J. Symbolic Computation (2001) **31**, 315–341
doi:10.1006/jsco.2000.0427
Available online at http://www.idealibrary.com on IDEAL®

Sylvester–Habicht Sequences and Fast Cauchy Index Computation

THOMAS LICKTEIG[†§] AND MARIE-FRANÇOISE ROY[‡¶]

[†] *Département de Mathématiques, Université de Limoges, 87060 Limoges Cedex, France,*
[‡] *Université de Rennes, Campus de Beaulieu, 35042 Rennes Cedex, France*

In this paper we show how Schönhage's strategy for computing continued fractions Schönhage (1971) can be combined with the theory of sub-resultants (Habicht, 1948; Collins, 1967; Brown, 1971; Brown and Traub, 1971; Loos, 1982; Gonzalez *et al.*, 1990, 1994; Ducos, 1996; Ho and Yap, 1996; Lazard, 1998; Quitté, 1998) in order to compute the Cauchy index of a rational function or the signature of a non-singular Hankel matrix in a fast and also storage efficient way. Over the integers our algorithms have bit complexity $O(\mathcal{M}(d,\sigma)\cdot\log(d))$ with $\sigma = O(d\tau)$ where $\mathcal{M}(d,\sigma) = O(d\sigma\cdot\log(d\sigma)\cdot\log\log(d\sigma))$ is Schönhage's bound for multiplication of integer polynomials of degrees bounded by d and bit size bounded by σ in the multi-tape Turing machine model (Schönhage, 1982). Thus our bound is

$$O(d^2\tau\cdot\log(d\tau)\cdot\log\log(d\tau)\cdot\log(d)).$$

As a byproduct of the necessary analysis we obtain a refinement of the Sub-resultant Theorem. We present a new exact divisibility for sub-resultants in the defective case which extends the formulæ for the non-defective situation in a natural way. We also prove that the size of coefficients in the ordinary remainder sequence is quadratic in d.

1. Introduction

Computing the Cauchy index of a rational function B/A between two numbers a and b is fundamental in most of the basic algorithms of real algebraic geometry: real root counting, exact sign determination, Routh–Hurwitz problem, signature of a Hankel matrix.

One way to compute the Cauchy index of B/A between a and b is to compute some variant of the Euclidean remainder sequence of A and B and to compute the signs of the successive remainders evaluated at a and b (Sturm, 1835; Sylvester, 1853; Roy, 1996). Thus, we want to compute efficiently the signs of the polynomials in the Euclidean remainder sequence evaluated at a given point.

In this paper we use the fact that it is enough to know the quotients and GCD to be able to evaluate the Euclidean remainder sequence at a given point. In order to compute the quotients and GCD efficiently, without computing all remainders, we "dance" in big steps through the remainder sequence. The choreography of this "ballet" has been given in Schönhage's (1971) paper on computing continued fractions of rational numbers and has been adapted by Moenck (1973) in a special case and by Brent *et al.* (1980) in the

[§]Supported in part by DFG Heisenberg Grant Li-405/2-2.
[¶]Supported in part by the project ESPRIT-LTR 21.024 FRISCO and by European Community contract CHRX-CT94-050.

0747–7171/01/030315 + 27 $35.00/0

general case (see also, Thull and Yap, 1990 and Yap, 1999) to the computation of GCDs of univariate polynomials.

After recalling the Cauchy index in Section 2, we describe in Section 3 how one can compute the Cauchy index and the signature of a non-singular Hankel matrix efficiently. We only count the number of field operations and comparisons. For input polynomials of degrees bounded by d we design an algorithm with complexity $O(\mathcal{M}(d) \cdot \log(d))$ for computing the Cauchy index; here $\mathcal{M}(d)$ denotes the cost of multiplying polynomials of degree at most d. One has $\mathcal{M}(d) = O(d \log(d))$ if the coefficient field allows Fourier transform, and $\mathcal{M}(d) = O(d \log(d) \log\log(d))$ otherwise (cf. Schönhage and Strassen, 1971). (Throughout we tacitly assume d to be sufficiently large in order to have the expressions in the "big O" notation defined and positive.)

The problem we consider later is to compute the Cauchy index with the same complexity in terms of arithmetic operations as above, but with a better control of the bit complexity.

This is done through the study of the Sylvester–Habicht sequence. In Section 4 we improve the Structure Theorem on the Sylvester–Habicht sequence

$$H_d = H_d(A, B), \ldots, H_0 = H_0(A, B)$$

of a couple of polynomials (A, B) of degrees $d = \deg A > \deg B \geq 0$, which is a signed variant of the well-known Sub-resultant Theorem (cf. Habicht, 1948; Collins, 1967; Brown, 1971; Brown and Traub, 1971; Loos, 1982; Gonzalez *et al.*, 1990; Ducos, 1996; Lazard, 1998; Quitté, 1998). The introduction of sub-resultants as a computational method is due to Collins (1967). (In order to avoid specialization problems appearing in Loos (1982), we consider always the Sylvester–Habicht polynomials $H_j = H_j(A, B) = H_j(A, d; B; d-1)$ (cf. Gonzalez *et al.*, 1990, 1994, 1998), see also Ho and Yap (1996) with respect to the degree pattern $(d, d-1)$ and omit this notationally.) We present a new exact divisibility for consecutive Sylvester–Habicht polynomials H_j and H_{j-1} in the case of a defective H_{j-1} of degree $k < j-1$. The new exact divisibility is a consequence (Corollary 4.3) of our studies of the Sylvester–Habicht transition matrices at the end of Section 4. These transition matrices will take over the algorithmic role of the successive quotients in Schönhage (1971).

