Rank metric and Gabidulin codes in characteristic zero

Daniel Augot, Pierre Loidreau, Gwezheneg Robert

Rank metric and Gabidulin codes in characteristic zero

Daniel Augot
INRIA Saclay-Île-de-France
École polytechnique
Palaiseau, France
Email: Daniel.Augot@inria.fr

Pierre Loidreau
DGA and IRMAR
Université de Rennes 1
Rennes, France
Email: Pierre.Loidreau@univ-rennes1.fr

Gwezheneg ROBERT
IRMAR
Université de Rennes 1
Rennes, France
Email: Gwezheneg.Robert@univ-rennes1.fr

***Abstract*—We transpose the theory of rank metric and Gabidulin codes to the case of fields of characteristic zero. The Frobenius automorphism is then replaced by any element of the Galois group. We derive some conditions on the automorphism to be able to easily transpose the results obtained by Gabidulin as well and a classical polynomial-time decoding algorithm. We also provide various definitions for the rank-metric.**

***Index Terms*—Space-time coding, Gabidulin codes, rank metric, skew polynomials, Ore rings, algebraic decoding, number fields.**

I. Motivation

Matricial codes with coefficients in a finite subset of the complex field are particularly well-suited for the design of space-time codes. When the metric of the code space is the rank metric, its minimum distance is called the diversity. This parameter is one of the crucial parameters in evaluating the performance of Minimum Distance Decoding [3].

A problem in the field of space-time coding is to construct codes with optimal rate/diversity trade-off. Lu and Kumar [7] used an original approach by transforming optimal codes in rank metric over finite fields, such as Gabidulin codes, into optimal codes for space-time coding over different types of constellations.

However a mapping $\mathbb{F}_q^k \to \mathbb{C}$ is used, which is difficult to reverse, yet its inverse is needed to recover information bits when decoding. Another construction based on Gabidulin codes over finite fields has been given in [8], using particular properties of Gaussian integers.

We propose in this paper to construct optimal codes similar to Gabidulin codes, with coefficients in $\mathbb{C}$, completely bypassing intermediate constructions using finite fields, using number fields and Galois automorphims. We also provide a decoding algorithm using with a polynomial number of field operations (this is not the bit complexity).

Further work is needed to study the proper use of this construction in the area of space-time coding.

II. Contribution

In the original paper of Gabidulin, the constructed codes are evaluation codes of linearized polynomials [5] with coefficients in a finite field. The associated metric is called *rank metric* and is of interest for correcting errors which occur along rows or columns of matrices. Transposing the results in characteristic zero fields is more tricky. Namely, in finite fields the Galois groups are well known and the field extensions are all cyclic. However in characteristic zero, it is abolutely not the case and one needs to be very careful and find some criteria so that we can transpose Gabidulin construction in that case.

We call polynomials equivalent to linearized polynomials *θ-polynomials*, where θ is an automorphism of a field extension $K \hookrightarrow L$ of degree m. The automorphism θ is of order n, which divides m. In the first section we establish conditions such that the θ-polynomials present robust properties, namely that the root-space of a θ-polynomial has dimension less than its degree. In a second section, we show that all the different possible metrics that we could think of concerning rank metric are in fact the same provided that the base field is exactly the fixed field of θ. Under this condition, we can define the *rank metric* in a unique way.

In the final section we construct Gabidulin codes, showing that they are optimal for the rank metric and that they can be decoded by using some of the existing decoding algorithms. And finally we give some examples. We refer the reader to [4] for basics on Galois theory.

III. θ-polynomials

In all the paper, we consider an algebraic field extension $K \hookrightarrow L$ with finite degree m, and an automorphism θ in the Galois group $\mathrm{Gal}(K \hookrightarrow L)$, of order $n \leq \mathrm{Gal}(K \hookrightarrow L) \leq m$. Given $v \in L$, we use the notation v^{θ^i} for $\theta^i(v)$. In the finite field case, when θ is the Frobenius automorphism $x \mapsto x^q$, $v^{\theta^i} = v^{q^i}$, and the similarity is nicely reflected in the notation.

