Recursive decoding of binary rank Reed-Muller codes and Plotkin construction for matrix codes

Alain Couvreur, Rakhi Pratihar

Recursive decoding of binary rank Reed-Muller codes and Plotkin construction for matrix codes

Alain Couvreur and Rakhi Pratihar
Inria & Laboratoire LIX, CNRS UMR 7161, École Polytechnique, Institut Polytechnique de Paris,
1 rue Honoré d'Estienne d'Orves, 91120 Palaiseau Cedex
Email: {alain.couvreur, rakhi.pratihar}@inria.fr

***Abstract*—We give a recursive decoding algorithm of the rank metric Reed–Muller codes introduced by Augot, Couvreur, Lavauzelle and Neri in 2021 for the binary case, i.e., $\mathrm{G} = (\mathbb{Z}/2\mathbb{Z})^m$. In a broad range of parameters, this recursive decoding algorithm has better complexity compared to a recently proposed decoding algorithm based on Dickson matrices. Imitating the recursive structure, we introduce a Plotkin-like construction of matrix rank metric codes over finite fields and provide a decoding algorithm associated to this construction.**

Keywords: Binary rank metric Reed-Muller codes, decoding, matrix codes, Plotkin construction

I. Introduction

Rank metric codes were introduced by Delsarte [1] as set of $m \times n$ matrices over a finite field $\mathbb{F}_q$, whereas Gabidulin independently defined a variant of rank metric codes [2] as $\mathbb{F}_{q^m}$-linear subspaces of $\mathbb{F}_{q^m}^n$. Another framework for studying such codes was introduced in [3] as subspaces of skew group algebra $\mathbb{L}[\mathrm{G}]$ for arbitrary Galois extension $\mathbb{L}/\mathbb{K}$ with Galois group $\mathrm{G} = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. This framework has been particularly useful in defining a rank analogue of Reed-Muller codes, also called *$\boldsymbol{\theta}$-Reed–Muller codes* in [3], where $\boldsymbol{\theta} = (\theta_1, \dots, \theta_m)$ specifies a generating set of the abelian group G. These $\boldsymbol{\theta}$-Reed-Muller codes can be considered as "multivariate" version of Gabidulin codes which are defined for G cyclic. To recall their definitions, let $\mathbb{L}/\mathbb{K}$ be an abelian extension with $\mathrm{G} = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_m\mathbb{Z}$ with a system of generators $\theta_1, \dots, \theta_m$, where a $\boldsymbol{\theta}$-monomial $\theta_1^{i_1} \cdots \theta_m^{i_m}$ describes the m-tuple $(i_1, \dots, i_m) \in \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_m\mathbb{Z}$. Thus, every element in $\mathbb{L}[\mathrm{G}]$ have a unique representation as a $\boldsymbol{\theta}$-polynomial

$$P = \sum_{(i_1,\dots,i_m)} b_{(i_1,\dots,i_m)} \theta_1^{i_1} \cdots \theta_m^{i_m}.$$

We define $\deg_{\boldsymbol{\theta}}(P) \stackrel{\text{def}}{=} \max\{i_1 + \cdots + i_m \colon b_{(i_1,\dots,i_m)} \neq 0\}$. For $0 < r \leqslant \sum_{i=1}^m (n_i - 1)$, the $\boldsymbol{\theta}$-Reed-Muller code of order r and type $\boldsymbol{n} \stackrel{\text{def}}{=} (n_1, \dots, n_m)$ is defined as

$$\mathrm{RM}_{\boldsymbol{\theta}}(r, \mathbf{n}) \stackrel{\text{def}}{=} \{P \in \mathbb{L}[\mathrm{G}] \colon \deg_{\boldsymbol{\theta}}(P) \leqslant r\}.$$

By fixing a $\mathbb{K}$-basis $\beta = \{\beta_1, \dots, \beta_N\}$ of $\mathbb{L}$, the code $\mathrm{RM}_{\boldsymbol{\theta}}(r, \mathbf{n})$ can be seen in the vector form as

$$\{(P(\beta_1), \dots, P(\beta_N)) \colon P \in \mathbb{L}[\mathrm{G}],\ \deg_{\boldsymbol{\theta}}(P) \leqslant r\} \subseteq \mathbb{L}^N,$$

where $N = |\mathrm{G}|$ and equivalently, every codeword can be seen as $N \times N$ matrices with entries in $\mathbb{K}$. When $m = 1$, i.e. G cyclic, we recover Gabidulin codes over $\mathbb{L}/\mathbb{K}$ as particular classes of $\boldsymbol{\theta}$-Reed–Muller codes. It is worth noting that contrary to Gabidulin codes $\boldsymbol{\theta}$–Reed–Muller codes cannot be defined over finite fields as soon as the underlying Galois group is not cyclic.

Towards various applications, for instance post–quantum cryptography, it is particularly important for a family of codes to have an efficient decoding algorithm. However, the known classes of rank metric codes with effective decoding algorithms are the only following few; simple codes [4], some families of MRD codes including Gabidulin codes [5] and its variants, cf. [6, Chapter 2], and low-rank parity-check (LRPC) codes [7] and the interleaved version of the aforementioned codes [7], [8]. In [9], the authors of the present article give a deterministic decoding algorithm for $\boldsymbol{\theta}$-Reed-Muller codes that involved so–called *G-Dickson matrices* and which corrects any error of rank up to half the minimum rank distance. In the present paper, we investigate a recursive structure of these codes in the "binary–like" case, i.e., when $\mathrm{G} \cong (\mathbb{Z}/2\mathbb{Z})^m$ and propose a new decoding technique resting on this recursive structure.

It is worth noting that the structure we identified can be considered as a rank–metric analogue to the recursive structure binary Reed-Muller codes posses in the Hamming metric. More precisely, in the Hamming setting, any codeword of $\mathrm{RM}_2(r, m)$ can be written as $(u \mid u + v)$ where $u \in \mathrm{RM}_2(r, m-1)$ and $v \in \mathrm{RM}_2(r-1, m-1)$. The general $(u \mid u + v)$ construction was introduced by Plotkin [10] and known as *Plotkin construction* for linear codes with Hamming metric. This recursive construction and its use for decoding have been studied extensively. Besides Hamming metric binary Reed–Muller codes and their decoding, Plotkin construction has striking applications since it naturally appears in the construction of polar codes or in the post–quantum signature *Wave* [11], [12]. One can also mention that this construction iteratively applied on Reed–Solomon codes permits to achieve the capacity of the discrete symmetric channel as proved in [13].

