

Toeplitz and Toeplitz-block-Toeplitz matrices and their correlation with syzygies of polynomials.

Houssam Khalil, Bernard Mourrain, Michelle Schatzman

▶ **To cite this version:**

Houssam Khalil, Bernard Mourrain, Michelle Schatzman. Toeplitz and Toeplitz-block-Toeplitz matrices and their correlation with syzygies of polynomials.. international seminar matrix methods and operator equations (MM&OE), Jul 2007, Moscou, Russia. pp.296-312. hal-00366292

HAL Id: hal-00366292
https://hal.science/hal-00366292

Submitted on 6 Mar 2009

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

TOEPLITZ AND TOEPLITZ-BLOCK-TOEPLITZ MATRICES AND THEIR CORRELATION WITH SYZYGIES OF POLYNOMIALS

HOUSSAM KHALIL*, BERNARD MOURRAIN†, AND MICHELLE SCHATZMAN‡

Abstract. In this paper, we re-investigate the resolution of Toeplitz systems $T\,u = g$, from a new point of view, by correlating the solution of such problems with syzygies of polynomials or moving lines. We show an explicit connection between the generators of a Toeplitz matrix and the generators of the corresponding module of syzygies. We show that this module is generated by two elements of degree n and the solution of $T\,u = g$ can be reinterpreted as the remainder of an explicit vector depending on g, by these two generators.

This approach extends naturally to multivariate problems and we describe for Toeplitz-block-Toeplitz matrices, the structure of the corresponding generators.

Key words. Toeplitz matrix, rational interpolation, syzygie

1. Introduction. Structured matrices appear in various domains, such as scientific computing, signal processing, ... They usually express, in a linearize way, a problem which depends on less parameters than the number of entries of the corresponding matrix. An important area of research is devoted to the development of methods for the treatment of such matrices, which depend on the actual parameters involved in these matrices.

Among well-known structured matrices, Toeplitz and Hankel structures have been intensively studied [5, 6]. Nearly optimal algorithms are known for the multiplication or the resolution of linear systems, for such structure. Namely, if A is a Toeplitz matrix of size n, multiplying it by a vector or solving a linear system with A requires $\tilde{\mathcal{O}}(n)$ arithmetic operations (where $\tilde{\mathcal{O}}(n) = \mathcal{O}(n\log^c(n))$ for some $c > 0$) [2, 12]. Such algorithms are called super-fast, in opposition with fast algorithms requiring $\mathcal{O}(n^2)$ arithmetic operations.

The fundamental ingredients in these algorithms are the so-called generators [6], encoding the minimal information stored in these matrices, and on which the matrix transformations are translated. The correlation with other types of structured matrices has also been well developed in the literature [10, 9], allowing to treat so efficiently other structures such as Vandermonde or Cauchy-like structures.

Such problems are strongly connected to polynomial problems [4, 1]. For instance, the product of a Toeplitz matrix by a vector can be deduced from the product of two univariate polynomials, and thus can be computed efficiently by evaluation-interpolation techniques, based on FFT. The inverse of a Hankel or Toeplitz matrix is connected to the Bezoutian of the polynomials associated to their generators.

However, most of these methods involve univariate polynomials. So far, few investigations have been pursued for the treatment of multilevel structured matrices [11], related to multivariate problems. Such linear systems appear for instance in resultant or in residue constructions, in normal form computations, or more generally in multivariate polynomial algebra. We refer to [8] for a general description of such correlations between multi-structured matrices and multivariate polynomials. Surprisingly, they also appear in numerical scheme and preconditionners. A main challenge here is to devise super-fast algorithms of complexity $\tilde{\mathcal{O}}(n)$ for the resolution of multi-structured systems of size n.

In this paper, we consider block-Toeplitz matrices, where each block is a Toeplitz matrix. Such a structure, which is the first step to multi-level structures, is involved in many bivariate problems, or in numerical linear problems.We re-investigate first the resolution of Toeplitz systems $T\,u = g$, from a new point of view, by correlating the solution of such problems with syzygies of polynomials or moving lines. We show an explicit connection between the generators of a Toeplitz matrix and the generators of the corresponding module of syzygies. We show that this module is generated by two elements of degree n and the solution of $T\,u = g$ can be reinterpreted as the remainder of an explicit vector depending on g, by these two generators.

*Institut Camille Jordan, 43 boulevard du 11 novembre 1918, 69622 Villeurbanne cedex France (khalil@math.univ-lyon1.fr).

†INRIA, GALAAD team, 2004 route des Lucioles, BP 93, 06902 Sophia Antipolis Cedex, France(mourrain@sophia.inria.fr).

‡Institut Camille Jordan, 43 boulevard du 11 novembre 1918, 69622 Villeurbanne cedex France (schatz@math.univ-lyon1.fr).

This approach extends naturally to multivariate problems and we describe for Toeplitz-block-Toeplitz matrices, the structure of the corresponding generators. In particular, we show the known result that the module of syzygies of k non-zero bivariate polynomials is free of rank $k-1$, by a new elementary proof.

Exploiting the properties of moving lines associated to Toeplitz matrices, we give a new point of view to resolve a Toeplitz-block-Toeplitz system.

In the next section we studie the scalar Toeplitz case. In the chapter 3 we consider the Toeplitz-block-Toeplitz case.

Let $R = \mathbb{K}[x]$. For $n \in \mathbb{N}$, we denote by $\mathbb{K}[x]_n$ the vector space of polynomials of degree $\leq n$. Let $L = \mathbb{K}[x, x^{-1}]$ be the set of Laurent polynomials in the variable x. For any polynomial $p = \sum_{i=-m}^{n} p_i\, x^i \in L$, we denote by p^+ the sum of terms with positive exponents: $p^+ = \sum_{i=0}^{n} p_i\, x^i$ and by p^-, the sum of terms with strictly negative exponents: $p^- = \sum_{i=-m}^{-1} p_i\, x^i$. We have $p = p^+ + p^-$.

For $n \in \mathbb{N}$, we denote by $\mathfrak{U}_n = \{\omega; \omega^n = 1\}$ the set of roots of unity of order n.

2. Univariate case. We begin by the univariate case and the following problem:

PROBLEM 2.1. *Given a Toeplitz matrix $T = (t_{i-j})_{i,j=0}^{n-1} \in \mathbb{K}^{n\times n}$ ($T = (T_{ij})_{i,j=0}^{n-1}$ with $T_{ij} = t_{i-j}$) of size n and $g = (g_0, \ldots, g_{n-1}) \in \mathbb{K}^n$, find $u = (u_0, \ldots, u_{n-1}) \in \mathbb{K}^n$ such that*

$$T\, u = g. \tag{2.1}$$

Let $E = \{1, \ldots, x^{n-1}\}$, and Π_E be the projection of R on the vector space generated by E, along $\langle x^n, x^{n+1}, \ldots\rangle$.

DEFINITION 2.2. *We define the following polynomials:*

- $T(x) = \displaystyle\sum_{i=-n+1}^{n-1} t_i x^i$,
- $\tilde{T}(x) = \displaystyle\sum_{i=0}^{2n-1} \tilde{t}_i x^i$ *with* $\tilde{t}_i = \begin{cases} t_i & \text{if } i < n \\ t_{i-2n} & \text{if } i \geq n \end{cases}$,
- $u(x) = \displaystyle\sum_{i=0}^{n-1} u_i x^i$, $g(x) = \displaystyle\sum_{i=0}^{n-1} g_i x^i$.