We note $\mathcal{B} \stackrel{\text{def}}{=} (b_1, \ldots, b_m)$ a K-basis of L. For finite fields, we use the notation $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^m}$. Similarly to *linearized polynomials*, we define *θ-polynomials*, which is a special case of *skew polynomials*, namely, when there is no derivation.

Definition 1: A θ-polynomial is a finite summation of the form $\sum_i p_i X^{\theta^i}$, with $p_i \in L$. The greatest integer $i < \infty$ such that $p_i \neq 0$ is called its θ-degree, and is denoted by $\deg_\theta(P)$. We denote the set of θ-polynomials by $L[X;\theta]$. We have the following operations on the set $L[X;\theta]$:

1) Componentwise scalar multiplication and addition;

2) Multiplication: for $P(X) = \sum_i p_i X^{\theta^i}$ and $Q(X) = \sum_i q_i X^{\theta^i}$,

$$P(X) \cdot Q(X) = \sum_{i,j} p_i \, q_j^{\theta^i} \, X^{\theta^{i+j}};$$

3) Evaluation: Given $v \in L$, and $P(X) = \sum_i p_i X^{\theta^i}$:

$$P(v) = \sum p_i v^{\theta^i}.$$

The multiplication formula is motivated by the composition law: $P(X) \cdot Q(X) = P(Q(X))$. The following is well known.

Proposition 1 ([9]): The set of θ-polynomials $(L[X;\theta], +, \cdot)$ is a non-commutative integral domain, with unity X^{θ^0}. It is also a left and right Euclidean ring.

Such a ring is an Ore ring with trivial derivative. The proof is the same regardless of the characteristic of the fields. Considering the case where $K = \mathbb{F}_q$ and $L = \mathbb{F}_{q^m}$ are finite fields, and where θ is the Frobenius automorphism $x \mapsto x^q$, we get the set of *linearized polynomials*, also called *q-polynomials*. In that particular case, one has the following important proposition.

Proposition 2 ([10]): The roots of a q-polynomial with q-degree t form a $\mathbb{F}_q$-vector space with dimension at most t.

We define the root-space of a θ-polynomial $P(X)$ to be the set of $v \in L$ such that $P(v) = 0$. Then Prop. 2 does not generalize to more general θ-polynomials, when θ is not well behaved, as shown below.

Example 1: Here is an example of a θ-polynomial whose root-space dimension is twice its θ-degree. Let us consider the field extension

$$K = \mathbb{Q} \hookrightarrow L = \mathbb{Q}[Y]/(Y^8 + 1).$$

Let α be a root of $Y^8 + 1$, such that $(1, \ldots, \alpha^7)$ is a K-basis of L. Consider the automorphism θ defined by $\alpha \mapsto \alpha^3$. The polynomial $X^{\theta^1} - X^{\theta^0}$ has a root-space of dimension 2, with two K-generators: 1 and $\alpha^2 + \alpha^6$. One can actually check that the characteristic polynomial of θ as a K-linear map is $Y^8 - 2Y^4 + 1 = (Y^4 - 1)^2$, i.e. non square-free, which is the cause of the problem.

Thus we have a simple criteria on θ to establish a property equivalent to Prop. 2 in the general case.

Theorem 1: If the characteristic polynomial of θ, considered as a K-linear application, is square-free, then the dimension of the root-space of a θ-polynomial is less than or equal to its θ-degree.

Proof: Let $P(X) = \sum p_i X^{\theta^i}$. Let us denote $\overline{P}(X) \stackrel{\text{def}}{=} \sum p_i X^i$. Let M be the matrix of θ in the basis $\mathcal{B}$. Let y be an element of L and $Y_{\mathcal{B}}$ the m-dimensional vector in K^m corresponding to its representation in the basis $\mathcal{B}$. We have

$$P(y) \stackrel{\text{def}}{=} \sum_i p_i \theta^i(y) = \overline{P}(M) \cdot Y_{\mathcal{B}}.$$