Section 5 presents our main results on computing the Cauchy index via the Sylvester–Habicht transition matrices. For integer input polynomials of bit size bounded by τ we design an algorithm with bit complexity $O(\mathcal{M}(d, \sigma) \cdot \log(d))$ with $\sigma = O(d\tau)$ where $\mathcal{M}(d, \sigma) = O(d\sigma \cdot \log(d\sigma) \cdot \log\log(d\sigma))$ is Schönhage's bound for multiplication of integer polynomials of degrees bounded by d and bit size bounded by σ in the multi-tape Turing machine model (cf. Schönhage, 1982). Thus our bound is $O(d^2\tau \cdot \log(d\tau) \cdot \log\log(d\tau) \cdot \log(d))$. We remark that even when usual polynomial multiplication is used the algorithm is still superior to traditional ones with respect to storage requirements. This is particularly important in parametric situations when the coefficients are polynomials in other variables.

We prove that the same complexity bound is valid for the computation of the signature of a non-singular Hankel matrix as well (Corollary 5.3, improving on Gemignani, 1991 and 1994). This is obtained through a combination with a classical sign rule for the successive principal minors of a *Hankel* matrix due to Jacobi (cf. Gantmacher, 1966, Chapter 10) which gives the signature of the Hankel matrix without any assumption on the non-vanishing of these minors.

Finally, in Section 6 we study the factors of proportionality between the polynomials

of the remainder sequence and the Sylvester–Habicht polynomials. These factors come from the successive Sylvester–Habicht transition matrices and are well-defined quotients of products of $O(d)$ minors of the Sylvester matrix. In particular, they show for integer polynomials of bit size bounded by τ that the coefficients of the remainders possess numerator-denominator representations of bit size $O(\tau d^2)$. Therefore the standard Euclidean algorithm does not produce an exponential "coefficient swell," *a priori* a possible behavior which, up to now, could not definitely be ruled out.

An extended abstract of most of the results presented here already appears in Lickteig and Roy (1996), see also Reischert (1997).

2. The Cauchy Index

We first recall the definition of the Cauchy index, give some of its applications, and explain how it can be computed from the Euclidean remainder sequence.

We consider two non-zero univariate polynomials A and B with coefficients in an ordered field K. Let R be a real closed extension field inducing the ordering on K. Let $a < b$ be elements in $\mathrm{R} \cup \{-\infty, +\infty\}$. The Cauchy index $I(B/A;]a, b[)$ of B/A between a and b is by definition the number of jumps of the function B/A from $-\infty$ to $+\infty$ minus the number of jumps of B/A from $+\infty$ to $-\infty$ on the open interval $]a, b[$.

As particular cases of the Cauchy index we have the following (see Roy, 1996).

PROPOSITION 2.1. *Let $a < b$ be elements in $\mathrm{R} \cup \{-\infty, +\infty\}$ that are not roots of A.*

$I(A'/A;]a, b[)$ is the number of roots of A in $]a, b[$.
$I(A'B/A;]a, b[)$ is the difference between the number of roots of A in $]a, b[$ where B is positive and the number of roots of A in $]a, b[$ where B is negative.

The Cauchy index also plays a role for counting the number of roots of polynomials in half planes of $\mathrm{C} = \mathrm{R}(i)$ (cf. Henrici, 1970, 1974).

THEOREM 2.1. (CF. HENRICI, 1974) *Let $P = A + iB \in \mathrm{C}[X]$ be a polynomial of degree n with positive leading coefficient in R with k roots in R (counted with multiplicity). Then the number m of zeros of P in the open upper half plane is given by*

$$m = \frac{1}{2}(n - k - I(B/A;]-\infty, +\infty[)).$$

The computation of the Cauchy index can be used as well for computing the number of complex roots of a real univariate polynomial in the complex half plane where the real part is strictly negative (see Gantmacher, 1966; Henrici, 1970). This is the Routh–Hurwitz problem and can be reduced to counting zeros in the upper half plane by a simple homography. The same remark applies to counting zeros in open disks.

The Cauchy index of a rational function and the signature of a Hankel matrix are related as follows. To a sequence $h = (h_0, \ldots, h_{2d-1}) \in \mathrm{K}^{2d}$ one can associate a $d \times d$ Hankel matrix

$$\mathrm{Han}_d(h) = (h_{i+j-2}) = \begin{pmatrix} h_0 & h_1 & \iddots & \iddots & h_{d-1} \\ h_1 & \iddots & \iddots & h_{d-1} & h_d \\ \iddots & \iddots & \iddots & \iddots & \iddots \\ \iddots & h_{d-1} & \iddots & \iddots & h_{2d-3} \\ h_{d-1} & h_d & \iddots & h_{2d-3} & h_{2d-2} \end{pmatrix}.$$

The following results are classical (see, e.g., Frobenius, 1884; Krein and Naimark, 1936; Gantmacher, 1966; Roy, 1996; Henrici, 1974; Knebusch and Scheiderer, 1989).

