Duals of linearized Reed-Solomon codes

Xavier Caruso, Amaury Durand

Duals of linearized Reed-Solomon codes

Xavier Caruso & Amaury Durand

October 2021

Abstract

We give a description of the duals of linearized Reed-Solomon codes in terms of codes obtained by taking residues of Ore rational functions. Our construction shows in particular that, under some assumptions on the base field, the class of linearized Reed-Solomon codes is stable under duality. As a byproduct of our work, we develop a theory of residues in the Ore setting, extending the results of [7].

Contents

Introduction

One of the oldest and most basic construction of codes is due to Reed and Solomon and consists in evaluating polynomials of small degree in a large number of points; due to the decalage between the degree and the number of evaluation points, one can hope recovering the initial polynomial even when some errors occur during the evaluation, or the transmission of the values. During the last decades, new problems in coding theory have emerged and new solutions have been proposed. In particular, one realizes than the rank metric (for which the distance between two codewords is given by the rank of some matrix) is more well-suited than the classical Hamming metric for some applications, *e.g.* network coding [24] or space-time coding [17, 2]. The rank metric has then gained more and more popularity over the years and many classical constructions have been extended to this framework.

In particular, Delsarte [9], Roth [23] and Gabidulin [10] (independently) noticed that replacing classical polynomials with linearized polynomials in Reed-Solomon's construction, one ends up with quite interesting codes as well. Those codes are nowadays referred to as Gabidulin codes. They appear naturally as linear subspaces of matrix algebras, hence the connexion of the rank metric.

After the work of Boucher and Ulmer [4], we prefer nowadays working with Ore polynomials in place of linearized polynomials; this indeed allows us to extend Gabidulin codes to arbitrary base fields, including in particular number fields [2] and, to some extent, to put the theory of Gabidulin codes in the perspective of differential algebras [5, 16].

More recently, Martínez-Peñas [18] managed to find a common generalization of Reed-Solomon codes, on the one hand, and Gabidulin codes, on the other hand. Martínez-Peñas' codes are called *linearized Reed-Solomon codes* are involves the so-called sum-rank metric. Moreover, Martínez-Peñas gives applications to his codes to multishot network coding in [20]. Since then, sum-rank metric codes have received some interest (see for example [20, 22, 6, 21]). In particular, the notion of duality for sum-rank metric codes have been addressed in [19] in which the authors proved that the duals of certain linearized Reed-Solomon remains of the same type (see [19, Theorem 4]).

The aim of the present paper is to study in a wider generality the duals of linearized Reed-Solomon codes. More precisely, we will consider linearized Reed-Solomon codes obtained from rings of Ore polynomials $K[X;\theta,\delta]$ satisfying the two following assumptions:

- **(H1)**: the base ring K is a *commutative* field,
- **(H2)**: the subfield F of K consisting of elements $x \in K$ such that $\theta(x) = x$ and $\delta(x) = 0$ has finite index in K.

These two assumptions do not allow us to work in the full generality of Martínez-Peñas' original paper but it turns out that they are sufficiently weak to cover the most interesting situations. For example, they are fulfilled when K is a finite field and θ is (a power of) the Frobenius endomorphism or when K is the field of rational functions in the variable t over a finite field and δ is the usual derivation $\frac{d}{dt}$.

In order to achieve our goal, we draw our inspiration from the classical case; indeed, it is a standard fact in the theory of algebraic geometry codes (see for instance [25, §4.1.2]) that the duals of standard Reed-Solomon codes can be described in terms of taking residues of differential forms over $\mathbb{P}^1$. In this paper, we extend this view point to Ore polynomials and linearized Reed-Solomon codes.

For this, several important ingredients are needed. The first one is a powerful theory of residues in the Ore setting. Such a theory has been already partially developed in a former paper of one of us [7]. Building on this work, we extend the theory to the general setting of this article and use it to give a new construction of codes for the sum-rank distance, that we call *linearized Goppa codes*. It turns out that these codes are (noncanonically) isomorphic to linearized Reed-Solomon codes; however having this alternative presentation in terms of residues will be of crucial importance.

Two other ingredients we shall need is a notion of trace and a notion of duality at the level of Ore rings. The former will be given by the so-called *reduced trace*, which is a somehow standard tool in this context (see for instance [13, §1.6]); however, we shall use a slightly unusual approach in this paper inspired by the theory of Azumaya algebras and better-suited to the applications we have in mind. As for duality maps, we introduce them in the present paper. We furthermore prove that the trace and the duality both satisfy nice commutation relations with evaluation morphisms and residue maps. Putting

all these inputs together, we finally prove that our linearized Goppa codes are the duals of Martínez-Peñas' linearized Reed-Solomon codes. As a corollary, we derive the following theorem that extends the theorem of Martínez-Peñas and Kschischang [19, Theorem 4] we have mentioned earlier.

Theorem 1. *Under the assumptions **(H1)** and **(H2)**, the dual of a linearized Reed-Solomon code is isomorphic to a linearized Reed-Solomon code.*

The article is organized as follows. In Section 1, we introduce linearized Reed-Solomon codes; we basically follow Martínez-Peñas' treatment but reformulate it in a slightly different language which will help us afterwards to carry out our constructions. In Section 2, we introduce the reduced trace maps, we show that they commute with evaluation morphisms and give entirely explicit formulas for them. Section 3 is devoted to the theory of residues: we define them and prove a noncommutative analogue of the residue formula. Duality questions are discussed in Section 4: we define a duality on Ore rings and establish useful commutation results with evaluation morphisms and residue maps. Finally, the construction of linearized Goppa codes and the duality theorem is addressed in Section 5.

1 From Ore polynomials to codes

The aim of this section is to recall Martínez-Peñas' construction of linearized Reed-Solomon codes [18]. Actually, our presentation differs slightly from that of *loc. cit.* in that it takes place in a more restricted setting which allows us to use more powerful arguments in some places and to adopt a more conceptual view (avoiding for instance the use of P-basis). This perspective on linearized Reed-Solomon codes will be quite useful for later developments we shall achieve in this article. For this reason, we have chosen to do a complete exposition of the theory and, in particular, include full detailed proofs.

Throughout this article, we consider a field K equipped with a ring homomorphism $\theta : K \to K$ and a θ-derivation $\delta : K \to K$, that is, by definition, an additive mapping such that $\delta(ab) = \theta(a)\delta(b) + \delta(a)b$ for all $a, b \in K$.

We denote by F the subfield of K consisting of elements $a \in K$ such that $\theta(a) = a$ and $\delta(a) = 0$. *We will always assume that the extension K/F is finite.* This hypothesis implies in particular that θ has finite order and hence is bijective.

1.1 Ore polynomials

Definition 1.1. The *ring of Ore polynomials* $K[X; \theta, \delta]$ is the ring whose elements are polynomials in X over K endowed with the usual addition and the multiplication defined by the rule:

$$Xa = \theta(a)X + \delta(a), \ \forall a \in K$$

When $\theta = \mathrm{id}_K$ and $\delta = 0$, the ring $K[X; \theta, \delta]$ is nothing but the ring of usual univariate polynomials in X. In what follows, in order to avoid this trivial cornercase, we shall always suppose that $(\theta, \delta) \neq (\mathrm{id}_K, 0)$. This additional assumption ensures in particular that F is a *strict* subfield of K.

Although $K[X;\theta,\delta]$ is noncommutative, it shares many properties with the ring of usual polynomials. First of all, we notice that the notion of degree extends *verbatim* to Ore polynomials: if $P = \sum_i a_i X^i \in K[X;\theta,\delta]$, its degree is the largest integer i for which $a_i \neq 0$. Besides, $K[X;\theta,\delta]$ is endowed with a right (resp. left[1]) Euclidean division: if $A, B \in K[X;\theta,\delta]$ with $B \neq 0$, there exist unique $Q, R \in K[X;\theta,\delta]$ such that $A = QB + R$ (resp. $A = BQ + R$) and $\deg R < \deg B$. This result has the usual consequences: the noncommutative ring $K[X;\theta,\delta]$ is left- and right-principal, it admits GCDs and LCMs (on the left and on the right) and those can be computed using a noncommutative version of the Euclidean algorithm. In what follows, we will denote by $A\%B$ the remainder in the right division of A by B.

Hilbert twist

An important tool in the study of Ore polynomials is that of *Hilbert twist*; this is an affine change of variables which has the effect of modifying the derivation. Set $\delta_0 = \theta - \mathrm{id}_K$; one checks that it is a θ-derivation and, consequently, that $\delta + a\delta_0$ is also a θ-derivation for all $a \in K$.

Proposition 1.2. *For any $a \in K$, the mapping:*

$$K[X;\theta,\delta] \xrightarrow{\sim} K[X;\theta,\delta+a\delta_0], \quad X \mapsto X + a$$

is an isomorphism of rings.

Proof. It suffices to check that $(X+a)b = \theta(b)(X+a) + \delta(b)$ holds in the Ore ring $K[X;\theta,\delta+a\delta_0]$ for all $b \in K$, which is a simple calculation. □

In addition, when θ is not the identity, one can classify the θ-derivations of K.

Proposition 1.3. *If $\theta \neq \mathrm{id}_K$, all θ-derivations of K are of the form $a\delta_0$ with $a \in K$.*

Proof. Let $x_0 \in K$ with $\theta(x_0) \neq x_0$, *i.e.* $\delta_0(x_0) \neq 0$. Given a θ-derivation δ and $x \in K$, we write:

$$\delta(x_0 x) = \theta(x_0)\delta(x) + \delta(x_0)x = \theta(x)\delta(x_0) + \delta(x)x_0$$

for what we deduce that $\delta(x) = \frac{\delta(x_0)}{\delta_0(x_0)}\delta_0(x)$ and finally that δ is proportionnal to δ_0. □

Combining Propositions 1.2 and 1.3, we find that the Ore polynomial ring $K[X;\theta,\delta]$ is isomorphic to $K[X;\theta,0]$ as soon as θ is not the identity. Therefore, one can split the study of Ore polynomials over fields into two cases: the "endomorphic" one where $\delta = 0$ and the "differential" one where $\theta = \mathrm{id}_K$.

The centre

Recall that the centre of a noncommutative ring A is by definition the subset of A consisting of elements x such that $xy = yx$ for all $y \in A$; in particular, the centre is always commutative.

[1] For the left division, we use that θ is bijective.

It turns out that the centre of Ore polynomial rings plays a quite important role and can be explicitely determined. Precisely, when $\delta = 0$, one checks that the centre of $K[X;\theta,0]$ is $F[X^s]$ where s is the order of θ (and we recall that F is by definition the subfield of K fixed by θ). The case where $\theta \neq \mathrm{id}_K$ reduces to the previous one using Hilbert twist; indeed, from Proposition 1.3, we know that $\delta = a\delta_0$ for some $a \in K$ and it then follows from Proposition 1.2 that the centre of $K[X;\theta,\delta]$ is $F[(X+a)^s]$ where, again, s denotes the order of θ.

The case where $\theta = \mathrm{id}_K$ is, by far, the more difficult one. By chance, it has already been studied in details in [1]. Recall that, in this case, F is defined as the subfield of constants of K. Let $Z(X) \in K[X]$ be the monic polynomial of minimal degree annihilating δ (which exists because all the δ^i are F-linear mappings of K, which is finite dimensional over F). The centre of $K[X;\mathrm{id}_K,\delta]$ is then the subring $F[Z(X)]$. Besides, it is proved in *loc. cit.* that $Z(X)$ is a monic linearized polynomial with coefficients in F, *i.e.* it takes the form:

$$Z(X) = X^{p^r} + z_{r-1}X^{p^{r-1}} + \cdots + z_1X^p + z_0X \quad (z_i \in F) \tag{1}$$

and its degree p^r is the degree of the extension K/F.

To summarize, the following proposition holds in all cases.

Proposition 1.4. *There exists a monic Ore polynomial $Z(X) \in K[X;\theta,\delta]$ such that the centre of $K[X;\theta,\delta]$ is $F[Z(X)]$. Moreover* $\deg Z(X) = [K : F]$.

Remark 1.5. The equality $\sum_{i=0}^{d} a_i Z(X)^i = \sum_{i=0}^{e} b_i Z(X)^i$ readily implies that $d = e$ and $a_i = b_i$ for all i. As a consequence, the centre $F[Z(X)]$ is an actual polynomial ring in one variable with coefficients in F.

Remark 1.6. The condition of Proposition 1.4 only determines $Z(X)$ uniquely but only up to an additive constant in F. However, one can always normalize it by requiring it to be a linearized polynomial when $\theta = \mathrm{id}_K$, or a power of a Ore polynomial of degree 1 otherwise.

1.2 On the evaluation of Ore polynomials

Evaluating Ore polynomials is not straightforward; indeed performing the substitution $X \mapsto c$ for some $c \in K$ does not define a ring homomorphism and hence is not relevant. An option which is often considered (see for instance [14]) is to define $P(c)$ as the remainder in the division of P by $X-c$. However, in this article, we will follow a different path based on the notion of pseudo-linear morphism which was first introduced by Jacobson in [12] and then further developed by Leroy in [15].

1.2.1 Definition of evaluation maps

We start by recalling Jacobson's definition of pseudo-linear morphisms.

Definition 1.7. Let M be a vector space over K. A *pseudo-linear endomorphism* $u : M \to M$ (with respect to θ and δ) is an additive map verifying:

$$u(ax) = \theta(a)u(x) + \delta(a)x$$

for all $a \in K$ and $x \in M$.

