogonal of W with respect to the trace bilinear form (see Subsection 1.3.3).

Moreover, if $\deg(A, W) < 0$, then we have $\lambda_{\mathbb{D}}(A, W) = 0$.

We show this theorem by extending the proof of the classical Riemann–Roch Theorem as presented in [Sti93, Chapter 1] and in [Sha13, Chapter 7]. As an important ingredient of the proof, we define adele spaces associated to $\mathbb{D}$ and differential spaces associated to $\mathbb{D}^*$, and we show a Serre-type duality theorem, establishing a perfect pairing between them. As in the classical case, this theorem brings along a canonical duality between linearized AG codes and some linearized Differential codes defined by means of residues (see Definition 2.1.1).

Theorem 3 (Theorem 2.1.2). *For any divisor A away from D and a particular choice of K , we have the following equalities of codes:*

$$\text{LAG}_{\mathbb{D}}(A, D)^{\perp} = \text{LD}_{\mathbb{D}^*}(A, D) = \text{LAG}_{\mathbb{D}^*}(K + \text{CoNr}(D) - A, D).$$

We note that a similar theorem was proved in [CD23] for linearized Reed–Solomon codes, which correspond to the case where $\mathbb{K} = \mathbb{F}_q(t)$, $\mathbb{L} = \mathbb{F}_{q^r}(t)$ and A is a scalar multiple of the point at infinity. On the other hand, in this situation, the result of [CD23] encompasses a more general setting, as it includes Ore polynomials with derivations, and restrictions of the morphisms $\bar{\varepsilon}_D$ to subspaces.

Organisation of the paper. The paper is structured as follows. In Section 1, we establish our Riemann–Roch Theorem. In Section 2, we move to applications to coding theory, establishing first the duality theory for linearized AG codes, and then designing their decoding algorithm. Besides, in Appendix A, we provide some results from a SageMath implementation of our algorithm.

1 Riemann–Roch theorem on division algebras

We consider the setting of [BC24]. Let $\mathbb{F}$ be an arbitrary field. Let $\mathbb{K}$ be an algebraic function field in one variable over its constant field $\mathbb{F}$. Let $\mathbb{L}/\mathbb{K}$ be a cyclic extension of degree $r \geq 1$. We denote by θ a generator of its cyclic Galois group.

We denote by $\mathcal{P}_{\mathbb{K}}$ and $\mathcal{P}_{\mathbb{L}}$ the sets of places of $\mathbb{K}$ and $\mathbb{L}$, respectively. For a place $P \in \mathcal{P}_{\mathbb{K}}$ (resp. $Q \in \mathcal{P}_{\mathbb{L}}$), we write $\mathbb{K}_P$ (resp. $\mathbb{L}_Q$) for the completion of $\mathbb{K}$ (resp. $\mathbb{L}$) at that place. We also use $\mathbb{L}_P$ (resp. $\mathbb{D}_P$) to denote the completion of $\mathbb{L}$ (resp. $\mathbb{D}$) at a place $P \in \mathcal{P}_{\mathbb{K}}$. We denote by v_P (resp. w_Q) the normalized valuation of $\mathbb{K}$ (resp. of $\mathbb{L}$) at a place P (resp. Q). We use the notation $Q|P$ to indicate that Q is a place of $\mathbb{L}$ above a place P of $\mathbb{K}$. Writing e_P the ramification index of $Q|P$, we have $w_Q = e_P v_P$. We also use the notation $\mathcal{O}_P$ (resp. $\mathcal{O}_Q$) for the valuation ring of $\mathbb{K}_P$ (resp. $\mathbb{L}_Q$) and set

$$\mathcal{O}_{\mathbb{L},P} := \prod_{Q|P} \mathcal{O}_Q \subset \mathbb{L}_P.$$

We consider the Ore polynomial ring $\mathbb{L}[T; \theta]$, defined in [Ore33] as polynomials equipped with a twisted multiplication given by the rule $Ta = \theta(a)T$ for any $a \in \mathbb{L}$. We note that the ring $\mathbb{L}[T; \theta]$ is left and right Euclidean as shown in [Ore33, Section 2]. Let $x \in \mathbb{K}$. We define as in [BC24] a cyclic algebra $\mathbb{D}$ by

$$\mathbb{D} := \frac{\mathbb{L}[T; \theta]}{T^r - x}.$$

Throughout the paper, we assume that x is chosen in such a way that $\mathbb{D}$ is a division algebra (see Hypothesis **(H1)** in [BC24, Section IV]). For $P \in \mathcal{P}_{\mathbb{K}}$, we set $\mathbb{D}_P = \mathbb{K}_P \otimes_{\mathbb{K}} \mathbb{D}$.

In the sequel, we will tacitly use the obvious isomorphisms

$$\begin{array}{ccc} \mathbb{D} & \xrightarrow{\sim} & \mathbb{L}^r \\ \sum_{i=0}^{r-1} \alpha_i T^i & \mapsto & (\alpha_i)_{i=0}^{r-1} \end{array} \quad \text{and} \quad \begin{array}{ccc} \mathbb{L} \otimes_{\mathbb{K}} \mathbb{K}_P & \xrightarrow{\sim} & \prod_{Q|P} \mathbb{L}_Q \\ y & \mapsto & (y_Q)_{Q|P} \end{array}.$$

We will denote by $y_i \in \mathbb{L}$ (resp. $y_i \in \prod_{P \in \mathcal{P}_{\mathbb{K}}} \mathbb{L} \otimes_{\mathbb{K}} \mathbb{K}_P$) the i -th component of $y \in \mathbb{D}$ (resp. $y \in \prod_{P \in \mathcal{P}_{\mathbb{K}}} \mathbb{D} \otimes_{\mathbb{K}} \mathbb{K}_P$), induced by the first isomorphism, and by $y_Q \in \mathbb{L}_Q$ the Q -th component of $y \in \mathbb{L} \otimes_{\mathbb{K}} \mathbb{K}_P$ for $Q|P$, induced by the second isomorphism.

Remark 1.0.1. As shown in [Rei75, Theorem 32.20], if $\mathbb{F}$ is a finite field, all finite dimensional central simple algebras are cyclic and can be represented in the form $\frac{\mathbb{L}[T; \theta]}{T^r - x}$. Therefore, in the context of application to linear codes over algebraic curves defined over a finite field of constants, our choice of $\mathbb{D}$ is general. However, for an arbitrary constant field $\mathbb{F}$ or for a higher dimensional function field $\mathbb{K}$, the decomposition $\frac{\mathbb{L}[T; \theta]}{T^r - x}$ does not represent all central simple algebras over $\mathbb{K}$ anymore.

The goal of this section is to prove a Riemann–Roch Theorem on $\mathbb{D}$. Beyond its own interest, this result will be pivotal to design our decoding algorithm for linearized AG codes.

We mention that, following the Ph.D. thesis of Witt [Wit34], Tamagawa [Tam51] and later Mattson [Mat61] showed a Riemann–Roch Theorem in the more general setting of central simple algebras over a function field. However, our approach based on the decomposition $\mathbb{D} = \frac{\mathbb{L}[T; \theta]}{T^r - x}$, is more explicit and allows for effective duality with differential forms. In particular, this will be pivotal, in Subsection 2.1, to canonically characterize the dual of a linearized AG code as a linearized Differential code.

1.1 The case of numerical divisors

For any place $P \in \mathcal{P}_{\mathbb{K}}$, we define the positive integer

$$b_P := \frac{r}{\gcd(e_P v_P(x), r)}.$$

We note that we have $b_P = 1$ at all places where $v_P(x) = 0$, hence almost everywhere.

We define the group of *divisors* of $\mathbb{D}$

$$\text{Div}(\mathbb{D}) := \bigoplus_{P \in \mathcal{P}_{\mathbb{K}}} \bigoplus_{Q|P} \frac{\mathbb{Z}}{b_P} Q.$$

The *degree* of a divisor $A = \sum_Q A_Q Q$ is, by definition, $\deg A := \sum_Q A_Q \deg Q$.

We define the following Q -functions ω_Q

$$\begin{aligned} \omega_Q : \quad \mathbb{D}_P \simeq \sum_{j=0}^{r-1} \mathbb{L}_P T^j &\longrightarrow \frac{\mathbb{Z}}{b_P} \\ y = \sum_{j=0}^{r-1} (y_{jQ'})_{Q'|P} T^j &\mapsto \min_{0 \leq j < r} \left(w_Q(y_{jQ}) + j \frac{w_Q(x)}{r} \right) \end{aligned}$$

and the gauge

$$\begin{aligned} \omega_P : \quad \mathbb{D}_P &\longrightarrow \frac{\mathbb{Z}}{b_P e_P} \\ (\alpha_Q)_{Q|P} &\mapsto \min_{Q|P} \frac{\omega_Q(\alpha_Q)}{e_P}. \end{aligned}$$

Note that the definition ω_Q corresponds to the definition $e_P \cdot w_{j,x}$ from [BC24].

Lemma 1.1.1. *The gauge ω_P is surmultiplicative, that is, for every $f, g \in \mathbb{D}_P$ it holds*

$$\omega_P(fg) \geq \omega_P(f) + \omega_P(g).$$

Proof. Let $P \in \mathcal{P}_{\mathbb{K}}$. For $f, g \in \mathbb{D}_P$, we have

$$\omega_P(fg) = \omega_P \left(\sum_{i=0}^r f_i T^i \sum_{i=0}^r g_i T^i \right) = \omega_P \left(\sum_{i=0}^r \sum_{k=0}^i f_k \theta^k(g_{i-k}) T^i + \sum_{i=r}^{2r-1} \sum_{k=i-r}^r f_k \theta^k(g_{i-k}) T^{i-r} \right).$$

Let i_0 be the index of a minimal summand. We let $Q_1, \dots, Q_{m_P}$ be the places above P , indexed such that $\Phi(Q_j) = Q_{(j+1)\%m_P}$. We distinguish the two cases $i_0 \geq r$ and $0 \leq i_0 < r$. In the first case, we have

$$\begin{aligned} \omega_P(fg) &\geq \min_j \left(\frac{w_{Q_j}(\sum_{0 \leq k \leq i_0} f_k \theta^k(g_{i_0-k}))}{e_P} + \frac{(i_0 - r)v_P(x)}{r} \right) \\ &\geq \min_j \min_{0 \leq k \leq i_0} \left(\frac{w_{Q_j}(x f_k \theta^k(g_{i_0-k}))}{e_P} + \frac{(i_0 - r)v_P(x)}{r} \right) \\ &\geq \min_j \min_{0 \leq k \leq i_0} \left(\frac{w_{Q_j}(f_k)}{e_P} + \frac{kv_P(x)}{r} + \frac{w_{Q_{(j+k)\%m_P}}(g_{i_0-k})}{e_P} + \frac{(i_0 - k)v_P(x)}{r} \right), \end{aligned}$$

which is greater than $\omega_P(f) + \omega_P(g)$. In the second case, we have

$$\begin{aligned} \omega_P(fg) &\geq \min_j \left(\frac{w_{Q_j}(\sum_{0 \leq k \leq i_0} f_k \theta^k(g_{i_0-k}))}{e_P} + \frac{i_0 v_P(x)}{r} \right) \\ &\geq \min_j \min_{0 \leq k \leq i_0} \left(\frac{w_{Q_j}(f_k \theta^k(g_{i_0-k}))}{e_P} + \frac{i_0 v_P(x)}{r} \right) \\ &\geq \min_j \min_{0 \leq k \leq i_0} \left(\frac{w_{Q_j}(f_k)}{e_P} + \frac{kv_P(x)}{r} + \frac{w_{Q_{(j+k)\%m_P}}(g_{i_0-k})}{e_P} + \frac{(i_0 - k)v_P(x)}{r} \right), \end{aligned}$$

which is also greater than $\omega_P(f) + \omega_P(g)$. □

Using the surmultiplicativity property of the gauge from Lemma 1.1.1, we can state the following definition.