THEOREM 2.2. *Let* $\sum_{k=0}^{\infty} h_k T^{k+1} \in \mathrm{K}[[T]]$ *be a formal power series. Then there exists a couple of polynomials* $A, B \in \mathrm{K}[X]$ *with* $\deg B < \deg A$ *such that*

$$\frac{B}{A} = \sum_{k=0}^{\infty} \frac{h_k}{X^{k+1}}$$

if and only if there is a number $d \in \mathbb{N}$ *such that the ranks of all the Hankel matrices* $\mathrm{Han}_d(h), \mathrm{Han}_{d+1}(h), \mathrm{Han}_{d+2}(h), \ldots$ *associated to the initial segments of the coefficient list are all equal to* d.

This condition on the ranks is equivalent to saying that

$$\det \mathrm{Han}_d(h) \neq 0, \qquad 0 = \det \mathrm{Han}_{d+1}(h) = \det \mathrm{Han}_{d+2}(h) = \cdots.$$

If it is satisfied, then there is an A *of degree* d *and a* B *of degree at most* $d-1$ *with the above representation. The minimal possible degree of the denominator polynomial* A *is* d, *and the couple* (A, B) *is uniquely determined by these degree requirements and the condition that* A *is monic. The polynomials* A *and* B *are then relatively prime.*

Conversely, if A *and* B *are relatively prime and* $\deg A = d > \deg B$, *then the rank of the Hankel matrix* $\mathrm{Han}_d(h)$ *associated to the rational function* B/A *through the above power series expansion is* d, *and the signature of* $\mathrm{Han}_d(h)$ *coincides with the global Cauchy index* $I(B/A;]-\infty, +\infty[)$ *of* B/A.

We are now going to define for two univariate polynomials A and B with coefficients in a field K such that $d \geq \deg A \geq \deg B \geq 0$ the sequence of *signed remainders* of A and B; the difference with the sequence of remainders comes from a change of signs.

The *quotient* $\mathrm{Quo}\,(A, B)$ and the *remainder* $\mathrm{Rem}\,(A, B)$ of two polynomials A and B are the uniquely determined polynomials of degrees $\deg \mathrm{Quo}\,(A, B) = \deg A - \deg B$ and $\deg \mathrm{Rem}\,(A, B) < \deg B$ such that

$$A = \mathrm{Quo}\,(A, B) \cdot B + \mathrm{Rem}\,(A, B).$$

The signed remainder sequence of (A, B) is the list

$$R_0 = R_0(A, B), R_1 = R_1(A, B), \ldots, R_w = R_w(A, B)$$

(where $w = w(A, B)$ also depends on (A, B)) defined by

$$\begin{aligned} R_0 &= A \\ R_1 &= B \\ R_2 &= -\mathrm{Rem}\,(R_0, R_1) \\ &\vdots \\ R_{i+1} &= -\mathrm{Rem}\,(R_{i-1}, R_i) \\ &\vdots \\ R_{w+1} &= -\mathrm{Rem}\,(R_{w-1}, R_w) = 0. \end{aligned}$$

The *quotient sequence of* (A, B) is the list

$$Q_0 = Q_0(A, B), \ldots, Q_{w-1} = Q_{w-1}(A, B)$$

defined by

$$\begin{aligned} Q_0 &= \mathrm{Quo}\,(R_0, R_1) \\ Q_1 &= \mathrm{Quo}\,(R_1, R_2) \\ &\vdots \\ Q_{w-1} &= \mathrm{Quo}\,(R_{w-1}, R_w). \end{aligned}$$

REMARK 2.1. When there will be no ambiguity, we simply write R_i, Q_i, etc.

Note that R_w is a GCD of A and B. Denoting by d_i the degree of R_i we have $\deg Q_i = d_i - d_{i+1}$, and $d_{i+1} < d_i$ for $i > 0$.

We remark that when $B = A'$, the signed remainder sequence is nothing but the Sturm sequence.

The number of *sign changes* $V([a_0, \ldots, a_n])$ in a list $[a_0, \ldots, a_n]$ of elements in $\mathrm{R} \setminus \{0\}$ is defined recursively, starting with $V([a_0]) = 0$, by

$$V([a_0, \ldots, a_{n+1}]) = \begin{cases} V([a_0, \ldots, a_n]) + 1 & \text{if } \operatorname{sign}(a_n a_{n+1}) = -1 \\ V([a_0, \ldots, a_n]) & \text{otherwise.} \end{cases}$$

This definition extends to any sequence of elements in R by dropping zeros into the considered sequence.

We denote by $V(a) = V(A, B; a)$ the *number of sign changes of the signed remainder sequence* of (A, B) at a.

The following theorem indicates how to compute the Cauchy index from the sequence of signed remainders.

