Generalization of Gabidulin Codes over Fields of Rational Functions

Daniel Augot

Generalization of Gabidulin Codes over Fields of Rational Functions

Daniel Augot

***Abstract*— We transpose the theory of rank metric and Gabidulin codes to the case of fields which are not finite fields. The Frobenius automorphism is replaced by any element of the Galois group of a cyclic algebraic extension of a base field. We use our framework to define Gabidulin codes over the field of rational functions using algebraic function fields with a cyclic Galois group. This gives a linear subspace of matrices whose coefficients are rational function, such that the rank of each of this matrix is lower bounded, where the rank is comprised in term of linear combination with rational functions. We provide two examples based on Kummer and Artin-Schreier extensions.The matrices that we obtain may be interpreted as generating matrices of convolutional codes.**

I. Introduction

Gabidulin codes are rank-metric codes defined over finite fields using so-called linearized polynomials [1]. They can be seen as analogues of Reed-Solomon codes, where polynomials are replaced by linearized polynomials, and the Hamming distance is replaced by the rank distance. For Gabidulin codes, the Frobenius automorphism $x \mapsto x^q$ plays a fundamental role. In [2], the authors generalized this construction to fields of characteristic zero, where the Frobenius automorphism does not exists, by considering extensions of number fields L/K, and using a Galois automorphism θ as the Frobenius automorphism, and replacing linearized polynomials by so-called skew polynomials or θ-polynomials. The theory of Gabidulin transposes nicely, and Maximum Rank Distance (MRD) codes can be built, with a decoding algorithm (for the rank distance) transposed from a simple decoding of Reed-Solomon codes.

In this paper, we use the general abstract framework of [2] in the case of the base field being the field of rational functions (over a finite field). First we briefly recall facts from [2], in the case of a cyclic Galois extension whose Galois group is generated by θ: θ-polynomials, rank metric, decoding. We give a construction with Kummer extensions, a more precise example over the ground field $\mathbb{F}_8$, and another example with an Artin-Schreier extension over $\mathbb{F}_5$.

II. θ-polynomials

In all the paper, we consider an algebraic field extension $K \hookrightarrow L$ with finite degree n, and an automorphism θ in the Galois group $\mathrm{Gal}(K \hookrightarrow L)$, of order $n = \mathrm{Gal}(K \hookrightarrow L)$. Given $x \in L$, we use the notation x^{θ^i} for $\theta^i(x)$. In the finite field case, when θ is the Frobenius automorphism $x \mapsto x^q$, $x^{\theta^i} = x^{q^i}$, and the similarity is nicely reflected in this notation. We define *θ-polynomials*, which are a special case of *skew polynomials*, namely, when there is no derivation.

[1] INRIA & LIX UMR 7161 X-CNRS, Bâtiment Alan Turing, Campus de l'École polytechnique, 91120 Palaiseau CEDEX, France

Definition 1: A θ-polynomial is a finite summation of the form $\sum_{i\geq 0} p_i Z^{\theta^i}$, 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 $L[Z;\theta]$. This is a L-vector space, which is also a non commutative algebra, using the skew product:

$$\left(\sum p_i Z^{\theta^i}\right) \cdot \left(\sum p_j Z^{\theta^j}\right) = \sum_{i,j} p_i \, {q_j}^{\theta^i} Z^{\theta^{i+j}}.$$

An evaluation map can also be defined, for $P \in L[Z;\theta]$, and $g \in L$:

$$\mathrm{ev}(P, g) = P(g) = \sum p_i g^{\theta^i}.$$

The following is well known.

Proposition 1 ([3]): The set of θ-polynomials $(L[Z;\theta], +, \cdot)$ is a non-commutative integral domain, with unity $Z^{\theta^0} = Z$. It is also a left and right Euclidean ring.

We define the root-space of a θ-polynomial $P(Z)$ to be the set of $x \in L$ such that $P(x) = 0$. Then we have:

Theorem 1: The dimension of the root-space of a θ-polynomial is less than or equal to its θ-degree.

Theorem 2: Let V be an s-dimensional K-subspace of L. Then there exists a unique monic θ-polynomial P_V with θ-degree s such that

$$P_V(x) = 0 \quad \text{for all } x \in V.$$

See [2] for proofs of these two Theorems.

