Decoding Algorithms for Tensor Codes

Lucien François, Eimear Byrne, Alain Couvreur

Decoding Algorithms for Tensor Codes

Lucien François and Eimear Byrne
Departement of Mathematics and Statistics
Univercity College Dublin
Email: {lucien.francois, ebyrne}@ucd.ie

Alain Couvreur
Inria, Laboratoire LIX, École Polytechnique
Institut Polytechnique de Paris,
Email: alain.couvreur@inria.fr

***Abstract*—Tensor codes are a generalisation of matrix codes. Such codes are defined as subspaces of order-r tensors for which the ambient space is endowed with the tensor-rank as a metric. A class of these codes was introduced by Roth who outlined a decoding algorithm for low tensor-rank errors for particular cases. They may be viewed as a generalisation of the well-known Delsarte-Gabidulin-Roth maximum rank distance codes. We study a generalised class of these codes. We investigate the properties of these codes and outline decoding techniques for different metrics that leverage their tensor structure. We first consider a fibre-wise decoding approach, as each fibre of a codeword corresponds to a Gabidulin codeword. We then give a generalisation of Loidreau's decoding method that corrects errors with properties constrained by the dimensions of the slice spaces and fibre spaces. The metrics we consider are upper bounded by the tensor-rank metric, and therefore these algorithms also decode tensor-rank weight errors.**

***Index Terms*—Tensor codes, evaluation codes, decoding algorithms**

Error-correcting codes are critical in ensuring data reliability in modern communication systems. Rank-metric codes such as the well-known Delsarte-Gabidulin-Roth codes, have attracted significant attention due to their applicability in network coding. Such codes have seen generalisations, such as the twisted Gabidulin codes [1], [2] and the tensor codes introduced by Roth in [3]. Roth's tensor codes are a family of subspaces of the vector space of tensors endowed with the tensor-rank as a metric constructed to have a known lower bound on the minimum tensor-rank distance. In addition, Roth described algorithms to decode tensor-rank errors of size at most two for particular subclasses of this family.

In this paper, we derive decoding algorithms for a generalisation of the tensor codes that were introduced in [3]. We base our first kind of algorithm on the direct sum of codes in which the code is included, and the second kind on the Welch-Berlekamp [4] [5, Sec 6.7] like algorithm introduced by Loidreau [6]. We show that the constructed algorithms correct errors of different tensor-ranks for this large family of tensor codes.

In the first section, we will introduce the properties of the polynomials that play a role in the construction of the code, and the properties of the code itself with respect to different metrics. In the second section, we present the different decoding algorithms. In the third section, we compare the different algorithms together with those introduced by Roth.

In this paper, we present the results for order three tensors, but they can be generalised to higher order tensors. We will present the notions for 3-tensors via their matrix representation over an extension field. We refer the reader to [7], [8], and [9] for further background reading.

Notation: Throughout, we let q be a fixed prime power and denote by $\mathbb{F}_q$ the finite field or order q. We let be n be a fixed positive integer and we define $[\![1,n]\!] := \{1,\dots,n\}$. Let $\{\alpha_1,\dots,\alpha_n\}$ be a basis of $\mathbb{F}_{q^n}/\mathbb{F}_q$ and set $\alpha = (\alpha_1,\dots,\alpha_n)$. For any $j \in \{1,2\}$, we write π_j to denote the surjective map $\pi_j : \mathbb{N}^2 \twoheadrightarrow \mathbb{N}, x \mapsto x_j$. We let X, Y, Z be indeterminates.

For any $j \in \mathbb{N}^2$ and $r \in \mathbb{N}$, we denote by $j + r$ the vector $j + r := (j_1 + r, j_2 + r)$. Likewise, if $J \subseteq \mathbb{N}^2$ and $R \subseteq \mathbb{N}$, we will define $J + R := \{j + r \mid j \in J,\ r \in R\}$.

For any $\mathbb{F}_q$-bilinear map $b : \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ we denote the left (*resp.* right) radical of b by $\mathfrak{Rad}_1(b)$ (resp. $\mathfrak{Rad}_2(b)$); see [10, Def 8.3].

Gabidulin codes: Consider the rank-metric code $\mathcal{G}_k(\alpha) := \{(V(\alpha_1),\dots,V(\alpha_n)) \mid V(Z) = \sum_{\ell=0}^{k-1} v_\ell Z^{q^\ell}, v_i \in \mathbb{F}_{q^n}\}$. This is the *Gabidulin code* of dimension k over $\mathbb{F}_{q^n}$ (evaluated at α). We denote by $\mathrm{rank}_{\mathbb{F}_q}(v)$ the $\mathbb{F}_q$-rank of a tuple v with coefficients in $\mathbb{F}_{q^n}$, that is, $\mathrm{rank}_{\mathbb{F}_q}(v) := \dim(\langle v_1,\dots,v_n\rangle_{\mathbb{F}_q})$.

Tensors and matrices: We denote by $\mathbb{F}_q^{n\times n}$ vector space of matrices of size $n \times n$ over the field with q elements. A **3-tensor** of size $n \times n \times n$ over a field $\mathbb{F}_q$ is any element of the n^3-dimensional $\mathbb{F}_q$-vector space $\mathbb{F}_q^n \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^n = (\mathbb{F}_q^n)^{\otimes 3}$. An element $T \in (\mathbb{F}_q^n)^{\otimes 3}$ is uniquely associated with its coordinate expression $(T[i])_{i\in[\![1,n]\!]^3}$ as a 3-dimensional array with respect to the basis $(e_{i_1} \otimes e_{i_2} \otimes e_{i_3})_{i\in[\![1,n]\!]^3}$, where we denote by $(e_\iota)_{\iota\in[\![1,n]\!]}$ the standard basis vector of $\mathbb{F}_q^n$, see [11, Corol 2.24].