THEOREM 2.3. (CF. ROY, 1996) *Let* K *be an ordered field and* R *a real closed extension field inducing the ordering on* K. *If* A *and* B *are two polynomials with coefficients in* K, $\deg A \geq \deg B$, *and* $a < b$ *are elements of* $\mathrm{R} \cup \{-\infty, +\infty\}$ *that are not roots of* A, *then*

$$I(B/A;]a, b[) = V(a) - V(b).$$

3. The Quotient Boot

Let K be a field. We are going to describe an algorithm taking as input a pair (A, B) of polynomials in $\mathrm{K}[X]$ together with an element $a \in \mathrm{K}$ and outputting the list

$$(R_0(a), \ldots, R_w(a))$$

of values of the signed remainders; the input polynomials are assumed to satisfy $d \geq \deg A \geq \deg B \geq 0$. The number of arithmetic operations and comparisons performed by the algorithm will be $O(\mathcal{M}(d) \log(d))$ where $\mathcal{M}(d)$ denotes the cost of multiplying two polynomials of degree no greater than d. This algorithm is a modification of the algorithm of Schönhage (1971) for integers as adapted in Moenck (1973) and Brent *et al.* (1980) for univariate polynomials.

Since the number of coefficients appearing in the complete remainder sequence is of order d^2, the algorithm will not output (or store) all this information. Following Schönhage (1971), Moenck (1973) and Brent *et al.* (1980), we note that the total number of coefficients appearing in the list of quotients and the last signed remainder polynomial $R_w(A,B)$ (a GCD of A and B) is only of order $O(d)$ rather than $O(d^2)$. The list

$$(Q_0(A,B),\ldots,Q_{w-1}(A,B),R_w(A,B))$$

is called the *quotient boot* of (A,B) because of its boot shape in the successive signed Euclidean division scheme.

The following remark is important in what follows.

REMARK 3.1. (STRASSEN, 1983) From the quotient boot of (A,B) and a value $a \in \mathrm{K}$ it is easy to recover the values of the signed remainder sequence at a. Indeed we have

$$\begin{pmatrix} R_1 \\ R_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & Q_0 \end{pmatrix} \cdot \begin{pmatrix} R_0 \\ R_1 \end{pmatrix},$$

and generally for $i = 1,\ldots,w$,

$$\begin{pmatrix} R_i \\ R_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & Q_{i-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ -1 & Q_0 \end{pmatrix} \cdot \begin{pmatrix} R_0 \\ R_1 \end{pmatrix}.$$

Therefore, inverting the unimodular 2×2 matrices, the evaluation in a of the polynomials of the signed remainder sequence from the quotient boot can be done according to the following Horner-like scheme requiring $O(d)$ arithmetic operations at most.

$$\begin{aligned}
\begin{pmatrix} R_{w-1}(a) \\ R_w(a) \end{pmatrix} &= \begin{pmatrix} Q_{w-1}(a) & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} R_w(a) \\ 0 \end{pmatrix} \\
\begin{pmatrix} R_{w-2}(a) \\ R_{w-1}(a) \end{pmatrix} &= \begin{pmatrix} Q_{w-2}(a) & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} R_{w-1}(a) \\ R_w(a) \end{pmatrix} \\
&\vdots \\
\begin{pmatrix} R_1(a) \\ R_2(a) \end{pmatrix} &= \begin{pmatrix} Q_1(a) & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} R_2(a) \\ R_3(a) \end{pmatrix} \\
\begin{pmatrix} R_0(a) \\ R_1(a) \end{pmatrix} &= \begin{pmatrix} Q_0(a) & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} R_1(a) \\ R_2(a) \end{pmatrix}.
\end{aligned}$$

Passing to leading coefficients, the same procedure works for $a \in \{-\infty,+\infty\}$ and the sign determination of the $R_i(a)$ as well.

We denote by $M_i = M_i(A,B) \in \mathrm{K}[X]^{2\times 2}$ the matrix product

$$M_i = \begin{pmatrix} 0 & 1 \\ -1 & Q_{i-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ -1 & Q_0 \end{pmatrix}$$

(with $M_0 = 2 \times 2$ identity matrix). Thus,

$$\begin{pmatrix} R_i \\ R_{i+1} \end{pmatrix} = M_i \cdot \begin{pmatrix} A \\ B \end{pmatrix}.$$

Defining the polynomials $K_{i-1}, L_{i-1}, K_i, L_i$ as the entries of this unimodular *signed*

Euclidean transition matrix

$$M_i(A,B) = \begin{pmatrix} K_{i-1} & L_{i-1} \\ K_i & L_i \end{pmatrix},$$

we have the following fact.

LEMMA 3.1. *If $i \geq 1$, then*

$$\deg K_i = d_1 - d_i$$

(where $d_i = \deg R_i$); if $i \geq 0$, then

$$\deg L_i = d_0 - d_i, \qquad \deg K_i \leq d_0 - d_i.$$

PROOF. By induction on i. □

Now we are going to examine the following idea from Schönhage (1971) which is fundamental in the algorithm: an initial segment of the quotients (if it is not too long) does not depend on the tail segment of the coefficient lists of the polynomials $A = R_0(A,B)$ and $B = R_1(A,B)$, but only on an initial segment of these.

