ALGEBRAIC GEOMETRY CODES IN THE SUM–RANK METRIC

ELENA BERARDINI

Eindhoven University of Technology, The Netherlands

XAVIER CARUSO

CNRS; IMB, Université de Bordeaux, 351 cours de la Libération, 33405 Talence, France

ABSTRACT. We introduce the first geometric construction of codes in the sum-rank metric, which we called linearized Algebraic Geometry codes, using quotients of the ring of Ore polynomials with coefficients in the function field of an algebraic curve. We study the parameters of these codes and give lower bounds for their dimension and minimum distance. Our codes exhibit quite good parameters, respecting a similar bound to Goppa's bound for Algebraic Geometry codes in the Hamming metric.

CONTENTS

INTRODUCTION

Linear codes in the Hamming metric have been playing a central role in the theory of error correction since the 50's. Codes in the rank metric, firstly introduced by Delsarte for combinatorial interest [Del78], were rediscovered in the last 20 years in the context of network coding and, in general, of error correction. Codes in the sum-rank metric were introduced more recently. They can be defined as follows. Let k be a field. For an integer

E-mail addresses: `elena_berardini@hotmail.it`, `xavier.caruso@normalesup.org`.

Key words and phrases. sum-rank metric codes, algebraic curves, function fields, Ore polynomials, finite fields.

s, let $\underline{V} = (V_1, \ldots, V_s)$ and $\underline{W} = (W_1, \ldots, W_s)$ be two s-uples of k-vector spaces. Write $n_i = \dim_k V_i$ and $m_i = \dim_k W_i$. Let $\mathrm{Hom}_k(W_i, V_i)$ denote the space of k-linear morphisms from W_i to V_i. We set

$$\mathrm{Hom}_k(\underline{W}, \underline{V}) := \mathrm{Hom}_k(W_1, V_1) \times \cdots \times \mathrm{Hom}_k(W_s, V_s).$$

This is a vector space over k of dimension $\sum_{i=1}^{s} m_i n_i$.

Definition. Let $\underline{\varphi} = (\varphi_1, \ldots, \varphi_s) \in \mathrm{Hom}_k(\underline{W}, \underline{V})$. The sum-rank weight of $\underline{\varphi}$ is defined as

$$w_{\mathrm{srk}}(\underline{\varphi}) := \sum_{i=1}^{s} \mathrm{rk}(\varphi_i) = \sum_{i=1}^{s} \dim_k \varphi_i(W_i).$$

The sum-rank distance between $\varphi, \psi \in \mathrm{Hom}_k(\underline{V}, \underline{W})$ is

$$d_{\mathrm{srk}}(\underline{\varphi}, \underline{\psi}) := w_{\mathrm{srk}}(\underline{\varphi} - \underline{\psi}).$$

Definition. A code $\mathcal{C}$ in the sum-rank metric is a k–linear subspace of $\mathrm{Hom}_k(\underline{V}, \underline{W})$ endowed with the sum-rank distance. By defintion, its *length* n is $\sum_{i=1}^{s} m_i n_i$. Its *dimension* δ is $\dim_k \mathcal{C}$. Its *minimum distance* is

$$d := \min \left\{ w_{\mathrm{srk}}(\underline{\varphi}) \mid \underline{\varphi} \in \mathcal{C}, \underline{\varphi} \neq \underline{0} \right\}.$$

When $n_i = m_i = 1$ for all $i \in \{1, \ldots, s\}$, the previous definition reduces to codes of length s with the Hamming metric and, in the case where $s = 1$, to rank-metric codes. However, the sum-rank metric does not reduce to a mere generalization of the two aforementioned metrics. For instance, codes in the sum-rank metric offer a solution to problems in multi-shot linear network coding, space-time coding, and distributed storage. We refer the reader to [MPSK22] for a detailed introduction to the theory of sum-rank metric codes and their applications.

An important case of interest occurs when we are given a finite extension ℓ of k of degree r, and we set $V_i = \ell$ for every i. In this case, $n_i = r$ for all i and the ambient space $\mathrm{Hom}_k(\underline{W}, \ell)$ is itself a vector space over ℓ. We are then more particularly interested in ℓ–linear codes which are, by definition, ℓ–linear subspaces $\mathcal{C} \subset \mathrm{Hom}_k(\underline{W}, \ell)$. Consequently, we define ℓ–variants of the parameters: the ℓ–length of $\mathcal{C}$ is $n_\ell := \sum_{i=1}^{s} m_i$, the ℓ–dimension of $\mathcal{C}$ is $\delta_\ell := \dim_\ell \mathcal{C}$, and the minimal distance d of $\mathcal{C}$ stays unchanged. Those three main parameters are related by the equivalent of the Singleton bound in the Hamming metric, that in the aforementioned setting writes $d + \delta_\ell \leq n_\ell + 1$ [MP18, Prop. 34]. Codes with parameters attaining this bound are called *Maximum Sum-Rank Distance (MSRD)*.

Among the most used families of linear codes in the Hamming metric are the Reed–Solomon codes [RS60]. They have parameters attaining the Singleton bound, and benefit from efficient decoding algorithms. The counterpart of Reed–Solomon codes in the rank metric are Gabidulin codes [Gab85], and linearized Reed–Solomon codes in the sum-rank metric [MP18]. These codes have parameters attaining the analogue of the Singleton Bound in their respective metric, and benefit from efficient decoding algorithms derived from the ones for Reed–Solomon codes [Loi06, PWZ16, CD18].

The main drawback of Reed–Solomon codes is that the storage size of the coordinates of the vectors increases logarithmically with the number of coordinates: in order to have *long* Reed–Solomon codes, one must work over *large* finite fields. The so-called Algebraic Geometry (AG) codes, introduced by V. D. Goppa [Gop82], generalize Reed–Solomon codes and benefit from similar properties, while being free of this limitation. AG codes are constructed by evaluating spaces of functions at rational points on algebraic curves. Since a curve of genus g defined over the finite field $\mathbb{F}_q$ can have up to $q+1+2g\sqrt{q}$ rational points by the Hasse–Weil bound, the construction proposed by Goppa yields codes that are generally longer than the Reed–Solomon codes, and thus allows to work on smaller finite fields. AG codes became particularly famous when Tsfasman, Vlăduţ, and Zink [TVZ82] used them with modular curves to construct codes with better asymptotic performances than random codes.

Motivations. In contrast with the situation of codes in the Hamming metric, only a few constructions of codes are known in the rank and the sum-rank metric. In particular, no geometric construction has been proposed in these two metrics so far. Furthermore, MSRD codes, such as linearized Reed–Solomon codes, suffer from the same limitation as Reed–Solomon codes. Indeed, keeping the same notation as before, and denoting by q the cardinality of k, in [BGLR21, Thm. 6.12] it is shown that if $\mathcal{C} \subseteq \mathrm{Hom}_k(\underline{W}, \ell)$ is a MSRD code with minimum distance $d \leq r+2$, then $s \leq q+1$ if $r=1$ and $s \leq q$ otherwise. Furthermore, for MSRD codes of ℓ–dimension 2, we have a similar bound, that we prove now.

Remark. To avoid heavy notations in the following lemma we assume $W_i = \ell$ for every i, and consider $\mathcal{C}$ to be a ℓ-subspace of $\mathrm{End}_k(\ell)^s$ instead of $\mathrm{Hom}_k(\underline{W}, \ell)$. However, our proof can be easily generalised to the latter.

Lemma. *Let $\mathcal{C} \subseteq \mathrm{End}_k(\ell)^s$ be a code in the sum-rank metric of ℓ-dimension 2 and of minimum distance $rs-1$. Then, if $r=1$ we have $s \leq q+1$, otherwise we have $s \leq q-1$.*

Proof. We consider a ℓ-basis of $\mathcal{C}$, say $(f_1, \dots, f_s), (g_1, \dots, g_s)$ with f_i and g_i k-linear endomorphisms of ℓ. For any $i \in \{1, ..., s\}$ and any $x \in \ell^\times := \ell \setminus \{0\}$, we define the following element of $\mathbb{P}^1(\ell)$:

$$v_{i,x} := [f_i(x) : g_i(x)].$$

It is easy to check that for any $a \in k^\times$, we have $v_{i,x} = v_{i,ax}$.