Our contributions in this article are two-fold:

- We demonstrate a recursive structure of binary–like rank metric Reed-Muller codes and give a decoding algorithm that can correct up to half minimum distance. This algorithm may fail on some unlikely instances but has a better complexity than the Dickson-based decoding of [9] in a broad range of parameters.

- Inspired by the structure of binary–like rank metric Reed–Muller codes, we adapt the recursive structure to propose Plotkin-like construction for matrix rank metric codes over any field. As a consequence, we provide new efficiently decodable matrix rank metric codes over finite fields which are not equivalent to Gabidulin codes.

Notation. We use $[a, b]$ to denote the interval of integers $\{a, a+1, \ldots, b\}$.

II. Binary Reed-Muller codes

A. The Hamming case

With a fixed ordering $p_1, \ldots, p_{2^m}$ of the elements of $\mathbb{F}_2^m$, the binary Reed-Muller code of order m and type r, denoted $\mathrm{RM}_2(r, m)$, is defined as

$$\{(f(p_1), \ldots, f(p_{2^m})) : f \in \mathbb{F}_2[x_1, \ldots, x_m], \deg f \leqslant r\}.$$

As a consequence of the observation that any degree r polynomial $f \in \mathbb{F}_2[x_1, \ldots, x_m]$ can be decomposed as

$$f(x_1, \ldots, x_m) = g(x_1, \ldots, x_{m-1}) + x_m h(x_1, \ldots, x_{m-1}),$$

where $\deg g \leqslant r$ and $\deg h \leqslant r-1$, the binary Reed-Muller codes posses the following crucial recursive structure, first studied by Plotkin:

$$\mathrm{RM}_2(r, m) = \left\{ (\mathbf{u} \mid \mathbf{u}+\mathbf{v}) \ : \ \begin{array}{l} \mathbf{u} \in \mathrm{RM}_2(r, m-1), \\ \mathbf{v} \in \mathrm{RM}_2(r-1, m-1) \end{array} \right\}.$$

The recursive structure implies in particular that the minimum distance of $\mathrm{RM}_2(r, m)$ is 2^{m-r}. Moreover, it leads to an efficient decoding algorithm correcting up to half their minimum distance in quasi-linear time in the block length.

Let us briefly sketch how the Plotkin structure permits to decode. Let $\mathbf{y} = (\mathbf{u} + \mathbf{e}_l \mid \mathbf{u} + \mathbf{v} + \mathbf{e}_r) \in \mathbb{F}_2^{2^m}$ be the received vector such that $(\mathbf{u} \mid \mathbf{u}+\mathbf{v}) \in \mathrm{RM}_2(r, m)$ and $(\mathbf{e}_l \mid \mathbf{e}_r) \in \mathbb{F}_2^{2^m}$ has Hamming weight less or equal to $2^{m-r-1} - 1$. By *folding* the received word *i.e.* by summing up its two halves, we get

$$(\mathbf{u} + \mathbf{e}_l) + (\mathbf{u} + \mathbf{v} + \mathbf{e}_r) = (\mathbf{v} + \mathbf{e}_l + \mathbf{e}_r)$$

with $\mathrm{w_H}(\mathbf{e}_l + \mathbf{e}_r) \leqslant \mathrm{w_H}(\mathbf{e}_l \mid \mathbf{e}_r) \leqslant 2^{m-r-1} - 1$. Since $\mathbf{v} \in \mathrm{RM}_2(r-1, m-1)$, a recursive call of the algorithm permits to recover $\mathbf{v}$ by decoding $\mathbf{v} + \mathbf{e}_l + \mathbf{e}_r$. Therefore, we now have to recover $\mathbf{u}$ from $(\mathbf{u} + \mathbf{e}_l \mid \mathbf{u} + \mathbf{e}_r)$, where either $\mathrm{w_H}(\mathbf{e}_l) \leqslant \frac{2^{m-r-1}-1}{2}$ or $\mathrm{w_H}(\mathbf{e}_r) \leqslant \frac{2^{m-r-1}-1}{2}$. Thus one of the two recursive calls respectively applied to $\mathbf{u} + \mathbf{e}_l$ and $\mathbf{u} + \mathbf{e}_r$ will succeed and we recover $\mathbf{u}$.

B. Binary-like rank Reed–Muller codes.

For a positive integer m and $\mathrm{G} \cong (\mathbb{Z}/2\mathbb{Z})^m$, the $\boldsymbol{\theta}$-polynomials resemble those in the case of binary Reed-Muller with Hamming metric and thus we call these codes *binary rank metric Reed-Muller codes*.

Definition II.1. Let r, m be positive integers such that $m > 1$ and $r \leqslant m$. A *rank–metric binary Reed-Muller code* of length $N = 2^m$ over the extension $\mathbb{L}/\mathbb{K}$ of order r and type m is the following $\mathbb{L}$-subspace of the skew group algebra $\mathbb{L}[\mathrm{G}]$:

$$\mathrm{RM}_{\mathbb{L}/\mathbb{K}}(r, m) \stackrel{\text{def}}{=} \left\{ f \in \mathbb{L}[\mathrm{G}] \ : \ f = \sum_{\mathfrak{g} \in \mathrm{G}, \ \mathrm{w_H}(\mathfrak{g}) \leqslant r} f_{\mathfrak{g}} \mathfrak{g} \right\},$$

where $\mathrm{w_H}(\mathfrak{g})$ is the Hamming weight of the $\mathfrak{g}$ seen as a vector in $(\mathbb{Z}/2\mathbb{Z})^m$.

From [3, Prop. 47 & 49], the dimension of $\mathrm{RM}_{\mathbb{L}/\mathbb{K}}(r, m)$ is $\sum_{i=0}^{r} \binom{m}{i}$ (as an $\mathbb{L}$-subspace of $\mathbb{L}[\mathrm{G}]$) and its rank minimum distance 2^{m-r}.

