Reed-Muller codes in the sum-rank metric

Elena Berardini, Xavier Caruso

REED–MULLER CODES IN THE SUM–RANK METRIC

ELENA BERARDINI

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

XAVIER CARUSO

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

ABSTRACT. We introduce the sum-rank metric analogue of Reed–Muller codes, which we called linearized Reed–Muller codes, using multivariate Ore polynomials. We study the parameters of these codes, compute their dimension and give a lower bound for their minimum distance. Our codes exhibit quite good parameters, respecting a similar bound to Reed–Muller codes in the Hamming metric. Finally, we also show that many of the newly introduced linearized Reed–Muller codes can be embedded in some linearized Algebraic Geometry codes, recently defined in [BC24], a property which could turn out to be useful in light of decoding.

Dedicated to Sudhir Ghorpade for his 60th birthday.

CONTENTS

INTRODUCTION

Error-correcting codes are powerful tools for securing data transmission over unreliable and noisy channels. Traditionally, one wants to protect data against bit erasure or

E-mail addresses: elena.berardini@math.u-bordeaux.fr, xavier.caruso@normalesup.org.

Key words and phrases. sum-rank metric codes, evaluation codes, multivariate Ore polynomials, finite fields.

bit flipping, which leads to consider the so-called Hamming distance. Nonetheless, for some specific applications (*e.g.* transmission of a message through a network in which some servers can be down or malicious) another metric is more relevant than the classical Hamming one: it is the rank metric. Interpolating between those, one finds the sum-rank metric; it was recently introduced and now finds applications in many areas of information theory, such as multi-shot linear network coding, space-time coding, and distributed storage systems (one can consult *e.g.* [MPSK22] for an overview of all these applications), and consequently have attracted significant attention of researchers from different fields. However, in contrast with the situation of codes in the other aforementioned metrics, particularly the Hamming one, only a few constructions of codes in the sum-rank metric are known and have been thoroughly studied.

Let $\mathbb{F}_q$ be a finite field with q elements, and let $\mathbb{F}_{q^r}$ be an extension of degree r of it. Classically, codes in the sum-rank metric are defined as subspaces of the product of some spaces of matrices with coefficients in $\mathbb{F}_q$. In particular, one can consider both $\mathbb{F}_q$-linear and $\mathbb{F}_{q^r}$-linear subspaces. In the present paper, we will only deal with $\mathbb{F}_{q^r}$-linear codes, and take the point of view of spaces of endomorphisms rather than spaces of matrices. In this context, sum-rank metric codes are defined as follows. For an integer s, set

$$\mathcal{H} := \prod_s \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}).$$

This is a vector space over $\mathbb{F}_{q^r}$, of dimension sr. Let $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_s) \in \mathcal{H}$. The sum-rank weight of $\boldsymbol{\varphi}$ is defined as

$$w_{\mathrm{srk}}(\boldsymbol{\varphi}) := \sum_{i=1}^{s} \mathrm{rank}(\varphi_i) = \sum_{i=1}^{s} \dim_{\mathbb{F}_q} \varphi_i(\mathbb{F}_{q^r}).$$

The sum-rank distance between φ and $\psi \in \mathcal{H}$ is

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

Definition. A ($\mathbb{F}_{q^r}$–linear) code $\mathcal{C}$ in the sum-rank metric is a $\mathbb{F}_{q^r}$–linear subspace of $\mathcal{H}$ endowed with the sum-rank distance. By definition, its *length* n is $\dim_{\mathbb{F}_{q^r}} \mathcal{H} = sr$. Its *dimension* k is $\dim_{\mathbb{F}_{q^r}} \mathcal{C}$. Its *minimum distance* is

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

The three main parameters of a code in the sum-rank metric are related by the equivalent of the Singleton bound in the Hamming metric, that in the aforementioned setting reads $d + k \leq n + 1$ [MP18, Proposition 34]. Codes with parameters attaining this bound are called *Maximum Sum-Rank Distance (MSRD)*. Let us mention that if $r = 1$, the previous definition reduces to codes of length s with the Hamming metric and, if $s = 1$, to rank-metric codes. This highlights why the sum-rank metric is considered as a generalization of both metrics. For a comprehensive overview on sum-rank metric codes we refer the reader to [GMPS23].

As for rank-metric codes, a central question in the study of sum-rank metric codes is to find constructions analogue to the existing ones in the Hamming metric. The counterpart of Reed–Solomon codes in the sum-rank metric are the so-called linearized Reed–Solomon codes [MP18], whose construction relies on the use of Ore polynomials. Algebraic Geometry codes in the sum-rank metric were recently introduced by the authors [BC24], using again Ore polynomials but with coefficients in the function field of an algebraic curve. Among the most used families of linear codes in the Hamming metric, Reed–Muller codes [Mul54, Ree54] constitute a widely studied class which however does not have its analogue in the sum-rank metric yet. The main goal of the present paper is to fill this gap.

Our contribution. In this paper we present the first analogue of Reed–Muller codes in the sum-rank metric, that we call linearized Reed–Muller codes. Classical Reed–Muller codes are constructed by evaluating multivariate polynomials at elements of an extension of $\mathbb{F}_q$. They are sometimes called affine Reed–Muller codes, in contraposition with projective Reed–Muller codes [Lac88, Sor91], where one evaluates homogenous polynomials over the elements of a projective space. Both families of Reed–Muller codes are fairly well-studied (see [KLP68, DGMW70] for affine Reed–Muller codes and [Lac90, GL23] for projective ones). In particular, computing the dimension of such codes boils down to compute the dimension of some space of polynomials of bounded degree, while for studying the minimum distance one needs to control the number of zeroes of multivariate polynomials. In the affine case this is a classical result [LN97, Theorem 6.13], while in the projective space the answer was given by Serre who proved a conjecture of Tsfasman [Ser89].

Coming back to the sum-rank metric, it is natural for constructing the analogue of Reed–Muller codes to look into multivariate Ore polynomials of bounded total degree. Therefore, firstly, we develop the theory of multivariate Ore polynomials and their evaluation. Secondly, we exploit this theory to propose the analogue of Reed–Muller codes in the sum-rank metric and study their parameters. Similarly to the Hamming case, the dimension is easily given by counting the number of monomials of a fixed degree, while to study the minimum distance we need to control the sum of the dimensions of the kernels of evaluations of multivariate Ore polynomials. This bound is proved in Theorem 2.4; besides its application to linearized Reed–Muller codes, we believe it is interesting in itself. After giving the parameters of linearized Reed–Muller codes (Theorem 2.2), we prove in addition that by allowing some flexibility in the construction, we can obtain a larger panel of codes with better parameters estimations (Theorem 2.8). Among all those codes, we get the best parameters when considering the "almost commutative" case which corresponds to the Ore polynomial algebra $\mathbb{F}_{q^r}[X_1, \dots, X_{m-1}][X_m; \Phi]$, where the only non commutative variable is the last one. Our last contribution is to show in Theorem 3.10 that, in many cases, linearized Reed–Muller codes embed in some linearized Algebraic Geometry (LAG) codes as introduced in [BC24]. This could turn to be crucial to decode the newly introduced linearized Reed–Muller codes as soon as a decoding algorithm for LAG codes will be available.

Finally, let us point out that an analogue of Reed–Muller codes in the *rank* metric was introduced in [ACLN21]. The first evident difference with the present paper, is that we consider the sum-rank metric. More interestingly, in the present paper we work over a finite field (for practical applications to coding theory) whereas the main motivation in [ACLN21] is to provide constructions in general abelian extensions. The latter falls in the finite fields setting only when the considered extension is cyclic, which was not the main case of interest in [ACLN21].

Organisation of the paper. Section 1 is devoted to the theory of rings of multivariate Ore polynomials and their evaluation. In Section 2, we introduce linearized Reed–Muller codes by evaluating multivariate Ore polynomials, and we study their parameters. Here we also show how one can improve on the parameters, and provide an example of our construction. Finally, in Section 3, we outline the construction of linearized Algebraic Geometry codes introduced in [BC24], and prove that, in many cases, our new linearized Reed–Muller codes can be embedded in some LAG codes.

1. Multivariate Ore polynomial rings

The simple algebra of univariate Ore polynomials was introduced by Ore in 1933 [Ore33]. Its theory has been extensively studied, and exploit in algebraic and geometric rank and sum-rank metric codes. In this section, we partially develop the theory of multivariate Ore polynomials for which, although probably not original, we could not find a concise presentation. We refer the reader to [Rei75] for the theory of central simple algebras, and to [Lan02, Chapter III] and [Eis13] for classical results on modules and more in general in commutative algebra, which are used without reference in what follows.

Throughout the article, we let $\mathbb{F}_q$ be a finite field with q elements, and $\mathbb{F}_{q^r}$ be an extension of degree $r > 0$. We consider $\Phi : \mathbb{F}_{q^r} \to \mathbb{F}_{q^r}$ to be the q-Frobenius endomorphism $x \mapsto x^q$. For $\boldsymbol{e} = (e_1, \dots, e_m) \in \mathbb{Z}^m$ such that $\gcd(e_1, \dots, e_m, r) = 1$, we consider the ring $\mathbb{F}_{q^r}[X_1, \dots, X_m; \Phi^{e_1}, \dots, \Phi^{e_m}]$ of multivariate Ore polynomials with usual sum, and multiplication given by

$$\begin{aligned} X_i \cdot X_j &= X_j \cdot X_i, \\ X_i \cdot a &= \Phi^{e_i}(a) \cdot X_i, \quad \forall a \in \mathbb{F}_{q^r}. \end{aligned}$$

For simplicity, we set $\theta_i = \Phi^{e_i}$, and write $\mathbb{F}_{q^r}[\boldsymbol{X}; \boldsymbol{\theta}]$ for $\mathbb{F}_{q^r}[X_1, \dots, X_m; \Phi^{e_1}, \dots, \Phi^{e_m}]$.

In what follows, we will often need to invert the variables X_i; this is possible because Φ is invertible, so that we can extend the commutative relations to X_i^{-1} by setting

$$X_i^{-1} \cdot a = \Phi^{-e_i}(a) \cdot X_i^{-1}, \quad \forall a \in \mathbb{F}_{q^r}.$$

The resulting ring is denoted by $\mathbb{F}_{q^r}[X_1^{\pm 1}, \dots, X_m^{\pm 1}; \Phi^{e_1}, \dots, \Phi^{e_m}]$, which we abbreviate as $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$. For $\boldsymbol{u} = (u_1, \dots, u_m) \in \mathbb{Z}^m$, we also use the short notation $\boldsymbol{X}^{\boldsymbol{u}}$ for the monomial $X_1^{u_1} \cdots X_m^{u_m} \in \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$. It is an easy computation to check that the general commutation relation between a monomial and a scalar reads

$$\boldsymbol{X}^{\boldsymbol{u}} \cdot a = \Phi^{\boldsymbol{e} \cdot \boldsymbol{u}}(a) \cdot \boldsymbol{X}^{\boldsymbol{u}}, \quad \forall \boldsymbol{u} \in \mathbb{Z}^m, \, a \in \mathbb{F}_{q^r}$$

where, by definition, $\boldsymbol{e}\cdot\boldsymbol{u} = e_1u_1 + \cdots + e_mu_m$ is the scalar product of $\boldsymbol{e}$ and $\boldsymbol{u}$.

1.1. **Evaluation of multivariate Ore polynomials.** In the classical case, evaluation of polynomials are defined by giving some value to the indeterminate. In the Ore setting, we will not substitute scalar values but matrices (or equivalently, linear maps); this is a crucial difference which allows somehow to "keep track" of the non-commutativity.

It turns out nevertheless that Ore evaluation (or, more generally, non-commutative evaluation) meets classical evaluation when one restricts to the centre. Recall that the centre of a commutative ring A is, by definition, the subset Z of A consisting of elements $z \in A$ such that $az = za$ for all $a \in A$. It is a commutative subring of A. Besides, any "matrix" evaluation morphism $\varepsilon : A \to M_n(F)$ (for a certain field F) induces a ring homomorphism from Z to the centre of $M_n(F)$, which is F. We then get an evaluation morphism in the classical sense, taking values in a field.

Before defining evaluation of multivariate Ore polynomials, it is therefore important to determine the centre of $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1};\boldsymbol{\theta}]$. For this, we introduce the following lattice:

$$L = \left\{ \boldsymbol{u} = (u_1, \ldots, u_m) \in \mathbb{Z}^m \mid \boldsymbol{e}\cdot\boldsymbol{u} \in r\mathbb{Z} \right\}.$$

Note that L is the kernel of the morphism $\mathbb{Z}^m \to \mathbb{Z}/r\mathbb{Z}$, $\boldsymbol{u} \mapsto \boldsymbol{e}\cdot\boldsymbol{u}$ which is surjective since $\gcd(e_1, \ldots, e_m, r) = 1$. So we get canonical isomorphisms $\mathbb{Z}^m/L \simeq \mathbb{Z}/r\mathbb{Z} \simeq \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$. We define

$$\mathbb{F}_q[\boldsymbol{X}^L] = \left\{ \sum_{\boldsymbol{u}\in L} a_{\boldsymbol{u}} X^{\boldsymbol{u}} \text{ (finite sum)} \mid a_{\boldsymbol{u}} \in \mathbb{F}_q \right\}.$$

Proposition 1.1. *The centre of* $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1};\boldsymbol{\theta}]$ *is* $\mathbb{F}_q[\boldsymbol{X}^L]$.