Let us prove that for $i, j \in \{1, \dots, s\}$ and $x, y \in \ell^\times$, we have $v_{i,x} \neq v_{j,y}$, unless $i=j$ and x and y are k-collinear. Indeed, suppose that $v_{i,x} = v_{j,y}$. Then, by construction, the vectors $(f_i(x), g_i(x))$ and $(f_j(y), g_j(y))$ are collinear. Thus, there exist u, v, not both zero, such that

$$(uf_i + vg_i)(x) = 0,$$
$$(uf_j + vg_j)(y) = 0.$$

If $i \neq j$, then $uf_i + vg_i$ and $uf_j + vg_j$ are both of rank smaller than r, hence $w_{srk}\left((uf_h + vg_h)_{h \in \{1,\dots,s\}}\right) \leq rs-2$, which contradicts the assumption on the minimum distance of $\mathcal{C}$. Similarly, if $i=j$, but x is not k-collinear to y, then we deduce that $uf_i + vg_i$

is of rank at most $r-2$, which again contradicts the hypothesis on the minimum distance of $\mathcal{C}$. In conclusion, we must have $i = j$ and $x \equiv y \pmod{k}$. We infer that the number of pairs (i, x) with $x \pmod{k} \in \ell^\times$ is at most equal to the cardinal of $\mathbb{P}^1(\ell)$, *i.e.*

$$s\frac{q^r - 1}{q-1} \leq q^r + 1,$$

and hence we have

$$s \leq (q-1)\frac{q^r+1}{q^r-1}. \tag{1}$$

Since s is necessarily an integer, this implies $s \leq q-1$ when $q^r > 2q-1$, which happens as soon as $r > 1$. If $r = 1$, then Equation (1) gives $s \leq q+1$. □

Remark. A bound similar to the one stated in the previous lemma can be retrieved using [BGLR21, Thm. 6.12] on the dual of the MSRD code of dimension 2. However, this would give a slightly worse bound, that is $s \leq q$ instead of $s \leq q-1$, when $r > 1$. Furthermore, our proof makes use of completely different techniques than the ones developed in the aforementioned paper, and we therefore believe it is of interest on itself.

Our contribution. In this paper we present the first geometric construction of codes in the sum-rank metric, from algebraic curves, that we call *linearized Algebraic Geometry codes*.

Gabidulin and linearized Reed–Solomon codes are constructed using so-called linearized polynomials and Ore polynomials, as introduced by Ore in 1933 [Ore33]. Taking inspiration from the approach of [MS98], where the authors propose a construction of AG codes in the Hamming metric using division algebras over the function field of a curve, in this paper we work with algebras obtained as quotient of rings of Ore polynomials. We develop the theory of Riemann–Roch spaces over Ore polynomials rings with coefficients in the function field of a curve, by exploiting the classical theory of divisors and Riemann–Roch spaces on algebraic curves. On the one hand, this allows us to propose an explicit construction of geometric codes in the sum-rank metric from curves. On the other hand, we can exploit our theory to study the parameters of these new codes.

The geometric codes that we propose are in general longer than linearized Reed–Solomon codes, and have parameters that turn out to respect a similar bound to Goppa's bound for AG codes in the Hamming metric.

Organisation of the paper. Section 1 is devoted to the background on the rings of Ore polynomials and to the proofs of some results on the algebras obtained as quotients of the ring of Ore polynomial. In Section 2, after recalling some general notions on algebraic curves and their function fields, we present the theory of Riemann–Roch spaces over the rings of Ore polynomials with coefficients in the function field of a curve, and we prove a bound on their dimension using the classical Riemann–Roch theorem. In Section 3, we construct linearized Algebraic Geometry codes, and study their parameters. When considering the case of curves of genus 0, we retrieve linearized Reed–Solomon codes. Finally, Section 4 serves as a general conclusion in which we compare our results with those of [MS98], and discuss several perspectives.

1. Ore polynomial rings

Throughout this section, we fix three positive integers r, d and m such that $r = md$. We consider a field K, together with a Galois extension L_0/K such that $\mathrm{Gal}(L_0|K) \simeq \mathbb{Z}/d\mathbb{Z}$. We denote by Φ_0 a generator of the former Galois group. We set $L := L_0^m$ and embed K and L_0 diagonally into L. We define

$$\Phi : L \to L, \quad (a_1, \dots, a_m) \mapsto \big(\Phi_0(a_m), a_1, \dots, a_{m-1}\big).$$

It is easy to check that Φ has order r, and that an element $x \in L$ is a fixed point of Φ if and only if x lies in K. Besides, an element $a = (a_1, \dots, a_m) \in L$ is invertible if and only if $a_i \neq 0$ for all i. We write $L^\times$ for the subset of invertible elements of L.

We denote by $N_{L_0/K} : L_0 \to K$ the norm map of L_0 over K and similarly, for $a = (a_1, \dots, a_m) \in L$, we set

$$N_{L/K}(a) := N_{L_0/K}(a_1) \cdot N_{L_0/K}(a_2) \cdots N_{L_0/K}(a_m).$$

This defines a multiplicative function $N_{L/K} : L \to K$ which sends $L^\times$ to $K^\times := K \setminus \{0\}$.

The goal of the rest of the section is to present some results from the standard theory of central simple algebras. A classical reference in this context is [Rei75]. Here we present the results in our setting, that is for the ring of Ore polynomials, which allows us to give more concise proofs.

1.1. **The algebra $D_{L,x}$.** We let $L[T;\Phi]$ denote the ring of Ore polynomials in the variable T. We recall briefly that elements of $L[T;\Phi]$ are usual polynomials with usual addition; however, the multiplication on $L[T;\Phi]$ is twisted by the rule $T \cdot a = \Phi(a)T$ for all $a \in L$.

Given an element $x \in K$, $x \neq 0$, we define

$$D_{L,x} := L[T;\Phi]/(T^r - x).$$

Since $T^r - x$ commutes with every element in $L[T;\Phi]$, the quotient $D_{L,x}$ inherits a ring structure.

Lemma 1.1. *(i) Let $u \in L^\times$ and write $v = N_{L/K}(u)$. We have an isomorphism of rings*

$$\gamma_u : D_{L,x} \xrightarrow{\sim} D_{L,v^{-1}x}, \quad T \mapsto uT.$$

(ii) When $x = 1$, we have an isomorphism of rings

$$\varepsilon : D_{L,1} \xrightarrow{\sim} \mathrm{End}_K(L), \quad T \mapsto \Phi.$$

Proof. It is easily checked that γ_u is a well-defined ring homomorphism and that $\gamma_{u^{-1}}$ is its inverse. This proves (i). For (ii), we first notice that ε is well-defined, given that Φ has order r. Injectivity boils down to proving that the family $\{\mathrm{Id}, \Phi, \dots, \Phi^{r-1}\}$ is free over L, which is a direct consequence of Artin's theorem on linear independence of characters. Surjectivity follows by comparing dimensions (over K). □

The quotient rings $D_{L,x}$ are equipped with a so-called *reduced norm map* $N_{\mathrm{rd}} : D_{L,x} \to K$ that we define now. For this, we first observe that $D_{L,x}$ is a free L-module of rank r with basis $(1, T, \dots, T^{r-1})$.

Definition 1.2. Let $f \in D_{L,x}$. The reduced norm of f, denoted by $N_{\mathrm{rd}}(f)$, is the determinant of the L-linear map $D_{L,x} \to D_{L,x}$, $g \mapsto gf$.

Concretely, the reduced norm of $f = a_0 + a_1 T + \ldots a_{r-1} T^{r-1} \in D_{L,x}$ is the determinant of the matrix

$$M_f = \begin{pmatrix} a_0 & x\cdot\Phi(a_{r-1}) & \cdots & x\cdot\Phi^{r-1}(a_1) \\ a_1 & \Phi(a_0) & \cdots & x\cdot\Phi^{r-1}(a_2) \\ \vdots & \vdots & & \vdots \\ a_{r-2} & \Phi(a_{r-3}) & \cdots & x\cdot\Phi^{r-1}(a_{r-1}) \\ a_{r-1} & \Phi(a_{r-2}) & \cdots & \Phi^{r-1}(a_0) \end{pmatrix}. \tag{2}$$

One readily checks that

$$\Phi(M_f) = \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ x^{-1} & & & \end{pmatrix} \cdot M_f \cdot \begin{pmatrix} & & & x \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{pmatrix},$$

from what we deduce that $N_{\mathrm{rd}}(f) = \det(M_f)$ is invariant under Φ; hence $N_{\mathrm{rd}}(f) \in K$ as we claimed earlier. Moreover, the reduced norm map behaves well with respect to the isomorphisms γ_u and ε of Lemma 1.1, as showed in the following lemma.

Lemma 1.3. *(i) For $f \in D_{L,x}$ and $u \in L^\times$, we have $N_{\mathrm{rd}}(f) = N_{\mathrm{rd}}(\gamma_u(f))$.*
(ii) For $f \in D_{L,1}$, we have $N_{\mathrm{rd}}(f) = \det(\varepsilon(f))$.

Proof. (i) Write $v = N_{L/K}(u)$ and let μ (resp μ') be the L-linear endomorphism of $D_{L,x}$ (resp. $D_{L,v^{-1}x}$) taking g to gf (resp. to $g\cdot\gamma_u(f)$). The maps μ and μ' are conjugated under the isomorphism γ_u. Hence, their determinants agree, showing that $N_{\mathrm{rd}}(f) = N_{\mathrm{rd}}(\gamma_u(f))$.

