Symmetric Subresultants and Applications

Cyril Brunie

Université de Limoges, Département de Mathématiques, 126 av. Albert Thomas, 87060 Limoges Cédex, France.

Philippe Saux Picart

Université de Bretagne Occidentale, Département de Mathématiques, 6 av. Victor Le Gorgeu, 29285 Brest Cédex, France.

Abstract

SCHUR's transforms of a polynomial are used to count its roots in the unit disk. These are generalized them by introducing the sequence of symmetric sub-resultants of two polynomials. Although they do have a determinantal definition, we show that they satisfy a structure theorem which allows us to compute them with a type of Euclidean division. As a consequence, a fast algorithm based on a dichotomic process and FFT is designed.

We prove also that these symmetric sub-resultants have a deep link with TOEPLITZ matrices. Finally, we propose a new algorithm of inversion for such matrices. It has the same cost as those already known, however it is fraction-free and consequently well adapted to computer algebra.

---

1 Introduction

Let $P = a_0 + a_1X + \cdots + a_dX^d$ be a polynomial in $\mathbb{C}[X]$. In 1918 SCHUR gave a method to compute the number of roots of P in the unit disk [28]. This work was completed by COHN in 1922 [7].

The so-called SCHUR-COHN algorithm works as follows. Suppose that $a_0a_d \neq 0$ and define the reciprocal of P by $P^* = X^d\bar{P}(1/X)$. Compute the following

---

Email addresses: `brunie@unilim.fr` (Cyril Brunie), `sauxpica@univ-brest.fr` (Philippe Saux Picart).

Preprint submitted to Elsevier Science *29 March 2007*

sequence of polynomials :

$$T(P) = \overline{P(0)}P - \mathrm{lc}\,(P)P^*, \;\; T^k(P) = T(T^{k-1}(P)),$$

where $\mathrm{lc}\,(P)$ denotes the leading coefficient of P. This sequence is finite : it has at most $\deg(P)$ polynomials with decreasing degrees and real constant terms. It is the variation of the signs of these constant terms, all supposed to be non-zero, which gives us the number of roots of P in the unit disk. See HENRICI [17] or MARDEN [25] for a precise description of this algorithm.

In this primary version, two difficulties arise. First, the algorithm does not work for every polynomial : if the difference of the degrees of two successive transforms $T^k(P)$ is more than one, or if some constant terms are zero, it is not possible to compute the number of roots of P. Second, the exact computation of these transforms suffer from an exponential increase of the size of the coefficients : at each step, the length of the coefficients is approximately doubled.

For these two reasons, we introduced the new sequence of SCHUR-COHN SUBTRANSFORMS (see SAUX PICART [33]). These subtransforms are equal to $T^k(P)$ up to a multiplicative factor, can be computed for every polynomial, have a determinantal definition, and an approximately linear increase is their coefficients. Moreover from the constant terms, we can compute the number of roots of the polynomial in the unit disk, using an adapted rule of signs.

Later on, it appeared that the sequence of the SCHUR-COHN SUBTRANSFORMS is linked to the sequence of the successive remainders of P and P^* in a special "symmetric" division (see BRUNIE and SAUX PICART [5]). This division consists in eliminating from the largest polynomial as many monomials as possible from the top as well as from the tail by adding good multiples of the "divisor". In the article cited above, we give a structural theorem, which describes the link between these two sequences built from P.

In the present article we generalise the definition of the SCHUR-COHN SUBTRANSFORMS and the symmetric division of two polynomials to a general situation (no restriction on P and P^*). We will speak of SYMMETRIC SUBRESULTANTS of two polynomials. We are then able to formulate a new general "structure-theorem" which constitutes a central result of our work. With this, we compute the sequence of symmetric subresultants, using a EUCLID-like algorithm instead of the determinantal definition. A dichotomic process and DFT allow us to produce a fast algorithm. Our methods are adaptated from ideas introduced by SCHÖNAGE for the computation of Euclidean remainder sequences in [29], and by LICKTEIG and ROY in [23] for the computation of classical subresultants. The algorithm cost is of $\mathcal{O}(\mathcal{M}(d)\log d)$ arithmetical operations, where $\mathcal{M}(d)$ denotes the cost of the multiplication of two polynomials of degree d.

We will not describe the application to the number of roots of a polynomial in the unit disk as it has already been discussed in [5]. However there are well-known relations between the problem of root isolation and TOEPLITZ matrices (see for example, M.G. KREIN and M.A. NAIMARK [20]). We use these links to give, in the last part, a fast algorithm for solving TOEPLITZ systems with exact computation. It has the same cost as the well-known algorithm of BRENT, GUSTAVSON and YUN in [2], or those of GEMIGNIANI in [13]. Morover, it is fraction free and consequently well adapted to computer algebra. We also give a new way to compute the signature of a Hermitian TOEPLITZ matrix.

This paper is organised as follows. Section 2 introduces notations and definitions. In Section 3, we state the structure-theorem. Section 4 describes how to efficiently compute the symmetric subresultants and the last section applies these results to TOEPLITZ matrices.

Finally, we wish to thank M.-F. ROY and T. LICKTEIG for their help and interest in this work.

2 Definitions and Notations

Consider a subring $\mathbb{D}$ of $\mathbb{C}$ and define the valuation of a nonzero polynomial $P \in \mathbb{D}[X]$, denoted by $v(P)$, as the greatest integer v such that X^v divides P (it is also named "X-adic valuation" in many books). For the zero polynomial put $\deg(0) = -\infty$ and $v(0) = \infty$. Denote by $\mathbb{D}'$ the quotient field of $\mathbb{D}$.

We write $\mathrm{co}_k(P)$ for the coefficient of order k of P. If $\deg P = d$, the leading coefficient $\mathrm{co}_d(P)$ is $\mathrm{lc}\,(P)$ and the trailing coefficient $\mathrm{co}_{v(P)}(P)$ is denoted by $\mathrm{tc}\,(P)$. Remark : if $v(P) \neq 0$, $\mathrm{tc}\,(P)$ is different from $P(0)$.

We will use Euclidean division of a polynomial A by a polynomial B in $\mathbb{D}[X]$: the notation $\mathrm{quo}(A, B)$ stands for the quotient and $\mathrm{rem}(A, B)$ for the remainder; they have their coefficients in the fraction-field $\mathbb{D}'$. We say that the division is *exact* if $\mathrm{quo}(A, B)$ and $\mathrm{rem}(A, B)$ are elements of $\mathbb{D}$. Please note : our definition of exact division differs from another definition common in the literature where exact division simply means vanishing of the Euclidean remainder.

Now, let us introduce the main object of our article.

2.1 Symmetric Subresultants

Let $A = \sum_{i=0}^{d} a_i X^i$ and $B = \sum_{i=0}^{d} b_i X^i$ be two polynomials in $\mathbb{D}[X]$. We suppose that one of them at least, say A, has its degree equal to d ; B can also be formally considered as having degree d : if $\deg B = d' < d$, B will be replaced by $0X^d + \cdots + 0X^{d-d'+1} + B$. We also assume that the valuation is 0 for at least one of them, otherwise we divide both polynomials by a power of X to ensure this condition. Define :

$$\mathrm{Sylv}_j(A,B) = \underbrace{\begin{pmatrix} a_0 & \cdots & \cdots & \cdots & \cdots & a_d & & \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & a_0 & \cdots & \cdots & \cdots & \cdots & a_d \\ b_0 & \cdots & \cdots & \cdots & \cdots & b_d & & \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & b_0 & \cdots & \cdots & \cdots & \cdots & b_d \end{pmatrix}}_{d+j} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \end{matrix}}\right\} j \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \end{matrix}}\right\} j \end{matrix}$$

to be a submatrix of the full SYLVESTER matrix $\mathrm{Sylv}_d(A,B)$.
For $\ell = 0, \ldots, d-j$, let $\mathrm{Sylv}_{j,\ell} = \mathrm{Sylv}_{j,\ell}(A,B)$ be the following $2j \times 2j$ square submatrix of $\mathrm{Sylv}_j(A,B)$:

$$\mathrm{Sylv}_{j,\ell} = \begin{pmatrix} a_0 & \cdots & a_{j-2} & a_{j-1+\ell} & a_d & & & \\ & \ddots & \vdots & \vdots & \vdots & \ddots & & \\ & & a_0 & a_{\ell+1} & a_{d-j+2} & \cdots & a_d & \\ & & 0 & a_\ell & a_{d-j+1} & \cdots & a_{d-1} & a_d \\ b_0 & \cdots & b_{j-2} & b_{j-1+\ell} & b_d & & & \\ & \ddots & \vdots & \vdots & \vdots & \ddots & & \\ & & b_0 & b_{\ell+1} & b_{d-j+2} & \cdots & b_d & \\ & & 0 & b_\ell & b_{d-j+1} & \cdots & b_{d-1} & b_d \\ \multicolumn{3}{c}{\underbrace{\hphantom{b_0 \quad \cdots \quad b_{j-2}}}_{j-1}} & & \multicolumn{4}{c}{\underbrace{\hphantom{b_{d-j+1} \quad \cdots \quad b_{d-1} \quad b_d}}_{j}} \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} j \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} j \end{matrix} .$$

The sequence $(S_j)_{-1 \le j \le d}$ of symmetric subresultants of A and B is defined by :

- $S_{-1} = A$,
- $S_0 = B$,
- $S_j(A,B) = \sum_{\ell=0}^{d-j} \det(\mathrm{Sylv}_{j,\ell}) X^\ell, \quad$ if $1 \le j \le d$.

Clearly, S_j is an element of $\mathbb{D}[X]$ for any j. The last one, S_d is just the resultant of A and B. In the generic situation, S_j is of degree $d-j$ and valuation 0.

However, the real degree could be less than $d-j$ and the valuation greater than 0. In order to describe these situations, we introduce the following definition.

Let (α, β) be such that :

$$\left\{\begin{array}{rcl} v(S_j) & = & 0 \\ \deg(S_j) & = & d-j \end{array}\right. \quad \text{and} \quad \left\{\begin{array}{rcl} v(S_{j+1}) & = & \alpha \\ \deg(S_{j+1}) & = & d-j-\beta \end{array}\right. ,$$

we will then say that the pair (S_j, S_{j+1}) is (α, β)**-defective**. The case $(0, 1)$ is just the general situation without special deflation.

Just as for the classical subresultants, we can express the S_j through a Bezout relation between A and B. This is estblished in the next lemma.

Lemma 1 *Let A and B be two polynomials in $\mathbb{D}[X]$ of the same degree d and valuation 0. For every $j \in \{0, 1, \ldots, d-1\}$, there exist two elements in $\mathbb{D}[X]$, U_j and V_j, such that :*

$$X^j S_{j+1} = U_j A + V_j B.$$

The degrees of U_j and V_j are at most j. These polynomials are unique under such an assumption.

Proof : Using a matrix with coefficients in $\mathbb{D}[X]$, we can write $X^j S_{j+1}$ as a determinant in the following way :

$$X^j S_{j+1} = \left| \begin{array}{ccccccc}
a_0 & \ldots & a_{j-1} & X^j a_j + \ldots + X^{d-1} a_{d-1} & a_d & & \\
 & \ddots & \vdots & X^j a_{j-1} + \ldots + X^{d-1} a_{d-2} & \vdots & \ddots & \\
 & & & \vdots & & & \\
 & & a_0 & X^j a_1 + \ldots + X^{d-1} a_{d-j+1} & \vdots & & \\
 & & & X^j a_0 + \ldots + X^{d-1} a_{d-j} & a_{d-j+1} & \ldots & a_d \\
b_0 & \ldots & b_{j-1} & X^j b_j + \ldots + X^{d-1} b_{d-1} & b_d & & \\
 & \ddots & \vdots & X^j b_{j-1} + \ldots + X^{d-1} b_{d-2} & \vdots & \ddots & \\
 & & & \vdots & & & \\
 & & b_0 & X^j b_1 + \ldots + X^{d-1} b_{d-j+1} & \vdots & & \\
 & & & X^j b_0 + \ldots + X^{d-1} b_{d-j} & b_{d-j+1} & \ldots & b_d
\end{array} \right| .$$

We do not change the value of this determinant by adding to the $(j+1)$-th column a linear combination of the other ones. More precisely, call C_i the i-th column of the above matrix ($i = 1, \dots, 2j+2$). Then add to the $(j+1)$-th column $C_1 + XC_2 + \dots + X^{j-1}C_j + X^dC_{j+2} + \dots + X^{d+j}C_{2j+2}$. We obtain :

$$X^jS_{j+1} = \left|\begin{array}{ccccccc}
a_0 & \dots & a_{j-1} & A & a_d & & \\
& \ddots & \vdots & XA & \vdots & \ddots & \\
& & & \vdots & & & \\
& & a_0 & X^{j-1}A & \vdots & & \\
& & & X^jA & a_{d-j} & \dots & a_d \\
b_0 & \dots & b_{j-1} & B & b_d & & \\
& \ddots & \vdots & XB & \vdots & \ddots & \\
& & & \vdots & & & \\
& & b_0 & X^{j-1}B & \vdots & & \\
& & & X^jB & b_{d-j} & \dots & b_d
\end{array}\right|.$$

Expand this determinant according to the $(j+1)$-th column, putting A as a factor in the first $j+1$ lines and B in the last $j+1$: therefore there exist two polynomials, U_j and V_j, of degree at most j such that :

$$X^jS_{j+1} = U_jA + V_jB.$$

Furthermore, we can express these polynomials as determinants. We have :

$$U_j = \left|\begin{array}{ccccccc}
a_0 & \dots & a_{j-1} & 1 & a_d & & \\
& \ddots & \vdots & X & \vdots & \ddots & \\
& & & \vdots & & & \\
& & a_0 & X^{j-1} & \vdots & & \\
& & & X^j & a_{d-j} & \dots & a_d \\
b_0 & \dots & b_{j-1} & 0 & b_d & & \\
& \ddots & \vdots & 0 & \vdots & \ddots & \\
& & & \vdots & & & \\
& & b_0 & 0 & \vdots & & \\
& & & 0 & b_{d-j} & \dots & b_d
\end{array}\right|,$$

and :

$$V_j = \left| \begin{array}{ccccccc} a_0 & \dots & a_{j-1} & 0 & a_d & & \\ & \ddots & \vdots & 0 & \vdots & \ddots & \\ & & & \vdots & & & \\ & & a_0 & 0 & \vdots & & \\ & & & 0 & a_{d-j} & \dots & a_d \\ b_0 & \dots & b_{j-1} & 1 & b_d & & \\ & \ddots & \vdots & X & \vdots & \ddots & \\ & & & \vdots & & & \\ & & b_0 & X^{j-1} & \vdots & & \\ & & & X^j & b_{d-j} & \dots & b_d \end{array} \right| .$$

$\square$

For $j = 0$, we simply have $S_1 = b_d A - a_d B$, *i.e.* $U_0 = b_d$ and $V_0 = -a_d$. Using the determinantal definition of U_j and V_j, we see that :

$$U_j(0) = b_0 \cdot \mathrm{co}_{d-j}(S_j), \quad \mathrm{co}_j(U_j) = \mathrm{lc}\,(U_j) = b_d \cdot S_j(0),$$

and also :

$$V_j(0) = -a_0 \cdot \mathrm{co}_{d-j}(S_j), \quad \mathrm{co}_j(V_j) = \mathrm{lc}\,(V_j) = -a_d \cdot S_j(0).$$

Finally, we can observe that these polynomials are uniquely determined, first when A and B are co-prime, and then in the general case. (The proof uses the same arguments as for the extended Euclidean algorithm for polynomials; see [11].)

2.2 Symmetric division of polynomials

The division we use is justified by the following lemma.