Definition 1.1.2. For any place $P \in \mathcal{P}_{\mathbb{K}}$, we define the order Λ_P as

$$\Lambda_P := \{f \in \mathbb{D} \mid \omega_P(f) \geq 0\}.$$

Definition 1.1.3. The *principal divisor* of a function $f \in \mathbb{D}$ is $(f) = \sum_{Q \in \mathcal{P}_{\mathbb{L}}} \omega_Q(f)Q$.

Definition 1.1.4 ([BC24, Definition 2.3]). For any $A \in \text{Div}(\mathbb{D})$, the *Riemann–Roch space* associated to A is

$$\Lambda_{\mathbb{D}}(A) := \{f \in \mathbb{D} \mid \omega_Q(f) + A_Q \geq 0 \quad \forall Q \in \mathcal{P}_{\mathbb{L}}\}.$$

We denote by $\lambda_{\mathbb{D}}(A)$ its dimension.

The aim of our Riemann–Roch Theorem is to relate $\lambda_{\mathbb{D}}(A)$ to the dimension of another Riemann–Roch space. We now introduce the necessary notions to define the parameters corresponding to this second Riemann–Roch space.

Definition 1.1.5. The *different divisor* Δ of $\mathbb{D}$ (relative to the gauges ω_P) is

$$\Delta := \sum_{P \in \mathcal{P}_{\mathbb{K}}} \sum_{Q|P} \frac{b_P - 1}{b_P} Q.$$

Definition 1.1.6. A *canonical divisor* of $\mathbb{D}$ is $K := K_{\mathbb{L}} + \Delta$ where $K_{\mathbb{L}}$ is a canonical divisor of $\mathbb{L}$.

Definition 1.1.7. The *genus* of $\mathbb{D}$ (relative to the gauges ω_P) is the rational number g defined by $2g - 2 = \deg(K)$.

The genus g does not depend on the choice of K as $\deg(K_{\mathbb{L}})$ does not either.

Definition 1.1.8. The *adjoint algebra* of $\mathbb{D}$ is

$$\mathbb{D}^{\star} := \frac{\mathbb{L}[T; \theta]}{T^r - x^{-1}}.$$

Definition 1.1.9. We define the *adjunction* on $\mathbb{D}$ as the following involution:

$$\begin{aligned} \mathbb{D} &\longrightarrow \mathbb{D}^{\star} \\ f = \sum_{i=0}^{r-1} \alpha_i T^i &\mapsto f^{\star} = \sum_{i=0}^{r-1} T^{-i} \alpha_i \quad (\text{with } \alpha_i \in \mathbb{L}). \end{aligned}$$

We readily check that $f \mapsto f^{\star}$ is an anti-isomorphism, *i.e.*, it satisfies $(fg)^{\star} = g^{\star} f^{\star}$, and that $\omega_P(f) = \omega_P(f^{\star})$ for any place $P \in \mathcal{P}_{\mathbb{K}}$. We define the maps

$$\begin{aligned} \text{Div}(\mathbb{D}) &\xrightarrow{\pi_i} \text{Div}(\mathbb{L}) & ; & \quad \text{Div}(\mathbb{D}^{\star}) \xrightarrow{\pi_i^{\star}} \text{Div}(\mathbb{L}) \\ \sum_{Q \in \mathcal{P}_{\mathbb{L}}} A_Q Q &\mapsto \sum_{Q \in \mathcal{P}_{\mathbb{L}}} [A_Q + i \frac{w_Q(x)}{r}] Q & & \quad \sum_{Q \in \mathcal{P}_{\mathbb{L}}} A_Q Q \mapsto \sum_{Q \in \mathcal{P}_{\mathbb{L}}} [A_Q - i \frac{w_Q(x)}{r}] Q \end{aligned}$$

where $\text{Div}(\mathbb{D}^{\star}) := \text{Div}(\mathbb{D})$. In the sequel, we shall use π_i and $\pi_i^{\star}$ in combination with the isomorphisms below as in [BC24, Equation (5)], and write

$$\Lambda_{\mathbb{D}}(A) \simeq \oplus_{i=0}^{r-1} L(\pi_i(A)) \quad \text{and} \quad \Lambda_{\mathbb{D}^{\star}}(A) \simeq \oplus_{i=0}^{r-1} L(\pi_i^{\star}(A)), \quad (1.1.1)$$

where $L(-)$ denotes the classical Riemann–Roch space of $\mathbb{L}$ associated to the divisor in argument.

Theorem 1.1.10 (Riemann–Roch Theorem). *For any $A \in \text{Div}(\mathbb{D})$ and any choice of a canonical divisor K , we have*

$$\lambda_{\mathbb{D}}(A) = r \cdot \deg A + r(1 - g) + \lambda_{\mathbb{D}^*}(K - A).$$

Proof. Applying the classical Riemann–Roch theorem on $\mathbb{L}$ [Sti93, Theorem 1.5.15], we have for any choice of $K_{\mathbb{L}}$ and for any $i \in \{0, \dots, r-1\}$

$$\dim L(\pi_i(A)) = \deg \pi_i(A) + 1 - g_{\mathbb{L}} + \dim L(K_{\mathbb{L}} - \pi_i(A)). \quad (1.1.2)$$

We sum the Equations (1.1.2) over the indices i and consider each summand of the equation separately. First, using Equation (1.1.1), we get $\sum_{i=0}^{r-1} \dim L(\pi_i(A)) = \lambda_{\mathbb{D}}(A)$. Secondly, from [BC24, Lemma 2.5], we have $\sum_{i=0}^{r-1} \deg(\pi_i(A)) = r \deg A - r \frac{\deg(\Delta)}{2}$. Thirdly, since $g_{\mathbb{L}} = g - \frac{\deg \Delta}{2}$, we have $\sum_{i=0}^{r-1} (1 - g_{\mathbb{L}}) = r(1 - g) + r \frac{\deg(\Delta)}{2}$. Finally, we set $a = A_Q + i \frac{w_Q(x)}{r}$. As a belongs to $\frac{\mathbb{Z}}{b_P}$, we get $\left\lfloor \frac{b_P-1}{b_P} - (a - [a]) \right\rfloor = 0$. Now, summing $-[a] = \left\lfloor \frac{b_P-1}{b_P} - a \right\rfloor$ over all places $Q \in \mathcal{P}_{\mathbb{L}}$, we get $-\pi_i(A) = \pi_i^*(\Delta - A)$. Thus, we get $K_{\mathbb{L}} - \pi_i(A) = K_{\mathbb{L}} + \pi_i^*(\Delta - A)$. As $K_{\mathbb{L}}$ belongs to $\text{Div}(\mathbb{L}) \subset \text{Div}(\mathbb{D})$, we have $K_{\mathbb{L}} + \pi_i^*(\Delta - A) = \pi_i^*(K - A)$. Hence, using Equation (1.1.1), we retrieve $\sum_{i=0}^{r-1} \dim L(K_{\mathbb{L}} - \pi_i(A)) = \sum_{i=0}^{r-1} \dim L(\pi_i^*(K - A)) = \lambda_{\mathbb{D}^*}(K - A)$.

Summing the four terms, we recover the statement. $\square$

1.2 Riemann theorem for extended divisors

We now aim at proving an extension of Theorem 1.1.10 allowing for more general divisors, that we call “extended divisors” (see Definition 1.2.1 below).

For this, we fix $\{P_1, \dots, P_s\}$, a finite set of s rational *unramified places* of $\mathbb{K}$ indexed by $[s] := \{1, \dots, s\}$ and set $D := P_1 + \dots + P_s \in \text{Div}(\mathbb{K})$. We assume moreover that all P_i satisfy the hypothesis **(H2- P_i)** of [BC24, Section IV A], *i.e.*, that there exist elements $u_Q \in \mathbb{L}_Q^\times$ such that, for all $Q \in \mathcal{P}_{\mathbb{L}}$ above P_i , we have

$$w_Q(u_Q) = \frac{w_Q(x)}{r} \quad \text{and} \quad x = \left(\text{Nr}_{\mathbb{L}_Q/\mathbb{K}_{P_i}}(u_Q) \right)_{Q|P} \in \mathbb{L}_P. \quad (1.2.1)$$

If we assume $\mathbb{F}$ to be finite, a sufficient condition for this to hold is that r divides $v_{P_i}(x)$ (see [BC24, Lemma 6]).

We set $u_{P_i} := (u_Q)_{Q|P_i} \in \mathbb{L}_{P_i}$ and recall from [BC24, Section IV A] that there is an isomorphism of $\mathbb{K}_{P_i}$ -algebras $\varepsilon_i : \mathbb{D}_{P_i} \rightarrow \text{End}_{\mathbb{K}_{P_i}}(\mathbb{L}_{P_i})$, $f(T) \mapsto f(u_{P_i}\theta)$. Moreover, its restriction to Λ_{P_i} induces a second isomorphism

$$\varepsilon_{i|\Lambda_{P_i}} : \Lambda_{P_i} \xrightarrow{\sim} \text{End}_{\mathcal{O}_{P_i}}(\mathcal{O}_{\mathbb{L}, P_i}). \quad (1.2.2)$$

For $i \in [s]$, we define the *residual algebra* at P by $V_i := \mathcal{O}_{\mathbb{L}, P_i} / P_i \mathcal{O}_{\mathbb{L}, P_i}$ and set $V_D := \bigoplus_{i=1}^s V_i$. Since P_i is a rational place, we have $\dim_{\mathbb{F}} V_i = r$ and so $\dim_{\mathbb{F}} V_D = sr$.

We denote by $\text{Div}(\mathbb{D}, D)$ the subgroup of divisors of $\mathbb{D}$ away from D , that is,

$$\text{Div}(\mathbb{D}, D) := \{A \in \text{Div}(\mathbb{D}) \mid A_Q = 0 \quad \forall Q|P_i \quad \forall i \in [s]\}.$$

Definition 1.2.1. An *extended divisor* (A, W) is a pair composed of a divisor $A \in \text{Div}(\mathbb{D}, D)$ and a direct sum of $\mathbb{F}$ -vector subspaces $W := \bigoplus_{i=1}^s W_i \subset V_D$, where $W_i \subset V_i$.

Its *degree* is $\deg(A, W) := \deg A - \dim_{\mathbb{F}}(W)$.

We recall the definition of the space of adeles $\mathcal{A}_{\mathbb{L}}(A)$ of $\mathbb{L}$ for a divisor $A = \sum_{Q \in \mathcal{P}_{\mathbb{L}}} A_Q Q \in \text{Div}(\mathbb{L})$ as in [Sti93, Definition 1.5.3]:

$$\mathcal{A}_{\mathbb{L}}(A) := \left\{ (y_Q)_Q \in \prod_{Q \in \mathcal{P}_{\mathbb{L}}} \mathbb{L}_Q \left| w_Q(y_Q) + A_Q \geq 0 \right. \right\}.$$

We also let $\mathcal{A}_{\mathbb{L}}$ be the union of all $\mathcal{A}_{\mathbb{L}}(A)$. It is also the set of sequences $(y_Q)_Q$ such that $w_Q(y_Q) \geq 0$ for almost all Q .

Definition 1.2.2. For a divisor $A = \sum_{Q \in \mathcal{P}_{\mathbb{L}}} A_Q Q \in \text{Div}(\mathbb{D})$, we define

$$\mathcal{A}_{\mathbb{D}}(A) := \left\{ (\alpha_P)_P \in \prod_{P \in \mathcal{P}_{\mathbb{K}}} \mathbb{D}_P \left| \omega_Q(\alpha_P) + A_Q \geq 0 \quad \forall P \quad \forall Q|P \right. \right\}$$

and let $\mathcal{A}_{\mathbb{D}}$ be the union of all $\mathcal{A}_{\mathbb{D}}(A)$.

Note that by definition, we have $\Lambda_{\mathbb{D}}(A) = \mathcal{A}_{\mathbb{D}}(A) \cap \mathbb{D}$.