Remark II.2. To draw the analogy with the Hamming metric case, we denote $\mathrm{RM}_{\mathbb{L}/\mathbb{K}}(r, m)$ with m instead of $\mathbf{n} = (2, \ldots, 2)$ and we choose $\mathbb{L}/\mathbb{K}$ as a subscript instead of $\boldsymbol{\theta}$, to keep track of various extension fields that appear in decoding.

III. Decoding binary rank metric Reed-Muller codes

In this section, we show a recursive structure of binary rank metric Reed-Muller codes analogous to the classical case of Hamming metric Reed-Muller codes. Then we describe a recursive decoding procedure resting on this structure. First we make the following observation regarding the Galois extension $\mathbb{L}/\mathbb{K}$ for $\mathrm{G} \cong (\mathbb{Z}/2\mathbb{Z})^m$.

Lemma III.1. *Let $\mathbb{K}$ be a field of characteristic $\neq 2$ and $\mathbb{L}/\mathbb{K}$ be a Galois extension with $G = Gal(\mathbb{L}/\mathbb{K}) \cong (\mathbb{Z}/2\mathbb{Z})^m$ and $m \geqslant 1$. Then, there exist $\alpha_1, \ldots, \alpha_m \in \mathbb{L}$ such that $\mathbb{L} = \mathbb{K}(\alpha_1, \ldots, \alpha_m)$ where $\mathbb{K}(\alpha_1), \ldots, \mathbb{K}(\alpha_m)$ are quadratic extensions over $\mathbb{K}$ and the minimal polynomials of the α_i's have the shape $X^2 - a_i$ for some $a_i \in \mathbb{K}$.*

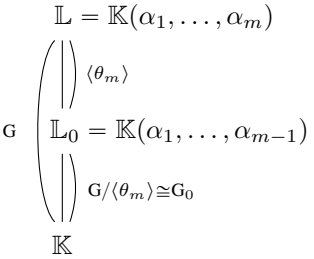
Remark III.2. Due to space reason, in this paper we only consider the case of $\mathrm{char}(\mathbb{K}) \neq 2$. The case of $\mathrm{char}(\mathbb{K}) \neq 2$ involving *Artin–Schreier* extensions instead of Kummer ones case is similar and will be discussed in a future longer version.

A. The recursive structure of rank Reed–Muller codes

Hence, in what follows $\mathbb{K}$ always has characteristic different from 2. We consider an extension $\mathbb{L} = \mathbb{K}(\alpha_1, \ldots, \alpha_m)$ where for any $i \in [1, m]$ $\alpha_i^2 = a_i$ for some $a_i \in \mathbb{K}$. Then $\mathrm{G} = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ has generators $\theta_1, \ldots, \theta_m$ with

$$\forall i, j \in [1, m], \quad \theta_i(\alpha_j) = (-1)^{\delta_{ij}} \alpha_j$$

where δ_{ij} denotes the Kronecker Delta. We introduce the intermediary extension $\mathbb{L}_0 \stackrel{\text{def}}{=} \mathbb{K}(\alpha_1, \ldots, \alpha_{m-1})$ and its associated Galois group $\mathrm{Gal}(\mathbb{L}_0/\mathbb{K}) = \mathrm{G}_0 \stackrel{\text{def}}{=} \langle \theta_1, \ldots, \theta_{m-1} \rangle$. This is summarized in the diagram below.



Proposition III.3 (Recursive structure in the Kummer case)**.** *Let* $\mathrm{char}\ \mathbb{K} \neq 2$*, Gal*$(\mathbb{L}/\mathbb{K}) \cong (\mathbb{Z}/2\mathbb{Z})^m$ *and* $r < m$ *be nonnegative integers. Then the Reed-Muller code RM*$_{\mathbb{L}/\mathbb{K}}(r,m)$ *has the following recursive structure*

$$\left\{ \begin{pmatrix} \mathbf{A}_0+\mathbf{B}_0 & a_m(\mathbf{A}_1-\mathbf{B}_1) \\ \mathbf{A}_1+\mathbf{B}_1 & \mathbf{A}_0-\mathbf{B}_0 \end{pmatrix} \ : \ \begin{matrix} \mathbf{A}_i \in RM_{\mathbb{L}_0/\mathbb{K}}(r,m-1), \\ \mathbf{B}_i \in RM_{\mathbb{L}_0/\mathbb{K}}(r-1,m-1) \end{matrix} \right\},$$

where $a_m \stackrel{def}{=} \alpha_m^2 \in \mathbb{K}$.

Proof: Since G splits into the disjoint union of the two cosets G_0 and $\mathrm{G}_0\theta_m$, we can split $F = \sum_{\mathfrak{g}\in\mathrm{G}} f_{\mathfrak{g}}\mathfrak{g} \in \mathbb{L}[\mathrm{G}]$ as

$$\begin{aligned} F &= \sum_{\mathfrak{g}\in\mathrm{G}_0} f_{\mathfrak{g}}\mathfrak{g} + \sum_{\mathfrak{h}\in\mathrm{G}_0\theta_m} f_{\mathfrak{h}}\mathfrak{h} \\ &= \sum_{\mathfrak{g}\in\mathrm{G}_0} f_{\mathfrak{g}}\mathfrak{g} + \left(\sum_{\mathfrak{g}\in\mathrm{G}_0} f_{\mathfrak{g}\theta_m}\mathfrak{g}\right)\theta_m. \end{aligned}$$

Since $\mathbb{L} = \mathbb{L}_0 \oplus \mathbb{L}_0\alpha_m$, for any $a \in \mathbb{L}$, let $a = a^0 + a^1\alpha_m$ with $a^0, a^1 \in \mathbb{L}_0$. Then F can be split as

$$\begin{aligned} F = \sum_{\mathfrak{g}\in\mathrm{G}_0} f^0_{\mathfrak{g}}\mathfrak{g} + \alpha_m \sum_{\mathfrak{g}\in\mathrm{G}_0} f^1_{\mathfrak{g}}\mathfrak{g} + \left(\sum_{\mathfrak{g}\in\mathrm{G}_0} f^0_{\mathfrak{g}\theta_m}\mathfrak{g}\right)\theta_m \\ + \alpha_m\left(\sum_{\mathfrak{g}\in\mathrm{G}_0} f^1_{\mathfrak{g}\theta_m}\mathfrak{g}\right)\theta_m. \end{aligned} \tag{1}$$