Notice that $\tilde{T} = T^+ + x^{2\,n}\, T^-$ and $T(w) = \tilde{T}(w)$ if $w \in \mathfrak{U}_{2\,n}$. We also have (see [8])

$$T\, u = g \Leftrightarrow \Pi_E(T(x)u(x)) = g(x).$$

For any polynomial $u \in \mathbb{K}[x]$ of degree d, we denote it as $u(x) = \underline{u}(x) + x^n \overline{u}(x)$ with $\deg(\underline{u}) \leq n-1$ and $\deg(\overline{u}) \leq d-n$ if $d \geq n$ and $\overline{u} = 0$ otherwise. Then, we have

$$\begin{aligned} T(x)\, u(x) &= T(x)\underline{u}(x) + T(x)x^n\overline{u}(x) \\ &= \Pi_E(T(x)\underline{u}(x)) + \Pi_E(T(x)x^n\overline{u}(x)) \\ &\quad +(\alpha_{-n+1}x^{-n+1} + \cdots + \alpha_{-1}x^{-1}) \\ &\quad +(\alpha_n x^n + \cdots + \alpha_{n+m}x^{n+m}) \\ &= \Pi_E(T(x)\underline{u}(x)) + \Pi_E(T(x)x^n\overline{u}(x)) \\ &\quad +x^{-n+1}A(x) + x^n B(x), \end{aligned} \tag{2.2}$$

with $m = \max(n-2, d-1)$,

$$\begin{aligned} A(x) &= \alpha_{-n+1} + \cdots + \alpha_{-1}x^{n-2}, \\ B(x) &= \alpha_n + \cdots + \alpha_{n+m}x^m. \end{aligned} \tag{2.3}$$

See [8] for more details, on the correlation between structured matrices and (multivariate) polynomials.

2.1. Moving lines and Toeplitz matrices. We consider here another problem, related to interesting questions in Effective Algebraic Geometry.

PROBLEM 2.3. *Given three polynomials $a, b, c \in R$ respectively of degree $< l, < m, < n$, find three polynomials $p, q, r \in R$ of degree $< \nu - l, < \nu - m, < \nu - n$, such that*

$$a(x)\, p(x) + b(x)\, q(x) + c(x)\, r(x) = 0. \tag{2.4}$$

We denote by $\mathcal{L}(a,b,c)$ the set of $(p,q,r) \in \mathbb{K}[x]^3$ which are solutions of (2.4). It is a $\mathbb{K}[x]$-module of $\mathbb{K}[x]^3$. The solutions of the problem (2.3) are $\mathcal{L}(a,b,c) \cap \mathbb{K}[x]_{\nu-l-1} \times \mathbb{K}[x]_{\nu-m-1} \times \mathbb{K}[x]_{\nu-n-1}$.

Given a new polynomial $d(x) \in \mathbb{K}[x]$, we denote by $\mathcal{L}(a,b,c;d)$ the set of $(p,q,r) \in \mathbb{K}[x]^3$ such that

$$a(x)\,p(x) + b(x)\,q(x) + c(x)\,r(x) = d(x).$$

THEOREM 2.4. *For any non-zero vector of polynomials $(a,b,c) \in \mathbb{K}[x]^3$, the $\mathbb{K}[x]$-module $\mathcal{L}(a,b,c)$ is free of rank 2.*

Proof. By the Hilbert's theorem, the ideal I generated by (a,b,c) has a free resolution of length at most 1, that is of the form:

$$0 \to \mathbb{K}[x]^p \to \mathbb{K}[x]^3 \to \mathbb{K}[x] \to \mathbb{K}[x]/I \to 0.$$

As $I \neq 0$, for dimensional reasons, we must have $p = 2$. □

DEFINITION 2.5. *A μ-base of $\mathcal{L}(a,b,c)$ is a basis (p,q,r), (p',q',r') of $\mathcal{L}(a,b,c)$, with (p,q,r) of minimal degree μ.*

Notice if μ_1 is the smallest degree of a generator and μ_2 the degree of the second generator (p',q',r'), we have $d = max(\deg(a),\deg(b),\deg(c)) = \mu_1 + \mu_2$. Indeed, we have

$$\begin{aligned} &0 \to \mathbb{K}[x]_{\nu-d-\mu_1} \oplus \mathbb{K}[x]_{\nu-d-\mu_2} \to \\ &\mathbb{K}[x]^3_{\nu-d} \to \mathbb{K}[x]_\nu \to \mathbb{K}[x]_\nu/(a,b,c)_\nu \to 0, \end{aligned}$$

for $\nu >> 0$. As the alternate sum of the dimension of the $\mathbb{K}$-vector spaces is zero and $\mathbb{K}[x]_\nu/(a,b,c)_\nu$ is 0 for $\nu >> 0$, we have

$$\begin{aligned} 0 &= 3\,(d-\nu-1) + \nu - \mu_1 - d + 1 + \nu - \mu_2 - d + 1 + \nu + 1 \\ &= d - \mu_1 - \mu_2. \end{aligned}$$

For $\mathcal{L}(\tilde{T}(x), x^n, x^{2n}-1)$, we have $\mu_1 + \mu_2 = 2\,n$. We are going to show now that in fact $\mu_1 = \mu_2 = n$:

PROPOSITION 2.6. *The $\mathbb{K}[x]$-module $\mathcal{L}(\tilde{T}(x), x^n, x^{2n}-1)$ has a n-basis.*

Proof. Consider the map

$$\begin{aligned} \mathbb{K}[x]^3_{n-1} &\to \mathbb{K}[x]_{3n-1} \\ (p(x),q(x),r(x)) &\mapsto \tilde{T}(x)p(x) + x^n q(x) + (x^{2n}-1)r(x) \end{aligned} \tag{2.5}$$

which $3n \times 3n$ matrix is of the form

$$S := \left(\begin{array}{c|c|c} T_0 & \mathbf{0} & -\mathbb{I}_n \\ T_1 & \mathbb{I}_n & \mathbf{0} \\ T_2 & \mathbf{0} & \mathbb{I}_n \end{array}\right). \tag{2.6}$$

where T_0, T_1, T_2 are the coefficient matrices of $(\tilde{T}(x),\, x\,\tilde{T}(x),\, \ldots,\, x^n\tilde{T}(x))$, respectively for the list of monomials $(1,\ldots,x^{n-1})$, $(x^n,\ldots,x^{2n-1})$, $(x^{2n},\ldots,x^{3n-1})$. Notice in particular that $T = T_0 + T_2$

Reducing the first rows of $(T_0|\mathbf{0}| - \mathbb{I}_n)$ by the last rows $(T_2|\mathbf{0}|\mathbb{I}_n)$, we replace it by the block $(T_0 + T_2|\mathbf{0}|\mathbf{0})$, without changing the rank of S. As $T = T_0 + T_2$ is invertible, this shows that the matrix S is of rank $3n$. Therefore, there is no syzygies in degree $n-1$. As the sum $2n = \mu_1 + \mu_2$ and $\mu_1 \leq n, \mu_2 \leq n$ where μ_1, μ_2 are the smallest degree of a pair of generators of $\mathcal{L}(\tilde{T}(x), x^n, x^{2n}-1)$ of degree $\leq n$, we have $\mu_1 = \mu_2 = n$. Thus there exist two linearly independent syzygies (u_1, v_1, w_1), (u_2, v_2, w_2) of degree n, which generate $\mathcal{L}(\tilde{T}(x), x^n, x^{2n}-1)$. □

A similar result can also be found in [12], but the proof much longer than this one, is based on interpolation techniques and explicit computations. Let us now describe how to construct explicitly two generators of $\mathcal{L}(\tilde{T}(x), x^n, x^{2n}-1)$ of degree n (see also [12]).