III. Rank Metric and θ-codes

In this section we recall the definition of the rank weight. All the proofs are to be found in [2]. The codes we are going to define have codewords $c \in L^n$. We note $B = (b_1, \ldots, b_m)$ a fixed K-basis of L. Let $c = (c_1, \cdots, c_n) \in L^n$. We define

$$M_c \stackrel{\text{def}}{=} \begin{pmatrix} c_{1,1} & \cdots & c_{n,1} \\ \vdots & \ddots & \vdots \\ c_{1,n} & \cdots & c_{n,n} \end{pmatrix},$$

where $c_i = \sum_{j=1}^n c_{i,j} b_j$. We then define the rank weight which is related to K-linear independence:

Definition 2: The *rank weight* is defined by

$$w(c) \stackrel{\text{def}}{=} \mathrm{rank}_K\left(c_B\right), \quad \text{for all } c \in L^n.$$

It is easy to see that the w provides a distance defined by $d(c_1, c_2) \stackrel{\text{def}}{=} w(c_1 - c_2)$. This definition is a generalization of rank metric as defined in Gabidulin [1]. In [2], we provided four equivalent definitions of the rank metric, a convenient

one being $w(c) \stackrel{\text{def}}{=} \deg_\theta(\min(I_c))$, where $\min(I_c)$ is the right generator of the ideal

$$I_c = \{P \in L[Z;\theta] : P(c_i) = 0,\ i = 1, \ldots, n\}.$$

We also define the generalization of Gabidulin codes.

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 $\mathrm{Gab}_{\theta,k}(g)$, as a L-subspace of L^N, is L-generated by the matrix

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

Using the evaluation map:

$$\begin{array}{rccl} \mathrm{ev}_g : & L[Z;\theta] & \to & L^n \\ & P(Z) & \mapsto & \mathrm{ev}_g(P) = (P(g_1), \cdots, P(g_n)) \end{array}$$

we may also define the code as an evaluation code:

$$\mathrm{Gab}_{\theta,k}(g) = \{\mathrm{ev}_g(P) :\ P \in L[Z;\theta],\ \deg_\theta P < k\}.$$

For $k \leq n$, the dimension of $\mathrm{Gab}_{\theta,k}(g)$ is indeed k.

Proposition 2 (Singleton bound): Let C be any $[n,k,d]_L$ code for the rank distance. Then $d \leq n - k + 1$.

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

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

We also briefly recall how to decode these codes. Actually, any decoding algorithm of Gabidulin codes may be transformed in a decoding algorithm for our codes, using θ in place of the Frobenius map: $x \mapsto x^q$. We present a high level view of the decoding algorithm, inspired from Gemmel and Sudan's presentation of the algorithm of Welch-Berlekamp [4], but relevant faster algorithms can be found in [5] or more recently in [6].

Consider a vector $y = (y_1, \cdots, y_n) \in L^n$ such that there exists $e = (e_1, \cdots, e_n),\ c = (c_1, \cdots, c_n) \in L^n$ such that

$$\begin{aligned} y &= c + e, \\ c &\in \mathrm{Gab}_{\theta,k}(g), \\ w(e) &\leq \lfloor (n-k)/2 \rfloor. \end{aligned}$$

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 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 $\deg_\theta(W) \leq t$; $W \neq 0$; $\deg_\theta(N) < k+t$; $W(y_i) = N(g_i)$, $i = 1, \ldots, n$.

When we have unique decoding, i.e. when the weight of the error e is less than or equal to $\lfloor (n-k)/2 \rfloor$, we have the following relations between the solutions of these problems.

Proposition 3: 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*. The solution f can be found by dividing N by W.

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 [5] whose complexity is $O(n^2)$. This does not reflect the bit-complexity, only the arithmetic complexity.

IV. Kummer extensions of function fields

We now use the previous theory when the field K is a function field on one variable, the simplest case being $K = k(x)$ the field of rational functions over a base field k. We need to build cyclic extensions of $k(x)$. An standard way of constructing a cyclic extension is to consider a Kummer extension. The ground field is the field of rational functions, which then extended by adding a n-th root of some element $u \in k(x)$.