Let $\omega = \{\omega_1,\dots,\omega_n\}$ be a basis of $\mathbb{F}_{q^n}/\mathbb{F}_q$. Then $\mathfrak{s}_\omega : (\mathbb{F}_q^n)^{\otimes 3} \to \mathbb{F}_{q^n}^{n\times n}, \Gamma \mapsto \sum_{i_3=1}^n \omega_{i_3}(\Gamma[i_1,i_2,i_3])_{(i_1,i_2)\in[\![1,n]\!]^2}$ is an $\mathbb{F}_q$-isomorphism and yields an expression of every 3-tensor over $\mathbb{F}_q$ as a $n\times n$ matrix over $\mathbb{F}_{q^n}$. Therefore, every $\mathbb{F}_q$-vector subspace $\mathcal{C}$ of $(\mathbb{F}_q^n)^{\otimes 3}$ can be seen as a $\mathbb{F}_q$-vector subspace $\mathfrak{s}_\omega(\mathcal{C})$ of $\mathbb{F}_{q^n}^{n\times n}$. We will call $\mathcal{C}$ the **associated tensor code** of $\mathfrak{s}_\omega(\mathcal{C})$ through the basis ω. This is a generalisation of the associated matrix codes of $\mathbb{F}_{q^n}$-linear codes introduced in [12]. For further details, we refer the reader to [9, Chapter 14].

Coefficients, submatrices and subtensors: Given a matrix $M \in \mathbb{F}_q^{n\times n}$ for any $i,j \in [\![1,n]\!]$, we denote equivalently by $M_{i,j}$, $M_{(i,j)}$, or $M[i,j]$ the coefficient of M at the i^{th} row and at the j^{th} column. The colon ":" notation in the brackets indicates the element (vector, matrix, tensor, array) obtained for which the index at the location of the colon varies. For instance, if $M \in \mathbb{F}_q^{n\times n}$ and if $i \in [\![1,n]\!]$, then $M[i,:] =$

$(M_{i,j})_{j\in[\![1,n]\!]}$ is the i^{th} row of the matrix M, and if $T \in \mathbb{F}_q^{n\times n\times n}$ is a 3-tensor, then $T[i,:,:] = (T[i,j,k])_{j,k\in[\![1,n]\!]}$ is the n^2-tuple / matrix of size $n\times n$ whose coefficient at (j,k) is $T[i,j,k]$.

Slices and fibres: Let $j \in \{1,2,3\}$ and let Γ be a tensor in $\mathbb{F}_q^{n\times n\times n}$. A j-**slice** of Γ is a matrix obtained by fixing *only the j^{th} coordinate* in the coordinates of Γ. For example, any matrix of the form $\Gamma[i_1,:,:] = (\Gamma[i_1,i_2,i_3])_{i_2=1,i_3=1}^{n,n}$, or $\Gamma[:,i_2,:]$, or $\Gamma[:,:,i_3]$ is a j-slice for $j=1,2$, or 3, respectively. The j^{th} slice-space of Γ, denoted $\mathrm{ss}_j(\Gamma)$ is the span of all of its j^{th} slices. A j-**fibre** of Γ is a vector obtained by fixing *all but the j^{th} coordinate* in the coordinates of Γ, so for example, any vector of the form $\Gamma[:,i_2,i_3] = (\Gamma[i_1,i_2,i_3])_{i_1=1}^{n}$ with i_2,i_3 fixed is a 1-fibre. The j^{th} fibre-space of Γ, denoted $\mathrm{fs}_j(\Gamma)$ is the span of its j^{th} fibres.

I. Bilinearised polynomials

Linearised polynomials or q-polynomials over $\mathbb{F}_{q^n}$ are univariate polynomials in the $\mathbb{F}_{q^n}$-linear subspace of $\mathbb{F}_{q^n}[Z]$ spanned by the monomials $Z^{q^r}, r \in \mathbb{N}$. We denote this vector space by $\mathcal{M}_{q,\mathbb{F}_{q^n}}[Z]$. Such polynomials have the form $\sum_{j=0}^{\ell} f_j Z^{q^j}$ for $f_j \in \mathbb{F}_{q^n}$ and are linear over $\mathbb{F}_q$. Moreover, the $\mathbb{F}_q$-dimension of the kernel of a non-zero linearised q-polynomial is upper-bounded by its q-degree, see [7, Chapter 4].

Definition I.1. *The **bilinearised q-polynomials** over $\mathbb{F}_{q^n}$ are the elements in the following subset of $\mathbb{F}_{q^n}[X,Y]$.*

$$\mathcal{M}_{q,\mathbb{F}_{q^n}}[X,Y] := \mathrm{Span}_{\mathbb{F}_{q^n}}\left\{ X^{q^{i_1}}Y^{q^{i_2}} \,\middle|\, i\in\mathbb{N}^2 \right\}.$$

*An element $F(X,Y) \in \mathcal{M}_{q,\mathbb{F}_{q^n}}[X,Y]$ has an expression as $F(X,Y) = \sum_{i\in S} F_i X^{q^{i_1}}Y^{q^{i_2}}$ for some finite set $S\subset\mathbb{N}^2$ and $(F_i)_{i\in S} \in (\mathbb{F}_{q^n})^S$. We then define the support of F to be $\mathrm{Supp}(F) := \{i\in S : F_i \neq 0\}$. If $F(X,Y)$ is non-zero, we define the **partial q-degree** of $F(X,Y)$ along X (resp. Y), expressed as $q\text{-deg}_X F(X,Y)$, (resp. $q\text{-deg}_Y F(X,Y)$) to be the q-logarithm of its respective partial degree.*

Example I.2. *The bilinearised q-polynomial $F(X,Y) = X^qY^{q^5} + XY^q + X^{q^3}Y$ has $q\text{-deg}_X F(X,Y) = 3$ and has $q\text{-deg}_Y F(X,Y) = 5$.*

This set is not a sub-algebra of $\mathbb{F}_{q^n}[X,Y]$ as it is not stable upon r^{th} power for any $r\in\mathbb{N}$ such that r and q are coprime. The q^{th} power of a bilinearised q-polynomial is also a bilinearised q-polynomial, therefore, the space is stable upon left-composition by a (single variable) linearised q-polynomial.