(ii) For $f \in L$ (resp. $f \in D_{L,1}$), let μ_f denote the right multiplication by f on L (resp. on $D_{L,1}$). We consider the tensor product $L \otimes_K L$ and view it as a L-vector space by letting L act on the first factor. Since L/K is Galois with cyclic group generated by Φ, it follows from Galois theory that we have a L-linear decomposition

$$\begin{array}{ccc} L \otimes_K L & \xrightarrow{\sim} & L^r \\ x \otimes y & \mapsto & \left(x\cdot\Phi^i(y)\right)_{0 \le i < r}. \end{array}$$

In the corresponding L-basis of $L \otimes_K L$, the matrices of the endomorphisms $1 \otimes \mu_a$ and $1 \otimes \Phi$ are, respectively,

$$\begin{pmatrix} a & & & \\ & \Phi(a) & & \\ & & \ddots & \\ & & & \Phi^{r-1}(a) \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} & & & 1 \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{pmatrix}.$$

Hence, the matrix of the endomorphism $1 \otimes \varepsilon(f)$ is exactly the matrix M_f defined in Equation (2). The equality $N_{\mathrm{rd}}(f) = \det(\varepsilon(f))$ follows. □

1.2. **Over Laurent series rings.** In this subsection, we assume that $K = k(\!(t)\!)$, where k is a field. We write $\mathcal{O}_K := k[\![t]\!]$ and let $v_t : K \to \mathbb{Z} \sqcup \{\infty\}$ be the t-adic valuation on K. The former extends uniquely to a valuation on L_0 that, in a slight abuse of notation, we continue to denote by v_t. Recall that, in full generality, v_t does not take integral values on L_0; more precisely, if e denotes the ramification index of L_0/K, v_t defines a surjective function from L_0 to $\frac{1}{e}\mathbb{Z} \sqcup \{\infty\}$. Note that e divides d and hence r. We write $\mathcal{O}_{L_0}$ for the ring of integers of L_0, that is the subring of L_0 formed by elements with nonnegative valuation.

We recall that we have defined $L = L_0^m$. We set $\mathcal{O}_L := (\mathcal{O}_{L_0})^m$ accordingly. For $j \in \{1, \ldots, m\}$, we consider the function $v_{j,t}$ on L defined by $v_{j,t}(c_1, \ldots, c_m) := v_t(c_j)$ for $c_1, \ldots, c_m \in L_0$. Similarly, for $f = a_0 + a_1 T + \cdots + a_{r-1} T^{r-1} \in D_{L,x}$ (with $a_i \in L$), we set

$$w_{j,x}(f) := \min_{0 \leq i < r} \left(v_{j,t}(a_i) + i \cdot \frac{v_t(x)}{r} \right).$$

This defines a function $w_{j,x} : D_{L,x} \to \frac{1}{r}\mathbb{Z} \sqcup \{\infty\}$ (for $1 \leq j \leq m$). We further define $w_x := \min_{1 \leq j \leq m} w_{j,x}$. Given $f, g \in D_{L,x}$, one checks that:

- $w_{j,x}(f+g) \geq \min\left(w_{j,x}(f), w_{j,x}(g)\right)$ for $1 \leq j \leq m$,
- $w_x(f+g) \geq \min\left(w_x(f), w_x(g)\right)$,
- $w_x(fg) \geq w_x(f) + w_x(g)$,
- $w_x(f) = \infty$ if and only if $f = 0$.

We define $\Lambda_{L,x}$ as the subset of $D_{L,x}$ consisting of elements f for which $w_{j,x}(f) \geq 0$ for all j; it is a subring of $D_{L,x}$.

Lemma 1.4. *Let $u = (u_1, \ldots, u_m) \in L^\times$ and set $y = N_{L/K}(u)^{-1} \cdot x$. Let $\gamma_u : D_{L,x} \to D_{L,y}$ be the isomorphism defined in Lemma 1.1.(i). If $v_t(u_1) = \cdots = v_t(u_m)$, then*

$$w_{j,x}(f) = w_{j,y}(\gamma_u(f))$$

for all $j \in \{1, \ldots, m\}$ and all $f \in D_{L,x}$. In particular, γ_u induces an isomorphism $\Lambda_{L,x} \xrightarrow{\sim} \Lambda_{L,y}$.

Proof. For simplicity, write v for the common value of $v_t(u_1), \ldots, v_t(u_m)$. The relation $y = N_{L/K}(u)^{-1} \cdot x$ then implies that $v_t(y) = v_t(x) - r \cdot v$.

Consider now an element $f = a_0 + a_1 T + \cdots + a_{r-1} T^{r-1} \in D_{L,x}$. By definition,

$$\gamma_u(f) = \sum_{i=0}^{r-1} a_i \, u \, \Phi(u) \cdots \Phi^{i-1}(u) \cdot T^i.$$

For all i and j, we have $v_{j,t}(a_i \, u \, \Phi(u) \cdots \Phi^{i-1}(u)) = v_{j,t}(a_i) + i \cdot v$. Hence

$$\begin{aligned} w_{j,y}(\gamma_u(f)) &= \min_{0 \leq i < r} \left(v_{j,t}(a_i) + i \cdot v + i \cdot \frac{v_t(y)}{r} \right) \\ &= \min_{0 \leq i < r} \left(v_{j,t}(a_i) + i \cdot \frac{v_t(x)}{r} \right) = w_{j,x}(f), \end{aligned}$$

which proves the lemma. $\square$

Proposition 1.5. *Let $m = 1$, L_0/K unramified and $\gcd(v_t(x), r) = 1$. Then, $D_{L,x}$ has no nonzero zero divisor.*

Proof. Let f and g be nonzero elements in $D_{L,x}$. We want to prove that fg cannot vanish. By our assumption on m, we have $v_{1,t} = v_t$ and $w_{1,x} = w_x$. We claim that the minimum in the definition of $w_x(f)$ is reached only once; in other words, if f is written as $f = a_0 + a_1 T + \cdots + a_{r-1} T^{r-1}$ (with $a_i \in L$), there exists a unique index $i_f \in \{0, \ldots, r-1\}$ such that

$$v_t(a_{i_f}) + i_f \cdot \frac{v_t(x)}{r} = w_x(f).$$

Indeed, given that $v_t(a_i)$ is an integer for all i by the assumption on the ramification, such an index i_f has to satisfy the congruence $i_f \cdot v_t(x) \equiv r \cdot w_x(f) \pmod r$. The latter has a unique solution, given that $v_t(x)$ is coprime with r. As a conclusion, we can write $f = c_f T^{i_f} + f_1$ where $c_f \in L$ and $f_1 \in D_{L,x}$ satisfy $w_x(c_f T^{i_f}) = w_x(f)$ and $w_x(f_1) > w_x(f)$.

Similarly, $g = c_g T^{i_g} + g_1$ where i_g is an integer in the range $[0, r)$, and $c_g \in L$ and $g_1 \in D_{L,x}$ are such that $w_x(c_g T^{i_g}) = w_x(g)$ and $w_x(g_1) > w_x(g)$. Computing the product fg, we find

$$fg = c_f\, \Phi^{i_f}(c_g) T^{i_f + i_g} + h_1,$$

with $w_x(h_1) > w_x(f) + w_x(g)$. On the other hand, we have

$$\begin{aligned} w_x\big(c_f\, \Phi^{i_f}(c_g) T^{i_f+i_g}\big) &= v_t\big(c_f\, \Phi^{i_f}(c_g)\big) + (i_f + i_g) \cdot \frac{v_t(x)}{r} \\ &= v_t(c_f) + v_t(c_g) + (i_f + i_g) \cdot \frac{v_t(x)}{r} = w_x(f) + w_x(g). \end{aligned}$$

Therefore $c_f\, \Phi^{i_f}(c_g) T^{i_f+i_g}$ cannot be equal to $-h_1$ (because the valuations differ), showing eventually that $fg \neq 0$, as wanted. □

We now examine the relationships between the valuations and the reduced norm.

Proposition 1.6. *For all $f \in D_{L,x}$, we have $v_t\big(N_{\mathrm{rd}}(f)\big) \geq d \cdot \sum_{j=1}^{m} w_{j,x}(f)$.*

Proof. Write $f = a_0 + a_1 T + \cdots + a_{r-1} T^{r-1}$ with $a_i \in L$. Let M_f be the matrix defined by Equation (2), and, for $1 \leq u, v \leq r$, let $m_{u,v}$ denote its entry in position (u, v). By definition,

$$m_{u,v} = \begin{cases} \Phi^{v-1}(a_{u-v}) & \text{if } u \geq v, \\ x \cdot \Phi^{v-1}(a_{u-v+r}) & \text{otherwise.} \end{cases}$$

We extend the valuation v_t on L by

$$v_t(a) = \frac{1}{m} \sum_{j=1}^{m} v_{j,t}(a) \qquad (a \in L).$$

We observe that v_t agrees on L_0 (embedded diagonally in L) with the valuation v_t we have defined previously; hence no risk of confusion is possible. Additionally, v_t is invariant under Φ. Note, however, that v_t is no longer a group morphism but it only satisfies $v_t(ab) \geq v_t(a) + v_t(b)$ for $a, b \in L$.