Set

$$\begin{aligned} A_0 &= \sum_{\mathfrak{g}\in\mathrm{G}_0} f^0_{\mathfrak{g}}\mathfrak{g} \quad A_1 = \sum_{\mathfrak{g}\in\mathrm{G}_0} f^1_{\mathfrak{g}}\mathfrak{g} \\ B_0 &= \sum_{\mathfrak{g}\in\mathrm{G}_0} f^0_{\mathfrak{g}\theta_m}\mathfrak{g} \quad B_1 = \sum_{\mathfrak{g}\in\mathrm{G}_0} f^1_{\mathfrak{g}\theta_m}\mathfrak{g}, \end{aligned}$$

then the degree constraint on $F \in \mathrm{RM}_{\mathbb{L}/\mathbb{K}}(r,m)$ entails

$$\begin{aligned} &A_0, B_0 \in \mathrm{RM}_{\mathbb{L}_0/\mathbb{K}}(r, m-1), \\ &A_1, B_1 \in \mathrm{RM}_{\mathbb{L}_0/\mathbb{K}}(r-1, m-1). \end{aligned}$$

Equation (1) can then be rewritten as

$$F = A_0 + \alpha_m A_1 + (B_0 + \alpha_m B_1)\theta_m. \tag{2}$$

Finally, we consider a $\mathbb{K}$-basis $\mathcal{B}_0 = (\beta_1, \ldots, \beta_{2^{m-1}})$ of $\mathbb{L}_0$, which yields a $\mathbb{K}$-basis $\mathcal{B} = \mathcal{B}_0 \cup \alpha_m\mathcal{B}_0$ of $\mathbb{L}$. By denoting $\mathbf{A}_0, \mathbf{A}_1, \mathbf{B}_0, \mathbf{B}_1$ the respective representations of A_0, A_1, B_0, B_1 in $\mathcal{B}_0$, we get the desired matrix form of F in $\mathcal{B}$. Indeed, as $\theta_{m|\mathbb{L}_0} = \mathrm{id}_{\mathbb{L}_0}$ and thus

$$F_{|\mathbb{L}_0} = (A_0 + B_0) + \alpha_m(A_1 + B_1),$$

the left-hand half of the matrix in the statement corresponds to $F_{|\mathbb{L}_0}$. Similarly, the right-hand half corresponds to the restriction of F to $\mathbb{L}_0\alpha_m$. To see this, let $u\alpha_m \in \mathbb{L}_0\alpha_m$ with $u \in \mathbb{L}_0$ which yields

$$F(u\alpha_m) = a_m(A_1(u) - B_1(u)) + \alpha_m(A_0(u) - B_0(u))$$

and thus the shape. ∎

B. Decoding

Now we give a recursive decoding algorithm for binary Reed-Muller codes with rank metric using the recursive structure identified in Proposition III.3.

Suppose we are given

$$\mathbf{Y} = \underbrace{\begin{pmatrix} \mathbf{A}_0+\mathbf{B}_0 & a_m(\mathbf{A}_1-\mathbf{B}_1) \\ \mathbf{A}_1+\mathbf{B}_1 & \mathbf{A}_0-\mathbf{B}_0 \end{pmatrix}}_{\mathbf{C}\in\mathrm{RM}_{\mathbb{L}/\mathbb{K}}(r,m)} + \underbrace{\begin{pmatrix} \mathbf{E}_{00} & \mathbf{E}_{01} \\ \mathbf{E}_{10} & \mathbf{E}_{11} \end{pmatrix}}_{\mathbf{E}\in\mathbb{K}^{2^m\times 2^m}},$$

where $\mathrm{Rk}\,(\mathbf{E}) \leqslant 2^{m-r-1} - 1$. Since the code $\mathrm{RM}_{\mathbb{L}/\mathbb{K}}(r,m)$ has minimum distance 2^{m-r}, the error rank is less than half the minimum distance.

a) ***Recursivity****:* To describe the recursive algorithm, we assume that we can decode up to half the minimum distance of any rank Reed–Muller code $\mathrm{RM}_{\mathbb{L}/\mathbb{K}'}(r',m')$ over field $\mathbb{K}'$ such that $\mathbb{K} \subset \mathbb{K}' \subset \mathbb{L}$ with any parameters $r' \leqslant r$ and $m' < m$. To initialize our recursion, for $r = 0$ the decoding of $\mathrm{RM}_{\mathbb{L}/\mathbb{K}'}(0,m')$ can be performed using the algorithm presented in [9] by reconstructing error the polynomial E using a minor cancellation of the associated Dickson matrix.

b) ***Overview of the algorithm****:* First we briefly describe the main steps of our decoding algorithm.

- *Step 1. Folding* $\mathbf{Y}$. We apply an operation that does not increase the error rank and permits to get rid of the $\mathbf{A}_i$'s and reduce to two instances of correcting $2^{m-r-1}-1$ errors for $\mathrm{RM}_{\mathbb{L}/\mathbb{K}(\alpha_m)}(r-1,m-1)$, each instance involving one of the $\mathbf{B}_i$'s.
- *Step 2. Recursive calls.* Two recursive calls to the algorithm permit to recover $\mathbf{B}_0, \mathbf{B}_1$ and get partial information on $\mathbf{E}$.
- *Step 3. Recovery of the* $\mathbf{A}_i$*'s.* Under some assumption on $\mathbf{E}$, the partial information we got on the error permits to recover the $\mathbf{A}_i$'s by solving linear systems.