Proposition I.3. *Let $F(X,Y) \in \mathcal{M}_{q,\mathbb{F}_{q^n}}[X,Y]$. Then the evaluation map given by $\mathbb{F}_{q^n}^2 \to \mathbb{F}_{q^n}, (x,y)\mapsto F(x,y)$ is bilinear over $\mathbb{F}_q$.*

A. Roth-tensor codes

Definition I.4. *Let $\mathcal{S}\subseteq[\![0,n-1]\!]^m$. We define the **(evaluation) Roth-tensor code** associated to $\mathcal{S}$ and α to be the following $\mathbb{F}_{q^n}$-linear code in $\mathbb{F}_{q^n}^{n\times n}$.*

$$\mathcal{C}_\alpha(\mathcal{S}) := \left\{ \left(f(\alpha_{i_1},\alpha_{i_2})\right)_{i\in[\![1,n]\!]^2} \,\middle|\, \begin{array}{l} f\in\mathcal{M}_{n,\mathbb{F}_{q^n}}[X,Y], \\ \mathrm{Supp}(f)\subseteq\mathcal{S} \end{array} \right\}.$$

We observe that every column or row of a codeword of a Roth-tensor code is a codeword of a Gabidulin code, as stated in the following proposition.

Proposition I.5. *Let $\mathcal{S}\subseteq[\![0,n-1]\!]^2$. Then $\mathcal{C}_\alpha(\mathcal{S})$ are $\mathbb{F}_{q^n}$-vector spaces of $\mathbb{F}_{q^n}$-dimension $|\mathcal{S}|$ and we have the following monomorphisms of $\mathbb{F}_{q^n}$-vector spaces.*

$$\phi_1 : \mathcal{C}_\alpha(\mathcal{S}) \hookrightarrow (\mathcal{G}_{\max(\pi_1(\mathcal{S}))+1}(\alpha))^n, C\mapsto (C[:,j])_{j\in[\![1,n]\!]}$$
$$\phi_2 : \mathcal{C}_\alpha(\mathcal{S}) \hookrightarrow (\mathcal{G}_{\max(\pi_2(\mathcal{S}))+1}(\alpha))^n, C\mapsto (C[i,:])_{i\in[\![1,m]\!]}.$$

As stated in [3, Section 3.2], we can give a dual expression of such codes through a given basis $\omega = (\omega_1,\dots,\omega_n)$ of $\mathbb{F}_{q^n}/\mathbb{F}_q$. For each subset $\mathcal{S}\subseteq[\![0,n-1]\!]^m$, the associated code of $\mathcal{C}_\alpha(\mathcal{S})$ regarding ω is the following, where $\alpha^\perp$ is the dual basis of α, see [7, Def 2.30]:

$$\left\{ \Gamma\in(\mathbb{F}_q^n)^{\otimes 3} \,\middle|\, \begin{array}{l} \forall r\in[\![0,n-1]\!]^m\backslash\mathcal{S}: \\ \sum_{i\in[\![1,n]\!]^3}\Gamma[i](\alpha_{i_1}^\perp)^{q^{r_1}}(\alpha_{i_2}^\perp)^{q^{r_2}}\omega_{i_3}=0 \end{array} \right\}.$$

Proposition I.6. *Let $F(X,Y)\in\mathcal{M}_{q,\mathbb{F}_{q^n}}[X,Y]$ and denote by F its evaluation map. If $\deg_Y F(X,Y) < q^n$ and $F(X,Y)\neq 0$, then $\dim_{\mathbb{F}_q}\mathfrak{Rad}_1(F) \le q\text{-deg}_X F(X,Y)$. Likewise, if $\deg_X F(X,Y) < q^n$ and $F(X,Y)\neq 0$, then $\dim_{\mathbb{F}_q}\mathfrak{Rad}_2(F) \le q\text{-deg}_Y F(X,Y)$.*

B. Fibre and slice weights

Definition I.7. *We define the **fibre weight** of a matrix $T\in\mathbb{F}_{q^n}^{n\times n}$ to be the integer $w_{\mathrm{fs}_3}(T)$ being the dimension of the $\mathbb{F}_q$-span of the entries of T.*

The dimension of the $\mathbb{F}_q$-span of the entries of the matrix $T\in\mathbb{F}_{q^n}^{n\times n}$ is exactly the $\mathbb{F}_q$-rank of its image through the isomorphism $\mathbb{F}_{q^n}^{n\times n}\to\mathbb{F}_{q^n}^{n^2}$. In particular, decoding any tensor-code with respect to this metric is directly equivalent to decode its isomorphic image in $\mathbb{F}_{q^n}^{n^2}$ for the rank-metric.

We will denote by $\mathcal{U}_1(T)$ (resp. $\mathcal{U}_2(T)$) the $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}^n$ spanned by all of the rows (1-slices), resp the columns (2-slices) of T over $\mathbb{F}_q$. They are respectively $\mathbb{F}_q$-isomorphic to their corresponding slice space of Γ, an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{n\times n}$.

Definition I.8. *For $j\in\{1,2\}$, we define the j-**slice space weight** of a tensor $T\in\mathbb{F}_{q^n}^{n\times n}$ to be the integer given by $w_{\mathrm{ss}_j}(T) = \dim_{\mathbb{F}_q}\mathcal{U}_j(T)$.*

Proposition I.9. *Let $T\in\mathbb{F}_{q^n}^{n\times n}$ and let $\Gamma\in\mathbb{F}_q^{n\times n\times n}$ be its associated tensor through any basis ω. Then $w_{\mathrm{ss}_1}(T)$, $w_{\mathrm{ss}_2}(T)$ and $w_{\mathrm{fs}_3}(T)$ are exactly the $\mathbb{F}_q$-dimensions of $\mathrm{ss}_1(\Gamma)$, $\mathrm{ss}_2(\Gamma)$ and $\mathrm{fs}_3(\Gamma)$ respectively, which do not depend on the choice of ω.*

Proposition I.10. *Let $\mathcal{S}$ be a non-empty subset of $[\![0,n-1]\!]^2$.*

- $\min_{C\in\mathcal{C}_\alpha(\mathcal{S})\backslash\{0\}} w_{\mathrm{fs}_3}(C) \ge n - \max_{j\in\{1,2\}}\max\pi_j(\mathcal{S})$.
- $\min_{C\in\mathcal{C}_\alpha(\mathcal{S})\backslash\{0\}} w_{\mathrm{ss}_j}(C) \ge n - \max\pi_j(\mathcal{S}), \forall j\in\{1,2\}$.

