Fast Root Finding for Interpolation-Based Decoding of Interleaved Gabidulin Codes

Hannes Bartz[1], Thomas Jerkovits[1,2], Sven Puchinger[2], Johan Rosenkilde[3]
[1]Institute of Communications and Navigation, German Aerospace Center (DLR), Germany
[2]Institute for Communications Engineering, Technical University of Munich (TUM), Germany
[3]Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Denmark

***Abstract*—We show that the root-finding step in interpolation-based decoding of interleaved Gabidulin codes can be solved by finding a so-called minimal approximant basis of a matrix over a linearized polynomial ring. Based on existing fast algorithms for computing such bases over ordinary polynomial rings, we develop fast algorithms for computing them over linearized polynomials. As a result, root finding costs $O^{\sim}(\ell^{\omega}\mathcal{M}(n))$ operations in $\mathbb{F}_{q^m}$, where ℓ is the interleaving degree, n the code length, $\mathbb{F}_{q^m}$ the base field of the code, $2 \leq \omega \leq 3$ the matrix multiplication exponent, and $\mathcal{M}(n) \in O(n^{1.635})$ is the complexity of multiplying two linearized polynomials of degree at most n. This is an asymptotic improvement upon the previously fastest algorithm of complexity $O(\ell^3 n^2)$, in some cases $O(\ell^2 n^2)$.**

***Index Terms*—Interleaved Gabidulin Codes, Interpolation-Based Decoding, Order Bases, Rank-Metric Codes, Root Finding**

I. Introduction

Rank-metric codes are sets of matrices whose pairwise distance is measured by the rank of their difference. These codes as well as the important subclass of Gabidulin codes were independently introduced in [1], [2], [3] and have found many applications, such as criss-cross error correction in memory chips, code-based cryptography, space-time codes for MIMO systems, network coding, low-rank matrix recovery, distributed storage systems, and digital watermarking.

In some of these applications it is possible to significantly increase the decoding radius of the decoder by considering (ℓ-)interleaved Gabidulin codes, which are direct sums of ℓ Gabidulin codes of the same length n and errors are assumed to occur in certain patterns. There are several known decoding algorithms for interleaved Gabidulin codes that all correct up to $\frac{\ell}{\ell+1}(n-\overline{k})$ errors, where $\overline{k} := \frac{1}{\ell}\sum_i k_i$ is the mean of the dimensions k_i of the constituent Gabidulin codes.

The first such decoder is due to Loidreau and Overbeck [4]. It is a partial unique decoder, which means that it either returns a unique codeword or a decoding failure for some errors beyond half the minimum distance. For random errors, [4] provides an upper bound on the failure probability of the decoder. The decoder is based on solving a linear system of equations and has complexity $O(n^3)$ in operations over $\mathbb{F}_{q^m}$.

A second decoder for interleaved Gabidulin codes was proposed by Sidorenko and Bossert [5] and is a syndrome-based partial unique decoder. The main computational task is to solve a key equation, which can be done in complexity $O(\ell n^2)$ using the Berlekamp–Massey-like algorithm proposed in [6] or the demand-driven row reduction algorithm in [7]. There are also algorithms asymptotically faster in the code length n, e.g., the divide & conquer variant of the Berlekamp–Massey-like algorithm in [8] or the Alekhnovich-like algorithm in [9]. Both algorithms have complexity $O^{\sim}(\ell^3\mathcal{M}(n))$, where $O^{\sim}$ neglects logarithmic factors and $\mathcal{M}(n)$ is the complexity of multiplying two linearized polynomials. The best-known cost bounds on $\mathcal{M}(n)$, for $n \leq m$, are $O(n^{\omega-2}m^2)$ [10] over $\mathbb{F}_q$ and $O(n^{\min\{\frac{\omega+1}{2}, 1.635\}})$ over $\mathbb{F}_{q^m}$ [11].

This work was supported by the German Israeli Project Cooperation (DIP) grant no. KR3517/9-1.

Wachter-Zeh and Zeh introduced an interpolation-based decoding algorithm for interleaved Gabidulin codes in [12]. The algorithm can be interpreted in two ways: as a partial unique or a list decoder with exponential worst-case but small average-case list size. The latter interpretation is an advantage over the other known decoders. As any other interpolation-based decoder, the algorithm consists of two steps: The *interpolation step* can be implemented with complexity $O(\ell^2 n^2)$ over $\mathbb{F}_{q^m}$ using the algorithm in [13] or with $O^{\sim}(\ell^3\mathcal{M}(\ell n))$ using the Alekhnovich-like algorithm in [9] (see also [14] for more details). The current bottleneck of the decoder (in asymptotic dependence on n) is the *root-finding* step, for which there exist two algorithms: the method in [13] computes an affine basis of the root space in $O(\ell^3 n^2)$ over $\mathbb{F}_{q^m}$ and the one in [15], [16] has complexity $O(\ell^2 n^2)$. The latter algorithm works only if there is a unique solution, which is a limitation.

In this paper we present a fast root-finding algorithm based on a computer-algebraic tool called minimal approximant bases. For $\mathbb{F}_{q^m}[x]$-matrices, also known as order basis or σ-basis, it is a powerful tool that evolved in the 1990's for solving generalizations of Padé approximations, with [17] introducing the iterative M-basis algorithm, with a complexity $O(\ell^3 n^2)$ on an $\ell \times \ell$ matrix of degree n. The PM-basis algorithm of [18] applies divide & conquer methods for reaching a cost of $O^{\sim}(\ell^{\omega}\mathcal{M}(n))$. These compute *row-reduced* matrices, a form of polynomial matrix introduced much earlier in control theory, see e.g. [19]. Row-reduced matrices possess two key properties: the predictable degree property, and the shifted-degree multiplicative property, see Lemmas 1 and 2. The former states that a row-reduced matrix consists of columns which are minimal in the column space of that matrix. The latter implies that the product of two such matrices is again a row-reduced matrix, which is key to the PM-basis algorithm. In the 2010's, minimal approximant bases for non-square matrices were generalized [20], [21].

The weak Popov form [22] is a slightly stronger form compared to the row-reduced form and is applied to coding theory in e.g. [23], [7], [9]. Neiger introduced the ordered weak Popov form in [24] for a few additional properties. An even stronger form is the Popov form [25] which is canonical for a given column space but considerably more involved to compute efficiently, see [24], [26]. In this work we use the ordered weak Popov form as well as the notation set out by [21], [24]. Linearized polynomial rings $\mathbb{L}_{q^m}[x]$ are isomorphic to special skew polynomial or Ore rings [27]. Ore rings over infinite rings such as $\mathbb{Q}(t)$ have interest in time-dependent

systems and differential equations, and since the late 1990s' the computer algebra community has developed algorithms for minimal approximants and row reductions of matrices over Ore rings, see e.g. [28], [29] and references therein, but with a focus on handling the coefficient growth of infinite rings. For the finite case, in particular $\mathbb{L}_{q^m}[x]$, faster methods are available, e.g. [7], [9]. This paper continues that line of work by observing that the fast PM-basis algorithm carries over to the Ore ring case, though we only consider $\mathbb{L}_{q^m}[x]$.