We now assume that $d \geq d_0 = \deg A \geq d_1 = \deg B \geq 0$ and define for a number ℓ such that $0 \leq \ell \leq d$ a *target number* $r = r(d,\ell,A,B)$ as follows:

if $\ell \geq \deg B$, $r := 0$,
if $\ell < \deg B$, r is determined by the condition $\deg R_{r+1}(A,B) > \ell \geq \deg R_{r+2}(A,B)$.

In other words, r is the number of Euclidean divisions to be performed such that after the next division the degree of the next remainder will become smaller than or equal to ℓ.

We now consider a further number m such that $d \geq m \geq 0$ and a further couple of polynomials $\tilde{A}$ and $\tilde{B}$ such that $\deg(A - \tilde{A}) \leq m$ and $\deg(B - \tilde{B}) \leq m$. Define for $i = 0, \ldots, r$ polynomials $\tilde{R}_i$ and $\tilde{R}_{i+1}$ by

$$\begin{pmatrix} \tilde{R}_i \\ \tilde{R}_{i+1} \end{pmatrix} = M_i(A,B) \cdot \begin{pmatrix} \tilde{A} \\ \tilde{B} \end{pmatrix}.$$

LEMMA 3.2. *If $r = r(d,\ell,A,B) > 0$, then for $i = 0, \ldots, r$,*

$$\deg(\tilde{R}_{i+1} - R_{i+1}) \leq d_0 - d_i + m < d - \ell + m.$$

PROOF. By Lemma 3.1 and the definition of $r = r(d,\ell,A,B)$. □

PROPOSITION 3.1. *Let $\deg(A - \tilde{A}) \leq m$ and $\deg(B - \tilde{B}) \leq m$. Assume that $r = r(d,\ell,A,B)$, and moreover $d - \ell + m \leq \ell$. Then $r = r(d,\ell,\tilde{A},\tilde{B})$, and equivalently*

$$Q_{i-1}(A,B) = Q_{i-1}(\tilde{A},\tilde{B}) \qquad \text{for } i = 1, \ldots, r,$$

and

$$M_i(A,B) = M_i(\tilde{A},\tilde{B}) \qquad \text{for } i = 1, \ldots, r.$$

PROOF. In a signed Euclidean division $f = q \cdot g - r$ of a polynomial f of degree d' and a polynomial g of degree $d'' \leq d'$ the coefficients of the quotient q are completely determined by the $d' - d'' + 1$ top terms of f and of g. This observation shows that the initial of quotients of (A, B) and of $(\tilde{A}, \tilde{B})$ coincide under the assumptions made. □

We now define the task $\mathcal{T}(d, \ell)$ for $d \geq \ell \geq 0$.

Input: a couple (A, B) of polynomials with $d \geq \deg A \geq \deg B \geq 0$.
Output: the list $(Q_0, \ldots, Q_{r-1}; M_r; R_r, R_{r+1})$ with $r = r(d, \ell, A, B)$.

REMARK 3.2. The outputs of the $\mathcal{T}(d, \ell)$ are "intermediate boots", where computation of the transition matrix M_r is included. The computation of the quotients and the transition matrix can be considered as the computation of the transition matrix and its factorization into the elementary matrices corresponding to the quotients.

Once $\mathcal{T}(d, \ell)$ is solved, one further signed Euclidean division of the consecutive couple of remainders R_r and R_{r+1} (with $r = r(d, \ell, A, B)$) gives the next remainder R_{r+2}. This gives rise to an additional cost of order $\mathcal{M}(d)$ only. Thus for $\ell = 0$, the output of $\mathcal{T}(d, 0)$ easily gives the quotient boot.

We are going to consider a divide and conquer strategy for the task family $\mathcal{T}$ based on the fact that the initial quotients depend only on the top terms of the pair of polynomials given (cf. Proposition 3.1).

We denote by $\mathcal{C}(d, \ell)$ the (worst case) cost of $\mathcal{T}(d, \ell)$ and by $\mathcal{M}(d)$ the cost of the multiplication of two polynomials of degree at most d. A signed Euclidean division of polynomials of degree at most d can also be performed with $O(\mathcal{M}(d))$ steps (cf. Sieveking, 1972; Kung, 1974).

We have the following lemmas.

LEMMA 3.3. *For $d \geq \ell \geq \ell' \geq 0$,*

$$\mathcal{C}(d, \ell') = \mathcal{C}(d, \ell) + \mathcal{C}(\ell, \ell') + O(\mathcal{M}(d)).$$

PROOF. For a given couple (A, B) of polynomials, one first solves $\mathcal{T}(d, \ell)$ for this couple. Now one performs with cost $O(\mathcal{M}(d))$ one signed Euclidean division

$$R_r = Q_r \cdot R_{r+1} - R_{r+2}$$

with $r = r(d, \ell, A, B)$. Let $r' = r(d, \ell', A, B)$. An inspection of the degree of R_{r+2} allows us to decide whether $r' > r$. If $r' = r$ then $\mathcal{T}(d, \ell')$ is already solved for (A, B). If $r' > r$ happens to be the case then $R_{r+2} \neq 0$, and one adds the quotient Q_r to the list of quotients already computed, computes the matrix product

$$M_{r+1} = \begin{pmatrix} 0 & 1 \\ -1 & Q_r \end{pmatrix} \cdot M_r$$

with additional cost $O(\mathcal{M}(d))$, and one performs a further signed Euclidean division

$$R_{r+1} = Q_{r+1} \cdot R_{r+2} - R_{r+3}$$

with cost $O(\mathcal{M}(d))$. An inspection of the degree of R_{r+3} allows us to decide whether