We observe that any pseudo-linear morphism is *a fortiori* F-linear. If $u : M \to M$ is a pseudo-linear morphism and $P = \sum_i a_i X^i \in K[X;\theta,\delta]$ is a Ore polynomial, we define $P(u) = \sum_i a_i u^i$. A simple computation then shows that $P(u) \circ Q(u) = (PQ)(u)$ for all $P, Q \in K[X;\theta,\delta]$. In other words, the mapping:

$$\mathrm{ev}_u : K[X;\theta,\delta] \longrightarrow \mathrm{End}_F(M), \quad P(X) \mapsto P(u)$$

is a ring homomorphism (where $\mathrm{End}_F(M)$ denotes the ring of F-linear endomorphisms of M). The case where M is K itself deserves particular attention. Indeed, we first observe that evaluation is then closely related to Euclidean division thanks to the formula:

$$\mathrm{ev}_u(P)(a) = (aP) \,\%\, \left(X - \tfrac{u(a)}{a}\right) \tag{2}$$

which is correct for any pseudo-linear endomorphism u of K, any $P \in K[X;\theta,\delta]$ and any $a \in K$, $a \neq 0$ (see also [15, Theorem 2.8]). Second, we have a complete classification of pseudo-linear endomorphisms of K.

Proposition 1.8. *The pseudo-linear endomorphisms of K are exactly the maps of the form $\delta + c\theta$ with $c \in K$.*

Proof. It is straightforward to check that $\delta + c\theta$ is a pseudo-linear morphism for any $c \in K$. Conversely, let $u : K \to K$ be a pseudo-linear endomorphism. For $x \in K$, it follows from the definition that $u(x) = \theta(x)u(1) + \delta(x)$. Therefore $u = \delta + c\theta$ with $c = u(1)$. □

In what follows, we will often use the notation ev_c in place of $\mathrm{ev}_{\delta+c\theta}$. We notice that those evaluation maps are compatible with Hilbert twists in the sense that the diagram below commutes for all $a, c \in K$:

$$\begin{array}{ccc} K[X;\theta,\delta] & \xrightarrow{X \mapsto X+a} & K[X;\theta,\delta+a\delta_0] \\ \Big\downarrow{\scriptstyle \mathrm{ev}_c} & & \Big\downarrow{\scriptstyle \mathrm{ev}_{c-a}} \\ \mathrm{End}_F(K) & = & \mathrm{End}_F(K) \end{array}$$

1.2.2 The kernel of the evaluation maps

We recall from Proposition 1.4 that the centre of $K[X;\theta,\delta]$ is of the form $F[Z(X)]$ and that the Ore polynomial $Z(X)$ can be normalized using the additional conditions of Remark 1.6. For $c \in K$, we define $\upsilon(c)$ as the remainder of the right Euclidean division of $Z(X)$ by $X-c$; by definition, $Z(X)-\upsilon(c)$ is then a right multiple of $X-c$.

Definition 1.9. We say that an element $c \in K$ is *ramified* (with respect to θ and δ) if $\delta+c\theta$ is a scalar multiple of id_K. Otherwise, we say that c is *unramified*.

One checks that K contains at most one ramified element. Precisely, when $\theta = \mathrm{id}_K$ (and $\delta \neq 0$), all elements of K are unramified while, when $\theta \neq \mathrm{id}_K$ and $\delta = a\delta_0$, the unique ramified element of K is $-a$.

Proposition 1.10. *Let c be an unramified element of K. Then $\mathrm{ev}_c : K[X;\theta,\delta] \to \mathrm{End}_F(K)$ is surjective and its kernel is the principal left ideal generated by $Z(X) - \upsilon(c)$.*

Proof. Let us first assume that $\delta = 0$ and let n be the order of θ. Then $Z(X) = X^n$ and $n = [K : F]$. Moreover, by Artin's linear independence theorem, we know that the family $(\mathrm{id}_K, \theta, \dots, \theta^{n-1})$ is K-free in $\mathrm{End}_F(K)$. By comparing dimensions, it is then enough to prove that ev_c vanishes on $X^n - \upsilon(c)$. Write $\varphi = \mathrm{ev}_c\big(X^n - \upsilon(c)\big) = (c\theta)^n - \upsilon(c)\,\mathrm{id}_K$. On the one hand, a direct computation using that $\theta^n = \mathrm{id}_K$ indicates that φ must be a multiple of id_K. On the other hand, the fact that $X^n - \upsilon(c)$ is a right multiple of $X - c$ implies that φ vanishes at 1. Putting these two inputs together, we deduce that φ vanishes, as wanted. The case where $\theta \neq \mathrm{id}_K$ reduces to the previous one using a well-chosen Hilbert twist (see Propositions 1.2 and 1.3).

Finally, we suppose that $\theta = \mathrm{id}_K$. Recall that $Z(X)$ is defined in this case as the minimal polynomial of δ and that it is linearized polynomial with coefficients in F. Observe now that

$$Z(X-c) = Z(X) - \upsilon(c). \tag{3}$$

Indeed, it follows from Proposition 1.2 that the mapping $X \mapsto X-c$ induces an automorphism of $K[X; \mathrm{id}_K, \delta]$, implying that $Z(X-c)$ has to be central and hence of the form $Z(X) - a$ for some $a \in F$. Taking remainders modulo $X-c$, we finally find $a = \upsilon(c)$.

It follows from Eq. (3) that $Z(X) - \upsilon(c)$ lies in the kernel of ev_c. Moreover, the fact that $Z(X)$ is the minimal polynomial of δ says that the family $(\delta^i)_{0 \leq i < p^r}$ is linearly independent over K. Hence the family $((\delta + c\cdot\mathrm{id}_K)^i)_{0 \leq i < p^r}$ is also, implying eventually that the kernel of ev_c is exactly the ideal generated by $Z(X) - \upsilon(c)$. The surjectivity of ev_c follows by comparing dimensions over F (and using that $\deg Z(X) = [K : F]$). □

An interesting (and unexpected) corollary of Proposition 1.10 is the following.

Corollary 1.11. *For all $c \in K$, we have $\upsilon(c) \in F$.*

Proof. To simplify notations, we write $a = \upsilon(c)$. From Proposition 1.10, we derive that the left principal ideal generated by $Z(X)-a$ is actually two-sided because it appears as the kernel of a ring homomorphism. In particular, it contains the commutator of $Z(X)-a$ and X, which is $(\theta(a)-a)X + \delta(a)$. Therefore the latter Ore polynomial is right-divisible by $Z(X)-a$ and so, by comparing degrees, it must vanish. Hence $\theta(a) = a$ and $\delta(a) = 0$, which exactly means that $a \in F$. □

Beyond Corollary 1.11, it is possible to write down explicit formulas for $\upsilon(c)$. Concretely, when $\delta = 0$, it is easy to check that the $\upsilon = N_{K/F}$, the norm of K over F. As usual, the case where $\delta = a\delta_0$ reduces to the previous one using Hilbert twist; in this setting, we find $\upsilon(c) = N_{K/F}(a+c)$. Finally, when $\theta = \mathrm{id}_K$, it follows from the computations of [11, No 12] (see in particular Eq. (35)) that

$$\upsilon(c) = \sum_{i=0}^{r} \sum_{j=0}^{i} \Big(z_i \delta^{p^j - 1}(c)\Big)^{p^{i-j}} \tag{4}$$

where the z_i's are the coefficients of $Z(X)$ as in Eq. (1). These explicit descriptions provide an alternative proof of Corollary 1.11.

1.2.3 Zeros of Ore polynomials

In the standard commutative case, it is well known that the number of roots of a polynomial cannot exceed its degree. In the Ore setting, analoguous bounds exist.

Proposition 1.12. *Let c be an unramified element of K and let $P \in K[X;\theta,\delta]$ be a nonzero polynomial. We have*

$$\dim_F \ker(\mathrm{ev}_c(P)) \leq \deg P$$

and equality holds if and only if P divides $Z(X) - \upsilon(c)$.

Proof. Let I be the left ideal of $\mathrm{End}_F(K)$ consisting of linear morphisms vanishing on $\ker(\mathrm{ev}_c(P))$. The inverse image of I by ev_c is an ideal of $K[X;\theta,\delta]$. Since $K[X;\theta,\delta]$ is principal, there exists $Q \in K[X;\theta,\delta]$ such that $\mathrm{ev}_c^{-1}(I) = K[X;\theta,\delta]Q$. We have the following equalities of dimensions:

$$\begin{aligned} r \cdot \deg Q &= \dim_F K[X;\theta,\delta]/K[X;\theta,\delta]Q \\ &= \dim_F K[X;\theta,\delta]/\mathrm{ev}_c^{-1}(I) \\ &= \dim_F \mathrm{End}_F(K)/I \\ &= r \cdot \dim_F \ker(\mathrm{ev}_c(P)). \end{aligned}$$

We deduce that $\deg Q = \dim_F \ker(\mathrm{ev}_c(P))$. Since P obviously belongs to $\mathrm{ev}_c^{-1}(I)$, we conclude that P divides Q, showing the inequality of the proposition.

Moreover, equality holds if and only if $\deg P = \deg Q$, *i.e.* P divides Q. If P indeed divides Q, we conclude that P divides $Z(X) - \upsilon(c)$ because Q is a divisor of $Z(X) - \upsilon(c)$ thanks to Proposition 1.10. Conversely, if P divides $Z(X) - \upsilon(c)$, we write $Z(X) - \upsilon(c) = PP'$ and, applying the inequality to P and P', we get:

$$\dim_F \ker(\mathrm{ev}_c(P)) + \dim_F \ker(\mathrm{ev}_c(P')) \leq \deg P + \deg P' = r.$$

On the other hand, we have:

$$r = \dim_F \ker(\mathrm{ev}_c(PP')) \leq \dim_F \ker(\mathrm{ev}_c(P)) + \dim_F \ker(\mathrm{ev}_c(P')).$$

All inequalities then need to be equalities, which concludes the proof. □

Corollary 1.13. *Let c be an unramified element of K. Given a F-linear subspace V of K, there exists a unique monic polynomial $P \in K[X;\theta,\delta]$ such that $\ker(\mathrm{ev}_c(P)) = V$ and $\deg P = \dim_F V$.*

Proof. It suffices to take the Ore polynomial P defined by $\mathrm{ev}_c^{-1}(I) = K[X;\theta,\delta]P$ where I denotes the ideal of $\mathrm{End}_F(K)$ consisting of functions vanishing on V. □

We can extend the above results to multiple evaluations.

Theorem 1.14. *Let $c_1, \ldots, c_m$ be unramified elements of K such that the $\upsilon(c_i)'s$ are pairwise distinct.*

1. *For all $P \in K[X;\theta,\delta]$, $P \neq 0$:*

$$\sum_{i=1}^{m} \dim_F \ker(\mathrm{ev}_{c_i}(P)) \leq \deg P$$

and equality holds if and only if P divides $\prod_{i=1}^{m} Z(X) - \upsilon(c_i)$.

2. *Given F-linear subspaces $V_1, \dots, V_m$ of K, there exists a unique monic polynomial $P \in K[X;\theta,\delta]$ of degree $\sum_{i=1}^m \dim_F V_i$ such that $\mathrm{ev}_{c_i}(P)$ vanishes on V_i.*

Proof. We consider the ring homomorphism:

$$\varepsilon : K[X;\theta,\delta] \to \mathrm{End}_F(K)^m, \quad P \mapsto \big(\mathrm{ev}_{c_1}(P), \dots, \mathrm{ev}_{c_m}(P)\big).$$

Let $P \in \ker \varepsilon$. By Proposition 1.10, P is a multiple of $Z(X) - \upsilon(c_i)$ for all i . Since these polynomials are pairwise coprime, we deduce that P is divisible by $\prod_{i=1}^m Z(X) - \upsilon(c_i)$. By comparing dimensions, we find that ε is surjective and its kernel is the principal ideal generated by $\prod_{i=1}^m Z(X) - \upsilon(c_i)$. With this imput, the proof is similar to the proofs of Proposition 1.12 and Corollary 1.13. □

1.3 Linearised Reed-Solomon codes

We fix a positive integer m together with a tuple $\underline{V} = (V_1, \dots, V_m)$ of F-linear subspaces of K. We set:

$$\mathrm{Hom}_F(\underline{V}, K) = \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K).$$

It is a vector space over K of dimension $\sum_{i=1}^m \dim_F V_i$. Following [18, Definition 25], we equip $\mathrm{Hom}_F(\underline{V}, K)$ with the sum-rank distance defined as follows.

Definition 1.15. The *sum-rank weight* of $\underline{\varphi} = \big(\varphi_1, \dots, \varphi_m\big) \in \mathrm{Hom}_F(\underline{V}, K)$ is:

$$w_{\text{s-rk}}(\underline{\varphi}) = \sum_{i=1}^m \dim_F \varphi_i(V_i)$$

The *sum-rank distance* between $\underline{\varphi}$ and $\underline{\psi}$ is $d_{\text{s-rk}}(\underline{\varphi}, \underline{\psi}) = w_{\text{s-rk}}(\underline{\varphi} - \underline{\psi})$.

Throughout this article, we will use the word *code* to refer to a K-linear subspace of $\mathrm{Hom}_F(\underline{V}, K)$. By definition, the *length* of a code C sitting in $\mathrm{Hom}_F(\underline{V}, K)$ is $\sum_{i=1}^m \dim_F V_i$, its *dimension* is $\dim_K C$ and its *minimal distance* is the minimal sum-rank weight of a nonzero element of C.

These three parameters are related by an analogue of the classical Singleton bound, which reads $k + d \leq n + 1$ in our setting (see [18, Proposition 34]). Codes attaining this bound are called MSRD (for *Maximal Sum-Rank Distance*).

