Fast algorithm for border bases of Artinian Gorenstein algebras

Bernard Mourrain

Fast algorithm for border bases of Artinian Gorenstein algebras

BERNARD MOURRAIN*

Abstract. Given a multi-index sequence σ, we present a new efficient algorithm to compute generators of the linear recurrence relations between the terms of σ. We transform this problem into an algebraic one, by identifying multi-index sequences, multivariate formal power series and linear functionals on the ring of multivariate polynomials. In this setting, the recurrence relations are the elements of the kernel I_σ of the Hankel operator H_σ associated to σ. We describe the correspondence between multi-index sequences with a Hankel operator of finite rank and Artinian Gorenstein Algebras. We show how the algebraic structure of the Artinian Gorenstein algebra $\mathcal{A}_\sigma$ associated to the sequence σ yields the structure of the terms σ_α for all $\alpha \in \mathbb{N}^n$. This structure is explicitly given by a border basis of $\mathcal{A}_\sigma$, which is presented as a quotient of the polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ by the kernel I_σ of the Hankel operator H_σ. The algorithm provides generators of I_σ constituting a border basis, pairwise orthogonal bases of $\mathcal{A}_\sigma$ and the tables of multiplication by the variables in these bases. It is an extension of Berlekamp-Massey-Sakata (BMS) algorithm, with improved complexity bounds. We present applications of the method to different problems such as the decomposition of functions into weighted sums of exponential functions, sparse interpolation, fast decoding of algebraic codes, computing the vanishing ideal of points, and tensor decomposition. Some benchmarks illustrate the practical behavior of the algorithm.

1. Introduction.

Discovering hidden structures from probing or sampling is a problem which appears in many contexts and in many applications. An interesting instance of this general problem is recovering the structure of a sequence of values, from the knowledge of some of its terms. It consists in guessing any term of the sequence from the first known terms. A classical way to tackle this problem, which goes back to Bernoulli, is to find linear recurrence relations between the first terms of a sequence, to compute the roots of the associated characteristic polynomial and to deduce the expression of any term of the sequence from these roots.

In this paper, we consider the structure discovering problem for multi-index sequences $\sigma = (\sigma_\alpha)_{\alpha\in\mathbb{N}^n} \in \mathbb{K}^{\mathbb{N}^n}$ of values in a field $\mathbb{K}$. Given a finite set of values σ_α for $\alpha \in \boldsymbol{a} \subset \mathbb{N}^n$, we want to guess a formula for the general terms of the sequence σ. An important step of this approach is to compute characteristic polynomials of the sequence $\sigma = (\sigma_\alpha)_{\alpha\in\mathbb{N}^n}$. They correspond to multi-index *recurrence relations* with constant coefficients between the terms of σ. The ideal of these recurrence relation polynomials define an Artinian Gorenstein algebra. We present a fast algorithm to compute a border basis of this ideal from the first terms of the sequence σ. This method also yields a basis of the Artinian Gorenstein algebra as well as its multiplicative structure.

Related works. The approach that we present is related to Prony's method in the univariate case and to its variants [33], [29], [17], [8], ... and to the more recent extensions in the multivariate case [1], [27], [18], [32]. Linear algebra tools are used to determine a basis of the quotient algebra $\mathcal{A}_\sigma$ or to compute an H-basis for the presentation of $\mathcal{A}_\sigma$. An analysis of the complexity of these approaches yields bounds in $\mathcal{O}(\tilde{s}^3)$ (or $\mathcal{O}(\tilde{s}^\omega)$), where $\tilde{s}$ is the size of the Hankel matrices involved in these methods, typically the number $\binom{d'+n}{n}$ of monomials in degree at most $d' < \frac{d}{2}$ if the terms of the sequence are known up to the degree d. The problem is also related to Padé approximants, well investigated in the univariate case [11], [3], [35], but much less developed in the multivariate case [28], [13].

Finding recurrence relations is a problem which is also well developed in the univariate case. Berlekamp [5] and Massey [20] proposed an efficient algorithm to compute such recurrence relations, with a complexity in $\mathcal{O}(r^2)$ where r is the size of the minimal recurrence relation. Exploiting further the properties of Hankel matrices, the complexity of computing recurrence relations can be reduced in the univariate case to $\tilde{\mathcal{O}}(r)$.

Sakata extended Berlekamp-Massey algorithm to multi-index sequences, computing a Gröbner basis of the polynomials in the kernel of a multi-index Hankel matrix [31]. See also [30] for an analysis and overview of the algorithm. The computation of multivariate linear recurrence relations have been further investigated, e.g. in [16] and more recently in [7], where the coefficients of the Gröbner basis are computed by solving multi-index Hankel systems.

*UCA, Inria Méditerranée, AROMATH, Sophia Antipolis, France, bernard.mourrain@inria.fr

Contributions. We translate the structure discovering problem into an algebraic setting, by identifying multi-index sequences of values, generating formal power series and linear functionals on the ring of polynomials. Through this identification, we associate to a multi-index sequence σ, a Hankel operator H_σ which kernel I_σ defines an Artinian Gorenstein Algebra $\mathcal{A}_\sigma$ when H_σ is of finite rank. We present a new efficient algorithm to compute the algebraic structure of $\mathcal{A}_\sigma$, using the first terms σ_α for $\alpha \in \boldsymbol{a} \subset \mathbb{N}^n$. The structure $\mathcal{A}_\sigma$ is described by a border basis of the ideal I_σ.

This algorithm is an extension of the Berlekamp-Massey-Sakata (BMS) algorithm. It computes border bases of the recurrence relations, which are more general than Gröbner bases. They also offer a better numerical stability [25] in the solving steps required to address the decomposition problem. The algorithm, based on a Gram-Schmidt orthogonalisation process, is simplified. The complexity bound also improves the previously known bounds for computing such recurrence relations. We show that the arithmetic complexity of computing a border basis is in $\mathcal{O}((r+\delta)rs)$ where r is the number of roots of I_σ (counted with multiplicities), δ is the size of the border of the monomial basis and s is the number of known terms of the sequence σ.

The algorithm outputs generators of the recurrence relations, a monomial basis, an orthogonal basis and the tables of multiplication by the variables in this basis of $\mathcal{A}_\sigma$. The structure of the terms of the sequence σ can be deduced from this output, by applying classical techniques for solving polynomial systems from tables of multiplication. We show how the algorithm can be applied to different problems such as the decomposition of functions into weighted sums of exponential functions, sparse interpolation, fast decoding of algebraic codes, vanishing ideal of points, and tensor decomposition.

Notation. Let $\mathbb{K}$ be a field, $\bar{\mathbb{K}}$ its algebraic closure, $\mathbb{K}[x_1,\ldots,x_n] = \mathbb{K}[\boldsymbol{x}]$ be the ring of polynomials in the variables $x_1,\ldots,x_n$ with coefficients in the field $\mathbb{K}$, $\mathbb{K}[[y_1,\ldots,y_n]] = \mathbb{K}[\boldsymbol{y}]$ be the ring of formal power series in the variables $y_1,\ldots,y_n$ with coefficients in $\mathbb{K}$. We denote by $\mathbb{K}^{\mathbb{N}^n}$ the set of sequences $\sigma = (\sigma_\alpha)_{\alpha\in\mathbb{N}^n}$ of numbers $\sigma_\alpha \in \mathbb{K}$, indexed by $\mathbb{N}^n$. $\forall \alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{N}^n$, $\alpha! = \prod_{i=1}^n \alpha_i!$, $\boldsymbol{x}^\alpha = \prod_{i=1}^n x_i^{\alpha_i}$. The monomials in $\mathbb{K}[\boldsymbol{x}]$ are the elements of the form $\boldsymbol{x}^\alpha$ for $\alpha \in \mathbb{N}^n$. For a set $B \subset \mathbb{K}[\boldsymbol{x}]$, $B^+ = \cup_{i=1}^n x_i B \cup B$, $\partial B = B^+ \setminus B$. A set B of monomials of $\mathbb{K}[\boldsymbol{x}]$ is connected to 1, if $1 \in B$ and for $\boldsymbol{x}^\beta \in B$ different from 1, there exists $\boldsymbol{x}^{\beta'} \in B$ and $i \in [1,n]$ such that $\boldsymbol{x}^\beta = x_i \boldsymbol{x}^{\beta'}$. For $F \subset \mathbb{K}[\boldsymbol{x}]$, $\langle F\rangle$ is the vector space of $\mathbb{K}[\boldsymbol{x}]$ spanned by F and (F) is the ideal generated by F. For $V, V' \subset \mathbb{K}[\boldsymbol{x}]$, $V \cdot V'$ is the set of products of an element of V by an element of V'.

2. Polynomial-Exponential series.

In this section, we recall the correspondence between sequences $\sigma = (\sigma_\alpha)_{\alpha\in\mathbb{N}^n} \in \mathbb{K}^{\mathbb{N}^n}$ associated to polynomial-exponential series and Artinian Gorenstein Algebras.

2.1. Duality.

A sequence $\sigma = (\sigma_\alpha)_{\alpha\in\mathbb{N}^n} \in \mathbb{K}^{\mathbb{N}^n}$ is naturally associated to a linear form operating on polynomials, that is, an element of $\mathrm{Hom}_{\mathbb{K}}(\mathbb{K}[\boldsymbol{x}],\mathbb{K}) = \mathbb{K}[\boldsymbol{x}]^*$, as follows:

$$p = \sum_{\alpha\in A\subset\mathbb{N}^n} p_\alpha \boldsymbol{x}^\alpha \in \mathbb{K}[\boldsymbol{x}] \mapsto \langle \sigma \mid p\rangle = \sum_{\alpha\in A\subset\mathbb{N}^n} p_\alpha \sigma_\alpha.$$

This correspondence is bijective since a linear form $\sigma \in \mathbb{K}[\boldsymbol{x}]^*$ is uniquely defined by the sequence $\sigma_\alpha = \langle \sigma \mid \boldsymbol{x}^\alpha\rangle$ for $\alpha \in \mathbb{N}^n$. The coefficients $\sigma_\alpha = \langle \sigma \mid \boldsymbol{x}^\alpha\rangle$ for $\alpha \in \mathbb{N}^n$ are also called the *moments* of σ. Hereafter, we will identify $\mathbb{K}^{\mathbb{N}^n}$ with $\mathbb{K}[\boldsymbol{x}]^* = \mathrm{Hom}_{\mathbb{K}}(\mathbb{K}[\boldsymbol{x}],\mathbb{K})$.

The dual space $\mathbb{K}[\boldsymbol{x}]^*$ has a natural structure of $\mathbb{K}[\boldsymbol{x}]$-module, defined as follows: $\forall \sigma \in \mathbb{K}[\boldsymbol{x}]^*, \forall p,q \in \mathbb{K}[\boldsymbol{x}]$,

$$\langle p \star \sigma \mid q\rangle = \langle \sigma \mid pq\rangle.$$

We check that $\forall \sigma \in \mathbb{K}[\boldsymbol{x}]^*, \forall p,q \in \mathbb{K}[\boldsymbol{x}]$, $(pq)\star\sigma = p\star(q\star\sigma)$. See e.g. [15], [21] for more details.