The adaption of such algorithms to the Ore case, or $\mathbb{L}_{q^m}[x]$, as made in [7], [9] and the present paper quite straightforward: minor amendments are necessary to accommodate the non-commutativity of the ring, but the bulk of the definitions and arguments carry over. The main contribution of this work is therefore the *observation* that these notions carry over and that they apply well to the coding theoretic applications.

II. Preliminaries

A. Linearized Polynomials

Let $\mathbb{F}_{q^m}/\mathbb{F}_q$ be a field extension. Linearized polynomials [30] over $\mathbb{F}_{q^m}$ are polynomials of the form

$$g = \sum_{i=0}^{d} g_i x^{q^i} = \sum_{i=0}^{d} g_i x^{[i]},$$

where $d \in \mathbb{Z}_{\geq 0}$, $g_i \in \mathbb{F}_{q^m}$, and we write $[i] := q^i$. The degree (sometimes called q-degree) of a linearized polynomial is defined as $\deg g := \max\{i : g_i \neq 0\}$ if $f \neq 0$ and $\deg f := -\infty$ otherwise. Using ordinary addition and composition of polynomials as multiplication, the polynomials form a non-commutative domain denoted by $\mathbb{L}_{q^m}[x]$. Furthermore, the ring is left and right Euclidean, i.e., there is a left and right division algorithm. We say that two linearized polynomials $a, b \in \mathbb{L}_{q^m}[x]$ are congruent left-modulo $c \in \mathbb{L}_{q^m}[x]$, written $a \equiv b \bmod_{\mathrm{l}} c$ if $a - b$ is divisible by c from the left, i.e. $a - b = cd$ for some $d \in \mathbb{L}_{q^m}[x]$.

B. Modules and Matrices over Linearized Polynomial Rings

In the following, we consider free right modules, vectors, and matrices over linearized polynomial rings. We use a similar notation as in [24], where all discussed notions were introduced over ordinary polynomial rings.

For a matrix $\boldsymbol{V} \in \mathbb{L}_{q^m}[x]^{a \times b}$ and $\boldsymbol{s} \in \mathbb{Z}^a$, we define the $\boldsymbol{s}$-shifted column degree of $\boldsymbol{V}$ to be the vector

$$\operatorname{cdeg}_{\boldsymbol{s}}(\boldsymbol{V}) = [d_1, \ldots, d_b] \in (\mathbb{Z} \cup \{-\infty\})^b$$

where d_j is the maximal shifted degree in the j-th column, i.e., $d_j := \max_{i=1,\ldots,a}\{\deg V_{ij} + s_i\}$. We write $\operatorname{cdeg}(\boldsymbol{V}) := \operatorname{cdeg}_{\boldsymbol{0}}(\boldsymbol{V})$, where $\boldsymbol{0} := [0, \ldots, 0]$. The maximal degree appearing in a matrix is denoted by $\deg \boldsymbol{V} := \max_{i,j}\{\deg V_{ij}\}$. Let $\boldsymbol{v} \in \mathbb{L}_{q^m}[x]^a \setminus \{\boldsymbol{0}\}$ and $\boldsymbol{s} = [s_1, \ldots, s_a] \in \mathbb{Z}^a$. We define the $\boldsymbol{s}$-pivot index of $\boldsymbol{v}$ to be the largest index i with $1 \leq i \leq a$ such that $\deg v_i + s_i = \operatorname{cdeg}_{\boldsymbol{s}}(\boldsymbol{v})$. If $a \geq b$, then we say that $\boldsymbol{V}$ is in (column) $\boldsymbol{s}$-ordered weak Popov form if the $\boldsymbol{s}$-pivot indices of its columns are distinct and non-decreasing in the column index.

C. Rank-Metric and Interleaved Gabidulin Codes

Rank-metric codes were independently introduced in [1], [2], [3]. Let $\boldsymbol{c} \in \mathbb{F}_{q^m}^n$ be a vector over an extension field $\mathbb{F}_{q^m}$. By fixing a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ we can expand elements in $\mathbb{F}_{q^m}$ into a vector in $\mathbb{F}_q^m$. Hence, we can represent $\boldsymbol{c}$ as a matrix $\boldsymbol{C} \in \mathbb{F}_q^{m \times n}$ The distance of two codewords $\boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathbb{F}_{q^m}^n$ with matrix representations $\boldsymbol{C}_1, \boldsymbol{C}_2$, respectively, is measured by the rank of their difference, i.e., $\mathrm{d_R}(\boldsymbol{c}_1, \boldsymbol{c}_2) = \mathrm{rk}(\boldsymbol{c}_1 - \boldsymbol{c}_2) := \mathrm{rk}(\boldsymbol{C}_1 - \boldsymbol{C}_2)$. A linear rank-metric code $\mathcal{C}$ with parameters $[n, k, d]$ over the field $\mathbb{F}_{q^m}$ is a k-dimensional subspace of $\mathbb{F}_{q^m}^n$ with minimum rank distance $d := \min_{\boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathcal{C},\, \boldsymbol{c}_1 \neq \boldsymbol{c}_2} \mathrm{d_R}(\boldsymbol{c}_1, \boldsymbol{c}_2)$.

Gabidulin codes [1], [2], [3] are rank-metric codes defined by evaluating degree-bounded linearized polynomials at fixed $\mathbb{F}_q$-linearly independent evaluation points $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^m}$:

$$\mathcal{C}_{\mathrm{Gab}}[n, k] = \left\{ \left[f(\alpha_1), \ldots, f(\alpha_n) \right] : f \in \mathbb{L}_{q^m}[x], \deg f < k \right\}.$$

$\mathcal{C}_{\mathrm{Gab}}[n, k]$ is $\mathbb{F}_{q^m}$-linear and has minimum rank distance $d = n - k + 1$, which achieves the Singleton-like bound in the rank metric with equality (see e.g. [2]).

An ℓ-interleaved Gabidulin code is a direct sum of ℓ Gabidulin codes $\mathcal{C}_{\mathrm{Gab}}[n, k_1], \ldots, \mathcal{C}_{\mathrm{Gab}}[n, k_\ell]$ with the same evaluation points, i.e.,

$$\mathcal{IC}_{\mathrm{Gab}} := \left\{ \begin{bmatrix} \boldsymbol{c}_1 \\ \vdots \\ \boldsymbol{c}_\ell \end{bmatrix} : \boldsymbol{c}_i \in \mathcal{C}_{\mathrm{Gab}}[n, k_i] \right\} \subseteq \mathbb{F}_{q^m}^{\ell \times n}.$$

The i-th row of a codeword matrix is obtained by evaluating a message polynomial $f_i \in \mathbb{L}_{q^m}[x]$ of degree $< k_i$ at the fixed evaluation points. The error model considered for interleaved codes is usually an additive matrix $\boldsymbol{E} \in \mathbb{F}_{q^m}^{\ell \times n}$ of $\mathbb{F}_q$-rank t. Note that the rank is taken with respect to the small field $\mathbb{F}_q$ and that the $\mathbb{F}_q$-rank equals the $\mathbb{F}_q$-rank of the tall $\ell m \times n$ matrix obtained by expanding $\boldsymbol{E}$ row-wise into $m \times n$-matrices over $\mathbb{F}_q$ and stacking them on top of each other.