Definition 1.16. Let k be an integer and $\underline{c} = (c_1, \dots, c_m)$ be a tuple of unramified elements of K. We set:

$$\begin{aligned} \mathrm{ev}_{\underline{c},\underline{V}} : K[X;\theta,\delta] &\to \mathrm{Hom}_F(\underline{V}, K) \\ P &\mapsto \big(\mathrm{ev}_{c_1}(P)_{|V_1}, \dots, \mathrm{ev}_{c_m}(P)_{|V_m}\big). \end{aligned}$$

The *linearised Reed-Solomon code* associated to $(k, \underline{c}, \underline{V})$ is:

$$\mathrm{LRS}(k, \underline{c}, \underline{V}) = \mathrm{ev}_{\underline{c},\underline{V}}\big(K[X;\theta,\delta]_{<k}\big)$$

where, by definition, $K[X;\theta,\delta]_{<k}$ denotes the subset of $K[X;\theta,\delta]$ of Ore polynomial of degree strictly less than k.

Remark 1.17. The linearized Reed-Solomon codes appear as a common generalization of Reed-Solomon codes on the one hand and Gabidulin codes on the other hand. Indeed, if we had been working with classical polynomials instead of Ore polynomials, we would have end up with a usual Reed-Solomon code, while the case $m = 1$ reduces to Gabidulin codes.

The following theorem gives the parameters of the linearized Reed-Solomon codes.

Theorem 1.18. *Let k be an integer, $\underline{c} = (c_1, \dots, c_m)$ be a tuple of unramified elements of K and $\underline{V} = (V_1, \dots, V_m)$ be a tuple of F-linear subspaces of K. We set $n = \sum_{i=1}^{m} \dim_F V_i$.*

If $k \leq n$ and the $v(c_i)$'s are pairwise distinct, the code $\mathrm{LRS}(k, \underline{c}, \underline{V})$ has length n, dimension k and minimal distance $n-k+1$; in particular, it is MSRD.

Proof. The fact that $\mathrm{LRS}(k, \underline{c}, \underline{V})$ has length n is obvious. Let $P \in K[X; \theta, \delta]$ be a Ore polynomial of degree strictly less than k. For $i \in \{1, \dots, m\}$, set $f_i = \mathrm{ev}_{c_i}(P)$ and let $\varphi_i : V_i \to K$ be the restriction of f_i to V_i. From Theorem 1.14, we derive:

$$\sum_{i=1}^{m} \dim_F \ker \varphi_i \leq \sum_{i=1}^{m} \dim_F \ker f_i \leq \deg P < k$$

the first inequality coming from the obvious inclusion $\ker \varphi_i \subset \ker f_i$. By the rank-nullity theorem, we conclude that $w_{\text{s-rk}}(\varphi_1, \dots, \varphi_m) > n - k$, which concludes the proof. □

2 Reduced trace of Ore polynomials

The aim of this section is to introduce and prove the main properties of the reduced trace map over the rings of Ore polynomials. This notion can be seen as an analogue of the usual trace over ring of matrices and, for this reason, it will play a central role when we will study duality in §4.

We keep the notations and hypothesis of §1: the letter K denotes a field equipped with an automorphism $\theta : K \to K$ and a θ-derivation $\delta : K \to K$. We let F be the subfield of K consisting of elements x such that $\theta(x) = x$ and $\delta(x) = 0$ and assume that the extension K/F is finite.

In order to simplify notations, we set $\mathcal{A}^+ = K[X; \theta, \delta]$ and let $\mathcal{Z}^+$ be its centre. By Proposition 1.4, we know that $\mathcal{Z}^+ = F[Z(X)]$ for some Ore polynomial $Z(X) \in \mathcal{A}^+$ of degree $s = [K : F]$. Moreover, $Z(X)$ can be chosen in a canonical way (see Remark 1.6). We set in addition $\mathcal{C}^+ = K[Z(X)]$; it is a commutative subring of $\mathcal{A}^+$ containing $\mathcal{Z}^+$. Besides, $\mathcal{A}^+$ appreas as a free left-module of rank s over $\mathcal{C}^+$, a basis of it being given by $(1, X, \dots, X^{s-1})$. We will refer to it as the canonical basis of $\mathcal{A}^+$ over $\mathcal{C}^+$.

Definition 2.1. Let $f \in \mathcal{A}^+$. The *reduced trace* of f, denoted by $T_{\mathrm{rd}}(f)$, is the trace of the map $x \mapsto xf$ viewed as a $\mathcal{C}^+$-linear endomorphism of $\mathcal{A}^+$.

This construction defines a mapping $T_{\mathrm{rd}} : \mathcal{A}^+ \to \mathcal{C}^+$. The reader should pay attention to the fact that T_{rd} is *not* $\mathcal{C}^+$-linear because of noncommutativity; it is however $\mathcal{Z}^+$-linear. Besides, it satisfies the classical trace relation $T_{\mathrm{rd}}(fg) = T_{\mathrm{rd}}(gf)$ for all $f, g \in \mathcal{A}^+$. Another remarkable property of T_{rd} is that it assumes values in $\mathcal{Z}^+$; this result is not obvious from Definition 2.1 but is a consequence of the explicit formulas we will obtain in §2.1 (see Propositions 2.2 and 2.3).

2.1 An explicit formula

Although Definition 2.1 is already rather explicit, it is possible to simplify it further and end up with simple close expressions for the reduced trace. The objective of this subsection is to derive such formulas. Our first theorem in this direction addresses the case $\delta = 0$, which is the simplest one. In this situation, we recall that F is the fixed subfield of θ and $Z(X) = X^s$. The integer s is exactly the order of θ.

Proposition 2.2. *We assume that $\delta = 0$. For $f = \sum_i a_i X^i \in \mathcal{A}^+$, we have:*

$$T_{\mathrm{rd}}(f) = \sum_i \mathrm{Tr}_{K/F}(a_{si}) X^{si} = \sum_i \mathrm{Tr}_{K/F}(a_{si}) Z(X)^i$$

where $\mathrm{Tr}_{K/F}$ is the trace map of K over F.

Proof. By $\mathcal{Z}^+$-linearity, it is enough to prove that $T_{\mathrm{rd}}(a) = \mathrm{Tr}_{K/F}(a)$ and $T_{\mathrm{rd}}(aX^i) = 0$ for $a \in K$ and $i \in \{1, \dots, s-1\}$. For the first assertion, we observe that the matrix of the multiplication map $x \mapsto xa$ in the canonical basis is diagonal and its diagonal entries are $a, \theta(a), \dots, \theta^{s-1}(a)$. Therefore its trace is $\mathrm{Tr}_{K/F}(a)$. Similarly, when $1 \leq i < s$, the matrix of the multiplication map $x \mapsto xaX^i$ has only nonzero entries at the position (u, v) with $v \equiv u+i \pmod{s}$. In particular, its diagonal vanishes. Hence so does its trace. □

As usual, the case where $\theta \neq \mathrm{id}_K$ reduces to the previous one using Hilbert twists. Precisely, writing $\delta = a\delta_0$ (see Proposition 1.3), we find the formula:

$$T_{\mathrm{rd}}\Big(\sum_i a_i (X+a)^i\Big) = \sum_i \mathrm{Tr}_{K/F}(a_{si}) (X+a)^{si}.$$

We now come to the case where $\theta = \mathrm{id}_K$. In this situation, we recall that F is the field of constants of K and that $Z(X)$ is defined as the minimal polynomial of δ; besides, we know that $Z(X)$ is a linearized polynomial over F, *i.e.* it takes the form:

$$Z(X) = X^{p^r} + z_{r-1} X^{p^{r-1}} + \cdots + z_1 X^p + z_0 X \tag{5}$$

with all the coefficients z_i in F. We then have $s = p^r$. For convenience, we also set $z_r = 1$.

Proposition 2.3. *For $a \in K$, we have:*

$$T_{\mathrm{rd}}(a) = T_{\mathrm{rd}}(aX) = \cdots = T_{\mathrm{rd}}\big(aX^{p^r-2}\big) = 0$$

and:

$$T_{\mathrm{rd}}\big(aX^{p^r-1}\big) = \sum_{j=0}^{r} z_j \delta^{p^j-1}(a).$$

Remark 2.4. Thanks to $\mathcal{Z}^+$-linearity, the above formulas are enough to compute the reduced trace of any Ore polynomial $f \in \mathcal{A}^+$. Besides, one immediately checks that the quantity $\sum_{j=0}^{r} z_j \delta^{p^j-1}(a)$ is annihilated by δ and hence lies in F. It follows from these observations that T_{rd} takes its values in $\mathcal{Z}^+ = F[Z(X)]$, in accordance with what we have announced in the introduction of §2.

The rest of this subsection is devoted to the proof of Proposition 2.3. For a Ore polynomial P, we denote by $\pi_i(P)$ its coefficient in front of X^i when P is written in the canonical $\mathcal{C}^+$-basis $\{1, X, \dots, X^{p^r-1}\}$ of $\mathcal{A}^+$. This defines a $\mathcal{C}^+$-linear map $\pi_i : \mathcal{A}^+ \to \mathcal{C}^+$.

Lemma 2.5. *For $0 \leq i < p^r$ and $-i \leq v < p^r$, we have:*

$$\begin{aligned} \pi_i(X^{i+v}) &= 1 && \text{if } v = 0 \\ &= -z_j && \text{if } v = p^r - p^j \text{ and } i \geq p^j \\ &= 0 && \text{otherwise.} \end{aligned}$$

Proof. We begin by noticing that, under the condition $v = p^r - p^j$, the fact that $i \geq p^j$ is equivalent to $i + v \geq p^r$. If $i + v < p^r$ then X^{i+v} is already written in the canonical basis and the result follows. On the contrary, if $i + v \geq p^r$, we write $i + v = p^r + k$ and:

$$X^{i+v} = X^{p^r} X^k = Z(X)X^k - \sum_{j=0}^{r-1} z_j X^{p^j+k}. \tag{6}$$

If $i + v < 2p^r - p^{r-1}$, then all the exposants $p^j + k$ are less than p^r and the writing above is the decomposition of X^{i+v} in the canonical basis. Hence the lemma follows in this case.

Finally, when $i + v \geq 2p^r - p^{r-1}$, applying π_i to Eq. (6), we get:

$$\pi_i(X^{i+v}) = Z(X)\pi_i(X^k) - \sum_{j=0}^{r-1} z_j \pi_i(X^{p^j+k}).$$

Observing that $p^j + k \leq p^{r-1} + k < p^{r+1} + p^r \leq 2p^r - p^{r-1}$ whenever $0 \leq j < r$, the lemma follows from what we have done previously. □

Let $n \in \{0, \ldots, p^r - 1\}$. By definition, the reduced trace of aX^n is given by:

$$T_{\mathrm{rd}}(aX^n) = \sum_{i=0}^{p^r-1} \pi_i(X^i a X^n).$$

Moving all the X to the right and writing $v = n - j$, we obtain the formula:

$$\begin{aligned} T_{\mathrm{rd}}(aX^n) &= \sum_{i=0}^{p^r-1} \sum_{v=n-i}^{n} \binom{i}{n-v} \delta^{n-v}(a) \cdot \pi_i(X^{i+v}) \\ &= \sum_{i=0}^{p^r-1} \sum_{v=-i}^{p^r-1} \binom{i}{n-v} \delta^{n-v}(a) \cdot \pi_i(X^{i+v}) \end{aligned}$$

the last equality being true because the binomial coefficients $\binom{i}{n-v}$ vanish when v is outside the range $[n-i, n]$. It follows from Lemma 2.5 that only the terms with $v = 0$ and $v = p^r - p^j$ contribute to the sum. Precisely, the contribution of the summands corresponding to $v = 0$ is:

$$\begin{aligned} \sum_{i=0}^{p^r-1} \binom{i}{n} \delta^n(a) = \binom{p^r}{n+1} \delta^n(a) &= 0 && \text{if } n < p^r - 1 \\ &= \delta^{p^r-1}(a) && \text{if } n = p^r - 1. \end{aligned}$$

Similarly, the contribution of the summands coming from $v = p^r - p^j$ is:

$$C_j = -z_j \sum_{i=p^j}^{p^r-1} \binom{i}{n-v} \delta^{n-v}(a) = -z_j \left(\binom{p^r}{n-v+1} - \binom{p^j}{n-v+1} \right) \delta^{n-v}(a).$$

When $n < p^r - 1$, *i.e.* $n - v + 1 < p^j$, the binomial coefficients $\binom{p^r}{n-v+1}$ and $\binom{p^j}{n-v+1}$ both vanish, implying that $C_j = 0$ as well. On the contrary, when $n = p^r - 1$, we find $C_j = z_j \delta^{p^j-1}(a)$.

Putting all the contributions together, we finally end up with the formula of Proposition 2.3.

2.2 Reduced trace and evaluation

We recall that we have introduced evaluation maps in §1.2. Precisely, for all unramified elements c of K, we have defined a ring homomorphism $\mathrm{ev}_c : \mathcal{A}^+ \to \mathrm{End}_F(K)$ taking a Ore polynomial $f(X)$ to $f(\delta + c\theta)$. We also recall that we have defined $\upsilon(c)$ as the remainder of the right Euclidean division of $Z(X)$ by $X - c$. By Corollary 1.11, we know that $\upsilon(c) \in F$.

Theorem 2.6. *For any unramified element $c \in K$, the following diagram is commutative:*

$$\begin{array}{ccc} \mathcal{A}^+ & \xrightarrow{\mathrm{ev}_c} & \mathrm{End}_F(K) \\ \Big\downarrow{\scriptstyle T_{\mathrm{rd}}} & & \Big\downarrow{\scriptstyle \mathrm{Tr}} \\ \mathcal{Z}^+ & \xrightarrow{Z(X)\mapsto \upsilon(c)} & F \end{array}$$

where Tr *denotes the usual trace map over* $\mathrm{End}_F(K)$.