Definition I.11. *We define the **tensor-rank** of an element $T\in\mathbb{F}_{q^n}^{n\times n}$ denoted $\mathrm{trank}_{\mathbb{F}_q}(T)$ is defined to be the tensor-rank $\mathrm{trank}(\Gamma)$ of an associated tensor $\Gamma\in(\mathbb{F}_q^n)^{\otimes 3}$ as defined in [9, Prop 14.44]. Elements of tensor-rank one are called elementary tensors.*

One can check that, for a given $\Gamma \in (\mathbb{F}_q^n)^{\otimes 3}$, if one writes $\Gamma = \sum_{r=1}^{\eta} M_r \otimes c_r$ with $M_1, \dots, M_\eta \in \mathbb{F}_q^{n\times n}$ and $c_1, \dots, c_\eta \in \mathbb{F}_q^n$ and η minimal, then $(M_1, \dots, M_\eta)$ and $(c_1, \dots, c_\eta)$ are respective bases of the the third slice-space and fibre-space of Γ.

Lemma I.12. *Let $\Gamma \in (\mathbb{F}_q^n)^{\otimes 3}$. Then for each $j \in [\![1, 3]\!]$ we have $\dim_{\mathbb{F}_q} \mathrm{ss}_j(\Gamma) = \dim_{\mathbb{F}_q} \mathrm{fs}_j(\Gamma)$.*

Proposition I.13. *Let $T \in \mathbb{F}_{q^n}^{n\times n}$ and $j \in \{1, 2\}$. We have $w_{\mathrm{fs}_3}(T) \leq \mathrm{trank}_{\mathbb{F}_q}(T)$ and $w_{\mathrm{ss}_j}(T) \leq \mathrm{trank}_{\mathbb{F}_q}(T)$.*

This is a direct consequence of [9, Prop. 14.45].

Corollary I.14. *Let $T \in \mathbb{F}_{q^n}^{n\times n}$. Then the have the upper bound $\max_{i_1\in[\![1,n]\!]} \mathrm{rank}_{\mathbb{F}_q} T[i_1, :] \leq \mathrm{trank}_{\mathbb{F}_q}(T)$ and $\max_{j\in[\![1,n]\!]} \mathrm{rank}_{\mathbb{F}_q} T[:, j] \leq \mathrm{trank}_{\mathbb{F}_q}(T)$.*

Consequently $\mathrm{trank}(C) \geq n - \max_{j\in\{1,2\}} \max \pi_j(\mathcal{S})$ for any codeword $C \in \mathcal{C}_\alpha(\mathcal{S})\backslash\{0\}$ where $\mathcal{S} \subseteq [\![0, n-1]\!]^2$.

II. Decoding

A. Decoding every Gabidulin codeword.

In [8], Gabidulin introduced an algorithm to decode Gabidulin codewords in $\mathcal{G}_k(\epsilon)$ of length n with errors of rank at most $\lfloor \frac{n-k}{2} \rfloor$. Since Proposition I.5 states that every column and row of a codeword in $\mathcal{C}_\alpha(\mathcal{S})$ is a Gabidublin codeword, we can infer a decoding algorithm that does not use the structure of the whole code but only the fact that $\mathcal{C}_\alpha(\mathcal{S})$ is embedded in a Cartesian product of Gabidulin codes. This motivates us to study this code with respect to the metric inherited from the structure of direct sums of rank-metric codes.

We denote by $\texttt{GabDec}(r, k, \alpha)$ the function that returns the unique Gabidulin codeword $c \in \mathcal{G}_k(\alpha)$ for $r = c + e$ with e a vector in $\mathbb{F}_{q^n}^n$ of rank at most $\lfloor \frac{n-k}{2} \rfloor$. We will assume that the function returns a random word if $r - c$ has rank greater than $\lfloor \frac{n-k}{2} \rfloor$ for each $c \in \mathcal{G}_k(\alpha)$.

Algorithm 1 Fibre-wise decoding (column-wise)

Input: n, q, $\mathcal{S} \subseteq [\![0, n-1]\!]^2$ and $R \in \mathbb{F}_{q^n}^{n\times n}$.
  $C \leftarrow 0 \in \mathbb{F}_{q^n}^{n\times n}$.
  for $i_2 \in [\![1, n]\!]$ **do**
    $C[:, i_2] \leftarrow \texttt{GabDec}(R[:, i_2], \max(\pi_1(\mathcal{S})) + 1, \alpha)$
  end for
  return C.

Algorithm 1 can decode with certainty any message $R = C + E$ such that $C \in \mathcal{C}_\alpha(\mathcal{S})$ and such that the $\mathbb{F}_q$-rank of every column of E is upper-bounded by half the minimum distance of the Gabidulin code of dimension $\max \pi_j(\mathcal{S})$, so it can decode any error subject to the following constraints.

$$\max_{i_2\in[\![1,n]\!]} \mathrm{rank}_{\mathbb{F}_q} E[:, i_2] \leq \left\lfloor \frac{n - \max \pi_1(\mathcal{S}) - 1}{2} \right\rfloor \quad (1)$$

We remind the reader that the Hamming weight of a vector is its number of non-zero entries. In the following part, we will assume that $\mathcal{S} = [\![0, \mu_1]\!] \times [\![0, \mu_2]\!]$.