D. Interpolation-Based Decoding of $\mathcal{IC}_{\mathrm{Gab}}$

There are several decoding algorithms for interleaved Gabidulin codes. Here, we consider the interpolation-based decoder by Wachter-Zeh–Zeh in [12]. The algorithm consists of two steps: the *interpolation step* computes $\ell' \leq \ell$ non-zero vectors of linearized polynomials

$$\boldsymbol{Q}^{(i)} = [Q_0^{(i)}, Q_1^{(i)}, \ldots, Q_\ell^{(i)}] \in \mathbb{L}_{q^m}[x]^{\ell+1} \setminus \{\boldsymbol{0}\},\ \forall i = 1, \ldots, \ell'$$

such that they fulfill certain degree and evaluation conditions with respect to the received matrix $\boldsymbol{C} + \boldsymbol{E}$. The *root-finding step* finds all message polynomial vectors $[f_1, \ldots, f_\ell]$ of degrees $\deg f_i < k_i$ such that

$$Q_0^{(i)} + \sum_{j=1}^{\ell} Q_j^{(i)} f_j = 0 \quad \forall\, i = 1, \ldots, \ell'.$$

If the rank of the error matrix $\boldsymbol{E}$ is at most $\frac{\ell}{\ell+1}(n - \overline{k})$ with $\overline{k} := \frac{1}{\ell} \sum_i k_i$, then at least one satisfactory interpolation vector $\boldsymbol{Q}^{(i)}$ exists (see [12]). The output list contains the transmitted message polynomial vector. The algorithm can be considered as a partial unique or list decoder [12].

In the following, we show that root finding can be done by computing a minimal approximant basis of a suitable matrix. This observation will lead to a fast algorithm in Section V.

III. Minimal Approximant Bases Over $\mathbb{L}_{q^m}[x]$

The central computational object that we study in this paper are minimal approximant bases, which are defined as follows.

Definition 1. *Let $\boldsymbol{Q} \in \mathbb{L}_{q^m}[x]^{a \times b}$, $d \in \mathbb{Z}_{\geq 0}$, and $\boldsymbol{s} \in \mathbb{Z}^b$. Then, a (right) approximant of $\boldsymbol{Q}$ of order d is a vector $\boldsymbol{v} \in \mathbb{L}_{q^m}[x]^{b \times 1}$ such that $\boldsymbol{Q}\boldsymbol{v} \equiv \boldsymbol{0} \bmod_{\mathrm{l}} x^{[d]}$. A (right) $\boldsymbol{s}$-minimal approximant basis of $\boldsymbol{Q}$ of order d is a full-rank matrix $\boldsymbol{F} \in \mathbb{L}_{q^m}[x]^{b \times b}$ such that*

1) *$\boldsymbol{F}$ is in $\boldsymbol{s}$-ordered weak Popov form.*
2) *The columns of $\boldsymbol{F}$ are a basis of all right approximants of $\boldsymbol{Q}$ of order d.*

Definition 1 only makes sense if the set of approximants of $\boldsymbol{Q}$ of order d is a right $\mathbb{L}_{q^m}[x]$-module of rank b. However, it is obvious that this set is closed under addition and under right-multiplication by elements of $\mathbb{L}_{q^m}[x]$. Further, the vector $[0,\dots,0,x^{[d]},0,\dots,0]^\top$ is clearly an approximant of $\boldsymbol{Q}$ of order d, so the module of all approximants must contain a module of rank b, hence itself be of rank b (since it cannot be greater than b).

The following is a variant of the "predictable degree property", see [19], which is central to row-reduced matrices such as those in weak Popov form. An analogous result holds for singular rank or non-square matrices, but we will need it only for square ones.

Lemma 1. *Let $\boldsymbol{s} \in \mathbb{Z}^b$, let $\boldsymbol{F} \in \mathbb{L}_{q^m}[x]^{b\times b}$ be full rank and in $\boldsymbol{s}$-ordered weak Popov form. Let $\boldsymbol{t} = [t_1,\dots,t_b] = \operatorname{cdeg}_{\boldsymbol{s}}(\boldsymbol{F})$, and let $\boldsymbol{p} = [p_1,\dots,p_b]^\top \in \mathbb{L}_{q^m}[x]^{b\times 1}$ be a non-zero vector in the column space of $\boldsymbol{F}$ with $\boldsymbol{\lambda} = [\lambda_1,\dots,\lambda_b]^\top \in \mathbb{L}_{q^m}[x]^{b\times 1}$ the unique vector such that $\boldsymbol{p} = \boldsymbol{F}\boldsymbol{\lambda}$. Then, $\operatorname{cdeg}_{\boldsymbol{s}} \boldsymbol{p} = \mu := \max_{j=1,\dots,b}\{\deg \lambda_j + t_j\}$ and the $\boldsymbol{s}$-pivot index of $\boldsymbol{p}$ is $h = \max\{j : \mu = \deg\lambda_j + t_j\}$.*

Proof. Since $\boldsymbol{p} = \boldsymbol{F}\boldsymbol{\lambda}$, then $\deg p_i \le \max_{j=1,\dots,b}\{\deg F_{ij} + \deg\lambda_j\} \le \max_{j=1,\dots,b}\{t_j - s_i + \deg\lambda_j\}$, and so $\operatorname{cdeg}_{\boldsymbol{s}}\boldsymbol{p} \le \mu$. Let $\boldsymbol{u} \in \mathbb{F}_{q^m}^{b\times 1}$ be the vector whose i-th entry is the $x^{[\mu-s_i]}$-coefficient of p_i (the coefficient is zero if $\deg p_i < \mu - s_i$). Hence, $\operatorname{cdeg}_{\boldsymbol{s}}\boldsymbol{p} = \mu$ iff $\boldsymbol{u} \neq \boldsymbol{0}$. Further, if $\boldsymbol{u} \neq \boldsymbol{0}$, then the $\boldsymbol{s}$-pivot index of $\boldsymbol{p}$ is the greatest non-zero index of $\boldsymbol{u}$.

Since $\deg F_{ij} \le t_j - s_i$ and $\deg\lambda_j \le \mu - t_j$, the entries of $\boldsymbol{u}$ only depend on some of the leading coefficients in the matrix $\boldsymbol{F}$ and vector $\boldsymbol{\lambda}$. Let $\operatorname{lm}_{\boldsymbol{s}}(\boldsymbol{F})$ be the $\boldsymbol{s}$-leading matrix of $\boldsymbol{F}$ whose (i,j)-th entry is the $x^{[t_j-s_i]}$-coefficient of F_{ij}, defined as 0 if $\deg F_{ij} < t_j - s_i$. Similarly, define l_j to be the $x^{[\mu-t_j]}$-coefficient of λ_j. Then, by the definition of linearized polynomial multiplication, u_i is the inner product of the i-th row of $\operatorname{lm}_{\boldsymbol{s}}(\boldsymbol{F})$ and the vector $\boldsymbol{l}_i := [l_1^{[t_1-s_i]},\dots,l_b^{[t_b-s_i]}]^\top$.