Proof. The proof is analogue to the one for univariate Ore polynomials. Let $P = \sum_{\boldsymbol{u}\in\mathbb{Z}^m} a_{\boldsymbol{u}}\boldsymbol{X}^{\boldsymbol{u}}$ be an element in the centre. For $i \in \{1, \ldots, m\}$, let $\boldsymbol{b}_i$ be the i-th vector of the standard basis. Then

$$0 = P \cdot X_i - X_i \cdot P = \sum_{\boldsymbol{u}\in\mathbb{Z}^m} (a_{\boldsymbol{u}} - \theta_i(a_{\boldsymbol{u}}))\boldsymbol{X}^{\boldsymbol{u}+\boldsymbol{b}_i}.$$

Therefore, we must have $a_{\boldsymbol{u}} = \theta_i(a_{\boldsymbol{u}})$ for any i. Since $\theta_i = \Phi^{e_i}$ and $\gcd(e_1, \ldots, e_m, r) = 1$, we entail $a_{\boldsymbol{u}} \in \mathbb{F}_q$. Now, take $a \in \mathbb{F}_{q^r}$. Then

$$0 = P \cdot a - a \cdot P = \sum_{\boldsymbol{u}\in\mathbb{Z}^m} a_{\boldsymbol{u}}(\Phi^{\boldsymbol{e}\cdot\boldsymbol{u}}(a) - a)\boldsymbol{X}^{\boldsymbol{u}}.$$

Therefore, we must have $\Phi^{\boldsymbol{e}\cdot\boldsymbol{u}}(a) = a$ for all $a \in \mathbb{F}_{q^r}$. Hence $\boldsymbol{e}\cdot\boldsymbol{u} \in r\mathbb{Z}$, that is $\boldsymbol{u} \in L$. □

Let us now consider a ring homomorphism $\varepsilon : \mathbb{F}_q[\boldsymbol{X}^L] \to \mathbb{F}_q$. It is of the form

$$\begin{array}{rccc} \varepsilon_\gamma : & \mathbb{F}_q[\boldsymbol{X}^L] & \to & \mathbb{F}_q \\ & \sum_{\boldsymbol{u}\in L} a_{\boldsymbol{u}}\boldsymbol{X}^{\boldsymbol{u}} & \mapsto & \sum_{\boldsymbol{u}\in L} a_{\boldsymbol{u}}\gamma(\boldsymbol{u}), \end{array}$$

where $\gamma : L \to \mathbb{F}_q^\times$ is a group morphism. Our goal is to extend ε_γ to a second ring homomorphism $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1};\boldsymbol{\theta}] \to \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}) \simeq M_r(\mathbb{F}_q)$. We will search the latter among

morphisms of the form

$$\begin{array}{rccc} \varepsilon_{\widetilde{\gamma}}: & \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1};\boldsymbol{\theta}] & \to & \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}) \\ & \sum_{\boldsymbol{u}\in\mathbb{Z}^m} a_{\boldsymbol{u}}\boldsymbol{X}^{\boldsymbol{u}} & \mapsto & \sum_{\boldsymbol{u}\in\mathbb{Z}^m} a_{\boldsymbol{u}}\widetilde{\gamma}(\boldsymbol{u})\Phi^{\boldsymbol{e}\cdot\boldsymbol{u}} \end{array}$$

where $\widetilde{\gamma}:\mathbb{Z}^m\to\mathbb{F}_{q^r}^\times$ is a function extending γ. One checks that $\varepsilon_{\widetilde{\gamma}}$ is a ring homomorphism if and only if $\widetilde{\gamma}$ satisfies the following property

$$\forall \boldsymbol{u},\boldsymbol{v}\in\mathbb{Z}^m,\quad \widetilde{\gamma}(\boldsymbol{u}+\boldsymbol{v})=\widetilde{\gamma}(\boldsymbol{u})\cdot\Phi^{\boldsymbol{e}\cdot\boldsymbol{u}}(\widetilde{\gamma}(\boldsymbol{v})). \tag{1}$$

Lemma 1.2. *The function γ extends to a function $\widetilde{\gamma}:\mathbb{Z}^m\to\mathbb{F}_{q^r}^\times$ satisfying the axiom (1).*

Proof. Since $\mathbb{Z}^m/L$ is isomorphic to $\mathbb{Z}/r\mathbb{Z}$, the theorem of structure of $\mathbb{Z}$-modules ensures that there exists a basis $(\boldsymbol{v}_1,\dots,\boldsymbol{v}_m)$ of $\mathbb{Z}^m$ such that $(\boldsymbol{v}_1,\dots,\boldsymbol{v}_{m-1},r\boldsymbol{v}_m)$ is a basis of L. We can moreover assume that $\boldsymbol{e}\cdot\boldsymbol{v}_m\equiv 1 \pmod r$. Let $\alpha\in\mathbb{F}_{q^r}^\times$ be a preimage of $\gamma(r\boldsymbol{v}_m)\in\mathbb{F}_q^\times$ by the norm map $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}$, *i.e.*

$$\gamma(r\boldsymbol{v}_m)=N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha)=\alpha\cdot\Phi(\alpha)\cdots\Phi^{r-1}(\alpha).$$

For $a_1,\dots,a_m\in\mathbb{Z}$, we write $a_m=q_mr+r_m$ with $1\le r_m\le r$ and set

$$\widetilde{\gamma}(a_1\boldsymbol{v}_1+\cdots+a_m\boldsymbol{v}_m)=\gamma(\boldsymbol{v}_1)^{a_1}\cdots\gamma(\boldsymbol{v}_{m-1})^{a_{m-1}}\cdot\gamma(r\boldsymbol{v}_m)^{q_m}\cdot\alpha\cdot\Phi(\alpha)\cdots\Phi^{r_m-1}(\alpha).$$

One finally checks that $\widetilde{\gamma}$ satisfies the requirements of the lemma. □

Remark 1.3. The preimage α is not unique, implying that there are in general many $\widetilde{\gamma}$ extending γ. However, two appropriate α always differ by multiplication by an element of norm 1, which eventually ensures that the morphisms $\varepsilon_{\widetilde{\gamma}}$ we get at the end of the process are conjugated.

Remark 1.4. A function $\widetilde{\gamma}$ respecting property (1) is called a 1-*cocycle*. In fact, Lemma 1.2 can also be obtained as a consequence of the inflation-restriction exact sequence in group cohomology, that in our context reads

$$0\to H^1(\mathbb{Z}^m/L,\mathbb{F}_{q^r}^\times)\to H^1(\mathbb{Z}^m,\mathbb{F}_{q^r}^\times)\to\mathrm{Hom}_{\mathrm{grp}}(L,\mathbb{F}_q^\times)\to H^2(\mathbb{Z}^m/L,\mathbb{F}_{q^r}^\times).$$

Noting that $\mathbb{Z}^m/L\simeq\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$, we find that $H^1(\mathbb{Z}^m/L,\mathbb{F}_{q^r}^\times)$ is trivial by Hilbert 90 Theorem and that $H^2(\mathbb{Z}^m/L,\mathbb{F}_{q^r})$ is the Brauer group of $\mathbb{F}_{q^r}/\mathbb{F}_q$ which is trivial too, given that $\mathbb{F}_q$ is a finite field. Therefore, we get an isomorphism $H^1(\mathbb{Z}^m,\mathbb{F}_{q^r}^\times)\simeq\mathrm{Hom}_{\mathrm{grp}}(L,\mathbb{F}_q^\times)$, which means that any $\gamma\in\mathrm{Hom}_{\mathrm{grp}}(L,\mathbb{F}_q^\times)$ extends to a 1-cocycle $\widetilde{\gamma}\in H^1(\mathbb{Z}^m,\mathbb{F}_{q^r}^\times)$ which is unique up to a 1-coboundary. We refer the reader to [Ser79] for more details on group cohomology.

Theorem 1.5. *We keep the above notation. Let $\mathfrak{m}_\gamma$ be the ideal of $\mathbb{F}_q[\boldsymbol{X}^L]$ generated by the $\boldsymbol{X}^{\boldsymbol{u}}-\gamma(\boldsymbol{u})$ for $\boldsymbol{u}\in L$, i.e. $\mathfrak{m}_\gamma=\ker\varepsilon_\gamma$. Then $\varepsilon_{\widetilde{\gamma}}$ induces an isomorphism*

$$\begin{array}{rccc} \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1};\boldsymbol{\theta}]/\mathfrak{m}_\gamma\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1};\boldsymbol{\theta}] & \xrightarrow{\sim} & \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}) \\ \sum_{\boldsymbol{u}\in\mathbb{Z}^m} a_{\boldsymbol{u}}\boldsymbol{X}^{\boldsymbol{u}} & \mapsto & \sum_{\boldsymbol{u}\in\mathbb{Z}^m} a_{\boldsymbol{u}}\widetilde{\gamma}(\boldsymbol{u})\Phi^{\boldsymbol{e}\cdot\boldsymbol{u}}. \end{array}$$

Proof. By Artin's theorem on independence of characters the family $\{\mathrm{Id}, \Phi, \dots \Phi^{r-1}\}$ generates $\mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r})$ over $\mathbb{F}_{q^r}$, whence the surjectivity. Injectivity follows by comparing the dimensions over $\mathbb{F}_q$. □

1.2. **Reduced norm.** A fundamental tool that makes the connection between Ore polynomials and classical polynomials is the reduced norm. Concretely, it takes the form of a multiplicative map from $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$ to its centre $\mathbb{F}_q[\boldsymbol{X}^L]$.

In order to define it, it is convenient to introduce intermediate rings between $\mathbb{F}_q[\boldsymbol{X}^L]$ and $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$. In what follows, we shall consider two of them, namely $\mathcal{C}_1 = \mathbb{F}_q[\boldsymbol{X}^{\pm 1}]$ and $\mathcal{C}_2 = \mathbb{F}_{q^r}[\boldsymbol{X}^L]$. We observe that both of them are commutative and endow $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$ with a structure of $\mathcal{C}_i$-module ($i = 1, 2$): for $c \in \mathcal{C}_i$ and $f \in \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$, the outcome of the action of c on f is simply the product cf computed in $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$. We note that $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$ is free of rank r over $\mathcal{C}_1$ and $\mathcal{C}_2$. In the former case, a basis is given by a basis of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$ while, in the latter, it is formed by the $\boldsymbol{X}^{\boldsymbol{u}}$ where $\boldsymbol{u}$ runs over a set of representatives of $\mathbb{Z}^m / L$.

For $i = 1, 2$, we define the norm map $N_i : \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}] \to \mathcal{C}_i$ as follows. Given a Ore polynomial $f \in \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$, we consider the map

$$\begin{array}{rccc} \mu_f : & \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}] & \to & \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}] \\ & g & \mapsto & gf \end{array}$$

and view it as a $\mathcal{C}_i$-linear endomorphism. We then set $N_i(f) = \det_{\mathcal{C}_i}(\mu_f)$. We note that, working in the bases we have mentioned earlier, it is possible to write down explicitly the matrix of μ_f. This provides an efficient method for computing the maps N_1 and N_2.

Theorem 1.6. *For all $f \in \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$, we have $N_1(f) = N_2(f) \in \mathbb{F}_q[\boldsymbol{X}^L]$.*

A key step in the proof of Theorem 1.6 is the following proposition.

Proposition 1.7. *For $i = 1, 2$, the map*

$$\begin{array}{rccc} \iota_i : & \mathcal{C}_i \otimes_{\mathbb{F}_q[\boldsymbol{X}^L]} \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}] & \longrightarrow & \mathrm{End}_{\mathcal{C}_i}\big(\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]\big) \simeq M_r(\mathcal{C}_i) \\ & c \otimes f & \mapsto & c \cdot \mu_f \end{array}$$

is an isomorphism of $\mathcal{C}_i$-algebras.

Proof. It is routine to check that ι_i is a morphism of $\mathcal{C}_i$-algebras. Since the domain and the codomain are both free of rank r^2 over $\mathcal{C}_i$, it is enough to show that ι_i is surjective.

We start with ι_1. Its image contains obviously the multiplication by the elements of $\mathbb{F}_{q^r}$. Besides, for $\boldsymbol{u} \in \mathbb{Z}^m$, we notice that ι_1 takes the element $\boldsymbol{X}^{\boldsymbol{u}} \otimes \boldsymbol{X}^{-\boldsymbol{u}}$ to $\Phi^{\boldsymbol{e}\cdot\boldsymbol{u}}$ (acting coefficient-wise on the Ore polynomial). By Artin's theorem, we conclude that the image of ι_1 contains at least $\mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}) \simeq M_r(\mathbb{F}_q)$ (see also the proof of Theorem 1.5). Since it is in addition a $\mathcal{C}_1$-module, we conclude that $\mathrm{im}\, \iota_1 = M_r(\mathcal{C}_1)$ and we are done.

We now move to ι_2. Let $\boldsymbol{v} \in \mathbb{Z}^m$ be an element such that $\boldsymbol{e}\cdot\boldsymbol{v} \equiv 1 \pmod r$. Then $\big(1, \boldsymbol{X}^{\boldsymbol{v}}, \boldsymbol{X}^{2\boldsymbol{v}}, \dots, \boldsymbol{X}^{(r-1)\boldsymbol{v}}\big)$ is a basis of $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$ over $\mathcal{C}_2$ and we use it to identify

$\mathrm{End}_{\mathcal{C}_2}\big(\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1};\boldsymbol{\theta}]\big)$ with $M_r(\mathcal{C}_2)$. One checks that, for any $\lambda, \alpha \in \mathbb{F}_{q^r}$,

$$\iota_2(\lambda \otimes \alpha) = \begin{pmatrix} \lambda\alpha & & & \\ & \lambda\Phi(\alpha) & & \\ & & \ddots & \\ & & & \lambda\Phi^{r-1}(\alpha) \end{pmatrix}.$$

Noticing that the map $\mathbb{F}_{q^r} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r} \to \mathbb{F}_{q^r}^r$, $\lambda \otimes \alpha \mapsto \big(\lambda\Phi^i(\alpha)\big)_{0\le i<r}$ is an isomorphism by Galois theory, we find that the image of ι_2 contains all diagonal matrices with coefficients in $\mathbb{F}_{q^r}$. Therefore it contains more generally all diagonal matrices with coefficients in $\mathcal{C}_2$ given that it is a module over $\mathcal{C}_2$. Finally, we observe that

$$\iota_2(1 \otimes \boldsymbol{X}^v) = \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ \boldsymbol{X}^{rv} & & & \end{pmatrix}.$$

Since the latter together with diagonal matrices generate $M_r(C_2)$, we conclude that ι_2 is surjective. □

Proof of Theorem 1.6. We define $\mathcal{C} = \mathcal{C}_1 \otimes_{\mathbb{F}_q[\boldsymbol{X}^L]} \mathcal{C}_2 \simeq \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}]$, so that we have the following isomorphisms of $\mathcal{C}$-algebras:

$$\begin{aligned} \mathcal{C} \otimes_{\mathbb{F}_q[\boldsymbol{X}^L]} \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1};\boldsymbol{\theta}] &\simeq \mathcal{C}_1 \otimes_{\mathbb{F}_q[\boldsymbol{X}^L]} M_r(\mathcal{C}_2) \simeq M_r(\mathcal{C}) \qquad (\textit{via } \mathcal{C}_1 \otimes \iota_2) \\ &\simeq \mathcal{C}_2 \otimes_{\mathbb{F}_q[\boldsymbol{X}^L]} M_r(\mathcal{C}_1) \simeq M_r(\mathcal{C}) \qquad (\textit{via } \mathcal{C}_2 \otimes \iota_1). \end{aligned}$$

It follows from the Skolem–Noether theorem [Rei75, Theorem 7.21] that the two above isomorphisms are conjugated over $\mathrm{Frac}\,\mathcal{C}$. In other words, there exists a matrix $P \in \mathrm{GL}_r(\mathrm{Frac}\,\mathcal{C})$ with the property that, for all $f \in \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1};\boldsymbol{\theta}]$, one has

$$\mathrm{Mat}_1(\mu_f) = P^{-1} \cdot \mathrm{Mat}_2(\mu_f) \cdot P,$$

where $\mathrm{Mat}_i(\mu_f)$ denotes the matrix of μ_f when it is viewed as a $\mathcal{C}_i$-linear map. Taking determinants, we end up with $N_1(f) = N_2(f)$.