Lemma 1.2.3. *We have the following isomorphism of $\mathcal{A}_{\mathbb{K}}$ -algebras*

$$\mathcal{A}_{\mathbb{D}} \simeq \bigoplus_{i=0}^{r-1} \mathcal{A}_{\mathbb{L}} T^i.$$

Proof. The support of (x) in $\mathcal{P}_{\mathbb{L}}$ being finite, we conclude using the isomorphism $\mathbb{L} \otimes_{\mathbb{K}} \mathbb{K}_P \simeq \prod_{Q|P} \mathbb{L}_Q$. $\square$

In the sequel, we will use that $\mathbb{L}$ (resp. $\mathbb{D}$) injects diagonally in $\mathcal{A}_{\mathbb{L}}$ (resp. $\mathcal{A}_{\mathbb{D}}$).

Lemma 1.2.4. *Let $A \in \text{Div}(\mathbb{D})$. We have the following isomorphisms of $\mathbb{F}$ -vector spaces*

$$\mathcal{A}_{\mathbb{D}}(A) \simeq \bigoplus_{i=0}^{r-1} \mathcal{A}_{\mathbb{L}}(\pi_i(A)) \quad \text{and} \quad \frac{\mathcal{A}_{\mathbb{D}}}{\mathcal{A}_{\mathbb{D}}(A) + \mathbb{D}} \simeq \bigoplus_{i=0}^{r-1} \frac{\mathcal{A}_{\mathbb{L}}}{\mathcal{A}_{\mathbb{L}}(\pi_i(A)) + \mathbb{L}}.$$

Proof. The first isomorphism is analogue to the isomorphism of Equation (1.1.1). The isomorphism of Lemma 1.2.3 and the isomorphism $\mathcal{A}_{\mathbb{D}}(A) + \mathbb{D} \simeq \bigoplus_{i=0}^{r-1} (\mathcal{A}_{\mathbb{L}}(\pi_i(A)) + \mathbb{L})$ together with the natural injection $\mathcal{A}_{\mathbb{D}}(A) + \mathbb{D} \hookrightarrow \mathcal{A}_{\mathbb{D}}$ induced by the diagonal embedding of $\mathbb{D}$ in $\mathcal{A}_{\mathbb{D}}$ allow us to build the quotients and prove the second isomorphism. $\square$

We recall the definition of the evaluation map at $P_i \in \mathcal{P}_{\mathbb{K}}$ for any divisor $A \in \text{Div}(\mathbb{D}, D)$ as the following composition of morphisms according to [BC24, Definition 3.3]:

$$\bar{\varepsilon}_i : \Lambda_{\mathbb{D}}(A) \hookrightarrow \Lambda_{P_i} \xrightarrow{\varepsilon_i} \text{End}_{\mathcal{O}_{P_i}}(\mathcal{O}_{\mathbb{L}, P_i}) \twoheadrightarrow \text{End}_{\mathbb{F}}(V_i), \quad (1.2.3)$$

where the first map is the inclusion and the last one is the projection.

Definition 1.2.5. Let (A, W) be an extended divisor. We define:

$$\begin{aligned} \mathcal{A}_{\mathbb{D}}(A, W) &:= \{ f \in \mathcal{A}_{\mathbb{D}}(A) \mid \bar{\varepsilon}_i(f)|_{W_i} = 0 \quad \forall i \in [s] \}, \\ \Lambda_{\mathbb{D}}(A, W) &:= \mathcal{A}_{\mathbb{D}}(A, W) \cap \mathbb{D}. \end{aligned}$$

We denote by $\lambda_{\mathbb{D}}(A, W)$ the dimension of $\Lambda_{\mathbb{D}}(A, W)$.

We define the conorm of a divisor as follows:

$$\begin{aligned} \text{CoNr} : \quad \text{Div}(\mathbb{K}) &\rightarrow \text{Div}(\mathbb{L}) \subset \text{Div}(\mathbb{D}) \\ P &\mapsto e_P \sum_{Q|P} Q \end{aligned}.$$

Lemma 1.2.6. For $A \in \text{Div}(\mathbb{D}, D)$, we have $\mathcal{A}_{\mathbb{D}}(A, V_D) = \mathcal{A}_{\mathbb{D}}(A - \text{CoNr}(D))$.

Proof. By definition, the kernel of $\varepsilon_i : \Lambda_{P_i} \xrightarrow{\varepsilon_i} \text{End}_{\mathcal{O}_{P_i}}(\mathcal{O}_{\mathbb{L}, P_i}) \rightarrow \text{End}_{\mathbb{F}}(V_i)$ is the inverse image of $\text{Hom}_{\mathcal{O}_{P_i}}(\mathcal{O}_{\mathbb{L}, P_i}, P_i \mathcal{O}_{\mathbb{L}, P_i})$ by ε_i , which is $\mathcal{A}_{\mathbb{D}}(A - \text{CoNr}(D))_{P_i}$. $\square$

Definition 1.2.7. The *index of speciality* of an extended divisor (A, W) is

$$i(A, W) := \lambda_{\mathbb{D}}(A, W) - r \deg(A, W) - r(1 - g).$$

Proposition 1.2.8. For any extended divisor (A, W) , we have

$$i(A, W) = \dim_{\mathbb{F}} \left(\frac{\mathcal{A}_{\mathbb{D}}}{\mathcal{A}_{\mathbb{D}}(A, W) + \mathbb{D}} \right).$$

Proof. We have an isomorphism

$$\begin{aligned} \bigoplus_{i=0}^{r-1} \text{Hom} \left(\frac{\mathcal{A}_i}{\mathcal{A}_{\mathbb{L}}(\pi_i(A)) + \mathbb{L}}, \mathbb{F} \right) &\xrightarrow{\sim} \text{Hom} \left(\frac{\mathcal{A}_{\mathbb{D}}}{\mathcal{A}_{\mathbb{D}}(A) + \mathbb{D}}, \mathbb{F} \right) \\ (\nu_0, \dots, \nu_{r-1}) &\mapsto (\alpha \mapsto \sum_{i=0}^{r-1} \nu_i(\alpha_i)) \end{aligned}$$

Indeed, the map is obviously injective and it is also surjective, a preimage of $\nu \in \text{Hom} \left(\frac{\mathcal{A}_{\mathbb{D}}}{\mathcal{A}_{\mathbb{D}}(A) + \mathbb{D}}, \mathbb{F} \right)$ being given by of the linear forms $\nu_i : \alpha_i \mapsto \nu((0, \dots, \alpha_i, \dots, 0))$. Now, using this isomorphism and the Riemann–Roch Theorem 1.1.10 applied to $\Lambda_{\mathbb{D}}(A)$, we get $i(A) = \dim \left(\frac{\mathcal{A}_{\mathbb{D}}}{\mathcal{A}_{\mathbb{D}}(A) + \mathbb{D}} \right)$. Thus, we have

$$\dim \left(\frac{\mathcal{A}_{\mathbb{D}}}{\mathcal{A}_{\mathbb{D}}(A, W) + \mathbb{D}} \right) = i(A) + \dim \left(\frac{\mathcal{A}_{\mathbb{D}}(A) + \mathbb{D}}{\mathcal{A}_{\mathbb{D}}(A, W) + \mathbb{D}} \right). \quad (1.2.4)$$

In order to relate the dimension of the latter quotient to $i(A, W)$, we consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda_{\mathbb{D}}(A, W) & \longrightarrow & \mathcal{A}_{\mathbb{D}}(A, W) & \longrightarrow & \frac{\mathcal{A}_{\mathbb{D}}(A, W) + \mathbb{D}}{\mathbb{D}} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Lambda_{\mathbb{D}}(A) & \longrightarrow & \mathcal{A}_{\mathbb{D}}(A) & \longrightarrow & \frac{\mathcal{A}_{\mathbb{D}}(A) + \mathbb{D}}{\mathbb{D}} & \longrightarrow & 0 \end{array}$$

Applying the snake lemma to it, we get the following exact sequence of cokernels

$$0 \longrightarrow \frac{\Lambda_{\mathbb{D}}(A)}{\Lambda_{\mathbb{D}}(A, W)} \longrightarrow \frac{\mathcal{A}_{\mathbb{D}}(A)}{\mathcal{A}_{\mathbb{D}}(A, W)} \longrightarrow \frac{\mathcal{A}_{\mathbb{D}}(A) + \mathbb{D}}{\mathcal{A}_{\mathbb{D}}(A, W) + \mathbb{D}} \longrightarrow 0.$$

Hence

$$\dim \left(\frac{\mathcal{A}_{\mathbb{D}}(A) + \mathbb{D}}{\mathcal{A}_{\mathbb{D}}(A, W) + \mathbb{D}} \right) = \dim \left(\frac{\mathcal{A}_{\mathbb{D}}(A)}{\mathcal{A}_{\mathbb{D}}(A, W)} \right) - \lambda(A) + \lambda(A, W). \quad (1.2.5)$$

Finally, we observe that, for any $i \in [s]$, we have a second commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{A}_{\mathbb{D}}(A, V_i)_{P_i} & \longrightarrow & \mathcal{A}_{\mathbb{D}}(A)_{P_i} & \xrightarrow{\varepsilon_i} & \text{Hom}_{\mathbb{F}}(V_i, V_i) & \longrightarrow & 0 \\ & & \parallel & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & \mathcal{A}_{\mathbb{D}}(A, V_i)_{P_i} & \longrightarrow & \mathcal{A}_{\mathbb{D}}(A, W_i)_{P_i} & \xrightarrow{\varepsilon_i} & \text{Hom}_{\mathbb{F}}(V_i/W_i, V_i) & \longrightarrow & 0 \end{array}$$

from which we derive that $\mathcal{A}_{\mathbb{D}}(A)_{P_i} / \mathcal{A}_{\mathbb{D}}(A, W_i)_{P_i} \simeq \text{Hom}_{\mathbb{F}}(W_i, V_i)$. Therefore $\mathcal{A}_{\mathbb{D}}(A) / \mathcal{A}_{\mathbb{D}}(A, W)$ is isomorphic to $\bigoplus_{i \in [s]} \text{Hom}_{\mathbb{F}}(W_i, V_i)$ and thus has dimension $r \dim(W)$. Combining with Equations (1.2.4) and (1.2.5), we get the desired result. $\square$

Theorem 1.2.9. *For any extended divisor (A, W) , we have*

$$\lambda_{\mathbb{D}}(A, W) = r \deg(A, W) + r(1 - g) + \dim(\mathcal{A}_{\mathbb{D}}/(\mathcal{A}_{\mathbb{D}}(A, W) + \mathbb{D})).$$

Moreover, if $\deg(A, W) < 0$, then $\lambda_{\mathbb{D}}(A, W) = 0$.

Proof. The first equality results from Proposition 1.2.8. The second assertion is a consequence of [BC24, Theorem 3.5]. $\square$

1.3 Differentials and residues

In order to prove the Riemann–Roch Theorem for extended divisors, we now need to relate the quotient $\mathcal{A}_{\mathbb{D}}/(\mathcal{A}_{\mathbb{D}}(A, W) + \mathbb{D})$ to an actual Riemann–Roch space. As in the classical case, we will use as an intermediate a certain space of differential forms over $\mathbb{D}$.

1.3.1 Definitions

In the sequel, we denote by $\Omega_{\mathbb{K}}$ (resp. $\Omega_{\mathbb{L}}$) the module of differentials of $\mathbb{K}$ (resp. $\mathbb{L}$) as defined in [Sha13, Chapter 5]. For any differential $\eta \in \Omega_{\mathbb{K}}$, we denote by $(\eta)_{\mathbb{K}}$, (resp. $(\eta)_{\mathbb{L}}$) the divisor of η viewed as a differential of $\Omega_{\mathbb{K}}$ (resp. $\Omega_{\mathbb{L}}$). They satisfy the Riemann–Hurwitz relation $(\eta)_{\mathbb{L}} = \text{CoNr}((\eta)_{\mathbb{K}}) + \text{Diff}(\mathbb{L}/\mathbb{K})$ as stated in [Sti93, Theorem 3.4.6], where $\text{Diff}(\mathbb{L}/\mathbb{K})$ is the different divisor of $\mathbb{L}/\mathbb{K}$ as defined in [Sti93, Definition 3.4.3].