The rest of this subsection is devoted to the proof of Theorem 2.6. Let I be the ideal of $\mathcal{Z}^+$ generated by $Z(X) - \upsilon(c)$. It follows from Proposition 1.10 that ev_c induces an isomorphism of rings:

$$\alpha : \mathcal{A}^+ / I\mathcal{A}^+ \xrightarrow{\sim} \mathrm{End}_F(K).$$

On the other hand, noticing that T_{rd} acts on the central element $Z(X) - \upsilon(c)$ by multiplication by $[K : F]$, we find that T_{rd} induces a map

$$\beta : \mathcal{A}^+ / I\mathcal{A}^+ \longrightarrow \mathcal{Z}^+ / I \simeq F$$

the identification between $\mathcal{Z}^+/I$ and F being induced by the map $Z(X) \mapsto \upsilon(c)$. After these observations, the theorem reduces to proving that $\beta = \mathrm{Tr} \circ \alpha$. For this, we rely on the following classical characterization of the trace map (which we reprove for completeness).

Lemma 2.7. *Let $\varphi : \mathrm{End}_F(K) \to F$ be a F-linear map such that $\varphi(uv) = \varphi(vu)$ for all $u, v \in \mathrm{End}_F(K)$. Then, there exists $\lambda \in F$ such that $\varphi = \lambda \cdot \mathrm{Tr}$.*

Proof. Fixing a basis, we can assume that the domain of φ is $M_s(F)$. For $1 \leq i, j \leq s$, let E_{ij} be the matrix whose unique nonzero entry is located at position (i, j) and is equal to 1. If $i \neq j$, we have the relations $E_{ij}E_{jj} = E_{ij}$ and $E_{jj}E_{ij} = 0$. Therefore applying φ, we get $\varphi(E_{ij}) = 0$. On the other hand, the fact that the matrices E_{ii} and E_{jj} are conjugated implies that $\varphi(E_{ii}) = \varphi(E_{jj})$. By F-linearity, we deduce that φ must be a scalar multiple of the trace map. □

Applying the previous lemma with $\varphi = \beta \circ \alpha^{-1}$, we conclude that there exists $\lambda \in F$ with the property that:

$$T_{\mathrm{rd}}(f) \equiv \lambda \cdot \mathrm{Tr}\big(\mathrm{ev}_c(f)\big) \pmod{I} \tag{7}$$

for all Ore polynomial $f \in \mathcal{A}^+$. We have to prove that $\lambda = 1$. When $\theta \neq \mathrm{id}_K$, we pick an element $a \in K$ whose trace over F does not vanish. Substituting $f = a$ in Eq. (7) and noticing that $\mathrm{ev}_c(a) : K \to K$ is the multiplication by a, we find $\mathrm{Tr}_{K/F}(a) = \lambda \cdot \mathrm{Tr}_{K/F}(a)$. Hence $\lambda = 1$ as wanted.

We now consider the case where $\theta = \mathrm{id}_K$. The field F is then the subfield of constants of δ and the polynomial $Z(X)$ is now given by Eq. (5). In accordance with Proposition 2.3, we set $\tau(a) = \sum_{i=0}^{r} z_i \delta^{p^i-1}(a)$ for $a \in K$. This defines a function τ which can be considered as a differential analogue of the trace map[2]. The following lemma summarizes the main properties of τ.

Lemma 2.8. *The function τ is F-linear and maps surjectively K onto F. Moreover* $\ker \tau = \mathrm{im}\, \delta$.

Proof. The fact that τ is F-linear is a straightforward verification. Similarly, we check that the composite $\delta \circ \tau$ vanishes. Therefore τ takes its values in F. Thanks to linearity, the surjectivity of τ will follow if we prove that τ is nonzero. But the vanishing of τ would mean that δ is annihilated by a polynomial of degree p^r-1, which contradicts the definition of $Z(X)$. It remains to prove that $\ker \tau = \mathrm{im}\, \delta$. For this, we observe that $\tau \circ \delta = 0$ and hence that $\ker \tau \subset \mathrm{im}\, \delta$. The equality follows by comparing dimensions (over F). □

We are now ready to complete the proof of Theorem 2.6. We fix an element $a \in K$ with $\tau(a) = 1$. Substituting $f = a(X-c)^{p^r-1}$ in Eq. (7), we find:

$$T_{\mathrm{rd}}\big(a\cdot(X-c)^{p^r-1}\big) = \lambda \cdot \mathrm{Tr}\big(a\delta^{p^r-1}\big). \tag{8}$$

Noticing that $a\cdot(X-c)^{p^r-1}$ is the sum of aX^{p^r-1} and of terms of smaller degrees, we deduce from Proposition 2.3 that the reduced trace of $a\cdot(X-c)^{p^r-1}$ is $\tau(a) = 1$. On the other hand, we can write $\delta^{p^r-1} = \tau - \sum_{i=0}^{r-1} z_i \delta^{p^i-1}$ and get:

$$\begin{aligned}\lambda \cdot \mathrm{Tr}\big(a\delta^{p^r-1}\big) &= \lambda \cdot \mathrm{Tr}(a\tau) - \sum_{i=0}^{r-1} \lambda \cdot \mathrm{Tr}(az_i\delta^{p^i-1}) \\ &= \lambda \cdot \mathrm{Tr}(a\tau) - \sum_{i=0}^{r-1} T_{\mathrm{rd}}\big(az_i(X-c)^{p^i-1}\big) = \lambda \cdot \mathrm{Tr}(a\tau).\end{aligned}$$

In order to compute the trace of $a\tau$, we consider a F-basis $(b_1, \ldots, b_{p^r-1})$ of $\ker \tau$. The family $(b_1, \ldots, b_{p^r-1}, a)$ is then a F-basis of K in which the matrix of $a\tau$ has all entries equal to 0 except the one in the bottom right corner which is 1. Hence the trace of $a\tau$ is 1. Plugging the values we found in both sides of Eq. (8), we end up with $\lambda = 1$, which concludes the proof.

3 Residues of Ore rational functions

Another important ingredient in the task of determining the duals of linearized Reed-Solomon codes is the extension of the notion of residues to Ore polynomials. This extension was already achieved in [7] in the case where the derivation δ is zero. In this section, we address the complementary case $\theta = \mathrm{id}_K$. By Hilbert's

[2]Note that, in the differential setting, the extension K/F is purely inseparable, so the usual trace map $\mathrm{Tr}_{K/F}$ vanishes.

reduction (see Propositions 1.2, 1.3 and the subsequent discussion), this will cover all cases.

Throughout this section, we then assume that $\theta = \mathrm{id}_K$. In other words, we work with a field K equipped with a derivation $\delta : K \to K$. We denote by F the subfield of constants and we assume that K/F is a finite extension. It follows from the fact that F contains all p-th powers that K/F is purely inseparable and hence has degree p^r for some integer r. As in the previous sections, we denote by $Z(X)$ the minimal polynomial of δ over K; it takes the form:

$$Z(X) = X^{p^r} + z_{r-1}X^{p^{r-1}} + \cdots + z_1 X^p + z_0 X$$

with all the coefficients z_i in F. For convenience, we also define $z_r = 1$. We set $\mathcal{A}^+ = K[X; \mathrm{id}_K, \delta]$ and define the commutative subrings $\mathcal{C}^+ = K[Z(X)]$ and $\mathcal{Z}^+ = F[Z(X)]$. The latter is the centre of $\mathcal{A}^+$.

3.1 Preliminaries

3.1.1 Differential trace and differential norm

In §1.2 and §2.2, we have introduced two functions $\upsilon : K \to F$ and $\tau : K \to F$ which, roughly speaking, play the role of the norm map and the trace map respectively in the differential setting. For future use, it will be convenient to extend those two functions to $\mathcal{C}^+$. For this, we first extend δ to a derivation of $\mathcal{C}^+$ by letting it act coefficientwise, *i.e.*

$$\delta\left(\sum_{i=0}^{d} a_i Z(X)^i\right) = \sum_{i=0}^{d} \delta(a_i) Z(X)^i.$$

One checks that δ continues to satisfy the Leibniz rule and that it takes its values of $\mathcal{Z}^+$.

Definition 3.1. For $C \in \mathcal{C}^+$, we set:

$$\tau(C) = \sum_{i=0}^{r} z_i \delta^{p^i-1}(C) \quad \text{and} \quad \upsilon(C) = \sum_{i=0}^{r} \sum_{j=0}^{i} \left(z_i \delta^{p^j-1}(C)\right)^{p^{i-j}}.$$

The above definition gives rise to two functions $\tau : \mathcal{C}^+ \to \mathcal{Z}^+$ and $\upsilon : \mathcal{C}^+ \to \mathcal{Z}^+$ that we call the *differential trace map* and the *differential norm map* respectively. We observe that τ is $\mathcal{Z}^+$-linear and that υ is additive. In addition, the next lemma shows that the differential trace is somehow the derivative of the differential norm as in the classical setting.

Lemma 3.2. *For $\varepsilon \in \mathcal{Z}^+$ and $C \in \mathcal{C}^+$, we have $\upsilon(\varepsilon C) \equiv \varepsilon\, \tau(C) \pmod{\varepsilon^2}$.*

Proof. By definition

$$\upsilon(\varepsilon C) = \sum_{i=0}^{r} \sum_{j=0}^{i} \left(z_i \delta^{p^j-1}(\varepsilon C)\right)^{p^{i-j}} = \sum_{i=0}^{r} \sum_{j=0}^{i} \left(z_i \varepsilon \delta^{p^j-1}(C)\right)^{p^{i-j}}$$

the second equality being correct since ε is in $\mathcal{Z}^+$ by assumption. We observe that only the terms with $i = j$ survive modulo ε^2, which gives the lemma. □

Besides, the next proposition shows that the differential norm is closely related to the computations in the noncommutative ring $\mathcal{A}^+$.

Proposition 3.3. *For $C \in \mathcal{C}^+$, the identity $Z(X+C) = Z(X) + v(C)$ holds in $\mathcal{A}^+$.*

Proof. This is a direct consequence of [11, No 12] (see in particular Eq. (30) and Eq. (35)). □

3.1.2 The fraction field of $\mathcal{A}^+$

In the commutative setting, residues have poor interest if we are restricting ourselves to polynomials and do not move to the field of rational functions. In the Ore setting, the same is true. However, since $\mathcal{A}^+$ is a noncommutative ring, defining its field of fractions is not as easy as usual. This can however be achieved (see for instance [8, §0.10]): using Ore condition, one proves that there exists a unique skew field $\mathcal{A}$ containing $\mathcal{A}^+$ for which the following universal property holds: for any noncommutative ring $\mathfrak{A}$ and any homomorphism of rings $\phi : \mathcal{A}^+ \to \mathfrak{A}$ such that $\phi(x)$ is invertible for all $x \in \mathcal{A}^+$, $x \neq 0$, there exists a unique morphism of rings $\psi : \mathcal{A} \to \mathfrak{A}$ making the following diagram commutative:

$$\begin{array}{ccc} \mathcal{A}^+ & \xrightarrow{\phi} & \mathfrak{A} \\ \downarrow & \nearrow_{\psi} & \\ \mathcal{A} & & \end{array} \tag{9}$$

Such a ring $\mathcal{A}$ is called the fraction field of $\mathcal{A}^+$. In our particular setting, it turns out that one has a rather simple description of $\mathcal{A}$.

Proposition 3.4. *The fraction field of $\mathcal{A}^+$ is $\mathcal{A} = \mathrm{Frac}(\mathcal{Z}^+) \otimes_{\mathcal{Z}^+} \mathcal{A}^+$.*

Proof. We first claim that any Ore polynomial $P \in \mathcal{A}^+$ has a nonzero left and a right multiple in $\mathcal{Z}^+$. Indeed, observe that the quotient $\mathcal{A}^+/P\mathcal{A}^+$ is a finite dimensional vector space over F. Therefore there exists a nontrivial relation of linear dependance of the form:

$$\sum_{i=0}^{n} a_i Z(X)^i \in P\mathcal{A}^+ \quad (a_i \in F).$$

Thus, there exists $Q \in \mathcal{A}^+$ with the property that $PQ \in \mathcal{Z}^+$. Besides, since PQ is central, we deduce that $QPQ = PQQ$ and, simplifying by Q on the right, we find that P and Q commute.

We are now ready to prove that $\mathrm{Frac}(\mathcal{Z}^+) \otimes_{\mathcal{Z}^+} \mathcal{A}^+$ is a skew field. Indeed, reducing to the same denominator, we remark that any nonzero element of $\mathrm{Frac}(\mathcal{Z}^+) \otimes_{\mathcal{Z}^+} \mathcal{A}^+$ can be written as $D^{-1} \otimes P$ where $D \in \mathcal{Z}^+$, $P \in \mathcal{A}^+$ and both of them do not vanish. By the first part of the proof, there exists $Q \in \mathcal{A}^+$ such that $PQ = QP \in \mathcal{Z}^+$. Letting $N = PQ$, we check that $N^{-1} \otimes QD$ is a multiplicative inverse of $D^{-1} \otimes P$.

We consider a noncommutative ring $\mathfrak{A}$ together with a ring homomorphism $\varphi : \mathcal{A}^+ \to \mathfrak{A}$ such that $\varphi(P)$ is invertible for all $P \in \mathcal{A}^+$, $P \neq 0$. If $\psi : \mathcal{A} \to \mathfrak{A}$ is an extension of φ, it must satisfy:

$$\psi\big(D^{-1} \otimes P\big) = \varphi(D)^{-1} \cdot \varphi(P). \tag{10}$$

This proves that, if such an extension exists, it is unique. On the other hand, using that $\mathcal{Z}^+$ is central in $\mathcal{A}^+$, one checks that the formula (10) determines a well-defined ring homomorphism $\mathcal{A} \to \mathfrak{A}$ making the diagram (9) commutative. □

3.2 Taylor expansions

The main ingredient of the theory of differential residues is a notion of Taylor expansion for elements of $\mathcal{A}^+$ extending the one we are familiar with in the commutative case.