Finally, given that N_1 and N_2 take values respectively in $\mathcal{C}_1 = \mathbb{F}_q[\boldsymbol{X}^{\pm 1}]$ and $\mathcal{C}_2 = \mathbb{F}_{q^r}[\boldsymbol{X}^L]$, the equality of those maps implies that they must assume values in the intersection $\mathcal{C}_1 \cap \mathcal{C}_2$, which is $\mathbb{F}_q[\boldsymbol{X}^L]$. □

The map $N_1 = N_2$ is called the *reduced norm map* and it will be denoted by N_{rd} in what follows. We will always consider it as a map from $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1};\boldsymbol{\theta}]$ to $\mathbb{F}_q[\boldsymbol{X}^L]$. We record the following facts which immediately follow from the corresponding properties of the determinant:

(i) the map N_{rd} is multiplicative, *i.e.* for all $f, g \in \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1};\boldsymbol{\theta}]$,

$$N_{\mathrm{rd}}(fg) = N_{\mathrm{rd}}(gf) = N_{\mathrm{rd}}(f) \cdot N_{\mathrm{rd}}(g)$$

(ii) for $f \in \mathbb{F}_q[\boldsymbol{X}^L]$, we have $N_{\mathrm{rd}}(f) = f^r$.

Coming back to the definition, one can also easily obtain bounds on the size of the reduced norm of a given Ore polynomial. For example, we have the following.

Lemma 1.8. *Let $f \in \mathbb{F}_{q^r}[\boldsymbol{X};\boldsymbol{\theta}]$ be of total degree c. Then $N_{\mathrm{rd}}(f) \in \mathbb{F}_q[\boldsymbol{X}^L] \cap \mathbb{F}_q[\boldsymbol{X}]$ and its total degree with respect to the variables $\boldsymbol{X}$ is at most rc.*

Proof. We use the description coming from the subring $\mathcal{C}_1$. Let $\mathcal{B} = (\alpha_1, \dots, \alpha_r)$ be a basis of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$. The entries of the matrix $\mathrm{Mat}_{\mathcal{B}}(\mu_f)$ representing μ_f in the basis $\mathcal{B}$ gathers the coordinates of the $f\alpha_i$ ($1 \le i \le r$) in the basis $\mathcal{B}$. Therefore, they are all polynomials in $\mathbb{F}_q[\boldsymbol{X}]$ of degree at most c. The determinant of $\mathrm{Mat}_{\mathcal{B}}(\mu_f)$, which is also $N_{\mathrm{rd}}(f)$, is then a polynomial in $\mathbb{F}_q[\boldsymbol{X}]$ of degree at most rc. □

Another decisive property of the reduced norm map is that its vanishing controls the size of the kernels of the evaluation morphisms $\varepsilon_{\widetilde{\gamma}}$ introduced earlier. In order to state a precise result in this direction, we need to introduce the *order of vanishing* of a central function: given $f \in \mathbb{F}_q[\boldsymbol{X}^L]$ and a group morphism $\gamma : L \to \mathbb{F}_q^\times$, we define

$$\mathrm{ord}_\gamma(f) = \inf\left\{ v \in \mathbb{N} \mid f \in \mathfrak{m}_\gamma^v \right\}$$

where we recall that $\mathfrak{m}_\gamma = \ker \varepsilon_\gamma$ is the ideal of $\mathbb{F}_q[\boldsymbol{X}^L]$ generated by the $\boldsymbol{X}^{\boldsymbol{u}} - \gamma(\boldsymbol{u})$, $\boldsymbol{u} \in L$. By convention $\mathrm{ord}_\gamma(0) = +\infty$ for all γ.

Theorem 1.9. *Let $f \in \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1};\boldsymbol{\theta}]$. Let also $\gamma : L \to \mathbb{F}_q^\times$ be a group morphism and $\widetilde{\gamma} : \mathbb{Z}^m \to \mathbb{F}_{q^r}^\times$ be a prolongation of γ satisfying the cocycle condition (1). Then*

$$\dim_{\mathbb{F}_q} \ker \varepsilon_{\widetilde{\gamma}}(f) \le \mathrm{ord}_\gamma\big(N_{\mathrm{rd}}(f)\big).$$

Proof. Throughout the proof, we write $\mathcal{C} = \mathcal{C}_2 = \mathbb{F}_{q^r}[\boldsymbol{X}^L]$. As in the proof of Lemma 1.8, let $\mathcal{B} = (\alpha_1, \dots, \alpha_r)$ be a basis of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$. We also fix a basis of $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1};\boldsymbol{\theta}]$ over $\mathcal{C}$ and write $\mathrm{Mat}(\mu_f)$ for the matrix of μ_f in this basis. By definition $N_{\mathrm{rd}}(f) = \det \mathrm{Mat}_{\mathcal{B}}(\mu_f)$. Besides, we notice that ε_γ induces an isomorphism between $\mathbb{F}_q[\boldsymbol{X}^L]/\mathfrak{m}_\gamma$ and $\mathbb{F}_q$. Therefore it also induces an isomorphism $\mathcal{C}/\mathfrak{m}_\gamma\mathcal{C} \simeq \mathbb{F}_{q^r}$. It then follows from Proposition 1.7 that we have an isomorphism

$$\begin{array}{rcl} \mathcal{C}/\mathfrak{m}_\gamma\mathcal{C} \otimes_{\mathbb{F}_q[\boldsymbol{X}^L]} \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1};\boldsymbol{\theta}] & \xrightarrow{\sim} & M_r(\mathbb{F}_{q^r}) \\ \lambda \otimes f & \mapsto & \lambda \cdot \mathrm{Mat}(\mu_f) \bmod \mathfrak{m}_\gamma\mathcal{C}. \end{array}$$

On the other hand, it follows from Theorem 1.5 that the evaluation morphism $\varepsilon_{\widetilde{\gamma}}$ induces another isomorphism

$$\mathcal{C}/\mathfrak{m}_\gamma\mathcal{C} \otimes_{\mathbb{F}_q[\boldsymbol{X}^L]} \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1};\boldsymbol{\theta}] \xrightarrow{\sim} M_r(\mathbb{F}_{q^r})$$

after scalar extension to $\mathbb{F}_{q^r}$. By Skolem–Noether theorem, those two isomorphisms are conjugated: there exists a matrix $P \in \mathrm{GL}_r(\mathbb{F}_{q^r})$ such that, for all $f \in \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1};\boldsymbol{\theta}]$,

$$\mathrm{Mat}_{\mathcal{B}}\big(\varepsilon_{\widetilde{\gamma}}(f)\big) \equiv P^{-1} \cdot \mathrm{Mat}(\mu_f) \cdot P \pmod{\mathfrak{m}_\gamma\mathcal{C}}. \tag{2}$$

Write $\delta = \dim_{\mathbb{F}_q} \ker \varepsilon_{\widetilde{\gamma}}(f)$ and pick a basis $\mathcal{B}' = (\alpha'_1, \dots, \alpha'_r)$ of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$ such that $\alpha'_1, \dots, \alpha'_\delta$ generate $\ker \varepsilon_{\widetilde{\gamma}}(f)$. Let $Q \in \mathrm{GL}_r(\mathbb{F}_q)$ be the change-of-basis matrix between $\mathcal{B}$ and $\mathcal{B}'$. Equation (2) then gives

$$\mathrm{Mat}_{\mathcal{B}'}\big(\varepsilon_{\widetilde{\gamma}}(f)\big) \equiv (PQ)^{-1} \cdot \mathrm{Mat}(\mu_f) \cdot PQ \pmod{\mathfrak{m}_\gamma \mathcal{C}}.$$

Therefore the matrix of μ_f is conjugated to a matrix whose δ first rows vanish modulo $\mathfrak{m}_\gamma \mathcal{C}$. As a consequence, its determinant $N_{\mathrm{rd}}(f)$ falls inside $\mathfrak{m}_\gamma^\delta \mathcal{C}$. Given that $N_{\mathrm{rd}}(f)$ also lies in $\mathbb{F}_q[\boldsymbol{X}^L]$, we find $N_{\mathrm{rd}}(f) \in \mathfrak{m}_\gamma^\delta$ which is equivalent to say that $\mathrm{ord}_\gamma\big(N_{\mathrm{rd}}(f)\big) \geq \delta$. □

2. Linearized Reed–Muller codes

In this section we introduce codes in the sum-rank metric constructed by evaluating multivariate Ore polynomials, that we call linearized Reed–Muller codes.

2.1. **The code construction.** We keep the notation of Section 1. Briefly, we recall that Φ denotes the Frobenius endomorphism $x \mapsto x^q$ acting on $\mathbb{F}_{q^r}$. We pick a tuple $\boldsymbol{e} = (e_1, \dots, e_m) \in \mathbb{Z}^m$ such that $\gcd(e_1, \dots, e_m, r) = 1$. We set $\boldsymbol{\theta} = (\Phi^{e_1}, \cdots, \Phi^{e_m})$ and consider the ring of Ore polynomials $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$. We recall that its centre is $\mathbb{F}_q[\boldsymbol{X}^L]$ where L is the kernel of the map $\mathbb{Z}^m \to \mathbb{Z}/r\mathbb{Z}$, $\boldsymbol{u} \mapsto \boldsymbol{e} \cdot \boldsymbol{u}$. It is a lattice in $\mathbb{Z}^m$ satisfying $\mathbb{Z}^m / L \simeq \mathbb{Z}/r\mathbb{Z} \simeq \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$.

Let $H := \mathrm{Hom}_{\mathrm{grp}}(L, \mathbb{F}_q^\times)$ be the set of group homomorphisms from L to $\mathbb{F}_q^\times$. For each $\gamma \in H$, we fix a prolongation $\widetilde{\gamma} : \mathbb{Z}^m \to \mathbb{F}_{q^r}^\times$ of γ satisfying the cocycle condition (1). It follows from Lemma 1.2 that such a prolongation always exists. Besides, we recall that it gives rise to an evaluation morphism $\varepsilon_{\widetilde{\gamma}} : \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}] \to \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r})$ (see Subsection 1.1). We put together all of those into a unique multievaluation morphism

$$\begin{array}{rccc} \varepsilon : & \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}] & \to & \prod_{\gamma \in H} \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}) \\ & f & \mapsto & \big(\varepsilon_{\widetilde{\gamma}}(f)\big)_{\gamma \in H} \end{array}.$$

The codomain of ε, namely

$$\mathcal{H} := \prod_{\gamma \in H} \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}),$$

will play an important role in what follows: it is the space in which all our codes will eventually sit. It is a vector space over $\mathbb{F}_{q^r}$; indeed given a scalar $a \in \mathbb{F}_{q^r}$ and a $\mathbb{F}_q$-linear endomorphism f of $\mathbb{F}_{q^r}$, the product af makes sense: it is simply the map $\mathbb{F}_{q^r} \to \mathbb{F}_{q^r}$ that takes $x \in \mathbb{F}_{q^r}$ to $a \cdot f(x)$. We underline that, for this structure, the map ε is $\mathbb{F}_{q^r}$-linear. Besides we notice that $\mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r})$ has dimension r^2 over $\mathbb{F}_q$, and hence it has dimension r over $\mathbb{F}_{q^r}$. Therefore

$$\dim_{\mathbb{F}_{q^r}} \mathcal{H} = r \cdot \mathrm{Card}(H) = r \cdot (q-1)^m,$$

the last equality coming from the fact that a group homomorphism $L \to \mathbb{F}_q^\times$ is entirely described by the datum of its values on a fixed basis of L (over $\mathbb{Z}$). Moreover, $\mathcal{H}$ is endowed with the sum-rank metric. Precisely, we define the *sum-rank weight* of a tuple

$\boldsymbol{\varphi} = (\varphi_\gamma)_{\gamma \in H} \in \mathcal{H}$ by

$$w_{\mathrm{srk}}(\boldsymbol{\varphi}) = \sum_{\gamma \in H} \mathrm{rank}(\varphi_\gamma).$$

Definition 2.1. Let $\boldsymbol{e}$ be as above and c be a positive integer. The *linearized Reed-Muller code* associated to $\boldsymbol{e}$ and c is

$$\mathrm{LRM}(\boldsymbol{e}; c) = \varepsilon\Big(\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]_{\leq c}\Big)$$

where $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]_{\leq c}$ is the subspace of $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$ consisting of multivariate Ore polynomials of total degree at most c.

Since ε is $\mathbb{F}_{q^r}$-linear, the code $\mathrm{LRM}(\boldsymbol{e}; c)$ is $\mathbb{F}_{q^r}$-linear as well, *i.e.* it is a $\mathbb{F}_{q^r}$-vector subspace of $\mathcal{H}$.

2.2. **Code's parameters.** We recall from the introduction that, for a $\mathbb{F}_{q^r}$-linear code $\mathcal{C}$ sitting inside $\mathcal{H}$, we define:

- its *length* n as the $\mathbb{F}_{q^r}$-dimension of the ambient space $\mathcal{H}$, *i.e.* $n \coloneqq r \cdot (q-1)^m$,
- its *dimension* k as its $\mathbb{F}_{q^r}$-dimension, *i.e.* $k \coloneqq \dim_{\mathbb{F}_{q^r}} \mathcal{C}$,
- its *minimum distance* d as the minimum sum-rank weight of a nonzero codeword in $\mathcal{C}$.

The next theorem provides the dimension and an explicit lower bound for the minimum distance of our codes.

Theorem 2.2. *Let $\boldsymbol{e} = (e_1, \dots, e_m) \in \mathbb{Z}^m$ with $\gcd(e_1, \dots, e_m, r) = 1$ as before. Let also c be an integer between 1 and $q-2$. Then, the dimension k and the minimum distance d of $\mathrm{LRM}(\boldsymbol{e}; c)$ satisfy*

$$k = \binom{c+m}{c} \qquad \text{and} \qquad d \geq r \cdot (q-1)^{m-1} \cdot (q-1-c).$$

The rest of this subsection is devoted to the proof of Theorem 2.2. A crucial ingredient is an upper bound on the "number of zeroes" of a multivariate Ore polynomial. Before addressing this question, we recall the corresponding result for classical multivariate polynomials.

Proposition 2.3. *Let $f \in \mathbb{F}_q[\boldsymbol{X}]$ be a nonzero polynomial of total degree at most c. Then*

$$\sum_{\boldsymbol{a} \in (\mathbb{F}_q^\times)^m} \mathrm{ord}_{\boldsymbol{a}}(f) \leq c \cdot (q-1)^{m-1}$$

where $\mathrm{ord}_{\boldsymbol{a}}$ denotes the order of vanishing at $\boldsymbol{a} = (a_1, \dots, a_m)$, that is, by definition, the smallest integer v such that $f \in \mathfrak{m}_{\boldsymbol{a}}^v$ where $\mathfrak{m}_{\boldsymbol{a}}$ is the ideal generated by $X_1 - a_1, \dots, X_m - a_m$.