From the previous properties, we derive

$$v_t(m_{u,v}) = \begin{cases} v_t(a_{u-v}) & \text{if } u \geq v, \\ v_t(a_{u-v+r}) + v_t(x) & \text{otherwise.} \end{cases}$$

On the other hand, it follows from the definition of $w_{j,x}$ that $v_{j,t}(a_i) \geq w_{j,x}(f) - i \cdot \frac{v_t(x)}{r}$ for all i and j. Summing over j, we get

$$v_t(a_i) \geq \frac{1}{m} \sum_{j=1}^{m} w_{j,x}(f) - i \cdot \frac{v_t(x)}{r},$$

and finally

$$v_t(m_{u,v}) \geq \frac{1}{m} \sum_{j=1}^{m} w_{j,x}(f) + (v - u) \cdot \frac{v_t(x)}{r}$$

for all $u, v \in \{1, \ldots, r\}$. If σ is a permutation of $\{1, \ldots, r\}$, we then find

$$v_t\left(\prod_{u=1}^{r} m_{u,\sigma(u)}\right) \geq d \cdot \sum_{j=1}^{m} w_{j,x}(f) + \frac{v_t(x)}{r} \sum_{u=1}^{r} (\sigma(u) - u).$$

The last sum vanishes given that σ is a permutation. We conclude that

$$v_t\big(N_{\mathrm{rd}}(f)\big) = v_t\big(\det(M_f)\big) \geq d \cdot \sum_{j=1}^{m} w_{j,x}(f),$$

and the proposition is proved. □

To conclude this subsection, we focus on the case $x = 1$. We recall from Lemma 1.1 that we have an isomorphism $\varepsilon : D_{L,1} \to \mathrm{End}_K(L)$, defined by $T \mapsto \Phi$. It follows from the definitions that, when $f \in \Lambda_{L,1}$, the map $\varepsilon(f)$ takes $\mathcal{O}_L$ to itself. Hence ε induces a ring homomorphism $\Lambda_{L,1} \to \mathrm{End}_{\mathcal{O}_K}(\mathcal{O}_L)$. Reducing modulo t on the right hand side, we get a third ring homomorphism $\bar{\varepsilon} : \Lambda_{L,1} \to \mathrm{End}_k(\mathcal{O}_L / t\mathcal{O}_L)$.

Proposition 1.7. *For all $f \in \Lambda_{L,1}$, we have $v_t\big(N_{\mathrm{rd}}(f)\big) \geq \dim_k \ker \bar{\varepsilon}(f)$.*

Proof. Write $\delta = \dim_k \ker \bar{\varepsilon}(f)$, and let $\bar{e}_1, \ldots, \bar{e}_r$ be a k-basis of $\mathcal{O}_L / t\mathcal{O}_L$ such that $\bar{\varepsilon}(\bar{e}_i) = 0$ for $i \in \{1, \ldots, \delta\}$. For $1 \leq i \leq r$, we choose an element $e_i \in \mathcal{O}_L$ whose reduction modulo t is $\bar{e}_i$. By Nakayama's lemma [Eis13, Cor. 4.8], the family $(e_1, \ldots, e_r)$ is a basis of $\mathcal{O}_L$ over $\mathcal{O}_K$. Let M be the matrix of $\varepsilon(f)$ in this basis. It has all entries in $\mathcal{O}_K$, while the first δ columns of M have entries divisible by t by construction. Therefore, $\det(M)$ is divisible by t^δ. Finally, we know from Lemma 1.3 that $N_{\mathrm{rd}}(f) = \det(M)$. The proposition follows. □

2. ALGEBRAIC CURVES

Throughout this section, we let k be a field.

2.1. **Divisors on curves and Riemann–Roch spaces.** In this subsection, we recall some classical definitions and results on algebraic curves, and refer the reader to [Sti09] for a nice exposition of this theory.

We consider a smooth projective irreducible algebraic curve X of genus g_X defined over k and we set $K = k(X)$ to be its function field. We denote by $X^\star$ the set of places (or, equivalently, closed points) of X. Given $\mathfrak{p} \in X^\star$, we let $K_\mathfrak{p}$ be the completion of K at the place $\mathfrak{p}$ [Sti09, §4.2]. It is equipped with the $\mathfrak{p}$-adic valuation $v_\mathfrak{p}$. We denote by $\mathcal{O}_\mathfrak{p}$ its ring of integers and by $k_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{p}$ its residue class field. The *degree* of $\mathfrak{p}$, denoted by $\deg_X(\mathfrak{p})$ in what follows, is by definition the degree of the extension $k_\mathfrak{p}/k$.

Definition 2.1. The divisor group of X, $\mathrm{Div}(X)$, is the free abelian group generated by the places of X. A *divisor* on X is therefore a formal sum

$$D = \sum_{\mathfrak{p}\in X^\star} n_\mathfrak{p}\mathfrak{p} \quad \text{with } n_\mathfrak{p} \in \mathbb{Z} \text{ almost all zero.}$$

The *degree* of D is defined by $\deg_X(D) = \sum_{\mathfrak{p}\in X^\star} n_\mathfrak{p} \deg_X(\mathfrak{p})$ and its *support* is $\mathrm{supp}(E) = \{\mathfrak{p} \in X^\star \mid n_\mathfrak{p} \neq 0\}$. The divisor E is called *effective*, written $E \geq 0$, if $n_\mathfrak{p} \geq 0$ for any $\mathfrak{p}$. Two divisors are added coefficientwise.

The *principal divisor* associated to a rational nonzero function $x \in K$ is

$$(x) = \sum_{\mathfrak{p}\in X^\star} v_\mathfrak{p}(x)\,\mathfrak{p}.$$

Since rational functions in K have the same number of zeros and poles, counted with multiplicity, principal divisors have zero degree.

For a divisor $D \in \mathrm{Div}(X)$, we define the associated Riemann–Roch space as

$$L_X(D) := \{x \in K^\times \mid (x) + D \geq 0\} \cup \{0\}. \tag{3}$$

This is a k-vector space of finite dimension.

Theorem 2.2 (Riemann–Roch theorem)**.** *For any divisor $D \in \mathrm{Div}(X)$ we have*

$$\dim_k L_X(D) = \deg_X(D) + 1 - g_X + \dim_k L_X(K_X - D),$$

where K_X denotes a canonical divisor on X.

2.2. **Riemann–Roch spaces in Ore polynomial rings.** We consider two smooth projective irreducible algebraic curves X and Y defined over k, together with an étale surjective map $\pi : Y \to X$. We assume that π is a Galois cover with cyclic Galois group of order r. Let $K := k(X)$ and $L := k(Y)$ denote the fields of functions of X and Y respectively. The map π induces a ring homomorphism $K \to L$, turning L into an extension of K. Moreover, our assumptions on π ensure that L/K is Galois with cyclic Galois group of order r. For definitions and classical results on Galois covers of curves we refer the reader to [Sti09, Chapter 3].

We denote by $\mathrm{Div}(X)$ and $\mathrm{Div}(Y)$ the group of divisors on X and Y, respectively, and we set $\mathrm{Div}_{\mathbb{Q}}(Y) := \mathrm{Div}(Y) \otimes \mathbb{Q}$. To avoid confusion, we reserve the letter $\mathfrak{p}$ (resp. $\mathfrak{q}$) to denote places of X (resp. of Y). We say that a place $\mathfrak{q}$ *divides* $\mathfrak{p}$ or, equivalently, that $\mathfrak{q}$ is *above* $\mathfrak{p}$, and we note $\mathfrak{q}|\mathfrak{p}$, when π maps $\mathfrak{q}$ to $\mathfrak{p}$. Let $\mathfrak{p} \in X^\star$ and let $K_\mathfrak{p}$ be the completion of K at the place $\mathfrak{p}$. We have the decomposition

$$K_\mathfrak{p} \otimes_K L \simeq \prod_{\mathfrak{q}|\mathfrak{p}} L_\mathfrak{q}. \tag{4}$$

For simplicity, we write $L_\mathfrak{p} = K_\mathfrak{p} \otimes_K L$.

We fix a generator $\Phi \in \mathrm{Gal}(L|K)$. For any place $\mathfrak{p} \in X^\star$, we note that Φ permutes cyclically the $L_\mathfrak{q}$'s of Equation (4). Hence, they are all isomorphic and one can number the places above $\mathfrak{p}$ as follows

$$\pi^{-1}(\mathfrak{p}) = \{\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_{m_\mathfrak{p}}\},$$

in such a way that Φ maps $L_{\mathfrak{q}_j}$ to $L_{\mathfrak{q}_{j+1}}$ for all j (with the convention that $\mathfrak{q}_{m_\mathfrak{p}+1} = \mathfrak{q}_1$). The morphism $\Phi^{m_\mathfrak{p}}$ then induces an automorphism $\Phi_{\mathfrak{p},0}$ of $L_{\mathfrak{q}_1}$ of order $d_\mathfrak{p} = r/m_\mathfrak{p}$. Setting $L_{\mathfrak{p},0} = L_{\mathfrak{q}_1}$, we finally see that the pair $(L_\mathfrak{p}, K_\mathfrak{p})$ fits in the framework of Subsection 1.2.