For any $\sigma \in \mathbb{K}[\boldsymbol{x}]^*$, the inner product associated to σ on $\mathbb{K}[\boldsymbol{x}]$ is defined as follows:

$$\begin{aligned}\mathbb{K}[\boldsymbol{x}] \times \mathbb{K}[\boldsymbol{x}] &\to \mathbb{K}\\ (p,q) &\mapsto \langle p,q\rangle_\sigma := \langle \sigma | pq\rangle.\end{aligned}$$

Sequences in $\mathbb{K}^{\mathbb{N}^n}$ are also in correspondence with series in $\mathbb{K}[[\boldsymbol{z}]]$, via the so-called $\boldsymbol{z}$-transform:

$$\sigma = (\sigma_\alpha)_{\alpha\in\mathbb{N}^n} \in \mathbb{K}^{\mathbb{N}^n} \mapsto \sigma(\boldsymbol{z}) = \sum_{\alpha\in\mathbb{N}^n} \sigma_\alpha \boldsymbol{z}^\alpha \in \mathbb{K}[[\boldsymbol{z}]].$$

If $\mathbb{K}$ is a field of characteristic 0, we can identify the sequence $\sigma = (\sigma_\alpha)_{\alpha\in\mathbb{N}^n} \in \mathbb{K}^{\mathbb{N}^n}$ with the series $\sigma(\boldsymbol{y}) = \sum_{\alpha\in\mathbb{N}^n} \sigma_\alpha \frac{\boldsymbol{y}^\alpha}{\alpha!} \in \mathbb{K}[[\boldsymbol{y}]]$. Using this identification, we have $\forall p \in \mathbb{K}[\boldsymbol{x}], \forall \sigma \in \mathbb{K}[[\boldsymbol{y}]]$, $p \star \sigma(\boldsymbol{y}) = p(\partial_{y_1}, \ldots, \partial_{y_n})(\sigma(\boldsymbol{y}))$.

Through these identifications, the dual basis of the monomial basis $(\boldsymbol{x}^\alpha)_{\alpha\in\mathbb{N}^n}$ is $(\boldsymbol{z}^\alpha)_{\alpha\in\mathbb{N}^n}$ in $\mathbb{K}[[\boldsymbol{z}]]$ and $\left(\frac{\boldsymbol{y}^\alpha}{\alpha!}\right)_{\alpha\in\mathbb{N}^n}$ in $\mathbb{K}[[\boldsymbol{y}]]$.

Among the elements of $\mathrm{Hom}(\mathbb{K}[\boldsymbol{x}], \mathbb{K})$, we have the evaluation $\boldsymbol{e}_\xi : p(\boldsymbol{x}) \in \mathbb{K}[\boldsymbol{x}] \mapsto p(\xi) \in \mathbb{K}$ at a point $\xi \in \mathbb{K}^n$, which corresponds to the sequence $(\xi^\alpha)_{\alpha\in\mathbb{N}^n}$ or to the series $\boldsymbol{e}_\xi(\boldsymbol{z}) = \sum_{\alpha\in\mathbb{N}^n} \xi^\alpha \boldsymbol{z}^\alpha = \frac{1}{\prod_{i=1}^n (1-\xi_i z_i)} \in \mathbb{K}[[\boldsymbol{z}]]$, or to the series $\boldsymbol{e}_\xi(\boldsymbol{y}) = \sum_{\alpha\in\mathbb{N}^n} \xi^\alpha \frac{\boldsymbol{y}^\alpha}{\alpha!} = e^{\xi_1 y_1 + \cdots + \xi_n y_n} = e^{\langle \xi, \mathbf{y}\rangle}$ in $\mathbb{K}[[\boldsymbol{y}]]$. These series belong to the more general family $\mathcal{POLYEXP}$ of polynomial-exponential series $\sigma = \sum_{i=1}^r \omega_i \boldsymbol{e}_{\xi_i} \in \mathbb{K}[[\boldsymbol{y}]]$ with $\xi_i \in \mathbb{K}^n, \omega_i \in \mathbb{K}[\boldsymbol{y}]$. This set corresponds in $\mathbb{K}[[\boldsymbol{z}]]$ to the set of series of the form

$$\sigma = \sum_{i=1}^r \sum_{\alpha\in A_i} \frac{\omega_{i,\alpha} \boldsymbol{z}^\alpha}{\prod_{j=1}^n (1-\xi_{i,j} z_j)^{1+\alpha_j}}$$

with $\xi_i \in \mathbb{K}^n, \omega_{i,\alpha} \in \mathbb{K}, \alpha \in A_i \subset \mathbb{N}^n$ and A_i finite.

Definition 2.1. *For a subset $D \subset \mathbb{K}[[\boldsymbol{y}]]$, the* inverse system *generated by D is the vector space spanned by the elements $p \star \delta$ for $\delta \in D$, $p \in \mathbb{K}[\boldsymbol{x}]$, that is, by the elements in D and all their derivatives.*

For $\omega \in \mathbb{K}[\boldsymbol{y}]$, we denote by $\mu(\omega)$ the dimension of the inverse system of ω, generated by ω and all its derivatives. For $\sigma = \sum_{i=1}^r \omega_i \boldsymbol{e}_{\xi_i} \in \mathcal{POLYEXP}(\boldsymbol{y})$, $\mu(\sigma) = \sum_{i=1}^r \mu(\omega_i)$.

2.2. Hankel operators. The external product $\star$ allows us to define a Hankel operator as a multiplication operator by a dual element $\in \mathbb{K}[\boldsymbol{x}]^*$:

Definition 2.2. *The Hankel operator associated to an element $\sigma \in \mathbb{K}[\boldsymbol{x}]^* = \mathbb{K}^{\mathbb{N}^n}$ is*

$$\begin{aligned} H_\sigma : \mathbb{K}[\boldsymbol{x}] &\to \mathbb{K}[\boldsymbol{x}]^* \\ p = \sum_{\beta\in B} p_\beta \boldsymbol{x}^\beta &\mapsto p \star \sigma = \left(\sum_{\beta\in B} p_\beta \sigma_{\alpha+\beta}\right)_{\alpha\in\mathbb{N}^n}. \end{aligned}$$

Its kernel is denoted I_σ. We say that the series σ has finite rank $r \in \mathbb{N}$ if $\mathrm{rank}\, H_\sigma = r < \infty$.

As $\forall p, q \in \mathbb{K}[\boldsymbol{x}]$, $pq \star \sigma = p \star (q \star \sigma)$, we easily check that $I_\sigma = \ker H_\sigma$ is an ideal of $\mathbb{K}[\boldsymbol{x}]$ and that $\mathcal{A}_\sigma = \mathbb{K}[\boldsymbol{x}]/I_\sigma$ is an algebra.

Given a sequence $\sigma = (\sigma_\alpha)_{\alpha\in\mathbb{N}^n} \in \mathbb{K}^{\mathbb{N}^n}$, the kernel of H_σ is the set of polynomials $p = \sum_{\beta\in B} p_\beta \boldsymbol{x}^\beta$ such that $\sum_{\beta\in B} p_\beta \sigma_{\alpha+\beta} = 0$ for all $\alpha \in \mathbb{N}^n$. This kernel is the set of *linear recurrence relations* of the sequence $\sigma = (\sigma_\alpha)_{\alpha\in\mathbb{N}^n}$.

Remark 2.3. The matrix of the operator H_σ in the bases $(\boldsymbol{x}^\alpha)_{\alpha\in\mathbb{N}^n}$ and its dual basis $(\boldsymbol{z}^\alpha)_{\alpha\in\mathbb{N}^n}$ is

$$[H_\sigma] = (\sigma_{\alpha+\beta})_{\alpha,\beta\in\mathbb{N}^n} = (\langle \sigma | \boldsymbol{x}^{\alpha+\beta} \rangle)_{\alpha,\beta\in\mathbb{N}^n}.$$

The coefficients of $[H_\sigma]$ depend only the sum of the multi-indices indexing the rows and columns, which explains why it is called a *Hankel* operator.

In the reconstruction problem, we are dealing with truncated series with known coefficients σ_α for α in a subset $\boldsymbol{a}$ of $\mathbb{N}^n$. This leads to the definition of truncated Hankel operators.

Definition 2.4. *For two vector spaces $V, V' \subset \mathbb{K}[\boldsymbol{x}]$ and $\sigma \in \langle V \cdot V' \rangle^* \subset \mathbb{K}[\boldsymbol{x}]^*$, the* truncated Hankel operator *on (V, V'), denoted by $H_\sigma^{V,V'}$, is the following map:*

$$\begin{aligned} H_\sigma^{V,V'} : V &\to V'^* = \mathrm{Hom}_{\mathbb{K}}(V', \mathbb{K}) \\ p(\boldsymbol{x}) &\mapsto p \star \sigma_{|V'}. \end{aligned}$$

If $B = \{b_1, \ldots, b_r\}$ (resp. $B' = \{b'_1, \ldots, b'_r\}$) is a basis of V (resp. V'), then the matrix of the operator $H_\sigma^{V,V'}$ in B and the dual basis of B' is

$$[H_\sigma^{B,B'}] = (\langle \sigma | b_j b'_i \rangle)_{1 \leqslant i,j \leqslant r}.$$

If B and B' are monomial sets, we obtain the so-called *truncated moment matrix* of σ:

$$[H_\sigma^{B,B'}] = (\sigma_{\beta+\beta'})_{\beta' \in B', \beta \in B}$$

(identifying a monomial $\boldsymbol{x}^\beta$ with its exponent β). These structured matrices share with the classical univariate Hankel matrices many interesting properties (see e.g. in [23]).

2.3. Artinian Gorenstein algebra. A $\mathbb{K}$-algebra $\mathcal{A}$ is *Artinian* if $\dim_{\mathbb{K}}(\mathcal{A}) < \infty$. It can be represented as the quotient $\mathcal{A} = \mathbb{K}[\boldsymbol{x}]/I$ of a polynomial ring $\mathbb{K}[\boldsymbol{x}]$ by a (zero-dimension) ideal $I \subset \mathbb{K}[\boldsymbol{x}]$.

A classical result states that the quotient algebra $\mathcal{A} = \mathbb{K}[\boldsymbol{x}]/I$ is finite dimensional, i.e. Artinian, iff $\mathcal{V}_{\mathbb{K}}(I)$ is finite, that is, I defines a finite number of (isolated) points in $\bar{\mathbb{K}}^n$ (see e.g. [12][Theorem 6] or [14][Theorem 4.3]).

The dual $\mathcal{A}^* = \mathrm{Hom}_{\mathbb{K}}(\mathcal{A}, \mathbb{K})$ of $\mathcal{A} = \mathbb{K}[\boldsymbol{x}]/I$ is naturally identified with the sub-space

$$I^\perp = \{\sigma \in \mathbb{K}[\boldsymbol{x}]^* \mid \forall p \in I, \langle \sigma | p \rangle = 0\}.$$

A *Gorenstein* algebra is defined as follows:

Definition 2.5. *A $\mathbb{K}$-algebra $\mathcal{A}$ is Gorenstein if $\exists \sigma \in \mathcal{A}^* = \mathrm{Hom}_{\mathbb{K}}(\mathcal{A}, \mathbb{K})$ such that $\forall \rho \in \mathcal{A}^*, \exists a \in \mathcal{A}$ with $\rho = a \star \sigma$ and $a \star \sigma = 0$ implies $a = 0$.*

In other words, $\mathcal{A} = \mathbb{K}[\boldsymbol{x}]/I$ is Gorenstein iff $\mathcal{A}^* = \{p \star \sigma \mid p \in \mathbb{K}[\boldsymbol{x}]\} = \mathrm{im}\, H_\sigma$ and $p \star \sigma = 0$ implies $p \in I$. Equivalently, $\mathcal{A} = \mathbb{K}[\boldsymbol{x}]/I$ is Gorenstein iff there exists $\sigma \in \mathbb{K}[\boldsymbol{x}]^*$ such that we have the exact sequence:

$$0 \to I \to \mathbb{K}[\boldsymbol{x}] \xrightarrow{H_\sigma} \mathcal{A}^* \to 0 \tag{1}$$

so that H_σ induces an isomorphism between $\mathcal{A} = \mathbb{K}[\boldsymbol{x}]/I$ and $\mathcal{A}^*$. In other words, a Gorenstein algebra $\mathcal{A}$ is the quotient of a polynomial ring by the kernel of a Hankel operator, or equivalently by an ideal of recurrence relations of a multi-index sequence.