Therefore the root-space of P is equal to the right kernel of the matrix $\overline{P}(M)$. Since by hypothesis the characteristic polynomial of θ is square-free, all its roots are distinct. Let $\alpha_1, \cdots, \alpha_m$ be its roots. Since θ is invertible 0 is not a root of the polynomial. Therefore, there exists a $m \times m$-non-singular matrix Q with coefficients in K, such that $M = Q^{-1} \cdot \underbrace{\text{Diag}\,(\alpha_1, \cdots, \alpha_m)}_{D} \cdot Q$. Hence

$$\begin{aligned}\overline{P}(M) &= Q^{-1} \cdot \sum_i p_i D^i \cdot Q \\ &= Q^{-1} \cdot \text{Diag}\left(\overline{P}(\alpha_1), \cdots, \overline{P}(\alpha_m)\right) \cdot Q.\end{aligned}$$

Therefore the dimension of the root-space of P is equal to the number of α_i's which are roots of $\overline{P}$. Since by hypothesis the α_i's are distinct and since the degree of $\overline{P}$ is the same as the degree of P, the dimension of the root-space of P is at most its degree. ∎

Note that the condition that the characteristic polynomial is square-free implies that $K = L^\theta$. We also need the following theorem, which show that we can find annihilator polynomials of K-subspaces of L.

Theorem 2: Let θ have a square-free characteristic polynomial. Let $\mathcal{V}$ be an s-dimensional K-subspace of L. Then there exists a unique monic θ-polynomial $P_{\mathcal{V}}$ with θ-degree s such that

$$\forall v \in \mathcal{V}, \quad P_{\mathcal{V}}(v) = 0. \tag{1}$$

Proof: The result is proven by induction. Suppose first that $\mathcal{V}$ has dimension 1, with $\mathcal{V} = \langle v_1 \rangle$, where v_1 is non-zero element of L. Then $P_{\mathcal{V}} = X^{\theta^1} - \frac{\theta(v_1)}{v_1} X^{\theta^0}$ satisfy Eq. 1. Suppose now that $\mathcal{V}$ has dimension $i+1$, with $\mathcal{V} = \langle v_1, \ldots, v_{i+1} \rangle$. The vectorspace $\mathcal{V}' = \langle v_1, \ldots, v_i \rangle$ has dimension i and

$$P_{\mathcal{V}}(X) = \left(X^{\theta^1} - \frac{\theta(P_{\mathcal{V}'}(v_{i+1}))}{P_{\mathcal{V}'}(v_{i+1})} X^{\theta^0} \right) \times P_{\mathcal{V}'}(X)$$

can be checked to satisfy Eq. 1. It is monic and has θ-degree $i+1$. Nevertheless we need to ascertain that $P_{\mathcal{V}'}(v_{i+1}) \neq 0$: Since by hypothesis the root-space of $P_{\mathcal{V}'}$ has dimension less than its degree and since v_{i+1} is not in this root-space, we get the desired result. To prove unicity, consider two monic θ-polynomials $P_{\mathcal{V}}$ and $Q_{\mathcal{V}}$ and of degree s vanishing on $\mathcal{V}$. Then $P_{\mathcal{V}} - Q_{\mathcal{V}}$ has degree less than s and admits $\mathcal{V}$ among its roots. This contradicts Th. 1. ∎

IV. Rank metric

In this section we present four definitions for the rank weight. We show that in fact they define only two different weights. We also give a condition under which these two weights are equal.

Definition 2: Let $X = (x_1, \cdots, x_N) \in L^N$. We define

$$X^\theta \stackrel{\text{def}}{=} \begin{pmatrix} x_1^{\theta^0} & \cdots & x_N^{\theta^0} \\ \vdots & \ddots & \vdots \\ x_1^{\theta^{n-1}} & \cdots & x_N^{\theta^{n-1}} \end{pmatrix},$$

and

$$X_{\mathcal{B}} \stackrel{\text{def}}{=} \begin{pmatrix} x_{1,1} & \cdots & x_{N,1} \\ \vdots & \ddots & \vdots \\ x_{1,m} & \cdots & x_{N,m} \end{pmatrix},$$

where $x_i = \sum_{j=1}^{m} x_{i,j} b_j$. We also define the left ideal

$$I_X \stackrel{\text{def}}{=} \{P \in L[X;\theta] : P(x_i) = 0,\ i = 1, \ldots, N\}.$$

The ideal I_X being a left ideal in a right Euclidian ring, it admits a right generator, denoted by $\min(I_X)$.