Proof. We proceed by induction on the pair (m, c) ordered by lexicographic order. For $b \in \mathbb{F}_q^\times$, we let f_b be the polynomial in $m-1$ variables obtained by substituting b to X_m in f. We distinguish between two cases.

Firstly, we assume that there exists $b \in \mathbb{F}_q^\times$ such that f_b vanishes. Then f factors as $f = (X_m - b) \cdot g$ where $g \in \mathbb{F}_q[\boldsymbol{X}]$ has total degree at most $c-1$. Moreover, we notice that a basis of the quotient $\mathfrak{m}_{\boldsymbol{a}}^v / \mathfrak{m}_{\boldsymbol{a}}^{v+1}$ is formed by the polynomials

$$(X_1 - a_1)^{v_1} \cdots (X_{m-1} - a_{m-1})^{v_{m-1}} \cdot (X_m - b)^w$$

where v_i and w range over nonnegative integers such that $v_1 + \cdots + v_{m-1} + w = v$. From this description, we deduce that the multiplication by $X_m - b$ induces an *injective* map $\mathfrak{m}_{\boldsymbol{a}}^{v-1} / \mathfrak{m}_{\boldsymbol{a}}^v \to \mathfrak{m}_{\boldsymbol{a}}^v / \mathfrak{m}_{\boldsymbol{a}}^{v+1}$ for all v. It follows that one has an equality $\operatorname{ord}_{\boldsymbol{a}}(f) = 1 + \operatorname{ord}_{\boldsymbol{a}}(g)$. Summing over $\boldsymbol{a}$, we thus get

$$\sum_{\boldsymbol{a} \in (\mathbb{F}_q^\times)^m} \operatorname{ord}_{\boldsymbol{a}}(f) = (q-1)^{m-1} + \sum_{\boldsymbol{a} \in (\mathbb{F}_q^\times)^m} \operatorname{ord}_{\boldsymbol{a}}(g).$$

We conclude by applying the induction hypothesis.

Secondly, we assume that f_b is a nonzero polynomial for all $b \in \mathbb{F}_q^\times$. We consider a tuple $\boldsymbol{a} = (a_1, \dots, a_{m-1}, b) \in (\mathbb{F}_q^\times)^m$ and write $\boldsymbol{a}^\star = (a_1, \dots, a_{m-1}) \in (\mathbb{F}_q^\times)^{m-1}$. We claim that, if $f \in \mathfrak{m}_{\boldsymbol{a}}^v$ for a given nonnegative integer v, then $f_b \in \mathfrak{m}_{\boldsymbol{a}^\star}^v$ with the same exponent v. Indeed, the assumption implies that f can be written as a combination of the form

$$f = \sum_j f_j \cdot (X_1 - a_1)^{v_{1,j}} \cdots (X_{m-1} - a_{m-1})^{v_{m-1,j}} \cdot (X_m - b)^{w_j}$$

with $f_j \in \mathbb{F}_q[\boldsymbol{X}]$ and $v_{1,j}, w_j \in \mathbb{N}$ are such that $v_{1,j} + \cdots + v_{m-1,j} + w_j = v$ for all j. Evaluating at $X_m = b$, we get

$$f_b = \sum_{\substack{j \text{ s.t.} \\ w_j = 0}} (f_j)_b \cdot (X_1 - a_1)^{v_{1,j}} \cdots (X_{m-1} - a_{m-1})^{v_{m-1,j}}.$$

Noticing that $v_{1,j} + \cdots + v_{m-1,j} = v$ whenever $w_j = 0$, we conclude that $f_b \in \mathfrak{m}_{\boldsymbol{a}^\star}^v$ as claimed. It now follows from the claim that $\operatorname{ord}_{\boldsymbol{a}}(f) \leq \operatorname{ord}_{\boldsymbol{a}^\star}(f_b)$. Summing over all $\boldsymbol{a}$'s, we arrive at

$$\begin{aligned} \sum_{\boldsymbol{a} \in (\mathbb{F}_q^\times)^m} \operatorname{ord}_{\boldsymbol{a}}(f) &= \sum_{b \in \mathbb{F}_q^\times} \sum_{\boldsymbol{a}^\star \in (\mathbb{F}_q^\times)^{m-1}} \operatorname{ord}_{\boldsymbol{a}^\star}(f_b) \\ &\leq \sum_{b \in \mathbb{F}_q^\times} c \cdot (q-1)^{m-2} = c \cdot (q-1)^{m-1}, \end{aligned}$$

the inequality coming from the induction hypothesis applied with the polynomial f_b. □

We now move to the case of multivariate Ore polynomials, for which we have a direct analogue of Proposition 2.3.

Theorem 2.4. *Let $f \in \mathbb{F}_{q^r}[\boldsymbol{X}; \boldsymbol{\theta}]$ be a nonzero Ore polynomial of total degree at most c. Then*

$$\sum_{\gamma \in H} \dim_{\mathbb{F}_q} \ker \varepsilon_{\widetilde{\gamma}}(f) \leq rc \cdot (q-1)^{m-1}.$$

Proof. The basic idea of the proof is to use Theorem 1.9 and to apply Proposition 2.3 to the reduced norm of f; however, this requires some precaution. On the one hand, we know from Lemma 1.8 that the reduced norm of f is a polynomial in $\mathbb{F}_q[\boldsymbol{X}^L]$ of total degree at most rc. On the other hand, we need to be careful before applying Proposition 2.3 because the evaluation points we are interested in correspond to group homomorphisms $L \to \mathbb{F}_q^\times$, which are not exactly the classical ones (which rather correspond to morphisms $\mathbb{Z}^m \to \mathbb{F}_q^\times$).

In order to relate them, two ingredients are needed. First of all, we need to compare the orders of vanishing for the two types of evaluation points we are dealing with. Let then $g \in \mathbb{F}_q[\boldsymbol{X}^L]$ be a central function. Of course, thanks to the inclusion $\mathbb{F}_q[\boldsymbol{X}^L] \subset \mathbb{F}_q[\boldsymbol{X}^{\pm 1}]$, g can also be considered as a classical Laurent polynomial. Let $\boldsymbol{a} \in (\mathbb{F}_q^\times)^m$ be an evaluation point. To it, we attach the group morphism $\gamma' : \mathbb{Z}^m \to \mathbb{F}_q^\times$, $\boldsymbol{u} \mapsto \boldsymbol{a}^{\boldsymbol{u}}$ where by definition $\boldsymbol{a}^{\boldsymbol{u}} = a_1^{u_1} \cdots a_m^{u_m}$ (with obvious notation). We define $\gamma = \gamma'_{|L}$ as the restriction of γ' to the lattice $L \subset \mathbb{Z}^m$. As in Proposition 2.3, we consider the ideal generated by $X_i - a_i$, $1 \le i \le m$. However, for this proof, it will be more convenient to work over the ring $\mathbb{F}_q[\boldsymbol{X}^{\pm 1}]$ (instead of $\mathbb{F}_q[\boldsymbol{X}]$). For this reason, we define $\mathfrak{m}_{\boldsymbol{a}}$ by

$$\mathfrak{m}_{\boldsymbol{a}} = \langle X_1 - a_1, \cdots, X_m - a_m \rangle_{\mathbb{F}_q[\boldsymbol{X}^{\pm 1}]}$$

where the notation means that we consider the generated ideal. We underline that this modification does not change the order of vanishing at $\boldsymbol{a}$ since the coordinates of $\boldsymbol{a}$ do not vanish by assumption. However, it allows us to perform changes-of-basis. Precisely, we consider a basis $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_m)$ of $\mathbb{Z}^m$ such that $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_{m-1}, r\boldsymbol{v}_m)$ is a basis of L. We have

$$\mathfrak{m}_{\boldsymbol{a}} = \left\langle \boldsymbol{X}^{\boldsymbol{v}_1} - \gamma'(\boldsymbol{v}_1), \dots, \boldsymbol{X}^{\boldsymbol{v}_m} - \gamma'(\boldsymbol{v}_m) \right\rangle_{\mathbb{F}_q[\boldsymbol{X}^{\pm 1}]}.$$

Similarly, we know that

$$\begin{aligned}\mathfrak{m}_\gamma &= \langle \boldsymbol{X}^{\boldsymbol{v}_1} - \gamma(\boldsymbol{v}_1), \dots, \boldsymbol{X}^{\boldsymbol{v}_{m-1}} - \gamma(\boldsymbol{v}_{m-1}), \boldsymbol{X}^{r\boldsymbol{v}_m} - \gamma(r\boldsymbol{v}_m) \rangle_{\mathbb{F}_q[\boldsymbol{X}^L]} \\ &= \left\langle \boldsymbol{X}^{\boldsymbol{v}_1} - \gamma'(\boldsymbol{v}_1), \dots, \boldsymbol{X}^{\boldsymbol{v}_{m-1}} - \gamma'(\boldsymbol{v}_{m-1}), \boldsymbol{X}^{r\boldsymbol{v}_m} - \gamma'(\boldsymbol{v}_m)^r \right\rangle_{\mathbb{F}_q[\boldsymbol{X}^L]}.\end{aligned}$$

Observing that $\boldsymbol{X}^{r\boldsymbol{v}_m} - \gamma'(\boldsymbol{v}_m)^r$ is a multiple of $\boldsymbol{X}^{\boldsymbol{v}_m} - \gamma'(\boldsymbol{v}_m)$ in $\mathbb{F}_q[\boldsymbol{X}^{\pm 1}]$, we conclude that $\mathfrak{m}_\gamma \subset \mathfrak{m}_{\boldsymbol{a}}$. For all nonnegative integer v, we thus have $\mathfrak{m}_\gamma^v \subset \mathfrak{m}_{\boldsymbol{a}}^v$ as well, which finally shows that

$$\operatorname{ord}_\gamma(g) \le \operatorname{ord}_{\boldsymbol{a}}(g). \tag{3}$$

The second important ingredient we shall need is a study of the prolongations to $\mathbb{Z}^m$ of group morphisms $L \to \mathbb{F}_q^\times$. Continuing to work in our distinguished basis $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_m)$, we see that a morphism $\gamma \in H$ extends to $\mathbb{Z}^m$ if and only if $\gamma(r\boldsymbol{v}_m)$ is a r-th power in $\mathbb{F}_q^\times$; in particular, it is not always the case. In order to handle this difficulty, we introduce, for each $t \in \mathbb{F}_q^\times$, the endomorphism of $\mathbb{F}_q$-algebras $\sigma_t : \mathbb{F}_q[\boldsymbol{X}^L] \to \mathbb{F}_q[\boldsymbol{X}^L]$ defined by

$$\sigma_t : \quad \boldsymbol{X}^{\boldsymbol{v}_i} \mapsto \boldsymbol{X}^{\boldsymbol{v}_i} \ (1 \le i < m), \quad \boldsymbol{X}^{r\boldsymbol{v}_m} \mapsto t\boldsymbol{X}^{r\boldsymbol{v}_m}$$

and similarly, we introduce the map $\rho_t : H \to H$ that takes γ to the group homomorphism $\rho_t(\gamma)$ defined by

$$\rho_t(\gamma): \quad \boldsymbol{v}_i \mapsto \gamma(\boldsymbol{v}_i)\ (1 \le i < m), \quad r\boldsymbol{v}_m \mapsto t \cdot \gamma(r\boldsymbol{v}_m).$$

One easily checks that σ_t is an isomorphism (with inverse $\sigma_{t^{-1}}$) and that it takes the maximal ideal $\mathfrak{m}_\gamma$ to $\mathfrak{m}_{\rho_t(\gamma)}$.

Let $R \subset \mathbb{F}_q^\times$ be a set of representatives of the quotient $\mathbb{F}_q^\times / (\mathbb{F}_q^\times)^r$ where $(\mathbb{F}_q^\times)^r$ denotes the subgroup of $\mathbb{F}_q^\times$ of r-th powers. Since $\mathbb{F}_q^\times$ is cyclic of order $q-1$, R has cardinality $\gcd(r, q-1)$. We also consider the set H' of group homomorphisms $\mathbb{Z}^m \to \mathbb{F}_q^\times$, together with the map $\iota : R \times H' \to H$, $(t, \gamma') \mapsto \rho_t(\gamma'_{|L})$. We claim that the preimage of any $\gamma \in H$ under ι has cardinality $\gcd(r, q-1)$. Indeed, a pair (t, γ') has image γ if and only if $\gamma'(\boldsymbol{v}_i) = \gamma(\boldsymbol{v}_i)$ for $i \in \{1, \dots, m-1\}$ and

$$t \cdot \gamma'(\boldsymbol{v}_m)^r = \gamma(r\boldsymbol{v}_m). \tag{4}$$

The latter condition is realized for exactly one element $t \in R$, namely the representative of $\gamma(r\boldsymbol{v}_m)$. Besides, once t is known, the solutions of Equation (4) are in (noncanonical) one-to-one correspondence with the group $\mu_r(\mathbb{F}_q)$ of r-th roots of unity in $\mathbb{F}_q$. Using again that $\mathbb{F}_q^\times$ is cyclic of order $q-1$, we find that the cardinality of $\mu_r(\mathbb{F}_q)$ is $\gcd(r, q-1)$, which proves our claim.

Summing over all pairs $(t, \gamma') \in R \times H'$ and using the inequality (3), we end up with

$$\sum_{\gamma \in H} \operatorname{ord}_\gamma\big(N_{\mathrm{rd}}(f)\big) = \frac{1}{\gcd(r, q-1)} \sum_{t \in R} \sum_{\boldsymbol{a} \in (\mathbb{F}_q^\times)^m} \operatorname{ord}_{\boldsymbol{a}}\big(\sigma_t\big(N_{\mathrm{rd}}(f)\big)\big). \tag{5}$$

We recall from Lemma 1.8 that $N_{\mathrm{rd}}(f)$ has total degree at most rc. It is then also the case for all the $\sigma_t\big(N_{\mathrm{rd}}(f)\big)$ since applying σ_t only affects the coefficients, leaving the exponents unchanged. Therefore we can apply Proposition 2.3 to those polynomials and obtain

$$\sum_{\boldsymbol{a} \in (\mathbb{F}_q^\times)^m} \operatorname{ord}_{\boldsymbol{a}}\big(\sigma_t\big(N_{\mathrm{rd}}(f)\big)\big) \le rc \cdot (q-1)^{m-1}$$

for each individual $t \in R$. Since R has cardinality $\gcd(r, q-1)$, combining with Equation (5) and Theorem 1.9, we finally get the theorem. □

Remark 2.5. For some choices of m and $\boldsymbol{e}$, the bound of Theorem 2.4 is sharp. For example, it is the case for $\mathbb{F}_{q^r}[X, Y; \mathrm{id}, \Phi]$: the bound is attained for instance with the polynomials $(X - a_1) \cdots (X - a_c)$ where $a_1, \dots, a_c$ are pairwise distinct elements of $\mathbb{F}_q^\times$. However, there are other parameters $(m, \boldsymbol{e})$ for which the bound is not tight. In particular, when $m = 2$ and $\boldsymbol{e} = (r_1, r_2)$ with $r_1 < r_2$, $r_1 r_2 = r$ and $\gcd(r_1, r_2) = 1$ then, using the same techniques, one can show that

$$\sum_{\gamma \in H} \dim_{\mathbb{F}_q} \ker \varepsilon_{\widetilde{\gamma}}(f) \le r_2 c \cdot (q-1)^{m-1}$$

improving then the upper bound of Theorem 2.4 by a factor r_1. It could be interesting to study these phenomena in more details.