Lemma II.1. *Let θ, κ be integers. Let $E \in \mathbb{F}_{q^n}^{n\times n}$ with the following condition.*

$$\min_{\substack{\mathcal{J}\subseteq[\![1,n]\!] \\ |\mathcal{J}|=\kappa}} \max_{j\in\mathcal{J}} \mathrm{rank}_{\mathbb{F}_q} E[:, j] \leq \theta \quad (2)$$

Assume that Algorithm 1 on a received message of the form $R = C + E$ with $C \in \mathcal{C}_\alpha(\mathcal{S})$ returns a matrix $\tilde{C}$ such that C and $\tilde{C}$ have identical columns where the rank of the corresponding column in E is less than θ, and the other columns of $\tilde{C}$ are unspecified. Then $\tilde{C} = C + \tilde{E}$ where all rows of $\tilde{E}$ have Hamming weight at most $n - \kappa$.

Algorithm 2 Two-way fibre-wise decoding

Input: n, q, $\mu_1, \mu_2 \in [\![0, n-1]\!]$ defining $\mathcal{S}$, and $R \in \mathbb{F}_{q^n}^{n\times n}$
  $C \leftarrow 0 \in \mathbb{F}_{q^n}^{n\times n}$
  $\tilde{C} \leftarrow 0 \in \mathbb{F}_{q^n}^{n\times n}$
  for $i_2 \in [\![1, n]\!]$ **do**
    $\tilde{C}[:, i_2] \leftarrow \texttt{GabDec}(R[:, i_2], \mu_1 + 1, \alpha)$
  end for
  for $i_1 \in [\![1, n]\!]$ **do**
    $C[i_1, :] \leftarrow \texttt{GabDec}(\tilde{C}[i_1, :], \mu_2 + 1, \alpha)$
  end for
  return C.

Theorem II.2. *Let $\mu_1, \mu_2 \in [\![0, n-1]\!]$. Let $R = C + E$ with $C \in \mathcal{C}_\alpha([\![0, \mu_1]\!] \times [\![0, \mu_2]\!])$ and $E \in \mathbb{F}_{q^n}^{n\times n}$ subject to the constraint (3). Then running Algorithm 2 with input R returns C.*

$$\min_{\substack{\mathcal{J}\subseteq[\![1,n]\!] \\ |\mathcal{J}|=\lceil \frac{n+\mu_2+1}{2} \rceil}} \max_{j\in\mathcal{J}} \mathrm{rank}_{\mathbb{F}_q} E[:, j] \leq \left\lfloor \frac{n - \mu_1 - 1}{2} \right\rfloor. \quad (3)$$

Clearly, on $\mathcal{C}_\alpha(\mathcal{S})$ for a fixed $\mathcal{S} = [\![0, \mu_1]\!] \times [\![0, \mu_2]\!]$, Algorithm 2 corrects the set of errors corrected by Algorithm 1 but corrects strictly more errors, see Section III.

B. Factoring on the left

Let $f(X, Y)$ be a bilinearised polynomial $f(X, Y) = \sum_{s\in\mathcal{S}} f_s X^{q^{s_1}} X^{q^{s_2}}$ with a given $\mathcal{S} \subseteq [\![0, n-1]\!]^2$, and let a pair $(V(Z), N(X, Y))$ where $V(Z) \in \mathcal{M}_{q,\mathbb{F}_{q^n}}[Z]$ is non-zero and $N(X, Y) \in \mathcal{M}_{q,\mathbb{F}_{q^n}}[X, Y]$ whose support is included in $\mathcal{S} + [\![0, q\text{-deg}\, V(Z)]\!]$, and $V(f(X, Y)) = N(X, Y)$. Computing the coefficients of $N(X, Y)$ shows that for each $s \in \mathcal{S}$, f_s is a function of the coefficients in $V(Z)$, in $N(X, Y)$ and of $f_{s-1}, f_{s-2}, \dots$ until the index $s - j$ exits $\mathcal{S}$. In addition, the same expression of the coefficients in $N(X, Y)$ shows that f_s such that $s \in \mathcal{S}$ and $(\forall j \in \mathbb{N}^* : s - j \notin \mathcal{S})$, can be computed only knowing $V(Z)$ and $N(X, Y)$, see Algorithm 3.

C. A Berlekamp-Welch-like decoder

We use the technique introduced in the Loidreau-Overbeck decoder to decode a different range of errors using the j-slice space weight. Let $\mu \in [\![0, n-2]\!]$ and fix $\mathcal{S} = [\![0, \mu]\!]^2$.

Let $t \in \mathbb{N}$ and let $E \in \mathbb{F}_{q^n}^{n\times n}$ with $w_{\mathrm{fs}_3}(E) \leq t$. Then if $R = C + E$ with a given $C \in \mathcal{C}_\alpha(\mathcal{S})$ with associated

Algorithm 3 Factoring on the left

Input: n, q, $\mathcal{S}$ a subset of $[\![0, n-1]\!]^2$, $V(Z)$ and $N(X,Y)$ q-polynomials with $V(Z) \neq 0$ and $\mathrm{Supp}(N) \subseteq \mathcal{S} + [\![0, \deg_q(V)]\!]$.

$M \leftarrow \max(\max \pi_1(\mathcal{S}), \max \pi_2(\mathcal{S}))$

$\theta \leftarrow \deg_q(V)$

$f \leftarrow 0 \in \mathcal{M}_{q,\mathbb{F}_{q^n}}[X,Y]$

$\nu \leftarrow \min\{\ell \in [\![0,t]\!] \mid v_\ell \neq 0\}$

▷ The function $\texttt{Coef}(F, \boldsymbol{m})$ returns the coefficient in front of the monomial $\boldsymbol{m}$ in the polynomial F.