Since $\boldsymbol{F}$ is full-rank and in $\boldsymbol{s}$-ordered weak Popov form, the $\boldsymbol{s}$-pivot index of its j-th column is j and $\operatorname{lm}_{\boldsymbol{s}}(\boldsymbol{F})$ is in upper triangular form with only non-zero entries on its diagonal. Moreover, $\boldsymbol{l}_i$ is non-zero since at least one λ_j fulfills $\deg\lambda_j + t_j = \mu$, and h as defined above is the greatest non-zero index of $\boldsymbol{l}_i$ (independent of i). Thus, u_h is non-zero and h is also the greatest non-zero index of $\boldsymbol{u}$, which proves the claim. □

Lemma 2. *Let $\boldsymbol{F} \in \mathbb{L}_{q^m}[x]^{b\times b}$ be in $\boldsymbol{s}$-ordered weak Popov form and $\boldsymbol{G} \in \mathbb{L}_{q^m}[x]^{b\times b}$ be in $\boldsymbol{t}$-ordered weak Popov form, where $\boldsymbol{t} = [t_1,\dots,t_b] := \operatorname{cdeg}_{\boldsymbol{s}}(\boldsymbol{F})$. Then, $\boldsymbol{F}\boldsymbol{G}$ is in $\boldsymbol{s}$-ordered weak Popov form.*

Proof. Let $\boldsymbol{u} = [u_1,\dots,u_b] = \operatorname{cdeg}_{\boldsymbol{t}}(\boldsymbol{G})$. Let $\boldsymbol{h}_i$ be the i-th column of $\boldsymbol{F}\boldsymbol{G}$. By Lemma 1 then $\operatorname{cdeg}_{\boldsymbol{s}}\boldsymbol{h}_j = \max_{i=1,\dots,b}\{\deg G_{ij} + t_i\} = u_j$, and further that the $\boldsymbol{s}$-pivot index of $\boldsymbol{h}_j$ is $\max\{i : \deg G_{ij} + t_i = u_j\}$ which is exactly the $\boldsymbol{t}$-pivot index of the j-th column of $\boldsymbol{G}$. Since these are all in strictly increasing order, so must the $\boldsymbol{s}$-pivots of $\boldsymbol{h}_1,\dots,\boldsymbol{h}_b$. Hence $\boldsymbol{F}\boldsymbol{G}$ is in ordered weak Popov form. □

IV. Root Finding by Minimal Approximant Basis

In the following, we show that the root-finding step of the Wachter-Zeh–Zeh interpolation-based decoder can be solved by finding a minimal approximant basis of a suitable matrix. We solve the following formal problem.

Problem 1 (Root-Finding Problem)**.** *Let $\boldsymbol{Q}^{(1)},\dots,\boldsymbol{Q}^{(\ell')} \in \mathbb{L}_{q^m}[x]^{\ell+1} \setminus \{\boldsymbol{0}\}$ be $\ell' \le \ell$ non-zero linearized polynomial vectors. Furthermore, let $k_1,\dots,k_\ell \in \mathbb{Z}_{>0}$ be positive integers. Find a basis of the affine $\mathbb{F}_{q^m}$-space*

$$\mathcal{R} := \big\{[f_1,\dots,f_\ell] \in \mathbb{L}_{q^m}[x]^\ell : Q_0^{(i)} + \textstyle\sum_{j=1}^{\ell} Q_j^{(i)} f_j = 0 \,\forall\, i,\ \deg f_j < k_j \,\forall\, j\big\}.$$

Theorem 1. *Consider an instance of Problem 1, with $\hat{k} := \max_i\{k_i\}$, and choose*

$$\boldsymbol{Q} := \begin{bmatrix} Q_0^{(1)} & Q_1^{(1)} & \dots & Q_\ell^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ Q_0^{(\ell')} & Q_1^{(\ell')} & \dots & Q_\ell^{(\ell')} \end{bmatrix} \in \mathbb{L}_{q^m}[x]^{s\times(\ell+1)}$$

$$\boldsymbol{s} := \begin{bmatrix} \hat{k} & \hat{k}-k_1+1 & \dots & \hat{k}-k_\ell+1 \end{bmatrix} \in \mathbb{Z}_{\ge 0}^{\ell+1}$$

$$d := \max_{i,j}\left\{\deg Q_j^{(i)}\right\} + \hat{k}.$$

Let $\boldsymbol{F}$ be a right $\boldsymbol{s}$-minimal approximant basis of $\boldsymbol{Q}$ of order d. Then,

$$\mathcal{R} = \left\{ \boldsymbol{F}\boldsymbol{v} : \operatorname{cdeg}_{\boldsymbol{t}}\boldsymbol{v} \le \hat{k} \text{ and } [\boldsymbol{F}\boldsymbol{v}]_1 = x \right\}, \tag{1}$$

where $\boldsymbol{t} = \operatorname{cdeg}_{\boldsymbol{s}}(\boldsymbol{F})$ and $[\boldsymbol{F}\boldsymbol{v}]_1$ is the first entry of $\boldsymbol{F}\boldsymbol{v}$.

Proof. By Lemma 1 then for any $\boldsymbol{v} \in \mathbb{L}_{q^m}[x]^{(\ell+1)\times 1}$, we have $\operatorname{cdeg}_{\boldsymbol{s}}(\boldsymbol{F}\boldsymbol{v}) = \max_{i=1,\dots,\ell+1}\{\deg(v_i) + t_i\} = \operatorname{cdeg}_{\boldsymbol{t}}\boldsymbol{v}$.

$\subseteq$: Note that $\mathcal{R}$ consists of those vectors of the right-kernel of $\boldsymbol{Q}$ having $\boldsymbol{s}$-degree at most $\hat{k}$ and first element being x. Any such kernel vector $\boldsymbol{f}$ of $\boldsymbol{Q}$ is in the column space of $\boldsymbol{F}$ by definition of minimal approximant basis, so let $\boldsymbol{v}$ be such that $\boldsymbol{f} = \boldsymbol{F}\boldsymbol{v}$. But then we have $\operatorname{cdeg}_{\boldsymbol{t}}\boldsymbol{v} = \operatorname{cdeg}_{\boldsymbol{s}}(\boldsymbol{F}\boldsymbol{v}) \le \hat{k}$.