As $\tilde{T}(x)$ is of degree $\leq 2\,n-1$ and the map (2.5) is a surjective function, there exists $(u,v,w) \in \mathbb{K}[x]^3_{n-1}$ such that

$$\tilde{T}(x)u(x) + x^n v(x) + (x^{2\,n}-1)\,w = \tilde{T}(x)x^n, \tag{2.7}$$

we deduce that $(u_1, v_1, w_1) = (x^n - u, -v, -w) \in \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$.

As there exists $(u', v', w') \in \mathbb{K}[x]^3_{n-1}$ such that

$$\tilde{T}(x)u'(x) + x^n v'(x) + (x^{2\,n} - 1)\, w' = 1 = x^n\, x^n - (x^{2\,n} - 1) \tag{2.8}$$

we deduce that $(u_2, v_2, w_2) = (-u', x^n - v', -w' - 1) \in \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$.

Now, the vectors (u_1, v_1, w_1), (u_2, v_2, w_2) of $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$ are linearly independent since by construction, the coefficient vectors of x^n in (u_1, v_1, w_1) and (u_2, v_2, w_2) are respectively $(1, 0, 0)$ and $(0, 1, 0)$.

PROPOSITION 2.7. *The vector u is solution of (2.1) if and only if there exist $v(x) \in \mathbb{K}[x]_{n-1}, w(x) \in \mathbb{K}[x]_{n-1}$ such that*

$$(u(x), v(x), w(x)) \in \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1; g(x))$$

Proof. The vector u is solution of (2.1) if and only if we have

$$\Pi_E(T(x)u(x)) = g(x).$$

As $u(x)$ is of degree $\leq n-1$, we deduce from (2.2) and (2.3) that there exist polynomial $A(x) \in \mathbb{K}[x]_{n-2}$ and $B(x) \in \mathbb{K}[x]_{n-1}$ such that

$$T(x)u(x) - x^{-n+1}A(x) - x^n B(x) = g(x).$$

By evaluation at the roots $\omega \in \mathfrak{U}_{2n}$, and since $\omega^{-n} = \omega^n$ and $\tilde{T}(\omega) = T(\omega)$ for $\omega \in \mathfrak{U}_n$, we have

$$\tilde{T}(\omega)u(\omega) + \omega^n v(\omega) = g(\omega), \forall \omega \in \mathfrak{U}_{2n}(\omega),$$

with $v(x) = -x\, A(x) - B(x)$ of degree $\leq n - 1$. We deduce that there exists $w(x) \in \mathbb{K}[x]$ such that

$$\tilde{T}(x)u(x) + x^n v(x) + (x^{2n} - 1)w(x) = g(x).$$

Notice that $w(x)$ is of degree $\leq n - 1$, because $(x^{2n} - 1)\, w(x)$ is of degree $\leq 3n - 1$.

Conversely, a solution $(u(x), v(x), w(x)) \in \mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1; g(x)) \cap \mathbb{K}[x]^3_{n-1}$ implies a solution $(u, v, w) \in \mathbb{K}^{3\,n}$ of the linear system:

$$S \begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} g \\ 0 \\ 0 \end{pmatrix}$$

where S is has the block structure (2.6), so that $T_2\, u + w = 0$ and $T_0\, u - w = (T_0 + T_2)u = g$. As we have $T_0 + T_2 = T$, the vector u is a solution of (2.1), which ends the proof of the proposition. □

2.2. Euclidean division. As a consequence of proposition 2.6, we have the following property:

PROPOSITION 2.8. *Let $\{(u_1, v_1, w_1), (u_2, v_2, w_2)\}$ a n-basis of $\mathcal{L}(\tilde{T}(x), x^n, x^{2n} - 1)$, the remainder of the division of $\begin{pmatrix} 0 \\ x^n\, g \\ g \end{pmatrix}$ by $\begin{pmatrix} u_1 & u_2 \\ v_1 & v_2 \\ w_1 & w_2 \end{pmatrix}$ is the vector solution given in the proposition (2.7).*

Proof. The vector $\begin{pmatrix} 0 \\ x^n\, g \\ -g \end{pmatrix} \in \mathcal{L}(\tilde{T}(x), x^n, x^{2\,n} - 1; g)$ (a particular solution). We divide it by $\begin{pmatrix} u_1 & u_2 \\ v_1 & v_2 \\ w_1 & w_2 \end{pmatrix}$ we obtain

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} 0 \\ x^n\, g \\ g \end{pmatrix} - \begin{pmatrix} u_1 & u_2 \\ v_1 & v_2 \\ w_1 & w_2 \end{pmatrix} \begin{pmatrix} p \\ q \end{pmatrix}$$

(u,v,w) is the remainder of division, thus $(u,v,w) \in \mathbb{K}[x]^3_{n-1} \cap \mathcal{L}(\tilde{T}(x), x^n, x^{2\,n}-1; g)$. However (u,v,w) is the unique vector $\in \mathbb{K}[x]^3_{n-1} \cap \mathcal{L}(\tilde{T}(x), x^n, x^{2\,n}-1; g)$ because if there is an other vector then their difference is in $\mathcal{L}(\tilde{T}(x), x^n, x^{2\,n}-1) \cap \mathbb{K}[x]^3_{n-1}$ which is equal to $\{(0,0,0)\}$. □

PROBLEM 2.9. *Given a matrix and a vector of polynomials* $\begin{pmatrix} e(x) & e'(x) \\ f(x) & f'(x) \end{pmatrix}$ *of degree* n, *and* $\begin{pmatrix} p(x) \\ q(x) \end{pmatrix}$ *of degree* $m \geq n$, *such that* $\begin{pmatrix} e_n & e'_n \\ f_n & f'_n \end{pmatrix}$ *is invertible; find the remainder of the division of* $\begin{pmatrix} p(x) \\ q(x) \end{pmatrix}$ *by* $\begin{pmatrix} e(x) & e'(x) \\ f(x) & f'(x) \end{pmatrix}$.

PROPOSITION 2.10. *The first coordinate of remainder vector of the division of* $\begin{pmatrix} 0 \\ x^n g \end{pmatrix}$ *by* $\begin{pmatrix} u & u' \\ r & r' \end{pmatrix}$ *is the polynomial* $v(x)$ *solution of* (2.1).

We describe here a generalized Euclidean division algorithm to solve problem (2.9).