We refer the reader to Stichtenoth's book [7] for the theory of algebraic function fields.

For simplicity, we consider the finite field case, when $k = \mathbb{F}_q$, for some prime power q, and k is containing an n-root of unity α, for n dividing $q-1$. Note that we can also deal with fields of characteristic zero like $\mathbb{Q}$, but we may have to extend them by adjoining n-th roots of unity, see [2]. Then $K = k(x)$ is the field of rational functions, and for $u \in K$ such $u \neq w^d$, for all $d|n$ and $w \in K$, we can build the field $L = K[y]$, where y is a root of $Y^n - u = 0$. Then L is a cyclic extension of K of degree n, with basis

$$B = g = \left(1, y, \ldots, y^{n-1}\right)$$

and whose Galois group is generated by $\theta : y \mapsto \alpha y$. We can use the previous general framework for building a θ-code $\mathrm{Gab}_{\theta,k}(g)$ for all $1 \leq k \leq n$. A generating matrix is

$$G \stackrel{\text{def}}{=} \begin{pmatrix} (1)^{\theta^0} & \cdots & \left(y^{n-1}\right)^{\theta^0} \\ \vdots & \ddots & \vdots \\ (1)^{\theta^{k-1}} & \cdots & \left(y^{n-1}\right)^{\theta^{k-1}} \end{pmatrix}.$$

Then, this matrix defines an MRD code over L. Its codewords are of the form $c = (c_1, \ldots, c_n) = (m_1, \ldots, m_k) \cdot G$, $c_i, m_i \in L$. Using the basis $B = \left(1, y, \ldots, y^{n-1}\right)$, a codeword can be seen as a matrix

$$M_c = \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \cdots & c_{nn} \end{pmatrix}$$

where the c_{ij}'s are $K = \mathbb{F}_q(x)$. The construction implies that for any codeword $\mathrm{rank}\, M_c \geq n - k + 1$, where is the rank is understood in terms of $\mathbb{F}_q(X)$-linear combinations.

$$m^T = \begin{pmatrix} \frac{\beta^3x+\beta^{10}}{x+\beta^5}y^4 + \frac{\beta^5x+\beta^2}{x+\beta^4}y^3 + \frac{\beta^6x+\beta^{13}}{x+\beta^3}y^2 + \frac{\beta^{10}x+\beta^6}{x+\beta^9}y + \frac{\beta x+\beta^{12}}{x+1} \\ \frac{\beta^9x+\beta^{14}}{x+\beta^6}y^4 + \frac{\beta^6x+\beta}{x+\beta^4}y^3 + \frac{\beta^{14}x+\beta^{13}}{x+\beta^3}y^2 + \frac{\beta^8x+\beta^7}{x+\beta^{12}}y + \frac{\beta^{11}x+\beta^{11}}{x+\beta} \\ \frac{\beta^4x+\beta^{11}}{x+\beta^5}y^4 + \frac{\beta^6x+\beta^{10}}{x+\beta^{11}}y^3 + \frac{\beta^5x+\beta^{11}}{x}y^2 + \frac{\beta^8x+\beta^6}{x+\beta^7}y + \frac{\beta x+\beta^{12}}{x+\beta^6} \end{pmatrix} \tag{1}$$