For any $X \in L^N$, we define the following quantities:

- $w_0(X) \stackrel{\text{def}}{=} \deg_\theta(\min(I_X))$;
- $w_1(X) \stackrel{\text{def}}{=} \text{rank}_L\left(X^\theta\right) = \text{rank}\left(X^\theta\right)$;

which are related to L-linear independance, while the following definitions are related to K-linear independance:

- $w_2(X) \stackrel{\text{def}}{=} \text{rank}_K\left(X^\theta\right)$;
- $w_3(X) \stackrel{\text{def}}{=} \text{rank}_K\left(X_{\mathcal{B}}\right) = \text{rank}\left(X_{\mathcal{B}}\right)$;

where rank_K stands for the maximum numberof K-linearly independent columns.

Proposition 3: For all $X \in L^N$, $w_0(X) = w_1(X)$.

Proof: Let us denote $w_0(X) = w_0$, $w_1(X) = w_1$. Since $\min(I_X)$ has degree w_0, then for any non zero $(c_1, \cdots, c_{w_0-1}) \in L^N$, we have

$$(c_0, \cdots, c_{w_0-1}) \cdot \begin{pmatrix} x_1^{\theta^0} & \cdots & x_N^{\theta^0} \\ \vdots & \ddots & \vdots \\ x_1^{\theta^{w_0-1}} & \cdots & x_N^{\theta^{w_0-1}} \end{pmatrix} \neq 0.$$

Thus the row rank over L of X^θ is larger than or equal to w_1. Therefore $w_0 \leq w_1$.

Writing $\min(I_X) = \sum_{k=0}^{w_0} a_i x^{\theta^i}$, we have

$$(a_0, \cdots, a_{w_0}) \cdot \begin{pmatrix} x_1^{\theta^0} & \cdots & x_N^{\theta^0} \\ \vdots & \ddots & \vdots \\ x_1^{\theta^{w_0}} & \cdots & x_N^{\theta^{w_0}} \end{pmatrix} = 0.$$

Therefore the (w_0+1)-th row of X^θ is a L-linear combination of the w first rows of X^θ. Applying θ^i, we have for all i:

$$\left(a_0^{\theta^i}, \cdots, a_w^{\theta^i}\right) \cdot \begin{pmatrix} x_1^{\theta^i} & \cdots & x_N^{\theta^i} \\ \vdots & \ddots & \vdots \\ x_1^{\theta^{w+i}} & \cdots & x_N^{\theta^{w+i}} \end{pmatrix} = 0.$$

This implies that the $(r+i)$-th row is a L-linear combination of the w_0 preceeding rows, thus of the w_0 first rows, by induction. Thus the L-rank of X^θ is less than w_0, and $w_1 \leq w_0$. ∎

Proposition 4: For all $X \in L^N$, $w_2(X) = w_3(X)$.

Proof: Let $w_3 = w_3(X) = \text{rank}_K\left(X_{\mathcal{B}}\right)$, and $w_2 = w_2(X) = \text{rank}_K\left(X^\theta\right)$. Without loss of generality, suppose that the first w_3 columns of $X_{\mathcal{B}}$ are K-linearly independent. Accordingly, consider the w_3 first columns of X^θ, and suppose that we have a dependence relation among them, i.e.

$$\sum_{i=1}^{w_3} \lambda_i x_i^{\theta^j} = 0, \quad j = 0, \ldots, n-1,$$

with $(\lambda_1, \cdots, \lambda_{w_3}) \in K^{w_3}$. Considering only $j = 0$, and rewriting $x_i = \sum_{j=1}^{m} x_{i,j} b_j$ over the basis $\mathcal{B}$, we get

$$0 = \sum_{i=1}^{w_3} \lambda_i \sum_{j=1}^{m} x_{i,j} b_j = \sum_{j=1}^{m} \left(\sum_{i=1}^{w_3} \lambda_i x_{i,j} \right) b_j.$$

Since the b_i's are a K-basis, we have, for $j = 1, \ldots, m$,

$$0 = \sum_{i=1}^{w_3} \lambda_i x_{i,j} = X_{\mathcal{B}} \cdot (\lambda_1, \cdots, \lambda_{w_3})^T.$$

By hypothesis the first w_3 columns of $X_{\mathcal{B}}$ are linearly independent, this implies $\lambda_i = 0$, $i = 1, \ldots, w_3$. So the first w_3 columns of X^θ are K-linearly independent. Therefore $w_2 \geq w_3$.