$\supseteq$: Let $\boldsymbol{v} \in \mathbb{L}_{q^m}[x]^{\ell+1}$ with $\operatorname{cdeg}_{\boldsymbol{t}}(\boldsymbol{v}) \le \hat{k}$. Then $\operatorname{cdeg}_{\boldsymbol{s}}(\boldsymbol{F}\boldsymbol{v}) \le \hat{k}$, i.e. $\operatorname{cdeg}(\boldsymbol{F}\boldsymbol{v}) \le \hat{k} - \min(\boldsymbol{s}) < \hat{k}$. Since $\boldsymbol{F}$ is a minimal approximant basis of $\boldsymbol{Q}$, then $\boldsymbol{Q}\boldsymbol{F}\boldsymbol{v} \equiv 0 \bmod_{\mathrm{l}} x^{[d]}$. But $\operatorname{cdeg}(\boldsymbol{Q}\boldsymbol{F}\boldsymbol{v}) \le \max_{i,j}(\deg Q_j^{(i)}) + \operatorname{cdeg}(\boldsymbol{F}\boldsymbol{v}) < d$, and hence we can conclude $\boldsymbol{Q}\boldsymbol{F}\boldsymbol{v} = 0$. In other words, $\boldsymbol{F}\boldsymbol{v}$ is a right kernel vector of $\boldsymbol{Q}$. Since it also has $\boldsymbol{s}$-degree at most $\hat{k}$, it must be in $\mathcal{R}$ as long as its first component is x. □

Theorem 1 shows that $\boldsymbol{F}$ is an implicit, compact representation of a basis of the affine space solving Problem 1: it is easy to tabulate the vectors $\boldsymbol{v}$ of $\operatorname{cdeg}_{\boldsymbol{t}}\boldsymbol{v} \le \hat{k}$. The requirement that $[\boldsymbol{F}\boldsymbol{v}]_1 = x$ is also easy: any column of $\boldsymbol{F}$ with $\boldsymbol{s}$-degree at most $\hat{k}$ has the first entry of the form ax with $a \in \mathbb{F}_{q^m}$. Only those columns of $\boldsymbol{F}$ with $\boldsymbol{s}$-degree at most $\hat{k}$ will have corresponding non-zero entries in $\boldsymbol{v}$ in the set $\mathcal{R}$ in (1).

Remark 1. *Without loss of generality, we can assume that $\boldsymbol{Q}$ has full rank since we can neglect dependent solutions of the interpolation step as they do not contribute to finding roots.*

Due to the degree restrictions in the interpolation step of the algorithm in [12], we have $d \in O(n)$.

V. Fast Computation of Minimal Approximant Bases over Linearized Polynomial Rings

In this section, we adapt the (left) PM-basis algorithm [18], [24] over ordinary polynomial rings to compute a (right) minimal approximant basis over linearized polynomials.

A. Base Case: Approximant Bases of Degree 1

Given a matrix $\boldsymbol{Q} \in \mathbb{L}_{q^m}[x]^{a\times b}$ with $\deg(\boldsymbol{Q}) < 1$ and a shift vector $\boldsymbol{s} \in \mathbb{Z}^b$, we want to construct a right $\boldsymbol{s}$-minimal approximant basis $\boldsymbol{F} \in \mathbb{L}_{q^m}[x]^{b\times b}$ of $\boldsymbol{Q}$ of degree $d = 1$ with

$$\boldsymbol{Q}\boldsymbol{F} \equiv \boldsymbol{0} \bmod_{\mathrm{l}} x^{[1]}. \tag{2}$$

In the ordinary $\mathbb{F}_{q^m}[x]$ base case this can be done efficiently using $\mathbb{F}_{q^m}$-linear algebra since any matrix from $\mathbb{F}_{q^m}[x]^{a\times b}$ of

Algorithm 1: RightLinBaseCase

Input : matrix $\boldsymbol{Q} \in \mathbb{L}_{q^m}[x]^{a\times b}$ with $\deg(\boldsymbol{Q}) < 1$, shifts $\boldsymbol{s} \in \mathbb{Z}^b$
Output: a right $\boldsymbol{s}$-minimal approximant basis of $\boldsymbol{Q}$ of order $d = 1$

$\pi_{\boldsymbol{s}} \leftarrow b \times b$ permutation matrix s.t. $[(s_1, 1), \ldots, (s_b, b)]\pi_{\boldsymbol{s}}$ is lex. increasing
$\boldsymbol{A} \in \mathbb{F}_{q^m}^{a\times b} \leftarrow$ defined by $\boldsymbol{Q} = \boldsymbol{A}\,\mathrm{diag}(x^{[0]}, \ldots, x^{[0]})$
$[i_1, \ldots, i_\rho], [j_1, \ldots, j_\rho] \leftarrow$ row and column rank profiles of $\boldsymbol{A}\pi_{\boldsymbol{s}}$
$[k_1, \ldots, k_{b-\rho}] \leftarrow \{1, \ldots, b\} \setminus \{j_1, \ldots, j_\rho\}$ sorted increasingly
$\boldsymbol{A}_1 \leftarrow$ submatrix of $\boldsymbol{A}\pi_{\boldsymbol{s}}$ with indices in $\{i_1, \ldots, i_\rho\} \times \{j_1, \ldots, j_\rho\}$
$\boldsymbol{A}_2 \leftarrow$ submatrix of $\boldsymbol{A}\pi_{\boldsymbol{s}}$ with indices in $\{i_1, \ldots, i_\rho\} \times \{k_1, \ldots, k_{b-\rho}\}$
$\pi \leftarrow$ permutation s.t. $[j_1 \ldots j_\rho k_1 \ldots k_{b-\rho}]\pi = [1 \ldots b]$
return $\pi_{\boldsymbol{s}}\pi^{-1}\begin{bmatrix} x^{[1]}\boldsymbol{I}_\rho & -\boldsymbol{A}_1^{-1}\boldsymbol{A}_2\boldsymbol{I}_{m-\rho} \\ \boldsymbol{0} & \boldsymbol{I}_{m-\rho}\end{bmatrix}\pi\pi_{\boldsymbol{s}}^{-1}$

degree less than 1 is a matrix over $\mathbb{F}_{q^m}$ (see [18], [24]). We will show how to solve the base case for linearized polynomials in (2) efficiently using similar $\mathbb{F}_{q^m}$-linear algebra.

Any matrix $\boldsymbol{Q} \in \mathbb{L}_{q^m}[x]^{a\times b}$ with $\deg(\boldsymbol{Q}) < 1$ can be decomposed as $\boldsymbol{Q} = \boldsymbol{A} \cdot \boldsymbol{I}_b$ with $\boldsymbol{A} \in \mathbb{F}_{q^m}^{a\times b}$ and $\boldsymbol{I}_b \stackrel{\text{def}}{=} \mathrm{diag}(x^{[0]}, \ldots, x^{[0]})$ being the diagonal matrix from $\mathbb{L}_{q^m}[x]^{b\times b}$ with $x = x^{[0]}$ as each diagonal entry.

The algorithm for solving the base case for linearized polynomials in (2) is given in Algorithm 1.

Theorem 2. *Algorithm 1 is correct and has complexity*

$$O(\rho^{\omega-2}ab) \le O(a^{\omega-1}b)$$

in operations over $\mathbb{F}_{q^m}$ where $\rho \le a$ is the rank of $\boldsymbol{Q}$.