An Artinian Gorenstein can thus be described by an element $\sigma \in \mathbb{K}[\boldsymbol{x}]^*$, such that $\mathrm{rank}\, H_\sigma = \dim \mathcal{A}^* = \dim \mathcal{A}$ is finite. In the following, we will assume that the Artinian Gorenstein algebra is given by such an element $\sigma \in \mathbb{K}[\boldsymbol{x}]^* \equiv \mathbb{K}^{\mathbb{N}^n}$. The corresponding algebra will be $\mathcal{A}_\sigma = \mathbb{K}[\boldsymbol{x}]/I_\sigma$ where $I_\sigma = \ker H_\sigma$.

By a multivariate generalization of Kronecker's theorem [22][Theorem 3.1], the sequences σ such that $\mathrm{rank}\, H_\sigma = r < \infty$ are the polynomial-exponential series $\sigma \in \mathcal{POLYEXP}$ with $\mu(\sigma) = r$.

The aim of the method we are presenting, is to compute the structure of the Artinian Gorenstein algebra $\mathcal{A}_\sigma$ from the first terms of the sequence $\sigma = (\sigma_\alpha)_{\alpha \in \mathbb{N}^n}$. We are going to determine bases of $\mathcal{A}_\sigma$ and generators of the ideal I_σ, from which we can deduce directly the multiplicative structure of $\mathcal{A}_\sigma$.

The following lemma gives a simple way to test the linear independency in $\mathcal{A}_\sigma$ using truncated Hankel matrices (see [22][Lemma 3.3]):

Lemma 2.6. *Let $\sigma \in \mathbb{K}[\boldsymbol{x}]^*$, $B = \{b_1, \ldots, b_r\}$, $B' = \{b'_1, \ldots, b'_r\} \subset \mathbb{K}[\boldsymbol{x}]$. If the matrix $H_\sigma^{B,B'} = (\langle \sigma | b_i b'_j \rangle)_{\in B, \beta' \in B'}$ is invertible, then B (resp. B') is linearly independent in $\mathcal{A}_\sigma$.*

This lemma implies that if $\dim \mathcal{A}_\sigma = r < +\infty$, $|B| = |B'| = r = \dim \mathcal{A}_\sigma$ and $H_\sigma^{B,B'}$ is invertible, then $(\boldsymbol{x}^\beta)_{\beta \in B}$ and $(\boldsymbol{x}^{\beta'})_{\beta' \in B'}$ are bases of $\mathcal{A}_\sigma$.

Given a Hankel operator H_σ of finite rank r, it is clear that the truncated operators will have at most rank r. We are going to use the so-called *flat extension* property, which gives conditions under which a truncated Hankel operator of rank r can be extended to a Hankel operator of the same rank (see [19] and extensions [10], [6], [22]).

THEOREM 2.7. *Let $V, V' \subset \mathbb{K}[\boldsymbol{x}]$ be vector spaces connected to 1, such that $x_1, \ldots, x_n \in V$ and let $\sigma \in \langle V \cdot V' \rangle^*$. Let $B \subset V$, $B' \subset V'$ such that $B^+ \subset V, B'^+ \subset V'$. If $\operatorname{rank} H_\sigma^{V,V'} = \operatorname{rank} H_\sigma^{B,B'} = r$, then there is a unique extension $\tilde{\sigma} \in \mathbb{K}[[\boldsymbol{y}]]$ such that $\tilde{\sigma}$ coincides with σ on $\langle V \cdot V' \rangle$ and $\operatorname{rank} H_{\tilde{\sigma}} = r$. In this case, $\tilde{\sigma} \in \mathcal{POLYEXP}$ with $r = \mu(\sigma)$ and $I_{\tilde{\sigma}} = (\ker H_\sigma^{B^+,B'})$.*

2.4. Border bases. We recall briefly the definition of border basis and the main properties, that we will need. Let B be a monomial set of $\mathbb{K}[\boldsymbol{x}]$.

DEFINITION 2.8. *A rewriting family F for a (monomial) set B is a set of polynomials $F = \{f_i\}_{i \in \boldsymbol{i}} \subset \mathbb{K}[\boldsymbol{x}]$ such that $f_i = \boldsymbol{x}^{\alpha_i} + b_i$ with $b_i \in \langle B \rangle$, $\alpha_i \in \partial B$, $\alpha_i \neq \alpha_j$ if $i \neq j$. The rewriting family f is complete if $(\boldsymbol{x}^{\alpha_i})_{i \in \boldsymbol{i}} = \partial B$.*

The monomial $\boldsymbol{x}^{\alpha_i}$ is called the leading monomial of f_i and denoted $\gamma(f_i)$.

DEFINITION 2.9. *A family $F \subset \mathbb{K}[\boldsymbol{x}]$ is a border basis with respect to B if it is a complete rewriting family for B such that $\mathbb{K}[\boldsymbol{x}] = \langle B \rangle \oplus (F)$.*

This means that any element of $\mathbb{K}[\boldsymbol{x}]$ can be projected along the ideal $I = (F)$ onto a unique element of $\langle B \rangle$. In other words, B is a basis of the quotient algebra $\mathcal{A} = \mathbb{K}[\boldsymbol{x}]/I$.

Let $B^{[0]} = B$ and for $k \in \mathbb{N}$, $B^{[k+1]} = (B^{[k]})^+$. If $1 \in B$, then for any $p \in \mathbb{K}[\boldsymbol{x}]$, there exist $k \in \mathbb{N}$, such that $p \in \langle B^{[k]} \rangle$.

For a complete rewriting family F with respect to a monomial set B containing 1, a projection π_F of $\mathbb{K}[\boldsymbol{x}]$ on $\langle B \rangle$ can be defined recursively on the set of monomials m of $\mathbb{K}[\boldsymbol{x}]$ by

- if $m \in B$, $\pi_F(m) = m$;
- if $m \in \partial B$, $\pi_F(m) = m - f$ where f is the (unique) polynomial in F for which $\gamma(f) = m$,
- if $m \in B^{[k+1]} - B^{[k]}$ for $k > 1$, there exists $m' \in B^{[k]}$ and $i_0 \in [1, n]$ such that $m = x_{i_0} m'$. Let $\pi_F(m) = \pi_F(x_{i_0} \pi_F(m'))$.

This map defines a projector from $\mathbb{K}[\boldsymbol{x}]$ onto $\langle B \rangle$. The kernel of π_F is contained in the ideal (F). The family F is a border basis iff $\ker(\pi_F) = (F)$.

Checking that a complete rewriting family is a border basis reduces to checking commutation properties. This leads to efficient algorithms to compute a border basis. For more details, see [24], [25], [26].

A special case of border basis is when the leading term $\gamma(f)$ of $f \in F$ is the maximal monomial of f for a monomial ordering $\succ$. Then F is a Gröbner basis of I for this monomial ordering $\succ$.

A border basis F with respect to a monomial set B gives directly the tables of multiplication M_i by the variables x_i in the basis B. For a monomial $b \in B$, $M_i(b) = \pi_F(x_i b) = x_i b - f$ with$f \in F$ such that $\gamma(f) = x_i b$ if $x_i b \in \partial B$ and $f = 0$ otherwise.

3. Border bases of series. Given the first terms σ_α for $\alpha \in \boldsymbol{a}$ of the sequence $\sigma = (\sigma_\alpha)_{\alpha \in \mathbb{N}^n} \in \mathbb{K}^{\mathbb{N}^n}$, where $\boldsymbol{a} \subset \mathbb{N}^n$ is a finite set of exponents, we are going to compute a basis of $\mathcal{A}_\sigma$ and generators of I_σ. We assume that the monomial set $\boldsymbol{x}^{\boldsymbol{a}} = \{\boldsymbol{x}^\alpha, \alpha \in \boldsymbol{a}\}$ is connected to 1.

3.1. Orthogonal bases of $\mathcal{A}_\sigma$. An important step in the decomposition method consists in computing a basis B of $\mathcal{A}_\sigma$. In this section, we describe how to compute a monomial basis $B = \{\boldsymbol{x}^\beta\}$ and two other bases $\boldsymbol{p} = (p_\beta)$ and $\boldsymbol{q} = (q_\beta)$, which are pairwise orthogonal for the inner product $\langle \cdot, \cdot \rangle_\sigma$:

$$\langle p_\beta, q_{\beta'} \rangle_\sigma = \begin{cases} 1 & \text{if } \beta = \beta' \\ 0 & \text{otherwise}. \end{cases}$$

To compute these pairwise orthogonal bases, we will use a projection process, similar to Gram-Schmidt orthogonalization process. The main difference is that we compute pairs p_β, q_β of orthogonal polynomials. As the inner product $\langle \cdot, \cdot \rangle_\sigma$ may be isotropic, the two polynomials p_β, q_β may not be equal, up to a scalar. For a polynomial f and two families of polynomials $\boldsymbol{p} = [p_1, \ldots, p_l]$, $\boldsymbol{m} = [m_1, \ldots, m_l]$, we will use the following procedure $\operatorname{proj}(f, \boldsymbol{p}, \boldsymbol{m})$.

Algorithm 1 Orthogonal projection

Input: $f \in \mathbb{K}[\boldsymbol{x}]$, $\boldsymbol{p} = [p_1, \ldots, p_l]$ and $\boldsymbol{m} = [m_1, \ldots, m_l]$ such that $\langle p_i, m_j\rangle_\sigma = 0$ if $j < i$ and $\langle p_i, m_i\rangle_\sigma = 1$.

- $g = f$;
- for i in $1 \ldots l$ do $g -= \langle g, m_i\rangle_\sigma p_i$;

Output: $g := \mathrm{proj}(f, \boldsymbol{p}, \boldsymbol{m})$

Algorithm 1 corresponds to the Modified Gram-Schmidt algorithm, when the scalar product is definite positive. It is known to have a better numerical behavior than the direct Gram-Schmidt orthogonalization process [34][Lecture 8]. It computes the polynomial $\mathrm{proj}(f, \boldsymbol{p}, \boldsymbol{m})$ characterized by the following lemma.

LEMMA 3.1. *If $\langle p_i, m_j\rangle_\sigma = 0$ if $j < i$ and $\langle p_i, m_i\rangle_\sigma = 1$, there is a unique polynomial g such that $g = f - \sum_{i=1}^{l} \lambda_i p_i$ with $\lambda_i \in \mathbb{K}$ and $\langle g, m_i\rangle_\sigma = 0$ for $i = 1, \ldots, l$.*

Proof. We prove by induction on the index i of the loop that g is orthogonal to $[m_1, \ldots, m_i]$. For $i = 1$, $g = f - \langle f, m_1\rangle_\sigma p_1$ is such that $\langle g, m_1\rangle_\sigma = \langle f, m_1\rangle_\sigma - \langle f, m_1\rangle_\sigma \langle p_1, m_1\rangle_\sigma = 0$.