Lemma 2 *Let $A, B \in \mathbb{D}[X]$, with $B \neq 0$, $\deg A = d \geq \deg B = d - \beta$ and $v(B) = \alpha$. There exist $Q, R \in \mathbb{D}'[X]$, where $\mathbb{D}'$ is the fraction field of $\mathbb{D}$, uniquely determined, such that $\deg Q = \alpha + \beta$ and $\deg R < d - (\alpha + \beta)$, and :*

$$A = Q \frac{B}{X^\alpha} + X^\beta R.$$

Proof : We sketch how to compute Q and R. First divide A by B/X^α with increasing powers of X up to order β. We obtain :

$$A = Q_1 \frac{B}{X^\alpha} + X^\beta R_1,$$

with $\deg Q_1 < \beta$ and $\deg R_1 = d - \beta$. Then, compute the Euclidean division of R_1 by B/X^α :

$$R_1 = Q_2 \frac{B}{X^\alpha} + R,$$

where $\deg R < d - \beta - \alpha$ and $\deg Q_2 = \alpha$. Then, define Q by $Q = Q_1 + X^\beta Q_2$ to establish the claim. Uniqueness is proven as usual. ☐

The polynomial Q is called the *symmetric quotient* of A by B, noted squo (A, B) and R the *symmetric remainder*, denoted $\mathrm{srem}(A, B)$.

It is clear that the computation of such a division has the same arithmetical cost as ordinary Euclidean division. It requires, at most, $d(\alpha + \beta + 1)$ arithmetical operations.

Historical note : We can find various kinds of "symmetric" division introduced by authors with specific aims. See for exemple, JEZEK [19], DEMEURE and MULLIS [9]. However, our definition is different from the one in [19] and, when $\alpha = \beta$, coincides with the one given by DEMEURE and MULLIS only in the case.

3 Structure-Theorem for symmetric subresultants

We now describe the relationship between the sequence of symmetric subresultants and the sequence of symmetric remainders of two polynomials. Our main result is :

Theorem 3 *Let $\mathbb{D}$ be a subring of $\mathbb{C}$, and let A and B be elements of $\mathbb{D}[X]$ of degree d and valuation 0. Let $(S_i)_{0\leq i\leq d}$ be the sequence of symmetric subresultants of A and B. Suppose that the pair (S_j, S_{j+1}) is (α, β)-defective. We have :*

(1)
- *if $\alpha > 0$ and $\beta > 1$, then $S_{j+k} \equiv 0$ for $k = 2, \ldots, \alpha + \beta - 1$*
- *if $\alpha = 0$ and $\beta > 1$, then, if $j > 0$:*

$$S_j(0) \cdot S_{j+k} = S_{j+1}(0)^{k-1} S_{j+1} \text{ for } k = 2, \ldots, \beta - 1.$$

If $j = 0$, $S_k = S_1(0)^{k-1} S_1$ for $k = 2, \ldots, \beta - 1$.

- *if* $\alpha > 0$ *and* $\beta = 1$, *then if* $j > 1$ *:*

$$\mathrm{lc}\,(S_j)^{k-1} \cdot S_{j+k} = (-1)^k \mathrm{lc}\,(S_{j+1})^{k-1} \cdot \frac{S_{j+1}}{X^{k-1}} \text{ for } k = 2, \ldots, \alpha.$$

If $j = 0$, $b_d^k \cdot S_k = (-1)^k \cdot \mathrm{lc}\,(S_1)^{k-1} \ldots S_1 X^{-k+1}$ *for* $k = 2, \cdots, \alpha$.

(2) In all cases, if $j > 0$, *we have :*

$$\mathrm{lc}\,(S_j)^{\alpha} \cdot S_j(0)^{\beta-1} \cdot S_{j+\alpha+\beta} = (-1)^{(\alpha+\beta)\alpha} \cdot \mathrm{lc}\,(S_{j+1})^{\alpha} \cdot \mathrm{tc}\,(S_{j+1})^{\beta-1} \cdot \frac{S_{j+1}}{X^{\alpha}},$$

and if $j = 0$, *then :*

$$b_d^{\alpha} \cdot S_{\alpha+\beta} = (-1)^{(\alpha+\beta)\alpha} \cdot b_0^{\alpha} \cdot \mathrm{lc}\,(S_1)^{\alpha} \cdot \mathrm{tc}\,(S_1)^{\beta-1} \cdot \frac{S_1}{X^{\alpha}}.$$

(3) In all cases, if $j > 0$, *we have :*

$$\begin{aligned} \mathrm{lc}\,(S_j) \cdot S_j(0) \cdot S_{j+\alpha+\beta+1} &= -\mathrm{lc}\,(S_{j+1}) \cdot S_{j+\alpha+\beta}(0) \cdot \mathrm{srem}(S_j, S_{j+1}) \\ &= -\mathrm{srem}\,(\mathrm{lc}\,(S_{j+1}) \cdot S_{j+\alpha+\beta}(0) \cdot S_j, S_{j+1}) \end{aligned}$$

and if $j = 0$ *then :*

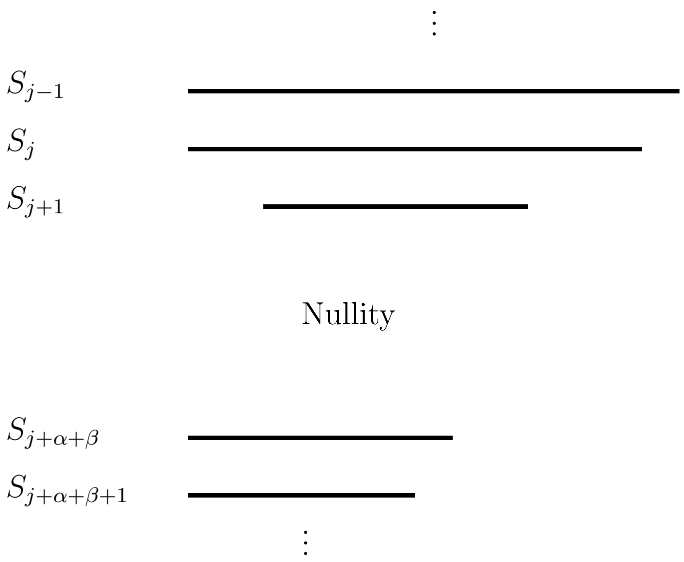
$$b_d \cdot S_{\alpha+\beta+1} = -\mathrm{srem}\,(\mathrm{lc}\,(S_1) \cdot S_{\alpha+\beta}(0) \cdot S_0, S_1)\,.$$

One remarkable fact is that the last symmetric divisions are exact in $\mathbb{D}$, as we shall prove later.

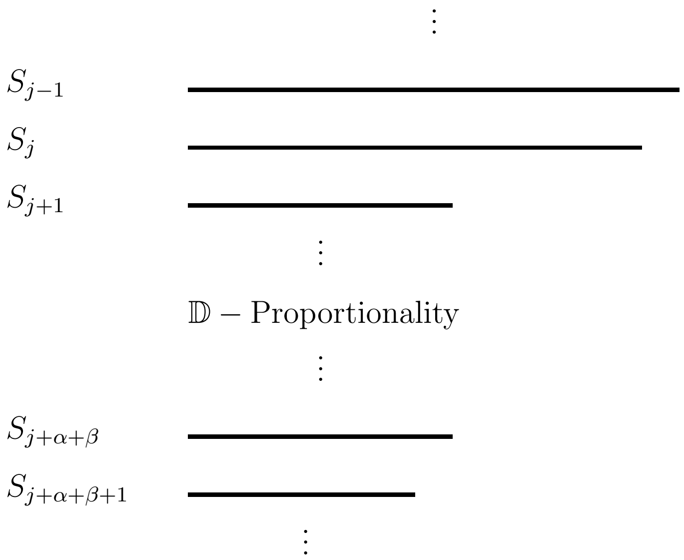
Observe that S_1 can also be expressed as a symmetric remainder : by Lemma 1, we have $S_1 = b_d A - a_d B = \mathrm{srem}(S_{-1}, S_0)$.

It could be helpful to the reader to visualize the different situations.

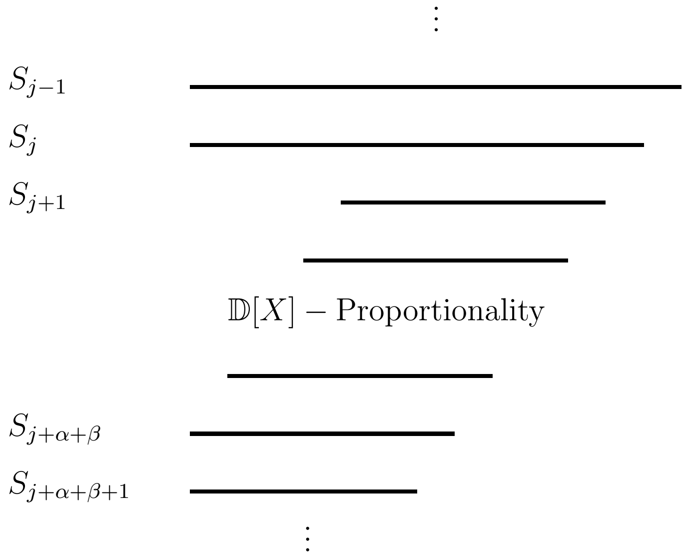
(1) Case (S_j, S_{j+1}) defective on "each side", $\alpha > 0, \beta > 1$:



(2) Case (S_j, S_{j+1}) defective on the “right-hand side”, $\alpha = 0, \beta > 1$:



(3) Case (S_j, S_{j+1}) defective on the “left-hand side”, $\alpha > 0, \beta = 1$:



Proof : Roughly speaking, we can say that the rows of $Sylv_i(A,B)$ are made of $A, XA, ..., X^{i-1}A$, and $B, XB, ..., X^{i-1}B$, identifying the vectors of the coefficients of these polynomials with the polynomials themselves. Furthermore, we consider them all of formal degree $d+i-1$.

Preliminary work : By Lemma 1, we know the existence of two polynomials, $U_j = \sum_{i=0}^{j} u_i X^i$ and $V_j = \sum_{i=0}^{j} v_i X^i$, such that :

$$\begin{aligned} X^j S_{j+1} &= U_j A + V_j B \\ &= \sum_{n=0}^{j} u_n (AX^n) + \sum_{n=0}^{j} v_n (BX^n). \end{aligned}$$

As the pair (S_j, S_{j+1}) is (α,β)-defective, $S_j(0)$ and $\mathrm{co}_{d-j}(S_j) = \mathrm{lc}\,(S_j)$ are different from zero. Because of the determinantal definition of U_j (see proof of Lemma 1), we have :

- if $j > 0$, $u_0 = b_0 \cdot \mathrm{lc}\,(S_j) \neq 0$, and $u_j = b_d \cdot S_j(0) \neq 0$,
- if $j = 0$, $u_0 = u_j = b_d \neq 0$.

Then, for every $\ell \geq 0$, we have :

$$X^{j+\ell} S_{j+1} = \sum_{n=0}^{j} u_n A X^{n+\ell} + \sum_{n=0}^{j} v_n B X^{n+\ell}, \quad (\dagger)$$

with u_0 and u_j different from 0.

For $k \geq 2$, and i fixed between 0 and $k-1$, we can replace the $(i+1)$-th row of Sylv_{j+k}, X^iA by the linear combination of the rows $X^iA, ..., X^{j+i}A$ and $X^iB, ..., X^{j+i}B$ described in (†). For $\ell = i$ we obtain $X^{j+i}S_{j+1}$ on the $(i+1)$-th row of Sylv_{j+k} instead of X^iA. The minors of order $2(j+k)$ of this new matrix are equal to u_0 times the corresponding ones in Sylv_{j+k}. This operation will be called the $(i, \downarrow)$-**transformation** of Sylv_{j+k}. The downward arrow means that the j rows directly below the $(i+1)$-st row are used.

We define also the $(j+i, \uparrow)$-**transformation** for $i = 0, ..., k-1$: this replaces the $(j+i+1)$-st row by $X^{j+i}S_{j+1}$ which is a linear combination of the rows $X^iA, ..., X^{j+i}A$ and $X^iB, ..., X^{j+i}B$, by (†). In this case the values of the minors of order $2(j+k)$ of Sylv_{j+k} are multiplied by u_j.

We use these two transformations in four different situations, described below. For each, we have drawn the corresponding matrix resulting from S_{j+k}: on each diagram, the rows with large dash patterns delimit the $j+k-1$ first columns and the $j+k$ last ones needed for the computation of $\text{Sylv}_{j+k,\ell}$ ($\ell = 0, ..., d-j-k$). The shadowed triangles highlight the coefficients of the matrix needed for the computation of $S_j(0)$.

We consider now the four different cases.

- $1 \leq \beta \leq \alpha$. Two situations have to be distinguished.
  ◇ If $2 \leq k \leq \alpha$, we use k $(i, \downarrow)$-transformations for $i = 0, ..., k-1$ in this order. We obtain the matrix $\mathbf{M_1}$ (fig. 1).

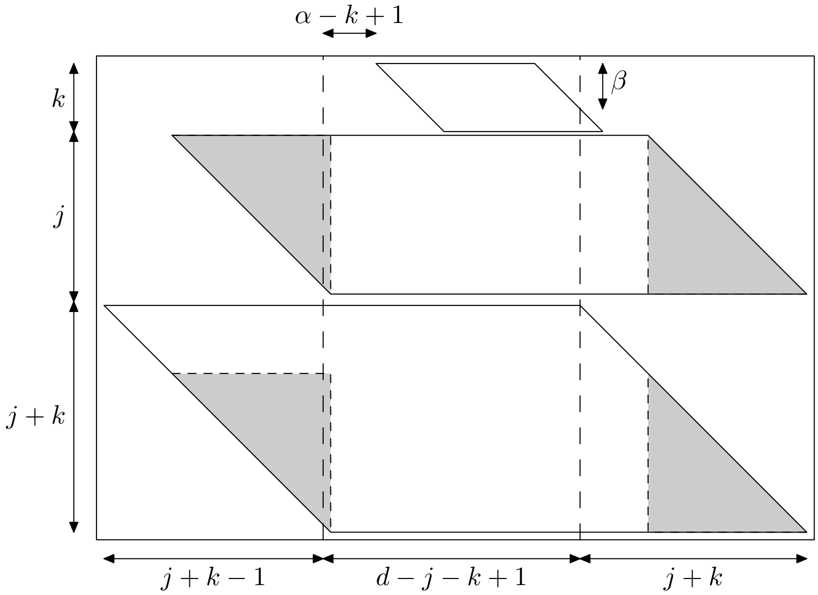


Fig. 1. Shape of the matrix M_1

For each $\ell \in \{0, ..., d-j-k\}$, the minor $\det(\text{Sylv}_{j+k,\ell})$ of Sylv_{j+k} is equal to the corresponding minor of the above matrix divided by u_0^k. If we denote this minor by $d_{j+k,\ell}$, we have :

$$u_0^k \cdot \det(\mathrm{Sylv}_{j+k,\ell}) = d_{j+k,\ell}.$$

- ◇ If $\alpha < k \leq \alpha + \beta$, we use α $(i, \downarrow)$-transformations for $i = 0, ..., \alpha - 1$, in this order, and then $k - \alpha$ $(j + i, \uparrow)$-transformations for $i = k - 1, ..., \alpha$, again in this order. We obtain the matrix $\mathbf{M_2}$ (fig. 2).