To prove that $w_2 \leq w_3$, let $(x_{i,j})_{j=1}^m$ be the i-th column of $X_{\mathcal{B}}$. Since the first w_3 columns of $X_{\mathcal{B}}$ generate the column space, we have $x_i = \sum_{k=1}^{w_3} \lambda_{iu} x_u$, $i = 1, \ldots, N$. By K-linearity of θ^j, we have

$$x_i^{\theta^j} = \sum_{u=1}^{w_3} \lambda_{iu} x_u^{\theta^j}, \quad j = 0, \ldots, n-1,$$

therefore the ith column $(x_i^{\theta^j})_{j=0}^{n-1}$ of X^θ is generated by the first w_3 columns of X^θ, and $w_2 \leq w_3$. ∎

Proposition 5: For all $X \in L^N$, $w_1(X) \leq w_2(X)$, with equality when K is the fixed subfield of L, i.e. $K = L^\theta$.

Proof: Let $X = (x_1, \cdots, x_N) \in L^N$. It is clear that a linear combination with coefficients in K is also a linear combination with coefficients in L, hence $w_1(x) \leq w_2(x)$.

Let $w_1 \stackrel{\text{def}}{=} \text{rank}_L\left(X^\theta\right)$. Noting the columns of X^θ

$$C_i = \left(x_i^{\theta^0}, \cdots, x_i^{\theta^{n-1}}\right)^T,$$

suppose that the columns $C_{i_1}, \ldots, C_{i_{w_1}}$ are L-linearly independent. Then any i-th column can be written $C_i = \sum_{j=1}^{w_1} \lambda_j C_{i_j}$, $\lambda_j \in L$. Applying θ^u, we get

$$C_i^{\theta^u} = \sum_{j=1}^{w_1} \lambda_j^{\theta^u} C_{i_j}^{\theta}, u = 1, \ldots, m,$$

which is the same as

$$C_i = \sum_{j=1}^{w_1} \lambda_j^{\theta^u} C_{i_j}, u = 1, \ldots, m,$$

since $C_i^{\theta^u}$ is a cyclic shift of C_i. By summation, we get

$$C_i = \sum_{j=1}^{w_1} \left(\sum_{u=0}^{m-1} \lambda_j^{\theta^u} \right) C_{i_j}.$$

We have

$$\left(\sum_{u=0}^{m-1} \lambda_j^{\theta^u} \right)^\theta = \sum_{u=1}^{m} \lambda_j^{\theta^u}.$$

However θ has order n which divides m. Therefore $\lambda_j^{\theta^m} = \lambda_j^{\theta^0}$, therefore $\sum_{u=0}^{m-1} \lambda_j^{\theta^u} \in K$ when $K = L^\theta$. This implies that the columns $C_{i_1}, \ldots, C_{i_{w_1}}$ K-generate the column space of X^θ: $w_2 \leq w_1$. ∎

It is easy to see that the w_i's provide distances defined by $d_i(X,Y) \stackrel{\text{def}}{=} w_i(X - Y)$. In the following, we suppose that we are in the case where all these metrics are equal, and the induced distance is called rank metric. We use the notation

$w(X)$, without indices. This definition is a generalization of rank metric as defined in Gabidulin [1].

Example 2: Here is an example of a vector whose ranks are different on K and on L. Let us consider again the field extension

$$K = \mathbb{Q} \hookrightarrow L = \mathbb{Q}[Y]/(Y^8 + 1).$$

Let α be a root of $Y^8 + 1$, such that $(1, \ldots, \alpha^7)$ is a K-basis of L. Consider again the automorphism θ defined by $\alpha \mapsto \alpha^3$. Let $x = (1, \alpha, \alpha^2, \alpha^4, \alpha^5, 3\alpha^4 + 2)$. We have that $w_0(x) = w_1(x) = 4 \leq w_2(x) = w_3(x) = 5$

V. Gabidulin codes in characteristic zero

For simplicity, we suppose in this section that the automorphism θ satisfies the following properties:

- θ generates the Galois group of $K \hookrightarrow L$, that is θ has order m;
- The characteristic polynomial of θ is square-free;
- $L^\theta = K$.