If the property is true at step $k \leqslant l$, i.e. $\langle g, m_i\rangle_\sigma = 0$ for $i < k$, then $g' = g - \langle g, m_k\rangle_\sigma p_k$ is such that $\langle g, m_i\rangle_\sigma - \langle g, m_k\rangle_\sigma \langle p_k, m_i\rangle_\sigma = \langle g, m_i\rangle_\sigma = 0$ by induction hypothesis. By construction, $\langle g', m_k\rangle = \langle g, m_k\rangle_\sigma - \langle g, m_k\rangle_\sigma \langle p_k, m_k\rangle_\sigma = 0$ and the induction hypothesis is true for k. As the matrix $(\langle p_{\mathrm{ij}}, m_i\rangle_\sigma)_{1 \leqslant i,j \leqslant l}$ is invertible, there exists a unique polynomial of the form $g = f - \sum_{j=1}^{l} \lambda_j p_j$, such that $\langle g, m_i\rangle_\sigma = 0$ for $i = 1, \ldots, l$, which concludes the proof of the lemma. □

Algorithm 2 for computing a border basis of $\mathcal{A}_\sigma$ proceeds inductively, starting from $\boldsymbol{p} = [], \boldsymbol{m} = [], \boldsymbol{b} = []$, extending the basis $\boldsymbol{p}$ with a new polynomial p_α, orthogonal to the vector space spanned by $\boldsymbol{m}$ for the inner product $\langle \cdot, \cdot\rangle_\sigma$, extending $\boldsymbol{m}$ with a new monomial m_α, such that $\langle p_\alpha, m_\alpha\rangle_\sigma = 1$ and $\langle p_\beta, m_\alpha\rangle = 0$ for $\beta \in \boldsymbol{b}$ and extending $\boldsymbol{b}$ with α.

Algorithm 2 Artinian Gorenstein border basis

Input: the coefficients σ_α of a series $\sigma \in \mathbb{K}[[\boldsymbol{y}]]$ for $\alpha \in \boldsymbol{a} \subset \mathbb{N}^n$ with $\boldsymbol{a}$ a finite set of exponents connected to $\mathbf{0}$.

- Let $\boldsymbol{b} := []$; $\boldsymbol{c} := []$; $\boldsymbol{d} = []$; $\boldsymbol{n} := [\mathbf{0}]$; $\boldsymbol{s} := \boldsymbol{a}$; $\boldsymbol{t} := \boldsymbol{a}$;
- while $\boldsymbol{n} \neq \emptyset$ do
  - for each $\alpha \in \boldsymbol{n}$,
    - a) $p_\alpha := \mathrm{proj}(\boldsymbol{x}^\alpha, [p_\beta]_{\beta \in \boldsymbol{b}}, [m_\beta]_{\beta \in \boldsymbol{b}})$;
    - b) find the first $\gamma \in \boldsymbol{t}$ such that $\boldsymbol{x}^\gamma p_\alpha \in \langle \boldsymbol{x}^{\boldsymbol{a}} \rangle$ and $\langle p_\alpha, \boldsymbol{x}^\gamma\rangle_\sigma \neq 0$;
    - c) if such a γ exists then
      let $m_\alpha := \frac{1}{\langle p_\alpha, \boldsymbol{x}^\gamma\rangle_\sigma} \boldsymbol{x}^\gamma$;
      `[optional]` let $q_\alpha := \mathrm{proj}(m_\alpha, [q_\beta]_{\beta \in \boldsymbol{b}}, [p_\beta]_{\beta \in \boldsymbol{b}})$;
      add α to $\boldsymbol{b}$; remove α from $\boldsymbol{s}$;
      add γ to $\boldsymbol{c}$; remove γ from $\boldsymbol{t}$;
      else
      let $k_\alpha = p_\alpha$;
      add α to $\boldsymbol{d}$; remove α from $\boldsymbol{s}$;
      end;
  - $\boldsymbol{n} := \mathrm{next}(\boldsymbol{b}, \boldsymbol{d}, \boldsymbol{c}, \boldsymbol{s})$;

Output:

- exponent sets $\boldsymbol{b} = [\beta_1, \ldots, \beta_r]$, $\boldsymbol{c} = [\gamma_1, \ldots, \gamma_r]$.
- bases $\boldsymbol{p} = [p_{\beta_i}]$, `[optional]` $\boldsymbol{q} = [q_{\beta_i}]$.
- the relations $\boldsymbol{k} = [p_\alpha]_{\alpha \in \boldsymbol{d}}$ where $p_\alpha = \boldsymbol{x}^\alpha - \sum_{i=1}^{r} \lambda_{\beta_i} p_{\beta_i}$ for $\alpha \in \boldsymbol{d}$.

The main difference with Algorithm 4.1 in [22] is the projection procedure and the list of monomials $\boldsymbol{s}$, $\boldsymbol{t}$ used to generate new monomials and to perform the projections. The lists $\boldsymbol{b}, \boldsymbol{d}, \boldsymbol{c}, \boldsymbol{s}, \boldsymbol{t}$ are lists of exponents, identified with monomials.

We verify that at each loop of the algorithm, the lists $\boldsymbol{b}$, $\boldsymbol{d}$ and $\boldsymbol{s}$ are disjoint and $\boldsymbol{b} \cup \boldsymbol{d} \cup \boldsymbol{s} = \boldsymbol{a}$.

We also verify that m_α are monomials up to a scalar, that the set of their exponents is $\boldsymbol{c}$, that $\boldsymbol{c}$ and $\boldsymbol{t}$ are disjoint and that $\boldsymbol{c} \cup \boldsymbol{t} = \boldsymbol{a}$.

The algorithm uses the function next$(\boldsymbol{b}, \boldsymbol{d}, \mathbf{c}, \boldsymbol{s})$, which computes the set of monomials $\mathfrak{n}$ in $\partial\boldsymbol{b} \cap \boldsymbol{s}$, which are not in $\boldsymbol{d}$ and such $\mathfrak{n} \cdot \mathbf{c} \subset \mathbf{a} = \boldsymbol{b} \cup \boldsymbol{d} \cup \boldsymbol{s}$.

We denote by $\prec$ the order induced by the treatment of the monomials of $\boldsymbol{a}$ in the loops of the algorithm, so that the monomials treated at the l^{th} loop are smaller than the monomials in $\boldsymbol{n}$ at the $(l+1)^{\text{th}}$ loop. For $\alpha \in \boldsymbol{a}$, we denote by $\boldsymbol{b}_{\prec\alpha}$ the list of monomial exponents $\beta \in \boldsymbol{b}$ with $\beta \prec \alpha$ and by $B_{\prec\alpha}$ the vector space spanned by these monomials. For $\alpha \in \boldsymbol{b}$, let $\boldsymbol{b}_{\preccurlyeq\alpha} = \boldsymbol{b}_{\prec\alpha} \cup [\alpha]$.

The following properties are also satisfied during this algorithm:

LEMMA 3.2. *For $\alpha \in \boldsymbol{b}$, we have $\forall \beta \in \boldsymbol{b}_{\prec\alpha}$, $\langle p_\alpha, m_\beta\rangle_\sigma = 0$ and $\langle p_\alpha, m_\alpha\rangle_\sigma = 1$. For $\alpha \in \boldsymbol{d}$, $\langle p_\alpha, \boldsymbol{x}^\gamma\rangle_\sigma = 0$ for all $\gamma \in \boldsymbol{a}$ such that $\boldsymbol{x}^\gamma p_\alpha \in \langle \boldsymbol{x}^{\boldsymbol{a}}\rangle$.*

Proof. By construction,

$$p_\alpha = \text{proj}(\boldsymbol{x}^\alpha, [p_\beta]_{\beta\in\boldsymbol{b}_{\prec\alpha}}, [m_\beta]_{\beta\in\boldsymbol{b}_{\prec\alpha}})$$

is orthogonal to m_β for $\beta \in \boldsymbol{b}_{\prec\alpha}$. We consider two exclusive cases: $\alpha \in \boldsymbol{b}$ and $\alpha \in \boldsymbol{d}$.

- If $\alpha \in \boldsymbol{b}$, then there exists $\boldsymbol{x}^\gamma \in \boldsymbol{s}$ such that $\langle p_\alpha, \boldsymbol{x}^\gamma\rangle_\sigma \neq 0$. Thus $m_\alpha = \frac{1}{\langle p_\alpha, \boldsymbol{x}^\gamma\rangle_\sigma}\boldsymbol{x}^\gamma$ is such that $\langle p_\alpha, m_\alpha\rangle_\sigma = 1$. By construction, $\langle p_\alpha, m_\beta\rangle_\sigma = 0$ for $\beta \in \boldsymbol{b}_{\prec\alpha}$.
- If $\alpha \in \boldsymbol{d}$, then there is no $\boldsymbol{x}^\gamma \in \boldsymbol{s}$ such that $\langle p_\alpha, \boldsymbol{x}^\gamma\rangle_\sigma \neq 0$ and $\boldsymbol{x}^\gamma p_\alpha \in \langle \boldsymbol{x}^{\boldsymbol{a}}\rangle$. Thus p_α is orthogonal to $\boldsymbol{x}^\gamma$ for all $\gamma \in \boldsymbol{s}$ with $\boldsymbol{x}^\gamma p_\alpha \in \langle \boldsymbol{x}^{\boldsymbol{a}}\rangle$. By construction, p_α is orthogonal to m_β for $\beta \in \boldsymbol{b}$. As $\boldsymbol{b} \cup \boldsymbol{s} = \boldsymbol{a}$, $\langle p_\alpha, \boldsymbol{x}^\gamma\rangle_\sigma = 0$ for all $\gamma \in \boldsymbol{a}$ such that $\boldsymbol{x}^\gamma p_\alpha \in \langle \boldsymbol{x}^{\boldsymbol{a}}\rangle$.

This concludes the proof of this lemma. ∎

LEMMA 3.3. *For $\alpha \in \boldsymbol{b}$, $\langle m_\beta\rangle_{\beta\in\boldsymbol{b}_{\preccurlyeq\alpha}} = \langle q_\beta\rangle_{\beta\in\boldsymbol{b}_{\preccurlyeq\alpha}}$ and the bases $\boldsymbol{p} = [p_\beta]_{\beta\in\boldsymbol{b}_{\preccurlyeq\alpha}}, \boldsymbol{q} = [q_\beta]_{\beta\in\boldsymbol{b}_{\preccurlyeq\alpha}}$ are pairwise orthogonal.*

Proof. We prove it by induction on α. If $\alpha = \mathbf{0}$ is not in $\boldsymbol{b}$, then $\sigma_\alpha = 0$ for all $\alpha \in \boldsymbol{a}$, $\boldsymbol{p}$ and $\boldsymbol{q}$ are empty and the property is satisfied. If $\alpha = \mathbf{0}$ is in $\boldsymbol{b}$, then $p_\alpha = 1$ and $q_\alpha = m_\alpha$ is such that $\langle p_\alpha, m_\alpha\rangle_\sigma = 1$. The property is true for $\alpha = \mathbf{0}$.