After this preparation, we are now ready to prove Theorem 2.2.

Proof of Theorem 2.2. Let $f \in \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]_{\leq c}$. It follows from Theorem 2.4 that

$$\begin{aligned} w_{\mathrm{srk}}\big(\varepsilon(f)\big) &= \sum_{\gamma \in H} \operatorname{rank} \varepsilon_{\widetilde{\gamma}}(f) \\ &= r \cdot (q-1)^m - \sum_{\gamma \in H} \dim_{\mathbb{F}_q} \ker \varepsilon_{\widetilde{\gamma}}(f) \geq r \cdot (q-1)^{m-1} \cdot (q-1-c), \end{aligned}$$

hence the bound on the minimum distance. The same computation shows in addition that ε is injective when restricted to the subspace $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]_{\leq c}$. Therefore, the dimension of the code $\mathrm{LRM}(\boldsymbol{e}; c)$ is the same as the dimension of $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]_{\leq c}$, *i.e.* it is the number of monomials in m variables of degree at most c. A standard computation indicates that it is the binomial coefficient $\binom{c+m}{c}$ as claimed. □

2.3. **Improving on the parameters.** In what precedes, we have built our codes by restricting to Ore polynomials of bounded total degree. This is certainly the most natural thing to do; however, as we shall see, allowing for more flexibility could sometimes lead to codes with better parameters.

Definition 2.6. Let $f = \sum_{\boldsymbol{u} \in \mathbb{Z}^m} a_{\boldsymbol{u}} \boldsymbol{X}^{\boldsymbol{u}} \in \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$. The *support* of f, denoted by $\mathrm{Supp}(f)$, is the subset of $\mathbb{Z}^m$ consisting of tuples $\boldsymbol{u}$ for which $a_{\boldsymbol{u}}$ does not vanish.

For a convex subset $C \subset \mathbb{R}^m$, we let $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]_C$ denote the subspace of $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$ consisting of Ore polynomials f with $\mathrm{Supp}(f) \subset C$.

Clearly $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]_C$ is a $\mathbb{F}_{q^r}$-vector subspace of $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$. A basis of it is given by the monomials $\boldsymbol{X}^{\boldsymbol{u}}$ for $\boldsymbol{u}$ running over the intersection $C \cap \mathbb{Z}^m$. In particular, it is finite dimensional when the latter intersection is finite; this occurs for instance as soon as C is compact.

Definition 2.7. Let C be a compact convex subset of $\mathbb{R}^m$. The *linearized Reed-Muller code* associated to $\boldsymbol{e}$ and C is $\mathrm{LRM}(\boldsymbol{e}; C) = \varepsilon\big(\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]_C\big)$.

Beyond noticing that all the codes $\mathrm{LRM}(\boldsymbol{e}; C)$ have length $r \cdot (q-1)^m$ (since they all sit in $\mathcal{H}$), studying them in full generality looks difficult. There is however a special case for which a lot can be said. Let $\underline{\boldsymbol{w}} = (\boldsymbol{w}_1, \dots, \boldsymbol{w}_m)$ be a basis of L and let $S_{\underline{\boldsymbol{w}}}$ be the simplex associated to it:

$$S_{\underline{\boldsymbol{w}}} = \big\{ \lambda_1 \boldsymbol{w}_1 + \cdots + \lambda_m \boldsymbol{w}_m \ : \ \lambda_i \in \mathbb{R}^+, \, \lambda_1 + \cdots + \lambda_m \leq 1 \big\}.$$

More generally, given an extra positive integer c, we consider its c-dilation:

$$cS_{\underline{\boldsymbol{w}}} = \big\{ \lambda_1 \boldsymbol{w}_1 + \cdots + \lambda_m \boldsymbol{w}_m \ : \ \lambda_i \in \mathbb{R}^+, \, \lambda_1 + \cdots + \lambda_m \leq c \big\}.$$

When $\underline{\boldsymbol{w}}$ and c vary, we obtain a family of codes $\mathrm{LRM}(\boldsymbol{e}; cS_{\underline{\boldsymbol{w}}})$ exhibiting quite nice properties. To start with, we mention that a famous theorem of Ehrhart [Ehr62] tells us that the number of integer points inside $cS_{\underline{\boldsymbol{w}}}$ varies quite regularly with respect to c. More precisely, there exists a polynomial $P_{\underline{\boldsymbol{w}}}(X)$, depending only on $\underline{\boldsymbol{w}}$ such that $\mathrm{Card}\big(cS_{\underline{\boldsymbol{w}}} \cap \mathbb{Z}^m\big) = P_{\underline{\boldsymbol{w}}}(c)$ for all nonnegative integer c. Besides, we know that $P_{\underline{\boldsymbol{w}}}(X)$ has

degree m, that its constant coefficient is 1 and that its leading coefficient is $\mathrm{Vol}(S_{\underline{w}}) = \frac{r}{m!}$. For c going to infinity, we then have the estimation

$$\mathrm{Card}\big(cS_{\underline{w}} \cap \mathbb{Z}^m\big) = P_{\underline{w}}(c) = \frac{r \cdot c^m}{m!} + O(c^{m-1}). \tag{6}$$

A general upper bound on Ehrhart's polynomials is also known. Precisely [BM85, Theorem 7.a] tells us that

$$P_{\underline{w}}(c) \leq \binom{m+c-1}{m} \cdot r + \binom{m+c-1}{m-1} = \frac{(c+1)\cdots(c+m-1)\cdot(rc+m)}{m!}. \tag{7}$$

for all nonnegative integer c.

Theorem 2.8. *We keep the previous notation and assume that c is an integer between 0 and $q-2$. Then the dimension k and the minimum distance d of* $\mathrm{LRM}(\boldsymbol{e}; cS_{\underline{w}})$ *satisfy*

$$k = \mathrm{Card}\big(cS_{\underline{w}} \cap \mathbb{Z}^m\big) = P_{\underline{w}}(c) \quad \textit{and} \quad d \geq r \cdot (q-1)^{m-1} \cdot (q-1-c).$$

Proof. The proof follows the same pattern than that of Theorem 2.2, with significant simplifications. For $i \in \{1, \dots, m\}$, write $Y_i = \boldsymbol{X}^{\boldsymbol{w}_i}$. Let $f \in \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]_C$. Repeating the proof of Lemma 1.8, we find that the reduced norm $N_{\mathrm{rd}}(f)$ has support included in $rcS_{\underline{w}}$. When viewed as a polynomial in $Y_1, \dots, Y_m$, it thus has total degree at most rc. Therefore, we can apply Proposition 2.3 directly and get

$$\sum_{\gamma \in H} \mathrm{ord}_\gamma\big(N_{\mathrm{rd}}(f)\big) \leq c \cdot (q-1)^{m-1}.$$

Using Theorem 1.9, we obtain

$$\sum_{\gamma \in H} \dim_{\mathbb{F}_q} \ker \varepsilon_{\widetilde{\gamma}}(f) \leq c \cdot (q-1)^{m-1}$$

and repeating the final argument of the proof of Theorem 2.2, we conclude that the sum-rank weight of $\varepsilon(f)$ is at least $r \cdot (q-1)^{m-1} \cdot (q-1-c)$. This gives the desired bound on the minimum distance. The formula for the dimension follows as well. □

It follows from all what precedes that Equation (6) gives the asymptotic behaviour of the dimension of our codes $\mathrm{LRM}(\boldsymbol{e}; cS_{\underline{w}})$. Comparing with the dimension of $\mathrm{LRM}(\boldsymbol{e}; c)$, we see that we gain a factor r; indeed for a fixed m and c going to infinity, we have $\binom{m+c}{c} \sim \frac{c^m}{m!}$. Nonetheless, the lower bound on the minimum distance remains the same. From this point of view, the codes $\mathrm{LRM}(\boldsymbol{e}; cS_{\underline{w}})$ look much better than their counterparts $\mathrm{LRM}(\boldsymbol{e}; c)$.

However, using $\mathrm{LRM}(\boldsymbol{e}; cS_{\underline{w}})$ might also have some small disadvantages. One of them is that enumerating the points in $cS_{\underline{w}} \cap \mathbb{Z}^m$ is not a straightforward task (although efficient algorithms exist for this). Related to this, Equation (6) only provides asymptotic information but is not applicable for small values of c. In practice, working with large values of c implies working over large finite fields as well (since c must be at most $q-2$), which could be an issue in some situations. Furthermore, for some applications where we are not only interesting in optimizing the minimum distance, the codes $\mathrm{LRM}(\boldsymbol{e}; c)$ could remain interesting as they seem to offer more diversity, in the sense that the domain where

we are picking the defining monomials is not directly related to the lattice L. Besides, after Remark 2.5, improving the estimation on the minimum distance looks plausible in certain cases.

2.4. **Some examples.**

2.4.1. *The "almost commutative" case.* We focus on the case $\boldsymbol{e} = (0, \dots, 0, 1)$ which turns out to be particularly interesting. In this situation, we have an isomorphism

$$\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}] \simeq \mathbb{F}_{q^r}[X_1^{\pm 1}, \dots, X_{m-1}^{\pm 1}][X_m^{\pm 1}; \Phi],$$

so that the multivariate Ore polynomial algebra we work with is a univariate Ore polynomial ring over a classical Laurent polynomial ring. Roughly speaking, the non-commutativity is entirely concentrated on the last variable X_m. The lattice L is easy to describe: if $(\boldsymbol{b}_1, \dots, \boldsymbol{b}_m)$ denotes the canonical basis of $\mathbb{Z}^m$, L is generated by the vectors $\boldsymbol{b}_1, \dots, \boldsymbol{b}_{m-1}, r\boldsymbol{b}_m$. We consider the associated family of codes

$$\mathrm{LRM}\big((0, \dots, 0, 1);\, cS_{(\boldsymbol{b}_1, \dots, \boldsymbol{b}_{m-1}, r\boldsymbol{b}_m)}\big),$$

for c varying in $\{1, \dots, q-2\}$. Theorem 2.8 provides estimations on the parameters of these codes: their dimension is given by the Ehrhart's polynomial $P_{\underline{w}}(c)$ and their minimum distance is at least $r(q-1)^{m-1}(q-1-c)$. In our particular case, we can be even more concrete and give a simple expression for the aforementioned Ehrhart's polynomial.

Proposition 2.9. *The dimension of the code* $\mathrm{LRM}\big((0, \dots, 0, 1);\, cS_{(\boldsymbol{b}_1, \dots, \boldsymbol{b}_{m-1}, r\boldsymbol{b}_m)}\big)$ *is*

$$\binom{m+c}{m} + (r-1) \cdot \binom{m+c-1}{m} = \frac{(c+1)\cdots(c+m-1)\cdot(rc+m)}{m!}$$

Proof. We need to find the number of integer points inside the simplex $cS_{(\boldsymbol{b}_1, \dots, \boldsymbol{b}_{m-1}, r\boldsymbol{b}_m)}$, *i.e.* to count the integral nonnegative solutions $(x_1, \dots, x_m)$ of

$$x_1 + \cdots + x_{m-1} + \frac{x_m}{r} \leq c. \tag{8}$$

We count separately the solutions $(x_1, \dots, x_m)$ with $x_m \equiv u \pmod r$ for u varying in $\{0, \dots, r-1\}$. Writing $x_m = y_m r + u$, Equation (8) reduces to $x_1 + \cdots + x_{m-1} + y_m \leq c$ for $u = 0$ and $x_1 + \cdots + x_{m-1} + y_m \leq c-1$ for $u > 0$. The formula in the statement of the proposition follows. □

We observe that the dimension provided by Proposition 2.9 meets the upper bound (7); hence "almost commutative" linearized Reed–Muller codes are optimal regarding dimension.

The codes $\mathrm{LRM}\big((0, \dots, 0, 1);\, cS_{(\boldsymbol{b}_1, \dots, \boldsymbol{b}_{m-1}, r\boldsymbol{b}_m)}\big)$ exhibit actually another quite interesting feature. Indeed, given that the variables $X_1, \dots, X_{m-1}$ are "commutative", we are not obliged to inverse them and can evaluate them at 0. Doing this, we obtain an extended code

$$\widetilde{\mathrm{LRM}}\big((0, \dots, 0, 1);\, cS_{(\boldsymbol{b}_1, \dots, \boldsymbol{b}_{m-1}, r\boldsymbol{b}_m)}\big)$$

with the following parameters:

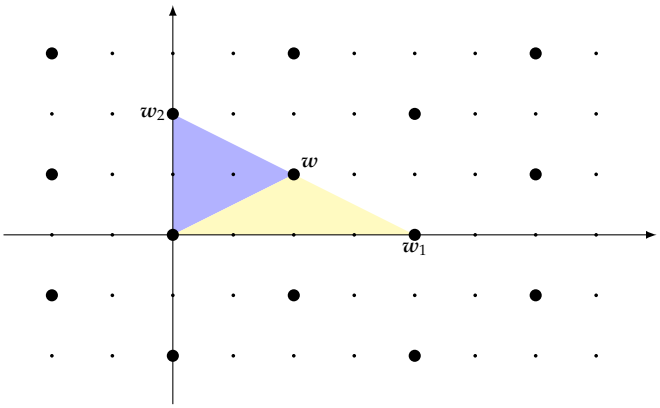

FIGURE 1. The lattice L for $\boldsymbol{e} = (3,2)$ and $r = 4$

- its length is $rq^{m-1}\cdot(q-1)$,
- its dimension is $(c+1)\cdots(c+m-1)\cdot(rc+m)/m!$, and
- its minimum distance is at least $rq^{m-1}\cdot(q-1-c)$.