Proof. In step 1 the columns of $\boldsymbol{Q}$ are ordered such that $\hat{\boldsymbol{s}} \stackrel{\text{def}}{=} \boldsymbol{s}\pi_{\boldsymbol{s}}$ is non-decreasing. This allows to compute an $\hat{\boldsymbol{s}}$-minimal approximant basis of $\hat{\boldsymbol{Q}} \stackrel{\text{def}}{=} \boldsymbol{Q}\pi_{\boldsymbol{s}}$ of order $d = 1$. Define $\hat{\boldsymbol{A}} \stackrel{\text{def}}{=} \boldsymbol{A}\pi_{\boldsymbol{s}}$ and

$$\hat{\boldsymbol{F}} \stackrel{\text{def}}{=} \pi^{-1}\begin{bmatrix} x^{[1]}\boldsymbol{I}_\rho & -\boldsymbol{A}_1^{-1}\boldsymbol{A}_2\boldsymbol{I}_{b-\rho} \\ \boldsymbol{0} & \boldsymbol{I}_{b-\rho}\end{bmatrix}\pi \tag{3}$$

We now show that $\hat{\boldsymbol{F}}$ is an $\hat{\boldsymbol{s}}$-minimal approximant basis of $\hat{\boldsymbol{Q}}$ and order $d = 1$. We have that $\hat{\boldsymbol{Q}}\pi^{-1}\begin{bmatrix} x^{[1]}\boldsymbol{I}_\rho \\ \boldsymbol{0}\end{bmatrix} = 0 \bmod_{\mathrm{l}} x^{[1]}$. Since $[1\ \ldots\ b]\pi^{-1} = [j_1\ \ldots\ j_\rho\ k_1\ \ldots\ k_{b-\rho}]$ we have that $\hat{\boldsymbol{Q}}\pi^{-1} = \begin{bmatrix}\boldsymbol{A}_1 & \boldsymbol{A}_2\end{bmatrix}\boldsymbol{I}_b$ and

$$\begin{bmatrix}\boldsymbol{A}_1 & \boldsymbol{A}_2\end{bmatrix}\boldsymbol{I}_b\begin{bmatrix} -\boldsymbol{A}_1^{-1}\boldsymbol{A}_2\boldsymbol{I}_{b-\rho} \\ \boldsymbol{I}_{b-\rho}\end{bmatrix} = 0. \tag{4}$$

Hence the columns of $\hat{\boldsymbol{F}}$ are approximants of $\hat{\boldsymbol{Q}}$ of degree $d = 1$. The matrix $\hat{\boldsymbol{F}}$ is upper triangular, where all non-diagonal entries have a lower degree than the diagonal entries in the same row. Hence, the $\hat{\boldsymbol{s}}$-pivot indices are distinct and non-decreasing in the column index implying that $\hat{\boldsymbol{F}}$ is in $\hat{\boldsymbol{s}}$-ordered weak Popov form. Finally, the matrix $\pi_{\boldsymbol{s}}\hat{\boldsymbol{F}}\pi_{\boldsymbol{s}}^{-1}$ is in $\boldsymbol{s}$-ordered weak Popov form since $\pi_{\boldsymbol{s}}$ performs a stable sort on $\boldsymbol{s}$ and thus on the rows of $\hat{\boldsymbol{F}}$.

Left is to prove that the column space $\hat{\boldsymbol{F}}$ contains all right approximants of $\hat{\boldsymbol{Q}}$ of order 1, or equivalently that the column space of $\pi\hat{\boldsymbol{F}}$ contains all right approximants of $\hat{\boldsymbol{Q}}\pi^{-1}$. Assume oppositely that $\boldsymbol{f} = [f_1, \ldots, f_b]^\top \in \mathbb{L}_{q^m}[x]^{b\times 1}$ is a non-zero approximant of $\hat{\boldsymbol{Q}}\pi^{-1}$ of order 1 not in the column space of $\pi\hat{\boldsymbol{F}}$, and assume under this constraint that $\boldsymbol{f}$ is chosen so the index h of the last non-zero element is minimal, i.e. $f_h \neq 0$ while $f_{h+1} = \ldots = f_b = 0$. If $h > \rho$, then $\boldsymbol{f} - F_h f_h$, where F_h is the h-th column of $\pi\hat{\boldsymbol{F}}$, is also an approximant, but it will have last non-zero entry at an index less than h, which is a contradiction. Therefore $h \le \rho$, so by canceling terms of $\boldsymbol{f}$ of degree ≥ 1 with the first ρ columns of $\pi\hat{\boldsymbol{F}}$ we can assume $\mathrm{cdeg}\,\boldsymbol{f} = 0$, i.e. $\boldsymbol{f} = \hat{\boldsymbol{f}}\cdot x$ with $\hat{\boldsymbol{f}} \in \mathbb{F}_{q^m}^{b\times 1}$. Hence $\mathrm{cdeg}(\hat{\boldsymbol{Q}}\pi^{-1}\boldsymbol{f}) = \boldsymbol{0}$ so since $\boldsymbol{f}$ is an approximant of degree 1, then $\hat{\boldsymbol{A}}\pi\hat{\boldsymbol{f}} = \boldsymbol{0}$. But since $\mathrm{rk}\,\boldsymbol{A} = \rho$, then $\hat{\boldsymbol{A}}\pi$ is equivalent under $\mathbb{F}_{q^m}$-row operations to a matrix $\left[\begin{array}{c|c}\boldsymbol{I}_\rho & \boldsymbol{B} \\ \hline \boldsymbol{0} & \end{array}\right]$, where $\boldsymbol{B} \in \mathbb{F}_{q^m}^{\rho\times(b-\rho)}$. If $\hat{\boldsymbol{A}}\pi\hat{\boldsymbol{f}} = \boldsymbol{0}$, then $[\boldsymbol{I}_\rho \mid \boldsymbol{B}]\hat{\boldsymbol{f}} = \boldsymbol{0}$, which is impossible since $\hat{\boldsymbol{f}}$ is only non-zero on the first ρ entries.

The main computational task is to compute the row and column rank profile of the matrix $\hat{\boldsymbol{A}} \in \mathbb{F}_{q^m}^{a\times b}$ of rank ρ which requires $O(\rho^{\omega-2}ab)$ operations in $\mathbb{F}_{q^m}$ [31, Thm. 2.10]. □

B. Recursive Algorithm: PM-Basis

To use the base case in Algorithm 1 to construct minimal approximant bases of order $d > 1$ we need the following.