$r' > r+1$. If $r' = r+1$ then $\mathcal{T}(d, \ell')$ is already solved for (A, B). If $r' > r+1$ happens to be the case then $R_{r+3} \neq 0$, and one adds the quotient Q_{r+1} to the list of quotients already computed, and computes the second matrix product

$$M_{r+2} = \begin{pmatrix} 0 & 1 \\ -1 & Q_{r+1} \end{pmatrix} \cdot M_{r+1},$$

again with additional cost $O(\mathcal{M}(d))$. Then, in a second round, one solves the task $\mathcal{T}(\ell, \ell')$ for the couple (R_{r+2}, R_{r+3}) getting the rest of the quotients and the transition matrix

$$M_{r''}(R_{r+2}, R_{r+3})$$

with $r'' = r(\ell, \ell', R_{r+2}, R_{r+3})$. After that one obtains the transition matrix $M_{r'} = M_{r'}(A, B)$ as the product

$$M_{r'} = M_{r''}(R_{r+2}, R_{r+3}) \cdot M_{r+2}$$

again with additional cost $O(\mathcal{M}(d))$. □

Lemma 3.4. *For $a \geq 0$,*

$$\mathcal{C}(d+a, \ell+a) \geq \mathcal{C}(d, \ell).$$

Proof. Multiplying the polynomials A and B by X^a multiples the remainders by X^a and does not modify the quotients. □

In the same way one remarks the following.

Lemma 3.5. *$\mathcal{C}(d, \ell)$ coincides with the cost of the task $\mathcal{T}(d+a, \ell+a)$ restricted to input polynomials that are multiples of X^a.*

Lemma 3.6. *For $\ell \geq d/2$,*

$$\mathcal{C}(2d, \ell+d) \leq \mathcal{C}(d, \ell) + O(\mathcal{M}(2d)).$$

Proof. Define $d' = 2d$, $\ell' = \ell + d$, $m' = d'/2 = d$. Then since $d \leq 2\ell$, $d' - \ell' + m' \leq \ell'$, and we can apply Proposition 3.1 and Lemma 3.5. The matrix $M_r = M_r(A, B)$, with $r = r(d', \ell', A, B)$, already found for an input couple (A, B), one computes with an additional amount of $O(\mathcal{M}(2d))$ operations the product

$$\begin{pmatrix} R_r \\ R_{r+1} \end{pmatrix} = M_r \cdot \begin{pmatrix} A \\ B \end{pmatrix}$$

in order to obtain the correct remainders. □

The consequences are the following (assuming for the reason of technical simplification d to be a power of 2).

For the task $\mathcal{T}(d, d/2)$, writing $d = 4s$,

$$\mathcal{C}(4s, 2s) \leq \mathcal{C}(4s, 3s) + \mathcal{C}(3s, 2s) + O(\mathcal{M}(4s))$$

according to Lemma 3.3. Since

$$\mathcal{C}(4s, 3s) \leq \mathcal{C}(2s, s) + O(\mathcal{M}(4s))$$

according to Lemma 3.6, and

$$\mathcal{C}(3s, 2s) \leq \mathcal{C}(4s, 3s) \leq \mathcal{C}(2s, s) + O(\mathcal{M}(4s))$$

according to Lemmas 3.4 and 3.6, we find that

$$\mathcal{C}(4s, 2s) \leq 2\mathcal{C}(2s, s) + O(\mathcal{M}(4s)).$$

One has $\mathcal{M}(d) = O(d \log(d))$ if the field K contains a primitive dth root of unity (or if such a root of unity lies in a low degree extension field of K), and $\mathcal{M}(d) = O(d \log(d) \log\log(d))$ otherwise (cf. Schönhage and Strassen, 1971). Thus we obtain

$$\mathcal{C}(d, d/2) = O(\mathcal{M}(d) \log(d)).$$

For the task $\mathcal{T}(d, 0)$, writing $d = 2s$,

$$\mathcal{C}(2s, 0) \leq \mathcal{C}(2s, s) + \mathcal{C}(s, 0) + O(\mathcal{M}(2s))$$

according to Lemma 3.3, so that

$$\mathcal{C}(2s, 0) \leq \mathcal{C}(s, 0) + O(\mathcal{M}(2s) \log(2s)),$$

leading to the same bound

$$\mathcal{C}(d, 0) = O(\mathcal{M}(d) \log(d)).$$

Finally we have proved the following theorem.

THEOREM 3.1. (MOENCK, 1973) *The quotient boot of a couple of polynomials* (A, B) *with* $d \geq \deg A \geq \deg B \geq 0$ *can be computed with a total number of arithmetic operations and equality comparisons* $O(\mathcal{M}(d) \log(d))$.

With slight modifications, which are left to the reader, we have more generally.