Let x be a fixed function in $K^\times$. We consider the algebras $D_{L,x} = L[T;\Phi]/(T^r - x)$ and $D_{L_\mathfrak{p},x} = L_\mathfrak{p}[T;\Phi]/(T^r - x)$. We recall that we have defined in Subsection 1.2 the valuations

$$w_{j,x} : D_{L_\mathfrak{p},x} \to \tfrac{1}{r}\mathbb{Z} \sqcup \{\infty\} \quad (1 \leq j \leq m_\mathfrak{p}).$$

Instead of indexing them by the integers $j \in \{1, \ldots, m_\mathfrak{p}\}$, it is more convenient here to index them by the places above $\mathfrak{p}$, *i.e.* writing $w_{\mathfrak{q}_j,x}$ for $w_{j,x}$. For an element $f \in D_{L_\mathfrak{p},x}$ written as $f = f_0 + f_1 T + \cdots + f_{r-1}T^{r-1}$ (with $f_i \in L_\mathfrak{p}$), we then have

$$w_{\mathfrak{q},x}(f) = \min_{0 \leq i < r} \left(\frac{v_\mathfrak{q}(f_i)}{e_\mathfrak{q}} + i \cdot \frac{v_\mathfrak{p}(x)}{r} \right),$$

where $e_\mathfrak{q}$ denotes the ramification index at $\mathfrak{q}$, which is also the ramification index of the extension $L_\mathfrak{q}/K_\mathfrak{p}$. Since all the $L_\mathfrak{q}$'s are isomorphic, we see that $e_\mathfrak{q}$ depends only on the place $\mathfrak{p}$ below; for this reason, we will often denote it by $e_\mathfrak{p}$ in what follows.

For a place $\mathfrak{p} \in X^\star$, we set

$$\rho_\mathfrak{p} = \frac{e_\mathfrak{p} \cdot v_\mathfrak{p}(x)}{r},$$

and define $a_\mathfrak{p}$ and $b_\mathfrak{p}$ by $\rho_\mathfrak{p} = \frac{a_\mathfrak{p}}{b_\mathfrak{p}}$, where the latter fraction is irreducible and its denominator $b_\mathfrak{p}$ is positive. Since $v_\mathfrak{p}(x)$ vanishes for almost all places $\mathfrak{p}$, we find that $\rho_\mathfrak{p} = 0$, $a_\mathfrak{p} = 0$ and $b_\mathfrak{p} = 1$ for almost all $\mathfrak{p} \in X^\star$.

Definition 2.3 (Riemann–Roch spaces of $D_{L,x}$)**.** Let $E = \sum_{\mathfrak{q} \in Y^\star} n_\mathfrak{q} \mathfrak{q} \in \mathrm{Div}_{\mathbb{Q}}(Y)$ where, for all $\mathfrak{q}$, the coefficient $n_\mathfrak{q}$ is in $\frac{1}{b_\mathfrak{p}}\mathbb{Z}$ where $\mathfrak{p} = \pi(\mathfrak{q})$ is the place below $\mathfrak{q}$. We define the *Riemann–Roch space* of $D_{L,x}$ associated with E as

$$\Lambda_{L,x}(E) := \{\, f \in D_{L,x} \mid e_\mathfrak{q} w_{\mathfrak{q},x}(f) + n_\mathfrak{q} \geq 0 \text{ for all } \mathfrak{q} \in Y^\star \,\}.$$

Remark 2.4. We use the letter E (instead of D) to denote the divisor in order to lower the risk to create confusion with the algebra $D_{L,x}$.

Keeping the notation of Definition 2.3, it follows readily from the definitions that

$$\Lambda_{L,x}(E) = \bigoplus_{i=0}^{r-1} L_Y(E_i) \cdot T^i, \tag{5}$$

where, letting $\lfloor \cdot \rfloor$ denote the integer part function, the divisors E_i are defined by

$$E_i := \sum_{\mathfrak{q} \in Y^\star} \lfloor n_\mathfrak{q} + i \cdot \rho_{\pi(\mathfrak{q})} \rfloor \cdot \mathfrak{q} \in \mathrm{Div}(Y) \qquad (0 \le i < r),$$

and the $L_Y(E_i)$'s are the "classical" Riemann–Roch spaces (on Y), as defined in Equation (3).

Lemma 2.5. *We have* $\displaystyle\sum_{i=0}^{r-1} \deg_Y(E_i) = r \cdot \deg_Y(E) - \frac{r^2}{2} \sum_{\mathfrak{p} \in X^\star} \frac{b_\mathfrak{p} - 1}{b_\mathfrak{p} e_\mathfrak{p}} \deg_X(\mathfrak{p})$.

Proof. Fix a place $\mathfrak{q} \in Y^\star$, and write $\mathfrak{p} = \pi(\mathfrak{q})$ and $n_\mathfrak{q} = \frac{c_\mathfrak{q}}{b_\mathfrak{p}}$. For $i \in \{0, \ldots, r-1\}$, we have

$$\lfloor n_\mathfrak{q} + i \cdot \rho_{\pi(\mathfrak{q})} \rfloor = \left\lfloor \frac{c_\mathfrak{q} + i \cdot a_\mathfrak{p}}{b_\mathfrak{p}} \right\rfloor = \frac{c_\mathfrak{q} + i \cdot a_\mathfrak{p} - \varepsilon_{i,\mathfrak{q}}}{b_\mathfrak{p}},$$

where $\varepsilon_{i,\mathfrak{q}}$ denotes the remainder in the division of $c_\mathfrak{q} + i \cdot a_\mathfrak{p}$ by $b_\mathfrak{p}$. From the fact that $a_\mathfrak{p}$ and $b_\mathfrak{p}$ are coprime, we derive that for each value $\varepsilon \in \{0, \ldots, b_\mathfrak{p} - 1\}$, there are exactly $\frac{r}{b_\mathfrak{p}}$ indices i for which $\varepsilon_{i,\mathfrak{q}} = \varepsilon$. Therefore, summing over i, we get

$$\begin{aligned}\sum_{i=0}^{r-1} \lfloor n_\mathfrak{q} + i \cdot \rho_{\pi(\mathfrak{q})} \rfloor &= r \cdot n_\mathfrak{q} + \frac{r(r-1)}{2} \cdot \rho_{\pi(\mathfrak{q})} - \frac{r(b_\mathfrak{p} - 1)}{2 b_\mathfrak{p}} \\ &= r \cdot n_\mathfrak{q} + \frac{r-1}{2} \cdot v_\mathfrak{q}(x) - \frac{r(b_\mathfrak{p} - 1)}{2 b_\mathfrak{p}}.\end{aligned}$$

Summing over $\mathfrak{q}$ and weighting by $\deg_Y(\mathfrak{q})$, and using that $\sum_{\mathfrak{q} \in Y^\star} v_\mathfrak{q}(x) \deg_Y(\mathfrak{q}) = 0$, we end up with

$$\sum_{i=0}^{r-1} \deg_Y(E_i) = r \cdot \deg_Y(E) - \frac{r}{2} \sum_{\mathfrak{q} \in Y^\star} \frac{b_{\pi(\mathfrak{q})} - 1}{b_{\pi(\mathfrak{q})}} \deg_Y(\mathfrak{q}).$$

Noticing finally that $\deg_Y(\mathfrak{q}) = \frac{r}{m_\mathfrak{p} e_\mathfrak{p}} \cdot \deg_X(\pi(\mathfrak{q}))$, we obtain the announced formula. $\square$

Corollary 2.6. *For a divisor* $E = \sum_{\mathfrak{q} \in Y^\star} n_\mathfrak{q} \mathfrak{q} \in \mathrm{Div}_\mathbb{Q}(Y)$ *as in Definition 2.3, the space* $\Lambda_{L,x}(E)$ *is finite dimensional over* k *and*

$$\dim_k \Lambda_{L,x}(E) \ge r \cdot \deg_Y(E) - r \cdot (g_Y - 1) - \frac{r^2}{2} \sum_{\mathfrak{p} \in X^\star} \frac{b_\mathfrak{p} - 1}{b_\mathfrak{p} e_\mathfrak{p}} \deg_X(\mathfrak{p}).$$

Proof. On the one hand, from Equation (5), we derive

$$\dim_k \Lambda_{L,x}(E) = \sum_{i=0}^{r-1} \dim_k L_Y(E_i).$$

On the other hand, it follows from the classical Riemann–Roch theorem (Theorem 2.2) that $\dim_k L_Y(E_i) \geq \deg_Y E_i - (g_Y - 1)$. Combining this input with Lemma 2.5, we get the corollary. □

Remark 2.7. We point out that equality in the bound of Corollary 2.6 is attained whenever for any i we have $\dim_k L_Y(E_i) = \deg_Y E_i - (g_Y - 1)$, which happens as soon as $\deg_Y E_i \geq 2g_Y - 1$ for any i.

3. Linearized Algebraic Geometry codes

In this section we introduce codes in the sum-rank metric from algebraic curves, that we call linearized Algebraic Geometry codes. We propose a general construction using a Galois cover $\pi : Y \to X$ between two curves (Subsection 3.1). We give bounds for the dimension and the minimum distance of our codes (Theorem 3.5). Finally, in Subsection 3.3, we consider the case of isotrivial covers. In particular, when the curve X has genus $g_X = 0$, we retrieve the construction of linearized Reed–Solomon codes, as proposed in [MP18, CD22].