Definition 1.3.1. The *left module of differentials* of $\mathbb{D}$ is defined by $\Omega_{\mathbb{D}} := \mathbb{D} \otimes_{\mathbb{K}} \Omega_{\mathbb{K}}$.

We recall that $\Omega_{\mathbb{K}}$ is a one-dimensional vector space over $\mathbb{K}$ [Sti93, Proposition 1.5.9]. Henceforth, any element $\nu \in \Omega_{\mathbb{D}}$ is of the form $\nu = f \otimes \eta$ for $f \in \mathbb{D}$ and $\eta \in \Omega_{\mathbb{K}}$.

Definition 1.3.2. Let $\nu = f \otimes \eta \in \Omega_{\mathbb{D}}$ with $f \in \mathbb{D}$ and $\eta \in \Omega_{\mathbb{K}}$. The *principal divisor* of ν is

$$(\nu)_{\mathbb{D}} := (f) + (\eta)_{\mathbb{L}} + \Delta.$$

Proposition 1.3.3. *The divisor $(\nu)_{\mathbb{D}}$ does not depend on the choice of the decomposition.*

Proof. Let $\nu = f' \otimes \eta'$ be another decomposition. Then $\eta' = u\eta$ and $f = uf'$ for some nonzero $u \in \mathbb{K}$. As for any $v \in \mathbb{K}$, $g \in \mathbb{D}$, and $Q \in \mathcal{P}_{\mathbb{L}}$, we have $\omega_Q(vg) = \omega_Q(gv) = w_Q(v) + \omega_Q(g)$, we obtain $(f) + (\eta)_{\mathbb{L}} = (f') + (u) + (\eta)_{\mathbb{L}} = (f') + (\eta')_{\mathbb{L}}$. $\square$

Definition 1.3.4. For any $A \in \text{Div}(\mathbb{D})$, we set $\Omega_{\mathbb{D}}(A) := \{\nu \in \Omega_{\mathbb{D}} \mid (\nu)_{\mathbb{D}} \geq A\}$.

Definition 1.3.5. Let $i \in [s]$ and let $t_i \in \mathbb{K}$ be a uniformizer at P_i . Let $\nu \in \Omega_{\mathbb{D}}$ and write $\nu = f \frac{dt_i}{t_i}$ with $f \in \mathbb{D}$. If $\omega_{P_i}(f) \geq 0$, we define the *residue endomorphism* of ν at P_i by

$$\text{Res}_{P_i}(\nu) := \bar{\varepsilon}_i(f)$$

where $\bar{\varepsilon}_i$ is defined in Equation (1.2.3).

Proposition 1.3.6. *The residue endomorphism $\text{Res}_P(\nu)$ does not depend on the choice of the decomposition of ν .*

Proof. Let t'_P be another uniformizer of $\mathbb{K}$ at P and write $\nu = f' \frac{dt'_P}{t'_P}$ with $f' \in \mathbb{D}$. We then have $f = f' \frac{dt'_P}{dt_P} \frac{t_P}{t'_P}$ and so $\omega_P(f') = \omega_P(f)$. Moreover $\varepsilon_P(f) = \varepsilon_P\left(f' \frac{dt'_P}{dt_P} \frac{t_P}{t'_P}\right) = \varepsilon_P(f')$. Indeed, writing $t'_P = \tau_0 t_P(1 + t_P(\tau_1 + t_P \rho))$ with $\rho \in \mathcal{O}_P$, $\tau_1 \in \mathbb{F}$ and $\tau_0 \in \mathbb{F}^\times$, we compute $\frac{dt'_P}{dt_P} \equiv \frac{t'_P}{t_P} \equiv \tau_0 \pmod{P}$. Finally, by definition, $v_P(t'_P) = v_P(t_P) = 1$. This ensures that $\tau_0 \neq 0 \pmod{P}$. $\square$

1.3.2 The residue formula

We observe that the residue endomorphisms at different places do not live in the same ambient space. Therefore, adding them does not make sense and we then cannot hope that their sum vanishes. However, this vanishing property does hold after taking traces, as we show now.

We first recall the notion of reduced trace on $\mathbb{D}$.

Definition 1.3.7. The *reduced trace* of an element f of $\mathbb{D}$ (resp. of $\mathbb{D}_P$), denoted by $\text{Trd}(f)$, is the trace of left- $\mathbb{L}$ (resp. left- $\mathbb{L}_P$) linear endomorphism of $\mathbb{D}$ (resp. $\mathbb{D}_P$) given by right multiplication by f .

Lemma 1.3.8. Let $P \in \mathcal{P}_{\mathbb{L}}$ and let $f = f_0 + f_1T + \cdots + f_{r-1}T^{r-1} \in \mathbb{D}_P$ with $f_j \in \mathbb{L}_P$. Then $\text{Trd}(f) = \text{Tr}_{\mathbb{L}_P/\mathbb{K}_P}(f_0)$.

If moreover $P = P_i$ for some $i \in [s]$, then $\text{Trd}(f) = \text{Tr}_{\mathbb{K}_{P_i}}(\varepsilon_i(f))$ (where we recall that ε_i is the morphism defined at the beginning of Subsection 1.2).

Proof. It is similar to the proof of [BC24, Lemma 2]. $\square$

Lemma 1.3.9. Let $P \in \mathcal{P}_{\mathbb{K}}$, and $f \in \mathbb{D}_P$. We have $v_P(\text{Trd}(f)) \geq \omega_P(f)$.

Proof. Let $f = f_0 + f_1T + \cdots + f_{r-1}T^{r-1} \in \mathbb{D}_P$ with all $f_i \in \mathbb{L}_P$. By Lemma 1.3.8 we have $\text{Trd}(f) = \text{Tr}_{\mathbb{L}/\mathbb{K}}(f_0)$. We conclude by the ultrametric inequality of ω_P that $v_P(\text{Trd}(f)) = \omega_P(\text{Tr}_{\mathbb{L}/\mathbb{K}}(f_0)) \geq \min_{0 \leq i < r}(\omega_P(\theta^i(f_0))) = \omega_P(f_0) \geq \omega_P(f)$. $\square$

Definition 1.3.10. We define the *reduced trace* on $\Omega_{\mathbb{D}}$ by

$$\begin{aligned} \text{Trd} : \Omega_{\mathbb{D}} &\longrightarrow \Omega_{\mathbb{K}} \\ f \otimes \eta &\longmapsto \text{Trd}(f) \cdot \eta \end{aligned}$$

For $\nu \in \Omega_{\mathbb{D}}$, we define the *reduced residue* of ν at a place P by

$$\text{Resrd}_P(\nu) := \text{Res}_P(\text{Trd}(\nu)),$$

where the right-hand side is the classical residue of $\text{Trd}(\nu) \in \Omega_{\mathbb{K}}$ at the place P .

Proposition 1.3.11. Let $i \in [s]$. Then, for any $\nu \in \Omega_{\mathbb{D}}$ such that $\text{Res}_{P_i}(\nu)$ is defined, we have $\text{Resrd}_{P_i}(\nu) = \text{Tr}_{\mathbb{F}}(\text{Res}_{P_i}(\nu))$.

Proof. We write $\nu = f \frac{dt_i}{t_i}$ where t_i is a uniformizer at P_i , so that $\omega_P(f) \geq 0$ and $\text{Res}_{P_i}(\nu) = \bar{\varepsilon}_i(f)$. From Lemma 1.3.9, we deduce $v_P(\text{Trd}(f)) \geq 0$ and then

$$\text{Resrd}_{P_i}(\nu) = \text{Res}_{P_i}(\text{Trd}(f) \frac{dt_i}{t_i}) = \text{Trd}(f) \bmod P_i.$$

On the other hand, Lemma 1.3.8 ensures that $\text{Trd}(f) = \text{Tr}_{\mathbb{K}_{P_i}}(\varepsilon_i(f))$. Reducing modulo P_i , we obtain $\text{Trd}(f) \bmod P_i = \text{Tr}_{\mathbb{F}}(\bar{\varepsilon}_i(f)) = \text{Tr}_{\mathbb{F}}(\text{Res}_{P_i}(\nu))$. $\square$

Theorem 1.3.12 (Residue Theorem). For $\nu \in \Omega_{\mathbb{D}}$, we have

$$\sum_{P \in \mathcal{P}_{\mathbb{K}}} \text{Resrd}_P(\nu) = 0.$$

Proof. We apply the residue theorem as stated in [Sha13, Theorem 3.27] to $\text{Trd}(\nu) \in \Omega_{\mathbb{K}}$ and conclude. $\square$

1.3.3 Riemann–Roch spaces

For all $i \in [s]$, we endow the space V_i with the bilinear form

$$\begin{aligned} \langle -, - \rangle : V_i \times V_i &\rightarrow \mathbb{F} \\ (v_i, w_i) &\mapsto \text{Tr}_{V_i/\mathbb{F}}(v_i w_i). \end{aligned}$$

It is nondegenerate given that the place P_i is supposed to be unramified in the extension $\mathbb{L}/\mathbb{K}$. If W_i is a vector subspace of V_i , we write $W_i^\perp$ for its orthogonal and, similarly, if $W = \bigoplus_{i=1}^s W_i$ is a subspace of V_D , we define $W^\perp = \bigoplus_{i=1}^s W_i^\perp$.

We now introduce Riemann–Roch spaces of differential forms: if (A, W) is an extended divisor, we set

$$\Omega_{\mathbb{D}}(A, W) := \{ \nu \in \Omega_{\mathbb{D}}(A - \text{CoNr}(D)) \mid \text{Res}_{P_i}(\nu)|_{W_i^\perp} = 0, \forall i \in [s] \}.$$

It follows from Lemma 1.2.6 that $\Omega_{\mathbb{D}}(A, 0) = \Omega_{\mathbb{D}}(A)$ for any $A \in \text{Div}(\mathbb{D}, D)$.

It turns out that Riemann–Roch spaces of differential forms are related to classical Riemann–Roch spaces. In order to make this relationship explicit, we choose $t_D \in \mathbb{K}$ such that $v_{P_i}(t_D) = 1$ for all $i \in [s]$ and set

$$K := \left(\frac{dt_D}{t_D} \right)_{\mathbb{D}} = \left(\frac{dt_D}{t_D} \right)_{\mathbb{L}} + \Delta. \quad (1.3.1)$$

It is a canonical divisor of $\mathbb{D}$ in the sense of Definition 1.1.6.

Definition 1.3.13. For an extended divisor (A, W) , we set $(A, W)^\star := (K + \text{CoNr}(D) - A, W^\perp)$.

Theorem 1.3.14. For any extended divisor (A, W) , we have the isomorphism:

$$\begin{aligned} \Lambda_{\mathbb{D}}((A, W)^\star) &\xrightarrow{\sim} \Omega_{\mathbb{D}}(A, W) \\ f &\mapsto f \frac{dt_D}{t_D} \end{aligned}$$

Proof. It follows directly from the definitions. $\square$

1.4 Serre duality and Riemann–Roch Theorem

The last step of the proof of the Riemann–Roch Theorem consists in relating the adelic quotient $\mathcal{A}_{\mathbb{D}}/(\mathcal{A}_{\mathbb{D}}(A, W) + \mathbb{D})$ to the space of differential forms $\Omega_{\mathbb{D}^\star}(A, W)$, where $\mathbb{D}^\star$ is the adjoint algebra as introduced in Definition 1.1.8.