Suppose that it is true for all $\beta \in \boldsymbol{b}_{\prec\alpha}$. By construction, the polynomial $q_\alpha = \text{proj}(m_\alpha, [q_\beta]_{\beta\in\boldsymbol{b}_{\prec\alpha}}, [p_\beta]_{\beta\in\boldsymbol{b}_{\prec\alpha}})$ is orthogonal to p_β for $\beta \prec \alpha$. By induction hypothesis, $[p_\beta]_{\beta\in\boldsymbol{b}_{\prec\alpha}}, \boldsymbol{q} = [q_\beta]_{\beta\in\boldsymbol{b}_{\prec\alpha}}$ are pairwise orthogonal, thus

$$q_\alpha = m_\alpha - \sum_{\beta\in\boldsymbol{b}_{\prec\alpha}} \langle p_\beta, m_\alpha\rangle_\sigma q_\beta.$$

By the induction hypothesis, we deduce that

$$\begin{aligned}\langle m_\beta\rangle_{\beta\in\boldsymbol{b}_{\preccurlyeq\alpha}} &= \langle m_\beta\rangle_{\beta\in\boldsymbol{b}_{\prec\alpha}} + \langle m_\alpha\rangle = \langle q_\beta\rangle_{\beta\in\boldsymbol{b}_{\prec\alpha}} + \langle m_\alpha\rangle \\ &= \langle q_\beta\rangle_{\beta\in\boldsymbol{b}_{\prec\alpha}} + \langle q_\alpha\rangle = \langle q_\beta\rangle_{\boldsymbol{b}_{\preccurlyeq\alpha}}.\end{aligned}$$

By Lemma 10, p_α is orthogonal to m_β for $\beta \in \boldsymbol{b}_{\prec\alpha}$ and thus to q_β for $\beta \in \boldsymbol{b}_{\prec\alpha}$. We deduce that

$$\begin{aligned}\langle p_\alpha, q_\alpha\rangle_\sigma &= \langle p_\alpha, m_\alpha\rangle_\sigma - \sum_{\beta\in\boldsymbol{b}_{\prec\alpha}} \langle p_\beta, m_\alpha\rangle_\sigma \langle p_\alpha, q_\beta\rangle_\sigma \\ &= \langle p_\alpha, m_\alpha\rangle_\sigma = 1.\end{aligned}$$

This shows that $[p_\beta]_{\beta\in\boldsymbol{b}_{\preccurlyeq\alpha}}$ and $\boldsymbol{q} = [q_\beta]_{\beta\in\boldsymbol{b}_{\preccurlyeq\alpha}}$ are pairwise orthogonal and concludes the proof by induction. ∎

LEMMA 3.4. *At the l^{th} loop of the algorithm, the polynomials p_α for $\alpha \in \boldsymbol{n}$ are of the form $p_\alpha = \boldsymbol{x}^\alpha + b_\alpha$ with $b_\alpha \in B_{\prec\alpha}$.*

Proof. We prove by induction on the loop index l that we have $p_\alpha = \boldsymbol{x}^\alpha + b_\alpha$ with $b_\alpha \in B_{\prec\alpha}$.

The property is clearly true for $l = 0$, $\alpha = \mathbf{0}$ and $p_\alpha = 1 = \boldsymbol{x}^{\mathbf{0}}$. Suppose that it is true for any $l' < l$ and consider the l^{th} loop of the algorithm. The polynomial p_α is constructed by projection of $\boldsymbol{x}^\alpha$ on $\langle p_\alpha\rangle_{\beta\in\boldsymbol{b}}$ orthogonally to $\langle m_\beta\rangle_{\beta\in\boldsymbol{b}}$ where $\boldsymbol{b} = \boldsymbol{b}_{\prec\alpha}$. By induction hypothesis, $p_\beta = \boldsymbol{x}^\beta + b_\beta$ with $b_\beta \in B_{\prec\beta} \subset B_{\prec\alpha}$. Then by Lemma 9, we have

$$p_\alpha = \boldsymbol{x}^\alpha + \sum_{\beta\prec\alpha} \lambda_\beta p_\beta = \boldsymbol{x}^\alpha + b_\alpha$$

with $\lambda_\beta \in \mathbb{K}$, $b_\alpha \in B_{\prec\alpha}$. Thus, the induction hypothesis is true for l, which concludes the proof. □

3.2. Quotient algebra structure. We show now that the algorithm outputs a border basis of an Artinian Gorenstein algebra $\mathcal{A}_{\tilde\sigma}$ for an extension $\tilde\sigma$ of σ, when all the border relations are computed, that is, when $\boldsymbol{d} = \partial\boldsymbol{b}$.

THEOREM 3.5. *Let $\boldsymbol{b} = [\beta_1, \ldots, \beta_r]$, $\boldsymbol{c} = [\gamma_1, \ldots, \gamma_r]$, $\boldsymbol{p} = [p_{\beta_1}, \ldots, p_{\beta_r}]$, $\boldsymbol{q} = [q_{\beta_1}, \ldots, q_{\beta_r}]$ and $\boldsymbol{k} = [p_{\alpha_1}, \ldots, p_{\alpha_s}]$ be the output of Algorithm 2. Let $V = \langle \boldsymbol{x}^{\boldsymbol{b}^+} \rangle$. If $\boldsymbol{d} = \partial\boldsymbol{b}$ and $\boldsymbol{c}^+ \subset \boldsymbol{b}'$ connected to 1 such that $\boldsymbol{x}^{\boldsymbol{b}^+} \cdot \boldsymbol{x}^{\boldsymbol{b}'} = \boldsymbol{x}^{\boldsymbol{a}}$ then σ coincides on $\langle \boldsymbol{x}^{\boldsymbol{a}} \rangle$ with a series $\tilde\sigma \in \mathbb{K}[[\boldsymbol{y}]]$ such that*

- $\operatorname{rank} H_{\tilde\sigma} = r$,
- *$(\boldsymbol{p}, \boldsymbol{q})$ are pairwise orthogonal bases of $\mathcal{A}_{\tilde\sigma}$ for the inner product $\langle \cdot, \cdot \rangle_{\tilde\sigma}$,*
- *The family $\boldsymbol{k} = \{p_\alpha, \alpha \in \partial\boldsymbol{b}\}$ is a border basis of the ideal $I_{\tilde\sigma}$, with respect to $\boldsymbol{x}^{\boldsymbol{b}}$.*
- *The matrix of multiplication by x_k in the basis $\boldsymbol{p}$ (resp. $\mathbf{q}$) of $\mathcal{A}_{\tilde\sigma}$ is $M_k := (\langle \sigma | x_k p_{\beta_j} q_{\beta_i} \rangle)_{1 \leqslant i,j \leqslant r}$ (resp. M_k^t).*

Proof. By construction, $\boldsymbol{x}^{\boldsymbol{b}^+}$ is connected to 1. Let $V = \langle \boldsymbol{x}^{\boldsymbol{b}^+} \rangle$ and $V' = \langle \boldsymbol{x}^{\boldsymbol{b}'} \rangle$. As $\boldsymbol{b}^+ = \boldsymbol{b} \cup \boldsymbol{d}$, a basis of V is formed by the monomials $\boldsymbol{x}^{\boldsymbol{b}}$ and the polynomials $p_\alpha = \boldsymbol{x}^\alpha + b_\alpha$ with $b_\alpha \in \langle \boldsymbol{x}^{\boldsymbol{b}} \rangle$ for $\alpha \in \boldsymbol{d}$. The matrix of $H_\sigma^{V,V'}$ in this basis of V and a basis of V', which first elements are $m_{\beta_1}, \ldots, m_{\beta_r}$, is of the form

$$H_\sigma^{V,V'} = \begin{pmatrix} L_r & 0 \\ * & 0 \end{pmatrix}$$

where L_r is a lower triangular invertible matrix of size r. The kernel of $H_\sigma^{V,V'}$ is generated by the polynomials p_α for $\alpha \in \boldsymbol{d}$.

By Theorem 6, σ coincides on $V \cdot V' = \langle \boldsymbol{x}^{\boldsymbol{a}} \rangle$ with a series $\tilde\sigma$ such that $\boldsymbol{x}^{\boldsymbol{b}}$ is a basis of $\mathcal{A}_{\tilde\sigma} = \mathbb{K}[\boldsymbol{x}]/I_{\tilde\sigma}$ and $I_{\tilde\sigma} = (\ker H_{\tilde\sigma}^{V,V'}) = (p_\alpha)_{\alpha \in \boldsymbol{d}}$.

By Lemma 12, $p_\alpha = \boldsymbol{x}^\alpha + b_\alpha$ with $\alpha \in \partial\boldsymbol{b}$ and $b_\alpha \in \langle \boldsymbol{x}^{\boldsymbol{b}} \rangle$. Thus $(p_\alpha)_{\alpha \in \partial\boldsymbol{b}}$ is a border basis with respect to $\boldsymbol{x}^{\boldsymbol{b}}$ for the ideal $I_{\tilde\sigma}$, since $\boldsymbol{x}^{\boldsymbol{b}}$ is a basis of of $\mathcal{A}_{\tilde\sigma}$. This shows that $\operatorname{rank} H_{\tilde\sigma} = \dim \mathcal{A}_{\tilde\sigma} = |\boldsymbol{b}| = r$.

By Lemma 11, $(\boldsymbol{p}, \boldsymbol{q})$ are pairwise orthogonal for the inner product $\langle \cdot, \cdot \rangle_\sigma$, which coincides with $\langle \cdot, \cdot \rangle_{\tilde\sigma}$ on $\langle \boldsymbol{x}^{\boldsymbol{a}} \rangle$. Thus they are pairwise orthogonal bases of $\mathcal{A}_{\tilde\sigma}$ for the inner product $\langle \cdot, \cdot \rangle_{\tilde\sigma}$.

As we have $x_k p_{\beta_j} \equiv \sum_{i=1}^r \langle x_k p_{\beta_j}, q_{\beta_i} \rangle_\sigma p_{\beta_i}$, the matrix of multiplication by x_k in the basis $\boldsymbol{p}$ of $\mathcal{A}_{\tilde\sigma}$ is

$$M_k := (\langle x_k p_{\beta_j}, q_{\beta_i} \rangle_\sigma)_{1 \leqslant i,j \leqslant r} = (\langle \sigma | x_k p_{\beta_j} q_{\beta_i} \rangle)_{1 \leqslant i,j \leqslant r}.$$

Exchanging the role of $\mathbf{p}$ and $\mathbf{q}$, we obtain M_k^t for the matrix of multiplication by x_k in the basis $\boldsymbol{q}$. □

LEMMA 3.6. *If $\prec$ is a monomial ordering and if at the end of the algorithm $\boldsymbol{d} = \partial\boldsymbol{b}$ and $\boldsymbol{c}^+ \subset \boldsymbol{b}'$ connected to 1 with $\boldsymbol{x}^{\boldsymbol{b}^+} \cdot \boldsymbol{x}^{\boldsymbol{b}'} = \boldsymbol{x}^{\boldsymbol{a}}$, then $\boldsymbol{b} = \boldsymbol{c}$ and $\boldsymbol{k}$ is a Gröbner basis of the ideal I_σ for the monomial ordering.*

Proof. If $\prec$ is a monomial ordering, then the polynomials $p_\alpha = \boldsymbol{x}^\alpha + b_\alpha$, $\alpha \in \partial\boldsymbol{b}$ are constructed in such a way that their leading term is $\boldsymbol{x}^\alpha$. Therefore the border basis $\boldsymbol{k} = (p_\alpha)_{\alpha \in \partial\boldsymbol{b}}$ is also a Gröbner basis.

By construction, $\boldsymbol{c}$ is the set of monomials $\gamma \in \boldsymbol{a}$ such that $\langle p_\beta, \boldsymbol{x}^\gamma \rangle_\sigma \neq 0$ for some $\beta \in \boldsymbol{b}$. Suppose that $\gamma \in \boldsymbol{c}$ is not in $\boldsymbol{b}$. Then $\boldsymbol{x}^\gamma \in (\boldsymbol{x}^{\boldsymbol{d}})$ and there is $\delta \in \boldsymbol{d}$ and $\gamma' \in \boldsymbol{a}$ such that $\gamma = \delta + \gamma'$. As $p_\delta \in \boldsymbol{k}$, we have $\langle p_\delta, \boldsymbol{x}^\alpha \rangle_\sigma = 0$ for $\alpha \in \boldsymbol{a}$ such that $p_\delta \boldsymbol{x}^\alpha \in \langle \boldsymbol{x}^{\boldsymbol{a}} \rangle$. By Lemma 12, $p_\delta = \boldsymbol{x}^\delta + b_\delta$ with $b_\delta \in \boldsymbol{b}_{\prec\delta}$ with $\boldsymbol{x}^\delta \succ b_\delta$.

$$\langle p_\beta, \boldsymbol{x}^\gamma \rangle_\sigma = \langle p_\beta, \boldsymbol{x}^\delta \boldsymbol{x}^{\gamma'} \rangle_\sigma = \langle p_\beta, p_\delta \boldsymbol{x}^{\gamma'} \rangle_\sigma - \langle p_\beta, b_\delta \boldsymbol{x}^{\gamma'} \rangle_\sigma.$$

We have $\langle p_\beta, p_\delta \boldsymbol{x}^{\gamma'} \rangle_\sigma = \langle p_\delta, p_\beta \boldsymbol{x}^{\gamma'} \rangle_\sigma = 0$ since $p_\delta \in \boldsymbol{k}$ and $p_\delta p_\beta \boldsymbol{x}^{\gamma'} \in \langle \boldsymbol{x}^{\boldsymbol{a}} \rangle$. As γ is the first monomial of $\boldsymbol{a}$ such that $\langle p_\beta, \boldsymbol{x}^\gamma \rangle_\sigma \neq 0$ and $b_\delta \boldsymbol{x}^{\gamma'} \prec \boldsymbol{x}^{\delta+\gamma'} = \boldsymbol{x}^\gamma$, we have $\langle p_\beta, b_\delta \boldsymbol{x}^{\gamma'} \rangle_\sigma$, which implies that $\langle p_\beta, \boldsymbol{x}^\gamma \rangle_\sigma = 0$. This is in contradiction with the hypothesis $\langle p_\beta, \boldsymbol{x}^\gamma \rangle_\sigma \neq 0$, therefore $\gamma \in \boldsymbol{b}$. We deduce that $\boldsymbol{c} \subset \boldsymbol{b}$ and the equality holds since the two sets have the same cardinality. □

Notice that to construct a minimal reduced Gröbner basis of $I_{\tilde\sigma}$ for the monomial ordering $\prec$, it suffices to keep the elements $p_\alpha \in \boldsymbol{k}$ with α minimal for the component-wise partial ordering.