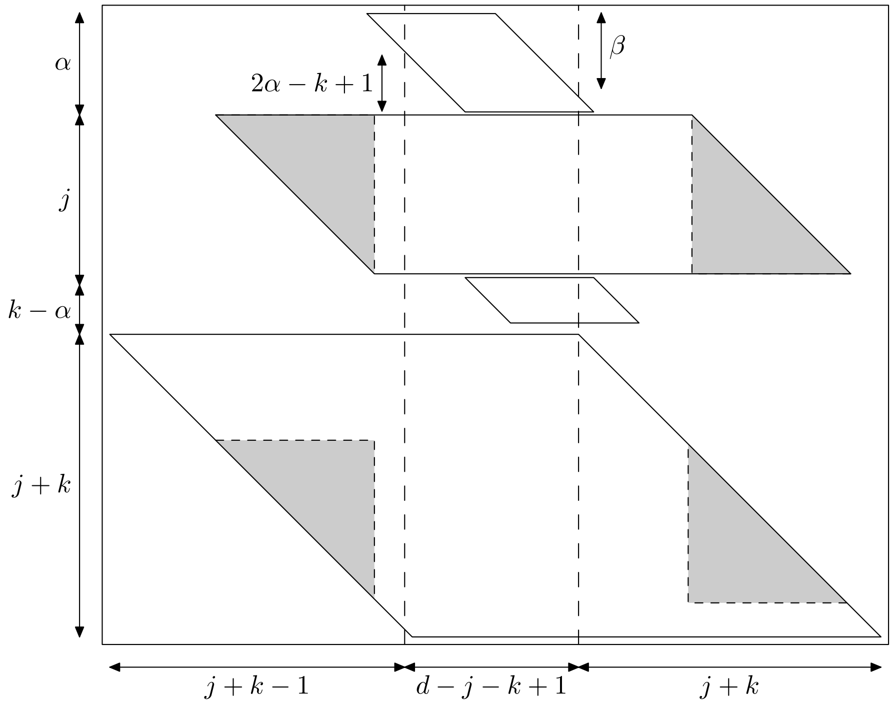


Fig. 2. Shape of the matrix M_2

With the same notation as in the first case, we have :

$$u_0^\alpha \cdot u_j^{k-\alpha} \cdot \det(\mathrm{Sylv}_{j+k,\ell}) = d_{j+k,\ell}.$$

- $0 \leq \alpha < \beta$. Once again two situations occur.
  - ◇ If $2 \leq k \leq \beta$, we perform k $(j + i, \uparrow)$-transformations with $i = k - 1, ..., 0$, in this order. We get the matrix $\mathbf{M_3}$ (fig. 3), and we have for $\ell \in \{0, ..., d - j - k\}$:

$$u_j^k \cdot \det(\mathrm{Sylv}_{j+k,\ell}) = d_{j+k,\ell}.$$

  - ◇ If $\beta < k \leq \alpha + \beta$, we use β $(j + i, \uparrow)$-transformations with $i = k - 1, ..., k - \beta$ in this order, and $k - \beta$ $(i, \downarrow)$-transformations with $i = 0, ..., k - \beta - 1$, in this order. We get the matrix $\mathbf{M_4}$ (fig. 4), and :

$$u_0^{k-\beta} \cdot u_j^\beta \cdot \det(\mathrm{Sylv}_{j+k,\ell}) = d_{j+k,\ell}.$$

We now prove the theorem, step by step.

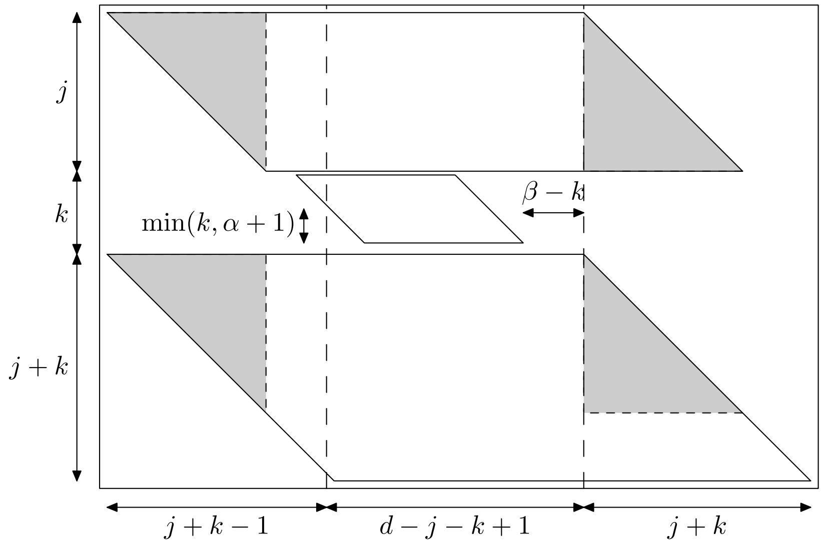


Fig. 3. Shape of the matrix M_3

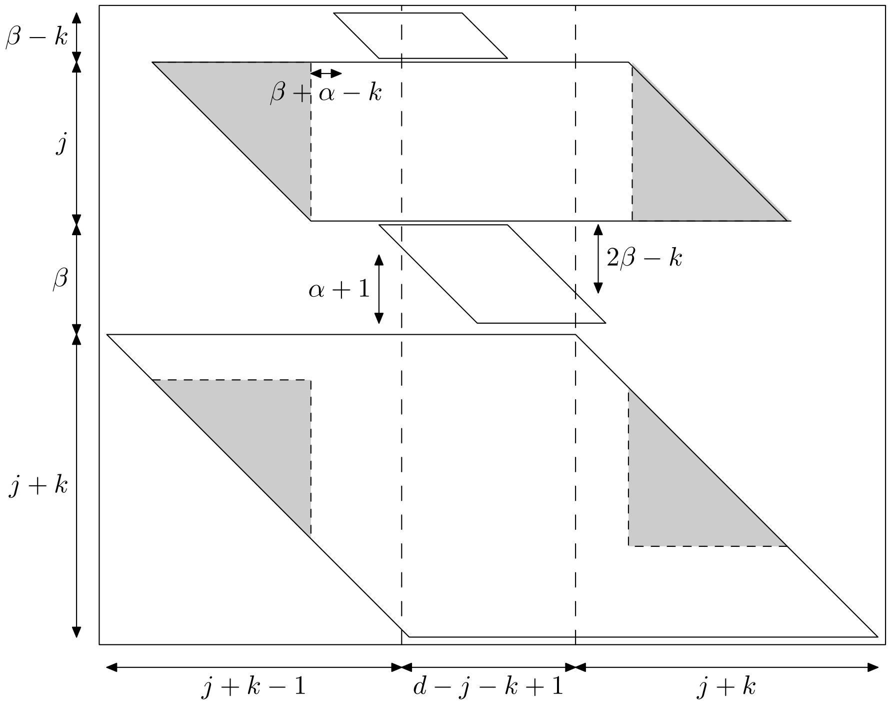


Fig. 4. Shape of the matrix M_4

Proof of (1) : $2 \leq k \leq \alpha + \beta - 1$

Since we have to show the nullity of S_{j+k} for $k = 2, ..., \alpha + \beta - 1$, we need to show that the coefficients $\det(Sylv_{j+k,\ell})$ vanish for $\ell = 0, ..., d - j - k$. This is equivalent to showing that $d_{j+k,\ell} = 0$, for one of the matrices $\mathbf{M_1}$, $\mathbf{M_2}$, $\mathbf{M_3}$ or $\mathbf{M_4}$, because u_0 and u_j are both different from zero.

- Case $\alpha > 0, \beta > 1$

Suppose that $1 < \beta \leq \alpha$ and $1 < k \leq \alpha$. We use $\mathbf{M_1}$: the submatrix corresponding to $d_{j+k,\ell}$ has at most one nonzero element on its first row. We use the corresponding column to expand it. The first row of the remaining minor has only zeros since $\beta \geq 2$. Hence $d_{j+k,\ell} = 0$.

If $1 < \beta \leq \alpha < k \leq \alpha + \beta - 1$, we use $\mathbf{M_2}$. We have $\alpha + \beta - k \geq 1$ and then

$$[(2\alpha - k + 1) + \beta] - \alpha \geq 2.$$

It follows that there are at least two among the first α rows for which at most one entry is nonzero, namely on the $(j+k)$-th column. Developing $d_{j+k,l}$ along those two rows shows that it is zero.

If $1 \leq \alpha < \beta$ and $1 < k \leq \beta$, we use $\mathbf{M_3}$ to expand $d_{j+k,\ell}$ along the $(j+k)$-th row, which has at most one nonzero coefficient. As $\min(k, \alpha+1) \geq 2$, the row immediately above also has this property, and we get $d_{j+k,\ell} = 0$.

Finally, if $1 \leq \alpha < \beta < k \leq \alpha + \beta - 1$, we use $\mathbf{M_4}$. Once again, in $d_{j+k,\ell}$ we have two successive rows with only one non-zero coefficient, on the $(j+k)$-th column (because $(\alpha+1) + (2\beta - k) \geq \beta + 2$).

In every case, we see that, if $\alpha > 0$ and $\beta > 1$, then $S_{j+k} \equiv 0$. This establishes the first part of 1.

- Case $\alpha = 0, \beta > 1$

  As $2 \leq k \leq \alpha + \beta - 1$, we have $1 < k \leq \beta$, $\min(k, \alpha+1) = 1$ and we can expand the minor $d_{j+k,\ell}$, using the rows $j+k, ..., j+1$ in $\mathbf{M_3}$, in this order, and then, using the last k columns. We obtain, for every $\ell = 0, ..., d-j-k$:

  $$d_{j+k,\ell} = \mathrm{co}_\ell(S_{j+1}) \cdot \mathrm{tc}\,(S_{j+1})^{k-1} \cdot b_d^k \cdot S_j(0).$$

  (The factors are written from left to right, in their order of appearance in the successive expansions.) As $d_{j+k,\ell} = u_j^k \det(Sylv_{j+k,\ell})$ and $u_j = b_d S_j(0)$, we have :

  $$S_j(0)^{k-1} \cdot S_{j+k} = \mathrm{tc}\,(S_{j+1})^{k-1} \cdot S_{j+1}.$$

  If $j = 0$, $u_j = b_d$ and $S_j(0)$ does not appear in $d_{j+k,\ell}$. Hence :

  $$S_k = \mathrm{tc}\,(S_1)^{k-1} \cdot S_1.$$

- $\alpha > 0, \beta = 1$

  We have $2 \leq k \leq \alpha$ and we use $\mathbf{M_1}$, expanded along the first k columns, and then along the first k rows. We obtain (the factors appear in order of expansions from the right-hand side of the formula) :

  $$\begin{aligned} d_{j+k,\ell} &= (-1)^{k(j+k+2)} \cdot b_0^k \cdot (-1)^{k(j+k+1)} \mathrm{co}_{j+k-1+\ell}(X^j S_{j+1}) \\ &\qquad \cdot \mathrm{lc}\,(S_{j+1})^{k-1} \cdot \mathrm{lc}\,(S_j) \\ &= (-1)^k \cdot b_0^k \cdot \mathrm{co}_{k-1+\ell}(S_{j+1}) \cdot \mathrm{lc}\,(S_{j+1})^{k-1} \cdot \mathrm{lc}\,(S_j). \end{aligned}$$

  The result follows. If $j = 0$, the computation is the same : however, in this case, all the rows of block B collapse.

Proof of (2) : $k = \alpha + \beta$

If $(\alpha, \beta) = (0, 1)$, the result is trivial. So, we suppose that $(\alpha, \beta) \neq (0, 1)$. For $j \neq 0$, we distinguish two cases.

- $\beta \leq \alpha$

  We use the matrix $\mathbf{M_2}$ and expand it along the row of order β to obtain :

$$\begin{aligned} d_{j+k,\ell} &= u_0^\alpha \cdot u_j^\beta \cdot \det(Sylv_{j+k,\ell}) \\ &= u_0^\alpha \cdot u_j^\beta \cdot (-1)^{n_0} \cdot \mathrm{co}_{j+k-1+\ell}(X^{j+\beta-1} S_{j+1}) \cdot \Delta \\ &= u_0^\alpha \cdot u_j^\beta \cdot (-1)^{n_0} \cdot \mathrm{co}_{\alpha+\ell}(S_{j+1}) \cdot \Delta, \end{aligned}$$

  where $n_0 = j + \alpha$ and Δ is a minor independent of ℓ.

  Then, we expand Δ along the first $\beta - 1$ rows, and see that :

$$\Delta = (-1)^{n_1} \cdot \mathrm{tc}\,(S_{j+1})^{\beta-1} \cdot \Delta_1,$$

  with $n_1 = (j + \alpha)(\beta - 1)$. We continue expanding Δ_1 along the first $\alpha - \beta$ rows ; we have :

$$\Delta_1 = (-1)^{n_2} \cdot \mathrm{lc}\,(S_{j+1})^{\alpha-\beta} \cdot \Delta_2,$$

  with $n_2 = (j + \alpha)(\alpha - \beta)$. We can then use rows $j + 1, ..., j + \beta$ to compute Δ_2 :

$$\Delta_2 = (-1)^{n_3} \cdot \mathrm{lc}\,(S_{j+1})^{\beta} \cdot \Delta_3$$

  ($n_3 = \alpha\beta$). Finally, Δ_3 can be expanded using the first α columns and the last β ones :

$$\Delta_3 = (-1)^{n_4} \cdot b_0^\alpha \cdot b_d^\beta \cdot S_j(0),$$

  with $n_4 = j\alpha$. In summary, we have obtained :

$$u_0^\alpha \cdot u_j^\beta \cdot \det(Sylv_{j+k,\ell}) = (-1)^N \cdot b_0^\alpha \cdot b_d^\beta \cdot \mathrm{tc}\,(S_{j+1})^{\beta-1} \cdot \mathrm{lc}\,(S_{j+1})^{\alpha} \cdot S_j(0) \cdot \mathrm{co}_{\alpha+\ell}(S_{j+1}),$$

  with $N = n_0 + n_1 + n_2 + n_3 + n_4 \equiv \alpha(\alpha + \beta) \bmod 2$. As this computation is valid for every $\ell = 0, ..., d - j - k$, we have :

$$\mathrm{lc}\,(S_j)^\alpha \cdot S_j(0)^{\beta-1} \cdot S_{j+\alpha+\beta} = (-1)^{\alpha(\alpha+\beta)} \cdot \mathrm{lc}\,(S_{j+1})^\alpha \cdot \mathrm{tc}\,(S_{j+1})^{\beta-1} \cdot \frac{S_{j+1}}{X^\alpha}.$$

- $\alpha < \beta$

  We use the same method as in the previous situation, starting with $\mathbf{M_4}$. We expand it along the row of order $j + \beta$ and obtain :

$$d_{j+k,\ell} = u_0^\alpha \cdot u_j^\beta \cdot \det(Sylv_{j+k,\ell}) = u_0^\alpha \cdot u_j^\beta \cdot (-1)^{n_0'} \cdot \mathrm{co}_{\alpha+\ell}(S_{j+1}) \cdot \Delta'.$$

  We expand Δ' along its rows $j + \beta + 1, ..., j + k$ to obtain :

$$\Delta' = (-1)^{n'_1} \cdot \mathrm{lc}\,(S_{j+1})^{\alpha} \cdot \Delta'_1,$$

then again along its rows $j+\beta-1, ..., j+\alpha+1$ to obtain :

$$\Delta'_1 = (-1)^{n'_2} \cdot \mathrm{tc}\,(S_{j+1})^{\beta-\alpha-1} \cdot \Delta'_2,$$

and then along its first α rows :

$$\Delta'_2 = (-1)^{n'_3} \cdot \mathrm{tc}\,(S_{j+1})^{\alpha} \cdot \Delta'_3,$$

to finally find that $\Delta_3 = \Delta'_3$. We now have :

$$\begin{aligned} n'_0 &= \alpha, \\ n'_1 &= \alpha^2, \\ n'_2 &= \alpha(\beta-\alpha-1), \\ n'_3 &= \alpha(j+\alpha), \\ n'_4 &= n_4 \;=\; j\alpha. \end{aligned}$$

We obtain exactly the same final relation as in the case $\beta \leq \alpha$.

If $j = 0$, we have $u_0 = u_j = b_d$; and $S_j(0)$ disappears at the end of the successive expansions of the minors. Therefore we get :

$$b_d^{\alpha} \cdot S_{\alpha+\beta} = (-1)^{\alpha(\alpha+\beta)} \cdot b_0^{\alpha} \cdot \mathrm{lc}\,(S_1)^{\alpha} \cdot \mathrm{tc}\,(S_1)^{\beta-1} \cdot \frac{S_1}{X^{\alpha}}.$$

Proof of (3) :

Here we cannot use the same transformations of $Sylv_{j+\alpha+\beta+1}$ as above.