We recall from Definition 1.1.9 that we have already introduced an adjunction $\mathbb{D} \rightarrow \mathbb{D}^\star$, $f \mapsto f^\star$ at the level of Ore polynomials. It naturally extends to differential forms as follows:

$$\begin{aligned} \Omega_{\mathbb{D}} &\longrightarrow \Omega_{\mathbb{D}^\star} \\ \nu = f \otimes \eta &\mapsto \nu^\star := f^\star \otimes \eta \end{aligned}$$

with, as usual, $f \in \mathbb{D}$ and $\eta \in \Omega_{\mathbb{K}}$. Besides, for all $i \in [s]$, the algebra $\text{End}_{\mathbb{F}}(V_i)$ is also endowed with an adjunction $\varphi_i \mapsto \varphi_i^\star$ defined by the standard property

$$\langle \varphi_i(v_i), w_i \rangle = \langle v_i, \varphi_i^\star(w_i) \rangle \quad (v_i, w_i \in V_i).$$

We recall the classical formulas $\ker(\varphi_i^\star) = \text{im}(\varphi_i)^\perp$ and $\text{im}(\varphi_i^\star) = \ker(\varphi_i)^\perp$.

If φ is a tuple $(\varphi_1, \dots, \varphi_s)$, we will often write $\varphi^\star = (\varphi_1^\star, \dots, \varphi_s^\star)$ for simplicity.

Lemma 1.4.1. Let $A \in \text{Div}(\mathbb{D}, D)$ and let $f \in \mathbb{D}$. If $i \in [s]$ is such that $\omega_{P_i}(f) \geq 0$, then

$$\bar{\varepsilon}_i(f)^\star = \bar{\varepsilon}_i(f^\star) \quad \text{and} \quad \text{Resrd}_{P_i} \left(f \frac{dt_D}{t_D} \right)^\star = \text{Resrd}_{P_i} \left(f^\star \frac{dt_D}{t_D} \right)$$

where, in a slight abuse of notation, we continue to write $\bar{\varepsilon}_i$ for the evaluation morphism on $\mathbb{D}^\star$.

Proof. We reuse the notation u_{P_i} introduced in Equation (1.2.1). By linearity, it is enough to check that $\langle \bar{\varepsilon}_i(f^\star)(v_i), w_i \rangle = \langle v_i, \bar{\varepsilon}_i(f)(w_i) \rangle$ for $f = f_j T^j$ and $v_i, w_i \in V_i$. Setting $\text{Nr}_{a,b}(u_P) := \prod_{k=a}^{b-1} \theta^k(u_P)$, we compute

$$\bar{\varepsilon}_i(f^\star) = \bar{\varepsilon}_i \left(\frac{T^{r-j}}{x^{-1}} f_j \right) = \frac{\text{Nr}_{0,r-j}(u_P^{-1}) \theta^{r-j}(f_j)}{\text{Nr}_{0,r}(u_P^{-1})} \theta^{r-j} = \frac{\theta^{r-j}(f_j)}{\text{Nr}_{r-j,r}(u_P^{-1})} \theta^{r-j}$$

as changing $x \mapsto x^{-1}$ in $\mathbb{D}^\star$ induces the change $u_{P_i} \mapsto u_{P_i}^{-1}$. Using $\theta^j(\text{Nr}_{r-j,r}(u_{P_i})) = \text{Nr}_{0,j}(u_{P_i})$, we get

$$\begin{aligned} \text{Tr}_{V_i/\mathbb{F}} \left(\frac{\theta^{r-j}(f_j)}{\text{Nr}_{r-j,r}(u_{P_i}^{-1})} \theta^{r-j}(v_i) w_i \right) &= \sum_{k=0}^{r-1} \theta^k \left(\frac{\theta^{r-j}(f_j)}{\text{Nr}_{r-j,r}(u_{P_i}^{-1})} \theta^{r-j}(v_i) w_i \right) \\ &= \text{Tr}_{V_i/\mathbb{F}} (v_i f_j \text{Nr}_{0,j}(u_{P_i}) \theta^j(w_i)), \end{aligned}$$

which concludes the proof. $\square$

Theorem 1.4.2. *For any extended divisor (A, W) , the $\mathbb{F}$ -bilinear form*

$$\begin{aligned} \Phi : \mathcal{A}_{\mathbb{D}}/(\mathcal{A}_{\mathbb{D}}(A, W) + \mathbb{D}) \times \Omega_{\mathbb{D}^\star}(A, W) &\longrightarrow \mathbb{F} \\ (\alpha, \nu) &\longmapsto \sum_{P \in \mathcal{P}_{\mathbb{K}}} \text{Resrd}(\alpha_P \nu^\star) \end{aligned}$$

is a perfect pairing.

Before diving into the proof, we show that this pairing is well-defined.

Lemma 1.4.3. *For $\nu \in \Omega_{\mathbb{D}^\star}(A, W)$, $\alpha \in \mathcal{A}_{\mathbb{D}}(A, W)$ and $a \in \mathbb{D}$, we have $\Phi(\alpha + a, \nu) = 0$.*

Proof. As we have $a\nu^\star \in \Omega_{\mathbb{D}}$, we get $\Phi(a, \nu) = 0$ by applying Theorem 1.3.12 to $a\nu^\star$.

It remains to prove $\Phi(\alpha, \nu) = 0$. Let $P \in \mathcal{P}_{\mathbb{K}}$. We first assume that P is one of the P_i , $i \in [s]$. Then $\text{Res}_{P_i}(\alpha_P \nu^\star)$ is defined and

$$\text{Res}_{P_i}(\alpha_P \nu^\star) = \bar{\varepsilon}_i(\alpha_P) \circ \text{Res}_{P_i}(\nu^\star) = \bar{\varepsilon}_i(\alpha_P) \circ \text{Res}_{P_i}(\nu)^\star.$$

Moreover, we know that $\bar{\varepsilon}_i(\alpha_P)$ and $\text{Res}_{P_i}(\nu)$ vanish on W_i and $W_i^\perp$ respectively. In other words $\text{im } \text{Res}_{P_i}(\nu)^\star = (\ker \text{Res}_{P_i}(\nu))^\perp \subset W_i \subset \ker \bar{\varepsilon}_i(\alpha_P)$. We deduce that $\text{Res}_{P_i}(\alpha_P \nu^\star)$ vanishes and so does its trace, *i.e.*, $\text{Resrd}_{P_i}(\alpha_P \nu^\star) = 0$.

We now consider the case where P is not an evaluation place. We write $\nu = f \otimes \eta$ where $f \in \mathbb{D}$ and $\eta \in \Omega_{\mathbb{K}}$ is chosen such that it has neither zero nor pole at P . We write $\alpha_P = \sum_{j=0}^{r-1} \alpha_j T^j$ (with $\alpha_j \in \mathbb{L}_P$) and $f = \sum_{j=0}^{r-1} f_j T^j$ (with $f_j \in \mathbb{L}$). It follows from Lemma 1.3.8 that

$$\text{Resrd}_P(\alpha_P \nu^\star) = \text{Res}_P(\text{Trd}(\alpha_P f^\star) \cdot \eta) = \sum_{j=0}^{r-1} \text{Res}_P(\text{Tr}_{\mathbb{L}_P/\mathbb{K}_P}(\alpha_j f_j) \cdot \eta).$$

On the other hand, we deduce from the definition of the Riemann–Roch spaces that, for any place $Q \mid P$, we have the estimations

$$\begin{aligned} w_Q(a_j) &\geq -A_Q - \frac{j}{r} v_P(x) \\ w_Q(f_j) + w_Q(\text{Diff}(\mathbb{L}/\mathbb{K})) &\geq A_Q + \frac{j}{r} v_P(x) - \frac{b_P - 1}{b_P} \end{aligned}$$

where $\text{Diff}(\mathbb{L}/\mathbb{K})$ denotes the different of $\mathbb{L}/\mathbb{K}$. Adding the two inequalities and replacing the right hand sides by their ceilings, we find that $w_Q(a_j f_j) \geq -w_Q(\text{Diff}(\mathbb{L}/\mathbb{K}))$, as $\lceil -\frac{b_P - 1}{b_P} \rceil \geq 0$. Hence, by definition of the different, $\text{Tr}_{\mathbb{L}_P/\mathbb{K}_P}(a_j f_j)$ has no pole at P . Therefore the residue at P of $\text{Tr}_{\mathbb{L}_P/\mathbb{K}_P}(a_j f_j) \cdot \eta$ vanishes, and we conclude that $\text{Resrd}_P(\alpha_P \nu^\star) = 0$. $\square$

Proof of Theorem 1.4.2. By Lemma 1.4.3 the pairing Φ is well-defined. The proof of its non-degeneracy breaks down into two parts, proving the injectivity and then the surjectivity of the morphism

$$\begin{aligned} \psi : \Omega_{\mathbb{D}^\star}(A, W) &\rightarrow \text{Hom}(\mathcal{A}_{\mathbb{D}}/(\mathcal{A}_{\mathbb{D}}(A, W) + \mathbb{D}), \mathbb{F}) \\ \nu &\mapsto (\alpha \mapsto \Phi(\alpha, \nu)) \end{aligned}.$$

Injectivity. Let P be a fixed evaluation place. Since P is unramified, we can find an element $a \in \mathcal{O}_{\mathbb{L}, P}$ such that $\text{Tr}_{\mathcal{O}_{\mathbb{L}, P}/\mathcal{O}_P}(a) \equiv 1 \pmod{P}$. We consider the adele $\beta \in \mathcal{A}_{\mathbb{D}}$ with coordinate a at P and 0 elsewhere. Let $\nu = f \otimes \frac{dt_P}{t_P} \in \Omega_{\mathbb{D}^\star}(A, W)$, $\nu \neq 0$. Since $\mathbb{D}$ is a division algebra, f is invertible and we can form the adele $\alpha = \beta \cdot (f^{-1})^\star \in \mathcal{A}_{\mathbb{D}}$. Then

$$\Phi(\alpha, \nu) = \text{Resrd}_P \left(a \frac{dt_P}{t_P} \right) = \text{Tr}_{\mathbb{L}_P/\mathbb{K}_P}(a) \pmod{P} = 1$$

and injectivity follows.

Surjectivity. By injectivity of ψ and Theorem 1.3.14, we have

$$\lambda_{\mathbb{D}^\star}((A, W)^\star) \leq i(A, W) = \lambda_{\mathbb{D}}(A, W) - (r \deg(A, W) + r(1 - g)).$$

Besides, since $K + \text{CoNr}(D) - A \in \text{Div}(\mathbb{D}^\star, D)$, we can apply the previous inequality to the extended divisor $(A, W)^\star$. It yields

$$\begin{aligned} \lambda_{\mathbb{D}}(A, W) &\leq \lambda_{\mathbb{D}^\star}((A, W)^\star) - (r \deg((A, W)^\star) + r(1 - g)) \\ &\leq \lambda_{\mathbb{D}}(A, W) - r \deg(A, W) - r \deg((A, W)^\star) + r(2g - 2) = \lambda_{\mathbb{D}}(A, W) \end{aligned}$$

as $\deg(A, W) + \deg((A, W)^\star) = 2g - 2$. Thus, all inequalities have to be equalities and we deduce $\lambda_{\mathbb{D}^\star}((A, W)^\star) = i(A, W)$. We conclude by invoking Theorem 1.3.14. $\square$

Finally, we can state and prove our Riemann–Roch Theorem for extended divisors.

Theorem 1.4.4 (Riemann–Roch Theorem). *For any extended divisor (A, W) , we have*

$$\lambda_{\mathbb{D}}(A, W) = r \deg(A, W) + r(1 - g) + \lambda_{\mathbb{D}^\star}((A, W)^\star).$$

Proof. It results by combining Theorem 1.2.9, Theorem 1.3.14 and Theorem 1.4.2. $\square$

2 Application to linearized Algebraic Geometry codes

In all what follows, we consider the same setting as in Section 1 and refer to the introduction of that section for the notation. In particular, the field $\mathbb{F}$ can still be arbitrary while, for applications to coding theory, the cases of most interest are finite fields $\mathbb{F} = \mathbb{F}_q$.