3.3. Complexity. Let $s = |\boldsymbol{a}|$ and $r = |\boldsymbol{b}|$, $\delta = |\partial\boldsymbol{b}|$. As $\boldsymbol{b} \subset \boldsymbol{a}$ and the monomials in $\partial\boldsymbol{b}$ are the product of a monomial in $\boldsymbol{b}$ by one of the variables $x_1, \ldots, x_n$, we have $r \leqslant s$ and $\delta \leqslant nr$.

PROPOSITION 3.7. *The complexity of the algorithm to compute the bases* $\boldsymbol{p}$ *and* $\boldsymbol{q}$ *is* $\mathcal{O}((r+\delta)rs)$.

Proof. At each step, the computation of p_α (resp. q_α) requires $\mathcal{O}(r^2)$ arithmetic operations, since the support of the polynomials p_β, q_β ($\beta \in \boldsymbol{b}$) is in $\boldsymbol{b}$ and $|\boldsymbol{b}| \leqslant r$. Computing $\langle \boldsymbol{x}^\gamma, p_\alpha \rangle_\sigma$ for all $\gamma \in \boldsymbol{t}$ requires $\mathcal{O}(rs)$ arithmetic operations. As the number of polynomials p_α is at most $|\boldsymbol{b}^+| = r+\delta$, the total cost for computing $\boldsymbol{p}$ and $\boldsymbol{q}$ is thus in $\mathcal{O}((r+\delta)(r^2+rs)) = \mathcal{O}((r+\delta)rs)$. ∎

As $\delta \leqslant nr$, the complexity of this algorithm is in $\mathcal{O}(nr^2 s)$.

The algorithm is connected to the *Berlekamp-Massey-Sakata* algorithm, which computes a Gröbner basis for a monomial ordering $\prec$. In the BMS algorithm, a minimal set $\mathcal{F}$ of recurrence polynomials valid for the monomials smaller that a given monomial m is computed. A monomial basis $\boldsymbol{b}^*$ generated by all the divisors of some corner elements is constructed. The successor m^+ of the monomial m for the monomial ordering $\prec$ is considered and the family $\mathcal{F}$ of valid recurrence polynomials is updated by computing their discrepancy at the monomial m^+ and by cancelling this discrepancy, if necessary, by combination with one lower polynomial [30].

Let δ be the size of the border $\partial \boldsymbol{b}^*$ of the monomial basis $\boldsymbol{b}^*$computed by BMS algorithm. At each update, there are at most δ polynomials in $\mathcal{F}$. Let s' be the maximum number of their non-zero terms. Then the update of $\mathcal{F}$ requires $\mathcal{O}(\delta s')$ arithmetic operations. The number of updates is bounded by the number $r+\delta$ of monomials in $\boldsymbol{b}^+$. Checking the discrepency of a polynomial in $\mathcal{F}$ for all the monomials in $\boldsymbol{x}^{\boldsymbol{a}}$ requires $\mathcal{O}(s's)$ arithmetic operations. Thus, the total cost of the BMS algorithm is in $\mathcal{O}((r+\delta)\delta s' + \delta s's)$. As the output polynomials in the Gröbner basis are not necessarily reduced, the maximal number of terms $s' \leqslant s$ can be of the same order than s. Thus the complete complexity of BMS algorithm is in $\mathcal{O}(\delta s^2) = \mathcal{O}(nrs^2)$, which is an order of magnitude larger than the bound of Proposition 15, assuming that $r \ll s$.

The method presented in [7] for computing a Gröbner basis of the recurrence polynomials computes the rank of a Hankel matrix of size the number $\tilde{s}$ of monomials of degree $\leqslant d$ for a bound d on the degree of the recurrence relations. It deduces a monomial basis $\boldsymbol{b}$ stable by division and obtains the valid recurrence relations for the border monomials by solving a linear Hankel system of size r. Thus the complexity is in $\mathcal{O}(\delta r^\omega + \tilde{s}^\omega)$ where $2.3 \leqslant \omega \leqslant 3$. It is also larger than the bound of Proposition 15. This bound could be improved by exploiting the rank displacement of the structured matrices involved in this method [9], but the known bounds on the displacement rank of the matrices involved in the computation do not improve the bound of Proposition 15.

4. Examples

4.1. Multivariate Prony method. Given a function $h(u_1,\ldots,u_n) = \sum_{i=1}^r \omega_i e^{\zeta_{i,1}u_1+\cdots+\zeta_{i,n}u_n}$, the problem is to compute its decomposition as a weighted sum of exponentials, from values of h. The method proposed by G. Riche de Prony for sums of univariate exponential functions consists in sampling the function at regularly spaced values [2]. In the multivariate extension of this method, the function is sampled on a grid in $\mathbb{R}^n$, for instance $\mathbb{N}^n$. The decomposition is computed from a subset of the multi-index sequence of evaluation $\sigma_\alpha = h(\alpha_1,\ldots,\alpha_n)$ for $\alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{N}^n$. The ideal I_σ associated to this sequence is the ideal defining the points $\xi_i = (e^{\zeta_{i,1}},\ldots,e^{\zeta_{i,1n}})$. To compute this decomposition, we apply the border basis algorithm to the sequence σ_α for $|\alpha| \leqslant d$ with d high enough, and obtain a border basis of the ideal I_σ defining the points $\xi_1,\ldots,\xi_r \in \mathbb{K}^n$, a basis of $\mathcal{A}_\sigma$ and the tables of multiplication in this basis. By applying the decomposition algorithm in [22], we deduce the points $\xi_i = (e^{\zeta_{i,1}},\ldots,e^{\zeta_{i,1n}})$. Taking the log of their coordinates $\log(\xi_{i,j}) = \zeta_{i,j}$ yields the coordinates of the frequencies ζ_i.

4.2. Fast decoding of algebraic-geometric codes. Let $\mathbb{K}$ be a finite field. We consider an algebraic-geometric code C obtained by evaluation of polynomials in $\mathbb{K}[x_1,\ldots,x_n]$ of degree $\leqslant d$ at points $\xi_1,\ldots,\xi_l \in \mathbb{K}^n$. It is a finite vector space in $\mathbb{K}^l$. We use the words of the orthogonal code $C^\perp = \{(m_1,\ldots,m_l) \mid m\cdot c = m_1c_1+\cdots+m_lc_l = 0\}$ for the transmission of information. Suppose that an error $\omega = (\omega_1,\ldots,\omega_l)$ occurs in the transmission of a message $m = (m_1,\ldots,m_l)$ so that the message $m^* = m+\omega$ is received. Let $\omega_{i_1},\ldots,\omega_{i_r}$ be the non-zero coefficients of the error vector ω. To correct the message r, we use the moments or syndromes $\sigma_\alpha = (\xi_1^\alpha,\ldots,\xi_l^\alpha)\cdot m^* = (\xi_1^\alpha,\ldots,\xi_l^\alpha)\cdot\omega = \sum_{j=1}^r w_{i_j}\xi_{i_j}^\alpha$ for $\alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{N}^n$ with $|\alpha| \leqslant d$. We compute generators of the set of error-locator polynomials, that is, the polynomials vanishing at the points $\xi_{i_1},\ldots,\xi_{i_r}$ and deduce the weights or errors ω_{i_j} by

solving the Vandermonde system

$$[\xi_{i_j}^{\alpha}]_{|\alpha|\leqslant d, 1\leqslant j\leqslant r}(\omega_{i_j}) = (\sigma_\alpha)_{|\alpha|\leqslant d}.$$

The points ξ_{i_j} correspond to the position of the errors and ω_{i_j} to their amplitude. By applying the border basis algorithm, we obtain a border basis of the ideal of error-locator polynomials, from which we deduce the position and amplitude of the errors.

4.3. Sparse interpolation. Given a sparse polynomial $h(u_1,\dots,u_n) = \sum_{i=1}^r \omega_i u_1^{\gamma_{i,1}} \cdots u_n^{\gamma_{i,n}}$, which is a weighted sum of r monomials with non-zero weights $\omega_i \in \mathbb{K}$, the problem is to compute the exponents $(\gamma_{i,1},\dots,\gamma_{i,n}) \in \mathbb{N}^n$ of the monomials and the weights ω_i, from evaluations of the blackbox functions h. The approach, proposed initially in [4], [36], consists in evaluating the function at points of the form $(\zeta_1^k,\dots,\zeta_n^k)$ for some values of $\zeta_1,\dots\zeta_n \in \mathbb{K}$ and to apply univariate Prony-type methods or Berlekamp-Massey algorithms to the sequence $\sigma_k = h(\zeta_1^k,\dots,\zeta_n^k)$, for $k \in \mathbb{N}$. The approach can be extended to multi-index sequences $(\sigma_\alpha)_{\alpha\in\mathbb{N}^n}$ by computing the terms

$$\sigma_\alpha = h(\zeta_1^{\alpha_1},\dots,\zeta_n^{\alpha_n}) = \sum_{i=1}^r \omega_i (\zeta_1^{\gamma_{i,1}})^{\alpha_1}\cdots(\zeta_n^{\gamma_{i,n}})^{\alpha_n}$$

for $\alpha = (\alpha_1,\dots,\alpha_n) \in \mathbb{N}^n$. It can also be extended to sequences constructed from polylog functions [22]. By applying the border basis algorithm to the multi-index sequence $\sigma_\alpha = h(\zeta_1^{\alpha_1},\dots,\zeta_n^{\alpha_n})$ for $|\alpha| \leqslant d$ with $d \in \mathbb{N}$ high enough, we obtain generators of the ideal I_σ defining the points $\xi_i = (\zeta_1^{\gamma_{i,1}},\dots,\zeta_n^{\gamma_{i,n}})$ and deduce the weights ω_i, $i = 1,\dots,r$. By computing the log of the coordinates of the points ξ_i, we deduce the exponent vectors $\gamma_i = (\gamma_{i,1},\dots,\gamma_{i,n}) \in \mathbb{N}^n$ for $i = 1,\dots,r$.