We suppose first that $j > 0$. Let $R = -\mathrm{srem}(S_j, S_{j+1})$ and $Q = \mathrm{squo}\,(S_j, S_{j+1})$. There exist four polynomials U_{j-1}, V_{j-1}, U_j and V_j such that :

$$\begin{aligned} X^{j-1}S_j &= U_{j-1}A + V_{j-1}B, \\ X^{j}S_{j+1} &= U_jA + V_jB \end{aligned}$$

with $\deg(U_{j-1}) \leq j-1$, $\deg(V_{j-1}) \leq j-1$, $\deg(U_j) = \deg(V_j) = j$. We also have :

$$X^{\beta}R = Q\frac{S_{j+1}}{X^{\alpha}} - S_j.,$$

and deduce that :

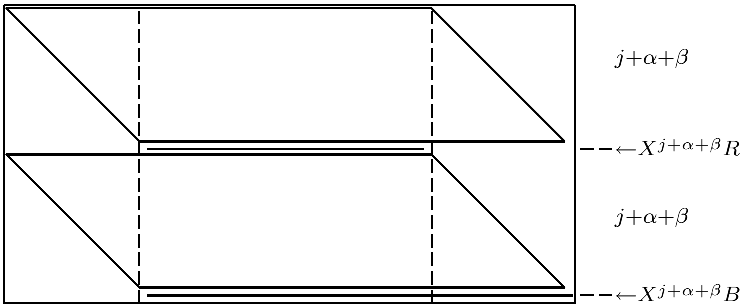
$$\begin{aligned} X^{j+\alpha+\beta}R &= (QU_j - X^{\alpha+1}U_{j-1})A + (QV_j - X^{\alpha+1}V_{j-1})B \\ &= UA + VB. \end{aligned}$$

As $\deg(QU_j) = j{+}\alpha{+}\beta$ and $\deg(X^{\alpha+1}U_{j-1}) \leq j{+}\alpha$, we have $\deg U = j{+}\alpha{+}\beta$. Likewise, $\deg V = j + \alpha + \beta$.

Also :

$$\mathrm{lc}\,(U) = \mathrm{lc}\,(Q)\mathrm{lc}\,(U_j) = \frac{\mathrm{lc}\,(S_j) \cdot b_d \cdot S_j(0)}{\mathrm{lc}\,(S_{j+1})}.$$

The equation $X^{j+\alpha+\beta}R = UA{+}VB$, with $\deg(U) = \deg(V) = j{+}\alpha{+}\beta$, shows that $X^{j+\alpha+\beta}R$ can be obtained as a linear combination of rows of $Sylv_{j+\alpha+\beta+1}$. As in the previous steps, we transform the row $j + \alpha + \beta + 1$ and obtain a matrix which has the following structure :



Therefore, for $\ell = 0, 1, ..., d - (j + \alpha + \beta + 1)$, we obtain :

$$\mathrm{lc}\,(U){\cdot}\det(\mathrm{Sylv}_{j+\alpha+\beta+1,\ell}) = \begin{array}{|cccccccc|} a_0 & \cdots & a_{j+\alpha+\beta-1} & a_{j+\alpha+\beta+\ell} & a_d & & & \\ & \ddots & \vdots & \vdots & \vdots & \ddots & & \\ & & a_0 & a_{\ell-1} & a_{d-j-\alpha-\beta+1} & \cdots & a_d & \\ & & 0 & \mathrm{co}_\ell(R) & 0 & \cdots & 0 & 0 \\ b_0 & \cdots & b_{j+\alpha+\beta-1} & b_{j+\alpha+\beta+\ell} & b_d & & & \\ & \ddots & \vdots & \vdots & \vdots & \ddots & & \\ & & b_0 & \vdots & \vdots & & \ddots & \\ & & 0 & b_\ell & b_{d-j-\alpha-\beta} & \cdots & \cdots & b_d \\ \multicolumn{3}{c}{\underbrace{\hphantom{a_0 \cdots a_{j+\alpha+\beta-1}}}_{j+\alpha+\beta}} & & \multicolumn{4}{c}{\underbrace{\hphantom{a_{d-j-\alpha-\beta+1} \cdots a_d \; 0}}_{j+\alpha+\beta+1}} \end{array}.$$

Expanding these determinants along the last column, and then along row $(j + \alpha + \beta + 1)$, we see that :

$$\mathrm{lc}\,(U) \cdot S_{j+\alpha+\beta+1} = b_d \cdot S_{j+\alpha+\beta}(0)R.$$

We use the value of $\mathrm{lc}\,(U)$ already computed to obtain the desired result :

$$\mathrm{lc}\,(S_j) \cdot S_j(0) \cdot S_{j+\alpha+\beta+1} = \mathrm{lc}\,(S_{j+1}) \cdot S_{j+\alpha+\beta}(0)R.$$

When $j = 0$, the polynomials U_{j-1}, V_{j-1}, U_j and V_j are very simple, as we have :

$$S_0 = 1.B, \quad S_1 = b_d A - a_d B.$$

The expression of $\mathrm{lc}\,(U)$ is now : $\mathrm{lc}\,(U) = \frac{\mathrm{lc}\,(S_0)\cdot b_d}{\mathrm{lc}\,(S_1)}$. However, the rest of the computation is unchanged, and we obtain :

$$\mathrm{lc}\,(S_0) \cdot S_{\alpha+\beta+1} = \mathrm{lc}\,(S_1) \cdot S_{\alpha+\beta}(0) R.$$

□

Remark : If we define the TOEPLITZ-BEZOUTIAN of two monic polynomials P and Q of the same degree as the matrix $Bez(P, Q)$ whose entries are the coefficients of the polynomial

$$\frac{P(X)Q^*(Y) - P^*(Y)Q(X)}{1 - XY}.$$

If $sc_i(M)$ denotes the i-th SCHUR-complement of the square matrix M whenever it exists, one can see that we have :

$$S_i(0)\mathrm{lc}\,(S_i) sc_i(Bez(S_{-1}, S_0)) = Bez(S_i, S_{i+1}).$$

(See Bini and Pan [3] p. 169 for the classical result over the Euclidean remainder sequence. Proof uses same methods).

4 Computation of the Symmetric Subresultants Sequence

The previous theorem gives us a direct method to compute the sequence of symmetric subresultants of two polynomials A and B, of same degree d and same valuation 0. It uses symmetric divisions instead of the determinantal definition. With parts 2 and 3 of Theorem 3, we can compute the subsequence $(S_{k_i})_{i=0,\ldots,s}$ $(s \leq d)$ of the sequence of the symmetric subresultants, such that, for each index i, the pair (S_{k_i}, S_{k_i+1}) is (α_i, β_i)-defective. This implies that, for each i, S_{k_i} is of valuation 0 and degree $d - k_i$ (we have $k_0 = 0$ as $S_0 = B$). Denote by Q_i the i-th symmetric quotient of (S_{k_i}, S_{k_i+1}). The sequence $(S_{k_i})_{i=0,\ldots,s}$ is obtained by the following Euclidean-like algorithm :

$$\begin{aligned}
\mathrm{lc}\,(S_1) \cdot S_{k_1}(0) \cdot S_0 &= Q_0 S_1 - \mathrm{lc}\,(S_0) \cdot S_{k_1+1}, \\
\mathrm{lc}\,(S_{k_1+1}) \cdot S_{k_2}(0) \cdot S_{k_1} &= Q_1 \frac{S_{k_1+1}}{X^{\alpha_1}} - X^{\beta_1} \mathrm{lc}\,(S_{k_1}) \cdot S_{k_1}(0) \cdot S_{k_2+1},
\end{aligned}$$

$$\vdots$$

$$\mathrm{lc}\,(S_{k_s+1}) \cdot S_{k_s+1}(0) \cdot S_{k_s} = Q_s \frac{S_{k_s+1}}{X^{\alpha_s}}.$$

For such an algorithm, a classical analysis of cost gives a bound of $\mathcal{O}(d^2)$ arithmetical operations. In the important case of $\mathbb{Z}$, we use HADAMARD's bound for a determinant : if the size of all the coefficients of the polynomials is bounded by σ, then the size of the coefficients of all the S_{k_i} is bounded by $2d(\sigma + \log(d))$. Therefore, in the case of $\mathbb{Z}$, the binary cost of the algorithm is in $\mathcal{O}(d^2\mathcal{M}(2d(\sigma + \log d)))$ where $\mathcal{M}(t)$ denotes the cost of the multiplication of two integers of absolute value less than 2^t.

However, this algorithm can be improved. In a previous article (see [5]), we studied the case where B is the reciprocal polynomial of A. In fact the improvement we gave can be applied to every pair of polynomials A and B in $\mathbb{D}[X]$ of same degree d and valuation zero. The next section is devoted to showing this.

The ideas we develop here are adaptations to the case of symmetric subresultants, of ideas already known for ordinary subresultants (see [21], [22],[23], [27]).

4.1 Transition Matrices

One idea is to express the transition from a pair (S_{k_i}, S_{k_i+1}) to a pair $(S_{k_{i+1}}, S_{k_{i+1}+1})$ with an appropriate matrix.

Let A and B be two polynomials in $\mathbb{D}[X]$ of same degree d and valuation 0. Suppose the pair (S_j, S_{j+1}) to be (α, β)-defective ; set $k = j+\alpha+\beta$ and denote by Q the symmetric quotient of $\mathrm{lc}\,(S_{j+1})S_k(0)S_j$ by S_{j+1}. With formulae 2 and 3 of the Structure-Theorem Th. 3, we can write, for $j > 0$:

$$\begin{pmatrix} X^{k-1}S_k \\ X^k S_{k+1} \end{pmatrix} = M_{j,k} \cdot \begin{pmatrix} X^{j-1}S_j \\ X^j S_{j+1} \end{pmatrix}$$

with

$$M_{j,k} = \begin{pmatrix} 0 & (-1)^{(\alpha+\beta)\alpha} \frac{\mathrm{lc}\,(S_{j+1})^{\alpha}\mathrm{tc}\,(S_{j+1})^{\beta-1}}{\mathrm{lc}\,(S_j)^{\alpha} S_j(0)^{\beta-1}} X^{\beta-1} \\ -\frac{\mathrm{lc}\,(S_{j+1})S_k(0)}{\mathrm{lc}\,(S_j)S_j(0)} X^{\alpha+1} & \frac{Q}{\mathrm{lc}\,(S_j)S_j(0)} \end{pmatrix}. \qquad (1)$$

In the case $j = 0$, we obtain :

$$\begin{pmatrix} X^{k-1}S_k \\ X^k S_{k+1} \end{pmatrix} = M_{0,k} \cdot \begin{pmatrix} S_0 \\ S_1 \end{pmatrix}$$

with

$$M_{0,k} = \begin{pmatrix} 0 & (-1)^{k\alpha} \frac{b_0^{\alpha} \operatorname{lc}(S_1)^{\alpha} \operatorname{tc}(S_1)^{\beta-1}}{b_d^{\alpha}} X^{\beta-1} \\ -\frac{\operatorname{lc}(S_1) S_k(0)}{b_d} X^{\alpha} & \frac{Q}{b_d} \end{pmatrix}. \tag{2}$$

Furthermore, we have (for $j = -1$) :

$$\begin{pmatrix} S_0 \\ S_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ b_d & -a_d \end{pmatrix} \cdot \begin{pmatrix} A \\ B \end{pmatrix}.$$

We can now state a general definition.

Definition 4 *Let* $A = \sum_{i=0}^{d} a_i X^i$ *and* $B = \sum_{i=0}^{d} b_i X^i$ *be two polynomials of* $\mathbb{D}[X]$ *of same degree* d *and same valuation 0. Let* $(S_i)_{-1 \leq i \leq d}$ *be the sequence of the symmetric sub-resultants of* A *and* B. *We denote by* $(k_i)_{i=0,\dots,s}$ *(with* $k_0 = 0 < k_1 < \dots < k_s$*) the sequence of indices such that* (S_{k_i}, S_{k_i+1}) *is* (α_i, β_i)*-defective.*

Then, for $i, j \in \{0, \dots, s\}$, *with* $i < j$, *we denote by* M_{k_i,k_j} *the matrix defined by :*

$$M_{k_i,k_j} = M_{k_{j-1},k_j} \cdot M_{k_{j-2},k_{j-1}} \cdot \dots \cdot M_{k_i,k_{i+1}},$$

where the matrices $M_{k_\ell,k_{\ell+1}}$ *are defined by the above formulae (1) and (2). If* $i > 0$, *we have :*

$$\begin{pmatrix} X^{k_j-1}S_{k_j} \\ X^{k_j} S_{k_j+1} \end{pmatrix} = M_{k_i,k_j} \cdot \begin{pmatrix} X^{k_i-1}S_{k_i} \\ X^{k_i} S_{k_i+1} \end{pmatrix},$$

and if $i = 0$ *:*

$$\begin{pmatrix} X^{k_j-1}S_{k_j} \\ X^{k_j} S_{k_j+1} \end{pmatrix} = M_{0,k_j} \cdot \begin{pmatrix} S_0 \\ S_1 \end{pmatrix}.$$

We call the matrix M_{k_i,k_j} *the* transition matrix *from the pair* (S_{k_i}, S_{k_i+1}) *to the pair* (S_{k_j}, S_{k_j+1}). *We denote by* M_{k_i} *the transition matrix from* (A, B) *to*

(S_{k_i}, S_{k_i+1}) :

$$M_{k_i} = M_{0,k_i} \cdot \begin{pmatrix} 0 & 1 \\ b_d & -a_d \end{pmatrix}.$$

with the convention that $M_{0,0}$ is the identity.

We can now justify the assertion of the previous section : all the quotients (and remainders) involved in the Structure-Theorem are fraction-free.

Proposition 5 *Let $A = \sum_{i=0}^{d} a_i X^i$ and $B = \sum_{i=0}^{d} b_i X^i$ be two polynomials of $\mathbb{D}[X]$ of same degree d, and same valuation 0. Let $(S_i)_{-1 \leq j \leq d}$ be the sequence of the symmetric sub-resultants of A and B. Let $j \in \{1, ..., d-1\}$ be such that (S_j, S_{j+1}) is (α, β)-defective. Put $k = j + \alpha + \beta$.*

Then the symmetric quotient of $\mathrm{lc}\,(S_{j+1}) S_k(0) S_j$ by S_{j+1} belongs to $\mathbb{D}[X]$, as does the symmetric remainder.

Proof : By Lemma 1 we have for $i > 0$:

$$\begin{aligned} X^{i-1} S_i &= U_{i-1} A + V_{i-1} B, \\ X^i S_{i+1} &= U_i A + V_i B. \end{aligned}$$

Therefore, we obtain, for each $j > 0$, the following expression of M_j :

$$M_j = \begin{pmatrix} U_{j-1} & V_{j-1} \\ U_j & V_j \end{pmatrix}.$$

We can directly deduce from (1) and (2) the value of $\det(M_{j,k})$. Moreover, if we consider the first line of

$$\begin{pmatrix} X^{k-1} S_k \\ X^k S_{k+1} \end{pmatrix} = M_{j,k} \cdot \begin{pmatrix} X^{j-1} S_j \\ X^j S_{j+1} \end{pmatrix},$$

we see that $\mathrm{lc}\,(S_k) = (-1)^{(\alpha+\beta)\alpha} \frac{\mathrm{lc}\,(S_{j+1})^{\alpha+1} \mathrm{tc}\,(S_{j+1})^{\beta-1}}{\mathrm{lc}\,(S_j)^{\alpha} S_j(0)^{\beta-1}}$. Therefore, we obtain, for $j > 0$:

$$\det(M_{j,k}) = \frac{\mathrm{lc}\,(S_k) S_k(0)}{\mathrm{lc}\,(S_j) S_j(0)} X^{\alpha+\beta},$$

and $j = 0$ yields :

$$\det(M_{0,k}) = \frac{\mathrm{lc}\,(S_k) S_k(0)}{b_d} X^{\alpha+\beta-1}.$$

As above, we denote by $(k_i)_{0\leq i\leq m}$ the indices such that (S_{k_i}, S_{k_i+1}) is (α_i, β_i)-defective with $k_0 = 0$ and $k_m = j$. We have :

$$\begin{aligned}
\det(M_j) &= \det(M_0) \cdot \left(\prod_{i=0}^{m-1} \det(M_{k_i,k_{i+1}})\right), \\
&= -b_d \cdot \prod_{i=0}^{m-1} \det(M_{k_i,k_{i+1}}), \\
&= -b_d \cdot \frac{\mathrm{lc}\,(S_{k_1})S_{k_1}(0)}{b_d} X^{\alpha_0+\beta_0-1} \cdot \prod_{i=1}^{m-1} \frac{\mathrm{lc}\,(S_{k_{i+1}})S_{k_{i+1}}(0)}{\mathrm{lc}\,(S_{k_i})S_{k_i}(0)} X^{\alpha_i+\beta_i}, \\
&= -\mathrm{lc}\,(S_{k_m})S_{k_m}(0)X^{k_1-k_0-1} \cdot \prod_{i=1}^{m-1} X^{k_{i+1}-k_i}, \\
&= -\mathrm{lc}\,(S_{k_j})S_{k_j}(0)X^{j-1}.
\end{aligned}$$

Consequently, the matrix M_j is invertible and we easily see that, if $j > 0$:

$$\det(M_j)M_j^{-1} = \begin{pmatrix} V_j & -V_{j-1} \\ -U_j & U_{j-1} \end{pmatrix}.$$

When $j = 0$, we get : $b_d M_0^{-1} = \begin{pmatrix} a_d & 1 \\ b_d & 0 \end{pmatrix}$.