PROPOSITION 3.2. *For every* d *and* ℓ, $0 \leq \ell \leq d$, *the task* $\mathcal{T}(d, \ell)$ *can be solved with a maximal number of arithmetic operations and equality comparisons* $O(\mathcal{M}(d) \log(d - \ell))$.

Using Remark 3.1 we immediately deduce the following two results.

THEOREM 3.2. (MOENCK, 1973; STRASSEN, 1983) *Given a couple of polynomials* (A, B) *with* $d \geq \deg A \geq \deg B \geq 0$ *together with a number* $a \in \mathrm{K}$, *the values of all polynomials of the signed remainder sequence of* (A, B) *in* $a \in K$ *can be computed with a total number of arithmetic operations and equality comparisons* $O(\mathcal{M}(d) \log(d))$.

When the field K is ordered, we obtain in linear time from the list of values of the signed remainder sequence the list of signs of the remainder sequence of A and B evaluated at a.

THEOREM 3.3. (MOENCK, 1973; STRASSEN, 1983) *Given a couple of polynomials* (A, B) *with* $d \geq \deg A \geq \deg B \geq 0$ *together with a couple* (a, b), $a < b$ *and* $a, b \in \mathrm{K} \cup \{-\infty, +\infty\}$ *both being no roots of* A, *the Cauchy index of* B/A *between* a *and* b *can be computed with* $O(\mathcal{M}(d) \log(d))$ *arithmetic operations and equality–inequality comparisons.*

REMARK 3.3. Except for some individual low order organizational overheads the above described algorithms essentially perform $O(\log(d))$ many multiplications of polynomials because their main recursion depth is of order $O(\log(d))$. Concerning bit complexity we shall follow a similar line in Section 5. However the bit complexity bounds will not be of the form "total number of arithmetic steps times maximal bit size". This is due to the fact that the best multiplication algorithm for integer polynomials (via a Kronecker type substitution; cf. Schönhage, 1982) does not follow such a pattern.

We end this section with an application to Hankel matrices.

THEOREM 3.4. *Given a list of numbers $h = (h_0, \ldots, h_{2d-1})$, the signature decision of the associated $d \times d$ Hankel matrix $\mathrm{Han}_d(h) = (h_{i+j-2})$ can be performed with maximally $O(\mathcal{M}(d)\log(d))$ arithmetic operations and equality–inequality comparisons, provided that the rank of $\mathrm{Han}_d(h)$ is d.*

PROOF. Consider the polynomials T^{2d} and $C = \sum_{k=0}^{2d-1} h_k T^k$.

We first consider the case when these are relatively prime, that is, when $h_0 \neq 0$. We solve task $\mathcal{T}(2d, d-1)$ for the couple (T^{2d}, C), apply one further signed Euclidean division, and find the transition matrix M_i and the two consecutive signed remainders R_i and R_{i+1} such that

$$\begin{pmatrix} R_i \\ R_{i+1} \end{pmatrix} = M_i \cdot \begin{pmatrix} T^{2d} \\ C \end{pmatrix} = \begin{pmatrix} K_{i-1} & L_{i-1} \\ K_i & L_i \end{pmatrix} \cdot \begin{pmatrix} T^{2d} \\ C \end{pmatrix},$$

and $\deg R_{i+1} \leq d-1$, $\deg R_i \geq d$, $\deg L_{i-1} \leq d-1$, and $\deg L_i \leq d$ (cf. Lemma 3.1).

By the assumption on the rank of the Hankel matrix and $h_0 \neq 0$ we have $L_i(0) \neq 0$. Departing from the Bézout relation

$$R_{i+1} = K_i \cdot T^{2d} + L_i \cdot C,$$

we obtain an identity in $\mathrm{K}[[T]]$

$$R_{i+1}/L_i = C + T^{2d} \cdot C'$$

with $R_{i+1}, L_i, C \in \mathrm{K}[[T]]$ all units. Denoting h_k to be the coefficients of the right-hand series we obtain polynomials A and B of respective degrees d and $d-1$ such that

$$\frac{B}{A} = \sum_{k=0}^{\infty} \frac{h_k}{X^{k+1}};$$

A and B are obtained from R_{i+1} and L_i by passing to the reverse polynomials. Next one computes the global Cauchy index of the Padé approximation B/A which coincides with the signature of $\mathrm{Han}_d(h)$ by Theorem 2.2.

If $h_0 = 0$, and T^δ is the maximal power of T dividing C, then one passes to the couple $(T^{2d-\delta}, CT^{-\delta})$ and considers now the first signed remainder with degree $\leq d-1-\delta$.

Altogether $O(\mathcal{M}(d)\log(d))$ arithmetic operations and comparisons are sufficient. □

4. Sylvester–Habicht Sequences

We define and study in this section Sylvester–Habicht sequences. Polynomials in the Sylvester–Habicht sequence of (A, B) are polynomials which are proportional to polyno-

mials in the remainder sequence of (A, B) but have better properties such as size control and specialization properties since they are defined through determinants. They are obtained by a sign modification from the sub-resultant sequence of (A, B). Difference of sign variations in the Sylvester–Habicht sequence of (A, B) determine the Cauchy index of B/A. The Sylvester–Habicht transition matrices will be the key notion used in our main algorithm in Section 5.