Lemma 3. *Let $d \in \mathbb{Z}_{>0}$, $\boldsymbol{Q} \in \mathbb{L}_{q^m}[x]^{a\times b}$ of degree less than d, and shifts $\boldsymbol{s} \in \mathbb{Z}^b$. Let $d_1, d_2 \in \mathbb{Z}_{>0}$ be such that $d_1 + d_2 = d$. Let $\boldsymbol{F}_1$ be a right $\boldsymbol{s}$-minimal approximant basis of $\boldsymbol{Q} \bmod_{\mathrm{l}} x^{[d_1]}$ of degree d_1 and $\boldsymbol{t} := \mathrm{cdeg}_{\boldsymbol{s}}(\boldsymbol{F}_1)$. Let $\boldsymbol{F}_2$ be a right $\boldsymbol{t}$-minimal approximant basis of $x^{[-d_1]}\boldsymbol{Q}\boldsymbol{F}_1 \bmod_{\mathrm{l}} x^{[d-d_1]}$ of degree d_2. Then, $\boldsymbol{F}_1\boldsymbol{F}_2$ is a right $\boldsymbol{s}$-minimal approximant basis of $\boldsymbol{Q}$.*

Proof: We show that all approximants of $\boldsymbol{Q}$ of order d are $\mathbb{L}_{q^m}[x]$-linear combinations of the columns of $\boldsymbol{F}_1\boldsymbol{F}_2$. First we show that all approximants of $\boldsymbol{Q}$ of order d are approximants of $\boldsymbol{Q} \bmod_{\mathrm{l}} x^{[d_1]}$ of order d_1. Let $\boldsymbol{f}$ be an approximant of $\boldsymbol{Q}$ of order d and decompose $\boldsymbol{Q}$ as $\boldsymbol{Q} = \boldsymbol{Q} \bmod_{\mathrm{l}} x^{[d_1]} + \tilde{\boldsymbol{Q}}$. Then

$$\begin{aligned}&(\boldsymbol{Q} \bmod_{\mathrm{l}} x^{[d_1]} + \tilde{\boldsymbol{Q}})\boldsymbol{f} \equiv \boldsymbol{0} \bmod_{\mathrm{l}} x^{[d]} \\ \implies\quad &(\boldsymbol{Q} \bmod_{\mathrm{l}} x^{[d_1]})\boldsymbol{f} \equiv \boldsymbol{0} \bmod_{\mathrm{l}} x^{[d_1]}\end{aligned}$$

since no entry of $\tilde{\boldsymbol{Q}}$ has non-zero coefficients of index smaller than d_1. Hence, $\boldsymbol{f}$ can be written as $\boldsymbol{f} = \boldsymbol{F}_1\boldsymbol{\lambda}$ for some $\boldsymbol{\lambda} \in \mathbb{L}_{q^m}[x]^{(\ell+1)\times 1}$. On the other hand, any approximant $\boldsymbol{p}$ of $\left(x^{[-d_1]}\boldsymbol{Q}\boldsymbol{F}_1 \bmod_{\mathrm{l}} x^{[d-d_1]}\right)$ of order d_2 satisfies

$$\begin{aligned}&\left(x^{[-d_1]}\boldsymbol{Q}\boldsymbol{F}_1 \bmod_{\mathrm{l}} x^{[d-d_1]}\right)\boldsymbol{p} \equiv \boldsymbol{0} \bmod_{\mathrm{l}} x^{[d-d_1]} \\ &\qquad\implies\quad \boldsymbol{Q}\boldsymbol{F}_1\boldsymbol{p} \equiv \boldsymbol{0} \bmod_{\mathrm{l}} x^{[d]}.\end{aligned}$$

The last line shows that all approximants $\boldsymbol{f}$ of $\boldsymbol{Q}$ can be written as $\boldsymbol{f} = \boldsymbol{F}_1\boldsymbol{\lambda}$ where $\boldsymbol{\lambda}$ is an approximant of $\left(x^{[-d_1]}\boldsymbol{Q}\boldsymbol{F}_1 \bmod_{\mathrm{l}} x^{[d-d_1]}\right)$ of order d_2. Hence, there exists a $\boldsymbol{\mu} \in \mathbb{L}_{q^m}[x]^{(\ell+1)\times 1}$ such that $\boldsymbol{f} = \boldsymbol{F}_1\boldsymbol{F}_2\boldsymbol{\mu}$.

By Lemma 2, $\boldsymbol{F}_1\boldsymbol{F}_2$ is in $\boldsymbol{s}$-ordered weak Popov form and the statement follows. ■

Using Lemma 3 with $d_1 = 1$ (i.e. the base case) and $d_2 = d - 1$ in an iterative manner results in a right linearized variant of [18, M-Basis] where the order of $\boldsymbol{F}$ is increased by one in each iteration. Due to space restrictions we omit the presentation of the right linearized variant of M-Basis.

Algorithm 2 is a fast divide & conquer algorithm for constructing (right) minimal approximant bases over linearized polynomial rings. The algorithm uses the result of Lemma 3 with $d_1 = \lceil d/2 \rceil$ and $d_2 = d - d_1$ recursively and is a fast right linearized variant of [18, PM-Basis].

Algorithm 2: RightLinPM-Basis

Input :
- positive integer $d \in \mathbb{Z}_{>0}$,
- matrix $\boldsymbol{Q} \in \mathbb{L}_{q^m}[x]^{a \times b}$ of maximal degree $< d$,
- shifts $\boldsymbol{s} \in \mathbb{Z}^b$.

Output: a right $\boldsymbol{s}$-minimal approximant basis of $\boldsymbol{Q}$ of degree d

1 **if** *d=1* **then**
2 **return** RightLinBaseCase($\boldsymbol{Q}, \boldsymbol{s}$)
3 **else**
4 $d_1 \leftarrow \lceil d/2 \rceil$, $d_2 \leftarrow d - d_1$
5 $\boldsymbol{F}_1 \leftarrow$ RightLinPM-Basis $\left(d_1, \boldsymbol{Q} \bmod_{\mathrm{l}} x^{[d_1]}, \boldsymbol{s}\right)$
6 $\boldsymbol{G} \leftarrow \left(x^{[-d_1]} \boldsymbol{Q} \boldsymbol{F}_1\right) \bmod_{\mathrm{l}} x^{[d_2]}$; $\boldsymbol{t} \leftarrow \mathrm{cdeg}_{\boldsymbol{s}}\left(\boldsymbol{F}_1\right)$
7 $\boldsymbol{F}_2 \leftarrow$ RightLinPM-Basis $\left(d_2, \boldsymbol{G}, \boldsymbol{t}\right)$
8 **return** $\boldsymbol{F}_1 \boldsymbol{F}_2$

Theorem 3. *Algorithm 2 is correct and has complexity*

$$O(\max\{a, b\}^{\omega} \mathcal{M}(d)).$$

Proof. Correctness follows from Lemma 3 and the fact that Algorithm 1 returns a right $\boldsymbol{s}$-minimal approximant basis of $\boldsymbol{Q}$ of order $d = 1$.

As for the complexity, the algorithm calls itself twice with input size $\approx d/2$. The any other costful operation is the matrix multiplication in Line 6. Since we multiply two matrices $\boldsymbol{Q}$ and $\boldsymbol{F}_1$ with maximal degree at most d and d_1, respectively, the cost of this line is $O(\max\{a, b\}^{\omega} \mathcal{M}(d))$. The base case, Algorithm 1, costs $O(a^{\omega-1} b)$. Hence, we obtain the claimed complexity by the master theorem. □

Theorem 3 together with Theorem 1 imply the main statement of this paper, which is given in the following corollary.