Let $E(x) = \begin{pmatrix} p(x) \\ q(x) \end{pmatrix}$ of degree m, $B(x) = \begin{pmatrix} e(x) & e'(x) \\ f(x) & f'(x) \end{pmatrix}$ of degree $n \leq m$. $E(x) = B(x)Q(x) + R(x)$ with $\deg(R(x)) < n$, and $\deg(Q(x)) \leq m-n$. Let $z = \frac{1}{x}$

$$\begin{aligned} & E(x) = B(x)Q(x) + R(x) \\ \Leftrightarrow\ & E(\frac{1}{z}) = B(\frac{1}{z})Q(\frac{1}{z}) + R(\frac{1}{z}) \\ \Leftrightarrow & z^m E(\frac{1}{z}) = z^n B(\frac{1}{z}) z^{m-n} Q(\frac{1}{z}) + z^{m-n+1} z^{n-1} R(\frac{1}{z}) \\ \Leftrightarrow\ & \hat{E}(z) = \hat{B}(z)\hat{Q}(z) + z^{m-n+1}\hat{R}(z) \end{aligned} \tag{2.9}$$

with $\hat{E}(z), \hat{B}(z), \hat{Q}(z), \hat{R}(z)$ are the polynomials obtained by reversing the order of coefficients of polynomials $E(z), B(z), Q(z), R(z)$.

$$\begin{aligned} (2.9) \Rightarrow \frac{\hat{E}(z)}{\hat{B}(z)} &= \hat{Q}(z) + z^{m+n-1}\frac{\hat{R}(z)}{\hat{B}(z)} \\ \Rightarrow \hat{Q}(z) &= \frac{\hat{E}(z)}{\hat{B}(z)} \mod z^{m-n+1} \end{aligned}$$

$\frac{1}{\hat{B}(z)}$ exists because its coefficient of highest degree is invertible. Thus $\hat{Q}(z)$ is obtained by computing the first $m-n+1$ coefficients of $\frac{\hat{E}(z)}{\hat{B}(z)}$.

To find $W(x) = \frac{1}{\hat{B}(x)}$ we will use Newton's iteration: Let $f(W) = \hat{B} - W^{-1}$.
$f'(W_l).(W_{l+1} - W_l) = -W_l^{-1}(W_l + 1 - W_l)W_l^{-1} = f(W_l) = \hat{B} - W_l^{-1}$, thus

$$W_{l+1} = 2W_l - W_l\hat{B}W_l.$$

and $W_0 = \hat{B}_0^{-1}$ which exists.

$$\begin{aligned} W - W_{l+1} &= W - 2W_l + W_l\hat{B}W_l \\ &= W(\mathbb{I}_2 - \hat{B}W_l)^2 \\ &= (W - W_l)\hat{B}(W - W_l) \end{aligned}$$

Thus $W_l(x) = W(x) \mod x^{2l}$ for $l = 0, \ldots, \lceil \log(m-n+1) \rceil$.

PROPOSITION 2.11. *We need* $\mathcal{O}(n\log(n)\log(m-n) + m\log m)$ *arithmetic operations to solve problem* (2.9)

Proof. We must do $\lceil \log(m-n+1) \rceil$ Newton's iteration to obtain the first $m-n+1$ coeficients of $\frac{1}{\hat{B}} = W(x)$. And for each iteration we must do $\mathcal{O}(n\log n)$ arithmetic operations (multiplication of polynimials of degree n). And then we need $\mathcal{O}(m\log m)$ aritmetic operations to do the multiplication $\hat{E}.\frac{1}{\hat{B}}$. □

2.3. Construction of the generators. The canonical basis of $\mathbb{K}[x]^3$ is denoted by $\sigma_1, \sigma_2, \sigma_3$. Let ρ_1, ρ_2 the generators of $\mathcal{L}(\bar{T}(x), x^n, x^{2n}-1)$ of degree n given by

$$\begin{array}{l} \rho_1 = x^n\sigma_1 - (u, v, w) = (u_1, v_1, w_1) \\ \rho_2 = x^n\sigma_2 - (u', v', w') = (u_2, v2, w_2) \end{array} \tag{2.10}$$

with (u, v, w), (u', v', w') are the vector given in (2.7) and (2.8).

We will describe here how we compute (u_1, v_1, w_1) and (u_2, v_2, w_2). We will give two methods to compute them, the second one is the method given in [12]. The first one use the Euclidean gcd algorithm:

We will recal firstly the algebraic and computational properties of the well known extended Euclidean algorithm (see [13]): Given $p(x), p'(x)$ two polynomials in degree m and m' respectively, let

$$\begin{array}{ll} r_0 = p, & r_1 = p', \\ s_0 = 1, & s_1 = 0, \\ t_0 = 0, & t_1 = 1. \end{array}$$

and define

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_i r_i, \\ s_{i+1} &= s_{i-1} - q_i s_i, \\ t_{i+1} &= t_{i-1} - q_i t_i, \end{aligned}$$

where q_i results when the division algorithm is applied to r_{i-1} and r_i, i.e. $r_{i-1} = q_i r_i + r_{i+1}$. $\deg r_{i+1} < \deg r_i$ for $i = 1, \ldots, l$ with l is such that $r_l = 0$, therefore $r_{l-1} = \gcd(p(x), p'(x))$.

PROPOSITION 2.12. *The following relations hold:*

$$s_i p + t_i p' = r_i \quad \textit{and} \quad (s_i, t_i) = 1 \quad \textit{for } i = 1, \ldots, l$$

and

$$\begin{cases} \deg r_{i+1} < \deg r_i, \quad i = 1, \ldots, l-1 \\ \deg s_{i+1} > \deg s_i \quad \textit{and} \quad \deg t_{i+1} > \deg t_i, \\ \deg s_{i+1} = \deg(q_i.s_i) = \deg v - \deg r_i, \\ \deg t_{i+1} = \deg(q_i.t_i) = \deg u - \deg r_i. \end{cases}$$

PROPOSITION 2.13. *By applying the Euclidean gcd algorithm in $p(x) = x^{n-1}T$ and $p'(x) = x^{2n-1}$ in degree $n-1$ and $n-2$ we obtain ρ_1 and ρ_2 respectively*

Proof. We saw that $Tu = g$ if and only if there exist $A(x)$ and $B(x)$ such that

$$\bar{T}(x)u(x) + x^{2n-1}B(x) = x^{n-1}b(x) + A(x)$$

with $\bar{T}(x) = x^{n-1}T(x)$ a polynomial of degree $\leq 2n-2$. In (2.7) and (2.8) we saw that for $g(x) = 1$ ($g = e_1$) and $g(x) = x^n T(x)$ ($g = (0, t_{-n+1}, \ldots, t_{-1})^T$) we obtain a base of $\mathcal{L}(\bar{T}(x), x^n, x^{2n}-1)$. $Tu_1 = e_1$ if and only if there exist $A_1(x)$, $B_1(x)$ such that

$$\bar{T}(x)u_1(x) + x^{2n-1}B_1(x) = x^{n-1} + A_1(x) \tag{2.11}$$

and $Tu_2 = (0, t_{-n+1}, \ldots, t_{-1})^T$ if and only if there exist $A_2(x)$, $B_2(x)$ such that