$$c^T = \begin{pmatrix} \frac{x^2+\beta^2x+\beta^8}{x^2+\beta^9x+\beta^{11}}y^4 + \frac{\beta^5x^2+\beta^7}{x^2+\beta^{13}x+1}y^3 + \frac{\beta^4x^2+\beta^7x+\beta^{14}}{x^2+\beta^3x}y^2 + \frac{\beta^{10}x^3+\beta^4x^2+\beta^{13}x+\beta^{13}}{x^3+\beta^{11}x^2+\beta^{13}x+\beta^{13}}y + \frac{\beta^{11}x^3+\beta^{13}x^2+\beta^3x+\beta^9}{x^3+\beta^{12}x^2+\beta^8x+\beta^7} \\ \frac{\beta^4x+\beta^5}{x+\beta^{11}}y^4 + \frac{\beta^5x^2+\beta x+\beta^5}{x^2+\beta^3x}y^3 + \frac{\beta^{11}x^2+\beta^2x+1}{x^3+\beta^{11}x^2+\beta^{13}x+\beta^{13}}y^2 + \frac{\beta^{10}x+\beta^5}{x^3+\beta^{12}x^2+\beta^8x+\beta^7}y + \frac{\beta^7x^2+\beta^6x}{x^2+\beta^9x+\beta^{11}} \\ \frac{\beta^{11}x^2+\beta^{13}x+\beta^{11}}{x^2+\beta^3x}y^4 + \frac{\beta^3x^3+\beta x^2+\beta^2}{x^3+\beta^{11}x^2+\beta^{13}x+\beta^{13}}y^3 + \frac{\beta^7x^3+\beta^7x^2+1}{x^3+\beta^{12}x^2+\beta^8x+\beta^7}y^2 + \frac{\beta^7x^3+\beta^4x^2+\beta^6x}{x^2+\beta^9x+\beta^{11}}y + \frac{x^3+\beta^3x^2+\beta^7x}{x^2+\beta^{13}x+1} \\ \frac{\beta^{13}x^3+\beta^6x^2+\beta^5x+\beta}{x^3+\beta^{11}x^2+\beta^{13}x+\beta^{13}}y^4 + \frac{\beta^{10}x^3+\beta^9x^2+\beta^4x+\beta^{12}}{x^3+\beta^{12}x^2+\beta^8x+\beta^7}y^3 + \frac{\beta^7x^3+\beta^{14}x^2+\beta^{14}x}{x^2+\beta^9x+\beta^{11}}y^2 + \frac{\beta^{13}x^3+\beta^{12}x^2+\beta^8x}{x^2+\beta^{13}x+1}y + \frac{\beta^6x^2+x+\beta^2}{x+\beta^3} \\ \frac{\beta^6x^2+\beta^6x+1}{x^3+\beta^{12}x^2+\beta^8x+\beta^7}y^4 + \frac{\beta^{14}x^3+\beta^3x^2+\beta^{11}x}{x^2+\beta^9x+\beta^{11}}y^3 + \frac{\beta^{12}x^3+\beta x^2+\beta x}{x^2+\beta^{13}x+1}y^2 + \frac{\beta^7x^2+\beta^3x+\beta^8}{x+\beta^3}y + \frac{\beta^8x^4+\beta^4x^2+\beta^{13}x}{x^3+\beta^{11}x^2+\beta^{13}x+\beta^{13}} \end{pmatrix} \tag{2}$$