3.1. **The code construction.** We consider the setting of Subsection 2.2 and keep all the notation from here. In particular, we fix a base field k and consider a Galois cover $\pi : Y \to X$ between smooth projective irreducible algebraic curves defined over k. We assume that $\mathrm{Gal}(Y|X)$ is cyclic of order r. We write $K := X(k)$ and $L := Y(k)$ for the function fields of X and Y, respectively. The extension L/K is Galois with cyclic Galois group of order r, generated by Φ. As in Subsection 2.2, we continue to use the letter $\mathfrak{p}$ (resp. $\mathfrak{q}$) to refer to places of X (resp. of Y). We fix in addition:

- a function $x \in K^\times$,
- a divisor $E = \sum_{\mathfrak{q} \in Y^\star} n_\mathfrak{q} \mathfrak{q} \in \mathrm{Div}_\mathbb{Q}(Y)$ satisfying the condition of Definition 2.3,
- a positive integer s and s *rational* places $\mathfrak{p}_1, \ldots, \mathfrak{p}_s \in X^\star$ which do not belong to $\pi(\mathrm{supp}(E))$.

For $i \in \{1, \ldots, s\}$, we write $K_i := K_{\mathfrak{p}_i}$ (the completion of K at the place $\mathfrak{p}_i$) and set $L_i := K_i \otimes_K L$. Since the $\mathfrak{p}_i$'s are rational, we have an isomorphism $K_i \simeq k(\!(t_i)\!)$, where t_i is a uniformizing parameter at $\mathfrak{p}_i$. We let m_i be the number of places above $\mathfrak{p}_i$.

We formulate several hypotheses, the second one depending on a place $\mathfrak{p}$ of X:

(H1) *the algebra $D_{L,x}$ has no nonzero zero divisor,*

(H2-$\mathfrak{p}$) *for all places $\mathfrak{q}$ above $\mathfrak{p}$, there exists $u_\mathfrak{q} \in L_\mathfrak{q}^\times$ such that $v_\mathfrak{q}(u_\mathfrak{q}) = \frac{e_\mathfrak{p}}{r} \cdot v_\mathfrak{p}(x)$ and*

$$x = \prod_{\mathfrak{q}|\mathfrak{p}} N_{L_\mathfrak{q}/K_\mathfrak{p}}(u_\mathfrak{q}),$$

(H2) *for all $i \in \{1, \ldots, s\}$, the hypothesis* **(H2-$\mathfrak{p}_i$)** *holds.*

We recall that a place $\mathfrak{p}$ is called *inert* if there is a unique place $\mathfrak{q}$ above $\mathfrak{p}$, with $e_\mathfrak{q} = 1$.

Lemma 3.1. *The hypothesis* **(H1)** *holds as soon as there exists a place $\mathfrak{p} \in X^\star$ which is inert in Y and at which $v_\mathfrak{p}(x)$ is coprime with r.*

Proof. Let $\mathfrak{p}$ be a place satisfying the requirements of the lemma. We embed $D_{L,x}$ into $D_{L_\mathfrak{p},x} = K_\mathfrak{p} \otimes_K D_{L,x}$. By Proposition 1.5, we know that the latter has no nonzero zero divisor. The lemma follows. □

The hypothesis **(H2-$\mathfrak{p}$)** clearly implies that $v_\mathfrak{p}(x)$ has to be divisible by $\frac{r}{e_\mathfrak{p}}$. The next lemma shows that the converse is true for unramified places over a finite field.

Lemma 3.2. *We assume that k is a finite field. Let $\mathfrak{p}$ be a place of X. If $\mathfrak{p}$ is unramified in Y and $v_\mathfrak{p}(x)$ is divisible by r, then* **(H2-$\mathfrak{p}$)** *holds.*

Proof. Let $m_\mathfrak{p}$ be the number of places of Y above $\mathfrak{p}$. Let $\mathfrak{q}$ be a place over $\mathfrak{p}$. By assumption, the extension $L_\mathfrak{q}/K_\mathfrak{p}$ is unramified of degree $d_\mathfrak{p} = r/m_\mathfrak{p}$. Since, moreover, the residue field on $K_\mathfrak{p}$ is finite, we conclude that any element of $K_\mathfrak{p}$ of valuation divisible by $d_\mathfrak{p}$ is a norm in the extension $L_\mathfrak{q}/K_\mathfrak{p}$.

Since r divides $v_\mathfrak{p}(x)$, one can write x as a product $x = \prod_{\mathfrak{q}|\mathfrak{p}} x_\mathfrak{q}$ where each $x_\mathfrak{q} \in K_\mathfrak{p}$ has valuation $v_\mathfrak{p}(x)/m_\mathfrak{p}$. For each place $\mathfrak{q}$ above $\mathfrak{p}$, one can then find $u_\mathfrak{q} \in L_\mathfrak{q}$ such that $N_{L_\mathfrak{q}/K_\mathfrak{p}}(u_\mathfrak{q}) = x_\mathfrak{q}$. This equality implies in particular that

$$v_\mathfrak{q}(u_\mathfrak{q}) = \frac{v_\mathfrak{p}(x_\mathfrak{q})}{d_\mathfrak{p}} = \frac{v_\mathfrak{p}(x)}{m_\mathfrak{p} d_\mathfrak{p}} = \frac{v_\mathfrak{p}(x)}{r}.$$

On the other hand, by construction, we have $\prod_{\mathfrak{q}|\mathfrak{p}} N_{L_\mathfrak{q}/K_\mathfrak{p}}(u_\mathfrak{q}) = \prod_{\mathfrak{q}|\mathfrak{p}} x_\mathfrak{q} = x$, which finally ensures that the hypothesis **(H2-$\mathfrak{p}$)** is fulfilled. □

We are now ready to define our code. For $i \in \{1, \ldots, s\}$, we consider the k-algebras $V_i := \mathcal{O}_{L_i}/t_i\mathcal{O}_{L_i}$ which are finite dimensional of dimension r. We form the k-vector space

$$\mathcal{H} := \mathrm{End}_k(V_1) \times \mathrm{End}_k(V_2) \times \cdots \times \mathrm{End}_k(V_s).$$

which is the ambient space in which our code will eventually sit. We equip $\mathcal{H}$ with the so-called *sum-rank weight* w_{srk} defined as in the Introduction by

$$w_{\mathrm{srk}}(\varphi_1, \ldots, \varphi_s) := \sum_{i=1}^{s} \mathrm{rk}(\varphi_i).$$

We now assume the hypothesis **(H2)**. For each i, we choose a family of elements $u_{i,\mathfrak{q}}$ indexed by the places $\mathfrak{q}$ above $\mathfrak{p}_i$ satisfying the requirements of **(H2-$\mathfrak{p}_i$)**. We form the element $u_i = (u_{i,\mathfrak{q}})_{\mathfrak{q}|\mathfrak{p}_i} \in L_i$. By Lemma 1.1, we have an isomorphism

$$\varepsilon_i : D_{L_i,x} \xrightarrow{\gamma_{u_i}} D_{L_i,1} \xrightarrow{\varepsilon} \mathrm{End}_{K_i}(L_i),$$

and Lemma 1.4 indicates moreover that γ_{u_i} induces an isomorphism $\Lambda_{L_i,x} \to \Lambda_{L_i,1}$.

Take $f \in D_{L_i,x}$. Unrolling the definitions, we realize that $\varepsilon_i(f) = f(u_i\Phi)$; hence the morphism ε_i can be thought of as the evaluation map at $u_i\Phi$. It follows moreover from the definitions (see Subsection 1.2) that $\varepsilon_i(f)$ stabilizes the lattice $\mathcal{O}_{L_i}$ whenever $f \in \Lambda_{L_i,x}$.

For those f, we let $\bar{\varepsilon}_i(f) \in \mathrm{End}_k(V_i)$ be the reduction of $\varepsilon_i(f)$ modulo t. Noticing finally that the assumption that $\mathfrak{p}_i \notin \pi(\mathrm{supp}(E))$ ensures that the Riemann–Roch space $\Lambda_{L,x}(E)$ (see Definition 2.3) is included in $\Lambda_{L_i,x}$, we define the "multi-evaluation" map

$$\begin{array}{rccc} \alpha: & \Lambda_{L,x}(E) & \longrightarrow & \mathcal{H} \\ & f & \mapsto & \big(\bar{\varepsilon}_i(f)\big)_{1\leq i\leq s}. \end{array} \tag{6}$$

Definition 3.3. The code $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$ is defined as the image of α.

Remark 3.4. The code $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$ depends on the choice of the u_i's for $i = 1, \ldots, s$. However, this dependence is quite weak, in the sense that changing the u_i's will eventually result in a code which is conjugated to the initial one by an element of $\prod_{i=1}^s \mathrm{GL}(V_i)$. That is the reason why we prefer omitting to mention the u_i's in the notation.