if $N = 0$ **then**

  return f

end if

for $\delta \in [\![-M, M]\!]$ **do**

  for τ **from** 0 **to** M **do**

    $s \leftarrow (\delta + \tau, \tau)$

    if $s \in \mathcal{S}$ **then**

$$\Sigma \leftarrow \sum_{\substack{\ell \in [\![\nu+1,\theta]\!] \\ s+\nu-\ell \in \mathcal{S}}} \texttt{Coef}(V, Z^{q^\ell}) \times \left(\texttt{Coef}\left(f, X^{q^{s_1+\nu-\ell}} Y^{q^{s_2+\nu-\ell}}\right)\right)^{q^\ell}$$

$$c \leftarrow \left((\texttt{Coef}(V, Z^{q^\nu})^{-1} \times \left(\texttt{Coef}\left(N, X^{q^{s_1+\nu}} Y^{q^{s_2+\nu}}\right) - \Sigma\right)\right)^{1/q^\nu}$$

$$f \leftarrow f + cX^{q^{s_1}} Y^{q^{s_2}}$$

    end if

  end for

end for

return f

polynomial $f(X,Y)$, we consider the following equation of unknowns $(V(Z), N(X,Y))$ with $V(Z) \in \mathcal{M}_{q,\mathbb{F}_{q^n}}[Z]$ and with $N(X,Y) \in \mathcal{M}_{q,\mathbb{F}_{q^n}}[X,Y]$ such that $q\text{-deg}\, V(Z) \leq t$ and $\mathrm{Supp}(N(X,Y)) \subseteq \mathcal{S} + [\![0,t]\!]$.

$$\forall i \in [\![1,n]\!]^2 : V(R_{i_1,i_2}) = N(\alpha_{i_1}, \alpha_{i_2}) \tag{4}$$

In this situation, $(V(Z), V(f(X,Y)))$ is a solution of Equation (4) for any q-polynomial $V(Z)$ with $q\text{-deg}\, V \leq t$.

Theorem II.3. *Let $\mu \in [\![1, n-1]\!]$ and fix $\mathcal{S} := [\![0, n-1]\!]$. Let $C \in \mathcal{C}_\alpha(\mathcal{S})$ corresponding to $f(X,Y)$. Let $E \in \mathbb{F}_{q^n}^{n\times n}$ and let $R = E + C$. Let $\Theta \in [\![0, n-\mu-2]\!]$ and assume that $\min_{j\in\{1,2\}} w_{\mathrm{ss}_j}(E) \leq \Theta$. Then any solution $(V(Z), N(X,Y))$ of Equation (4) for $t = n - \mu - 1 - \Theta$ satisfies $V(f(X,Y)) = N(X,Y)$.*

Sketch of proof: Let $(V(Z), N(X,Y))$ a solution of (4) such that $q\text{-deg}\, V(Z) \leq t$ and $\mathrm{Supp}(N(X,Y)) \subseteq \mathcal{S} + [\![0,t]\!]$. For each $(i_1, i_2) \in [\![1,n]\!]^2$ we have

$$(V \circ f - N)(\alpha_{i_1}, \alpha_{i_2}) = -V(E[i_1, i_2]). \tag{5}$$

Let $W := (V(E[i_1,i_2]))_{(i_1,i_2)\in[\![1,n]\!]^2} \in \mathbb{F}_{q^n}^{n\times n}$. Assume that $\dim_{\mathbb{F}_q} \mathcal{U}_1(E) \leq \Theta$. Let $\ell : \mathbb{F}_{q^n}^n \to \mathbb{F}_{q^n}^n$ be the $\mathbb{F}_{q^n}$-linear map uniquely defined by $\ell(e_{i_1}) = W[i_1, :]$ for all $i_1 \in [\![1,n]\!]$. One can check that $w_{\mathrm{ss}_1}(W) \leq w_{\mathrm{ss}_1}(E)$ hence $w_{\mathrm{ss}_1}(W) \leq \Theta$. In addition, expressing the coefficients of the elements in the radical of $V \circ f - N$ using (5) yields an isomorphism between $\mathfrak{Rad}_1(V \circ f - N)$ and $\ker(\ell) \cap \mathbb{F}_q^n$, the kernel of the restriction of ℓ to $\mathbb{F}_q^n$, which has image $\mathcal{U}_1(W)$. Hence, the rank-nullity theorem applied on this restriction yields the following.

$$\dim_{\mathbb{F}_q}(\mathbb{F}_q^n \cap \ker(\ell)) = \dim_{\mathbb{F}_q} \mathbb{F}_q^n - w_{\mathrm{ss}_1}(W) \geq n - \Theta.$$

Finally, assume that $(V \circ f - N)(X,Y)$ is not the zero polynomial. Since $(V \circ f - N)$ has support in $\mathcal{S} + [\![0,t]\!]$. Therefore, the q-degrees of $(V \circ f - N)(X,Y)$ are upper bounded by $n - \Theta - 1$, which contradicts Proposition I.6. ■

Corollary II.4. *Assume that we have the following condition.*

$$w_{\Sigma\mathrm{ss}}(E) := w_{\mathrm{fs}_3}(E) + \min_{j\in\{1,2\}} w_{\mathrm{ss}_j}(E) \leq n - \mu - 1 \tag{6}$$

Then there exists $t \in [\![0, n-1]\!]$ such that every solution $(V(Z), N(X,Y))$ of Equation (4) where $q\text{-deg}\, V(Z) \leq t$ and $\mathrm{Supp}(N) \subseteq \mathcal{S} + [\![0,t]\!]$ is of the form $N(X,Y) = V(Z) \circ f(X,Y)$.

Hence Algorithm 4 can retrieve any codeword in $\mathcal{C}_\alpha(\mathcal{S})$ with $\mathcal{S} = [\![0,\mu]\!]^2$ with an error $E \in \mathbb{F}_{q^n}^{n\times n}$ such that $\min_{j\in\{1,2\}} w_{\mathrm{ss}_j}(E)$ at most $n - \mu - t - 1$ and $w_{\mathrm{fs}_3}(\mathcal{S})$ at most t for a given $t \in [\![0, n-1]\!]$.

Algorithm 4 Radical Decoding with specified fibre-weight.

Input: n, q, $t \in [\![0, n-1]\!]$, μ defining $\mathcal{S}$, $R \in \mathbb{F}_{q^n}^{n\times n}$.