c) ***Step 1. Folding****:* Denoting by $\mathbf{I} \in \mathbb{K}^{2^{m-1}\times 2^{m-1}}$ the identity matrix, the following operations will be the analogue of the folding in the Hamming case

$$\begin{aligned} \left(\tfrac{1}{\alpha_m}\mathbf{I} \quad \mathbf{I}\right)\mathbf{Y}\begin{pmatrix} \mathbf{I} \\ -\frac{1}{\alpha_m}\mathbf{I} \end{pmatrix} &= \frac{2}{\alpha_m}\mathbf{B}_0 + 2\mathbf{B}_1 \\ &+ \frac{1}{\alpha_m}\mathbf{E}_{00} - \frac{1}{\alpha_m}\mathbf{E}_{01} + \mathbf{E}_{10} - \frac{1}{\alpha_m}\mathbf{E}_{11}, \end{aligned} \tag{3}$$

$$\begin{aligned} \left(-\tfrac{1}{\alpha_m}\mathbf{I} \quad \mathbf{I}\right)\mathbf{Y}\begin{pmatrix} \mathbf{I} \\ \frac{1}{\alpha_m}\mathbf{I} \end{pmatrix} &= 2\mathbf{B}_1 - \frac{2}{\alpha_m}\mathbf{B}_0 \\ &- \frac{1}{\alpha_m}\mathbf{E}_{00} - \frac{1}{\alpha_m}\mathbf{E}_{01} + \mathbf{E}_{10} + \frac{1}{\alpha_m}\mathbf{E}_{11}. \end{aligned} \tag{4}$$

Remark III.4. It is worth noting that if the matrices $\mathbf{A}_i, \mathbf{B}_i$ and $\mathbf{E}_{ij}$ have their entries in $\mathbb{K}$, then the matrices obtained in reductions (3) and (4) have their entries in $\mathbb{K}(\alpha_m)$. Also, the operations on $\mathbf{E}$ by left-and-right multiplication do not increase the rank.

d) ***Step 2. Recursive calls to recover*** $\mathbf{B}_0, \mathbf{B}_1$*:* Reductions (3) and (4) yield the sum of an element of $\mathrm{RM}_{\mathbb{L}/\mathbb{K}(\alpha_m)}(r-1,m-1)$ and an error term of rank $\leqslant \mathrm{Rk}\,(\mathbf{E}) \leqslant 2^{m-r-1}-1$, which is less than half the minimum distance of $\mathrm{RM}_{\mathbb{L}/\mathbb{K}(\alpha_m)}(r-1,m-1)$. Based on our assumption that Reed–Muller codes of parameters $r' \leqslant r$ and $m' < m$ can be decoded up to half their minimum distance, two successive

recursive calls of the algorithm respectively applied on the expressions (3) and (4) permit to recover

$$\frac{2}{\alpha_m}\mathbf{B}_0 + 2\mathbf{B}_1 \qquad \text{and} \qquad -\frac{2}{\alpha_m}\mathbf{B}_0 + 2\mathbf{B}_1$$

and a simple calculation yields $\mathbf{B}_0, \mathbf{B}_1$.

*e) **Step 3. Recovery of** $\mathbf{A}_0, \mathbf{A}_1$:* Removing $\mathbf{B}_0, \mathbf{B}_1$ from $\mathbf{Y}$, we consider the new decoding problem:

$$\widetilde{\mathbf{Y}} = \underbrace{\begin{pmatrix} \mathbf{A}_0 & a_m\mathbf{A}_1 \\ \mathbf{A}_1 & \mathbf{A}_0 \end{pmatrix}}_{\widetilde{\mathbf{C}} \in \mathrm{RM}_{\mathbb{L}/\mathbb{K}}(r,m)} + \underbrace{\begin{pmatrix} \mathbf{E}_{00} & \mathbf{E}_{01} \\ \mathbf{E}_{10} & \mathbf{E}_{11} \end{pmatrix}}_{\mathbf{E} \in \mathbb{K}^{2^m \times 2^m}}. \tag{5}$$

To recover $\mathbf{A}_0$, $\mathbf{A}_1$, the technique used in the Hamming case does not adapt. However, the previous step permitted us also to recover from (3) and (4) the following matrices:

$$\mathbf{E}' \stackrel{\text{def}}{=} \frac{1}{\alpha_m}\mathbf{E}_{00} - \frac{1}{a_m}\mathbf{E}_{01} + \mathbf{E}_{10} - \frac{1}{\alpha_m}\mathbf{E}_{11}, \tag{6}$$

$$\mathbf{E}'' \stackrel{\text{def}}{=} -\frac{1}{\alpha_m}\mathbf{E}_{00} - \frac{1}{a_m}\mathbf{E}_{01} + \mathbf{E}_{10} + \frac{1}{\alpha_m}\mathbf{E}_{11}. \tag{7}$$

Here we make the following assumption.

Assumption 1. The matrices $\mathbf{E}', \mathbf{E}'' \in \mathbb{K}(\alpha_m)^{\frac{N}{2}\times\frac{N}{2}}$ have rank t and so do their foldings and so on until depth r, *i.e.* we assume any iterated folding of $\mathbf{E}$ of size $2^{m-i} \times 2^{m-i}$ with $i \leqslant r$ to have rank $t \leqslant 2^{m-r-1} - 1$.

Remark III.5. This assumption is actually what happens "most of the time". We observed using *SageMath* [14] that this is the typical behaviour of random matrices with prescribed rank $t < \frac{N}{2}$ and entries in finite fields. Moreover, when applied to finite fields we analyse in Section IV-A the probability that the folding of such a matrix $\mathbf{E}$ keeps the same rank and we prove that this probability is exponentially close to 1.

Now, consider

$$\widetilde{\mathbf{Y}}\begin{pmatrix} \mathbf{I} \\ -\frac{1}{\alpha_m}\mathbf{I} \end{pmatrix} = \begin{pmatrix} \mathbf{A}_0 + \alpha_m\mathbf{A}_1 \\ \mathbf{A}_1 - \alpha_m^{-1}\mathbf{A}_0 \end{pmatrix} + \underbrace{\begin{pmatrix} \mathbf{E}_{00} - \alpha_m^{-1}\mathbf{E}_{01} \\ \mathbf{E}_{10} - \alpha_m^{-1}\mathbf{E}_{11} \end{pmatrix}}_{\mathbf{F}}. \tag{8}$$