4.4. Tensor decomposition. Given a homogeneous polynomial

$$t = \sum_{\alpha_0+\alpha_1+\cdots+\alpha_n=d} t_\alpha \binom{d}{\alpha} x_0^{\alpha_0} x_1^{\alpha_1}\dots x_n^{\alpha_n}$$

of degree $d \in \mathbb{N}$ with $t_\alpha \in \mathbb{K}$, $\binom{d}{\alpha} = \frac{d!}{\alpha_0!\cdots\alpha_n!}$, we want to a decomposition of t as sum of powers of linear forms:

$$t = \sum_{i=1}^r \omega_i (\xi_{i,0}x_0 + \xi_{i,1}x_1 + \cdots + \xi_{i,n}x_n)^d \tag{2}$$

with a minimal r, $\omega_i \neq 0$ and $(\xi_{i,0},\dots,\xi_{i,n}) \neq 0$. By a change of variables, we can assume that $\xi_{i,0} \neq 0$ in such a decomposition, and by dividing each linear form by $\xi_{i,0}$ and multiplying ω_i by $\xi_{i,0}^d$, we can even assume that $\xi_{i,0} = 1$. Then by expansion of the powers of the linear forms and by identification of the coefficients, we obtain

$$\sigma_\alpha := t_{(d-\alpha_1\cdots-\alpha_n,\alpha_1,\dots,\alpha_n)} = \sum_{i=1}^r \omega_i \xi_{i,1}^{\alpha_1}\cdots\xi_{i,n}^{\alpha_n} = \sum_{i=1}^r \omega_i \xi_i^\alpha$$

for $\alpha = (\alpha_1,\dots,\alpha_n) \in \mathbb{N}^n$ with $|\alpha| \leqslant d$. We apply the border basis algorithm to this sequence, in order to obtain generators of the ideal I_σ defining the points $\xi_1,\dots,\xi_r \in \mathbb{K}^n$ and providing the weights ω_i. If the number of terms r is small enough compared to the number of terms σ_α, then the set of border relations are complete and it is possible to compute the decomposition (2).

4.5. Vanishing ideal of points. Given a set of points $\Xi = \{\xi_1,\dots,\xi_r\} \subset \mathbb{K}^n$, we want to compute polynomials defining these points, that is, a set of generators of the ideal of polynomials vanishing on Ξ. For that purpose, we choose non-zero weights $w_i \in \mathbb{K}$, a degree $d \in \mathbb{N}$ and we compute the sequence of moments $\sigma_\alpha = \sum_{i=1}^r \omega_i \xi^\alpha$ for $|\alpha| \leqslant d$. The generating series σ associated to these moments define an Artinian Gorenstein algebra $\mathcal{A}_\sigma = \mathbb{K}[\boldsymbol{x}]/I_\sigma$, where I_σ is the ideal of polynomials vanishing Ξ [22]. This ideal I_σ defines the points ξ_i with multiplicity 1. The idempotents $\{\boldsymbol{u}_i\}_{i=1\dots r}$ associated to the points Ξ form a family of interpolation polynomials at these points: $\boldsymbol{u}_i(\xi_j) = 0$ if $i \neq j$ and $\boldsymbol{u}_i(\xi_i) = 1$. They are the common eigenvectors of the multiplication operators in $\mathcal{A}_\sigma$. By applying

the border basis algorithm to the sequence σ_α for $|\alpha| \leqslant d$ with d high enough, we obtain generators of the ideal I_σ defining the points $\xi_1, \ldots, \xi_r \in \mathbb{K}^n$, a basis of $\mathcal{A}_\sigma$ and the tables of multiplication in this basis. By computing the eigenvectors of a generic combination of the multiplication tables by a variable, we obtain a family of interpolation polynomials at the roots Ξ.

4.6. Benchmarks. We present some experimentations of an implementation of Algorithm 2[1] in the programming language Julia[2]. The arithmetic operations are done in the finite field $\mathbb{Z}/32003\mathbb{Z}$. We choose r random points ξ_i with n coordinates in $\mathbb{Z}/32003\mathbb{Z}$, take the sequence of moments $\sigma_\alpha = \sum_{i=1}^{r} \xi_i^\alpha$ up for $|\alpha| \leqslant d$ with weights equal to 1. Figure 4.6 shows the timing (in sec.) to compute the border basis, checking the validity of the recurrence relations up to degree d. The computation is done on a MacOS El Capitan, 2.8 GHz Intel Core i7, 16 Go.

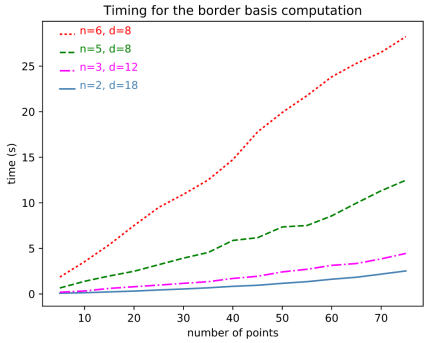

Fig. 4.6: Vanishing ideal of random points.

The timing is approximately linear in the number r of points, with a slope increasing quadratically in n.

REFERENCES

[1] F. Andersson, M. Carlsson, and M. V. de Hoop. Nonlinear approximation of functions in two dimensions by sums of exponential functions. *Applied and Computational Harmonic Analysis*, 29(2):156–181, 2010.
[2] G. Riche Baron de Prony. Essai expérimental et analytique: Sur les lois de la dilatabilité de fluides élastique et sur celles de la force expansive de la vapeur de l'alcool, à différentes températures. *J. Ecole Polyt.*, 1:24–76, 1795.
[3] B. Beckermann and G. Labahn. A uniform approach for the fast computation of matrix-type Padé approximants. *SIAM J. on Matrix Analysis and Applications*, 15(3):804–823, 1994.
[4] M. Ben-Or and P. Tiwari. A deterministic algorithm for sparse multivariate polynomial interpolation. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 301–309. ACM, 1988.
[5] E. R. Berlekamp. Nonbinary BCH decoding. *IEEE Transactions on Information Theory*, 14(2):242–242, 1968.
[6] A. Bernardi, J.Brachat, P. Comon, and B. Mourrain. General tensor decomposition, moment matrices and applications. *J. of Symbolic Computation*, 52:51–71, 2013.
[7] J. Berthomieu, B. Boyer, and J.-C. Faugère. Linear Algebra for Computing Gröbner Bases of Linear Recursive Multidimensional Sequences. In *International Symposium on Symolic and Algebraic Compution*, pages 61–68. ACM Press, 2015.
[8] G. Beylkin and L. Monzón. On approximation of functions by exponential sums. *Applied and Computational Harmonic Analysis*, 19(1):17–48, July 2005.
[9] A. Bostan, C.-P. Jeannerod, and É. Schost. Solving structured linear systems with large displacement rank. *Theoretical Computer Science*, 407(1-3):155–181, November 2008.
[10] J. Brachat, P. Comon, B. Mourrain, and E. P. Tsigaridas. Symmetric tensor decomposition. *Linear Algebra and Applications*, 433(11-12):1851–1872, 2010.
[11] R. P. Brent, F. G Gustavson, and D. Y. Yun. Fast solution of toeplitz systems of equations and computation of Padé approximants. *J. of Algorithms*, 1(3):259–295, September 1980.
[12] D. A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics. Springer, 1992.
[13] A. Cuyt. How well can the concept of Padé approximant be generalized to the multivariate case? *J. of Computational and Applied Mathematics*, 105(1-2):25–50, 1999.
[14] M. Elkadi and B. Mourrain. *Introduction à la résolution des systèmes polynomiaux*, volume 59 of *Mathématiques et Applications*. Springer, 2007.
[15] J. Emsalem. Géométrie des points épais. *Bulletin de la S.M.F.*, 106:399–416, 1978.

[1] available at https://gitlab.inria.fr/mourrain/PolyExp
[2] https://julialang.org/

[16] P. Fitzpatrick and G. H. Norton. Finding a basis for the characteristic ideal of an n-dimensional linear recurring sequence. *IEEE Transactions on Information Theory*, 36(6):1480–1487, 1990.
[17] G. Golub and V. Pereyra. Separable nonlinear least squares: The variable projection method and its applications. *Inverse Problems*, 19(2):R1–R26, 2003.
[18] S. Kunis, T. Peter, T. Römer, and U. von der Ohe. A multivariate generalization of Prony's method. *Linear Algebra and its Applications*, 490:31–47, 2016.
[19] M. Laurent and B. Mourrain. A generalized flat extension theorem for moment matrices. *Archiv der Mathematik*, 93(1):87–98, 2009.
[20] J. Massey. Shift-register synthesis and BCH decoding. *IEEE transactions on Information Theory*, 15(1):122–127, 1969.
[21] B. Mourrain. Isolated points, duality and residues. *J. of Pure and Applied Algebra*, 117&118:469–493, 1996.
[22] B. Mourrain. Polynomial-exponential decomposition from moments, 2016. hal-01367730, arXiv:1609.05720.
[23] B. Mourrain and V. Y. Pan. Multivariate Polynomials, Duality, and Structured Matrices. *J. of Complexity*, 16(1):110–180, 2000.
[24] B. Mourrain and Ph. Trébuchet. Generalized normal forms and polynomial system solving. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, pages 253–260. ACM Press, 2005.
[25] B. Mourrain and Ph. Trébuchet. Stable normal forms for polynomial system solving. *Theoretical Computer Science*, 409(2):229–240, 2008.
[26] B. Mourrain and Ph. Trébuchet. Border basis representation of a general quotient algebra. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, pages 265–272. ACM, 2012.
[27] D. Potts and M. Tasche. Parameter estimation for multivariate exponential sums. *Electronic Transactions on Numerical Analysis*, 40:204–224, 2013.
[28] S. C. Power. Finite rank multivariable Hankel forms. *Linear Algebra and its Applications*, 48:237–244, 1982.
[29] R. Roy and T. Kailath. ESPRIT-estimation of signal parameters via rotational invariance techniques. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, 37(7):984–995, 1989.
[30] K. Saints and Ch. Heegard. Algebraic-geometric codes and multidimensional cyclic codes: A unified theory and algorithms for decoding using Grobner bases. *IEEE Transactions on Information Theory*, 41(6):1733–1751, 1995.
[31] S. Sakata. Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array. *J. of Symbolic Computation*, 5(3):321–337, 1988.
[32] T. Sauer. Prony's method in several variables. *Numerische Mathematik*, pages 1–28, 2016. To appear.
[33] A. Lee Swindlehurst and Th. Kailath. A performance analysis of subspace-based methods in the presence of model errors. I. The MUSIC algorithm. *IEEE Transactions on signal processing*, 40(7):1758–1774, 1992.
[34] L. N. Trefethen and D. Bau. *Numerical Linear Algebra*. SIAM, 1997.
[35] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 3rd edition, 2013.
[36] R. Zippel. Interpolating polynomials from their values. *J. of Symbolic Computation*, 9(3):375–403, 1990.

Examples

Example 1.

We consider the sequence $\sigma \in \mathbb{K}^{\mathbb{N}}$ such that $\sigma_{d_1} = 1$ and $\sigma_i = 0$ for $0 \leqslant i \neq d_1 \leqslant d$ and $d_1 < d$.

In the first step of the algorithm, we take $p_0 = 1$ and compute the first $\gamma \in [0, \ldots, d]$ such that $\langle x^\gamma, p_1\rangle_\sigma$ is not zero. This yields $m_0 = x^{d_1}$ and $\boldsymbol{b} = [0]$, $\boldsymbol{c} = [d_1]$.

In a second step, we have $p_1 = x - \langle x, m_1\rangle_\sigma p_0 = x$. The first $\gamma \in [0, \ldots, d] \setminus \{d_1\}$ such that $\langle x^i, p_1\rangle_\sigma$ is not zero yields $\boldsymbol{b} = [0, 1]$, $\boldsymbol{c} = [d_1, d_1 - 1]$, $m_1 = x^{d_1-1}$.