To start with, we recall the construction of linearized AG codes as settled in [BC24]. As in Subsection 1.2, we fix a finite set of unramified places $\{P_1, \dots, P_s\} \subset \mathcal{P}_{\mathbb{K}}$ satisfying the hypothesis **(H2- P_i)** and we let V_i denote the residue algebra of $\mathbb{L}$ at P_i . The ambient space in which our codes live is

$$\mathcal{H} := \text{End}_{\mathbb{F}}(V_1) \times \dots \times \text{End}_{\mathbb{F}}(V_s).$$

By choosing $\mathbb{F}$ -bases of the V_i , $\mathcal{H}$ becomes isomorphic to the s -th power of a matrix algebra, namely $(\mathbb{F}^{r \times r})^s$. However, in the algebraic context of this article, it will be convenient to work with endomorphisms, given that the evaluation morphisms $\bar{\varepsilon}_i$ (see Equation (1.2.3)) naturally

produce endomorphisms. In any case, $\mathcal{H}$ is a vector space of dimension sr over $\mathbb{F}$ and we endow it with the sum-rank metric defined by

$$d_{\text{srk}}(\varphi, \psi) = w_{\text{srk}}(\varphi - \psi) \quad \text{with} \quad w_{\text{srk}}(\varphi_1, \dots, \varphi_s) = \sum_{i=1}^s \text{rank}(\varphi_i).$$

We set $D := P_1 + \dots + P_s \in \text{Div}(\mathbb{K})$.

Definition 2.0.1. Let $A \in \text{Div}(\mathbb{D}, D)$. The *linearized Algebraic Geometry* code associated to A and D is the image of

$$\bar{\varepsilon}_D : \Lambda(A) \longrightarrow \mathcal{H}, \quad f \mapsto (\bar{\varepsilon}_1(f), \dots, \bar{\varepsilon}_s(f)).$$

It is denoted by $\text{LAG}_{\mathbb{D}}(A, D)$.

The aim of this section is to apply the theory we developed previously to characterize the duals of linearized AG codes and to decode them. In the special case where $\mathbb{K} = \mathbb{F}(t)$, $\mathbb{L} = \mathbb{F}'(t)$ for a finite cyclic extension $\mathbb{F}'/\mathbb{F}$ and A is a multiple of the point at infinity, the code $\text{LAG}_{\mathbb{D}}(A, D)$ is a linearized Reed–Solomon code [MP18a], for which the duals have already been described in [CD23] and a decoding algorithm is known [MPK19]. Another corner case corresponds to the situation where the extension $\mathbb{L}/\mathbb{K}$ is trivial: in this case, $\text{LAG}_{\mathbb{D}}(A, D)$ is nothing but a classical AG code, and our results extend the classical ones.

We also mention that, as it was pointed out in [BC25, Section IV], linearized Reed–Muller codes [BC25] can be embedded in larger linearized AG codes and hence can be decoded using our decoding algorithm.

2.1 Duality

We recall that each V_i is endowed with a nondegenerate bilinear pairing (see Subsection 1.3.3), which allows to define an adjunction $\varphi_i \mapsto \varphi_i^*$ on $\text{End}_{\mathbb{F}}(V_i)$. We use it to endow $\mathcal{H}$ with another nondegenerate bilinear pairing defined by:

$$\begin{aligned} \mathcal{H} \times \mathcal{H} &\longrightarrow \mathbb{F} \\ (\varphi, \psi) &\mapsto \langle \varphi, \psi \rangle := \sum_{i=1}^s \text{Tr}_{\mathbb{F}}(\varphi_i \circ \psi_i^*), \end{aligned}$$

where φ_i and ψ_i are the coordinates of φ and ψ respectively. We define the dual of a linearized AG code with respect to this pairing, as follows:

$$\text{LAG}_{\mathbb{D}}(A, D)^{\perp} = \{\psi \in \mathcal{H} \mid \langle \varphi, \psi \rangle = 0, \forall \varphi \in \text{LAG}_{\mathbb{D}}(A, D)\}.$$

We will now apply the duality theory developed in Subsection 1.4 to define linearized Differential (LD) codes and subsequently show that they are the duals of linearized AG codes.

Definition 2.1.1. The *linearized Differential code* associated to the divisors A and D , denoted by $\text{LD}_{\mathbb{D}}(A, D)$, is the image of the following map:

$$\begin{aligned} \Omega_{\mathbb{D}^{\bullet}}(A, V_D) &\longrightarrow \mathcal{H} \\ \nu &\mapsto (\text{Res}_{P_1}(\nu), \dots, \text{Res}_{P_s}(\nu)) \end{aligned}$$

where Res is the endomorphism residue introduced in Definition 1.3.5.

Theorem 2.1.2. Let K be the canonical divisor defined in Equation (1.3.1). Then, we have the following equalities of codes:

$$\text{LAG}_{\mathbb{D}}(A, D)^{\perp} = \text{LD}_{\mathbb{D}^{\bullet}}(A, D) = \text{LAG}_{\mathbb{D}^{\bullet}}(K + \text{CoNr}(D) - A, D).$$

Proof. We have the following commutative diagram

$$\begin{array}{ccc} \Lambda_{\mathbb{D}^*}(K + \text{CoNr}(D) - A) & \xrightarrow{f \mapsto f \frac{dt_P}{t_D}} & \Omega_{\mathbb{D}^*}(A, V_D) \\ \downarrow (\bar{\varepsilon}_i)_i & & \downarrow (\mathcal{R}\text{es}_{P_i})_i \\ \mathcal{H} & \xrightarrow{\text{Id}} & \mathcal{H} \end{array}$$

whose top arrow is an isomorphism thanks to Theorem 1.3.14. The equality between $\text{LD}_{\mathbb{D}^*}(A, D)$ and $\text{LAG}_{\mathbb{D}^*}(K + \text{CoNr}(D) - A, D)$ follows.

Let $f \in \Lambda_{\mathbb{D}^*}(A)$ and $\nu \in \Omega_{\mathbb{D}^*}(A, V_D)$. By the Residues Theorem (Theorem 1.3.12), we know that $\sum_{P \in \mathcal{P}_{\mathbb{K}}} \text{Resrd}_P(f\nu^*) = 0$. Moreover, it follows from the proof of Lemma 1.4.3 that

$$\text{Resrd}(f\nu^*) = \begin{cases} \text{Tr}_{\mathbb{F}}(\bar{\varepsilon}_i(f) \circ \mathcal{R}\text{es}_{P_i}(\nu)^*) & \text{if } P = P_i, \\ 0 & \text{if } P \notin \{P_1, \dots, P_s\}. \end{cases}$$

We deduce that the codewords attached to f , on the one hand, and ν , on the other hand, are orthogonal in $\mathcal{H}$, *i.e.*, $\text{LAG}_{\mathbb{D}}(A, D) \subset \text{LD}_{\mathbb{D}^*}(A, D)^\perp$. To show the reverse inclusion, we compare the dimensions. First of all, noticing that the kernel of $\bar{\varepsilon}_D$ is $\Lambda(A, V_D)$, we find

$$\dim_{\mathbb{F}} \text{LAG}_{\mathbb{D}}(A, D) = \lambda_{\mathbb{D}}(A) - \lambda_{\mathbb{D}}(A, V_D).$$

Then, using the first part of the theorem, we obtain similarly

$$\begin{aligned} \dim_{\mathbb{F}} \text{LD}_{\mathbb{D}^*}(A, D) &= \lambda_{\mathbb{D}^*}(K + \text{CoNr}(D) - A) - \lambda_{\mathbb{D}^*}(K + \text{CoNr}(D) - A, V_D) \\ &= sr^2 - \lambda_{\mathbb{D}}(A) - \lambda_{\mathbb{D}}(A, V_D) \end{aligned}$$

the last equality coming from the Riemann–Roch Theorem (Theorem 1.4.4) and the fact that $\dim_{\mathbb{F}} V_D = sr$. Observing that the two dimensions sum to $sr^2 = \dim_{\mathbb{F}} \mathcal{H}$ concludes the proof. $\square$

Corollary 2.1.3. *We assume $2g - 2 < \deg A < sr$. Then the code $\text{LD}_{\mathbb{D}^*}(A, D)$ has length sr^2 , dimension $sr^2 - r \deg A + r(g - 1)$ over $\mathbb{F}$ and minimum distance at least $\deg A - (2g - 2)$.*

Proof. This results from the estimates on the parameters of a linearized AG code given in [BC24, Theorem 2]. $\square$

Remark 2.1.4. As recalled in [MPSK22], a maximum sum-rank distance (MSRD) code in the sum-rank metric is a code achieving the sum-rank metric Singleton-type bound $rd + k = n + r$ where $[n, k, d]$ are the code parameters: length, dimension, and minimum distance. In our situation, both $\text{LAG}_{\mathbb{D}}(A, D)$ and its dual $\text{LD}_{\mathbb{D}^*}(A, D)$ meet the Singleton bound up to a defect of rg , *i.e.*, they both satisfy $rd + k \geq n + r(1 - g)$.

2.2 Decoding

In what follows we describe and prove a decoding algorithm for linearized AG codes with unramified evaluation places. Our algorithm can be seen as the sum-rank metric version of the one given in [Sti93, Section 8.5] for AG codes in the Hamming metric. We make the usual injectivity hypothesis on the evaluation maps giving the code and its dual, respectively, as follows.

Hypothesis 2.2.1. From now on, we assume the following condition on A :

$$2g - 2 < \deg A < sr.$$

Remark 2.2.2. The map $\bar{\varepsilon}_D$ defining the code $\text{LAG}_{\mathbb{D}}(A, D)$ is injective if and only if $\lambda_{\mathbb{D}}(A, V_D) = 0$. This latter condition is fulfilled if $\deg A < sr$. Similarly, the defining morphism of the dual code $\text{LAG}_{\mathbb{D}^*}(K + \text{CoNr}(D) - A, D)$ is injective when $\deg A > 2g - 2$. The two inequalities of Hypothesis 2.2.1 thus imply the injectivity of both $\text{LAG}_{\mathbb{D}}(A, D)$ and its dual.

We shall need the following consequence of the Riemann–Roch Theorem.

Theorem 2.2.3. *Let (A, W) be an extended divisor satisfying $2g - 2 < \deg(A, W)$. Then, the following short sequence is exact*

$$0 \rightarrow \Lambda(A, W) \rightarrow \Lambda(A) \xrightarrow{\bar{\varepsilon}_{D|W}} \prod_{i=1}^s \text{Hom}_{\mathbb{F}}(W_i, V_i) \rightarrow 0$$

where, by definition, $\bar{\varepsilon}_{D|W}(f) = (\bar{\varepsilon}_1(f)|_{W_1}, \dots, \bar{\varepsilon}_s(f)|_{W_s})$.

Proof. The short sequence is left exact by definition. By applying Theorem 1.4.4 to $\Lambda(A)$ and $\Lambda(A, W)$, we check that the difference of their dimensions is $r \dim(W)$. We then conclude to the surjectivity of $\bar{\varepsilon}_{D|W}$. $\square$

We will also need a variant of the pairing $\langle -, - \rangle$ relative to a subspace $W = \bigoplus_{i=1}^s W_i$ with $W_i \subset V_i$. Precisely, given such a subspace W , we consider the $\mathbb{F}$ -bilinear form

$$\begin{aligned} \Phi_W : \prod_{i=1}^s \text{Hom}_{\mathbb{F}}(V_i, W_i) \times \prod_{i=1}^s \text{Hom}_{\mathbb{F}}(W_i, V_i) &\rightarrow \mathbb{F} \\ (\varphi, \psi) &\mapsto \sum_{i=1}^s \text{Tr}(\varphi_i \circ \psi_i) \end{aligned}$$

where φ_i and ψ_i stand for the coordinates of φ and ψ respectively.