The top part

$$\widetilde{\mathbf{Y}}_0 \stackrel{\text{def}}{=} \mathbf{A}_0 + \alpha_m\mathbf{A}_1 + \mathbf{F}_0, \quad \mathbf{F}_0 \stackrel{\text{def}}{=} (\mathbf{E}_{00} - \alpha_m^{-1}\mathbf{E}_{01})$$

gives an instance of the decoding problem for the code $\mathrm{RM}_{\mathbb{L}/\mathbb{K}(\alpha_m)}(r, m-1)$. Moreover, since

$$\mathbf{F} = \mathbf{E}\begin{pmatrix} \mathbf{I} \\ -\frac{1}{\alpha_m}\mathbf{I} \end{pmatrix} \quad \text{and} \quad \mathbf{E}' = \begin{pmatrix} \frac{1}{\alpha_m}\mathbf{I} & \mathbf{I} \end{pmatrix}\mathbf{F}, \tag{9}$$

then $t = \mathrm{Rk}(\mathbf{E}) \geqslant \mathrm{Rk}(\mathbf{F}) \geqslant \mathrm{Rk}(\mathbf{E}')$ and, thanks to Assumption 1, all these matrices have rank t. Next, the right–hand equation of (9) entails that the row space of $\mathbf{E}'$ is contained in that of $\mathbf{F}$ and, these row spaces are actually equal because they both have dimension t. Thus, the row space of $\mathbf{F}_0 = \mathbf{E}_{00} - \alpha_m^{-1}\mathbf{E}_{01}$ is contained in that of $\mathbf{E}'$.

Since $\mathbf{E}'$ is known, we know its row space $V \subseteq \mathbb{K}(\alpha)^{\frac{N}{2}}$ and the previous discussion asserts that V contains the row space of $\mathbf{F}_0$. Similarly to the Hamming case, with this partial knowledge of the row space (that can be regarded as a rank-metric counterpart of the support in the Hamming metric) of $\mathbf{F}_0$, the decoding boils down to the resolution of a linear system (see, for instance [15, § IV.1] or [16, § III.1] for further details) and permits to recover $\mathbf{A}_0 + \alpha_m\mathbf{A}_1$. Finally since both $\mathbf{A}_0, \mathbf{A}_1$ have their entries in $\mathbb{K}$, they can be immediately deduced from $\mathbf{A}_0 + \alpha_m\mathbf{A}_1$. Note that V has dimension at most $t = 2^{m-r-1} - 1$ which is less than the minimum distance of $\mathrm{RM}_{\mathbb{L}/\mathbb{K}(\alpha_m)}(r, m-1)$ which guarantees the uniqueness of the solution of the decoding.

Remark III.6. The aforementioned procedure can be regarded as a rank-metric analogue of the erasure decoding: we solve a decoding problem where the row space of the error (which can be considered as its support) is known.

C. Complexity analysis

To evaluate the complexity of the previous algorithm, we introduce the notation $\mathcal{M}_{\mathbb{K}}(\mathbb{K}_1)$ the number of operations in $\mathbb{K}$ that costs a multiplication of two elements of an extension $\mathbb{K}_1$ of $\mathbb{K}$. For space reasons, we admit the following statement.

Theorem III.7. *Denote* $N \stackrel{\text{def}}{=} 2^m$. *Let* $1 < \alpha \leqslant 2$ *such that for any field* $\mathbb{K}'$ *with* $\mathbb{K} \subset \mathbb{K}' \subset \mathbb{L}$

$$\forall \varepsilon > 0, \qquad \mathcal{M}_{\mathbb{K}}(\mathbb{K}') = \mathcal{O}([\mathbb{K}' : \mathbb{K}]^{\alpha+\varepsilon}).$$

Under Assumption 1, the decoding of $RM_{\mathbb{L}/\mathbb{K}}(r, m)$ *can be performed with a deterministic algorithm in*

$$\begin{cases} \mathcal{O}(N^\omega + t^{\omega-1}N\log N\mathcal{M}_{\mathbb{K}}(\mathbb{L})) & \text{if } \alpha < \omega - 1 \\ \mathcal{O}(N^{\alpha+1} + t^{\omega-1}N\log N\mathcal{M}_{\mathbb{K}}(\mathbb{L})) & \text{otherwise} \end{cases}$$

operations in $\mathbb{K}$ *and with a Las-Vegas algorithm in*

$$\mathcal{O}(t^{\omega-1}N\log N\mathcal{M}_{\mathbb{K}}(\mathbb{L})) \quad \text{operations in } \mathbb{K}.$$

Remark III.8. It is worth noting that the recursive algorithm we presented in this paper fares well compared to the Dickson matrix-based decoding algorithm in [9, Theorem 5.15]. Indeed, the algorithm in [9] has a complexity in $\mathcal{O}(kt^\omega)$ operations in $\mathbb{L}$ i.e. $\mathcal{O}(kt^\omega\mathcal{M}_{\mathbb{K}}(\mathbb{L}))$ operations in $\mathbb{K}$, which yields $\mathcal{O}(N^{\frac{\omega+2}{2}}\mathcal{M}_{\mathbb{K}}(\mathbb{L}))$ operations when $k = \Theta(N)$ and $t = \Theta(\frac{N}{2})$. On the other hand, from Theorem III.7, if $\alpha < \omega - 1$, we get a complexity in $\mathcal{O}(N^{\frac{w+1}{2}}\log N\mathcal{M}_{\mathbb{K}}(\mathbb{L}))$ operations, which is negligible compared to $\mathcal{O}(N^{\frac{\omega+2}{2}}\mathcal{M}_{\mathbb{K}}(\mathbb{L}))$ operations.

IV. Plotkin construction for matrix codes

Inspired by the previous sections where an analogue of Plotkin $(u \mid u+v)$ structure was identified for rank metric binary Reed–Muller codes, we will abstract this structure to provide a rank analogue of Plotkin construction. A particular interest of this approach is that contrary to rank metric Reed–Muller codes that can be defined only over infinite fields, we can here propose a structure that can be applied to any rank metric codes, in particular over finite fields, which is the context we consider from now on: in the sequel the ground field will be a finite field $\mathbb{F}_q$ with q odd.