Pick a non-zero solution $(V(Z), N(X,Y))$ of Equation (4).

if $V(Z) = Z$ **then**

  return R

end if

Run **Algorithm 3** to factorize $N(X,Y)$ into $V(f(X,Y))$.

Create C the codeword associated to $f(X,Y)$.

return C

We observe that as t increases, Equation (4) has more and more solutions, but if the shape of E does not satisfy the criterion of Theorem II.3 (for as t increases, the maximum possible Θ decreases) the solutions of the equations can no longer be solutions of the form $V \circ f = N$, and hence do not retrieve the codeword. Therefore, if at least one configuration fits the requirements of Theorem II.3, we can find the first of these occurrences to ensure that we find a correct solution. That way, instead of treating the allowed fibre weight as a parameter of the problem, Algorithm 5 can correct any error E such that $w_{\Sigma\mathrm{ss}}(E) \leq n - \mu - 1$.

III. Comparisons

A. Roth's algorithms

In his paper [3], Roth gave two algorithms to decode his codes "$\mathcal{C}(n,3,3;q)$" (generalised to any order) and "$\mathcal{C}(n,5,3;q)$" for errors respectively of tensor-rank at most one and two. The codes are respectively isomorphic to the codes $\mathcal{C}_\alpha(\mathcal{S}_1)$ and $\mathcal{C}_\alpha(\mathcal{S}_2)$ with $\mathcal{S}_1 \supseteq \{s \in [\![0,n-1]\!]^2 \mid s_1 + s_2 > 1\}$ and $\mathcal{S}_2 \supseteq \{s \in [\![0,n-1]\!]^2 \mid s_1 + s_2 > 3\}$. Since the sets $\mathcal{S}_1$ and $\mathcal{S}_2$ have maximum $n-1$ on all directions, running Algorithms 1 or 4 would result in no error correction capability.

Algorithm 5 Radical Decoding.

Input: n, q, μ defining $\mathcal{S}$, $R \in \mathbb{F}_{q^n}^{n\times n}$.
Find the smallest t s.t. Equation (4) has an non-zero solution.
if no such t exists **then**
return "No solution".
end if
Pick a non-zero solution $(V(Z), N(X,Y))$ of Equation (4).
if $V(Z) = Z$ **then**
return R
end if
Run Algorithm 3 to factorize $N(X,Y)$ into $V(f(X,Y))$.
Create C the codeword associated to $f(X,Y)$.
return C

Algorithm	**Dimension of the code over $\mathbb{F}_{q^n}$**	**Asymptotic number of correctable errors**
Algorithm 1 on $\mathcal{C}_\alpha([\![0,n-1]\!]\times[\![0,n-3]\!])$	$n(n-2)$	$\frac{q^{2n^2}}{(q-1)^n}$
Algorithm 2 on $\mathcal{C}_\alpha([\![0,n-3]\!]^2)$	$(n-2)^2$	$n\frac{q^{3n^2-2n}}{(q-1)^{n-1}}$
Roth decoder on $\mathcal{C}(n,5,3,q)$	n^2-10	$\frac{q^{6n}}{2(q-1)^4}$
Roth decoder on $\mathcal{C}(n,3,3,q)$	n^2-3	$\frac{q^{3n}}{(q-1)^2}$

Fig. 1. Comparison of the decoding algorithms.

The code $\mathcal{C}(n,3,3;q)$ has $\mathbb{F}_{q^n}$-dimension at least n^2-3 correcting every error of tensor-rank at most 1 in $(\mathbb{F}_q^n)^{\otimes 3}$, *i.e.* with at least $\frac{(q^n-1)^3}{(q-1)^2}+1$ correctable errors.

The code $\mathcal{C}(n,5,3;q)$ has $\mathbb{F}_{q^n}$-dimension at least n^2-10 correcting every error of tensor-rank at most 2 in $(\mathbb{F}_q^n)^{\otimes 3}$, and one can check that it corresponds to the following number of correctable errors.

$$\frac{q(q^n-1)^3(q^{n-1}-1)^2\left(\frac{1}{2}q^2(q+1)(q^{n-1}-1)+3(q-1)\right)}{(q-1)^3(q^2-1)}+\frac{(q^n-1)^3}{(q-1)^2}+1 \tag{7}$$

B. Fibre-wise decoders

Since the number of matrices of a given size and a given rank over a given field is known (c.f. [13, Thm 25.2]), it is possible to compute the number of errors satisfying (1) or (3).

Since Roth codes introduced in Subsection III-A have dimension strictly larger than any Roth tensor code $\mathcal{C}_\alpha(\mathcal{S})$ for which at least one of the algorithms above corrects non-trivial errors, we can compare the former with the largest Roth tensor code for which Algorithms 1 and 2 can decode non-trivial errors, see Figure 1 where are displayed their asymptotic equivalents, for $n \geq 3$.

C. Fibre and radical.

Proposition III.1. *With a given code $\mathcal{C}_\alpha([\![0,\mu]\!]^2)$. There exists errors satisfying (1) that do no do not satisfy Equation (6). If an error satisfies (6), either itself or its transpose satisfies (1), but not necessarily both.*

The computational complexity of the algorithms above in terms of operations over $\mathbb{F}_q$ in the following. With [14], Algorithm 1 and Algorithm 2 have same asymptotic complexity $\mathcal{O}(n^4\log n)$. Since Equation (4), for a given t, is a system of n^3 equations and $n((\mu+1)^2+(2\mu+1)t)$ unknowns on $\mathbb{F}_q$, yielding a complexity $\mathcal{O}(n^9)$ for Algorithm 4 and $\mathcal{O}(n^9\log n)$ for Algorithm 5, see [15, Chapter 3].

D. Remarks on the tensor rank

As shown in Subsection I-B, each metric introduced, including $w_{\Sigma\mathrm{ss}}$, gives a lower bound on the tensor-rank metric. In particular if a code is t-error correcting one of these metrics, then it is t-error correcting for the tensor rank.