3.2. **Code's parameters.** For a k-linear code $\mathcal{C}$ sitting inside $\mathcal{H}$, we define:

- its *length* n as the k-dimension of the ambient space $\mathcal{H}$, *i.e.* $n := sr^2$,
- its *dimension* δ as its k-dimension, *i.e.* $\delta := \dim_k \mathcal{C}$,
- its *minimum distance* d as the minimal sum-rank weight of a nonzero codeword in $\mathcal{C}$.

Those parameters are related by the Singleton inequality which reads $rd + \delta \leq n + r$ in our setting [BGLR21, Thm. 3.1]. The next theorem provides explicit lower bounds for the dimension and the minimum distance of our codes.

Theorem 3.5. *We keep the previous notations. We assume* **(H1)** *and* **(H2)**, *and that* $\deg_Y(E) < sr$. *Then, the dimension* δ *and the minimum distance* d *of* $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$ *satisfy*

$$\delta \geq r\cdot \deg_Y(E) - r\cdot(g_Y - 1) - \frac{r^2}{2} \sum_{\mathfrak{p}\in X^\star} \frac{b_\mathfrak{p} - 1}{b_\mathfrak{p} e_\mathfrak{p}} \deg_X(\mathfrak{p}),$$

$$d \geq sr - \deg_Y(E).$$

Proof. Let $f \in \Lambda_{L,x}(E)$ be a nonzero function and set ω to be the sum-rank weight of $\alpha(f)$, where α is the evaluation map defined in Equation (6). By definition, we have $\sum_{i=1}^s \mathrm{rk}\, \bar{\varepsilon}_i(f) = \omega$, where we recall that the $\bar{\varepsilon}_i$'s are the components of α. We set $d_i := \dim_k \ker \bar{\varepsilon}_i(f)$ for $i \in \{1, \ldots, s\}$. By standard linear algebra, we get

$$\sum_{i=1}^s d_i = \sum_{i=1}^s \dim_k V_i - \mathrm{rk}\, \bar{\varepsilon}_i(f) = sr - \omega. \tag{7}$$

Recall that $E = \sum_{\mathfrak{q}\in Y^\star} n_\mathfrak{q} \mathfrak{q}$. We introduce the divisor

$$E' := -\sum_{i=1}^s d_i \mathfrak{p}_i + \sum_{\mathfrak{p}\in X^\star} \left\lfloor \sum_{\mathfrak{q}|\mathfrak{p}} \frac{r\cdot n_\mathfrak{q}}{e_\mathfrak{p} m_\mathfrak{p}} \right\rfloor \mathfrak{p} \in \mathrm{Div}(X),$$

where $e_\mathfrak{p}$ and $m_\mathfrak{p}$ were defined in Subsection 2.2. It follows from Lemma 1.4 and Propositions 1.6 and 1.7 that $N_{\mathrm{rd}}(f) \in L_X(E')$. Besides, we have

$$\deg_Y(E') \leq -\sum_{i=1}^s d_i + \sum_{\mathfrak{q}\in Y^\star} \frac{r\cdot n_\mathfrak{q}}{e_\mathfrak{p} m_\mathfrak{p}} \deg_X(\pi(\mathfrak{q})) = \omega - sr + \deg_Y(E),$$

the last equality coming from Equation (7) and the relation $e_{\mathfrak{p}} m_{\mathfrak{p}} \deg_Y(\mathfrak{q}) = r \cdot \deg_X(\pi(\mathfrak{q}))$. As a consequence, if $\omega < sr - \deg_Y(E)$, we have $N_{\mathrm{rd}}(f) = 0$. Since $N_{\mathrm{rd}}(f)$ is, by definition, the determinant of the map $\mu_f : D_{L,x} \to D_{L,x}, g \mapsto gf$, its vanishing implies that μ_f is not injective. In other words, f is a zero divisor in $D_{L,x}$. Thanks to hypothesis **(H1)**, we conclude that f has to vanish. In conclusion, we showed that $\omega \geq sr - \deg_Y(E)$, hence the bound on d.

As a byproduct of what precedes, we obtain the injectivity of α. Therefore $\delta = \dim_k \Lambda_{L,x}(E)$, and the announced lower bound on δ now follows from Corollary 2.6. $\square$

Corollary 3.6. *Under the assumptions of Theorem 3.5, and still writing n, δ and d for the length, the dimension and the minimum distance of $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$, respectively, we have*

$$rd + \delta \geq n + r - \left(r \cdot g_Y + \frac{r^2}{2} \sum_{\mathfrak{p} \in X^\star} \frac{b_{\mathfrak{p}} - 1}{b_{\mathfrak{p}} e_{\mathfrak{p}}} \deg_X(\mathfrak{p}) \right).$$

Remark 3.7. More generally, one can consider k-subspaces $W_i \subset V_i$ and replace α by the restricted multi-evaluation map

$$\begin{array}{ccc} \Lambda_{L,x}(E) & \longrightarrow & \mathrm{Hom}_k(W_1, V_1) \times \cdots \times \mathrm{Hom}_k(W_s, V_s) \\ f & \mapsto & \left(\bar{\varepsilon}_i(f)_{|W_i}\right)_{1 \leq i \leq s}. \end{array}$$

Doing so, we obtain more general codes, for which the bounds of Theorem 3.5 stay valid.

3.3. **The case of isotrivial covers.** Let ℓ be a finite cyclic extension of k of order r. Given X as before, the curve $Y = \operatorname{Spec} \ell \times_{\operatorname{Spec} k} X$ is a cyclic Galois cover of X of degree r for which the theory developed earlier applies. In this particular case, we notice that:

(1) the cover $\pi : Y \to X$ is unramified everywhere, *i.e.* $e_{\mathfrak{p}} = 1$ for all places $\mathfrak{p} \in X^\star$,
(2) the Riemann–Hurwitz formula [Sti09, Thm. 3.4.13] asserts that $g_Y - 1 = r \cdot (g_X - 1)$,
(3) all rational places of X are inert in Y and, more generally, all places whose residue field is linearly disjoint from ℓ are inert; however, the reader should be careful that if $\mathfrak{p}$ is a inert place of X and $\mathfrak{q}$ is the unique place above $\mathfrak{p}$, we have $\deg_Y(\mathfrak{q}) = r \cdot \deg_X(\mathfrak{p})$,
(4) the residue field of any place of Y is a ℓ-algebra; in particular the codes $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$ are always ℓ-linear, *i.e.* they are ℓ-subvector spaces of $\mathcal{H}$.

In this setting, it is relevant to work with the ℓ-length and the ℓ-dimension. Precisely, if $\mathcal{C}$ is a ℓ-linear code sitting inside $\mathcal{H}$, we define:

- its ℓ-length n_ℓ as the dimension over ℓ of the ambient space $\mathcal{H}$, *i.e.* $n_\ell := sr$,
- its ℓ-dimension δ_ℓ by $\delta_\ell := \dim_\ell \mathcal{C}$.

The Singleton bound now reads $d + \delta_\ell \leq n_\ell + 1$ where d still denotes the minimum distance. For the code $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$ with parameters satisfying the hypotheses **(H1)** and **(H2)**, Theorem 3.5 provides the following lower bounds

$$\delta_\ell \geq \deg_Y(E) - r \cdot (g_X - 1) - \frac{r}{2} \sum_{\mathfrak{p} \in X^\star} \frac{b_{\mathfrak{p}} - 1}{b_{\mathfrak{p}}} \deg_X(\mathfrak{p}), \tag{8}$$

$$d \geq sr - \deg_Y(E), \tag{9}$$

from what we derive

$$d + \delta_\ell \geq n_\ell + 1 - \left(r \cdot (g_X - 1) + 1 + \frac{r}{2} \sum_{\mathfrak{p} \in X^\star} \frac{b_\mathfrak{p} - 1}{b_\mathfrak{p}} \deg_X(\mathfrak{p}) \right).$$

Linearized Reed–Solomon codes. To conclude this subsection, we consider the example where $X = \mathbb{P}^1_k$ and $Y = \mathbb{P}^1_\ell$, both viewed as curves over $\operatorname{Spec} k$. We have $g_X = 0$. We call t the coordinate on X and Y. The function fields of X and Y are then $K = k(t)$ and $L = \ell(t)$, respectively. A place $\mathfrak{p} \in X^\star$ (resp. $\mathfrak{q} \in Y^\star$) corresponds to either ∞ or to a irreducible monic polynomial in $k[t]$ (resp. in $\ell[t]$). A place $\mathfrak{p} \in X^\star$ is rational when the corresponding polynomial has degree 1, *i.e.* rational places of X are in one-to-one correspondence with the elements in k.

We choose the function $x = t \in K^\times$. For this choice, we have $b_\mathfrak{p} = 1$ for all $\mathfrak{p} \in X^\star$, except for the places corresponding to 0 and ∞ where $b_\mathfrak{p} = r$. Moreover, the algebra

$$D_{L,x} = \ell(t)[T; \Phi]/(T^r - t),$$

where Φ is a given generator of $\operatorname{Gal}(\ell|k)$, is canonically isomorphic to the fraction field of $\ell[T; \Phi]$.