3.2.1 Existence of Taylor expansions

We consider an element $z \in F$ and set $N = Z(X) - z \in \mathcal{Z}^+$. The usual Taylor expansion yields an isomorphism of K-algebras:

$$\begin{array}{ccc} \varprojlim_{m>0} \mathcal{C}^+/N^m\mathcal{C}^+ & \xrightarrow{\sim} & K[\![T]\!] \\ f(Z(X)) & \mapsto & f(z) + f'(z)T + \cdots + \frac{f^{(n)}(z)}{n!}T^n + \cdots \end{array}$$

which is uniquely determined by the fact that it maps N to T and it induces the identify after quotienting out by N on the left and by T on the right. The next theorem tells that this isomorphism extends to $\mathcal{A}^+$.

Theorem 3.5. *With the above notations, there exists an isomorphism of K-algebras:*

$$\varprojlim_{m>0} \mathcal{A}^+/N^m\mathcal{A}^+ \xrightarrow{\sim} (\mathcal{A}^+/N\mathcal{A}^+)[\![T]\!]$$

sending N to T and inducing the identity when we quotient out by N on the left and by T on the right.

Proof. Throughout the proof, we fix an element $a \in K$ such as $\tau(a) = 1$; such an element exists thanks to Lemma 2.8. We are going to construct by induction a sequence $(\zeta_m)_{m>0}$ of elements of $\mathcal{Z}^+$ such that $\zeta_1 = 0$ and, for $m > 0$,

- $\zeta_{m+1} \equiv \zeta_m \pmod{N^m}$,
- $N(X + a\zeta_m) \in N^m\mathcal{A}^+$.

We suppose that the sequence has been built until the index m. The next term ζ_{m+1} is of the form $\zeta_m + N^m P$ for some polynomial $P \in \mathcal{Z}^+$. Besides it satisfies our requirements if and only if $N(X + a\zeta_{m+1}) \in N^{m+1}\mathcal{A}^+$. Relying on Lemma 3.2 and Proposition 3.3, we carry out the following computation:

$$\begin{aligned} N(X + a\zeta_{m+1}) &= N(X) + v(a\zeta_{m+1}) = N(X) + v(a\zeta_m) + v(aN^mP) \\ &\equiv N(X + a\zeta_m) + N^mP \pmod{N^{m+1}} \end{aligned}$$

given that $\tau(a) = 1$ and $N^mP \in \mathcal{Z}^+$. Since $N(X + a\zeta_m)$ is divisible by N^m thanks to our induction hypothesis, one can choose P in order to ensure that $N(X + a\zeta_{m+1}) \equiv 0 \pmod{N^{m+1}}$. This completes the construction of ζ_{m+1}.

We now set:

$$\zeta = (\zeta_m)_{m>0} \in \varprojlim_{m>0} \mathcal{Z}^+/N^m\mathcal{Z}^+.$$

Passing to the limit, we find $N(X + a\zeta) = 0$. This property allows us to define a morphism of K-algebras:

$$\iota : \mathcal{A}^+/N\mathcal{A}^+ \longrightarrow \varprojlim_{m>0} \mathcal{A}^+/N^m\mathcal{A}^+, \quad X \mapsto X + a\zeta.$$

Furthermore, as $C \equiv 0 \pmod{N}$, ι reduces to the identity map modulo N. By sending T to N, we can extend ι to a second morphism :

$$\rho : (\mathcal{A}^+/N\mathcal{A}^+)[\![T]\!] \longrightarrow \varprojlim_{m>0} \mathcal{A}^+/N^m\mathcal{A}^+.$$

This morphism reduces to the identity when we quotient out by T on the left and by N on the right. It is moreover bijective since its domain and codomain are both separated and complete (for the T-adic and N-adic topology respectively). Its inverse then satisfies all the requirements of the theorem. □

3.2.2 Unicity of Taylor expansions

Unfortunately, unlike the commutative case, an isomorphism satisfying the conditions of Theorem 3.5 is not unique in general. For this reason, it is convenient to introduce the following definition.

Definition 3.6. Keeping the above notations, an isomorphism

$$\varprojlim_{m>0} \mathcal{A}^+/N^m\mathcal{A}^+ \longrightarrow (\mathcal{A}^+/N\mathcal{A}^+)[\![T]\!]$$

is called *z-admissible* (or simply *admissible* if there is no risk of confusion) if it maps N to T and it induces the identity after quotienting out by N on the left and by T on the right.

Proposition 3.7. *Let*

$$\tau_1, \tau_2 : \varprojlim_{m>0} \mathcal{A}^+/N^m\mathcal{A}^+ \xrightarrow{\sim} (\mathcal{A}^+/N\mathcal{A}^+)[\![T]\!]$$

be two admissible isomorphisms. Then there exists $V \in (\mathcal{A}^+/N\mathcal{A}^+)[\![T]\!]$ *with* $V \equiv 1 \pmod{T}$ *such that* $\tau_1(f) = V^{-1}\tau_2(f)V$ *for all* $f \in \varprojlim_{m>0} \mathcal{A}^+/N^m\mathcal{A}^+$.

Proof. For simplicity, we write $R = \mathcal{A}^+/N\mathcal{A}^+$. We first claim that R is a simple central algebra over $\mathcal{Z}^+/N\mathcal{Z}^+ \simeq F$. Indeed, it is central because the formation of centres commutes with the tensor product. In order to prove that it is simple, let I be a nonzero two-sided ideal of R. Since it is in particular a right ideal, there exists a monic divisor P of N such that $I = P\mathcal{A}^+/N\mathcal{A}^+$. Observe that the commutator $PX - XP$ lies in I and has degree strictly less that $\deg P$. Hence it has to vanish, meaning that $PX = XP$ in R. Similarly, we prove that $Pa = aP$ for all $a \in K$. Therefore P is central in R, which shows that $P \in \mathcal{Z}^+/N\mathcal{Z}^+$. Since the latter is a field, we deduce that P is invertible in R and finally that $I = R$. Hence R is simple.

Define $\tau = \tau_1 \circ \tau_2^{-1}$; it is an automorphism of $R[\![T]\!]$ which takes T to itself and is congruent to the identity modulo T. Since R is simple central, it follows from [3, Theorem 9.1] (applied with $\varphi = \tau_{|R}$) that there exists an invertible element $c \in R[\![T]\!]$ such that $\tau(x) = c^{-1}xc$ for all $x \in R$. In fact, the latter equality holds more generally for any $x \in R[\![T]\!]$ given that $\tau(T) = T$. Finally, the fact that τ is congruent to the identity modulo T indicates that $c_0 = c \bmod T$ must be central in R. The proposition then holds for $V = c_0^{-1}c$. □

3.3 Construction of skew residues

We recall that we have constructed earlier the fraction field of $\mathcal{A}^+$ (see Proposition 3.4); in what follows, we will denote it by $\mathcal{A}$. Similarly, we set $\mathcal{C} = \mathrm{Frac}(\mathcal{C}^+)$ and $\mathcal{Z} = \mathrm{Frac}(\mathcal{Z}^+)$. Besides, as before, we consider an element $z \in F$ and set $N = Z(X) - z \in \mathcal{Z}^+$. We choose an admissible isomorphism τ_z and consider the compositum:

$$\mathrm{TS}_z : \mathcal{A}^+ \longrightarrow \varprojlim_{m>0} \mathcal{A}^+/N^m\mathcal{A}^+ \xrightarrow{\tau_z} (\mathcal{A}^+/N\mathcal{A}^+)[\![T]\!]$$

where the first map is induced by the canonical projections $\mathcal{A}^+ \to \mathcal{A}^+/N^m\mathcal{A}^+$.

Lemma 3.8. *For any $f \in \mathcal{Z}$, the series $\mathrm{TS}_z(f)$ is invertible in $(\mathcal{A}^+/N\mathcal{A}^+)(\!(T)\!)$.*

Proof. It is enough to prove the lemma when f is monic and irreducible in $\mathcal{Z}^+$. It is clear when $f = N$ because TS_a maps N to T, which is by definition invertible in $(\mathcal{A}^+/N\mathcal{A}^+)(\!(T)\!)$. On the other hand, if f is different from N, it must be coprime with N by irreducibility. It is then invertible in each quotient $\mathcal{Z}^+/N^m\mathcal{Z}^+$ and thus it is also a unit in each $\mathcal{A}^+/N^m\mathcal{A}^+$. Passing to the limit, we find that f is invertible in $\varprojlim_{m>0} \mathcal{A}^+/N^m\mathcal{A}^+$; it is then also in $(\mathcal{A}^+/N\mathcal{A}^+)[\![T]\!]$ given that τ_a is an isomorphism. □

Combining Proposition 3.4 and Lemma 3.8, we find that TS_z uniquely extends to a ring homomorphism $\mathcal{A} \to (\mathcal{A}^+/N\mathcal{A}^+)(\!(T)\!)$ that, in a slight abuse of notations, we continue to denote by TS_z.

It turns out that the previous construction extends to elements lying in extensions of F. Precisely, let F^{s} denote a fixed separable closure of F and set $K^{\mathrm{s}} = F^{\mathrm{s}} \otimes_F K$. Since K/F is purely inseparable, it is linearly disjoint from F^{s}, implying that K^{s} is a field. Moreover, the derivation $\delta : K \to K$ extends uniquely by F^{s}-linearity to a derivation of K^{s} whose field of constant is F^{s} and minimal polynomial is still $Z(X)$. In what follows, we continue to call δ this extension. We define $\mathcal{A}^{\mathrm{s},+} = K^{\mathrm{s}}[X;\delta]$ and $\mathcal{A}^{\mathrm{s}} = \mathrm{Frac}(\mathcal{A}^{\mathrm{s},+})$. Applying what we have done previously with K replaced by K^{s} (and F replaced by F^{s} accordingly), we end up with a ring homomorphism:

$$\mathrm{TS}_z : \mathcal{A} \to \big(\mathcal{A}^{\mathrm{s},+}/(Z(X)-a)\mathcal{A}^{\mathrm{s},+}\big)(\!(T)\!)$$

for any $z \in F^{\mathrm{s}}$. The series $\mathrm{TS}_z(f)$ is called the *Taylor expansion* of f around a.

We insist on the fact that it does depend on a choice of the admissible isomorphism τ_z. However, from Proposition 3.7, we derive that two different choices of τ_z lead to two mappings TS_z which are conjugated by an element congruent to 1 modulo T. In particular, the two following quantities are defined without ambiguity:

- the *order of vanishing* of f at z, denoted by $\mathrm{ord}_z(f)$, defined as the T-adic valuation of $\mathrm{TS}_z(f)$,
- the *principal part* of f at z, denoted by $\mathcal{P}_z(f)$, defined as the coefficient of $T^{\mathrm{ord}_z(f)}$ in the series $\mathrm{TS}_z(f)$.

We are now ready to define skew residues.

Definition 3.9. Given $f \in \mathcal{A}$ and $z \in F^{\mathrm{s}}$, the *skew residue* of f at z, denoted by $\mathrm{sres}_z(f)$, is the coefficient of T^{-1} in the series $\mathrm{TS}_z(f)$.

Again, we insist on the fact that skew residues do depend on the choice of an admissible isomorphism. However, they are defined without ambiguity when the Ore function f has at most a *simple pole* at the point z we are looking at, *i.e.* if $\mathrm{ord}_z(f) \geq -1$. We shall see in §3.4 below that some quantities related to $\mathrm{sres}_a(f)$ are also well-defined in full generality.

3.4 Reduced traces of skew residues

We recall that we have introduced in §2 the reduced trace map $T_{\mathrm{rd}} : \mathcal{A}^+ \to \mathcal{Z}^+$ and that we have given an explicit formula for it in Proposition 2.3. Using Proposition 3.4, we extend by $\mathcal{Z}$-linearity the map T_{rd} to a mapping $\mathcal{A} \to \mathcal{Z}$ (we recall that $\mathcal{Z} = \mathrm{Frac}(\mathcal{Z}^+)$) and continue to call T_{rd} this extension.

Proposition 3.10. *For all $f \in \mathcal{A}$ and all $z \in F^{\mathrm{s}}$, we have:*

$$T_{\mathrm{rd}}\big(\mathrm{sres}_z(f)\big) = \mathrm{res}_z\big(T_{\mathrm{rd}}(f)\, dZ(X)\big)$$

where $\mathrm{res}_z(\omega)$ denotes the residue at z of the differential form ω.