$$\bar{T}(x)(u_2(x) + x^n) + x^{2n-1}B_2(x) = A_2(x) \tag{2.12}$$

with $\deg A_1(x) \leq n-2$ and $\deg A_2(x) \leq n-2$. Thus By applying the extended Euclidean algorithm in $p(x) = x^{n-1}T$ and $p'(x) = x^{2n-1}$ until we have $\deg r_l(x) = n-1$ and $\deg r_{l+1}(x) = n-2$ we obtain

$$u_1(x) = \frac{1}{c_1}s_l(x), \quad B_1(x) = \frac{1}{c_1}t_l(x), \quad x^{n-1} + A_1(x) = \frac{1}{c_1}r_l(x)$$

and

$$x^n + u_2(x) = \frac{1}{c_2} s_{l+1}(x), \quad B_2(x) = \frac{1}{c_2} t_{l+1}(x), \quad A_2(x) = \frac{1}{c_2} r_{l+1}(x)$$

with c_1 and c_2 are the highest coefficients of $r_l(x)$ and $s_{l+1}(x)$ respectively, in fact: The equation (2.11) is equivalent to

$$\begin{array}{c} \overbrace{}^{n} \quad \overbrace{}^{n-1} \\ \left.\begin{array}{l} \\ n-1 \\ \\ n \\ \\ n-1 \\ \\ \end{array}\right\{ \end{array} \left(\begin{array}{ccc|ccc} t_{-n+1} & & & & & \\ \vdots & \ddots & & & & \\ \hline t_0 & \dots & t_{-n+1} & & & \\ \vdots & \ddots & \vdots & & & \\ t_{n-1} & \dots & t_0 & & & \\ \hline & \ddots & \vdots & 1 & & \\ & & & & \ddots & \\ & & t_{n-1} & & & 1 \end{array}\right) \left(\begin{array}{c} u_1 \\ \\ B_1 \\ \\ \end{array}\right) = \left(\begin{array}{c} A_1 \\ \hline 1 \\ 0 \\ \vdots \\ 0 \end{array}\right)$$

since T is invertible then the $(2n-1) \times (2n-1)$ block at the bottom is invertible and then u_1 and B_1 are unique, therefore u_1, B_1 and A_1 are unique. And, by proposition (2.12), $\deg r_l = n-1$ ($r_l = c_1(x^n + A_1(x))$ then $\deg s_{l+1} = (2n-1) - (n-1) = n$ and $\deg t_{l+1} = (2n-2) - (n-1) = n-1$ thus, by the same proposition, $\deg s_l \leq n-1$ and $\deg t_l \leq n-2$. Therfore $\frac{1}{c_1} s_l = u_1$ and $\frac{1}{c_1} t_l = B_1$.

Finaly, $Tu = e_1$ if and only if there exist $v(x)$, $w(x)$ such that

$$\tilde{T}(x)u(x) + x^n v(x) + (x^{2n} - 1)w(x) = 1 \tag{2.13}$$

$\tilde{T}(x) = T^+ + x^{2n} T^- = T + (x^{2n} - 1)T^-$thus

$$T(x)u(x) + x^n v(x) + (x^{2n} - 1)(w(x) + T^-(x)u(x)) = 1 \tag{2.14}$$

of a other hand $T(x)u(x) - x^{-n+1}A_1(x) + x^n B_1(x) = 1$ and $x^{-n+1}A_1(x) = x^n(xA_1) - x^{-n}(x^{2n} - 1)xA_1$ thus

$$T(x)u(x) + x^n(B(x) - xA(x)) + (x^{2n} - 1)x^{-n+1}A(x) = 1 \tag{2.15}$$

By comparing (2.14) and (2.15), and as $1 = x^n x^n - (x^{2n} - 1)$ we have the proposition and we have $w(x) = x^{-n+1}A(x) - T_-(x)u(x) + 1$ which is the part of positif degree of $-T_-(x)u(x) + 1$. □

Remark 2.14. *A superfast euclidean gcd algorithm, wich uses no more then $\mathcal{O}(nlog^2 n)$, is given in [13] chapter 11.*

The second methode to compute (u_1, v_1, w_1) and (u_2, v_2, w_2) is given in [12]. We are interested in computing the coefficients of σ_1, σ_2, the coefficients of σ_3 correspond to elements in the ideal $(x^{2n} - 1)$ and thus can be obtain by reduction of $(\tilde{T}(x)\, x^n).B(x)$ by $x^{2n} - 1$, with $B(x) = \begin{pmatrix} x^n - u_0 & -v_0 \\ -u_1 & x^n - v_1 \end{pmatrix} = \begin{pmatrix} u(x) & v(x) \\ u'(x) & v'(x) \end{pmatrix}$.

A superfast algorithm to compute $B(x)$ is given in [12]. Let us describe how to compute it.

By evaluation of (2.10) at the roots $\omega_j \in \mathfrak{U}_{2n}$ we deduce that $(u(x)\, v(x))^T$ and $(u'(x)\, v'(x))^T$ are the solution of the following rational interpolation problem:

$$\left\{ \begin{array}{l} \tilde{T}(\omega_j)u(\omega_j) + \omega_j^n v(\omega_j) = 0 \\ \tilde{T}(\omega_j)u'(\omega_j) + \omega_j^n v'(\omega_j) = 0 \end{array} \right. \quad \text{with}$$

$$\left\{ \begin{array}{l} u_n = 1,\ v_n = 0 \\ u'_n = 0,\ v'_n = 1 \end{array} \right.$$

Definition 2.15. *The τ-degree of a vector polynomial $w(x) = (w_1(x)\, w_2(x))^T$ is defined as*

$$\tau - \deg w(x) := \max\{\deg w_1(x),\ \deg w_2(x) - \tau\}$$

$B(x)$ is a $n-$reduced basis of the module of all vector polynomials $r(x) \in \mathbb{K}[x]^2$ that satisfy the interpolation conditions

$$f_j^T r(\omega_j) = 0, \;\; j = 0, \ldots, 2n-1$$

with $f_j = \begin{pmatrix} \tilde{T}(\omega_j) \\ \omega_j^n \end{pmatrix}$.

$B(x)$ is called a $\tau-$reduced basis (with $\tau = n$) that corresponds to the interpolation data (ω_j, f_j), $j = 0, \ldots, 2n-1$.

DEFINITION 2.16. *A set of vector polynomial in $\mathbb{K}[x]^2$ is called τ-reduced if the τ-highest degree coefficients are lineary independent.*

THEOREM 2.17. *Let $\tau = n$. Suppose J is a positive integer. Let $\sigma_1, \ldots, \sigma_J \in \mathbb{K}$ and $\phi_1, \ldots, \phi_J \in \mathbb{K}^2$ wich are $\neq (0\,0)^T$. Let $1 \leq j \leq J$ and $\tau_J \in \mathbb{Z}$. Suppose that $B_j(x) \in \mathbb{K}[x]^{2\times 2}$ is a τ_J-reduced basis matrix with basis vectors having τ_J-degree δ_1 and δ_2, respectively, corresponding to the interpolation data $\{(\sigma_i, \phi_i); i = 1, \ldots, j\}$.*

Let $\tau_{j\to J} := \delta_1 - \delta_2$. Let $B_{j\to J}(x)$ be a $\tau_{j\to J}$-reduced basis matrix corresponding to the interpolation data $\{(\sigma_i, B_j^T(\sigma_j)\phi_i); i = j+1, \ldots, J\}$.