2.4.2. *A concrete example.* We take $m = 2$, $r = 4$ and $\boldsymbol{e} = (3,2)$. By definition, the lattice L is the set of pairs $(x,y) \in \mathbb{Z}^2$ such that $3x + 2y \equiv 0 \pmod 4$, *i.e.* $x \equiv 2y \pmod 4$. It is represented on Figure 1. It contains the points $\boldsymbol{w}_1 = (4,0)$, $\boldsymbol{w}_2 = (0,2)$ and $\boldsymbol{w} = (2,1)$ and the families $(\boldsymbol{w}_1, \boldsymbol{w})$ and $(\boldsymbol{w}_2, \boldsymbol{w})$ are two bases of L.

One can then form the corresponding codes $\mathcal{C}_1(c) := \mathrm{LRM}(\boldsymbol{e}; cS_{(\boldsymbol{w}_1,\boldsymbol{w})})$ and $\mathcal{C}_2(c) := \mathrm{LRM}(\boldsymbol{e}; cS_{(\boldsymbol{w}_2,\boldsymbol{w})})$ for $c < q-1$. We infer from Theorem 2.8 that they have minimum distance at least $4\cdot(q-1)\cdot(q-1-c)$. Moreover it is easy, in our case, to compute exactly the polynomials $P_{(\boldsymbol{w}_1,\boldsymbol{w})}$ and $P_{(\boldsymbol{w}_2,\boldsymbol{w})}$, which will eventually give the dimension of the codes $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively. Indeed, we know that they take the form $P_{(\boldsymbol{w}_i,\boldsymbol{w})}(x) = 2x^2 + a_i x + 1$ where a_i is the unique unknown coefficient. One can find it by evaluating at $x = 1$: counting the integer points insides $S_{(\boldsymbol{w}_i,\boldsymbol{w})}$, we find that $P_{(\boldsymbol{w}_1,\boldsymbol{w})}(x) = 6$ and $P_{(\boldsymbol{w}_2,\boldsymbol{w})}(x) = 5$ from what we finally derive:

$$P_{(\boldsymbol{w}_1,\boldsymbol{w})}(x) = 2x^2 + 3x + 1 \quad \text{and} \quad P_{(\boldsymbol{w}_2,\boldsymbol{w})}(x) = 2x^2 + 2x + 1.$$

The dimension of $\mathcal{C}_1(c)$ (resp. of $\mathcal{C}_2(c)$) is then exactly $2c^2 + 3c + 1$ (resp. $2c^2 + 2c + 1$) for any c. We observe that the former is greater than the latter, and that both of them are larger than $\binom{c+2}{2} = \frac{c(c+1)}{2}$ by a factor of at least $r = 4$.

Remark 2.10. The Ehrhart's polynomial $P_{(\boldsymbol{w}_1,\boldsymbol{w})}(x)$ factors as $(x+1)(2x+1)$ and meets the upper bound (7). This is in fact not a surprise because the code $\mathcal{C}_1(c)$ is isomorphic to a "almost commutative" linearized Reed–Muller code through the transformation $X_1 \mapsto X_1$, $X_2 \mapsto X_1^{-2}X_2$.

Although $(\boldsymbol{w}_1, \boldsymbol{w}_2)$ is not a basis of L, it makes sense to consider the code $\mathcal{C}(c) := \mathrm{LRM}(\boldsymbol{e}; cS_{(\boldsymbol{w}_1,\boldsymbol{w}_2)})$. Using a variation on Remark 2.5, one can prove that its minimum

distance is at least $4(q-1)(q-1-2c)$. For $c < \frac{q-1}{2}$, Ehrhart's result then implies that its dimension is $4c^2+4c+1 = (2c+1)^2$.

3. Embeddings into LAG codes

An nice feature of classical Reed–Muller codes is that they can be embedded in large Reed–Solomon codes [PW04], a property which notably allows for efficient decoding.

In this section, we highlight a similar feature for the codes $\mathrm{LRM}(\boldsymbol{e}; cS_{\underline{\boldsymbol{w}}})$ introduced in Subsection 2.3. The main difference is that the latter codes will not embed into linearized Reed–Solomon codes but in some linearized Algebraic Geometry (LAG) codes, which were recently introduced by the same authors in [BC24]. Unfortunately, no efficient decoding algorithm for LAG codes have been designed so far. However, it looks feasible to extend standard methods for decoding AG codes to the linearized setting; we hope to come back on this question soon.

3.1. **Quick review on LAG codes.** We briefly review the theory of LAG codes as developed in [BC24]. Since we will be using them in a very special case, we only focus on this particular setting (which actually avoids talking about algebraic curves). On the contrary, for our purpose, we will need to use LAG codes defined over extensions of $\mathbb{F}_q$. That is why, for better consistency, we prefer as of now considering a positive integer n and working over $\mathbb{F}_{q^n}$.

We pick in addition a second positive integer r and form the finite field $\mathbb{F}_{q^{nr}}$, which is an extension of $\mathbb{F}_{q^n}$ of degree r. Let $\Phi_n : \mathbb{F}_{q^{nr}} \to \mathbb{F}_{q^{nr}}$, $x \mapsto x^{q^n}$ be the relative Frobenius of $\mathbb{F}_{q^{nr}}/\mathbb{F}_{q^n}$, and let $\theta = \Phi_n^e$ for some integer e, coprime with r. We also consider a new variable Y and denote by $\mathbb{F}_{q^{nr}}(Y)$ the field of rational functions in Y. The morphism θ extends naturally to an automorphism $\mathbb{F}_{q^{nr}}(Y) \to \mathbb{F}_{q^{nr}}(Y)$ by acting on the coefficients and letting Y unchanged; in a slight abuse of notation, we continue to call θ this extended morphism.

In order to define our LAG codes, we need extra data. First of all, we consider a polynomial $P(Y) \in \mathbb{F}_{q^n}[Y]$ and, following [BC24], we form the quotient

$$D_P = \mathbb{F}_{q^{nr}}(Y)[T;\theta]/(T^r - P(Y)). \tag{9}$$

Lemma 3.1. *We assume that the gcd of the orders of vanishing of $P(Y)$ at all points $y \in \mathbb{F}_{q^n}$ is coprime with r. Then D_P is a division algebra.*

Proof. We recall from [Rei75, §31] that, to any central simple algebra C over $\mathbb{F}_q(Y)$, one can associate a family of local invariants $\mathrm{inv}_{\mathfrak{p}}(C) \in \mathbb{Q}/\mathbb{Z}$ indexed by the places $\mathfrak{p}$ of $F(Y)$. They satisfy in addition the following two properties:

(i) the invariants of C are the same than the invariants of $M_n(C)$ for all $n > 0$ (see [Rei75, §28])
(ii) if C has dimension s^2 over $F(Y)$, the invariants of C are all in $s^{-1}\mathbb{Z}/\mathbb{Z}$ (see [Rei75, Theorem 29.22]).

Besides, the invariants of D_P are easy to write down; indeed, it follows from [Rei75, Equation (31.7)] that

$$\mathrm{inv}_{\mathfrak{p}}(D_P) = \frac{v_{\mathfrak{p}}\big(P(Y)\big)}{r} \in \mathbb{Q}/\mathbb{Z}$$

where $v_{\mathfrak{p}}$ is the normalized valuation associated to the place $\mathfrak{p}$. In particular, when $\mathfrak{p} = \mathfrak{p}_y$ is the place corresponding to a point $y \in \mathbb{F}_{q^n}$, the invariant $\mathrm{inv}_{\mathfrak{p}_y}(D_P)$ is $-\mathrm{ord}_y(P(Y))/r \bmod \mathbb{Z}$.

We now invoke the Artin–Wedderburn theorem [Rei75, Theorem 7.4] which tells us that D_P has to be isomorphic to a matrix algebra over a division algebra Δ over $\mathbb{F}_q(Y)$. Write $\dim_{\mathbb{F}_q(Y)} \Delta = s^2$. Using the properties recalled earlier, we find that

$$-\frac{\mathrm{ord}_y(P(Y))}{r} \equiv \mathrm{inv}_{\mathfrak{p}_y}(D_P) = \mathrm{inv}_{\mathfrak{p}_y}(\Delta) \in s^{-1}\mathbb{Z}/\mathbb{Z}$$

for all $y \in \mathbb{F}_{q^n}$. In other words $s \cdot \mathrm{ord}_y(P(Y)) \in r\mathbb{Z}$ for all $y \in \mathbb{F}_{q^n}$. Since the gcd of $\mathrm{ord}_y(P(Y))$ (for y running over $\mathbb{F}_{q^n}$) is coprime with r, Bézout's theorem shows that s must lie in $r\mathbb{Z}$ as well. Thus $s = r$, which further implies by comparing dimensions that $D_P = \Delta$ and finally that D_P is itself a division algebra. □

For now on, we assume that the hypothesis of Lemma 3.1 is fulfilled. Another important ingredient we need is the notion of Riemann–Roch space inside D_P. For our purpose, we will only need them in a particular case, so we restrict ourselves to this one (see [BC24, Subsection 2.2] for the general definition).

Definition 3.2. To each nonnegative integer v, we attach the *Riemann–Roch space* $\Lambda_P(v)$ defined as the $\mathbb{F}_{q^{nr}}$-vector subspace of D_P consisting of Ore polynomials of the form $\sum_{i=0}^{r-1} \frac{u_i(Y)}{v_i(Y)} T^i$ where, for all i, the polynomials $u_i(Y), v_i(Y) \in \mathbb{F}_{q^{nr}}(Y)$ are subject to the following conditions:

- $\gcd(u_i(Y), v_i(Y)) = 1$,
- $r \cdot \big(\deg u_i(Y) - \deg v_i(Y)\big) + i \cdot \deg P(Y) \leq v$,
- $v_i(Y)^r$ divides $P(Y)^i$.

Remark 3.3. We note that $\Lambda_P(v)$ contains the following simpler space

$$\widetilde{\Lambda}_P(v) = \left\{ \sum_{i=0}^{r-1} u_i(Y) T^i \ : \ u_i(Y) \in \mathbb{F}_{q^{nr}}[Y],\, r \cdot \deg u_i(Y) + i \cdot \deg P(Y) \leq v \right\},$$

which is in fact the one we will work with afterwards.

We also define $\Lambda_P = \Lambda_P(\infty)$ as the union of the $\Lambda_P(v)$ when v varies; it is a subalgebra of D_P. We consider elements $y_1, \dots, y_s \in \mathbb{F}_{q^n}$ such that $P(y_i) \neq 0$ for all i. By [BC24, Lemmas 1.1 & 3.2], the latter assumption implies the existence of isomorphisms

$$\eta_i : \Lambda_P / (Y - y_i)\Lambda_P \xrightarrow{\sim} \mathrm{End}_{\mathbb{F}_{q^n}}(\mathbb{F}_{q^{nr}}). \tag{10}$$

We combine them into a unique multievaluation map

$$\eta = (\eta_1, \dots, \eta_s) : \Lambda_P \longrightarrow \mathrm{End}_{\mathbb{F}_{q^n}}(\mathbb{F}_{q^{nr}})^s.$$

Definition 3.4. The *linearized Algebraic Geometry* code attached to the previous data is

$$\mathrm{LAG}\big(P(Y);\, v;\, y_1, \dots, y_s\big) = \eta\big(\Lambda_P(v)\big).$$

By definition, the code $\mathrm{LAG}\big(P(Y);\, v;\, y_1, \dots, y_s\big)$ sits in $\mathrm{End}_{\mathbb{F}_{q^n}}(\mathbb{F}_{q^{nr}})^s$. The latter is a vector space over $\mathbb{F}_{q^{nr}}$ of dimension sr, the length of the code. We notice moreover that the ambient space $\mathrm{End}_{\mathbb{F}_{q^n}}(\mathbb{F}_{q^{nr}})^s$ is naturally equipped with the sum-rank metric; hence it makes sense to talk about the minimum sum-rank distance of the code $\mathrm{LAG}\big(P(Y);\, v;\, y_1, \dots, y_s\big)$. It follows from [BC24, Theorem 3.5] that this minimum distance is at least

$$d^\star\big(\mathrm{LAG}\big(P(Y);\, v;\, y_1, \dots, y_s\big)\big) := sr - v. \tag{11}$$

In what follows, this lower bound will be called the *designed minimum distance* of $\mathrm{LAG}\big(P(Y);\, v;\, y_1, \dots, y_s\big)$.

3.2. **Relating the centre to a univariate rational function field.** We now come back to the setting of Section 2: we consider the multivariate Ore algebra $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$ where $\boldsymbol{X} = (X_1, \dots, X_m)$ and $\boldsymbol{\theta} = (\theta_1, \dots, \theta_m)$ with $\theta_i = \Phi^{e_i}$ and $\Phi : \mathbb{F}_{q^r} \to \mathbb{F}_{q^r}$ is the Frobenius $x \mapsto x^q$. We assume as usual that $\gcd(e_1, \dots, e_m, r) = 1$ and write $\boldsymbol{e} = (e_1, \dots, e_m)$. We recall that the centre of $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$ is $\mathbb{F}_q[\boldsymbol{X}^L]$ where L is the lattice

$$L = \big\{\, \boldsymbol{u} = (u_1, \dots, u_m) \in \mathbb{Z}^m \mid \boldsymbol{e} \cdot \boldsymbol{u} \in r\mathbb{Z} \,\big\}.$$

From now, we fix a $\mathbb{Z}$-basis $\underline{\boldsymbol{w}} = (\boldsymbol{w}_1, \dots, \boldsymbol{w}_m)$ of L. This choice gives rise to an isomorphism between $\mathbb{F}_q[\boldsymbol{X}^L]$ and the multivariate Laurent polynomial ring $\mathbb{F}_q[Z_1^{\pm 1}, \dots, Z_m^{\pm 1}]$ where the variable Z_i corresponds to $\boldsymbol{X}^{\boldsymbol{w}_i}$. To shorten notation, we use again bold symbols for tuples and set $\boldsymbol{Z} = (Z_1, \dots, Z_m)$ and $\mathbb{F}_q[\boldsymbol{Z}^{\pm 1}] = \mathbb{F}_q[Z_1^{\pm 1}, \dots, Z_m^{\pm 1}]$.

The first step in our construction is to relate $\mathbb{F}_q[\boldsymbol{X}^L] \simeq \mathbb{F}_q[\boldsymbol{Z}^{\pm 1}]$ to the univariate rational function field $\mathbb{F}_{q^n}(Y)$ for any $n \geq m$. In order to do so, we choose a basis $(b_1, \dots, b_n)$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. For each $i \in \{1, \dots, n\}$, we define the $\mathbb{F}_q$-linear form

$$\beta_i : \mathbb{F}_{q^n} \to \mathbb{F}_q, \quad y \mapsto \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b_i y)$$

where $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ is the trace map. It is a well-known fact (see *e.g.* [Lan02, Theorem VI.5.2]) that the β_i's form a basis of $\mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_{q^n}, \mathbb{F}_q)$. Hence the map $\beta = (\beta_1, \dots, \beta_n) : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$ is a $\mathbb{F}_q$-linear isomorphism. Let E be the inverse image by β of $\mathbb{F}_q^m \times \{0\}^{n-m} \subset \mathbb{F}_q^n$, *i.e.* $E = \bigcap_{j>m} \ker \beta_j$. By what precedes, it is a $\mathbb{F}_q$-vector space of dimension m; more precisely, $\beta_{\leq m} := (\beta_1, \dots, \beta_m)$ induces an isomorphism between E and $\mathbb{F}_q^m$. The following lemma asserts that $\beta_{\leq m}$ is a polynomial function of controlled degree.