Proof. Write $N = Z(X) - z$. The proposition will follow if you prove the commutativity of the following diagram:

$$\begin{array}{ccc} \mathcal{A} & \xrightarrow{\mathrm{TS}_z} & \big(\mathcal{A}^{\mathrm{s},+}/N\mathcal{A}^{\mathrm{s},+}\big)(\!(T)\!) \\ \Big\downarrow{\scriptstyle T_{\mathrm{rd}}} & & \Big\downarrow{\scriptstyle T_{\mathrm{rd}}} \\ \mathcal{Z} & \xrightarrow{\mathrm{TS}_z} & \big(\mathcal{Z}^{\mathrm{s},+}/N\mathcal{Z}^{\mathrm{s},+}\big)(\!(T)\!) = F^{\mathrm{s}}(\!(T)\!). \end{array}$$

By $\mathcal{Z}$-linearity, it is enough to consider the case where $f \in \mathcal{A}^+$. We equip $\mathcal{A}^+$ (resp. $\mathcal{A}^{\mathrm{s},+}/N\mathcal{A}^{\mathrm{s},+}$) with its canonical basis $(1, X, \ldots, X^{p^r-1})$ over $\mathcal{C}^+$ (resp. $\mathcal{C}^{\mathrm{s},+}/N\mathcal{C}^{\mathrm{s},+}$). Let M be the matrix of the map $x \mapsto xf$ acting on $\mathcal{A}^+$ and similarly, let N be the matrix of the map $x \mapsto x \cdot \mathrm{TS}_z(f)$ acting on $\big(\mathcal{A}^{\mathrm{s},+}/N\mathcal{A}^{\mathrm{s},+}\big)[\![T]\!]$. By definition $T_{\mathrm{rd}}(f)$ is the trace of M while $T_{\mathrm{rd}} \circ \mathrm{TS}_z(f)$ is the trace of N. On the other hand, from the fact that TS_z is a ring homomorphism, we deduce that the matrices $\mathrm{TS}_z(M)$ and N and conjugated so, they have the same trace. Hence $T_{\mathrm{rd}} \circ \mathrm{TS}_z(f) = \mathrm{TS}_z \circ T_{\mathrm{rd}}(f)$ and we have proved our claim. □

Remark 3.11. Proposition 3.10 can be refined as follows. Let $\sigma_0 : \mathcal{A}^+ \to \mathcal{C}^+$ be the $\mathcal{C}^+$-linear form defined by $\sigma_0(X^i) = 0$ for $0 \leq i < p^r - 1$ and $\sigma_0(X^{p^r-1}) = 1$. Extending scalars, we find that σ_0 induces mappings $\mathcal{A} \to \mathcal{C}$ and $(\mathcal{A}^{\mathrm{s},+}/N\mathcal{A}^{\mathrm{s},+})(\!(T)\!) \to (\mathcal{C}^{\mathrm{s},+}/N\mathcal{C}^{\mathrm{s},+})(\!(T)\!)$. With these notations, one can prove that:

$$\sigma_0\big(\mathrm{sres}_z(f)\big) = \mathrm{res}_z\big(\sigma_0(f)\, dZ(X)\big)$$

This latter statement gives back Proposition 3.10 after applying τ on both sides; it then indeed appears as a refinement of the proposition.

Proposition 3.10 admits several interesting corollaries. For example, it shows that the reduced trace of $\mathrm{sres}_z(f)$ is canonical in the sense that it does not depend on a choice of an admissible isomorphism τ_z. Besides, one has a noncommutative analogue of the residue formula given by the next theorem.

Theorem 3.12 (Residue formula)**.** *Let $f = \frac{P}{D} \in \mathcal{A}$ with $P \in \mathcal{A}^+$ and $D \in \mathcal{Z}^+$, $D \neq 0$. If $\deg P \leq \deg D - 2$, we have:*

$$\sum_{z \in F^s} T_{\mathrm{rd}}\big(\mathrm{sres}_z(f)\big) = 0.$$

Proof. Write $g = T_{\mathrm{rd}}(f) = \frac{T_{\mathrm{rd}}(P)}{D} \in \mathcal{Z}$ and define the differential form $\omega = g \cdot dZ(X)$. Applying Proposition 3.10 to each summand, we obtain:

$$\sum_{z \in F^s} T_{\mathrm{rd}}\big(\mathrm{sres}_z(f)\big) = \sum_{z \in F^s} \mathrm{res}_z(\omega). \tag{11}$$

By the condition on the degrees, the differential form ω has no pole at infinity. It may have poles at inseparable points but the corresponding residues all vanish. From the classical residue formula, we then deduce that the right hand side of Eq. (11) vanishes. The left hand side then vanishes as well, establishing the theorem. □

4 Duality over Ore polynomial rings

In this section, we discuss duality over Ore rings and its relation with evaluation morphisms and residue maps.

We keep the framework of the previous sections: we consider a field K equipped with a ring homomorphism $\theta : K \to K$ and a θ-derivation $\delta : K \to K$. We denote by F the subfield of K consisting of elements $a \in K$ such that $\theta(a) = a$ and $\delta(a) = 0$ and we assume as always that K/F is a finite extension. We set $\mathcal{A}^+ = K[X; \theta, \delta]$.

We recall that the centre $\mathcal{Z}^+$ of $\mathcal{A}^+$ is the ring of univariate polynomials over F in a distinguished element $Z(X)$. When $\theta = \mathrm{id}_K$, this special central polynomial $Z(X)$ takes the form

$$Z(X) = X^{p^r} + z_{r-1}X^{p^{r-1}} + \cdots + z_1 X^p + z_0 X \quad (z_i \in F) \tag{12}$$

(see Eq. (1)). On the contrary, when $\theta \neq \mathrm{id}_K$, we have $Z(X) = (X+a)^s$ where $s = [K : F]$ is the order of θ and a is some element of K. If $\theta = \mathrm{id}_K$, we define $s = p^r$. In both cases, we then have $s = \deg Z = [K : F]$.

4.1 Two perfect pairings

To begin with, we recall the definition of duality in the context of the sum-rank metric. Our presentation differs slightly from the most usual one in the sense we do not work with matrices and transposes but instead with pairings and adjoints.

When $\theta = \mathrm{id}_K$, we define $\tau : K \to F$ as in §2.2 by the formula:

$$\tau(f) = \sum_{i=0}^{r} z_i \delta^{p^i - 1}(f).$$

On the contrary, when $\theta \neq \mathrm{id}_K$, we let τ denote the trace map of K/F.

Proposition 4.1. *The pairing $K \times K \to F$, $(f, g) \mapsto \langle f, g \rangle_K = \tau(fg)$ is F-bilinear and nondegenerate.*

Proof. Bilinearity follows from the linearity of τ. When $\theta = \mathrm{id}_K$, nondegeneracy follows from the fact that $\tau : K \to F$ is surjective (see Lemma 2.8).

When $\theta \neq \mathrm{id}_K$, we claim that F is the subfield of K fixed by θ. Indeed, by Proposition 1.3, we know that δ is a scalar multiple of $\delta_0 = \theta - \mathrm{id}_K$. Therefore δ vanishes on the subfield fixed by θ and our claim is proved. It follows that the extension K/F is separable, implying eventually that τ is nondegenerate. □

From now on, we endow K with the bilinear pairing $\langle f, g\rangle_K = \tau(fg)$. If V is a F-linear subspace of K, we recall that the *orthogonal* of V, denoted by $V^\perp$, is defined as the set of all $f \in K$ such that $\langle f, g\rangle_K = 0$ for all $g \in V$. Similarly, if $\varphi : K \to K$ is a F-linear map, we define the *adjoint* of φ, denoted by $\varphi^\star$, as the endomorphism of K determined by the adjunction rule:

$$\langle \varphi^\star(f), g\rangle_K = \langle f, \varphi(g)\rangle_K$$

which is required to hold true for all $f, g \in K$. It is important to notice that for all $a \in K$, the multiplication by a (*i.e.* the mapping $\mu_a : K \to K$, $x \mapsto ax$) is self-adjoint (*i.e.* $\mu_a^\star = \mu_a$).

It is well-known that $\ker(\varphi^\star) = \mathrm{im}\,(\varphi)^\perp$ and $\mathrm{im}\,(\varphi^\star) = \ker(\varphi)^\perp$. From these equalities, it follows that φ vanishes on some F-linear subspace V of K if and only if $\varphi^\star$ takes its values in $V^\perp$. The adjoint construction then induces a bijection between $\mathrm{Hom}_F(K/V, K)$ and $\mathrm{Hom}_F(K, V^\perp)$. Replacing V by $V^\perp$, we find that is also induces an isomorphism $\mathrm{Hom}_F(K/V^\perp, K) \xrightarrow{\sim} \mathrm{Hom}_F(K, V)$.

Lemma 4.2. *For any F-linear subspace V of K, the mapping :*

$$\begin{array}{rcl} \mathrm{Hom}_F(K/V^\perp, K) \times \mathrm{Hom}_F(V, K) & \longrightarrow & F \\ (\varphi, \psi) & \mapsto & \langle \varphi, \psi\rangle = \mathrm{Tr}(\varphi^\star \circ \psi) \end{array}$$

(where Tr *denotes the trace map) is a perfect F-bilinear pairing.*

Proof. As $\mathrm{Hom}_F(K/V^\perp, K)$ and $\mathrm{Hom}_F(V, K)$ have the same dimension, it is enough to establish the following property: if $\psi \in \mathrm{Hom}_F(V, K)$ is such that $\mathrm{Tr}(\varphi^\star \circ \psi) = 0$ for all $\varphi \in \mathrm{Hom}_F(K/V^\perp, K)$, then $\psi = 0$. Given that the adjunction induces an isomorphism between $\mathrm{Hom}_F(K/V^\perp, K)$ and $\mathrm{Hom}_F(K, V)$, it is enough to prove that $\psi = 0$ if $\mathrm{Tr}(\varphi \circ \psi) = 0$ for all $\varphi \in \mathrm{Hom}_F(K, V)$. Taking basis and writing $s = [K{:}F]$, $d = \dim_F V$, we are reduced to check that if a matrix $M \in \mathcal{M}_{s,d}$ satisfies $\mathrm{Tr}(NM) = 0$ for all $N \in \mathcal{M}_{d,s}$, then M is zero. This finally follows from the observation that $\mathrm{Tr}(NM)$ is the (i, j) coefficient of M when N is the matrix with all entries equal to 0 except the one in position (j, i) which is equal to 1. □

Remark 4.3. An important particular case occurs when $V = K$; in this situation $K/V^\perp$ is equal to K as well and the bilinear form $\langle -, -\rangle$ of Lemma 4.2 defines a perfect pairing over $\mathrm{End}_F(K)$.

If C is a F-linear subspace of $\mathrm{Hom}_F(V, K)$ (resp. of $\mathrm{Hom}_F(K/V^\perp, K)$), we will denote by $C^\perp$ its orthogonal in $\mathrm{Hom}_F(K/V^\perp, K)$ (resp. in $\mathrm{Hom}_F(V, K)$). Since our pairing is nondegenrate, we always have $(C^\perp)^\perp = C$ and the following equality of dimensions:

$$\dim_F C + \dim_F C^\perp = \dim_F \mathrm{Hom}_F(V, K) = [K : F] \cdot \dim_F V. \tag{13}$$

Besides, it is worth noticing that both $\mathrm{Hom}_F(K/V^\perp, K)$ and $\mathrm{Hom}_F(V, K)$ are endowed with a natural structure of K-linear vector spaces since K acts on the codomains. The next lemma ensures that K-linearity is preserved under duality.

Lemma 4.4. *If C is a K-linear subspace of $\mathrm{Hom}_F(V, K)$, then $C^\perp$ is a K-linear subspace of $\mathrm{Hom}_F(K/V^\perp, K)$. Moreover, we have:*

$$\dim_K C + \dim_K C^\perp = \dim_F V.$$

Proof. Let $\varphi \in C^\perp$. Let $a \in K$ and let $\mu_a : K \to K$ denote the multiplication map by a. Given $\psi \in C$, we compute:

$$\mathrm{Tr}\big((\mu_a \circ \varphi)^\star \circ \psi\big) = \mathrm{Tr}\big(\varphi^\star \circ \mu_a \circ \psi\big) = 0$$

the first equality coming from the fact that μ_a is self-adjoint while the second one is correct because $\mu_a \circ \psi$ is in C given that C is a K-linear subspace by assumption. Consequently $\mu_a \circ \varphi \in C^\perp$ and we have proved that $C^\perp$ is stable under multiplication by K.

Finally, the equality of dimensions follows immediately from Eq. (13). □

4.2 Construction of duality

We recall that we have proved in §1.1 that the pair (θ, δ) is either of the form (id_K, δ) with $\delta \neq 0$ or $(\theta, a\delta_0)$ with $a \in K$ and $\delta_0 = \theta - \mathrm{id}_K$. We recall also that we have defined the notion of ramified elements in Definition 1.9. When $\theta = \mathrm{id}_K$, all elements are actually unramified whereas there is exactly one ramified element in the second case, which is $-a$. Accordingly we define:

$$\begin{aligned} \mathcal{A}^{\mathrm{ur}} &= \mathcal{A}^+ && \text{if } \theta = \mathrm{id}_K \\ &= \mathcal{A}^+\big[\tfrac{1}{X+a}\big] = \mathcal{Z}^+\big[\tfrac{1}{(X+a)^s}\big] \otimes_{\mathcal{Z}^+} \mathcal{A}^+ && \text{if } \theta \neq \mathrm{id}_K \text{ and } \delta = a\delta_0. \end{aligned}$$

where we recall that s is the degree of the extension K/F.

Definition 4.5. For $f \in \mathcal{A}^{\mathrm{ur}}$, we define $f^\star$ as follows.

- If $\theta = \mathrm{id}_K$, we write $f = \sum_{i=0}^n a_i X^i$ and set:

$$f^\star = \sum_{i=0}^n (-1)^i X^i a_i.$$

- If $\theta \neq \mathrm{id}_K$ and $\delta = a\delta_0$, we write $f = \sum_{i=v}^n a_i (X+a)^i$ and set:

$$f^\star = \sum_{i=v}^n (X+a)^{-i} a_i.$$

It is a straightforward calculation in check in both cases that the three following properties hold true for all f, g in $\mathcal{A}^{\mathrm{ur}}$: (i) $f^{\star\star} = f$, (ii) $(f+g)^\star = f^\star + g^\star$ and (iii) $(fg)^\star = g^\star f^\star$. In other words, the duality construction $f \mapsto f^\star$ defines a ring homomorphism $(\mathcal{A}^{\mathrm{ur}})^{\mathrm{op}} \to \mathcal{A}^{\mathrm{ur}}$ which is an involution. Here $(\mathcal{A}^{\mathrm{ur}})^{\mathrm{op}}$ denotes the opposite ring of $\mathcal{A}^{\mathrm{ur}}$ which is defined by reversing the

direction of the multiplication. By the universal property of the fraction field, the duality extends to a ring homomorphism $\mathcal{A}^{\mathrm{op}} \to \mathcal{A}$. Notice that:

$$\begin{aligned} Z(X)^\star &= -Z(X) && \text{if } \theta = \mathrm{id}_K \\ &= Z(X)^{-1} && \text{otherwise.} \end{aligned}$$

We now want to compare the above duality with the evaluation maps ev_c we have introduced in §1.2. We recall that we have already computed the kernel of ev_c in Proposition 1.10; it is the principal ideal generated by $Z(X)-\upsilon(c)$ where $\upsilon(c)$ is given explicitely by Eq. (4) when $\theta = \mathrm{id}_K$ and is equal to $N_{K/F}(c+a)$ otherwise.