We consider the divisor $E = \frac{m}{r} \cdot \infty \in \operatorname{Div}_\mathbb{Q}(Y)$ for a positive integer m. Coming back to the definitions, we find that the Riemann–Roch space $\Lambda_{L,x}(E)$ is equal to the set $\ell[T; \Phi]_{\leq m}$ of Ore polynomials in T of degree at most m.

We fix rational places $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ corresponding to elements $c_1, \ldots, c_s \in k \sqcup \{\infty\}$. We note that they satisfy the hypothesis **(H2)** if and only if $c_i \in N_{\ell/k}(\ell^\times)$ for all i; we assume this from now on. The multi-evaluation morphism α is given by

$$\begin{array}{rccc} \alpha : & \ell[T; \Phi]_{\leq m} & \longrightarrow & \mathcal{H} \\ & f & \mapsto & \big(f(u_i \Phi)\big)_{1 \leq i \leq s}, \end{array}$$

where $u_i \in \ell^\times$ is a preimage of c_i by the norm map. We then recover exactly the construction of linearized Reed–Solomon codes [MP18, CD22]. The lower bounds (8) and (9) specialize to $\delta_\ell \geq m + 1$ and $d \geq sr - m = n_\ell - m$. The Singleton bound is then reached in this case, reproving that linearized Reed–Solomon codes are MSRD codes.

4. Conclusion

In this article, we introduced a new family of codes for the sum-rank metric and provided lower bounds on their dimension and minimum distance, showing that our codes exhibit quite good parameters. Our construction is based on algebraic geometry and can be considered as an extension of that of AG codes to a noncommutative framework.

4.1. **Comparison with Morandi and Sethuraman's codes.** In [MS98], Morandi and Sethuraman proposed a construction quite similar to ours, whose initial input is a maximal order in a central simple algebra over the function field of a curve. Our approach meets Morandi and Sethuraman's one because the rings $D_{L,x}$ we considered in this paper turns out to be central simple algebras over $K = k(X)$ (where we recall that X is a curve defined over k). Additionally, the main ingredient in Morandi and Sethuraman's article is a noncommutative version of the Riemann–Roch's theorem [MS98, Thm. 4] (which is initially due to Van Geel [VG81, VDGO81]), which looks similar to our Corollary 2.6. Nevertheless, our contribution differs from [MS98] in several important points.

First, we are working with the sum-rank distance while Morandi and Sethuraman work with the classical Hamming metric. Beyond this obvious separation, the setup of [MS98] forces the authors to choose "evaluation points" which are totally ramified places of the central simple algebra. In comparison, we have more freedom in our framework, being only constrained by the hypothesis **(H2-$\mathfrak{p}$)**, which is of different nature but usually much weaker.

Secondly, Morandi and Sethuraman's construction uses *maximal* orders in the underlying division algebra whereas the explicit rings $\Lambda_{L,x}$ we introduced are usually *non-maximal* orders. Here, the divergence is more subtle but, in some sense, it is the same as the difference between smooth and singular curves in the classical Riemann–Roch's theorem. Indeed, in the commutative setting, the ring of functions on smooth curves which are regular outside one fixed place is a Dedekind domain which is a maximal order in the corresponding field of functions. On the contrary, when the curve is singular, the order defined by the ring of regular functions is no longer maximal (and desingularizing the curve consists in replacing this order by the maximal one). Following this analogy, our Corollary 2.6 can be thought as a (weak) instance of an hypothetic extension of the Riemann–Roch's theorem for central simple algebras to the singular case.

Lastly, on the practical side, our construction looks better suited for concrete implementation. Indeed, the main ingredients we are using are Ore polynomials and Riemann–Roch spaces. Both of them are available in standard softwares of Symbolic Computation (*e.g.* MAGMA [Mag23], SAGEMATH [Sag23]), making rather concrete the perspective of implementing our codes and potentially use them. Instead, Morandi and Sethuraman use abstract central simple algebras (encoded by their Hasse invariants) and the general theory of maximal orders inside them. Although these objects are very important in algebraic geometry, as far as we know, a full support for manipulating them on computers is not yet available. For sake of completeness, we mention however that an implementation in the framework of number fields is available in PARI/GP [PAR23], after the work of Aurel Page.

4.2. **Perspectives.** To start, we plan to understand the interactions between our construction and that of [MS98], and possibly to set up a general framework which encompasses both approaches. This is a long-term project since, as discussed above, it will require at least to extend Van Geel's noncommutative version of Riemann–Roch's theorem to the "singular case". It will also need to allow for more general divisors. Indeed, the shape of divisors $\sum_{\mathfrak{q}} n_{\mathfrak{q}}\mathfrak{q}$ with which we have worked in the present article looks more general than the divisors considered in [VG81, VDGO81, MS98], which were restricted to the form $\sum_{\mathfrak{p}} n_{\mathfrak{p}}\mathfrak{p}$ (the sum is taken over $\mathfrak{p}$, not over $\mathfrak{q}$).

Apart from this, we plan to study the decoding problem, at least in the case of unique decoding. Indeed, efficient decoding algorithms are available for both AG codes and linearized Reed–Solomon codes. It is then a natural question to try to extend those algorithms to the setting of the present paper.

Finally, it would be desirable to have a duality theorem for the codes $\mathcal{C}(x; E; \mathfrak{p}_1, \dots, \mathfrak{p}_s)$, in the spirit of the main result of [CD22]. Again, this is not immediate as it will require to develop the theory of differential forms and residues in the framework of central simple algebras. We nevertheless plan to go back on this question in a forthcoming article.

Acknowledgements. This work was funded in part by the grants ANR-21-CE39-0009-BARRACUDA and ANR-18-CE40-0026-01-CLap–CLap from the French National Research Agency. The first author has also received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska–Curie grant agreement No 899987.

References

[BGLR21] Eimear Byrne, Heide Gluesing-Luerssen, and Alberto Ravagnani. Fundamental properties of sum-rank-metric codes. *IEEE Transactions on Information Theory*, 67(10):6456–6475, 2021.

[CD18] Xavier Caruso and Amaury Durand. Reed–Solomon–Gabidulin Codes. *arXiv preprint arXiv:1812.09147*, 2018.

[CD22] Xavier Caruso and Amaury Durand. Duals of linearized Reed–Solomon codes. *Designs, Codes and Cryptography*, pages 1–31, 2022.

[Del78] Philippe Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of combinatorial theory, Series A*, 25(3):226–241, 1978.

[Eis13] David Eisenbud. *Commutative algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media, 2013.

[Gab85] Ernest Mukhamedovich Gabidulin. Theory of codes with maximum rank distance. *Problemy peredachi informatsii*, 21(1):3–16, 1985.

[Gop82] Valerii Denisovich Goppa. Algebraico–geometric codes. *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya*, 46(4):762–781, 1982.

[Loi06] Pierre Loidreau. A Welch–Berlekamp like algorithm for decoding Gabidulin codes. In *Coding and Cryptography: International Workshop, WCC 2005, Bergen, Norway, March 14-18, 2005. Revised Selected Papers*, pages 36–45. Springer, 2006.

[Mag23] The Magma Developers. *Magma, (Version 2.27-8)*, 2023. `http://magma.maths.usyd.edu.au`.

[MP18] Umberto Martínez-Peñas. Skew and linearized Reed–Solomon codes and maximum sum rank distance codes over any division ring. *Journal of Algebra*, 504:587–612, 2018.

[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.

[MS98] Patrick J. Morandi and Bharath Al Sethuraman. Divisors on division algebras and error correcting codes. *Communications in Algebra*, 26(10):3211–3221, 1998.

[Ore33] Oystein Ore. Theory of non-commutative polynomials. *Annals of mathematics*, pages 480–508, 1933.

[PAR23] The PARI Group, Univ. Bordeaux. *PARI/GP version* `2.15.1`, 2023. available from `http://pari.math.u-bordeaux.fr/`.

[PWZ16] Sven Puchinger and Antonia Wachter-Zeh. Sub-quadratic decoding of Gabidulin codes. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 2554–2558. IEEE, 2016.

[Rei75] Irving Reiner. Maximal orders. *New York-London*, 1975.

[RS60] Irving S. Reed and Gustave Solomon. Polynomial codes over certain finite fields. *Journal of the society for industrial and applied mathematics*, 8(2):300–304, 1960.

[Sag23] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.8)*, 2023. `https://www.sagemath.org`.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer Science & Business Media, 2009.

[TVZ82] Michael A. Tsfasman, Serge G. Vladut, and Thomas Zink. On Goppa codes which are better than the Varshamov–Gilbert bound. *Math. Nachr*, 109:21–28, 1982.

[VDGO81] Jean-Pierre Van Deuren, Jan Van Geel, and Fred Van Oystaeyen. Genus and a Riemann–Roch theorem for non-commutative function fields in one variable. In *Séminaire d'Algèbre Paul Dubreil et Marie-Paule Malliavin*, pages 295–318. Springer, 1981.

[VG81] Jan Van Geel. *Places and valuations in noncommutative ring theory*, volume 71 of *Lecture Notes in Pure and Applied Mathematics*. Marcel Dekker, Inc., New York, 1981.