$$M_c = \begin{pmatrix} \frac{\beta^{11}x^3+\beta^{13}x^2+\beta^3x+\beta^9}{x^3+\beta^{12}x^2+\beta^8x+\beta^7} & \frac{\beta^{10}x^3+\beta^4x^2+\beta^{13}x+\beta^{13}}{x^3+\beta^{11}x^2+\beta^{13}x+\beta^{13}} & \frac{\beta^4x^2+\beta^7x+\beta^{14}}{x^2+\beta^3x} & \frac{\beta^5x^2+\beta^7}{x^2+\beta^{13}x+1} & \frac{x^2+\beta^2x+\beta^8}{x^2+\beta^9x+\beta^{11}} \\ \frac{\beta^7x^2+\beta^6x}{x^2+\beta^9x+\beta^{11}} & \frac{\beta^{10}x+\beta^5}{x^3+\beta^{12}x^2+\beta^8x+\beta^7} & \frac{\beta^{11}x^2+\beta^2x+1}{x^3+\beta^{11}x^2+\beta^{13}x+\beta^{13}} & \frac{\beta^5x^2+\beta x+\beta^5}{x^2+\beta^3x} & \frac{\beta^4x+\beta^5}{x+\beta^{11}} \\ \frac{x^3+\beta^3x^2+\beta^7x}{x^2+\beta^{13}x+1} & \frac{\beta^7x^3+\beta^4x^2+\beta^6x}{x^2+\beta^9x+\beta^{11}} & \frac{\beta^7x^3+\beta^7x^2+1}{x^3+\beta^{12}x^2+\beta^8x+\beta^7} & \frac{\beta^3x^3+\beta x^2+\beta^2}{x^3+\beta^{11}x^2+\beta^{13}x+\beta^{13}} & \frac{\beta^{11}x^2+\beta^{13}x+\beta^{11}}{x^2+\beta^3x} \\ \frac{\beta^6x^2+x+\beta^2}{x+\beta^3} & \frac{\beta^{13}x^3+\beta^{12}x^2+\beta^8x}{x^2+\beta^{13}x+1} & \frac{\beta^7x^3+\beta^{14}x^2+\beta^{14}x}{x^2+\beta^9x+\beta^{11}} & \frac{\beta^{10}x^3+\beta^9x^2+\beta^4x+\beta^{12}}{x^3+\beta^{12}x^2+\beta^8x+\beta^7} & \frac{\beta^{13}x^3+\beta^6x^2+\beta^5x+\beta}{x^3+\beta^{11}x^2+\beta^{13}x+\beta^{13}} \\ \frac{\beta^8x^4+\beta^4x^2+\beta^{13}x}{x^3+\beta^{11}x^2+\beta^{13}x+\beta^{13}} & \frac{\beta^7x^2+\beta^3x+\beta^8}{x+\beta^3} & \frac{\beta^{12}x^2+\beta x}{x^2+\beta^{13}x+1} & \frac{\beta^{14}x^3+\beta^3x^2+\beta^{11}x}{x^2+\beta^9x+\beta^{11}} & \frac{\beta^6x^2+\beta^6x+1}{x^3+\beta^{12}x^2+\beta^8x+\beta^7} \end{pmatrix} \tag{3}$$

V. A worked out example

We set $k = \mathbb{F}_{16} = \mathbb{F}_2[\beta]$, with $\beta^4 + \beta + 1 = 0$, and we set $\alpha = \beta^3$, which is a primitive 5-th root of unity. Then, a Kummer extension is constructed by adjoining to $K = \mathbb{F}_{16}(x)$, y a root of $Y^5 - x$, which is an irreducible polynomial, to build $L = K[y]$. The Galois group $\mathrm{Gal}(L \hookrightarrow K)$ has order 5, with generator $\theta : y \mapsto \alpha y$. The matrix of the conjugates of the basis is given by:

$$\begin{pmatrix} 1 & y & y^2 & y^3 & y^4 \\ 1 & \beta^3 y & \beta^6 y^2 & \beta^9 y^3 & \beta^{12} y^4 \\ 1 & \beta^6 y & \beta^{12} y^2 & \beta^3 y^3 & \beta^9 y^4 \\ 1 & \beta^9 y & \beta^3 y^2 & \beta^{12} y^3 & \beta^6 y^4 \\ 1 & \beta^{12} y & \beta^9 y^2 & \beta^6 y^3 & \beta^3 y^4 \end{pmatrix}$$

Picking the first three rows gives a generating matrix for a 3 dimensional θ-code:

$$G = \begin{pmatrix} 1 & y & y^2 & y^3 & y^4 \\ 1 & \beta^3 y & \beta^6 y^2 & \beta^9 y^3 & \beta^{12} y^4 \\ 1 & \beta^6 y & \beta^{12} y^2 & \beta^3 y^3 & \beta^9 y^4 \end{pmatrix}$$

We give in Eqs. 1, 2, 3 an example of a codeword. A message $m \in L^3$ is shown (in transpose form) in Eq. 1, then $c = m \cdot G \in L^5$ is computed, as shown in Eq. 2. We can expand c in the basis $1, y, \ldots, y^4$ to obtain the matrix M_c, (Eq. 3).

Note that we obtain matrices with (unbounded) coefficients in $K = \mathbb{F}_{16}[x]$, where the function field construction with the Kummer extension may be discarded.