Then $B_J(x) := B_j(x)B_{j\to J}(x)$ is a τ_J-reduced basis matrix corresponding to the interpolation data $\{(\sigma_i, \phi_i); i = 1, \ldots, J\}$.

Proof. For the proof, see [12]. □

When we apply this theorem for the $\omega_j \in \mathfrak{U}_{2n}$ as interpolation points, we obtain a superfast algorithm ($\mathcal{O}(n \log^2 n)$) wich compute $B(x)$.[12]

We consider the two following problems:

3. Bivariate case. Let $m \in \mathbb{N}, m \in \mathbb{N}$. In this section we denote by $E = \{(i,j);\ 0 \leq i \leq m-1, 0 \leq j \leq n-1\}$, and $R = \mathbb{K}[x,y]$. We denote by $\mathbb{K}[x,y]_n^m$ the vector space of bivariate polynomials of degree $\leq m$ in x and $\leq n$ in y.

NOTATION 3.1. *For a block matrix M, of block size n and each block is of size m, we will use the following indication :*

$$M = \left(M_{(i_1,i_2),(j_1,j_2)}\right)_{\substack{0\leq i_1,j_1\leq m-1 \\ 0\leq i_2,j_2\leq n-1}} = (M_{\alpha\beta})_{\alpha,\beta\in E}. \tag{3.1}$$

(i_2, j_2) gives the block's positions, (i_1, j_1) the position in the blocks.

PROBLEM 3.2. *Given a Toeplitz block Toeplitz matrix $T = (t_{\alpha-\beta})_{\alpha\in E,\beta\in E} \in \mathbb{K}^{mn\times mn}$ ($T = (T_{\alpha\beta})_{\alpha,\beta\in E}$ with $T_{\alpha\beta} = t_{\alpha-\beta}$) of size mn and $g = (g_\alpha)_{\alpha\in \mathtt{E}} \in \mathbb{K}^{mn}$, find $u = (u_\alpha)_{\alpha\in\mathtt{E}}$ such that*

$$T\,u = g \tag{3.2}$$

DEFINITION 3.3. *We define the following polynomials:*

- $T(x,y) := \sum_{\substack{(i,j)\in \mathtt{E}-\mathtt{E} \\ 2n-1,2m-1}} t_{i,j} x^i y^j$,
- $\tilde{T}(x,y) := \sum_{i,j=0} \tilde{t}_{i,j} x^i y^j$ *with*

$$\tilde{t}_{i,j} := \begin{cases} t_{i,j} & si\ i < m, j < n \\ t_{i-2m,j} & si\ i \geq m, j < n \\ t_{i,j-2n} & si\ i < m, j \geq n \\ t_{i-2m,j-2n} & si\ i \geq m, i \geq n \end{cases},$$

- $u(x,y) := \sum_{(i,j)\in\mathtt{E}} u_{i,j}\, x^i y^j$, $g(x,y) := \sum_{(i,j)\in\mathtt{E}} g_{i,j} x^i y^j$.

3.1. Moving hyperplanes. For any non-zero vector of polynomials $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{K}[x,y]^n$, we denote by $\mathcal{L}(\mathbf{a})$ the set of vectors $(h_1, \ldots, h_n) \in \mathbb{K}[x,y]^n$ such that

$$\sum_{i=1}^{n} a_i\, h_i = 0. \tag{3.3}$$

It is a $\mathbb{K}[x,y]$-module of $\mathbb{K}[x,y]^n$.

PROPOSITION 3.4. *The vector u is solution of (3.2) if and only if there exist $h_2,\dots,h_9 \in \mathbb{K}[x,y]_{\substack{m-1\\n-1}}$ such that $(u(x,y),h_2(x,y),\dots,h_9(x,y))$ belongs to*
$\mathcal{L}(\tilde{T}(x,y),x^m,x^{2\,m}-1,y^n,x^m\,y^n,(x^{2\,m}-1)\,y^n,y^{2\,n}-1,x^m(y^{2\,n}-1),(x^{2\,m}-1)\,(y^{2\,n}-1))$.

Proof. Let $L=\{x^{\alpha_1}y^{\alpha_2},0\le\alpha_1\le m-1,0\le\alpha_2\le n-1\}$, and Π_E the projection of R on the vector space generated by L. By [8], we have

$$T\,u=g\Leftrightarrow\Pi_E(T(x,y)\,u(x,y))=g(x,y) \tag{3.4}$$

which implies that

$$\begin{aligned}T(x,y)u(x,y)=g(x,y)+x^my^nA_1(x,y)+x^my^{-n}A_2(x,y)+x^{-m}y^nA_3(x,y)+x^{-m}y^{-n}A_4(x,y)\\+x^mA_5(x,y)+x^{-m}A_6(x,y)+y^nA_7(x,y)+y^{-n}A_8(x,y),\end{aligned} \tag{3.5}$$

where the $A_i(x,y)$ are polynomials of degree at most $m-1$ in x and $n-1$ in y. Since $\omega^m=\omega^{-m}$, $\upsilon^n=\upsilon^{-n}$, $\tilde{T}(\omega,\upsilon)=T(\omega,\upsilon)$ for $\omega\in\mathfrak{U}_{2\,m}$, $\upsilon\in\mathfrak{U}_{2\,n}$, we deduce by evaluation at the roots $\omega\in\mathfrak{U}_{2\,m}$, $\upsilon\in\mathfrak{U}_{2\,n}$ that

$$R(x,y):=\tilde{T}(x,y)u(x,y)+x^mh_2(x,y)+y^nh_4(x,y)+x^my^nh_5(x,y)-g(x,y)\in(x^{2\,m}-1,y^{2\,n}-1)$$

with $h_2=-(A_5+A_6)$, $h_4=-(A_7+A_8)$, $h_5=-(A_1(x,y)+A_2(x,y)+A_3(x,y)+A_4(x,y))$.

By reduction by the polynomials $x^{2\,m}-1$, $y^{2\,n}-1$, and as $R(x,y)$ is of degree $\le 3m-1$ in x and $\le 3n-1$ in y, there exist $h_3(x,y),h_6(x,y),\dots,h_8(x,y)\in\mathbb{K}[x,y]_{\substack{m-1\\n-1}}$ such that

$$\begin{aligned}&\tilde{T}(x,y)u(x,y)+x^m\,h_2(x,y)+(x^{2m}-1)h_3(x,y)+y^nh_4(x,y)+x^my^nh_5(x,y)+\\&(x^{2m}-1)y^nh_6(x,y)+(y^{2n}-1)h_7(x,y)+x^m(y^{2m}-1)h_7(x,y)+(x^{2n}-1)(y^{2n}-1)h_8(x,y)=g(x,y).\end{aligned} \tag{3.6}$$

Conversely a solution of (3.6) can be transformed into a solution of (3.5), which ends the proof of the proposition. □

In the following, we are going to denote by $\mathbf{T}$ the vector $\mathbf{T}=(\tilde{T}(x,y),x^m,x^{2\,m}-1,y^n,x^m\,y^n,(x^{2\,m}-1)\,y^n,y^{2\,n}-1,x^m(y^{2\,n}-1),(x^{2\,m}-1)\,(y^{2\,n}-1))$.