By definition of M_j, we have for $0 \leq j < k$, $M_{j,k} = M_k \cdot M_j^{-1}$. Then for $j > 0$:

$$-\mathrm{lc}\,(S_j)S_j(0)X^{j-1}M_{j,k} = \begin{pmatrix} U_{k-1} & V_{k-1} \\ U_k & V_k \end{pmatrix} \cdot \begin{pmatrix} V_j & -V_{j-1} \\ -U_j & U_{j-1} \end{pmatrix},$$

and for $j = 0$:

$$-b_d M_{0,k} = \begin{pmatrix} U_{k-1} & V_{k-1} \\ U_k & V_k \end{pmatrix} \cdot \begin{pmatrix} a_d & 1 \\ b_d & 0 \end{pmatrix}.$$

Identifying the bottom right-hand side entries of these matrices, yields if $j > 0$:

$$X^{j-1}Q = U_{j-1}V_k - U_k V_{j-1} \in \mathbb{D}[X],$$

and $Q = -U_k$ when $j = 0$. □

The computation of the symmetric quotient of two polynomials does not involve all of their coefficients. In fact, we only need the leading and trailing terms of the divisor. More generally, the computation of successive symmetric quotients can be done with only the knowledge of a few leading and trailing terms of the first divisors. This way it appears cheaper to compute successive quotients instead of successive remainders, as we use only small parts, which we will refer to as "symmetric truncation" of the polynomials.

First we define the symmetric truncation of a polynomial.

Definition 6 *Let* $P = \sum_{i=0}^{d} p_i X^i$ *be an element of* $\mathbb{D}[X]$, $P \neq 0$. *For* $\ell \in \{1, ..., \lfloor d/2 \rfloor\}$, *we denote by* $P_{|\ell}$ *the polynomial*

$$P_{|\ell} = p_0 + \cdots + p_{\ell-1}X^{\ell-1} + p_{d-\ell+1}X^{\ell} + \cdots + p_d X^{2\ell-1}.$$

For $\ell = 0$, *we write* $P_{|0} = 0$, *and for* $\ell > \lfloor d/2 \rfloor$, $P_{|\ell} = P$.

We now analyse the cases where truncation of two polynomials does not affect their symmetric quotient.

Lemma 7 *Let* P *and* P_1 *be two polynomials of* $\mathbb{D}[X]$ *such that* $\deg(P) = d$, $\deg(P_1) = d - \beta \leq d$, $v(P) = 0$ *and* $v(P_1) = \alpha \geq 0$. *Then,*

$$\operatorname{squo}(P, P_1) = \operatorname{squo}(P_{|(\alpha+\beta+1)}, P_{1|(\alpha+\beta+1)}),$$

where P_1 *is considered as a polynomial of degree* d *in order to compute its truncation.*

Proof : Set $\widehat{P} = P_{|(\alpha+\beta+1)}$, $\widehat{P}_1 = P_{1|(\alpha+\beta+1)}$ and $\gamma = d - 2(\alpha+\beta) - 1$. We have $\deg \widehat{P} = 2(\alpha+\beta)+1$, $\deg \widehat{P}_1 = 2\alpha+\beta+1$, $v(\widehat{P}) = 0$, and $v(\widehat{P}_1) = \alpha$. Then, let us consider the following symmetric divisions :

$$\begin{aligned} P &= Q\frac{P_1}{X^\alpha} + X^\beta R \quad \text{with} \quad \deg(R) < d - \alpha - \beta, \\ \widehat{P} &= \widehat{Q}\frac{\widehat{P}_1}{X^\alpha} + X^\beta \widehat{R} \quad \text{with} \quad \deg(\widehat{R}) < \alpha + \beta + 1. \end{aligned}$$

We have $\deg(Q) = \deg(\widehat{Q}) = \alpha + \beta$ and we can write : $Q = Q_1 X^\beta + Q_2$ and $\widehat{Q} = \widehat{Q}_1 X^\beta + \widehat{Q}_2$, where $\deg Q_2$ and $\deg \widehat{Q}_2$ are strictly less than β, and $\deg Q_1 = \deg \widehat{Q}_1 = \alpha$.

Then :

$$P - X^\gamma \widehat{P} = Q\frac{P_1 - X^\gamma \widehat{P}_1}{X^\alpha} + (Q - \widehat{Q})\frac{\widehat{P}_1 X^\gamma}{X^\alpha} + X^\beta(R - X^\gamma \widehat{R}).$$

Since $\deg(P - X^\gamma \widehat{P})$ and $\deg(P_1 - X^\gamma \widehat{P}_1)$ are less than $d - \alpha - \beta$, we see that $\deg(Q - \widehat{Q}) < \beta$, and therefore, $Q_1 = \widehat{Q}_1$. Similarly, we compare the valuation of both sides at the identity :

$$P - \widehat{P} = Q\frac{P_1 - \widehat{P}_1}{X^\alpha} + (Q - \widehat{Q})\frac{\widehat{P}_1}{X^\alpha} + X^\beta(R - \widehat{R}).$$

As $v(P - \widehat{P}) > \alpha + \beta$ and $v((P_1 - \widehat{P}_1)/X^\alpha) > \beta$, we conclude that $v(Q - \widehat{Q}) \geq \beta$, *i.e.* $Q_2 = \widehat{Q}_2$. Hence $Q = \widehat{Q}$.

□

We can also compare the truncation of the symmetric subresultants of two polynomials with the symmetric subresultants of their truncations.

Lemma 8 *Let A and B be in $\mathbb{D}[X]$ of same degree d and valuation 0. Let $(S_i)_{-1 \leq i \leq d}$ be the sequence of the symmetric subresultants of A and B. Let, $(\widehat{S}_j)_{-1 \leq j \leq 2\ell - 1}$ be the sequence of the symmetric subresultants of $A_{|\ell}$ et $B_{|\ell}$ (ℓ fixed in $\{1, ..., \lfloor d/2 \rfloor\}$). Then for $1 \leq j < \ell$, we have :*

$$S_{j|(\ell - j)} = \widehat{S}_{j|(\ell - j)}.$$

Proof : The proof is based on the definition of the coefficients of the symmetric subresultants. Set $A = \sum_{i=0}^{d} a_i X^i$ and $\widehat{A} = \sum_{i=0}^{2\ell-1} \hat{a}_i X^i$ (respectively $B = \sum_{i=0}^{d} b_i X^i$ and $\widehat{B} = \sum_{i=0}^{2\ell-1} \hat{b}_i X^i$). For $0 \leq k < \ell - j$, the coefficient of order k of $\widehat{S}_{j|\ell-j}$ is given by :

$$\mathrm{co}_k(\widehat{S}_{j|\ell-j}) = \left|\begin{array}{ccccccc}
\hat{a}_0 & \dots & \hat{a}_{j-2} & \hat{a}_{k+j-1} & \hat{a}_{2\ell-1} & & \\
 & \ddots & \vdots & \vdots & \vdots & \ddots & \\
 & & \hat{a}_0 & \vdots & \vdots & & \\
 & & 0 & \hat{a}_k & \hat{a}_{2\ell-j} & \dots & \hat{a}_{2\ell-1} \\
\hat{b}_0 & \dots & \hat{b}_{j-2} & \hat{b}_{k+j-1} & \hat{b}_{2\ell-1} & & \\
 & \ddots & \vdots & \vdots & \vdots & \ddots & \\
 & & \hat{b}_0 & \vdots & \vdots & & \\
 & & 0 & \hat{b}_k & \hat{b}_{2\ell-j} & \dots & \hat{b}_{2\ell-1}
\end{array}\right|$$

$$
= \begin{vmatrix}
a_0 & \dots & a_{j-2} & a_{k+j-1} & a_d & & \\
& \ddots & \vdots & \vdots & \vdots & \ddots & \\
& & a_0 & \vdots & \vdots & & \\
& & 0 & a_k & a_{d-j+1} & \dots & a_d \\
b_0 & \dots & b_{j-2} & b_{k+j-1} & b_d & & \\
& \ddots & \vdots & \vdots & \vdots & \ddots & \\
& & b_0 & \vdots & \vdots & & \\
& & 0 & b_k & b_{d-j+1} & \dots & b_d
\end{vmatrix} = \mathrm{co}_k(S_{j|\ell-j}).
$$

In the same way, if $\ell - j \leq k < 2\ell - 2j$, we have :

$$
\begin{aligned}
\mathrm{co}_k(\widehat{S}_{j|\ell-j}) &= \mathrm{co}_{k+j}(\widehat{S}_j), \\
&= \begin{vmatrix}
\hat{a}_0 & \dots & \hat{a}_{j-2} & \hat{a}_{k+2j-1} & \hat{a}_{2\ell-1} & & \\
& \ddots & \vdots & \vdots & \vdots & \ddots & \\
& & \hat{a}_0 & \vdots & \vdots & & \\
& & 0 & \hat{a}_{k+j} & \hat{a}_{2\ell-j} & \dots & \hat{a}_{2\ell-1} \\
\hat{b}_0 & \dots & \hat{b}_{j-2} & \hat{b}_{k+j-1} & \hat{b}_{2\ell-1} & & \\
& \ddots & \vdots & \vdots & \vdots & \ddots & \\
& & \hat{b}_0 & \vdots & \vdots & & \\
& & 0 & \hat{b}_k & \hat{b}_{2\ell-j} & \dots & \hat{b}_{2\ell-1}
\end{vmatrix} \\
&= \begin{vmatrix}
a_0 & \dots & a_{j-1} & a_{d-2\ell+k+2j} & a_d & & \\
& \ddots & \vdots & \vdots & \vdots & \ddots & \\
& & a_0 & \vdots & \vdots & & \\
& & 0 & a_{d-2\ell+k+j+1} & a_{d-j+1} & \dots & a_d \\
b_0 & \dots & b_{j-1} & b_{d-2\ell+k+2j} & b_d & & \\
& \ddots & \vdots & \vdots & \vdots & \ddots & \\
& & b_0 & \vdots & \vdots & & \\
& & 0 & b_{d-2\ell+k+j+1} & b_{d-j+1} & \dots & b_d
\end{vmatrix} \\
&= \mathrm{co}_{d-2\ell+k+j+1}(S_j) = \mathrm{co}_k(S_{j|(\ell-j)}).
\end{aligned}
$$

Therefore $S_{j|(\ell-j)}$ and $\widehat{S}_{j|(\ell-j)}$ have the same coefficients. $\square$

As a consequence, we have $S_{j|k} = \widehat{S}_{j|k}$ for every k such that $0 \leq k \leq l-j$. Also $S_j(0) = \widehat{S}_j(0)$ and $\mathrm{lc}\,(S_j) = \mathrm{lc}\,(\widehat{S}_j)$ for every $j < \ell$.

Further, for a given ℓ, we can predict how many symmetric quotients will be preserved if we replace A and B by $A_{|\ell}$ and $B_{|\ell}$ in the computations.

Theorem 9 *Let A and B be in $\mathbb{D}[X]$ of same degree $d \geq 4$ and valuation 0. Let $(S_i)_{-1\leq i\leq d}$ be the sequence of the symmetric subresultants of A and B. For $\ell \in \{2, ..., \lfloor d/2 \rfloor\}$, let $(\widehat{S}_j)_{-1\leq j\leq 2\ell-1}$ be the sequence of the symmetric subresultants of $A_{|\ell}$ et $B_{|\ell}$.*

Let $(k_i)_{0\leq i\leq s}$, respectively $(\widehat{k}_i)_{0\leq i\leq s'}$, be the indices such that the pairs (S_{k_i}, S_{k_i+1}), respectively $(\widehat{S}_{\widehat{k}_i}, \widehat{S}_{\widehat{k}_i+1})$, are (α_i, β_i)-defective, respectively $(\widehat{\alpha}_i, \widehat{\beta}_i)$-defective (we have $k_0 = \widehat{k}_0 = 0$).

For each i such that $S_{k_i+1} \neq 0$, set $Q_i = \mathrm{lc}\,(S_{k_i+1}) S_{k_i+1}(0) \mathrm{squo}\,(S_{k_i}, S_{k_i+1})$ and for each i such that $\widehat{S}_{\widehat{k}_i+1} \neq 0$, set $\widehat{Q}_i = \mathrm{lc}\,(\widehat{S}_{\widehat{k}_i+1})\widehat{S}_{\widehat{k}_i+1}(0)$ $\mathrm{squo}\,(\widehat{S}_{\widehat{k}_i}, \widehat{S}_{\widehat{k}_i+1})$. Then $M_{k_i,k_{i+1}}$, respectively $\widehat{M}_{\widehat{k}_i,\widehat{k}_{i+1}}$, are the transition matrices of the sequence $(S_j)_{1\leq j\leq d}$, respectively $(\widehat{S}_j)_{1\leq j\leq 2\ell-1}$.

Let m be an index such that $1 \leq m \leq s$ and let $k_m + 1 < \ell$, then for all $i = 0, 1, ..., m-1$, we have :

$$\alpha_i = \widehat{\alpha}_i, \;\; \beta_i = \widehat{\beta}_i, \;\; Q_i = \widehat{Q}_i, k_i = \widehat{k}_i,$$

and finally, $\widehat{M}_{\widehat{k}_i,\widehat{k}_{i+1}} = M_{k_i,k_{i+1}}$.

Proof : First notice that for any $i = 0, ..., m-1$, we have $k_{i+1} = k_i + \alpha_i + \beta_i$; it follows that :

$$\sum_{i=0}^{m-1} \alpha_i + \beta_i < \ell.$$

For each $j < \ell$, by Lemma 8, we have $S_{j|\ell-j} = \widehat{S}_{j|\ell-j}$. Therefore, for each $j = 1, 2, ..., \ell-1$, we have $S_j(0) = \widehat{S}_j(0)$ as well as $\mathrm{lc}\,(S_j) = \mathrm{lc}\,(\widehat{S}_j)$. Then, we see that $k_i = \widehat{k}_i$ for every $i = 0, 1, ..., m$. Furthermore, as $k_{i+1} - k_i = \alpha_i + \beta_i$, and $\widehat{k}_{i+1} - \widehat{k}_i = \widehat{\alpha}_i + \widehat{\beta}_i$, we have $\alpha_i + \beta_i = \widehat{\alpha}_i + \widehat{\beta}_i$ for every $i = 0, 1, ..., m-1$.

We claim that $\alpha_i = \widehat{\alpha}_i$ ($i = 0, \ldots, m-1$). This will also imply that $\beta_i = \widehat{\beta}_i$ for each $i = 0, 1, ..., m-1$. Indeed, we have $S_{k_i+1|\ell-k_i-1} = \widehat{S}_{k_i+1|\ell-k_i-1}$. Therefore, the $\ell-k_i-1$ bottom coefficients of S_{k_i+1} and $\widehat{S}_{k_i+1}$ are equal. But $v(S_{k_i+1}) = \alpha_i$ and we have $k_i + \alpha_i + \beta_i = k_{i+1} \leq k_m < \ell$. Thus α_i is less than $\ell - k_i - \beta_i \leq \ell - k_i - 1$. The valuations of S_{k_i+1} and $\widehat{S}_{k_i+1}$ must then be equal.

Having proved that the sequences of indices $(k_i)_{0\leq i<m}$, $(\alpha_i)_{0\leq i<m}$, $(\beta_i)_{0\leq i<m}$

are equal to their counterparts, we now show the equality of the symmetric quotients.