Lemma 2.2.4. *The bilinear form Φ_W is nondegenerate.*

Proof. If there existed a nonzero s -tuple of homomorphisms $(\varphi_1, \dots, \varphi_s)$ with $\varphi_i \in \text{Hom}_{\mathbb{F}}(V_i, W_i)$, such that, say, $a_{i_0} \neq 0$ and $\sum_{i=1}^s \text{Tr}(a_i \text{Hom}_{\mathbb{F}}(W_i, V_i)) = 0$, then taking $\psi_i = 0 \in \text{Hom}_{\mathbb{F}}(W_i, V_i)$ for $i \neq i_0$, we would have $\text{Tr}(\varphi_{i_0} \text{Hom}_{\mathbb{F}}(W_{i_0}, V_{i_0})) = 0$. This contradicts [CD23, Lemma 4.2]. $\square$

In all what follows, we set

$$\rho_{\text{algo}} := \left\lfloor \frac{d^*(A) - g - 1}{2} \right\rfloor = \left\lfloor \frac{sr - \deg A - g - 1}{2} \right\rfloor.$$

It is the maximal number of errors that we intend to decode with our algorithm.

2.2.1 An auxiliary divisor

Definition 2.2.5. A divisor $A \in \text{Div}(\mathbb{D})$ is called *Galois* if $A_Q = A_{Q'}$ when Q and Q' are above the same place.

Lemma 2.2.6. *Let $A_1, A_2 \in \text{Div}(\mathbb{D})$. If A_2 is Galois then $\Lambda_{\mathbb{D}^*}(A_1)\Lambda_{\mathbb{D}^*}(A_2) \subset \Lambda_{\mathbb{D}^*}(A_1 + A_2)$.*

Proof. Let us denote by Q_j the m_P places above the place $P \in \mathcal{P}_{\mathbb{K}}$. If we do not apply $\min_{Q_j|P}$ and thus replace ω_P by ω_{Q_j} in the proof of the surmultiplicativity of the gauge of Lemma 1.1.1, we get for any f in $\Lambda_{\mathbb{D}^*}(A_1)$ and for any g in $\Lambda_{\mathbb{D}^*}(A_2)$ that

$$\omega_{Q_j}(fg) \geq \min_{0 \leq k \leq i_0} \left(w_{Q_j}(f_k) + k \frac{w_Q(x)}{r} + w_{Q_{(j+k)\%m_P}}(g_{i_0-k}) + (i_0 - k) \frac{w_Q(x)}{r} \right).$$

Hence, for some $k_0 \in \{0, \dots, i_0\}$, we have

$$\omega_{Q_j}(fg) \geq -(A_1)_{Q_j} - (A_2)_{Q_{(j+k_0)\%m_P}} = -(A_1)_{Q_j} - (A_2)_{Q_j} = -(A_1 + A_2)_{Q_j},$$

where the first equality holds since A_2 is a Galois divisor. $\square$

We make the following assumption on $\mathbb{L}/\mathbb{K}$, which will be helpful to construct Galois divisors.

Hypothesis 2.2.7. There exists a place $P \in \mathcal{P}_{\mathbb{K}} \setminus \{P_1, \dots, P_s\}$ such that $e_P f_P = r$ and $\deg P = 1$.

Lemma 2.2.8. *There exists a divisor $A_1 \in \text{Div}(\mathbb{D}^*, D)$ such that*

- (i) $A + A_1$ is Galois,
- (ii) $\deg(A + A_1) < sr - \rho_{\text{algo}}$,
- (iii) $\lambda_{\mathbb{D}}(A_1) > r \cdot \rho_{\text{algo}}$.

Proof. Using Hypothesis 2.2.7, we can pick a Galois divisor G of degree $sr - \rho_{\text{algo}} - 1$ with support concentrated at the place P . We set $A_1 := G - A$. The first and second conditions are then clearly fulfilled. For the last one, we use the Riemann–Roch Theorem (Theorem 1.1.10), which implies

$$\frac{\lambda_{\mathbb{D}}(A_1)}{r} \geq \deg(A_1) - g + 1 = \deg(G) - \deg(A) - g + 1 = sr - \deg(A) - g - \rho_{\text{algo}}.$$

Besides, it readily follows from the definition of ρ_{algo} that $sr - \deg(A) - g \geq 2\rho_{\text{algo}} + 1$ and the proposition follows. $\square$

From now on, we fix a divisor A_1 satisfying the requirements of Lemma 2.2.8 (so, in particular, we assume Hypothesis 2.2.7).

2.2.2 Error localization

We denote by $m = c + e$ the received message as the sum of a codeword $c \in \text{LAG}_{\mathbb{D}}(A, D)$ and an error $e = (e_1, \dots, e_s)$ with $w_{\text{srk}}(e) \leq \rho_{\text{algo}}$. The first step for decoding consists in finding a localizing function $f \in \mathbb{D}^*$ in the following sense.

Definition 2.2.9. An *error localizing function* relative to the code $\text{LAG}_{\mathbb{D}}(A, D)$ and an error e is a function $f \in \mathbb{D}^*$ such that $e_i^* \circ \bar{\varepsilon}_i(f) = 0$ for all $i \in [s]$.

We note that the vanishing condition $e_i^* \circ \bar{\varepsilon}_i(f) = 0$ is equivalent to the inclusion $\text{im } e_i \subset \ker(\bar{\varepsilon}_i(f^*))$, which justifies the terminology of “localizing function”.

Proposition 2.2.10. *There exists a nonzero localizing function in $\Lambda_{\mathbb{D}}(A_1)$.*

Proof. It follows from the Riemann–Roch Theorem that

$$\lambda_{\mathbb{D}}(A_1) - \lambda_{\mathbb{D}}(A_1, \ker e^*) \leq r \cdot \dim_{\mathbb{F}}(\ker e^*) = r \cdot w_{\text{srk}}(e).$$

As $\lambda_{\mathbb{D}}(A_1) > r \cdot w_{\text{srk}}(e)$, we deduce that $\lambda_{\mathbb{D}}(A_1, \ker e^*) > 0$. We conclude by noticing that any function in $\Lambda_{\mathbb{D}^*}(A_1, \text{im}(e))$ is an error localizing function. $\square$

Proposition 2.2.11. *A function $f \in \Lambda_{\mathbb{D}^*}(A_1)$ is an error localizing function if and only if*

$$\forall h \in \Lambda_{\mathbb{D}^*}(K + \text{CoNr}(D) - A - A_1), \quad \langle \bar{\varepsilon}_D(fh), m \rangle = 0. \quad (2.2.1)$$

Proof. Let $f \in \Lambda_{\mathbb{D}^*}(A_1)$ and set $A_2 := K + \text{CoNr}(D) - A - A_1$ for simplicity. Noticing that K and $\text{CoNr}(D)$ are both Galois divisors, we conclude that A_2 is Galois too. By Lemma 2.2.6, we thus have:

$$\Lambda_{\mathbb{D}^*}(A_1) \cdot \Lambda_{\mathbb{D}^*}(A_2) \subset \Lambda_{\mathbb{D}^*}(K + \text{CoNr}(D) - A).$$

It then follows from Theorem 2.1.2 that $\langle \bar{\varepsilon}_D(fh), c \rangle = 0$ for all $h \in \Lambda_{\mathbb{D}^\star}(A_2)$. Thus

$$\langle \bar{\varepsilon}_D(fh), m \rangle = \langle \bar{\varepsilon}_D(fh), e \rangle = \sum_{i=0}^s \text{Tr}_{\mathbb{F}}(\bar{\varepsilon}_i(fh) \circ e_i^\star) = \sum_{i=0}^s \text{Tr}_{\mathbb{F}}(e_i^\star \circ \bar{\varepsilon}_i(f) \circ \bar{\varepsilon}_i(h)). \quad (2.2.2)$$

If f is a localizing function, then $e_i^\star \circ \bar{\varepsilon}_i(f) = 0$, so $\langle \bar{\varepsilon}_D(fh), m \rangle$ vanishes as well.

Conversely, let us assume that $\langle \bar{\varepsilon}_D(fh), m \rangle = 0$ for all $h \in \Lambda_{\mathbb{D}^\star}(A_2)$. We define $W_i := \text{im } e_i^\star$ and set $W := \bigoplus_{i=1}^s W_i$ accordingly. We notice that the right hand side of Equation (2.2.2) can be rewritten as $\Phi_W(e_i^\star \circ \bar{\varepsilon}_i(f), \bar{\varepsilon}_i(h)|_{W_i})$. Our assumption then reads

$$\forall h \in \Lambda_{\mathbb{D}^\star}(A_2), \quad \Phi_W(e_i^\star \circ \bar{\varepsilon}_i(f), \bar{\varepsilon}_i(h)|_{W_i}) = 0. \quad (2.2.3)$$

Observing moreover that

$$\begin{aligned} \deg(K + \text{CoNr}(D) - A - A_1, W) &= 2g - 2 + sr - \deg(A + A_1) - \dim_{\mathbb{F}} W \\ &> 2g - 2 + \rho_{\text{algo}} - w_{\text{srk}}(e) > 2g - 2 \end{aligned}$$

we can apply Theorem 2.2.3 to get the surjectivity of the map

$$\bar{\varepsilon}_{D|W} : \Lambda_{\mathbb{D}^\star}(K + \text{CoNr}(D) - A - A_1) \longrightarrow \prod_{i=1}^s \text{Hom}_{\mathbb{F}}(W_i, V_i).$$

Therefore Equation (2.2.3) shows that $e_i^\star \circ \bar{\varepsilon}_i(f)$ is orthogonal (for Φ_W) to the whole space $\prod_{i=1}^s \text{Hom}_{\mathbb{F}}(W_i, V_i)$. Thanks to Lemma 2.2.4, it then must vanish. $\square$

2.2.3 Syndrome equation

It now only remains to solve the syndrome equation restricted to the localizing space previously determined.

Proposition 2.2.12. *Let f be a nonzero localizing error and let $e' = (e'_1, \dots, e'_s) \in \prod_{i=1}^s \text{End}_{\mathbb{F}}(V_i)$ such that*

1. *for all $i \in [s]$, we have $\text{im}(e'_i) \subset \ker \bar{\varepsilon}_i(f^\star)$,*
2. *for all $h \in \Lambda_{\mathbb{D}^\star}(K + \text{CoNr}(D) - A)$, we have $\langle \bar{\varepsilon}_D(h), e' \rangle = \langle \bar{\varepsilon}_D(h), m \rangle$.*

Then $e' = e$.

Proof. From Theorem 2.1.2, we derive that the difference $e' - e$ lies in $\text{LAG}_{\mathbb{D}}(A, D)$. Besides its image lies in $\bigoplus_{i=1}^s \text{im}(e_i)$ and thus $w_{\text{srk}}(e' - e) \leq w_{\text{srk}}(e) \leq \rho_{\text{algo}}$. Since the minimum distance of $\text{LAG}_{\mathbb{D}}(A, D)$ is at least $d^*(A) > \rho_{\text{algo}}$, we conclude that $e' = e$. $\square$

Algorithm 1 summarizes our decoding algorithm.

Theorem 2.2.13. *We assume Hypothesis 2.2.1 and 2.2.7. Then, Algorithm 1 can decode any error of weight at most*

$$\rho_{\text{algo}} = \left\lfloor \frac{d^*(A) - g - 1}{2} \right\rfloor.$$

Moreover, its complexity is polynomial in s and r .

Proof. Correctness follows from Propositions 2.2.8, 2.2.10 and 2.2.11. All steps clearly have polynomial complexity in s and r , as the dimensions of both $\Lambda_{\mathbb{D}^\star}(K + \text{CoNr}(D) - A)$ and $\Lambda_{\mathbb{D}^\star}(K + \text{CoNr}(D) - A - A_1)$ are in $O(sr)$. $\square$

Algorithm 1: Decoding algorithm for linearized Algebraic Geometry codes

Input: A message m with an error of weight at most $\rho_{\text{algo}} = \left\lfloor \frac{d^*(A) - g - 1}{2} \right\rfloor$.

Output: The error e corresponding to the maximum likelihood principle.

1: Pick a divisor $A_1 \in \text{Div}(\mathbb{D}, D)$ satisfying the requirements of Lemma 2.2.8.