PROPOSITION 3.5. *There is no elements of $\mathbb{K}[x,y]_{\substack{m-1\\n-1}}$ in $\mathcal{L}(\mathbf{T})$.*

Proof. We consider the map

$$\mathbb{K}[x,y]^9_{\substack{m-1\\n-1}}\to\mathbb{K}[x,y]_{\substack{3m-1\\3n-1}} \tag{3.7}$$

$$p(x,y)=(p_1(x,y),\dots,p_9(x,y))\mapsto\mathbf{T}.p \tag{3.8}$$

$$\tag{3.9}$$

which $9mn\times 9mn$ matrix is of the form

$$S:=\left(\begin{array}{c|cc|ccc|ccc}
 & E_{21} & -E_{11}+E_{31} & & & & -E_{11} & -E_{21} & E_{11}-E_{31}\\
T_0 & \vdots & \vdots & & & & \vdots & \vdots & \vdots\\
 & E_{2n} & -E_{1n}+E_{3n} & & & & -E_{1n} & -E_{2n} & E_{1n}-E_{3n}\\
\hline
 & & & E_{11} & E_{21} & -E_{11}+E_{31} & & & \\
T_1 & & & \vdots & \vdots & \vdots & & & \\
 & & & E_{1n} & E_{2n} & -E_{1n}+E_{3n} & & & \\
\hline
 & & & & & & E_{11} & E_{21} & -E_{11}+E_{31}\\
T_2 & & & & & & \vdots & \vdots & \vdots\\
 & & & & & & E_{1n} & E_{2n} & -E_{1n}+E_{3n}
\end{array}\right) \tag{3.10}$$

with E_{ij} is the $3m\times mn$ matrix $e_{ij}\otimes I_m$ and e_{ij} is the $3\times n$ matrix with entries equal zero except

the (i,j)th entrie equal 1. And the matrix $\begin{pmatrix} T_0 \\ T_1 \\ T_2 \end{pmatrix}$ is the following $9mn \times m$ matrix

$$\left(\begin{array}{cccc} t_0 & 0 & \dots & 0 \\ t_1 & t_0 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ t_{n-1} & \dots & t_1 & t_0 \\ \hline 0 & t_{n-1} & \dots & t_1 \\ t_{-n+1} & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & t_{-n+1} \\ t_{-1} & \dots & t_{-n+1} & 0 \\ \hline 0 & t_{-1} & \dots & t_{-n+1} \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & t_{-1} \\ 0 & \dots & \dots & 0 \end{array}\right) \text{ and } t_i = \left(\begin{array}{cccc} t_{i,0} & 0 & \dots & 0 \\ t_{i,1} & t_{i,0} & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ t_{i,n-1} & \dots & t_{i,1} & t_{i,0} \\ \hline 0 & t_{i,m-1} & \dots & t_{i,1} \\ t_{i,-m+1} & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & t_{i,-m+1} \\ t_{i,-1} & \dots & t_{i,-m+1} & 0 \\ \hline 0 & t_{i,-1} & \dots & t_{i,-m+1} \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & t_{i,-1} \\ 0 & \dots & \dots & 0 \end{array}\right)$$

For the same reasons in the proof of proposition (2.6) the matrix S is invertible. □

THEOREM 3.6. *For any non-zero vector of polynomials* $\mathbf{a} = (a_i)_{i=1,\dots,n} \in \mathbb{K}[x,y]^n$*, the* $\mathbb{K}[x,y]$*-module* $\mathcal{L}(a_1,\dots,a_n)$ *is free of rank* $n-1$*.*

Proof. Consider first the case where a_i are monomials.

$a_i = x^{\alpha_i} y^{\beta_i}$ that are sorted in lexicographic order such that $x < y$, a_1 being the biggest and a_n the smallest. Then the module of syzygies of $\mathbf{a}$ is generated by the S-polynomials:

$$S(a_i,a_j) = \operatorname{lcm}(a_i,a_j)\left(\frac{\sigma_i}{a_i} - \frac{\sigma_j}{a_j}\right),$$

where $(\sigma_i)_{i=1,\dots,n}$ is the canonical basis of $\mathbb{K}[x,y]^n$ [3]. We easily check that $S(a_i,a_k) = \frac{\operatorname{lcm}(a_i,a_k)}{\operatorname{lcm}(a_i,a_j)} S(a_i,a_j) - \frac{\operatorname{lcm}(a_i,a_k)}{\operatorname{lcm}(a_j,a_k)} S(a_j,a_k)$ if $i \neq j \neq k$ and $\operatorname{lcm}(a_i,a_j)$ divides $\operatorname{lcm}(a_i,a_k)$. Therefore $\mathcal{L}(\mathbf{a})$ is generated by the $S(a_i,a_j)$ which are minimal for the division, that is, by $S(a_i,a_{i+1})$ (for $i = 1,\dots,n-1$), since the monomials a_i are sorted lexicographically. As the syzygies $S(a_i,a_{i+1})$ involve the basis elements σ_i, σ_{i+1}, they are linearly independent over $\mathbb{K}[x,y]$, which shows that $\mathcal{L}(\mathbf{a})$ is a free module of rank $n-1$ and that we have the following resolution:

$$0 \to \mathbb{K}[x,y]^{n-1} \to \mathbb{K}[x,y]^n \to (\mathbf{a}) \to 0.$$

Suppose now that a_i are general polynomials $\in \mathbb{K}[x,y]$ and let us compute a Gröbner basis of a_i, for a monomial ordering refining the degree [3]. We denote by $m_1,\dots,m_s$ the leading terms of the polynomials in this Gröbner basis, sorted by lexicographic order.

The previous construction yields a resolution of $(m_1, \dots, m_s)$:

$$0 \to \mathbb{K}[x,y]^{s-1} \to \mathbb{K}[x,y]^s \to (m_i)_{i=1,\dots,s} \to 0.$$

Using [7] (or [3]), this resolution can be deformed into a resolution of $(\mathbf{a})$, of the form

$$0 \to \mathbb{K}[x,y]^p \to \mathbb{K}[x,y]^n \to (\mathbf{a}) \to 0,$$

which shows that $\mathcal{L}(\mathbf{a})$ is also a free module. Its rank p is necessarily equal to $n-1$, since the alternate sum of the dimensions of the vector spaces of elements of degree $\leq \nu$ in each module of this resolution should be 0, for $\nu \in \mathbb{N}$. □

3.2. Generators and reduction. In this section, we describe an explicit set of generators of $\mathcal{L}(\mathbf{T})$. The canonical basis of $\mathbb{K}[x,y]^9$ is denoted by $\sigma_1,\dots,\sigma_9$.