Definition IV.1. Let $a \in \mathbb{F}_q$ (possibly $a = 1$). Let $\mathscr{C}$ be an $[m \times m, k_1, d_1]_q$ code and $\mathscr{D}$ be an $[m \times m, k_2, d_2]_q$ code. We

define the Plotkin construction of $\mathscr{C}$ and $\mathscr{D}$ to be the $\mathbb{F}_q$-linear matrix rank metric code:

$$\mathscr{C}\diamondsuit_a\mathscr{D} \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} \mathbf{A}_0+\mathbf{B}_0 & a(\mathbf{A}_1-\mathbf{B}_1) \\ \mathbf{A}_1+\mathbf{B}_1 & \mathbf{A}_0-\mathbf{B}_0 \end{pmatrix} \;:\; \begin{matrix} \mathbf{A}_i\in\mathscr{C}, \\ \mathbf{B}_i\in\mathscr{D} \end{matrix} \right\}.$$

Proposition IV.2. *In the context of Definition IV.1,*

$$\dim_{\mathbb{F}_q}\mathscr{C}\diamondsuit_a\mathscr{D} = 2(\dim_{\mathbb{F}_q}\mathscr{C}+\dim_{\mathbb{F}_q}\mathscr{D}).$$

Proof: It suffices to observe that the maps

$$(\mathbf{A}_0,\mathbf{B}_0)\mapsto(\mathbf{A}_0+\mathbf{B}_0,\mathbf{A}_0-\mathbf{B}_0) \qquad \text{and}$$
$$(\mathbf{A}_1,\mathbf{B}_1)\mapsto(\mathbf{A}_1+\mathbf{B}_1,a(\mathbf{A}_1-\mathbf{B}_1))$$

are injective. ∎

Theorem IV.3. *Let $\mathscr{C}$ be an $[m\times m,k_1]_q$ code and $\mathscr{D}$ an $[m\times m,k_2]_q$ code where q is an odd prime. Suppose that for $\mathscr{D}$, we can correct $t\leqslant\frac{m}{2}$ errors for some positive integer t and that for $\mathscr{C}$ we can correct t erasures (*i.e. *errors of rank t whose row or column space is known). Then, we have an algorithm taking as input*

$$\mathbf{Y}=\mathbf{C}+\mathbf{E}$$

where $\mathbf{C}\in\mathscr{C}\diamondsuit_a\mathscr{D}$ and $\mathbf{E}$ is uniformly random among the $2m\times 2m$ matrices with rank t, which returns the pair $(\mathbf{C},\mathbf{E})$ with probability $1-\mathcal{O}(q^{t-m-1})$. Its complexity is in $\mathcal{O}(m^2+C(m)+D(m))$ operations in $\mathbb{F}_q$, where $C(m)$ and $D(m)$ denote respectively the complexity of correcting t erasures for $\mathscr{C}$ and t errors for $\mathscr{D}$.

The decoding works similar to the method explained for decoding binary rank Reed-Muller codes with the only difference that recursive calls are replaced by calls to the decoding of $\mathscr{D}$ first and then calls to the erasure decoding of $\mathscr{C}$. The complexity comes from the fact that folding costs $\mathcal{O}(m^2)$ and then the rest of the algorithm consists in calls to the decoders of $\mathscr{C}$ and $\mathscr{D}$. The probability analysis is discussed in the subsequent section.

Remark IV.4. Of course, exactly as in the case of rank binary Reed–Muller codes or in the spirit of [13], [17] in Hamming metric, this Plotkin–like construction can be iterated and decoded with a recursive decoder ultimately calling other decoders.

A. Probability analysis

According to Assumption 1, for the algorithm to succeed, we need that the following *folding* of $\mathbf{E}$ has the same rank as $\mathbf{E}$. The folding has, up to scalar multiplication the following form:

$$\text{Fold}(\mathbf{E}) \stackrel{\text{def}}{=} \begin{pmatrix}\mathbf{I}_m & b\mathbf{I}_m\end{pmatrix}\mathbf{E}\begin{pmatrix}b'\mathbf{I}_m \\ \mathbf{I}_m\end{pmatrix}$$

for some nonzero b,b' which are either elements of $\mathbb{F}_q$ or elements $\mathbb{F}_{q^2}$ whose squares are in $\mathbb{F}_q$, depending on whether a is a square or a non square in $\mathbb{F}_q$. Both cases (a is a square or a non square) lead to probability estimates but due to space reasons, we will limit our analysis to the case where a is a square which is what we assume in the sequel.

To estimate the probability that $\text{Fold}(\mathbf{E})$ has rank t we proceed in two steps. First we evaluate the probability:

$$\mathbb{P}\left(\text{Rk}\left(\begin{pmatrix}\mathbf{I}_m & b\mathbf{I}_m\end{pmatrix}\mathbf{E}\right)=t\right)$$

and then we evaluate $\mathbb{P}\left(\text{Rk}\left(\text{Fold}(\mathbf{E})=t\right)\right)$.

Note first that the right kernel of $\begin{pmatrix}\mathbf{I}_m & b\mathbf{I}_m\end{pmatrix}$ has dimension m. Denote by K this kernel. Second, note that since $\mathbf{E}$ is a uniformly random $2m\times 2m$ matrix of rank t, its column space U is a uniformly random subspace of $\mathbb{F}_q^{2m}$ of dimension t. For the rank not to collapse during the first part of the folding we should have $U\cap K=\{0\}$. Here we use the following statement that we will assume for space reasons.

Lemma IV.5. *Let K be a subspace of $\mathbb{F}_q^{2m}$ of dimension m and U be a uniformly random subspace of $\mathbb{F}_q^{2m}$ of dimension $t<m$. Then*

$$\mathbb{P}\left(U\cap K\neq 0\right)=\mathcal{O}(q^{t-m-1}).$$

As a consequence of this lemma the probability that the first folding keeps rank t is in $1-\mathcal{O}(q^{t-m-1})$. For the second folding, assuming that it has rank t, then the obtained matrix has a row space V of dimension t which is nothing but the row space of $\mathbf{E}$. Hence it is a uniformly random space of dimension t in $\mathbb{F}_q^{2m}$.

Denote by K' the left kernel of $\begin{pmatrix}\mathbf{I}_m \\ b'\mathbf{I}_m\end{pmatrix}$, then, according to Lemma IV.5,

$$\mathbb{P}\left(V\cap K'\neq 0\right)=\mathcal{O}(q^{t-m-1}).$$

In summary, the probability that both folding have rank t is $1-\mathcal{O}(q^{t-m-1})$.