First we have, by Lemma 7 :

$$\begin{aligned} Q_i &= \operatorname{squo}(\operatorname{lc}(S_{k_i+1}) S_{k_{i+1}}(0) \cdot S_{k_i}, S_{k_i+1}) \\ &= \operatorname{squo}(\operatorname{lc}(S_{k_i+1}) S_{k_{i+1}}(0) \cdot S_{k_i|\alpha_i+\beta_i+1}, S_{k_i+1|\alpha_i+\beta_i+1}), \end{aligned}$$

since (S_{k_i}, S_{k_i+1}) is (α_i, β_i)-defective .

If $i < m$ and $k_m + 1 < \ell$, we have $\alpha_i + \beta_i + 1 < \ell - k_i$, and, by Lemma 8, $S_{k_i|\alpha_i+\beta_i+1} = \widehat{S}_{k_i|\alpha_i+\beta_i+1}$. In respect of $S_{k_i+1|\alpha_i+\beta_i+1}$, the truncature is applied to S_{k_i+1} considered of formal degree $d - k_i$ (Lemma 7). But, by Lemma 8, we have $S_{k_i+1|\alpha_i+\beta_i+1} = \widehat{S}_{k_i+1|\alpha_i+\beta_i+1}$, polynomials being truncated with their actual degree. However using formal degree $d - k_i$ instead of actual degree $d - k_i - \beta_i$, we do not take into account so many coefficients and the equality of the truncatures holds as well.

Since the leading coefficients and constant terms of the sequence $(S_j)_{0\le j<\ell}$ and $(\widehat{S}_j)_{0\le j<\ell}$ are equal, we can write :

$$\begin{aligned} Q_i &= \operatorname{squo}(\operatorname{lc}(\widehat{S}_{k_i+1}) \widehat{S}_{k_{i+1}}(0) \cdot \widehat{S}_{k_i|\alpha_i+\beta_i+1}, \widehat{S}_{k_i+1|\alpha_i+\beta_i+1}) \\ &= \widehat{Q}_i. \end{aligned}$$

Finally, inspecting the expression of the transition matrix $M_{k_i,k_{i+1}}$ given by (1) and (2), we see that all the ingredients have been proven to be equal for the two matrices $M_{k_i,k_{i+1}}$ and $\widehat{M}_{k_i,k_{i+1}}$ $(i = 0, \ldots, m-1)$.

□

4.3 Fast Algorithm

We now describe the **FSSR** Algorithm which is written in pseudo-code further down.

Let A and B be two polynomials of $\mathbb{D}[X]$ of same degree and valuation 0. They are considered as global variables. The **FSSR** Algorithm takes as input a pair (S_{k_i}, S_{k_i+1}) of two successive symmetric subresultants of A and B, (α_i, β_i)-defective and an integer $r < (d - k_i)$.

It returns the sequence of the symmetric quotients $(Q_j, \alpha_j, \beta_j)_{i\le j<v-1}$ with v the largest index such that $k_v < k_i + r$. It returns also the transition matrix M_{k_i,k_v}.

In the general case, we are interested in finding the entire sequence of symmetric quotients of A and B, and $\mathbf{FSSR}(S_0, S_1, d)$ with $S_0 = B$, $S_1 = \mathrm{lc}\,(B)A - \mathrm{lc}\,(A)B$ will suffice. This way, we compute the entire sequence of symmetric quotients except perhaps for the last one which can be obtained with an extra division.

How does this work ? We use a strategy of *divide and conquer*, to compute a partial sequence at each step. Here is a description of each non-trivial step.

Step 1 : If S_{k_i+1} is 0, we have already reached the end of the sequence of the symmetric subresultants of A and B.

Step 2 : If $r \leq 2$, the algorithm performs symmetric divisions starting with the polynomials $S_{k_i|r}$ and $S_{k_i+1|r}$ whose degrees are at most 3. It computes also directly the corresponding transition matrix.

Step 4 : a call to $\mathbf{FSSR}\left(S_{k_i|r}, S_{k_i+1|r}, \lceil \frac{r}{2} \rceil\right)$ is executed.

Since the third recursive call, the coefficient of truncature is stricktly lower than $\lfloor \frac{d-k_i}{2} \rfloor$, and therefore Theorem 9 can be applied : the algorithm computes Q_j, α_j, β_j for $j = i, \ldots, u-1$ as well as M_{k_i,k_u}, with u the largest index such that $k_u < k_i + \lceil r/2 \rceil$.

Step 5 : We compute S_{k_u}, and S_{k_u+1} via M_{k_i,k_u}.

Step 6 : Then, via a symmetric quotient, we compute Q_u and add it to the list of quotients already computed. $M_{k_i,k_{u+1}}$ is computed as well as $(S_{k_{u+1}}, S_{k_{u+1}+1})$.

This intermediary step is needed to guarantee that the coefficient of truncature in the next call to $\mathbf{FSSR}$ (step 7) is smaller than $\lceil \frac{r}{2} \rceil$.

Step 7 : We perform a second call to $\mathbf{FSSR}\Big(S_{k_{u+1}|r}, S_{k_{u+1}+1|r}, r - (k_{u+1} - k_i)\Big)$. We therefore obtain symmetric quotients Q_u up to Q_{v-1} with v the largest index such that $k_v + 1 < r + k_i$.

Step 8 : We get together the pieces already computed.

Remark : throughout the algorithm, instead of computing $M_{k_i,k_m} = M_{k_j,k_m} \cdot M_{k_i,k_j}$ for $0 \leq i < j < m \leq s$, it is preferable to compute :

$$M_{k_i,k_m} = \Big(\Big((\mathrm{lc}\,(S_{k_j})S_{k_j}(0)) \cdot M_{k_j,k_m}\Big) \cdot M_{k_i,k_j}\Big) / (\mathrm{lc}\,(S_{k_j})S_{k_j}(0))$$

using the order of operations indicated by the parentheses. In doing so, we keep all computations in $\mathbb{D}[X]$ and the algorithm remains fraction-free.

```
ALGORITHM FSSR

INPUT :       – $(S_{k_i}, S_{k_i+1})$, a pair $(\alpha_i, \beta_i)$-defective of symmetric
                subresultants of $A$, $B$,
              – $r$ a positive integer, $r \leq d - k_i$.
OUTPUT :      – the list $L := [Q_i, \alpha_i, \beta_i, ..., Q_{v-1}, \alpha_{v-1}, \beta_{v-1}]$ and $M_{k_i,k_v}$, where $v$ is the
              biggest integer such that $k_v < r + k_i$.

MAIN PART :   1 – IF $S_{k_i+1} = 0$ then RETURN $L := []$, and $M := Id_2$.
              2 – ELSE IF $r \leq 2$ then compute $L$ using symmetric divisions of $S_{k_i|r}$ with
              $S_{k_i+1|r}$ and $M_{k_i,k_u}$ from definition.
                – ELSE
              3 – $r' := \lceil \frac{r}{2} \rceil$;
              4 – $L_1$ :=FSSR($S_{k_i|r}, S_{k_i+1|r}, r'$);
                      % $L_1$ contains :
                      % $Q_i, \alpha_i, \beta_i, ..., Q_{u-1}, \alpha_{u-1}, \beta_{u-1}$,
                      % we get also : $M_{k_i,k_u}$,
                      % with u, largest integer such that $k_u < r' + k_i$.
              5 – Compute $S_{k_u}$ and $S_{k_u+1}$ by :
                      $$\begin{pmatrix} X^{k_u-1}S_{k_u} \\ X^{k_u}S_{k_u+1} \end{pmatrix} = M_{k_i,k_u} \cdot \begin{pmatrix} X^{k_i-1}S_{k_i} \\ X^{k_i}S_{k_i+1} \end{pmatrix}.$$
              6 – $Q_u = \mathrm{lc}\,(S_{k_u+1}) S_{k_{u+1}}(0) \mathrm{squo}\,(S_{k_u}, S_{k_u+1})$ ;
                  $L_1 = L_1 \bigcup \{Q_u\}$. $M_{k_i,k_{u+1}} = M_{k_u,k_{u+1}} \cdot M_{k_i,k_u}$
                Compute $S_{k_{u+1}}$ and $S_{k_{u+1}+1}$ by :
                      $$\begin{pmatrix} X^{k_{u+1}-1}S_{k_{u+1}} \\ X^{k_{u+1}}S_{k_{u+1}+1} \end{pmatrix} = M_{k_i,k_{u+1}} \cdot \begin{pmatrix} X^{k_i-1}S_{k_i} \\ X^{k_i}S_{k_i+1} \end{pmatrix}.$$
              7 – $L_2$ :=FSSR($S_{k_{u+1}|r}, S_{k_{u+1}+1|r}, r - (k_{u+1} - k_i)$);
                      % $L_2$ contains :
                      % $Q_{u+1}, \alpha_{u+1}, \beta_{u+1}, ..., Q_{v-1}, \alpha_{v-1}, \beta_{v-1}$;
                      % we get also : $M_{k_{u+1},k_v}$.
                      % with $v$, largest integer such that $k_v < r + k_{u+1}$.
              8 – $L := L_1 \bigcup L_2$ ; $M_{k_i,k_v} = M_{k_{u+1},k_v} \cdot M_{k_i,k_{u+1}}$

END.
```

We now consider its cost.

Theorem 10 *Let $\mathbb{D}$ be a sub-ring of $\mathbb{C}$ and let A and B be two polynomials of same degree d in $\mathbb{D}[X]$. The algorithm **FSSR**(S_0, S_1, d) with $S_0 = B$ and $S_1 = \mathrm{lc}\,(B)A - \mathrm{lc}\,(A)B$ uses at most*

$$\mathcal{O}(\mathcal{M}(d).\log(d)) = \mathcal{O}(d \log^2(d) \log\log(d))$$

arithmetical operations in $\mathbb{D}$ ($\mathcal{M}(d)$ denotes the cost in arithmetical operations of multiplying two polynomials of degree at most d in $\mathbb{D}[X]$).

*If A and B are elements of $\mathbb{Z}[X]$ or $\mathbb{Z}[i][X]$, and if the size of their coefficients is bounded by σ, then **FSSR**(S_0, S_1, d) is executed in less than*

$$\mathcal{O}\Big((d^2.(\sigma + \log(d)).\log(d\sigma + d\log(d)).\log\big(\log(d\sigma + d\log(d))\big).\log(d)\Big)$$

binary operations on a multiband Turing *machine, using DFT.*

Proof : Let us denote by $\mathcal{CF}(\delta)$ the cost in terms of arithmetical operations of the computation of **FSSR**(S_0, S_1, δ). We do not take into account the degrees of the polynomials S_0 and S_1, as, from the very beginning of the algorithm, these polynomials are truncated to order δ and the degrees of the polynomials that we really manipulate are lower than $2\delta - 1$.

During the execution of **FSSR**(S_0, S_1, δ), we use two calls of **FSSR** with δ replaced by $\lceil \frac{\delta}{2} \rceil$. The intermediate computation consists of some multiplications and a symmetric division : the number of arithmetical operations is bounded by $\mathcal{O}(\mathcal{M}(\delta))$. Therefore, we have :

$$\mathcal{CF}(\delta) \leq 2\mathcal{CF}\Big(\Big\lceil \frac{\delta}{2} \Big\rceil\Big) + \mathcal{O}(\mathcal{M}(\delta)).$$

It follows that $\mathcal{CF}(\delta)$ is bounded by $\mathcal{O}\left(\mathcal{M}(\delta)\log(\delta)\right)$. Hence the first assertion with $\delta = d$.

In the case of $\mathbb{Z}$ or $\mathbb{Z}[i]$, we follow the same arguments. However, we have to bound the size of the coefficients appearing in the algorithm. These coefficients are minors of $\mathrm{Sylv}_d(A, B)$. They can be bounded by Hadamard's formula : their size is less than $\tau = 2d(\sigma + \log(d))$. The coefficients of the transition matrices M_{k_i,k_j} are of the same size. If $\mathcal{M}(d, \tau)$ is the binary cost to compute the product of two polynomials of degree less than d with coefficients of size bounded by τ, we get :

$$\mathcal{CF}(d, \sigma) \leq \mathcal{O}\left(\mathcal{M}(d, \tau)\log(d)\right).$$

This proves the result in the case of a multiband Turing machine. □

Remark : it might surprise the reader that we compute the sequence of symmetric quotients instead of the symmetric sub-resultants. Indeed as far as applications are concerned the important elements are the symmetric remainders and not the symmetric quotients. In fact, the applications we know of use either the constant terms of a sequence of symmetric remainders, or a particular symmetric remainder. When the sequence of symmetric quotients is known, the sequence of $S_{k_i}(0)$ can be computed in $\mathcal{O}(d)$ as we can see in the introduction to Part 4.

In this case, when a particular symmetric remainder is needed, computing the corresponding transition matrix is enough to determine this specific remainder, up to a few additional operations.

5 Application to Toeplitz matrices

In this section we consider the relationship between sequences of principal minors of a TOEPLITZ matrix and of the symmetric sub-resultants of polynomials. As a consequence, we will get new algorithms to compute the signature and the inverse of such a matrix. We do not improve the cost of algorithms presented in [2] and [13] and already used in the complex numerical case. However, in the case of integer coefficients, we control the size of results and use fraction-free computations; this is well suited for computer algebra.

5.1 Relationship between TOEPLITZ *matrices and symmetric sub-resultants*

We first establish a link between constant terms of the symmetric subresultants and principal minors of a TOEPLITZ matrix.

Proposition 11 *Let $F = \sum_{i=0}^{d} f_i X^i$ and $G = \sum_{i=0}^{d} g_i X^i$ be two polynomials of equal valuation; we suppose that the degree of F is exactly d; the degree of G is formally considered equal to d but could be less. Let*

$$\frac{G}{F} = v + \sum_{i\geq 1} v_i X^i$$

be the expansion around zero of G/F, and

$$\frac{G}{F} = -u - \sum_{i\geq 1} u_i X^{-i}$$

its expansion around infinity. Let $\mathcal{T}_k(F,G) = (t_{i,j})_{1\leq i,j,\leq k}$ be the TOEPLITZ *matrix :*

$$\begin{cases} t_{i,j} = v_{j-i} & \text{if} \quad i < j \\ t_{i,j} = u_{i-j} & \text{if} \quad i > j \\ t_{i,j} = u + v & \text{if} \quad i = j \end{cases} .$$

Then, if $(S_j)_{-1\leq j\leq d}$ is the sequence of symmetric sub-resultants computed with $S_{-1}=F$ and $S_0=G$, we have, for any $k=1,...,d$:

$$S_k(0)=(-1)^k.f_0^k.f_d^k\det(\mathcal{T}_k(F,G)).$$

Proof : As we have $G=(-u-\sum_{i>0}u_iX^{-i})F$, the following sequence of relations holds :

$$\begin{aligned}
g_0 &= -uf_0-u_1f_1-\cdots-u_{d-1}f_{d-1}-u_df_d,\\
g_1 &= -uf_1-u_1f_2-\cdots-u_{d-1}f_d,\\
&\vdots\\
g_d &= -uf_d.
\end{aligned}$$

Now define for $k=1,...,d$, the following three $k\times k$ matrices :

$$\widetilde{\mathbf{F}}_k=\begin{pmatrix} f_d & 0 & 0\\ f_{d-1} & f_d & \\ \vdots & & \ddots \\ f_{d-k+1} & \cdots\cdots & f_d\end{pmatrix},\quad \widetilde{\mathbf{G}}_k=\begin{pmatrix} g_d & 0 & 0\\ g_{d-1} & g_d & \\ \vdots & & \ddots \\ g_{d-k+1} & \cdots\cdots & g_d\end{pmatrix},$$

$$\mathbf{U}_k=\begin{pmatrix} u & 0 & 0\\ u_1 & u & \\ \vdots & & \ddots \\ u_{k-1} & \cdots\cdots & u\end{pmatrix}.$$

Our relations can be translated by the following matricial relation :

$$\widetilde{\mathbf{G}}_k=-\mathbf{U}_k\cdot\widetilde{\mathbf{F}}_k.$$

Likewise, comparing the coefficients of $G=(v+\sum_{i>0}v_iX^i)F$, we obtain :

$$\mathbf{G}_k=\mathbf{V}_k\cdot\mathbf{F}_k$$

with

$$\mathbf{F}_k = \begin{pmatrix} f_0 & \cdots\cdots & f_{k-1} \\ & f_0 & f_{k-2} \\ & \ddots & \vdots \\ & & f_0 \end{pmatrix}, \quad \mathbf{G}_k = \begin{pmatrix} g_0 & \cdots\cdots & g_{k-1} \\ & g_0 & g_{k-2} \\ & \ddots & \vdots \\ & & g_0 \end{pmatrix},$$

$$\mathbf{V}_k = \begin{pmatrix} v & v_1 & \cdots & v_{k-1} \\ & v & & v_{k-2} \\ & & \ddots & \vdots \\ & & & v \end{pmatrix}.$$

These relations imply :

$$\begin{pmatrix} \mathbf{I}_k & \mathbf{I}_k \\ \mathbf{V}_k & -\mathbf{U}_k \end{pmatrix} \cdot \begin{pmatrix} \mathbf{F}_k & \mathbf{0} \\ \mathbf{0} & \widetilde{\mathbf{F}}_k \end{pmatrix} = \begin{pmatrix} \mathbf{F}_k & \widetilde{\mathbf{F}}_k \\ \mathbf{G}_k & \widetilde{\mathbf{G}}_k \end{pmatrix}.$$

($\mathbf{I}_k$ denotes the identity matrix of order k.) Now, we can compute the determinant of each side. For the left most matrix we subtract the i-th column from the $(i+k)$-th one $(i = 1, ..., k)$. The result follows. $\square$

5.2 Signature of an Hermitian TOEPLITZ *matrix*

Given an Hermitian TOEPLITZ matrix :

$$\mathcal{T}_d = \begin{pmatrix} t_0 & \bar{t}_1 & \cdots & \bar{t}_{d-1} \\ t_1 & \ddots & & \vdots \\ \vdots & & \ddots & \bar{t}_1 \\ t_{d-1} & \cdots & t_1 & t_0 \end{pmatrix},$$

we want to compute the signature of the associated Hermitian form. We didn't find any reference in the literature to this simple problem, although there are several methods proposed in the case of real HANKEL matrices (see [12] and [32]).