First as $\tilde{T}(x,y)$ is of degree $\leq 2m-1$ in x and $\leq 2n-1$ in y and as the function (3.7) in surjective, there exists $u_1, u_2 \in \mathbb{K}[x,y]^9_{\substack{m-1 \\ n-1}}$ such that $\mathbf{T} \cdot u_1 = \tilde{T}(x,y)x^m$, $\mathbf{T} \cdot u_2 = \tilde{T}(x,y)y^n$. Thus,

$$\rho_1 = x^m\sigma_1 - u_1 \in \mathcal{L}(\mathbf{T}),$$
$$\rho_2 = y^n\sigma_1 - u_2 \in \mathcal{L}(\mathbf{T}).$$

We also have $u_3 \in \mathbb{K}[x,y]^{m-1,3}_{n-1}$, such that $\mathbf{T}\cdot u_3 = 1 = x^m\, x^m - (x^{2\,m}-1) = y^n\, y^n - (y^{2\,n}-1)$. We deduce that

$$\rho_3 = x^m\sigma_2 - \sigma_3 - u_3 \in \mathcal{L}(\mathbf{T}),$$
$$\rho_4 = y^n\sigma_4 - \sigma_7 - u_3 \in \mathcal{L}(\mathbf{T}).$$

Finally, we have the obvious relations:

$$\rho_5 = y^n\sigma_2 - \sigma_5 \in \mathcal{L}(\mathbf{T}),$$
$$\rho_6 = x^m\sigma_4 - \sigma_5 \in \mathcal{L}(\mathbf{T}),$$
$$\rho_7 = x^m\sigma_5 - \sigma_6 + \sigma_4 \in \mathcal{L}(\mathbf{T}),$$
$$\rho_8 = y^n\sigma_5 - \sigma_8 + \sigma_2 \in \mathcal{L}(\mathbf{T}).$$

PROPOSITION 3.7. *The relations $\rho_1,\ldots,\rho_8$ form a basis of $\mathcal{L}(\mathbf{T})$.*

Proof. Let $\mathbf{h} = (h_1,\ldots,h_9) \in \mathcal{L}(\mathbf{T})$. By reduction by the previous elements of $\mathcal{L}(\mathbf{T})$, we can assume that the coefficients h_1, h_2, h_4, h_5 are in $\mathbb{K}[x,y]^{m-1,3}_{n-1}$. Thus, $\tilde{T}(x,y)h_1 + x^m h_2 + y^n h_4 + x^m y^n h_5 \in (x^{2\,n}-1, y^{2\,m}-1)$. As this polynomial is of degree $\leq 3\,m-1$ in x and $\leq 3\,n-1$ in y, by reduction by the polynomials, we deduce that the coefficients $h_3, h_6, \ldots, h_9$ are in $\mathbb{K}[x,y]^{m-1,3}_{n-1}$. By proposition 3.5, there is no non-zero syzygy in $\mathbb{K}[x,y]^{9}_{m-1,n-1}$. Thus we have $\mathbf{h} = 0$ and every element of $\mathcal{L}(\mathbf{T})$ can be reduced to 0 by the previous relations. In other words, $\rho_1,\ldots,\rho_8$ is a generating set of the $\mathbb{K}[x,y]$-module $\mathcal{L}(\mathbf{T})$. By theorem 3.6, the relations ρ_i cannot be dependent over $\mathbb{K}[x,y]$ and thus form a basis of $\mathcal{L}(\mathbf{T})$. □

3.3. Interpolation. Our aim is now to compute efficiently a system of generators of $\mathcal{L}(\mathbf{T})$.

More precisely, we are interested in computing the coefficients of $\sigma_1, \sigma_2, \sigma_4, \sigma_5$ of ρ_1, ρ_2, ρ_3. Let us call $B(x,y)$ the corresponding coefficient matrix, which is of the form:

$$\begin{pmatrix} x^m & y^n & 0 \\ 0 & 0 & x^m \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \mathbb{K}[x,y]^{4,3}_{m-1,n-1} \tag{3.11}$$

Notice that the other coefficients of the relations ρ_1, ρ_2, ρ_3 correspond to elements in the ideal $(x^{2\,m}-1, y^{2\,n}-1)$ and thus can be obtained easily by reduction of the entries of $(\tilde{T}(x,y), x^m, y^n, x^m\, y^n)\cdot B(x,y)$ by the polynomials $x^{2\,m}-1, y^{2\,n}-1$.

Notice also that the relation ρ_4 can be easily deduced from ρ_3, since we have $\rho_3 - x^m\sigma_2 + \sigma_3 + y^n\,\sigma_4 - \sigma_7 = \rho_4$. Since the other relations ρ_i (for $i > 4$) are explicit and independent of $\tilde{T}(x,y)$, we can easily deduce a basis of $\mathcal{L}(\mathbf{T})$ from the matrix $B(x,y)$.

As in $\mathcal{L}(\mathbf{T}) \cap \mathbb{K}[x,y]^{m-1,3}_{n-1}$ there is only one element, thus by computing the basis given in proposition (3.7) and reducing it we can obtain this element in $\mathcal{L}(\mathbf{T}) \cap \mathbb{K}[x,y]^{m-1,3}_{n-1}$ which gives us the solution of $Tu = g$. We can give a fast algorithm to do these two step, but a superfast algorithm is not available.

4. Conclusions. We show in this paper a correlation between the solution of a Toeplitz system and the syzygies of polynomials. We generalized this way, and we gave a correlation between the solution of a Toeplitz-block-Toeplitz system and the syzygies of bivariate polynomials. In the univariate case we could exploit this correlation to give a superfast resolution algorithm. The generalization of this technique to the bivariate case is not very clear and it remains an important challenge.

REFERENCES

[1] D. Bini and V. Y. Pan. *Polynomial and matrix computations. Vol. 1.* Progress in Theoretical Computer Science. Birkhäuser Boston Inc., Boston, MA, 1994. Fundamental algorithms.

[2] R. Bitmead and B. Anderson. Asymptotically fast solution of Toeplitz and related systems of equations. *Linear Algebra and Its Applications*, 34:103–116, 1980.

[3] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[4] P. Fuhrmann. *A polynomial approach to linear algebra*. Springer-Verlag, 1996.

[5] G. Heinig and K. Rost. *Algebraic methods for Toeplitz-like matrices and operators*, volume 13 of *Operator Theory: Advances and Applications*. Birkhäuser Verlag, Basel, 1984.

[6] T. Kailath and A. H. Sayed. Displacement structure: theory and applications. *SIAM Rev.*, 37(3):297–386, 1995.
[7] H. M. Möller and F. Mora. New constructive methods in classical ideal theory. *J. Algebra*, 100(1):138–178, 1986.
[8] B. Mourrain and V. Y. Pan. Multivariate polynomials, duality, and structured matrices. *J. Complexity*, 16(1):110–180, 2000.
[9] V. Y. Pan. Nearly optimal computations with structured matrices. In *Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms (San Francisco, CA, 2000)*, pages 953–962, New York, 2000. ACM.
[10] V. Y. Pan. *Structured matrices and polynomials*. Birkhäuser Boston Inc., Boston, MA, 2001. Unified superfast algorithms.
[11] E. Tyrtyshnikov. Fast algorithms for block Toeplitz matrices. *Sov. J. Numer. Math. Modelling*, 1(2):121–139, 1985.
[12] M. Van Barel, G. Heinig, and P. Kravanja. A stabilized superfast solver for nonsymmetric Toeplitz systems. *SIAM J. Matrix Anal. Appl.*, 23(2):494–510 (electronic), 2001.
[13] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, second edition, 2003.