Given an unramified element $c \in K$, it is convenient to put:

$$\begin{aligned} c^\vee &= -c && \text{if } \theta = \mathrm{id}_K \\ &= \tfrac{1}{c+a} - a && \text{if } \theta \neq \mathrm{id}_K \text{ and } \delta = a\delta_0. \end{aligned}$$

Theorem 4.6. *Let $c \in K$ be an unramified element and set $N = Z(X) - \upsilon(c)$. The following diagram is commutative:*

$$\begin{array}{ccc} \mathcal{A}^{\mathrm{ur}}/N\mathcal{A}^{\mathrm{ur}} & \xrightarrow{\mathrm{ev}_c} & \mathrm{End}_F(K) \\ \Big\downarrow{\scriptstyle f \mapsto f^\star} & & \Big\downarrow{\scriptstyle \varphi \mapsto \varphi^\star} \\ \mathcal{A}^{\mathrm{ur}}/N^\star\mathcal{A}^{\mathrm{ur}} & \xrightarrow[\mathrm{ev}_{c^\vee}]{} & \mathrm{End}_F(K) \end{array}$$

where $\varphi^\star$ is the adjoint of φ for the pairing $\langle x, y\rangle_K = \tau(xy)$ as in §4.1.

Proof. By linearity and using the fact that the multiplication by elements of K are self-adjoint, it is enough to prove the theorem when $f = X^i$ (resp. $f = (X+a)^i$) for some i when $\theta = \mathrm{id}_K$ (resp. $\theta \neq \mathrm{id}_K$). By the multiplicativity property of adjoints, this further amounts to checking that $\delta^\star = -\delta$ (resp. $\theta^\star = \theta^{-1}$).

We first consider the case where $\theta = \mathrm{id}_K$. Let $x, y \in K$. From the relation $\tau(\delta(xy)) = 0$ (see Lemma 2.8), we derive $\tau(x\delta(y)) = -\tau(\delta(x)y)$, which also reads $\langle x, \delta(y)\rangle_K = \langle -\delta(x), y\rangle_K$. We can then conclude in this case. In the case where $\theta \neq \mathrm{id}_K$, we need to show that $\langle \theta(x), y\rangle_K = \langle x, \theta^{-1}(y)\rangle_K$ for $x, y \in K$. By definition, this reduces to verify that $\tau\big(\theta(x)\cdot y\big) = \tau\big(x\cdot\theta^{-1}(y)\big)$ which is obvious because τ, being the trace map $\mathrm{Tr}_{K/F}$ in this case, takes the same value on two conjugated elements. □

We now focus on the comparison between duality and residues. We recall that residues have been constructed in [7] in the case of $K[X;\theta,0]$ and in §3 in the case of $K[X;\mathrm{id}_K,\delta]$. Using Hilbert twists (see Propositions 1.2 and 1.3), these two special situations cover all cases.

Theorem 4.7. *Let $z \in F^{\mathrm{s}}$ and assume that $z \neq 0$ if $\theta \neq \mathrm{id}_K$. Set $\bar{z} = -z$ if $\theta = \mathrm{id}_K$ and $\bar{z} = z^{-1}$ otherwise. Then, for all $f \in \mathcal{A}$ and for any z-admissible isomorphism, there exists a $\bar{z}$-admissible isomorphism such that:*

$$\begin{aligned} \mathrm{sres}_z(f^\star) &= -\mathrm{sres}_{\bar{z}}(f)^\star && \text{if } \theta = \mathrm{id}_K \\ &= -Z(X)^{-2}\cdot \mathrm{sres}_{\bar{z}}(f)^\star && \text{otherwise} \end{aligned}$$

(where the skew residues are computed according to the corresponding choices of admissible isomorphisms).

Before giving the proof of Theorem 4.7, we record the following lemma.

Lemma 4.8. *We keep the assumptions of Theorem 4.7. Set $N = Z(X) - z$ and let $S \in \mathcal{A}^+/N\mathcal{A}^+[\![T]\!]$ be a series with constant term 0. Let :*

$$\begin{array}{rccc} \psi : & \mathcal{A}^+/N\mathcal{A}^+(\!(T)\!) & \longrightarrow & \mathcal{A}^+/N\mathcal{A}^+(\!(T)\!) \\ & \displaystyle\sum_i a_i T^i & \mapsto & \displaystyle\sum_i a_i S^i. \end{array}$$

For all $f \in \mathcal{A}^+/N\mathcal{A}^+(\!(T)\!)$, we have the formula :

$$\operatorname{res}\left(\psi(f)\frac{\partial S}{\partial T}\right) = \operatorname{res}(f),$$

where res *is the application selecting the coefficient in T^{-1}.*

Proof. If $f \in \mathcal{A}^+/N\mathcal{A}^+[\![T]\!]$, both sides of the formula vanish and the lemma holds. As res and ψ are K-linear, it is enough to verify the lemma when $f = T^i$ for $i < 0$. Then, the formula becomes $\operatorname{res}\big(S^i \frac{\partial S}{\partial T}\big) = \operatorname{res}(T^i)$, which is a direct consequence of the classical formula of change of variables for residues. □

Proof of Theorem 4.7. We consider a z-admissible isomorphism:

$$\tau_z : \varprojlim_{m>0} \mathcal{A}^+/N^m\mathcal{A}^+ \xrightarrow{\sim} (\mathcal{A}^+/N\mathcal{A}^+)[\![T]\!].$$

Conjugating it by the duality on both sides, we end up with a second isomorphism:

$$\tau_z^\star : \varprojlim_{m>0} \mathcal{A}^+/N^{\star m}\mathcal{A}^+ \xrightarrow{\sim} (\mathcal{A}^+/N^\star\mathcal{A}^+)[\![T]\!].$$

Write $S = -T$ if $\theta = \mathrm{id}_K$ and $S = \frac{-z^2T}{1+zT}$ otherwise. If ψ is the corresponding morphism of Lemma 4.8, an easy computation shows that $\tau_{\bar{z}} = \psi \circ \tau_z^\star$ is $\bar{z}$-admissible. Theorem 4.7 now follows from Lemma 4.8 after noticing that $\frac{\partial S}{\partial T} = -1$ if $\theta = \mathrm{id}_K$ and:

$$\frac{\partial S}{\partial T} = -\frac{z^2}{(1+zT)^2} = \tau_{\bar{z}}\big(-Z(X)^{-2}\big)$$

otherwise. □

5 Duals of linearized Reed-Solomon codes

After all the preparations achieved in the previous sections, we are finally ready to give an explicit construction of the duals of the Martínez-Peñas' linearized Reed-Solomon codes.

We come back to the setting of §1.3: in addition of K, θ and δ, we consider a positive integer m, a tuple $\underline{c} = (c_1, \dots, c_m)$ of unramified elements of K and another tuple $\underline{V} = (V_1, \dots, V_m)$ of F-linear subspaces of K. For each index i, we set $z_i = v(c_i)$. We always assume that the z_i's are pairwise distinct. We

further define $N_i = Z(X) - z_i \in \mathcal{Z}^+$ and $N = \prod_{i=1}^m N_i \in \mathcal{Z}^+$. For simplicity, we also write:

$$\begin{aligned}
\mathrm{Hom}_F(\underline{V}, K) &= \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K),\\
\mathrm{Hom}_F(K/\underline{V}, K) &= \mathrm{Hom}_F(K/V_1, K) \times \cdots \times \mathrm{Hom}_F(K/V_m, K),\\
\mathrm{Hom}_F(K/\underline{V}^\perp, K) &= \mathrm{Hom}_F(K/V_1^\perp, K) \times \cdots \times \mathrm{Hom}_F(K/V_m^\perp, K).
\end{aligned}$$

It follows from Lemma 4.2 that the formula:

$$\big\langle (\varphi_1, \ldots, \varphi_m), (\psi_1, \ldots, \psi_m) \big\rangle = \sum_{i=1}^m \mathrm{Tr}(\varphi_i^\star \circ \psi_i)$$

defines a perfect F-bilinear pairing between the spaces $\mathrm{Hom}_F(K/\underline{V}^\perp, K)$ and $\mathrm{Hom}_F(\underline{V}, K)$. For any K-linear code in $\mathrm{Hom}_F(\underline{V}, K)$, we let $C^\perp$ denote its orthogonal in $\mathrm{Hom}_F(K/\underline{V}^\perp, K)$. From Lemma 4.4, we derive that $C^\perp$ is a K-linear code of same length and complementary dimension.

Our aim is to give an alternative description of the code $\mathrm{LRS}(k, \underline{c}, \underline{V})^\perp$ which sits inside $\mathrm{Hom}_F(K/\underline{V}^\perp, K)$.

5.1 Linearized Goppa codes

In this subsection, we introduce a new family of codes for the sum-rank metric constructing by taking residues, that we call linearized Goppa codes. We then prove that they those codes are isomorphic to some linearized Reed-Solomon codes. We keep the notations $\mathcal{A}^+$, $\mathcal{Z}^+$, $\mathcal{A}$, $\mathcal{Z}$, *etc.* of the previous sections. Let D be the monic polynomial attached to the c_i's and V_i's by the result of Theorem 1.14.(2).

Lemma 5.1. *Let $f \in \mathcal{A}^+ D^{-1}$. Then, for all $i \in \{1, \ldots, m\}$, f has at most a simple pole at z_i and $\mathrm{ev}_{c_i}(\mathrm{sres}_{z_i}(f))$ vanishes on V_i.*

Proof. We write $f = gD^{-1}$ for some $g \in \mathcal{A}^+$. By theorem 1.14, there exists $D' \in \mathcal{A}^+$ such that $N = D'D$. Thus, $f = gD'N^{-1}$ and the first assertion of the lemma follows. Fix $i \in \{1, \ldots, m\}$ and let $\hat{N}_i$ be the multiplicative inverse of N/N_i in $\mathcal{Z}^+/N_i\mathcal{Z}^+ \subset \mathcal{A}^+/N_i\mathcal{A}^+$. Then $\mathrm{sres}_{z_i}(f)$ is the image of $g\hat{N}_i D' \in \mathcal{A}^+/N_i\mathcal{A}^+$. Applying ev_{c_i}, we obtain:

$$\mathrm{ev}_{c_i}(\mathrm{sres}_{z_i}(f)) = \mathrm{ev}_{c_i}(g\hat{N}_i) \circ \mathrm{ev}_{c_i}(D').$$

On the other hand, we deduce from $N = D'D$ that $\mathrm{ev}_{c_i}(D') \circ \mathrm{ev}_{c_i}(D) = 0$ and so that $\mathrm{ev}_{c_i}(D')$ vanishes on $V_i = \mathrm{im}\,\mathrm{ev}_{c_i}(D)$. Therefore $\mathrm{ev}_{c_i}(\mathrm{sres}_{z_i}(f))$ vanishes on V_i as well and the lemma is proved. □

We consider the K-linear map:

$$\begin{array}{rccl}
\gamma_{\underline{c},\underline{V}}: & \mathcal{A} & \to & \mathrm{Hom}_F(K/\underline{V}, K)\\
& f & \mapsto & \big(\mathrm{ev}_{c_1}(\mathrm{sres}_{z_1}(f)), \ldots, \mathrm{ev}_{c_m}(\mathrm{sres}_{z_m}(f))\big).
\end{array}$$

This mapping depends *a priori* on choices of z_i-admissible morphisms but it follows from Lemma 5.1 that the restriction of $\gamma_{\underline{c},\underline{V}}$ to $\mathcal{A}^+D^{-1}$ is independant from any choice. We notice that its restriction to $\mathcal{Z}$ is also uniquely determined because the TS_{z_i}'s have to agree with the usual Taylor expansion on the centre. As a conclusion, the values of $\gamma_{\underline{c},\underline{V}}$ on $\mathcal{Z}\mathcal{A}^+D^{-1}$ are determined without ambiguity.

Definition 5.2. We set $n = \sum_{i=1}^{m} \dim_F K/V_i$ and consider a positive integer $k < n$. The *linearised Goppa code* attached to the parameters $(k, \underline{c}, \underline{V})$ is:

$$\mathrm{LG}(k, \underline{c}, \underline{V}) = \gamma_{\underline{c},\underline{V}}\big(\mathcal{A}^+_{<k} \cdot P\big)$$

where $\mathcal{A}^+_{<k}$ is the subspace of $\mathcal{A}^+$ consisting of Ore polynomials of degree strictly less than k and where $P \in \mathcal{Z}\mathcal{A}^+D^{-1}$ is defined by:

$$\begin{aligned} P &= D^{-1} && \text{if } \theta = \mathrm{id}_K \\ &= Z(X)^{-m-1}(X+a)^{n-k}D^{-1} && \text{if } \theta \neq \mathrm{id}_K \text{ and } \delta = a\delta_0. \end{aligned}$$

We now want to relate linearized Goppa codes to linearized Reed-Solomon codes. As in the proof of Lemma 5.1, we pick a Ore polynomial D' such that $D'D = DD' = N$ and define $\hat{N}_i$ as the multiplicative inverse of N/N_i in $\mathcal{Z}^+/N_i\mathcal{Z}^+$. We set $\tilde{\tau}_i = \varepsilon_{c_i}(PN_i)$ where P is the Ore polynomial of Definition 5.2; note that $\tilde{\tau}_i$ is well-defined because PN_i has no pole at $z_i = \upsilon(c_i)$. Noticing that $N_i \equiv D\hat{N}_iD' \pmod{N_i^2}$, we find $\tilde{\tau}_i = \varepsilon_{c_i}(PD) \circ \varepsilon_{c_i}(\hat{N}_iD')$, from what we deduce that $\tilde{\tau}_i$ vanishes on $V_i = \mathrm{im}\ \mathrm{ev}_{c_i}(D)$. Therefore $\tilde{\tau}_i$ induces a surjective F-linear morphism $\tau_i : K/V_i \to W_i$ where $W_i = \mathrm{im}\,\tilde{\tau}_i$.