The K-vector space L^N is endowed with the rank metric defined in the previous section. In this metric space, a linear code is as usual an L-vector space of length N, dimension k and minimum rank distance d. It is denoted a $[N, k, d]_{(L,\theta)}$ code.

A. Definition

Definition 3: Let $g = (g_1, \cdots, g_N) \in L^N$, be K-linearly independent elements of L. The generalized Gabidulin code, with dimension k and length N, denoted $Gab_{\theta,k}(g)$, as a L-subspace of L^N, is L-generated by the matrix

$$G \stackrel{\text{def}}{=} \begin{pmatrix} g_1^{\theta^0} & \cdots & g_N^{\theta^0} \\ \vdots & \ddots & \vdots \\ g_1^{\theta^{k-1}} & \cdots & g_N^{\theta^{k-1}} \end{pmatrix},$$

For $k \leq N$, the dimension of $Gab_{\theta,k}(g)$ is indeed k. We can show that the parity-check matrix of $Gab_{\theta,k}(g)$ can be given by

$$H \stackrel{\text{def}}{=} \begin{pmatrix} h_1^{\theta^0} & \cdots & h_N^{\theta^0} \\ \vdots & \ddots & \vdots \\ h_1^{\theta^{d-2}} & \cdots & h_N^{\theta^{d-2}} \end{pmatrix},$$

where $d = N - k + 1$ for some $h_i \in L$ which are also K-linearly independent.

B. Maximum Rank Distance codes

Proposition 6: Let $\mathcal{C}$ be an $[N, k, d]_{(L,\theta)}$ code. We have $d \leq N - k + 1$.

Proof: Omitted due to lack of space. ∎

An optimal code satisfying the property that $d = N - k + 1$ is called a Maximum Rank Distance (MRD) code.

Theorem 3: The generalized Gabidulin $Gab_{\theta,k}(g)$ is an MRD code.

Proof: Let $C = (c_1, \cdots, c_N) \in Gab_{\theta,k}(g)$ be a non-zero codeword. By definition of generalized Gabidulin codes, there exists a θ-polynomial $P(X)$ of θ-degree $\leq k - 1$ such that

$$\forall i = 1, \ldots, N, \quad c_i = P(g_i).$$

Now, C has rank d if and only if the K-vector space generated by its components has K-dimension d. Therefore, by Th. 2, there exists a θ-polynomial of θ-degree d such that $P_C(c_i) = 0$ for all i. Hence

$$\forall i = 1, \ldots, N, \quad P_C \times P(g_i) = 0.$$

Since $< g_1, \ldots, g_N >$ has K-dimension N, since P has degree at most k, and since we are in the case where the dimension of the root-space of a θ-polynomial is at most its degree, we have $d + k - 1 \geq N$ therefore $d - 1 = N - k$. ∎

C. Unique decoding

Our version of the algorithm is inspired from Gemmel and Sudan's presentation of the algorithm of Welch-Berlekamp [2]. A more efficient variant can be used using [6], but we prefer to present here a more intuitive version. Consider a vector $Y = (y_1, \cdots, y_N) \in L^N$ such that there exists $E = (e_1, \cdots, e_N) \in L^N$ such that

$$Y = C + E, \tag{2}$$

$$C \in Gab_{\theta,k}(g), \tag{3}$$

$$\text{rank}(E) \leq (N - k)/2. \tag{4}$$

Write $t = \lfloor (N - k)/2 \rfloor$. We define the following series of problems related to this situation.

Definition 4 (Decoding): Given $Y \in L^N$, find, if it exists, a pair (f, E) such that $y_i = f(g_i) + e_i$, $i = 1, \ldots, N$; $w(E) \leq t$; $\deg_\theta(f) < k$.

Definition 5 (Nonlinear reconstruction): Given $Y \in L^N$, find, if it exists, a pair of θ-polynomials (V, f) such that $\deg_\theta(V) \leq t$; $V \neq 0$; $\deg_\theta(f) < k$; $V(y_i) = V(f(g_i))$, $i = 1, \ldots, N$.