VI. Artin-Schreier case

For completeness, we describe the Artin-Schreier situation, which is particular to the positive characteristic case. The theory of such extensions is also described in [7]. Assume that k has characteristic p, and consider $K = k(x)$, with an element $u \in K$ such that

$$u \neq w^p - w \text{ for all } w \in K.$$

Then the extension $L = K[y]$, where y is a root of $Y^p - Y = w$ is an Artin-Schreier extension. Its Galois group is cyclic of order p, whose generator θ is defined by $\theta(y) = y + 1$. Consider as an example $k = \mathbb{F}_5$, $K = k(x)$, and $L = K[y]$, with $y^5 - y = x$. Then $\theta(y) = y + 1$, and we can build a $[5, 3, 3]_L$ code with generating matrix G given in Eq. 4. We give in Eqs. 5, 6, 7 an example of a codeword.

VII. Polynomial matrices

We briefly mention that in both constructions the basis are integral bases of $L/K = L/k(x)$. The generating matrices G consist of integral elements. In that case, we can choose our messages $m \in k[x, y]$ instead of $k(x)[y]$, and the corresponding codewords will also belong to $k[x, y]$. When the codewords are expanded as matrices, we find $n \times n$ matrices with polynomial coefficients.

VIII. Conclusion

We have generalized Gabidulin codes to the field of rational functional, using cyclic extensions L of $k(x)$, for instance Kummer extensions, or Artin-Schreier extensions. We can easily find generating matrices for codes with symbols in L. These codewords, when expanded over $k(x)$ give naturally matrices which have high rank, where the rank has to understood by considering $k(x)$ linear combinations of the rows of the matrix. When the Gabidulin code has dimension k, each of these matrices has $k(x)$-rank at least $n - k + 1$, since the codes are Maximum Rank Distance. Given such a matrix, when its weight, i.e. its rank, is w, its gives rise to a rate w/n convolutional codes, using the language of rational fractions as in [8], replacing x with D, the delay operator. We did not consider the framework of Laurent series as in [9], but we think we can adapt the general theory to this field.

$$G = \begin{pmatrix} 1 & y & y^2 & y^3 & y^4 \\ 1 & y+1 & y^2+2y+1 & y^3+3y^2+3y+1 & y^4+4y^3+y^2+4y+1 \\ 1 & y+2 & y^2+4y+4 & y^3+y^2+2y+3 & y^4+3y^3+4y^2+2y+1 \end{pmatrix} \tag{4}$$

$$m = \begin{pmatrix} \frac{x+1}{x+3}y^4 + \frac{1}{x}y^3 + (4x+4)y^2 + \frac{x+2}{x}y + \frac{4x+1}{x}, \\ (3x+2)y^4 + \frac{4x+3}{x}y^3 + \frac{1}{x+2}y^2 + (2x+1)y + 1, \\ \frac{2}{x+1}y^4 + \frac{4x+4}{x+2}y^3 + 4y^2 + y + \frac{3}{x+1} \end{pmatrix} \tag{5}$$

$$c^T = \begin{pmatrix} \frac{3x^3+x+3}{x^2+4x+3}y^4 + \frac{3x^2+x+3}{x^2+2x}y^3 + \frac{4x^2+x+2}{x+2}y^2 + \frac{2x^2+3x+2}{x}y + \frac{4x+1}{x^2+x} \\ \frac{3x^4+4x^3+x+3}{x^3+3x^2+2x}y^4 + \frac{4x^3+3x^2+x+1}{x^2+2x}y^3 + \frac{2x^3+4}{x^2+2x}y^2 + \frac{x^2+2x+3}{x^2+3x}y + \frac{3x^4+2x^2+3x+1}{x^2+4x+3} \\ \frac{2x^3+x^2+3x+1}{x^2+x}y^4 + \frac{2x^2+3x+4}{x+2}y^3 + \frac{2x^4+2x^2+4x+1}{x^3+x}y^2 + \frac{3x^6+4x^5+3x^4+2x^3+x^2+x+4}{x^4+x^3+x^2+x}y + \frac{x^4+2x^2+3x+4}{x^2+3x+2} \\ \frac{4x^2+x+1}{x^2+x}y^4 + \frac{4x^4+x^3+2x^2+4}{x^3+x}y^3 + \frac{3x^6+x^5+2x^2+4x+4}{x^4+x^3+x^2+x}y^2 + \frac{4x^4+3x^3+3x^2+x+4}{x^2+x}y + \frac{3x^3+x^2+x+3}{x+2} \\ \frac{4x^5+x^4+2x^3+2x+3}{x^4+x^3+x^2+x}y^4 + \frac{3x^6+x^4+3x^3+2x^2+x+2}{x^4+x^3+x^2+x}y^3 + \frac{2x^5+2x^4+2x^3+x^2+2x+4}{x^3+3x^2+2x}y^2 + \frac{2x^3+x^2+2x}{x+1}y + \frac{4x^4+3x+3}{x^2+3x+2} \end{pmatrix} \tag{6}$$