B. An example

Let $\mathscr{C},\mathscr{D}\subset\mathbb{F}_q^{m\times m}$ be two matrix representation of Gabidulin codes over $\mathbb{F}_{q^m}$ of respective $\mathbb{F}_{q^m}$–dimensions k_1,k_2. Recall that these codes have respective minimum distances $m-k_1+1$ and $m-k_2+1$. Moreover, Loidreau's algorithm [5] permits to decode $\mathscr{D}$ up to $\frac{m-k_2}{2}$ and that it is possible to correct up to $m-k_1$ rank erasure for $\mathscr{C}$. Suppose that $m=2k_1-k_2$ so that

$$t\stackrel{\text{def}}{=}(m-k_1)=\frac{m-k_2}{2}. \tag{10}$$

Then, according to Proposition IV.2 and Theorem IV.3, the code $\mathscr{C}\diamondsuit_a\mathscr{D}$ has $\mathbb{F}_q$–dimension $2m(k_1+k_2)$ and benefits from a decoder correcting up to t errors.

Remark IV.6. To conclude, note that $\mathscr{C}\diamondsuit_a\mathscr{D}$ contains some

$$\begin{pmatrix}\mathbf{A}_0 & (0)\\ (0) & \mathbf{A}_0\end{pmatrix},$$

with $\mathbf{A}_0\in\mathscr{C}$ of weight $m-k_1+1$. Hence the minimum distance of $\mathscr{C}\diamondsuit_a\mathscr{D}$ is less than $2m-2k_1+2$. If $m-k_2>2$, then (10) entails that the latter minimum distance is strictly below the rank Singleton bound $2m-k_1-k_2+1$. Therefore, $\mathscr{C}\diamondsuit_a\mathscr{D}$ is never MRD and hence cannot be equivalent to a Gabidulin code. The obtained family of rank–metric codes is hence a new one equipped with an efficient decoder.

REFERENCES

[1] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *J. Combin. Theory Ser. A*, vol. 25, no. 3, pp. 226–241, 1978.

[2] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problemy Peredachi Informatsii*, vol. 21, no. 1, pp. 3–16, 1985.

[3] D. Augot, A. Couvreur, J. Lavauzelle, and A. Neri, "Rank-metric codes over arbitrary Galois extensions and rank analogues of Reed–Muller codes," *SIAM J. Appl. Algebra Geom.*, vol. 5, no. 2, pp. 165–199, 2021.

[4] P. Gaborit, A. Hauteville, D. H. Phan, and J.-P. Tillich, "Identity-based encryption from codes with rank metric," in *Advances in Cryptology – CRYPTO 2017*, J. Katz and H. Shacham, Eds. Cham: Springer International Publishing, 2017, pp. 194–224.

[5] P. Loidreau, "A Welch-Berlekamp like algorithm for decoding Gabidulin codes," in *Coding and cryptography*, ser. Lecture Notes in Comput. Sci. Berlin: Springer, 2006, vol. 3969, pp. 36–45.

[6] H. Bartz, L. Holzbaur, H. Liu, S. Puchinger, J. Renner, and A. Wachter-Zeh, "Rank-metric codes and their applications," *Found. Trends Commun. Inf. Theory*, vol. 19, no. 3, pp. 390–546, May 2022.

[7] J. Renner, T. Jerkovits, and H. Bartz, "Efficient decoding of interleaved low-rank parity-check codes," in *2019 XVI International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY)*, 2019, pp. 121–126.

[8] V. Sidorenko and M. Bossert, "Decoding interleaved gabidulin codes and multisequence linearized shift-register synthesis," in *2010 IEEE International Symposium on Information Theory*. IEEE, 2010, pp. 1148–1152.

[9] A. Couvreur and R. Pratihar, "Decoding rank metric Reed–Muller codes," *arXiv preprint arXiv:2501.04766*, 2025.

[10] F. J. MacWilliams and N. J. A. Sloane, "The theory of error-correcting codes," *Elsevier Science Publishers BV google schola*, vol. 2, pp. 39–47, 1977.

[11] G. Banegas, K. Carrier, A. Chailloux, A. Couvreur, T. Debris-Alazard, P. Gaborit, P. Karpman, J. Loyer, R. Niederhagen, N. Sendrier, B. Smith, and J.-P. Tillich, "Wave," Round 1 Additional Signatures to the NIST Post-Quantum Cryptography: Digital Signature Schemes Call, Jun. 2023. [Online]. Available: https://wave-sign.org

[12] T. Debris-Alazard, N. Sendrier, and J.-P. Tillich, "Wave: A new family of trapdoor one-way preimage sampleable functions based on codes," in *Advances in Cryptology - ASIACRYPT 2019, Part I*, ser. Lecture Notes in Comput. Sci., S. D. Galbraith and S. Moriai, Eds., vol. 11921. Kobe, Japan: Springer, Dec. 2019, pp. 21–51. [Online]. Available: https://doi.org/10.1007/978-3-030-34578-5_2

[13] I. Márquez-Corbella and J.-P. Tillich, "Attaining capacity with iterated $(u|u+v)$ codes based on AG codes and Koetter–Vardy soft decoding," in *2017 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2017, pp. 6–10.

[14] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 9.5)*, 2022, `https://www.sagemath.org`.

[15] P. Gaborit, O. Ruatta, and J. Schrek, "On the complexity of the rank syndrome decoding problem," *IEEE Trans. Inform. Theory*, vol. 62, no. 2, pp. 1006–1019, 2016.

[16] N. Aragon, P. Gaborit, A. Hauteville, and J.-P. Tillich, "A new algorithm for solving the rank syndrome decoding problem," in *2018 IEEE International Symposium on Information Theory, ISIT 2018, Vail, CO, USA, June 17-22, 2018*. IEEE, 2018, pp. 2421–2425.

[17] I. Márquez-Corbella and J.-P. Tillich, "Using Reed–Solomon codes in the $(u|u+v)$ construction and an application to cryptography," in *2016 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2016, pp. 930–934.