Note that this problem gives rise to quadratic equations, considering as indeterminates the coefficients of the unknowns (V, f) over the basis $\mathcal{B}$. We thus consider a linear version of the system.

Definition 6 (Linearized reconstruction): Given $Y \in L^N$, find, if it exists, a pair of θ-polynomials (W, N) such that $\deg_\theta(W) \leq t$; $W \neq 0$; $\deg_\theta(N) < k + t$; $W(y_i) = N(g_i)$, $i = 1, \ldots, N$.

Since we require the weight of the error to be less than or equal to $t = (N - k)/2$, we have unicity of the solution for the three above problems. Now the following propositions give relations between the solutions of these problems.

Proposition 7: Any solution of *Nonlinear reconstruction* give a solution of *Decoding*.

Proof: Let (V, f) be a solution of *Nonlinear reconstruction*. We define $e_i \stackrel{\text{def}}{=} y_i - f(g_i)$. Then we have $y_i = f(g_i) + e_i$, $i = 1, \ldots, N$; $\deg_\theta(f) < k$; $w(E) \leq t$. Indeed, since the e_i's are roots of a θ-polynomial with degree at most t,we must have $\deg \min(I_E) \leq t$, thus, $w(E) \leq t$. ∎

Under an existence condition, we have the following statement.

Proposition 8: If $t \leq (N - k)/2$, and if there is a solution to *Nonlinear reconstruction*, then any solution of *Linear reconstruction* gives a solution to *Nonlinear reconstruction*.

Proof: Let (V, f) be a non zero solution of *Nonlinear reconstruction*, and let (W, N) be a solution of *Linearized reconstruction*. Letting $e_i \stackrel{\text{def}}{=} y_i - f(g_i)$, $i = 1, \ldots, N$, we have $V(e_i) = V(y_i - f(g_i)) = 0$. Thus $V \in I_E$, with $\deg V \leq t$, so $E = (e_1, \cdots, e_N)$ has rank at most t.

We also have $W(e_i) = W(y_i) - W(f(g_i))$ so $W(e_i) = N(g_i) - W(f(g_i))$. Since $W(e_i)$ has rank at most t, we can find U with degree at most t, such that $U(W(e_i)) = U(N(g_i) - W(f(g_i))) = 0$.

Then $(U \times (N - W \times f))(g_i) = 0$, $i = 1, \ldots, N$. As $t \leq (N-k)/2$, degree computations show that $U \times (N - W \times f)$ is a θ-polynomial with degree at most $N-1$. Since it is zero at N K-linearly independent values, it must be the zero polynomial: $U \times (N - W \times f) = 0$. As there is no zero divisor in $L[X; \theta]$, we conclude that $N = W \times f$. Then $(W, N) = (W, W \times f)$, and (W, f) is a solution of *Nonlinear reconstruction*. ∎

The above propositions imply that unique decoding is equivalent to solving *Linearized reconstruction*. Now we give the explicit system of equations to be solved.

Theorem 4: Solving *Linearized reconstruction* amounts to solving the following linear system of equations

$$S \cdot \begin{pmatrix} N \\ -W \end{pmatrix} = 0,$$

where

$$S \stackrel{\text{def}}{=} \begin{pmatrix} g_1^{\theta^0} & \cdots & g_1^{\theta^{k+t-1}} & y_1^{\theta^0} & \cdots & y_1^{\theta^t} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ g_N^{\theta^0} & \cdots & g_N^{\theta^{k+t-1}} & y_N^{\theta^0} & \cdots & y_N^{\theta^t} \end{pmatrix}$$

with unknowns

$$N = (n_0, \cdots, n_{k+t-1})^T \in L^{k+t}$$
$$W = (w_0, \cdots, w_t)^T \in L^{t+1}.$$

Proof: Each row of the product corresponds to the evaluation of N and W in the g_i's and in the y_i's. ∎

Remark 1: The number of arithmetic operations used in this method is easily seen to be of $O(N^3)$, using for instance Gaussian elimination for solving the linear system. However, since the system is highly structured, a better algorithm exists [6] whose complexity is $O(N^2)$.

Remark 2: Note that we only deal with the algebraic complexity, i.e. the number of elementary additions and multiplications in L. Since we may compute over infinite fields, this does not reflect the bit-complexity, which shall be studied in a longer version of the paper.