$$M_c = \begin{pmatrix} \frac{4x+1}{x^2+x} & \frac{2x^2+3x+2}{x} & \frac{4x^2+x+2}{x+2} & \frac{3x^2+x+3}{x^2+2x} & \frac{3x^3+x+3}{x^2+4x+3} \\ \frac{3x^4+2x^2+3x+1}{x^2+4x+3} & \frac{x^2+2x+3}{x^2+3x} & \frac{2x^3+4}{x^2+2x} & \frac{4x^3+3x^2+x+1}{x^2+2x} & \frac{3x^4+4x^3+x+3}{x^3+3x^2+2x} \\ \frac{x^4+2x^2+3x+4}{x^2+3x+2} & \frac{3x^6+4x^5+3x^4+2x^3+x^2+x+4}{x^4+x^3+x^2+x} & \frac{2x^4+2x^2+4x+1}{x^3+x} & \frac{2x^2+3x+4}{x+2} & \frac{2x^3+x^2+3x+1}{x^2+x} \\ \frac{3x^3+x^2+x+3}{x+2} & \frac{4x^4+3x^3+3x^2+x+4}{x^2+x} & \frac{3x^6+x^5+2x^2+4x+4}{x^4+x^3+x^2+x} & \frac{4x^4+x^3+2x^2+4}{x^3+x} & \frac{4x^2+x+1}{x^2+x} \\ \frac{4x^4+3x+3}{x^2+3x+2} & \frac{2x^3+x^2+2x}{x+1} & \frac{2x^5+2x^4+2x^3+x^2+2x+4}{x^3+3x^2+2x} & \frac{3x^6+x^4+3x^3+2x^2+x+2}{x^4+x^3+x^2+x} & \frac{4x^5+x^4+2x^3+2x+3}{x^4+x^3+x^2+x} \end{pmatrix} \tag{7}$$

IX. Acknowledgments

We are thankful to V. Sidorenko for suggesting us to expand the framework of [2] to the context of rational function fields. We also thank Hans-Andrea Loeliger, Emina Soljanin, and Judy L. Walker, the organizers of the Dagstuhl "Coding Theory" Seminar, 25–30 August 2013, for providing a nice atmosphere for discussing these topics.

References

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

[2] D. Augot, P. Loidreau, and G. Robert, "Rank metric and Gabidulin codes in characteristic zero," in *Proceedings of the 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, July 7-12, 2013*. IEEE, 2013, pp. 509–513.

[3] Ö. Øre, "Theory of non-commutative polynomials," *Annals of Mathematics. Second Series*, vol. 34, no. 3, pp. 480–508, 1932.

[4] P. Gemmel and M. Sudan, "Highly resilient correctors for polynomials," *Information Processing Letters*, vol. 43, no. 4, pp. 169–174, 1992.

[5] P. Loidreau, "Welch-Berlekamp like algorithm for decoding Gabidulin codes," in *Coding and Cryptography - WCC 2005, 4th International workshop on Coding and Cryptography*, ser. Lecture Notes in Computer Science, Ø. Ytrehus, Ed., no. 3969. Springer, 2006, pp. 36–45.

[6] A. Wachter-Zeh, V. Afanassiev, and V. Sidorenko, "Fast decoding of Gabidulin codes," *Designs, Codes and Cryptography*, vol. 66, no. 1-3, pp. 57–73, 2013.

[7] H. Stichtenoth, *Algebraic Function Fields and Codes*. Berlin-Heidelberg-New York: Springer, 1993.

[8] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003.

[9] R. Roth, *Introduction to Coding Theory*. Cambridge University Press, 2006.