2: Pick a nonzero solution $f \in \Lambda_{\mathbb{D}^\star}(A_1)$ of the linear system

$$\forall h \in \Lambda_{\mathbb{D}^\star}(K + \text{CoNr}(D) - A - A_1), \quad \langle \bar{\varepsilon}_D(fh), m \rangle = 0.$$

3: Solve the linear system with $e \in \prod_{i=1}^s \text{Hom}_{\mathbb{F}}(V_i, \ker \bar{\varepsilon}_i(f^\star))$:

$$\forall h \in \Lambda_{\mathbb{D}^\star}(K + \text{CoNr}(D) - A), \quad \langle \bar{\varepsilon}_D(h), e \rangle = \langle \bar{\varepsilon}_D(h), m \rangle.$$

4: Return e .

Acknowledgments

This work was supported by ANR-21-CE39-0009-BARRACUDA and ANR-22-CPJ2-0047-01.

A SageMath implementation of the decoding algorithm

We provide some results from a SageMath implementation of our decoding algorithm. The source code is available at <https://plmlab.math.cnrs.fr/drain/lag-decoding.git>. We set a Kummer, Artin–Schreier or Artin–Schreier–Witt extension $\mathbb{L}/\mathbb{K}$ and assume the place(s) at infinity to be totally ramified in $\mathbb{L}/\mathbb{K}$. For simplicity, we also assume the evaluation places $Q_{i,j}|P_i$ to be totally split. The code $\text{LAG}_{\mathbb{D}}(A, D)$ is the image of the following morphisms up to conjugation in a basis corresponding to the fiber $(Q_{i,0}, \dots, Q_{i,r-1})$ above P_i :

$$\varepsilon'_i : \Lambda_{\mathbb{D}}(A) \rightarrow \mathbb{F}_q^{r \times r}$$

$$\lambda, T \mapsto \begin{bmatrix} \pi_{i,0}(\lambda) & 0 & \dots & 0 & 0 \\ 0 & \pi_{i,1}(\lambda) & \dots & 0 & 0 \\ 0 & 0 & \ddots & & 0 \\ \vdots & & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 0 & \pi_{i,r-1}(\lambda) \end{bmatrix}, \begin{bmatrix} 0 & 0 & \dots & 0 & \pi_{i,0}(x) \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \ddots & & 0 \\ \vdots & & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}$$

where $\pi_{i,j}$ denotes the projection $\mathcal{O}_{Q_{i,j}} \rightarrow \mathcal{O}_{Q_{i,j}}/Q_{i,j}$. These morphisms ε'_i extend to the gauge order Λ_{P_i} and are conjugated to the evaluation morphisms $\bar{\varepsilon}_i$. Indeed, we check

$$\varepsilon'_i(-) = \varepsilon_i(u_{P_i}^{-1} \cdot - \cdot u_{P_i}).$$

SageMath use case

We present hereunder a decoding test for a Kummer extension $\mathbb{L}/\mathbb{K}$ of degree 2 over another Kummer extension $\mathbb{K}/\mathbb{F}_{81}(t)$ of degree 2.

```
sage: load('LAG_decoding.sage') 1
None 2
sage: F = GF(81) 3
```

```

sage: DLx = DivisionAlgebra(F=F, rK=2, r=2, pol_K_arg=[0,2,1,1],      4
    pol_L_arg=[0,1], pol_x_arg=[F.gen(),1])
sage: LAG = LinearizedAGCode(DLx=DLx, degA=7, s_eval=7)              5
sage: LAG                                                            6
LinearizedAGCode:                                                    7
D:DivisionAlgebra:                                                  8
    K:Function field in x defined by x^2 + 2*t^3 + 2*t^2 + t,        9
    L:Function field in y defined by y^2 + 2*x,                      10
    xD:t + z4,                                                        11
    gK:1, gL:3, gD:4,                                                12
    s:31,                                                             13
degA:7,                                                              14
s_eval:7                                                             15
parameters:[14, 4, 7]                                              16
sage: omega = LAG.maximal_decodable_error_weight()                  17
sage: omega                                                         18
1                                                                     19
sage: error = LAG.random_error(omega)                               20
sage: error # RANDOM ERROR                                          21
[0 0]                                                                22
[0 0]                                                                23
[0 0]                                                                24
[0 0]                                                                25
[0 0]                                                                26
[0 0]                                                                27
[ 2*z4^3 + 2*z4 + 2 2*z4^3 + 2*z4^2 + 2]                          28
[      z4^3 + z4      2*z4^2 + 2*z4 + 2]                          29
[0 0]                                                                30
[0 0]                                                                31
[0 0]                                                                32
[0 0]                                                                33
[0 0]                                                                34
[0 0]                                                                35
sage: word = LAG.random_codeword()                                  36
sage: message = word + error                                         37
sage: message # RANDOM MESSAGE                                       38
[z4^3 + 2*z4^2 + 2*z4 + 1 2*z4^3 + 2*z4^2 + z4 + 1]              39
[      2*z4      2*z4^3 + 2]                                       40
[      z4^3 + 2*z4 + 1      z4^2 + 2]                             41
[      z4^3 + z4^2 + z4 2*z4^3 + z4^2 + 2*z4]                   42
[2*z4^3 + 2*z4^2 + z4 + 2      z4 + 1]                           43
[      z4^3 + 2*z4 + 2      2*z4^2 + 1]                           44
[      2*z4 + 1      2*z4^3 + 2*z4^2 + 1]                         45
[ 2*z4^3 + 2*z4^2 + 2*z4 z4^3 + 2*z4^2 + 2*z4 + 1]              46
[ 2*z4^2 + 2*z4 + 1      2*z4^3 + z4^2]                           47
[ 2*z4^2 + z4 + 2 2*z4^3 + 2*z4^2 + 2]                           48
[      0      2*z4^2 + 2*z4]                                       49
[2*z4^3 + 2*z4^2 + 1      2*z4 + 1]                               50
[      z4^3      z4^2 + 1]                                       51
[z4^3 + 2*z4^2 + 2*z4 + 2      z4^3 + z4^2 + z4 + 1]           52
sage: decoded_error = LAG.decode_msg(message) # DECODING ...       53
sage: decoded_error == error # CHECKING THE RESULT                 54
True                                                                55

```

	$\mathbb{F}$	$\mathbb{K}$	$\mathbb{L}$	$x_{\mathbb{D}}$	$g_{\mathbb{K}}$	$g_{\mathbb{L}}$	$g_{\mathbb{D}}$	s
$C(2)$	$\mathbb{F}_{5^2}$	$\mathbb{F}_{5^2}(t)$	$\frac{\mathbb{F}_{5^2}(t)[y]}{y^2+4t^3+4t^2+4t}$	$t+z_2$	0	1	3/2	14
$C(3)$	$\mathbb{F}_{3^3}$	$\mathbb{F}_{3^3}(t)$	$\frac{\mathbb{F}_{3^3}(t)[y]}{y^3+2y+2t^3+2t^2+2t}$	$t+z_3$	0	1	2	9
$C(4)$	$\mathbb{F}_{5^2}$	$\mathbb{F}_{5^2}(t)$	$\frac{\mathbb{F}_{5^2}(t)[y]}{y^4+4t^3+4t^2+4t}$	$t+z_2$	0	3	9/2	7
$C(5)$	$\mathbb{F}_{5^2}$	$\mathbb{F}_{5^2}(t)$	$\frac{\mathbb{F}_{5^2}(t)[y]}{y^5+4y+4t^3+4t^2+4t}$	$t+z_2$	0	4	6	7
$C(8)$	$\mathbb{F}_{7^2}$	$\mathbb{F}_{7^2}(t)$	$\frac{\mathbb{F}_{7^2}(t)[y]}{y^8+6t^3+6t^2+6t}$	$t+z_2$	0	7	21/2	6
$C(2,2)$	$\mathbb{F}_{3^4}$	$\frac{\mathbb{F}_{3^4}(t)[x]}{x^2+2t^3+2t^2+t}$	$\frac{\mathbb{K}(x)[y]}{y^2+2x}$	$t+z_4$	1	3	4	15

Figure 1: Description of the tested codes, where z_n denotes a generator of $\mathbb{F}_{p^n}^\times$.

	ω	$\deg A$	time	ω	$\deg A$	time	ω	$\deg A$	time
$C(2)$	1	23	1.985	6	12	2.978	11	2	4.003
$C(3)$	1	22	4.697	6	12	5.996	10	3	7.756
$C(4)$	1	20	7.023	4	14	7.682	7	8	8.793
$C(5)$	1	26	21.415	5	18	23.994	8	11	27.936
$C(8)$	1	34	142.395	4	27	153.397	8	20	164.652
$C(2,2)$	1	23	15.738	15	15	23.138	9	7	30.225

Figure 2: CPU Timings in seconds for constructing a code.

SageMath benchmark

We tested the decoding of linearized AG codes on different Kummer and Artin–Schreier–Witt extensions. A benchmark is reported on Figure 2 (resp. Figure 3) for the initial computation of Riemann–Roch spaces (resp. iterative message decoding corresponding to codes described in Figure 1). The computations were run on a computer with AMD Ryzen 7 PRO 8840U (3,30 GHz up to 5,10 GHz) Processor and 16 Go DDR5-5 600MT/s (SODIMM).

References

- [BC24] E. Berardini and X. Caruso. Algebraic geometry codes in the sum-rank metric. *IEEE Transactions on Information Theory*, 70(5):3345–3356, May 2024.
- [BC25] E. Berardini and X. Caruso. Reed–Muller codes in the sum-rank metric. *Journal of Algebra and Its Applications*, April 2025.
- [CD23] X. Caruso and A. Durand. Duals of linearized Reed–Solomon codes. *Designs, Codes and Cryptography*, 91(1):241–271, 2023.
- [Mat61] HF Mattson. A generalization of the Riemann–Roch theorem. *Illinois Journal of Mathematics*, 5(3):355–375, 1961.
- [MP18a] Umberto Martínez-Peñas. Skew and linearized Reed–Solomon codes and maximum sum rank distance codes over any division ring. *J. Algebra*, 504:587–612, 2018.
- [MP18b] U. Martínez-Peñas. Skew and linearized Reed–Solomon codes and maximum sum rank distance codes over any division ring, 2018.

	ω	$\deg A$	time	ω	$\deg A$	time	ω	$\deg A$	time
$C(2)$	1	23	0.009	6	12	0.026	11	2	0.052
$C(3)$	1	22	0.016	6	12	0.045	10	3	0.094
$C(4)$	1	20	0.032	4	14	0.065	7	8	0.137
$C(5)$	1	26	0.093	5	18	0.236	8	11	0.440
$C(8)$	1	34	1.386	4	27	2.394	8	20	4.741
$C(2, 2)$	1	23	0.016	5	15	0.028	9	7	0.047

Figure 3: CPU Timings in seconds for decoding a single random message in a code.

- [MPK19] Umberto Martínez-Peñas and Frank R. Kschischang. Reliable and secure multishot network coding using linearized Reed–Solomon codes. *IEEE Transactions on Information Theory*, 65(8):4785–4803, 2019.
- [MPSK22] Umberto Martínez-Peñas, Mohannad Shehadeh, and Frank R. Kschischang. Codes in the sum-rank metric: fundamentals and applications. *Foundations and Trends in Communications and Information Theory*, 19(5):814–1031, 2022.
- [Ore33] O. Ore. Theory of non-commutative polynomials. *Annals of Mathematics*, 34(3):480–508, 1933.
- [Rei75] I. Reiner. *Maximal Orders*. Institute for Research on Poverty Monograph Series. Academic Press, 1975.
- [Sha13] Igor R Shafarevich. *Basic algebraic geometry; 3rd ed.* Springer, Berlin, 2013.
- [Sti93] H. Stichtenoth. *Algebraic function fields and codes*. Universitext (Berlin. Print). Springer-Verlag, 1993.
- [Tam51] T. Tamagawa. On the theorem of Riemann-Roch. *J. Fac. Sci., Univ. Tokyo, Sect. I*, 6:133–144, 1951.
- [Wit34] E. Witt. *Riemann-Roch-Satz und Zeta-Funktion im hyperkomplexen*. Dissertation, University of Göttingen, 1934. Thesis directed by Emmy Noether.