Lemma 3.5. *There exist polynomials $B_1(Y), \dots, B_m(Y) \in \mathbb{F}_{q^n}[Y]$ of degree at most q^{m-1} such that $\beta_i(y) = B_i(y)$ for all $y \in E$ and all $i \in \{1, \dots, m\}$.*

Proof. We consider the ring of univariate Ore polynomials $\mathbb{F}_{q^n}[U; \Phi]$ where $\Phi : x \mapsto x^q$ is the Frobenius and U is again a new variable. We recall from [Ore33] that it is left and right

Euclidean. In particular, it is left and right principal and it admits left and right gcd and lcm. We consider the standard evaluation morphism

$$\varepsilon : \mathbb{F}_{q^n}[U;\Phi] \longrightarrow \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n}), \quad f \mapsto f(\Phi).$$

Each β_i defines an element in $\mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ and we check that $\beta_i = \varepsilon(T_i)$ with

$$\begin{aligned} T_i &= \left(1 + U + U^2 + \cdots + U^{n-1}\right) \cdot b_i \\ &= b_i + b_i^q U + b_i^{q^2} U^2 + \cdots + b_i^{q^{n-1}} U^{n-1}. \end{aligned}$$

Let $\mathcal{I}$ be the left ideal of $\mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ consisting of endomorphisms vanishing on E. Coming back to the definition of E, we infer that $\varepsilon^{-1}(\mathcal{I})$ is the principal left ideal generated by $T_{>m} = \mathrm{rgcd}(T_{m+1}, \ldots, T_n)$, where the notation rgcd refers to the right gcd. Hence, ε induces a $\mathbb{F}_{q^n}$-linear isomorphism

$$\bar{\varepsilon} : \mathbb{F}_{q^n}[U;\Phi] \,/\, \mathbb{F}_{q^n}[U;\Phi]\cdot T_{>m} \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{F}_q}(E, \mathbb{F}_{q^n}).$$

By comparing dimensions, we derive that the degree of $T_{>m}$ is equal to m. Let $i \in \{1, \ldots, m\}$. The restriction of β_i to E, namely $\beta_{i|E}$, can be seen as an element of $\mathrm{Hom}_{\mathbb{F}_q}(E, \mathbb{F}_{q^n})$. Let $\widetilde{B}_i$ by the unique representative of $\bar{\varepsilon}^{-1}\big(\beta_{i|E}\big)$ of degree at most $m-1$. By definition, we have $\widetilde{B}_i(\Phi)(y) = \beta_i(y)$ for all $y \in E$. Finally, given that Φ itself is a polynomial function of degree q, we find that $\widetilde{B}_i(\Phi)$ is a polynomial function of degree $q^{\deg \widetilde{B}_i} \leq q^{m-1}$. This concludes the proof by setting $B_i = \widetilde{B}_i(\Phi)$. □

Remark 3.6. The polynomial $B_i(Y)$ vanishes on the space $E_i := E \cap \ker \beta_i$, which has cardinality q^{m-1}. Therefore, there must exist a nonzero constant $c_i \in \mathbb{F}_{q^n}^\times$ such that

$$B_i(Y) = c_i \cdot \prod_{y \in E_i} (Y - y).$$

In particular, we notice that $B_i(Y)$ is separable and has exactly degree q^{m-1}.

We use the polynomials $B_1(Y), \ldots, B_m(Y)$ of Lemma 3.5 to build the following morphism of $\mathbb{F}_q$-algebras

$$\begin{array}{rccc} \zeta : & \mathbb{F}_q[\boldsymbol{X}^L] \simeq \mathbb{F}_q[\boldsymbol{Z}^{\pm 1}] & \longrightarrow & \mathbb{F}_{q^n}\left[Y, \frac{1}{B(Y)}\right] \subset \mathbb{F}_{q^n}(Y) \\ & Z_i & \mapsto & B_i(Y) \end{array}$$

where we have set $B(Y) = B_1(Y) \cdots B_m(Y)$ for simplicity. We take a few moment to describe the action of ζ on evaluation points. To start with, we recall from Subsection 1.1 that an evaluation point for $\mathbb{F}_q[\boldsymbol{X}^L]$ is given by a group homomorphism $\gamma : L \to \mathbb{F}_q^\times$. Transferring it *via* the identification $\mathbb{F}_q[\boldsymbol{X}^L] \simeq \mathbb{F}_q[\boldsymbol{Z}^{\pm 1}]$, it simply corresponds to the multi-evaluation point $\big(\gamma(\boldsymbol{w}_1), \ldots, \gamma(\boldsymbol{w}_m)\big)$. From this, it is routine to check that the following

diagram commutes

$$\begin{array}{ccc} \mathbb{F}_q[\boldsymbol{X}^L] & \xrightarrow{\zeta} & \mathbb{F}_{q^n}\left[Y, \frac{1}{B(Y)}\right] \\ \Big\downarrow{\scriptstyle \varepsilon_\gamma} & & \Big\downarrow{\scriptstyle Y \mapsto \beta_{\leq m}^{-1}(\gamma(\boldsymbol{w}_1),\ldots,\gamma(\boldsymbol{w}_m))} \\ \mathbb{F}_q & \longrightarrow & \mathbb{F}_{q^n} \end{array} \tag{12}$$

where the bottom arrow is the canonical inclusion. In other words, we have shown that γ corresponds to the evaluation point $\beta_{\leq m}^{-1}\big(\gamma(\boldsymbol{w}_1),\ldots,\gamma(\boldsymbol{w}_m)\big)$.

3.3. **Extension to the Ore algebra.** So far, we have constructed a morphism $\zeta : \mathbb{F}_q[\boldsymbol{X}^L] \to \mathbb{F}_{q^n}(Y)$ which, in some sense, relates the multivariate case to the univariate one. The next step in the construction is to extend ζ to the Ore algebra $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$. For this, we recall that the map $\boldsymbol{u} \mapsto \boldsymbol{e}\cdot\boldsymbol{u}$ induces a group isomorphism $\mathbb{Z}^m/L \to \mathbb{Z}/r\mathbb{Z}$. We choose a vector $\boldsymbol{v} \in \mathbb{Z}^m$ such that $\boldsymbol{e}\cdot\boldsymbol{v} \equiv 1 \pmod r$. By what precedes $\mathbb{Z}^m$ is generated as a group by L and $\boldsymbol{v}$. Therefore $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$ is generated as an algebra by its centre $\mathbb{F}_q[\boldsymbol{X}^L]$ and the monomial $\boldsymbol{X}^{\boldsymbol{v}}$. Besides, by our choice of $\boldsymbol{v}$, the commutation relation $\boldsymbol{X}^{\boldsymbol{v}} \cdot a = \Phi(a) \cdot \boldsymbol{X}^{\boldsymbol{v}}$ holds for all $a \in \mathbb{F}_{q^r}$. It follows from this observation that we have a surjective morphism

$$\begin{array}{ccc} \mathbb{F}_q[\boldsymbol{X}^L] \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}[T;\Phi] & \longrightarrow & \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}] \\ T & \mapsto & \boldsymbol{X}^{\boldsymbol{v}} \end{array}.$$

The kernel of this map obviously contains the ideal generated by $T^r - \boldsymbol{X}^{r\boldsymbol{v}}$ (note that $r\boldsymbol{v} \in L$); by comparing dimensions, we conclude that the reverse inclusion also holds true. Consequently, we get an isomorphism of $\mathbb{F}_q$-algebras

$$\alpha : \mathbb{F}_q[\boldsymbol{X}^L] \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}[T;\Phi]/(T^r - \boldsymbol{X}^{r\boldsymbol{v}}) \xrightarrow{\sim} \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}].$$

Composing the inverse of α by $\zeta \otimes \mathrm{id}$, we obtain a second morphism

$$\iota : \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}] \longrightarrow \mathbb{F}_{q^n}\left[Y, \tfrac{1}{B(Y)}\right] \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}[T;\Phi]/(T^r - P(Y))$$

where, by definition, $P(Y) = \zeta(\boldsymbol{X}^{r\boldsymbol{v}}) \in \mathbb{F}_{q^n}[Y]$.

From now on, we assume that, in addition to be greater or equal to m, the integer n is chosen in such a way that $\gcd(n, r) = 1$. The extensions $\mathbb{F}_{q^n}$ and $\mathbb{F}_{q^r}$ are then linearly disjoint over $\mathbb{F}_q$, implying that the tensor product $\mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}$ is a field. Since the latter has cardinality q^{rm}, it must be isomorphic to $\mathbb{F}_{q^{nr}}$. Therefore, the codomain of ι is isomorphic to

$$\mathbb{F}_{q^{nr}}\left[Y, \tfrac{1}{B(Y)}\right][T;\theta]/(T^r - P(Y)) \tag{13}$$

where θ is the automorphism acting as the identity on the subfield $\mathbb{F}_{q^n}$ and as $x \mapsto x^q$ on the subfield $\mathbb{F}_{q^r}$. From these properties, we infer that $\theta = \Phi_n^{n'}$ where n' is a multiplicative inverse of n modulo r and we recall that Φ_n is the relative Frobenius of $\mathbb{F}_{q^{nr}}/\mathbb{F}_{q^n}$, *i.e.* $\Phi_n : x \mapsto x^{q^n}$. In Equation (13), we recognize an integral version of the algebra

$$D_P = \mathbb{F}_{q^{nr}}(Y)[T;\theta]/(T^r - P(Y))$$

already considered in Subsection 3.1; precisely, the algebra of Equation (13) is $\Lambda_P\left[\frac{1}{B(Y)}\right]$ where Λ_P was introduced right after Definition 3.2.

Lemma 3.7. *D_P is a division algebra.*

Proof. Let $\mu_1, \dots, \mu_m \in \mathbb{Z}$ be the coordinates of $r\boldsymbol{v}$ in the basis $(\boldsymbol{w}_1, \dots, \boldsymbol{w}_m)$, so that we have $r\boldsymbol{v} = \mu_1\boldsymbol{w}_1 + \cdots + \mu_m\boldsymbol{w}_m$. Taking the scalar product of this equality by $\boldsymbol{e}$, we find the relation

$$\boldsymbol{v}\cdot\boldsymbol{e} = \mu_1 \cdot \frac{\boldsymbol{w}_1\cdot\boldsymbol{e}}{r} + \cdots + \mu_m \cdot \frac{\boldsymbol{w}_m\cdot\boldsymbol{e}}{r}.$$

Note that each quotient $(\boldsymbol{w}_i\cdot\boldsymbol{e})/r$ is an integer, given that $\boldsymbol{w}_i$ lies in L. Besides, by our choice of $\boldsymbol{v}$, we know that $\boldsymbol{v}\cdot\boldsymbol{e} \equiv 1 \pmod r$. Hence, we deduce that $\gcd(\mu_1, \dots, \mu_m, r) = 1$.

Thanks to Lemma 3.1, it suffices to find elements $y_1, \dots, y_m \in \mathbb{F}_{q^n}$ such that the order of vanishing of $P(Y)$ at y_i is μ_i for all i. For this, note that $P(Y) = \zeta(\boldsymbol{X}^{r\boldsymbol{v}}) = B_1(Y)^{\mu_1}\cdots B_m(Y)^{\mu_m}$. Moreover, we know from Remark 3.6 that the $B_i(y)$'s are all separable. Therefore, it is enough to find $y_i \in \mathbb{F}_{q^n}$ which is a root of $B_i(Y)$, but not a root of the other $B_j(Y)$'s. An element satisfying these requirements is, for example, $y_i = \beta_{\le m}^{-1}(1, \dots, 1, 0, 1, \dots, 1)$ where the 0 is in the ith position. □

We now aim at comparing evaluation points in the spirit of the diagram (12). In order to do so, we first recall that, each time we are given an element $y \in \mathbb{F}_{q^n}$ such that $P(y) \neq 0$, we have an evaluation map $\eta_y : \Lambda_P \longrightarrow \mathrm{End}_{\mathbb{F}_{q^n}}(\mathbb{F}_{q^{nr}})$ whose kernel is the principal twosided ideal generated by $Y - y$. We note that η_y maps $B(Y)$ to the scalar multiplication by $B(y)$. Thus, if y is chosen outside the roots of $B(Y)$, the morphism η_y extends to a second homomorphism of $\mathbb{F}_{q^n}$-algebras

$$\Lambda_P\left[\frac{1}{B(Y)}\right] \longrightarrow \mathrm{End}_{\mathbb{F}_{q^n}}(\mathbb{F}_{q^{nr}})$$

that, in a slight abuse of notation, we continue to denote by η_y.

On the other hand, we recall from Subsection 1.1 that, whenever we are given a group homomorphism $\gamma : L \to \mathbb{F}_q^\times$ together with a prolongation $\widetilde{\gamma} : \mathbb{Z}^m \to \mathbb{F}_{q^r}^\times$ satisfying the axiom (1), we can build an evaluation map

$$\varepsilon_{\widetilde{\gamma}} : \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}] \longrightarrow \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}).$$

By Theorem 1.5, we know moreover that the kernel of $\varepsilon_{\widetilde{\gamma}}$ is the twosided ideal generated by the elements $\boldsymbol{X}^{\boldsymbol{u}} - \gamma(\boldsymbol{u})$, $\boldsymbol{u} \in L$. In particular, it only depends on γ, and not on the choice of the prolongation $\widetilde{\gamma}$.

Lemma 3.8. *Keeping the previous notation and setting $y = \beta_{\le m}^{-1}(\gamma(\boldsymbol{w}_1), \dots, \gamma(\boldsymbol{w}_m))$, the diagram*

$$\begin{array}{ccc} \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}] & \xrightarrow{\ \iota\ } & \Lambda_P\left[\frac{1}{B(Y)}\right] \\ \Big\downarrow{\scriptstyle \varepsilon_{\widetilde{\gamma}}} & & \Big\downarrow{\scriptstyle \eta_y} \\ \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}) & \longrightarrow & \mathrm{End}_{\mathbb{F}_{q^n}}(\mathbb{F}_{q^{nr}}) \end{array}$$

commutes up to conjugacy, i.e. there exists a $\mathbb{F}_{q^n}$-linear automorphism $h_{\widetilde{\gamma}} : \mathbb{F}_{q^{nr}} \to \mathbb{F}_{q^{nr}}$ such that

$$\eta_y\big(\iota(f)\big) = h_{\widetilde{\gamma}}^{-1} \circ \big(\mathrm{id}_{\mathbb{F}_{q^n}} \otimes \varepsilon_{\widetilde{\gamma}}(f)\big) \circ h_{\widetilde{\gamma}}$$

for all $f \in \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$.