VI. Examples

We have previously seen the importance of the hypotheses about θ and what happen when they are not satisfied. Now, we will see that Kummer extensions always provide automorphisms with the good properties.

Example 3: Let us consider the Kummer extension

$$K = \mathbb{Q}[X]/(X^4 + 1) \hookrightarrow L = K[Y]/(Y^8 - 3).$$

Let h be a root of $X^4 + 1$, such that $(1, h, h^2, h^3)$ is a $\mathbb{Q}$-basis of K, and let α be a root of $Y^8 - 3$, such that $(1, \ldots, \alpha^7)$ is a K-basis of L. Consider this time the automorphism θ defined by $\alpha \mapsto h\alpha$. Its characteristic polynomial is $Y^8 - 1$, which is square-free. Thus, we can define generalized Gabidulin codes with symbols in L, of length 8, and any dimension less than or equal to 8. Besides being simply $\mathbb{Q}$-linear, these codes are also K-linear.

More generally, with Kummer extensions, we can design rank-metric $[N, k, d]$ codes, accomplishing the MRD condition $N - k = d - 1$. Below is also given a classical infinite family.

Example 4: Consider p an odd prime number, and let ζ be a primitive p-root of unity in $\mathbb{C}$. Then $\mathbb{Q} \hookrightarrow \mathbb{Q}[\zeta]$ is an extension of degree $p-1$, and its Galois group is isomorphic to $(\mathbb{Z}/pZ)^\star$, and is thus cyclic. We let $K = \mathbb{Q}$, and $L = \mathbb{Q}[\zeta]$. For any u with $\gcd(u, p-1) = 1$, consider $\theta : \zeta \mapsto \zeta^u$. Then θ has order $p-1$ and $\mathbb{Q}$ is the subfield stable under θ. Then, for $k \leq p-1$, can build $\mathbb{Q}$-codes in L^{p-1}, of dimension k over L, such that the K-rank of any codeword is at least $(p-1) - k + 1 = p - k$.

VII. Conclusion

For a θ-polynomial, we have seen the link between its degree and the dimension of its kernel. Particularly, we gave sufficient condition for the root-space dimension being at most the degree of a θ-polynomial, namely.

Then, we have seen four different ways to define notions related to the rank-metric. This reduces to only two metrics, which are furthermore the same in the case of θ having a square-free characteristic polynomial.

We have also given a generalized definition of Gabidulin codes, seen that they are MRD codes, and can be easily decoded up to half the minimum distance. Since computations are not carried over finite fields, the bit complexity will be properly evaluated in the future.

Finally, properly applying this theory to space-time coding needs further work.

References

[1] E. M. Gabidulin. Theory of codes with maximal rank distance. *Problems of Information Transmission*, 21:1–12, 1985.

[2] P. Gemmel and M. Sudan. Highly resilient correctors for polynomials. *Information Processing Letters*, 43(4):169–174, 1992.

[3] A. R. Hammons and H. El Gamal. On the theory of space-time codes for the PSK modulation. *IEEE Transactions on Information Theory*, 46(2), 2000.

[4] Serge Lang. *Algebra*. Springer, third edition, 2002.

[5] R. Lidl and H. Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, October 1996.

[6] P. Loidreau. Welch-Berlekamp like algorithm for decoding Gabidulin codes. In Ø. Ytrehus, editor, *Coding and Cryptography - WCC 2005, 4th International workshop on Coding and Cryptography*, number 3969 in Lecture Notes in Computer Science, pages 36–45. Springer, 2006.

[7] H. F. Lu and P. V. Kumar. A unified construction of space-times codes with optimal rate-diversity tradeoff. *IEEE Transactions on Information Theory*, 51(5), 2005.

[8] P. Lusina, Ernst Gabidulin, and M. Bossert. Maximum rank distance codes as space-time codes. *IEEE Transactions on Information Theory*, 49(10):2757–2760, 2003.

[9] Ö. Øre. Theory of non-commutative polynomials. *Annals of Mathematics. Second Series*, 34(3):480–508, 1932.

[10] Ö. Øre. On a special class of polynomials. *Transactions of the American Mathematical Society*, 35(3):559–584, 1933.