Corollary 1. *The root-finding step of interpolation-based decoding of an ℓ-interleaved Gabidulin code of length n can be implemented with complexity $O^{\sim}(\ell^{\omega} \mathcal{M}(n))$.*

VI. Conclusion

We have presented a fast algorithm for root finding in interpolation-based decoding of interleaved Gabidulin codes, which is based on computing minimal approximant bases over linearized polynomials and has complexity $O^{\sim}(\ell^{\omega} \mathcal{M}(n))$.

The methodology can also be applied to other decoding problems: for instance, we expect that a left variant of the algorithms can speed up the interpolation step of the Wachter-Zeh–Zeh decoder, thereby reducing its cost from $O^{\sim}(\ell^3 \mathcal{M}(\ell n))$ to $O^{\sim}(\ell^{\omega-1} \mathcal{M}(n))$. For $\mathcal{M}(n) \in \Theta(n^{1.635})$ and $\omega = 2.37$ (Coppersmith–Winograd matrix multiplication), this would be a speed-up from $\ell^{4.645} n^{1.635}$ to $\ell^{2.37} n^{1.635}$. Furthermore, the results can be used for interpolation-based decoding of interleaved subspace codes [15], [16].

References

[1] P. Delsarte, "Bilinear Forms over a Finite Field with Applications to Coding Theory," *Journal of Combinatorial Theory, Series A*, vol. 25, no. 3, pp. 226–241, 1978.

[2] E. M. Gabidulin, "Theory of Codes with Maximum Rank Distance," *Problems of Information Transmission*, vol. 21, no. 1, pp. 3–16, 1985.

[3] R. M. Roth, "Maximum-Rank Array Codes and their Application to Crisscross Error Correction," *IEEE Transactions on Information Theory*, vol. 37, no. 2, pp. 328–336, 1991.

[4] P. Loidreau and R. Overbeck, "Decoding Rank Errors Beyond the Error Correcting Capability," in *International Workshop on Algebraic and Combinatorical Coding Theory*, 2006, pp. 186–190.

[5] V. Sidorenko and M. Bossert, "Decoding Interleaved Gabidulin Codes and Multisequence Linearized Shift-Register Synthesis," in *IEEE International Symposium on Information Theory*, 2010, pp. 1148–1152.

[6] V. Sidorenko, L. Jiang, and M. Bossert, "Skew-Feedback Shift-Register Synthesis and Decoding Interleaved Gabidulin Codes," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 621–632, 2011.

[7] S. Puchinger, J. Rosenkilde né Nielsen, W. Li, and V. Sidorenko, "Row Reduction Applied to Decoding of Rank-Metric and Subspace Codes," *Designs, Codes and Cryptography*, vol. 82, no. 1-2, pp. 389–409, 2017.

[8] V. Sidorenko and M. Bossert, "Fast Skew-Feedback Shift-Register Synthesis," *Des. Codes Cryptogr.*, vol. 70, no. 1-2, pp. 55–67, 2014.

[9] S. Puchinger, S. Müelich, D. Mödinger, J. Rosenkilde, and M. Bossert, "Decoding Interleaved Gabidulin Codes Using Alekhnovich's Algorithm," *Elec. Notes Discr. Math.*, vol. 57, pp. 175–180, 2017.

[10] X. Caruso and J. Le Borgne, "Fast Multiplication for Skew Polynomials," in *ISSAC*, 2017.

[11] S. Puchinger and A. Wachter-Zeh, "Fast Operations on Linearized Polynomials and their Applications in Coding Theory," *J Symb Comput*, vol. 89, pp. 194–215, 2018.

[12] A. Wachter-Zeh and A. Zeh, "List and Unique Error-Erasure Decoding of Interleaved Gabidulin Codes with Interpolation Techniques," *Designs, Codes and Cryptography*, vol. 73, no. 2, pp. 547–570, 2014.

[13] H. Xie, J. Lin, Z. Yan, and B. W. Suter, "Linearized Polynomial Interpolation and Its Applications," *IEEE Transactions on Signal Processing*, vol. 61, no. 1, pp. 206–217, Jan. 2013.

[14] S. Puchinger, "Construction and Decoding of Evaluation Codes in Hamming and Rank Metric," Ph.D. dissertation, Universität Ulm, 2018.

[15] H. Bartz and A. Wachter-Zeh, "Efficient List Decoding of Interleaved Subspace and Gabidulin Codes Using Gröbner Bases," *Advances in Mathematics of Communications*, vol. 12, no. 4, Nov. 2018.

[16] H. Bartz, "Algebraic Decoding of Subspace and Rank-Metric Codes," Ph.D. dissertation, Technische Universität München, 2017.

[17] B. Beckermann and G. Labahn, "A Uniform Approach for the Fast Computation of Matrix-Type Padé Approximants," *SIAM J. Matrix Anal. Appl.*, vol. 15, no. 3, pp. 804–823, Jul. 1994.

[18] P. Giorgi, C.-P. Jeannerod, and G. Villard, "On the complexity of polynomial matrix computations," in *ISSAC*. New York, NY, USA: ACM, 2003, pp. 135–142.

[19] T. Kailath, *Linear Systems*. Prentice-Hall, 1980.

[20] W. Zhou and G. Labahn, "Efficient Algorithms for Order Basis Computation," *J Symb Comput*, vol. 47, no. 7, pp. 793–819, Jul. 2012.

[21] C.-P. Jeannerod, V. Neiger, E. Schost, and G. Villard, "Fast Computation of Minimal Interpolation Bases in Popov Form for Arbitrary Shifts," in *ISSAC*, 2016.

[22] T. Mulders and A. Storjohann, "On Lattice Reduction for Polynomial Matrices," *J Symb Comput*, vol. 35, no. 4, pp. 377–401, 2003.

[23] J. S. R. Nielsen, "Generalised Multi-Sequence Shift-Register Synthesis Using Module Minimisation," in *IEEE International Symposium on Information Theory*, 2013, pp. 882–886.

[24] Neiger, Vincent, "Bases of Relations in One or Several Variables: Fast Algorithms and Applications," Ph.D. dissertation, École Normale Supérieure de Lyon - University of Waterloo, 2016.

[25] V. Popov, "Some properties of the control systems with irreducible matrix-transfer functions," in *Seminar on Differential Equations and Dynamical Systems, II*, 1970, pp. 169–180.

[26] V. Neiger, "Fast computation of shifted Popov forms of polynomial matrices via systems of modular polynomial equations," in *ISSAC*, Jul. 2016.

[27] Ø. Ore, "Theory of Non-Commutative Polynomials," *Annals of Mathematics*, pp. 480–508, 1933.

[28] H. Cheng, "Algorithms for Normal Forms for Matrices of Polynomials and Ore Polynomials," Ph.D. dissertation, University of Waterloo, 2003.

[29] M. Khochtali, J. Rosenkilde né Nielsen, and A. Storjohann, "Popov Form Computation for Matrices of Ore Polynomials," in *ISSAC*, 2017.

[30] Ø. Ore, "On a Special Class of Polynomials," *Transactions of the American Mathematical Society*, vol. 35, no. 3, pp. 559–584, 1933.

[31] A. Storjohann, "Algorithms for Matrix Canonical Forms," Ph.D. dissertation, ETH Zurich, 2000.