Proof. It follows from Theorem 1.5 that, after scalar extension to $\mathbb{F}_{q^n}$, $\varepsilon_{\widetilde{\gamma}}$ induces an isomorphism of $\mathbb{F}_{q^n}$-algebras

$$\mathrm{id}_{\mathbb{F}_{q^n}} \otimes \varepsilon_{\widetilde{\gamma}}(f) : \mathbb{F}_{q^{nr}}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}] / \mathfrak{m}_\gamma \mathbb{F}_{q^{nr}}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}] \xrightarrow{\sim} \mathrm{End}_{\mathbb{F}_{q^n}}(\mathbb{F}_{q^{nr}}) \tag{14}$$

where we recall that $\mathfrak{m}_\gamma = \ker \varepsilon_\gamma$. On the other hand, we deduce from Equation (10) that η_y induces an isomorphism of $\mathbb{F}_{q^n}$-algebras

$$\eta_y : \Lambda_P\left[\tfrac{1}{B(Y)}\right] / (Y - y)\Lambda_P\left[\tfrac{1}{B(Y)}\right] \xrightarrow{\sim} \mathrm{End}_{\mathbb{F}_{q^n}}(\mathbb{F}_{q^{nr}}).$$

Looking at the diagram (12), we find that the inverse image by ι of the ideal generated by $Y - y$ is the ideal generated by $\mathfrak{m}_\gamma$. As a consequence, the composite $\eta_y \circ \iota$ induces another isomorphism

$$\eta_y \circ \iota : \mathbb{F}_{q^{nr}}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}] / \mathfrak{m}_\gamma \mathbb{F}_{q^{nr}}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}] \xrightarrow{\sim} \mathrm{End}_{\mathbb{F}_{q^n}}(\mathbb{F}_{q^{nr}}). \tag{15}$$

We conclude by invoking the Skolem–Noether theorem, which ensures that the isomorphisms (14) and (15) have to be conjugated by an element in $\mathrm{GL}_{\mathbb{F}_{q^n}}(\mathbb{F}_{q^{nr}})$. □

3.4. **Comparison of codes.** After this long preparation, we are now ready to relate the code $\mathrm{LRM}(\boldsymbol{e}; cS_{\underline{\boldsymbol{w}}})$ to some well-chosen LAG code. To start with, let us recall briefly from Subsection 2.1 that the former is defined as the image of $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]_{cS_{\underline{\boldsymbol{w}}}}$ under the multi-evaluation morphism

$$\begin{array}{rccc} \varepsilon : & \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}] & \longrightarrow & \prod_{\gamma \in H} \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}) \\ & f & \mapsto & \varepsilon_{\widetilde{\gamma}}(f) \end{array}$$

where $H = \mathrm{Hom}_{\mathrm{grp}}(L, \mathbb{F}_q^\times)$ and for each $\gamma \in H$, we have chosen a cocycle $\widetilde{\gamma} : \mathbb{Z}^m \to \mathbb{F}_{q^r}^\times$ extending γ. Recall also that, in what precedes, $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]_{cS_{\underline{\boldsymbol{w}}}}$ is the $\mathbb{F}_{q^r}$-linear subspace of $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}]$ spanned by the monomial $\boldsymbol{X}^{\boldsymbol{u}}$, $\boldsymbol{u} \in cS_{\underline{\boldsymbol{w}}}$.

We now contemplate the commutative diagram of Lemma 3.8. Taking the product over all $\gamma \in H$, the following diagram also commutes up to conjugacy:

$$\begin{array}{ccc} \mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1}; \boldsymbol{\theta}] & \xrightarrow{\quad\iota\quad} & \Lambda_P\left[\tfrac{1}{B(Y)}\right] \\ \Big\downarrow{\scriptstyle \varepsilon} & & \Big\downarrow{\scriptstyle \eta = (\eta_y)_{y \in I}} \\ \prod_{\gamma \in H} \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}) & \longrightarrow & \prod_{y \in I} \mathrm{End}_{\mathbb{F}_{q^n}}(\mathbb{F}_{q^{nr}}) \end{array}$$

where the index set I is $\beta_{\leq m}^{-1}\big((\mathbb{F}_q^\times)^m\big)$ and the arrow on the bottom is induced by the correspondence $H \simeq I$, $\gamma \mapsto y = \beta_{\leq m}^{-1}(\gamma(\boldsymbol{w}_1), \ldots, \gamma(\boldsymbol{w}_m))$. As a consequence, if we can

prove that ι takes $\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1};\boldsymbol{\theta}]_{cS_{\underline{\boldsymbol{w}}}}$ to some explicit Riemann–Roch space inside $\Lambda_P\left[\frac{1}{B(Y)}\right]$, we will infer a relation between $\mathrm{LRM}(\boldsymbol{e};\, cS_{\underline{\boldsymbol{w}}})$ and a suitable LAG code. This is achieved in the next lemma.

Lemma 3.9. *We have* $\iota\big(\mathbb{F}_{q^r}[\boldsymbol{X}^{\pm 1};\boldsymbol{\theta}]_{cS_{\underline{\boldsymbol{w}}}}\big) \subset \Lambda_P\big(q^{m-1}rc\big)$.

Proof. By linearity, it is enough to prove that $\iota(\boldsymbol{X}^{\boldsymbol{u}}) \in \Lambda_P\big(q^{m-1}rc\big)$ for all $\boldsymbol{u} \in cS_{\underline{\boldsymbol{w}}}$. For this, we write $\boldsymbol{u} = \boldsymbol{w} + \lambda \boldsymbol{v}$ with $\boldsymbol{w} \in L$, $\lambda \in \{0,\dots,r-1\}$, and where $\boldsymbol{v}$ is the special vector we fixed at the beginning of Subsection 3.3. We decompose $\boldsymbol{w}$ and $r\boldsymbol{v}$, which are both elements of L, on the basis $(\boldsymbol{w}_1,\dots,\boldsymbol{w}_m)$, namely we write $\boldsymbol{w} = \lambda_1\boldsymbol{w}_1 + \cdots + \lambda_m\boldsymbol{w}_m$ and $r\boldsymbol{v} = \mu_1\boldsymbol{w}_1 + \cdots + \mu_m\boldsymbol{w}_m$, where the λ_i and the μ_i are integers. From these equalities, we derive

$$\boldsymbol{u} = \left(\lambda_1 - \frac{\lambda}{r}\mu_1\right)\boldsymbol{w}_1 + \cdots + \left(\lambda_m - \frac{\lambda}{r}\mu_m\right)\boldsymbol{w}_m$$

and the assumption that $\boldsymbol{u} \in cS_{\underline{\boldsymbol{w}}}$ tells us that

$$r\lambda_i - \lambda\mu_i \geq 0 \quad \text{for all } i \qquad \text{and} \qquad \sum_{i=1}^{m} r\lambda_i - \lambda\mu_i \leq rc. \tag{16}$$

On the other hand, it follows from the definition of ι that

$$\iota(\boldsymbol{X}^{\boldsymbol{u}}) = \iota(\boldsymbol{X}^{\boldsymbol{w}_1})^{\lambda_1}\cdots\iota(\boldsymbol{X}^{\boldsymbol{w}_m})^{\lambda_m}\cdot\iota(\boldsymbol{X}^{\boldsymbol{v}})^{\lambda} = B_1(Y)^{\lambda_1}\cdots B_m(Y)^{\lambda_m}\cdot T^{\lambda}.$$

Hence, in order to prove that $\iota(\boldsymbol{X}^{\boldsymbol{u}}) \in \Lambda_P\big(q^{m-1}rc\big)$, we have to check that

$$-\lambda\cdot\deg P(Y) + r\cdot\sum_{i=1}^{m}\lambda_i \deg B_i(Y) \leq q^{m-1}rc.$$

This follows directly from Equation (16) after remembering that $\deg B_i(Y) \leq q^{m-1}$ for all i (see Lemma 3.5) and that $P(Y) = \iota(\boldsymbol{X}^{r\boldsymbol{v}}) = B_1(Y)^{\mu_1}\cdots B_m(Y)^{\mu_m}$, which ensures that $\deg P(Y) = \sum_{i=1}^{m}\mu_i \deg B_i(Y)$. □

Finally, we have proved the following theorem.

Theorem 3.10. *With the previous notation, the code* $\mathbb{F}_{q^n}\otimes_{\mathbb{F}_q}\mathrm{LRM}\big(\boldsymbol{e};cS_{\underline{\boldsymbol{w}}}\big)$ *is isomorphic to a subcode of* $\mathrm{LAG}\big(P(Y);q^{m-1}rc;I\big)$. *Moreover the isomorphism is explicit and it preserves the sum-rank distance.*

We emphasize that the theorem is valid for any integer $n \geq m$ which is coprime with r; in particular, we can always choose n in the range $[m, m+r]$. On a different note, it is also instructive to compare the designed minimum distances of $\mathrm{LRM}\big(\boldsymbol{e};cS_{\underline{\boldsymbol{w}}}\big)$ and $\mathrm{LAG}\big(P(Y);q^{m-1}rc;I\big)$. After Theorem 2.8 and Equation (11), we have the following explicit values for them:

$$\begin{aligned} d^{\star}\big(\mathrm{LRM}\big(\boldsymbol{e};cS_{\underline{\boldsymbol{w}}}\big)\big) &= (q-1)^m r - (q-1)^{m-1}rc, \\ d^{\star}\big(\mathrm{LAG}\big(P(Y);\, q^{m-1}rc;\, I\big)\big) &= (q-1)^m r - q^{m-1}rc. \end{aligned}$$

We observe that they almost coincide apart from the factor $(q-1)^{m-1}$ which is replaced by q^{m-1} in the second case. The conclusion is that the embedding of $\mathrm{LRM}\big(\boldsymbol{e}; cS_{\underline{\boldsymbol{w}}}\big)$ in $\mathrm{LAG}\big(P(Y); q^{m-1}rc; I\big)$ does not alter too much the (designed) minimum distance. Hence, any efficient decoder for linearized Algebraic Geometry codes will provide a barely less efficient decoder for linearized Reed–Muller codes of the type $\mathrm{LRM}\big(\boldsymbol{e}; cS_{\underline{\boldsymbol{w}}}\big)$.

Remark 3.11. In the "almost commutative" case (see §2.4.1), the embedding of Theorem 3.10 extends to an embedding (up to conjugacy)

$$\mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} \widetilde{\mathrm{LRM}}\big(\boldsymbol{e}; cS_{\underline{\boldsymbol{w}}}\big) \hookrightarrow \mathrm{LAG}\big(P(Y); q^{m-1}rc; \widetilde{I}\big)$$

with $\widetilde{I} = \beta_{\leq m}^{-1}(\mathbb{F}_q^{m-1} \times \mathbb{F}_q^{\times})$. The designed minimum distance of the involved LAG code is now

$$d^\star\big(\mathrm{LAG}\big(P(Y);\, q^{m-1}rc;\, \widetilde{I}\big)\big) = q^{m-1}(q-1)r - q^{m-1}rc = q^{m-1}r \cdot (q-1-c)$$

which meets the designed distance of the extended linearized Reed–Muller code. In this case, the drop on the minimum distance has then been absorbed.

Acknowledgements. This work was funded by the grant ANR-21-CE39-0009-BARRACUDA.

REFERENCES

[ACLN21] Daniel Augot, Alain Couvreur, Julien Lavauzelle, and Alessandro Neri. Rank-metric codes over arbitrary Galois extensions and rank analogues of Reed–Muller codes. *SIAM Journal on Applied Algebra and Geometry*, 5(2):165–199, 2021.

[BC24] Elena Berardini and Xavier Caruso. Algebraic geometry codes in the sum–rank metric. *IEEE Transactions on Information Theory*, 70(5):3345–3356, 2024.

[BM85] Ulrich Betke and Peter McMullen. Lattice points in lattice polytopes. *Monatsh. Math.*, 99(4):253–265, 1985.

[DGMW70] Philippe Delsarte, Jean-Marie Goethals, and F. Jessie Mac Williams. On generalized Reed–Muller codes and their relatives. *Information and control*, 16(5):403–442, 1970.

[Ehr62] Eugène Ehrhart. Sur les polyèdres rationnels homothétiques à n dimensions. *C. R. Acad. Sci. Paris*, 254:616–618, 1962.

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

[GL23] Sudhir R. Ghorpade and Rati Ludhani. On the minimum distance, minimum weight codewords, and the dimension of projective Reed-Muller codes. *arXiv preprint arXiv:2309.10196*, 2023.

[GMPS23] Elisa Gorla, Umberto Martínez-Peñas, and Flavio Salizzoni. Sum-rank metric codes. *arXiv preprint arXiv:2304.12095*, 2023.

[KLP68] Tadao Kasami, Shu Lin, and W Peterson. New generalizations of the Reed-Muller codes–I: Primitive codes. *IEEE Transactions on information theory*, 14(2):189–199, 1968.

[Lac88] Gilles Lachaud. Projective Reed–Muller codes. In *Coding Theory and Applications: 2nd International Colloquium Cachan-Paris, France, November 24–26, 1986 Proceedings 2*, pages 125–129. Springer, 1988.

[Lac90] Gilles Lachaud. The parameters of projective Reed–Müller codes. *Discrete Mathematics*, 81(2):217–221, 1990.

[Lan02] Serge Lang. Algebra (revised third edition). *Graduate Text in Mathematics*, 2002.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite fields*. Number 20. Cambridge university press, 1997.

[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.

[Mul54] David E. Muller. Application of Boolean algebra to switching circuit design and to error detection. *Transactions of the IRE professional group on electronic computers*, (3):6–12, 1954.

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

[PW04] Ruud Pellikaan and Xin-Wen Wu. List decoding of q-ary Reed-Muller codes. *IEEE Transactions on Information Theory*, 50(4):679–682, 2004.

[Ree54] Irving S Reed. A class of multiple-error-correcting codes and the decoding scheme. *IEEE Transactions on Information Theory*, 4(4):38–49, 1954.

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

[Ser79] Jean-Pierre Serre. *Galois cohomology*. Springer, 1979.

[Ser89] Jean-Pierre Serre. Lettre à M. Tsfasman. *Astérisque*, 198:199–200, 1989.

[Sor91] Anders Bjaert Sorensen. Projective Reed–Muller codes. *IEEE Transactions on Information Theory*, 37(6):1567–1576, 1991.