Lemma 5.3. *For all $i \in \{1, \ldots, m\}$, the morphism τ_i is an isomorphism.*

Proof. We have to show that $\ker \tilde{\tau}_i = V_i$. Since PD and $\hat{N}_i$ are invertible in $\mathcal{A}^+/N_i\mathcal{A}^+$, it is enough to prove that $\ker \varepsilon_{c_i}(D') = V_i$. The inclusion $V_i \subset \ker \varepsilon_{c_i}(D')$ has been already noticed in the proof of Lemma 5.1. On the other hand, the first part of Theorem 1.14 shows that:

$$\sum_{i=1}^{m} \dim_F \ker \varepsilon_{c_i}(D') \leq \deg D' = \deg N - \deg D = \sum_{i=1}^{m} \dim_F V_i.$$

The lemma follows by comparing dimensions. □

We now define $\underline{W} = (W_1, \ldots, W_m)$ and:

$$\begin{array}{rccc} \Psi : & \mathrm{Hom}_F(\underline{W}, K) & \longrightarrow & \mathrm{Hom}_F(K/\underline{V}, K) \\ & (\varphi_1, \ldots, \varphi_m) & \mapsto & (\varphi_1 \circ \tau_1, \ldots, \varphi_m \circ \tau_m) \end{array}$$

Given that the τ_i's are all isomorphisms, we deduce that Ψ is an isomorphism. Moreover, since composing by an isomorphism obviously preserves the rank, Ψ preserves the sum-rank weight and the sum-rank distance.

Theorem 5.4. *With the above notations, the map Ψ induces an isomorphism of codes between* $\mathrm{LRS}(k, \underline{c}, \underline{W})$ *and* $\mathrm{LG}(k, \underline{c}, \underline{V})$.

Proof. This follows from the relation $\varepsilon_{c_i}(\mathrm{sres}_{z_i}(f)) = \varepsilon_{c_i}(g) \circ \tilde{\tau}_i$ which holds true for any $f \in \mathcal{A}^+P$ in all cases. □

Corollary 5.5. *Let k, $\underline{c}$ and $\underline{V}$ as in Definition 5.2 and assume that the $\upsilon(c_i)$'s are pairwise distinct. Then:*

- *the length of $LG(k, \underline{c}, \underline{V})$ is $n = \sum_{i=1}^{m} \dim_F K/V_i$,*
- *its dimension is k,*
- *its minimal sum-rank distance is $d = n - k + 1$.*

In particular, the code $LG(k, \underline{c}, \underline{V})$ is MSRD.

Proof. This is a direct consequence of Theorem 5.4 and Theorem 1.18. □

5.2 The duality theorem

We are finally ready to state and prove our main duality theorem. We recall that, for an unramified element $c \in K$, we have defined in §4.2:

$$\begin{aligned} c^\vee &= -c && \text{if } \theta = \mathrm{id}_K \\ &= \tfrac{1}{c+a} - a && \text{if } \theta \neq \mathrm{id}_K \text{ and } \delta = a\delta_0. \end{aligned}$$

Theorem 5.6. *Let k and m be two positives integers. Let $\underline{c} = (c_1, \dots, c_m)$ be a tuple of m unramified elements of K such that the $v(c_i)$'s are pairwise distinct. Let $\underline{V} = (V_1, \dots, V_m)$ be a tuple of F-linear subspace of K. We set $n = \dim_F \underline{V}$ and we suppose $k \leqslant n$. Then:*

$$\mathrm{LRS}(k,\, \underline{c},\, \underline{V})^\perp \;=\; \mathrm{LG}(n{-}k,\, \underline{c}^\vee,\, \underline{V}^\perp)$$

where $\underline{c}^\vee = (c_1^\vee, \dots, c_m^\vee)$ and $\underline{V}^\perp = (V_1^\perp, \dots, V_m^\perp)$.

Proof. Since the dimensions of $\mathrm{LRS}(k, \underline{c}, \underline{V})$ and $\mathrm{LG}(n{-}k, \underline{c}^\vee, \underline{V}^\perp)$ sum up to n, it is enough to prove that $\langle \underline{\varphi}, \underline{\psi} \rangle = 0$ for all $\underline{\varphi} \in \mathrm{LRS}(k, \underline{c}, \underline{V})$ and for all $\underline{\psi} \in \mathrm{LG}(n{-}k, \underline{c}^\vee, \underline{V}^\perp)$. For simplicity, we write $\rho = \mathrm{ev}_{\underline{c},\underline{V}}$ (see Definition 1.16) and $\gamma = \gamma_{\underline{c}^\vee, \underline{V}^\perp}$. We have to prove that $\langle \gamma(f), \rho(g) \rangle = 0$ for $f \in \mathcal{A}^+_{<n-k} P$ and $g \in \mathcal{A}^+_{<k}$ where P is the Ore polynomial introduced in Definition 5.2 (for the parameters $\underline{c}^\vee$ and $\underline{V}^\perp$). We compute:

$$\langle \gamma(f), \rho(g) \rangle = \sum_{i=1}^m \mathrm{Tr}\big(\gamma(f)^\star \circ \rho(g)\big) = \sum_{i=1}^m \mathrm{Tr}\big(\varepsilon_{c_i^\vee}(\mathrm{sres}_{\bar{z}_i}(f))^\star \circ \varepsilon_{c_i}(g)\big) \qquad (14)$$

where we have set $\bar{z}_i = v(c_i^\vee)$. We recall that $\bar{z}_i = -z_i$ if $\theta = \mathrm{id}_K$ and $\bar{z}_i = z_i^{-1}$ otherwise (the assumption that c_i is unramified indicates that z_i cannot vanish in the latter case). From Theorems 4.6 and 4.7, we deduce that:

$$\varepsilon_{c_i^\vee}\big(\mathrm{sres}_{\bar{z}_i}(f)\big)^\star = \varepsilon_{c_i}\big(\mathrm{sres}_{\bar{z}_i}(f)^\star\big) = \varepsilon_{c_i}\big(u \cdot \mathrm{sres}_{z_i}(f^\star)\big)$$

where the multiplicative prefactor u is -1 when $\theta = \mathrm{id}_K$ and $-Z(X)^2$ otherwise. On the other hand, since $f^\star$ has at most a simple pole at z_i and u has no pole at z_i, we have $\mathrm{sres}_{z_i}(u \cdot f^\star) = u \cdot \mathrm{sres}_{z_i}(f^\star)$. Therefore, we conclude that:

$$\varepsilon_{c_i^\vee}\big(\mathrm{sres}_{\bar{z}_i}(f)\big)^\star = \varepsilon_{c_i}\big(\mathrm{sres}_{z_i}(uf^\star)\big)$$

and plugging this into Eq. (14), we obtain:

$$\begin{aligned} \langle \gamma(f), \rho(g) \rangle &= \sum_{i=1}^m \mathrm{Tr}\big(\varepsilon_{c_i}(\mathrm{sres}_{z_i}(uf^\star)) \circ \varepsilon_{c_i}(g)\big) \\ &= \sum_{i=1}^m \mathrm{Tr}\big(\varepsilon_{c_i}(\mathrm{sres}_{z_i}(uf^\star) \cdot g)\big) = \sum_{i=1}^m \mathrm{Tr}\big(\varepsilon_{c_i}(\mathrm{sres}_{z_i}(uf^\star g)\big). \end{aligned}$$

since again $f^\star$ has at most a simple pole at z_i and g has no pole at z_i. Now using Theorem 2.6, we end up with:

$$\langle \gamma(f), \rho(g) \rangle = \sum_{i=1}^m T_{\mathrm{rd}}\big(\mathrm{sres}_{z_i}(uf^\star g)\big).$$

We write $f = f_0 P$ where f_0 is a Ore polynomial of degree at most $n-k-1$ and we consider D' such as $D'D = N$. We have:

$$\begin{aligned} uf^\star g = uP^\star f_0^\star g &= \frac{(D')^\star \cdot f_0^\star \cdot g}{N^\star} && \text{if } \theta = \mathrm{id}_K \\ &= \frac{(D')^\star \cdot Z(X)^{m-1} \cdot X^{-k} \cdot f_0^\star \cdot g}{N^\star} && \text{otherwise.} \end{aligned}$$

When $\theta = \mathrm{id}_K$, the numerator $(D')^\star \cdot f_0^\star \cdot g$ is a Ore polynomial of degree at most $ms-2$ (where we recall that $s = [K : F]$) and it then follows from the skew residue formula (Theorem 3.12) that $\langle \gamma(f), \rho(g) \rangle$ vanishes. Similarly, if $\theta \neq \mathrm{id}_K$, we find that the numerator has only terms in $(X+a)^i$ with i in the range $(-s, (m-1)s)$ and deduce from this that the skew residues of $uf^\star g$ at 0 and ∞ both vanish. Hence the skew residue formula (see [7, Theorem 3.2.1]) also implies the vanishing of $\langle \gamma(f), \rho(g) \rangle$ in this case. □

References

[1] W. Arriagada, H. Ramírez, *Centers of skew polynomial rings*, Publ. Inst. Math. **97(111)** (2015), 181–186

[2] D. Augot, P. Loidreau, G. Robert, *Generalized Gabidulin codes over fields of any characteristic*, Designs, Codes and Crypto. **86** (2018), 1807–1848

[3] M. Brešar, C. Hanselka, I. Klep, J. Volčič, *Skolem-Noether algebras*, J. Algebra **498** (2018), 294–314

[4] D. Boucher, F. Ulmer, *Coding with skew polynomial rings*, J. Symbolic Comput. **44** (2009), 1644–1656

[5] D. Boucher, F. Ulmer, *Linear codes using skew polynomials with automorphisms and derivations* Designs, Codes and Crypto. **70** (2014), 405–431

[6] E. Byrne, H. Gluesing-Luerssen, A. Ravagnani, *Fundamental Properties of Sum-Rank Metric Codes*, in IEEE Transactions on Information Theory, to appear

[7] X. Caruso, *A theory of residues for skew rational functions*, J. Éc. polytech. **8** (2021), 1159–1192

[8] P. M. Cohn, *Free Rings and Their Relations*, London Math. Soc. Monographs, Academic Press (1971)

[9] P. Delsarte, *Bilinear Forms over a Finite Field with Applications to Coding Theory*, J. Combin. Theory **25** (1978), 226–241

[10] E. Gabidulin, *Theory of codes with maximum rank distance*, Problemy Peredachi Informatsii **21** (1985), no. 1, 3–16

[11] N. Jacobson, *Abstract derivation and Lie algebras*, Trans. Amer. Math. Soc. **42** (1937), 206–224.

[12] N. Jacobson, *Pseudo-linear transformations*, Ann. Math. **38** (1937), 484–507

[13] N. Jacobson, *Finite-Dimensional Division Algebras Over Fields*, Grundlehren der Mathematischen Wissenschaften Series (1996), Springer

[14] T. Y. Lam., *A general theory of Vandermonde matrices*, Expositiones Mathematicae **4** (1986), 193–215

[15] A. Leroy, *Pseudo linear transformations and evaluation in Ore extensions*, Bull. Soc. Math. Belg. **2** (1995), 321–347

[16] S. Liu, *Generalized Skew Reed-Solomon Codes and Other Applications of Skew Polynomial Evaluation*, PhD thesis (2016), available at https://tspace.library.utoronto.ca/bitstream/1807/73073/1/Liu_Siyu_201606_PhD_thesis.p

[17] H.-F. Lu, P. Kumar, *A unified construction of space-time codes with optimal rate-diversity tradeoff*, IEEE Trans. Inform. Theory **51** (2005), 1709–1730

[18] U. Martínez-Peñas, *Skew and linearized Reed-Solomon codes and maximum sum rank distance codes over any division ring*, J. Algebra **504** (2018), 587–612

[19] U. Martínez-Peñas, F. Kschischang, *Reliable and Secure Multishot Network Coding using Linearized Reed-Solomon Codes*, IEEE Trans. Inform. Theory **65** (2019), 4785–4803

[20] U. Martínez-Peñas, *Theory of supports for linear codes endowed with the sum-rank metric*, Designs, Codes and Crypto. **87** (2019), 2295–2320

[21] C. Ott, S. Puchinger, M. Bossert, *Bounds and Genericity of Sum-Rank-Metric Codes*, preprint (2021), available at https://arxiv.org/abs/2102.02244

[22] S. Puchinger, J. Renner, J. Rosenkilde *Generic Decoding in the Sum-Rank Metric*, in IEEE International Symposium on Information Theory (2021), 54–59

[23] R. Roth, *Maximum-Rank Array Codes and their Application to Crisscross Error Correction*, IEEE Trans. Inform. Theory (1991)

[24] D. Silva, F. Kschischang, R. Kötter, *A rank-metric approach to error control in random network coding*, IEEE Trans. Info. Theory **54** (2008), 3951–3967

[25] M. Tsfasman, S. Vlăduţ, D. Nogin, *Algebraic Geometric Codes: Basic Notions*, Mathematical Surveys and Monographs **139** (2007), 338 pp