The signature of $\mathcal{T}_d$ can be computed from the sequence of signs of its principal minors. The rule given by IOHVIDOV [18] and, independently, by one of us [33], works even when some of these minors vanish. Once the minors are computed, the signature is obtained in $\mathcal{O}(d)$ arithmetic operations.

The problem is then reduced to the computation of the sequence of principal minors of $\mathcal{T}_d$. This can be achieved by the computation of the constant terms of the sequence of the symmetric subresultants of two polynomials as the next proposition shows.

Proposition 12 *Let $\mathcal{T}_d$ be a Hermitian* TOEPLITZ *matrix, defined as above, and T the polynomial :*

$$T = -\bar{t} - \bar{t}_1 X - \cdots - \bar{t}_{d-1} X^{d-1} + t_{d-1} X^d + \cdots + t_1 X^{2d-2} - t X^{2d-1},$$

with $t \neq 0$ and $t_0 = t + \bar{t}$.

Let $(S_j)_{-1 \leq j \leq 2d}$ be the sequence of symmetric subresultants of $X^{2d-1} + 1$ and T. For $j = 1, ..., d$, we have :

$$\delta_j = S_j(0),$$

where δ_j is the j-th principal minor of $\mathcal{T}_d$.

Proof : We can use Proposition 11 in this special case. But the result can also be seen directly as well. Indeed, we have for each $j = 1, \ldots, d$:

$$S_j(0) = \begin{array}{|cccccccc|}
1 & & & 0 & 1 & & & \\
 & \ddots & & \vdots & & \ddots & & \\
 & & 1 & \vdots & & & \ddots & \\
 & & 0 & 1 & & & & 1 \\
-\bar{t} & \cdots & -\bar{t}_{j-2} & -\bar{t}_{j-1} & t & & & \\
 & \ddots & \vdots & \vdots & \vdots & \ddots & & \\
 & & -\bar{t} & \vdots & \vdots & & \ddots & \\
 & & 0 & -\bar{t} & t_{j-1} & \cdots & \cdots & t \\
\multicolumn{3}{c}{\underbrace{\hphantom{-\bar{t} \cdots -\bar{t}_{j-2}}}_{j-1}} & & \multicolumn{4}{c}{\underbrace{\hphantom{t_{j-1} \cdots \cdots t}}_{j}}
\end{array}$$

$$
= \left| \begin{array}{cccccccc}
1 & & & 0 & 0 & \cdots & \cdots & 0 \\
 & \ddots & & & \vdots & & & \vdots \\
 & & \ddots & & \vdots & & & \vdots \\
0 & & & 1 & 0 & \cdots & & 0 \\
-\bar{t} & -\bar{t}_1 & \cdots & -\bar{t}_{j-1} & t_0 & \bar{t}_1 & \cdots & \bar{t}_{j-1} \\
 & \ddots & \ddots & \vdots & t_1 & \ddots & & \vdots \\
 & & \ddots & \bar{t}_1 & \vdots & \ddots & \ddots & \bar{t}_1 \\
 & & & -\bar{t} & t_{j-1} & \cdots & t_1 & t_0
\end{array} \right|
$$

$$= \delta_j .$$

□

Using **FSSR** Algorithm, we can then compute the signature of a Hermitian TOEPLITZ matrix of order d in $\mathcal{O}(d\log(d)^2\log\log(d))$ arithmetical operations.

BRUNIE in [4] has shown that it is possible to improve the algorithm also to get the rank of the matrix, but this extra computation has an arithmetical cost of $\mathcal{O}(d^2)$ operations. There still exists no fast solution to the rank problem.

5.3 TOEPLITZ *linear systems*

We now consider a much more popular application than the signature problem. Let $\mathcal{T}_d$ be a TOEPLITZ matrix of dimension d. Suppose it is invertible and we want to compute $\mathcal{T}_d^{-1}$. Several authors have given fast algorithms to solve the problem. BRENT, GUSTAVSON and YUN in [2] have a solution using PADÉ approximants, continued fractions and Euclidean algorithms. Their solution has a cost of $\mathcal{O}(d\log(d)^2\log\log(d))$ arithmetical operations and uses the GOHBERG-SEMENCUL formulae. More recently GEMIGNIANI in [13] and [14] has used the SCHUR decomposition of a matrix with the advantage that in defective cases no extra computation is needed. Both algorithms have the same cost. BINI and PAN give in [3] the state of the art on this problem.

The solution developed here also works with the formulae of GOHBERG-SEMENCUL. However we use the symmetric subresultants; therefore we are able to manage the defective cases directly with the **FSSR** algorithm without extra computation. Our cost is the same as in [2], although, in defective cases, we approximately divide computation time of by a factor two. Furthermore, our algorithm is fraction free, until the last step.

As it is one of our tools, we recall first the Gohberg-Semencul formulae [15].

Theorem 13 *Let $\mathcal{T}_d = (t_{i-j})_{0\le i,j\le d-1}$ be an invertible* Toeplitz *matrix. We denote by $\mathbf{x} = (x_0, \ldots, x_{d-1})^t$ the first column and by $\mathbf{y} = (y_0, ..., y_{d-1})^t$ the last column of $\mathcal{T}_d^{-1}$. If $x_0 \neq 0$, we have :*

$$\mathcal{T}_d^{-1} = \frac{1}{x_0}\left[\begin{pmatrix} x_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 \\ x_{d-1} & \cdots & \cdots & x_0 \end{pmatrix} \cdot \begin{pmatrix} y_{d-1} & \cdots & \cdots & y_0 \\ 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & y_{d-1} \end{pmatrix} \right.$$
$$\left. - \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ y_0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ y_{d-2} & \cdots & y_0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & x_{d-1} & \cdots & x_1 \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & x_{d-1} \\ 0 & \cdots & \cdots & 0 \end{pmatrix} \right]. \quad (*)$$

If $x_0 = 0$, there exists an extension $\mathcal{T}_{d+1} = (t_{i-j})_{0\le i,j\le d}$ of $\mathcal{T}_d$ which is invertible and such that the first column of $\mathcal{T}_{d+1}^{-1}$, say $\tilde{\mathbf{x}} = (\tilde{x}_0, \ldots, \tilde{x}_d)$, has its first coordinate different from zero. Let $\tilde{\mathbf{y}} = (\tilde{y}_0, \ldots, \tilde{y}_d)$ denote the last column of $\mathcal{T}_{d+1}^{-1}$. In this case, we have :

$$\mathcal{T}_d^{-1} = \frac{1}{\tilde{x}_0}\left[\begin{pmatrix} \tilde{x}_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 \\ \tilde{x}_{d-1} & \cdots & \cdots & \tilde{x}_0 \end{pmatrix} \cdot \begin{pmatrix} \tilde{y}_d & \cdots & \cdots & \tilde{y}_1 \\ 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \tilde{y}_d \end{pmatrix} \right.$$
$$\left. - \begin{pmatrix} \tilde{y}_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 \\ \tilde{y}_{d-1} & \cdots & \cdots & \tilde{y}_0 \end{pmatrix} \cdot \begin{pmatrix} \tilde{x}_d & \cdots & \cdots & \tilde{x}_1 \\ 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \tilde{x}_d \end{pmatrix} \right]. \quad (**)$$

Therefore, if $\mathcal{T}_d = (t_{i-j})_{0\le i,j\le d-1}$ is an invertible Toeplitz matrix, the problem is reduced to the computation of the vectors $\mathbf{x}$ and $\mathbf{y}$ or $\tilde{\mathbf{x}}$ and $\tilde{\mathbf{y}}$ depending on the situation. We can use the symmetric subresultants algorithm for this task.

Let us define the two polynomials :

$$S_{-1} = X^{2d+1} + 1,$$

$$S_0 = T_{\gamma,\delta} = -t_- - t_{-1}X - \cdots - t_{-d+1}X^{d-1} + \gamma X^d + \delta X^{d+1} + t_{d-1}X^{d+2} + \cdots + t_+ X^{2d+1},$$

where coefficients t_+ and t_- are different from 0 and satisfy $t_+ + t_- = t_0$. The complex coefficients γ and δ will be determined later on during the computation in order to apply Theorem 13.

One can note that from $F = S_{-1}$ and $G = S_0$ we can rebuild the matrix T using Proposition 11 : we have $T = T_d(S_{-1}, S_0)$.

Let $(S_j)_{-1 \leq j \leq 2d+1}$ be the sequence of symmetric subresultants computed with S_{-1} and S_0. As $\mathcal{T}_d$ is invertible, we have $S_d(0) = (-1)^d \det(\mathcal{T}_d) \neq 0$ (use Proposition 11). We will write $S_d = \sum_{i=0}^{d+1} s_i X^i$. There also exist two polynomials $U_{d-1} = \sum_{i=0}^{d-1} u_i X^i$ and $V_{d-1} = \sum_{i=0}^{d-1} v_i X^i$, such that :

$$X^{d-1} S_d = U_{d-1}(X^{2d+1} + 1) + V_{d-1} T_{\gamma,\delta}.$$

This relation can be translated into matricial terms as follows :

$$\left(\begin{array}{cccc}
1 & 0 & \cdots & 0 \\
0 & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & 0 \\
0 & \cdots & 0 & 1 \\
\hline
0 & \cdots & \cdots & 0 \\
\vdots & & & \vdots \\
 & & & \\
\vdots & & & \vdots \\
0 & \cdots & \cdots & 0 \\
\hline
1 & 0 & \cdots & 0 \\
0 & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & 0 \\
0 & \cdots & 0 & 1
\end{array}\right) \cdot \begin{pmatrix} u_0 \\ \vdots \\ \vdots \\ u_{d-1} \end{pmatrix} +$$

$$\left(\begin{array}{cccc} -t_- & 0 & \cdots & 0 \\ -t_{-1} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ -t_{-d+1} & \cdots & -t_{-1} & -t_- \\ \hline -\gamma & -t_{-d+1} & \cdots & -t_{-1} \\ \delta & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & -\gamma \\ t_1 & & t_{d-1} & \delta \\ \hline t_+ & t_1 & \cdots & t_{d-1} \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & t_1 \\ 0 & \cdots & 0 & t_+ \end{array}\right) \cdot \begin{pmatrix} v_0 \\ \vdots \\ \vdots \\ v_{d-1} \end{pmatrix} = \left(\begin{array}{c} 0 \\ \vdots \\ 0 \\ s_0 \\ \hline s_1 \\ \vdots \\ \vdots \\ \vdots \\ s_{d+1} \\ \hline 0 \\ \vdots \\ \vdots \\ 0 \end{array}\right) \begin{array}{l} \left.\vphantom{\begin{array}{c} \vdots \\ 0 \\ s_0 \end{array}}\right\} d \\ \left.\vphantom{\begin{array}{c} s_1 \\ \vdots \\ \vdots \\ \vdots \\ s_{d+1} \end{array}}\right\} d+1 \, . \\ \left.\vphantom{\begin{array}{c} 0 \\ \vdots \\ \vdots \end{array}}\right\} d \end{array}$$

If we subtract the first d lines from the last d ones, we obtain :

$$\mathcal{T}_d^{\,t} \begin{pmatrix} v_0 \\ \vdots \\ \vdots \\ v_{d-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -s_0 \end{pmatrix},$$

with $s_0 = S_d(0) = (-1)^d \det(\mathcal{T}_d) \neq 0$. Therefore, we see that $\dfrac{-1}{s_0} \begin{pmatrix} v_{d-1} \\ \vdots \\ \vdots \\ v_0 \end{pmatrix}$ is the first column of $\mathcal{T}_d^{-1}$. The same trick applied to $\mathcal{T}_d^t$ gives the last column of our matrix. If $v_{d-1} \neq 0$, we can apply the first formula of Gohberg-Semencul to conclude.

By the proof of Lemma 1, we get $v_{d-1} = -S_{d-1}(0) = (-1)^d \det(\mathcal{T}_{d-1})$. If $v_{d-1} = 0$, we have to compute the next symmetric subresultants, S_{d+1}. There exist two polynomials, U_d and V_d, of degree at most d, such that :

$$X^d S_{d+1} = U_d(X^{2d+1} + 1) + V_d T_{\gamma,\delta}.$$

In this case, $\deg(V_d) = d$, because $\mathrm{co}_d(V_d) = v_d = (-1)^{d+1}\det(\mathcal{T}_d) \neq 0$. If $S_{d+1}(0) \neq 0$, we see, by the same computation as in the generic case just above, that the coefficients of $-V_d/S_{d+1}(0)$ determine the first column of the inverse of :

$$\mathcal{T}_{d+1} = \left(\begin{array}{c|c} & \gamma \\ \mathcal{T}_d & t_{-d+1} \\ & \vdots \\ & t_{-1} \\ \hline \delta\ t_{d-1} \cdots t_1 & t_0 \end{array}\right).$$

Therefore we have to choose the coefficients γ and δ in order to satisfy $S_{d+1}(0) = (-1)^d \det(\mathcal{T}_{d+1}) \neq 0$.