We repeat this computation until $\boldsymbol{b} = [0, \ldots, d_1]$, $\boldsymbol{c} = [d_1, d_1 - 1, \ldots, 1]$ with $m_i = x^{d_1-i}$, $p_i = x^i$ for $i = 0, \ldots, d_1$.

In the following step, we have $p_{d_1+1} = \mathrm{proj}(x^{d_1+1}, \boldsymbol{p}, \boldsymbol{m}) = x^{d_1+1} - \langle x^{d_1+1}, m_1\rangle_\sigma p_1 - \cdots - \langle x^{d_1+1}, m_{d_1}\rangle_\sigma p_{d_1} = x^{d_1+1}$ such that $\langle x^{d_1+1}, x^j\rangle_\sigma = 0$ for $0 \leqslant j \leqslant d$. The algorithm stops and outputs $\boldsymbol{b} = [1, \ldots, x^{d_1}]$, $\boldsymbol{c} = [x^{d_1}, x^{d_1-1}, \ldots, 1]$, $\boldsymbol{k} = [x^{d_1+1}]$.

Example 2.

We consider the function $h(u_1, u_2) = 2 + 3 \cdot 2^{u_1} 2^{u_2} - 3^{u_1}$. Its associated generating series is $\sigma = \sum_{\alpha\in\mathbb{N}^2} h(\alpha)\boldsymbol{z}^\alpha = 4 + 5z_1 + 7z_2 + 5z_1^2 + 11z_1z_2 + 13z_2^2 + \cdots$.

At the first step, we have $\mathbf{x}^{\boldsymbol{b}} = [1]$, $\boldsymbol{p} = [1]$, $\boldsymbol{q} = \left[\frac{1}{4}\right]$. At the second step, we compute $\mathbf{x}^{\boldsymbol{b}} = [1, x_1, x_2]$, $\boldsymbol{p} = [1, x_1 - \frac{5}{4}, x_2 - \frac{9}{5}x_1 - 4] = [p_1, p_{x_1}, p_{x_2}]$ and $\boldsymbol{q} = \left[\frac{1}{4}p_1, -\frac{4}{5}p_{x_1}, \frac{5}{24}p_{x_2}\right]$. At the next step, we obtain $\boldsymbol{k} = [], \boldsymbol{d} = [x_1^2, x_1x_2, x_2^2]$.

$$\begin{aligned} x_1p_1 &\equiv \frac{5}{4}p_1 + p_{x_1} \\ x_1\,p_{x_1} &\equiv -\frac{5}{16}p_1 + \frac{91}{20}p_{x_1} - p_{x_2} \\ x_1p_{x_2} &\equiv \sum_{i=1}^{3}\langle x_1p_{x_2}, \boldsymbol{q}_i\rangle_\sigma \boldsymbol{p}_i = \frac{96}{25}p_{x_1} + \frac{1}{5}p_{x_2} \end{aligned}$$

The matrix of multiplication by x_1 in the basis $\boldsymbol{p}$ is

$$M_1 = \begin{bmatrix} \frac{5}{4} & -\frac{5}{16} & 0 \\ 1 & \frac{91}{20} & \frac{96}{25} \\ 0 & -1 & \frac{1}{5} \end{bmatrix}.$$

Its eigenvalues are $[1, 2, 3]$ and the corresponding matrix of eigenvectors is

$$U := \begin{bmatrix} \frac{1}{2} & \frac{3}{4} & -\frac{1}{4} \\ \frac{2}{5} & -\frac{9}{5} & \frac{7}{5} \\ -\frac{1}{2} & 1 & -\frac{1}{2} \end{bmatrix},$$

that is, the polynomials $U(x) = [2 - \frac{1}{2}\,x_1 - \frac{1}{2}\,x_2, -1 + x_2, \frac{1}{2}\,x_1 - \frac{1}{2}\,x_2]$. By computing the Hankel matrix

$$H_\sigma^{U,[1,x_1,x_2]} = \begin{bmatrix} 2 & 3 & -1 \\ 2\times 1 & 3\times 2 & -1\times 3 \\ 2\times 1 & 3\times 2 & -1\times 1 \end{bmatrix}$$

we deduce the weights $2, 3, -1$ and the frequencies $(1,1),\ (2,2), (3,1)$, which corresponds to the decomposition $\sigma = e^{y_1+y_2} + 3e^{2y_1+2y_2} - e^{2y_1+y_2}$ associated to $h(u_1,u_2) = 2 + 3\cdot 2^{u_1+u_2} - 3^{u_1}$.

Example 3.

We consider the following symmetric tensor or homogeneous polynomial:

$$\begin{aligned} \tau = \quad & -x_0^4 - 24\,x_0^3x_1 - 8\,x_0^3x_2 - 60\,x_0^2x_1^2 - 168\,x_0^2x_1x_2 - 12\,x_0^2x_2^2 \\ & -96\,x_0x_1^3 - 240\,x_0x_1^2x_2 - 384\,x_0x_1x_2^2 + 16\,x_0x_2^3 \\ & -46\,x_1^4 - 200\,x_1^3x_2 - 228\,x_1^2x_2^2 - 296\,x_1x_2^3 + 34\,x_2^4. \end{aligned}$$

The associated series is

$$\begin{aligned} \sigma = & -1 - 6\,z_1 - 2\,z_2 - 10\,z_1^2 - 14\,z_2z_1 - 2\,z_2^2 \\ & -24\,z_1^3 - 20\,z_2z_1^2 - 32\,z_2^2z_1 + 4\,z_2^3 \\ & -46\,z_1^4 - 50\,z_2z_1^3 - 38\,z_2^2z_1^2 - 74\,z_2^3z_1 + 34\,z_2^4 \end{aligned}$$

To decompose it into a sum of powers of linear forms, we apply the border basis algorithm to the series σ. The algorithm projects successively the monomials $1, x_1, x_2, x_1^2, x_1x_2, x_2^2, \ldots$ onto the family of polynomials $\boldsymbol{p}$, starting with $\boldsymbol{p} = [1]$. We obtain $\mathbf{x}^{\boldsymbol{b}} = \boldsymbol{c} = [1, x_1, x_2]$, $\boldsymbol{p} = [1, x_1 - 6, x_2 + \frac{1}{13}x_1 - \frac{32}{13}]$ and the border basis is

$$\boldsymbol{k} = [x_1^2 - \frac{3}{2}x_1 - \frac{3}{2}x_2 + 2, x_1x_2 - \frac{5}{2}x_1 - \frac{1}{2}x_2 + 2, x_2^2 + \frac{1}{2}x_1 - \frac{7}{2}x_2 + 2],$$

giving the projection of the border monomials $\boldsymbol{d} = [x_1^2, x_1x_2, x_2^2]$ on the basis $\mathbf{x}^{\boldsymbol{b}}$. The decomposition of τ is deduced from the eigenvectors of the operator of multiplication by x_1:

$$M_1 = \begin{bmatrix} 0 & -2 & -2 \\ 0 & \frac{1}{2} & \frac{3}{2} \\ 1 & \frac{5}{2} & \frac{3}{2} \end{bmatrix}.$$

Its eigenvalues are $[-1,1,2]$ and the eigenvectors correspond to the polynomials

$$\boldsymbol{u} = \left[\begin{array}{ccc} \frac{1}{2}\,x_2 - \frac{1}{2}\,x_1 & -2 + \frac{3}{4}\,x_2 + \frac{1}{4}\,x_1 & -1 + \frac{1}{2}\,x_2 + \frac{1}{2}\,x_1 \end{array} \right].$$

Computing $\omega_i = \langle \sigma \mid \boldsymbol{u}_i \rangle$ and $\xi_{i,j} = \frac{\langle \sigma | x_j \boldsymbol{u}_i \rangle}{\langle \sigma | \boldsymbol{u}_i \rangle}$ (see [22]), we obtain the decomposition:

$$\tau = (x_0 - x_1 + 3\,x_2)^4 + (x_0 + x_1 + x_2)^4 - 3\,(x_0 + 2\,x_1 + 2\,x_2)^4.$$

Example 4.

We consider the algebraic code over $\mathbb{K} = \mathbb{Z}/32003\mathbb{Z}$ defined by

$$C = \{c \in \mathbb{K}^{11} \mid \sum_{i=1}^{11} c_i\,\xi_i^\alpha = 0,\ \forall \alpha \in \mathbb{N}^3 \ s.t.\ |\alpha| \leq 2\}$$

where

$$\Xi = \left[\begin{array}{ccccccccccc} 1 & 1 & 1 & -1 & -1 & 0 & 0 & 2 & 1 & 1 & 0 \\ 0 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 2 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{array} \right]$$

and ξ_i is the i^{th} column of Ξ. Suppose that we receive the word

$$r = [0,3,3,3,0,0,-6,-2,0,-1,0]$$

which is the sum $r = c + \omega$ of a code word $c \in C$ and an error vector $\omega \in \mathbb{K}^{11}$. We want to correct it and find the corresponding word c of the code C.

Computing the syndromes $\sigma_\alpha = \sum_{i=1}^{11} r_i \xi_i^\alpha = \sum_{i=1}^{11} \omega_i \xi_i^\alpha$ for $|\alpha| \leq 2$ and the corresponding (truncated) generating series, we get

$$\sigma = -2\,z_1 + z_2 + 3\,z_1\,z_2 - 2\,z_1\,z_3 - 3\,z_2^2 + z_2\,z_3.$$

We apply the border basis algorithm to obtain error locator polynomials. The monomials are considered in the order $\mathbf{x}^{\mathbf{a}} = [1, x_1, x_2, x_3, x_1^2, x_1\,x_2, \ldots, x_3^2]$. Here are the different steps, where $\mathfrak{n}$ denotes the new monomial introduced at each loop of the algorithm.

Step 1. $\mathfrak{n} = 1$, $\mathbf{x}^{\boldsymbol{b}} = [1]$, $\mathbf{x}^{\boldsymbol{c}} = [x_1]$, $\boldsymbol{k} = []$.

Step 2. $\mathfrak{n} = x_1$, $\mathbf{x}^{\boldsymbol{b}} = [1, x_1]$, $\mathbf{x}^{\boldsymbol{c}} = [x_1, 1]$, $\boldsymbol{k} = []$.

Step 3. $\mathfrak{n} = x_2$, $\mathbf{x}^{\boldsymbol{b}} = [1, x_1]$, $\mathbf{x}^{\boldsymbol{c}} = [x_1, 1]$, $\boldsymbol{k} = [x_2 + \frac{1}{2}x_1 + \frac{3}{2}]$.

Step 4. $\mathfrak{n} = x_3$, $\mathbf{x}^{\boldsymbol{b}} = [1, x_1]$, $\mathbf{x}^{\boldsymbol{c}} = [x_1, 1]$, $\boldsymbol{k} = [x_2 + \frac{1}{2}x_1 + \frac{3}{2}, x_3 - 1]$.

The algorithm stops at this step, since the new monomial $\mathfrak{n} = x_1^2$ is of degree 2 and $\mathfrak{n} \cdot \mathbf{x}^{\mathbf{c}} \not\subset \mathbf{x}^{\mathbf{a}}$. It outputs two error locator polynomials: $x_2 + \frac{1}{2}x_1 + \frac{3}{2}, x_3 - 1$.

We check that only ξ_5, ξ_{10} are roots of the error locator polynomials. We deduce the non-zero weights ω_5, ω_{10} by solving the system $\omega_5 \xi_5^\alpha + \omega_{10} \xi_{10}^\alpha = \sigma_\alpha$ for $\alpha \in \{(0,0,0), (1,0,0)\}$. This yields $\omega_5 = 1, \omega_{10} = -1$, so that the code word is

$$c = [0,3,3,3,-1,0,-6,-2,0,0,0].$$