Corollary III.2. *The $\mathbb{F}_q$-tensor code $\mathcal{C}_\alpha([\![0,\mu]\!]^2)$ of dimension $n(\mu+1)^2$ endowed with the tensor-rank metric is $\left\lfloor\frac{n-\mu-1}{2}\right\rfloor$-error correcting, and Algorithms 1, 2 and 4 reach the decoding radius.*

Remark III.3. *Let $\kappa \in [\![1,n-1]\!]$. We remark that given a $T \in \mathbb{F}_{q^n}^{n\times n}$, there is no clear deterministic exploitable improvement of the bound $\mathrm{trank}(T) \geq \min_{\mathcal{J},|\mathcal{J}|=\kappa}\max_{j\in\mathcal{J}}\ \mathrm{rank}_{\mathbb{F}_q} T[:,j]$, which is a consequence of Corollary I.14, e.g. $T_1, T_2 \in \mathbb{F}_{q^n}^{n\times n}$ defined by $T_1[i] = \alpha_{i_1}\mathbf{1}_{i_1\leq a}\mathbf{1}_{i_2\leq n-\kappa}$ and $T_2[i] = \alpha_{i_1}\mathbf{1}_{i_1\leq a}$.*

Contrarily to decoders specifically designed for the tensor-rank, the Algorithms above can correct more errors, *e.g.* Figure 1. Let $R \in \mathbb{N}^*$. On one hand, the number of elements in $\mathbb{F}_{q^n}^{n\times n}$ of tensor rank at most R is at most $\frac{(q^n-1)^{3(R+1)}}{(q-1)^{2(R-1)}}$, as every such tensor can be expressed as a sum of $R+1$ elementary tensors, *e.g.* $\Gamma = \Gamma+\tau-\tau$ for $\mathrm{trank}(\Gamma) = R-1$ and τ an elementary tensor. On the other hand, the number of tensors $E \in \mathbb{F}_{q^n}^{n\times n}$ with $w_{\Sigma\,\mathrm{ss}}(E) < 2R$, condition implied by $(w_{\mathrm{ss}_1}(E), w_{\mathrm{ss}_2}(E), w_{\mathrm{fs}_3}(E)) = (R, R-1, n)$, is at least $q^{nR(R-1)}$. Therefore, the number of $E \in \mathbb{F}_{q^n}^{n\times n}$ corrected by Algorithm 5 with $\mathrm{trank}_{\mathbb{F}_q}(E) > R = \left\lfloor\frac{n-\mu-1}{2}\right\rfloor$ is at least $q^{nR(R-1)} - \frac{(q^n-1)^{3(R+1)}}{(q-1)^{2(R+1)}}$. If $R = \lfloor an+b\rfloor$ with $a \in [0,1]$ and $b \in \mathbb{Z}_{\leq 0}$, unless $a = 1$, then the term on the right will be ultimately negligible compared to the term on the left.

Remark III.4. *It is non trivial to check if lower-bound on the tensor-rank of Corollary I.14 is met or not. It is however the case for $\mu = n-1$ as the evaluation of $a\,\mathrm{tr}(bX)\,\mathrm{tr}(cY)$ has tensor rank one, with $a, b, c \in \mathbb{F}_q$ with an argument similar to [9, Prop 14.44], with [7, Thm 2.24].*

ACKNOWLEDGEMENTS

This work has emanated from research conducted with the financial support of the European Union MSCA Doctoral Networks, (HORIZON-MSCA-2021-DN-01, Project 101072316), the French *Agence Nationale de la Recherche* project ANR-21-CE39-0009-BARRACUDA and by *Plan France 2030* ANR-22-PETQ-0008.

Link to GitHub repository with programs:
https://github.com/lucienfrancois/RothTensorCodes

REFERENCES

[1] G. Lunardon, R. Trombetti, and Y. Zhou, "Generalized twisted gabidulin codes," *Journal of Combinatorial Theory, Series A*, vol. 159, pp. 79–106, 2018.

[2] J. Sheekey, "A new family of linear maximum rank distance codes," *Adv. Math. Commun.*, vol. 10, 2016.

[3] R. Roth, "Tensor codes for the rank metric," *IEEE Transactions on Information Theory*, vol. 42, no. 6, pp. 2146–2157, 1996.

[4] L. R. Welch and E. R. Berlekamp, "Error correction for algebraic block codes," Patent, Dec. 30, 1986, uS Patent 4,633,470.

[5] R. E. Blahut, *Decoding of Cyclic Codes and Codes on Curves*, ser. Handbook of Coding Theory Vol II. Elsevier, 1998, pp. 1569–1633.

[6] P. Loidreau, "A Welch-Berlekamp like algorithm for decoding Gabidulin codes," in *Coding and Cryptography*, Ø. Ytrehus, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 36–45.

[7] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, ser. Encyclopedia of Mathematics. Cambridge University Press, 1994.

[8] E. Gabidulin, "Theory of codes with maximum rank distance (translation)," *Problems of Information Transmission*, vol. 21, pp. 1–12, 01 1985.

[9] P. Bürgisser, T. Lickteig, M. Clausen, and M. Shokrollahi, *Algebraic Complexity Theory*, ser. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013.

[10] B. Cooperstein, *Advanced linear algebra*. CRC Press, 2010.

[11] S. Lang, *The Tensor Product*. New York, NY: Springer New York, 2002, pp. 601–640.

[12] A. Ravagnani, "Rank-metric codes and their duality theory," *Designs, codes, and cryptography*, vol. 80, no. 1, pp. 197–216, 2016.

[13] J. H. Van Lint and R. M. Wilson, *A course in combinatorics*. Cambridge: Cambridge University Press, 1992.

[14] A. Wachter-Zeh, V. Afanassiev, and V. Sidorenko, "Fast decoding of gabidulin codes," *Designs, Codes and Cryptography*, vol. 66, no. 1, pp. 57–73, Jan 2013.

[15] G. Golub and C. Van Loan, *Matrix Computations*, ser. Johns Hopkins Studies in the Mathematical Sciences. Johns Hopkins University Press, 2013.