Proposition 14 *Using the above definitions, suppose that* $\det(\mathcal{T}_{d-1}) = 0$ *and* $\det(\mathcal{T}_d) \neq 0$*. Define the three vectors of dimension d :*

$$\mathbf{V}_- = \begin{pmatrix} 0 \\ t_{-d+1} \\ \vdots \\ t_{-1} \end{pmatrix}, \mathbf{V}_+ = \begin{pmatrix} 0 \\ t_{d-1} \\ \vdots \\ t_1 \end{pmatrix} \text{ and } \mathbf{e_0} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Then, the determinant of $\mathcal{T}_{d+1}$ *satisfies :*

$$\det(\mathcal{T}_{d+1}) = -\det(\mathcal{T}_d) \cdot (\gamma \mathbf{V}_+{}^t \mathcal{T}_d^{-1} \mathbf{e}_0 + \delta \mathbf{e}_0^t \mathcal{T}_d^{-1} \mathbf{V}_- + \mathbf{V}_+{}^t \mathcal{T}_d^{-1} \mathbf{V}_- - t_0).$$

Furthermore, in the above relation, the coefficients $\mathbf{V}_+{}^t \mathcal{T}_d^{-1} \mathbf{e}_0$ *and* $\mathbf{e}_0^t \mathcal{T}_d^{-1} \mathbf{V}_-$*, of* γ *and* δ *respectively, cannot vanish.*

Proof : We can factorize $\mathcal{T}_{d+1}$ as follows :

$$\mathcal{T}_{d+1} = \left(\begin{array}{c|c} & 0 \\ \mathcal{T}_d & \vdots \\ & 0 \\ \hline \delta\ t_{d-1} \cdots t_1 & f \end{array}\right) \cdot \left(\begin{array}{c|c} \mathcal{I}_d & r \\ \hline 0 \cdots 0 & 1 \end{array}\right),$$

with $r = \mathcal{T}_d^{-1} \begin{pmatrix} \gamma \\ t_{-d+1} \\ \vdots \\ t_{-1} \end{pmatrix} = \mathcal{T}_d^{-1}(\gamma \mathbf{e_0} + \mathbf{V}_-)$ and :

$$f = t_0 - (\delta \mathbf{e_0} + \mathbf{V}_+)^t \cdot \mathcal{T}_d^{-1}(\gamma \mathbf{e_0} + \mathbf{V}_-).$$

Then, we have :

$$f = t_0 - (\gamma\delta \cdot \mathbf{e_0}^t \mathcal{T}_d^{-1} \mathbf{e_0} + \gamma \cdot \mathbf{V}_+{}^t \mathcal{T}_d^{-1} \mathbf{e_0} + \delta \cdot \mathbf{e_0}^t \mathcal{T}_d^{-1} \mathbf{V}_- + \mathbf{V}_+{}^t \mathcal{T}_d^{-1} \mathbf{V}_-).$$

But $\mathbf{e_0}^t \mathcal{T}_d^{-1} \mathbf{e_0}$ is, up to the factor $1/\det(\mathcal{T}_d)$, equal to $\det(\mathcal{T}_{d-1})$ which is zero. Therefore, we obtain the stated formula.

We know that $\mathcal{T}_d$ is invertible; let $(x_0, \ldots, x_{d-1})^t$ be the first column of its inverse. Since $\det(\mathcal{T}_{d-1}) = 0$, we have $x_0 = 0$. If we suppose that $\mathbf{V}_+{}^t \mathcal{T}_d^{-1} \mathrm{e}_0 = 0$, we have $(0, t_{d-1}, \ldots, t_1) \cdot \begin{pmatrix} 0 \\ x_1 \\ \vdots \\ x_{d-1} \end{pmatrix} = 0$, and we can write :

$$\left(\begin{array}{c|c} \mathcal{T}_d & \begin{matrix} 0 \\ t_{-d+1} \\ \vdots \\ t_{-1} \end{matrix} \\ \hline 0 \; t_{d-1} \; \cdots \; t_1 & t_0 \end{array}\right) \cdot \left(\begin{array}{c} 0 \\ x_1 \\ \vdots \\ x_{d-1} \\ \hline 0 \end{array}\right) = \left(\begin{array}{c} 1 \\ 0 \\ \vdots \\ 0 \\ \hline 0 \end{array}\right)$$

$$= \left(\begin{array}{c|c} t_0 & t_{-1} \; \cdots \; t_{-d+1} \; 0 \\ \hline \begin{matrix} t_1 \\ \vdots \\ t_{d-1} \\ 0 \end{matrix} & \mathcal{T}_d \end{array}\right) \cdot \left(\begin{array}{c} 0 \\ \hline x_1 \\ \vdots \\ x_{d-1} \\ 0 \end{array}\right)$$

We therefore conclude that :

$$\mathcal{T}_d \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_{d-1} \\ 0 \end{pmatrix} = 0.$$

However, as $\mathcal{T}_d$ is invertible, the equation $\mathcal{T}_d \cdot X = 0$ has only one solution, that is the zero vector. This leads to a contradiction since $x_1, \ldots, x_{d-1}$ are not all equal to zero. Therefore, the coefficient $\mathbf{V}_+{}^t\mathcal{T}_d^{-1}\mathbf{e_0}$ cannot vanish. A similar argument works with $\mathbf{e_0}{}^t\mathcal{T}_d^{-1}\mathbf{V}_-$. □

Now we are able to choose a pair (γ, δ) such that $\det(\mathcal{T}_{d+1}) \neq 0$. In fact, as the set of pairs (γ, δ) that make $\det(\mathcal{T}_{d+1})$ zero is a line, after three attempts we are guaranteed to find an acceptable value (for example, we try $(0,0)$, then $(0,1)$ and if, with both values, the determinant is zero, we can then use $(1,0)$ as a good coefficient).

Before we describe the algorithm for fast inversion of a Toeplitz matrix, we have to make some important remarks.

First, the polynomials U_{d-1} and V_{d-1} defined by:

$$X^{d-1}S_d = U_{d-1}(X^{2d-1}+1) + V_{d-1}T_{\gamma,\delta}, \quad (\ddagger)$$

are obtained from **FSSR** applied to $X^{2d+1}+1$ and $T_{\gamma,\delta}$ with $r = d+2$. As $S_d(0) \neq 0$, if $\deg S_d = d+1$, there exists k_ℓ such that $k_\ell = d$. We can then compute M_d. The coefficients on the second line of this matrix, M_d, are exactly U_{d-1} and V_{d-1}, as we can see from the proof of Proposition 5.

Otherwise, if $\deg S_d < d+1$, we observe that for the biggest ℓ such that $k_\ell < d$ we have the pair $(S_{k_\ell}, S_{k_\ell}+1)$ right-defective (indeed Theorem 3 shows that all other situations lead to $S_k(0) = 0$ for $k_\ell < k < k_{\ell+1}$). We know that in this case $S_{k_\ell}+1$ and S_d are proportional ; the coefficient of proportionality is given by Theorem 3. From **FSSR** we obtain only :

$$X^{k_\ell}S_{k_\ell+1} = U_{k_\ell}(X^{2d-1}+1) + V_{k_\ell}T_{\gamma,\delta},$$

Multiplication by the right coefficient provides formula (‡).

Furthermore, whatever the situation might be, in this call to **FSSR**, γ and δ do not occur because we use a truncation to the order $d-1$.

This provides the first column of $\mathcal{T}_d^{-1}$. The same computation applied to $X^{2d-1}+1$ and $\bar{S}_0^*$ gives the last column.

Next, we do not need any extra call to **FSSR** when we test, for example, $(\gamma, \delta) = (0,0)$, $(1,0)$ or $(0,1)$. The computations are different only for the last step, the transition from S_d to S_{d+1}, and we do not need to begin again the computation from S_{-1} and S_0. This is the first advantage of our **FITM** algorithm over the one in [2]. A second advantage is that it is fraction-free.

Finally we can rewrite our result in a TOEPLITZ-Bezoutian form. If (U,V) is a pair of polynomials of degree at most d such that

$$X^d S_{d+1}(S_{-1}, S_0) = (X^{2d+1}+1)V + UP,$$

and if (u,v) is a pair of polynomials of degree at most d such that

$$X^d S_{d+1}(S_{-1}, S_0^*) = (X^{2d+1}+1)v + uP,$$

then, in the non-degenerative situation, we have :

$$Bez(U^*, u)T_d(S_{-1}, S_0) = S_d(0)S_{d+1}(0)I_d$$

where I_d is the identity matrix of order d. (It comes from a well-known matrix representation of Bezoutian - see [3], p.156.)

There are certainly relations between our computations and those proposed by GEMIGNIANI in [13] and [14]. Bezoutians are used instead of symmetric sub-resultants. But, these algorithms start with quite the same polynomials. In the literature one finds several links between resultants and Bezoutians (see for example [20]). However, in our particular case, the relation between these two methods is not easy to describe and will be the object of future work.

Of course, all that we have said in this sub-section can be simplified in the case of a Hermitian TOEPLITZ matrix. It has been described in detail in [4].

We can now summarize our results in the **FITM** algorithm for fast inversion of a TOEPLITZ matrix.

6 Conclusion

We have generalized the concepts introduced for the improvement of the SCHUR-COHN algorithm. The sequence of sub-resultants defined for a pair (P, P^*) can now be computed for a general pair of polynomials and the fast algorithm designed in the previous situation has been extended.

```
ALGORITHM FITM

INPUT :          $\mathcal{T}_d = (t_{i-j})_{0 \le i,j \le d-1}$, a TOEPLITZ matrix of dimension $d$
OUTPUT :         $\mathcal{T}_d^{-1}$ if $\mathcal{T}_d$ is invertible and, if not, a message that $\mathcal{T}_d$ is not invertible

INITIALISATION   – $S_{-1} = X^{2d+1} + 1$
                 – $S_0 = T_{0,0} = -t - t_{-1}X - \cdots - t_{-d+1}X^{d-1} + t_{d-1}X^{d+2} + \cdots + tX^{2d+1}$,
MAIN PART :      – FSSR$(S_{-1}, S_0, d+2)$
                         % we get $M_{k_l}$ with
                         % $k_l$ the largest index such that $k_l \le d$.
                 – if $k_l = d$ and $S_{k_l}(0) = 0$ or if $k_l < d$, and $S_{k_l+1}(0) = 0$,
                         $\mathcal{T}_d$ is not invertible. STOP
                 – compute $V_{d-1}$ from $M_{k_l}$ and possible use of Theorem 3
                 – FSSR$(S_{-1}, \bar{S}_0^*, d+2)$
                         % we get $\widetilde{S}_{\widetilde{k_l}}, \widetilde{U}_{k_l-1}, \widetilde{V}_{k_l-1}$ with
                         % $\widetilde{k_l}$ the largest index such that $\widetilde{k_l} \le d$.
                 – compute $\widetilde{V}_{d-1}$ from $\widetilde{M_{k_l}}$ and possible use of Theorem 3
                 – If $\deg V_{d-1} = d-1$, then $\mathcal{T}_d^{-1}$ is computed via formula (*)
                 – If $\deg \widetilde{V}_{d-1} = d-1$, then $(\mathcal{T}_d^t)^{-1}$ is computed via formula (*)
                 – If $\deg V_{d-1} < d-1$ and $\deg \widetilde{V}_{d-1} < d-1$, compute $S_{d+1}$ using $M_{k_l}$.
                 – If $S_{d+1}(0) \neq 0$, then $\mathcal{T}_d^{-1}$ is computed via formula (**)
                 – otherwise redo the computation of $S_{d+1}$ with $T_{0,1}$ or with $T_{1,0}$.
                         % one of them will give $S_{d+1}(0) \neq 0$.
END.
```

The effectiveness of the algorithms presented has been studied in [4] where they have been effectively programmed in TP language, using the DFT. It has been shown that the bounds are effective and that, for polynomials of degrees greater than 300 and coefficients bounded by 2^{32}, these algorithms are faster than their counterpart programmed without DFT.

Of course, the fast version of the SCHUR-COHN algorithm has not changed, but we can present applications to TOEPLITZ matrices which are new. It would be an interesting study to compare the different algorithms for the inversion of TOEPLITZ matrices and to explore the links between them.

References

[1] BECKERMANN B., LABAHN G. (2000), *Fraction-Free Computation of Matrix Rational Interpolants and Matrix GCD.* Siam J. Matrix Anal. Appl., vol. 22, 1, p. 114-144.

[2] BRENT R., GUSTAVSON F., YUN D. (1980), *Fast Solution of Toeplitz Systems of Equations and Computation of Padé Approximants.* Journal of Algorithms. 1, 259-295.

[3] BINI D., PAN V. (1994), *Polynomial and Matrix Computations.* Birkhauser.

[4] BRUNIE C. (2001), *Etude et preuve de la faisabilité de l'apporche combinée fractions continues/sous-résultants symétriques, implantation sur la machine de Turing TP de Schönhage et application.* PhD Thesis, LACO, Université de Limoges. Birkhauser.

[5] BRUNIE C. AND SAUX PICART PH. (2000), *A fast version of the* SCHUR-COHN *algorithm* . Journal of Complexity, vol. 16, 1, 54-69.

[6] BASU S., POLLACK R., ROY M.-F. (2003), *Algorithm in Real Algebraic Geometry.* Springer.

[7] COHN A. (1922)*Über die Anzahl des Wurzlen einer algebraischen Gleischung in einem Kreise.* Math. Z., 14.

[8] COLLINS G. E. (1967), *Subresultants and Reduced Polynomial Remainder Sequences.* J.A.C.M. 14, 128–142.

[9] DEMEURE C. J., MULLIS, C. T. (1990), *A Newton-Raphson Method for Moving-Average Spectral Factorisation Using the Euclid Algorithm.* IEEE trans. on Acoustic, Speech and Signal, vol. 38, 1697-1709.

[10] FUJIWARA M. (1926), *Über die algebraischen Gleichungen, deren Wurzeln in einem Kreise oder in einer Halbebene liegen.* Math. Z., 24 .

[11] GEDDES K. O., CZAPOR S.R., LABAHN G. (1995), *Algorithms for Computer Algebra.* Kluwer Academic Press.

[12] GEMIGNANI L. (1991), *Computing the Inertia of Bezout and Hankel Matrices*, Calcolo, vol. 28, 267-274.

[13] GEMIGNANI L. (1992), *Fast Inversion of Hankel and Toeplitz Matrices*, Information Process Letter, vol. 41, 119-123.

[14] GEMIGNANI L. (1994), *Solving Hankel Systems over the integers*, J. Symb. Comp., vol. 18, 573-584.

[15] GOHBERG I. C. , SEMENCUL A. (1972), *On the inversion of finite* TOEPLITZ *matrices and their continuous analogs*, Math. Issled, vol. 2, 201-233.

[16] GOHBERG I. C., N. KRUPNIK K. (1972), *A formula for the inversion of finite* TOEPLITZ *matrices*, Math. Issled, vol. 7, 272-283.

[17] HENRICI P. (1974), *Applied and Computational Complex Analysis*, Vol. 1. New York, Wileys.

[18] IOHVIDOV I. S. (1982), *Hankel and Toeplitz Matrices and Forms : Algebraic Theory.* Boston, MA, Birkhauser.

[19] JEZEK J. (1983), *Conjugated and Symmetric Polynomial Equations.* Kibernetika, vol. 19, 196-211.

[20] KREIN M. G., NAIMARK M. A.(1981) , *Methods of symmetric and Hermitian forms in the theory of separation of the roots of algebraic equations*, Lin. Mult. Alg., vol. 10.

[21] LAUER D. (2000), *Effiziente Algorithmen zur Berechnung von Resultanten und Subresultanten,* Dissertation, Univ. Bonn, Informatik, Shaker Verlag.

[22] LICKTEIG T. ,ROY M.-F. (1996), *Cauchy index computation.* Calcolo,vol. 33, 337-351.

[23] LICKTEIG T., ROY M.-F. (2001), *Sylvester-Habicht sequences and fast Cauchy index computation.*,J. Symb. Comp. 31, 3, 315-341.

[24] LOMBARDI H., ROY M.-F., SAFEY EL DIN M.*New Structure Theorem for Subresultants* J. Symb. Comp. 29, 663-690.

[25] MARDEN M. (1966), *Geometry of Polynomials,* Providence, RI, American Mathematical Society.

[26] MOENCK R. T. (1973), *Fast computation of GCDs.* Proc. STOC'73, 142–151.

[27] REISCHERT D. (1997), *Asymptotically fast computation of resultants.* ISSAC'97 Hawai, 233-240, ACM Press.

[28] SCHUR I. (1918)*Über Potenzreihen, die im Innern des Einheitskreises beschraenkt sind,* J. Reine Angew. Math., 148.

[29] SCHÖNHAGE A. (1971)*Schnelle Berechnung von Kettenbruchentwicklungen,* Acta Informatica 1, 139-144.

[30] SCHÖNHAGE A., STRASSEN V. (1971)*Schnelle Multiplikation grosser Zahlen,* Computing 7, 281-292.

[31] SIEVEKING M. (1972) *An Algorithm for Division of Power Series.* Computing, vol. 10, 153-156.

[32] SENDRA R., LLOVET J. (1990), *Hankel Matrices and Computer Algebra.* ACM SIGSAM Bulletin vol. 34, 17-26 ISSAC'97 Hawai, 233-240, ACM Press.

[33] SAUX-PICART PH. (1998), *The Schur-Cohn Algorithm revisited* J. Symb. Comp. : 26, no. 4, 387–408.

[34] STRASSEN V. (1983), *The Computational Complexity of Continued Fractions.* SIAM J. Comp., vol. 12/1, 1–27.