For a number $d \geq 1$ we call (A, B) a *(regular) d-couple* if $d = \deg A > \deg B$. If d is clear from the context we simply speak of a regular couple.

REMARK 4.1. We shall assume that $\deg A > \deg B$ throughout this section. If (A, B) is not a regular d-couple, simple adaptations are possible which do not change the Cauchy index and do not change the bit size consideration later on in case of integer polynomials.

(1) If $d > d_0 = \deg A > d_1 = \deg B$, one can simply pass to the regular d-couple (AX^{d-d_0}, BX^{d-d_0}). This neither changes the Cauchy index nor the sequence of signed Euclidean quotients.
(2) If $d \geq d_1 = \deg B \geq d_0 = \deg A \geq 1$, one can for instance pass to the $(d_0 + 2d_1)$-couple $((B^2 + 1)A, B)$. This neither changes the ideal nor the Cauchy index, and only adds one further initial signed Euclidean quotient. (For the Cauchy index alone, one can likewise take $((X^{2k} + 1)A, B)$ for a suitable k.)

Let D be a domain, K its quotient field. For a d-couple (A, B) in $\mathrm{D}[X]$ and $j \leq d - 1$, let the *jth Sylvester matrix* of (A, B), denoted $\mathrm{Syl}_j = \mathrm{Syl}_j(A, B)$, be the matrix the rows of which are the coefficient vectors of the polynomials

$$AX^{d-2-j}, AX^{d-3-j}, \ldots, AX, A, B, BX, \ldots, BX^{d-2-j}, BX^{d-1-j}$$

with respect to the monomial basis

$$X^{2d-2-j}, X^{2d-3-j}, \ldots, X, 1.$$

This matrix has $2d - 1 - 2j = (d - 1 - j) + (d - j)$ rows and $2d - 1 - j$ columns. If

$$\begin{aligned} A &= a_d X^d + a_{d-1} X^{d-1} + a_{d-2} X^{d-2} + \cdots + a_0, \\ B &= b_{d-1} X^{d-1} + b_{d-2} X^{d-2} + \cdots + b_0 \end{aligned}$$

(allowing top terms of B to vanish), then Syl_j has the shape

$$\mathrm{Syl}_j = \underbrace{\begin{pmatrix} a_d & \cdots & \cdots & \cdots & \cdots & a_0 & & \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & a_d & \cdots & \cdots & \cdots & \cdots & a_0 \\ & & & b_{d-1} & \cdots & \cdots & \cdots & b_0 \\ & & b_{d-1} & \cdots & \cdots & \cdots & b_0 & \\ & \iddots & \iddots & \iddots & \iddots & \iddots & & \\ b_{d-1} & \cdots & b_{j+1} & \cdots & b_0 & & & \end{pmatrix}}_{2d-1-j} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \end{matrix}}\right\} d-1-j \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \end{matrix}}\right\} d-j \end{matrix}$$

and is a sub-matrix of the full Sylvester matrix $\mathrm{Syl}_0 = \mathrm{Syl}_0(A, B)$.

REMARK 4.2. We name the rows by the corresponding polynomials AX^r and BX^s,

respectively, and the columns by the corresponding monomials X^t. For instance, the first column is the X^{2d-2-j}-column.

For $\ell = 0, \ldots, 2d-2-j$, let $\mathrm{Syl}_{j,\ell} = \mathrm{Syl}_{j,\ell}(A,B)$ be the square matrix of dimension $(2d-1-2j)\times(2d-1-2j)$ obtained by taking the columns of $X^{2d-2-j}, X^{2d-3-j}, \ldots, X^{j+1}$ (the first $2d-2-2j$ ones) and the X^ℓ-column of Syl_j.

The *Sylvester–Habicht sequence* of a d-couple (A,B) is the sequence

$$H_d = H_d(A,B), \ldots, H_0 = H_0(A,B)$$

defined as follows:

$$\begin{aligned} &H_d = A, \\ &H_j = \textstyle\sum_{\ell=0}^{j} \det(\mathrm{Syl}_{j,\ell}) X^\ell, \text{ if } 0 \le j \le d-1. \end{aligned}$$

Note that $H_{d-1} = B$. (Formally we add the definition $H_{-1} = 0$ and use for convenience the degree and leading coefficient definitions $\deg 0 = -1$, $\mathrm{lc}\, 0 = 0$ for the zero polynomial.) The *sequence of principal Sylvester–Habicht coefficients*

$$h_d = h_d(A,B), \ldots, h_0 = h_0(A,B)$$

is defined as $h_d = 1$, and $h_j = \mathrm{cf}_j(H_j)$ as the formal leading coefficient of H_j for $0 \le j < d$ (with the extension $h_{-1} = 0$). If $h_j = 0$, the polynomial H_j is called *defective*. Thus $h_j \neq 0$ boils down to saying that (H_j, H_{j-1}) is a regular (j-) couple. We define $t_j = \frac{h_j^2}{\mathrm{lc}\, H_j}$ for those j such that $h_j \neq 0$ (with an extension for all $j \ge \deg \gcd(A,B)$ later on), so $t_j = h_j$ with the exception $t_d = a_d^{-1}$ and $h_d = 1$.

Remark 4.3. (1) For reasons of signs we consider the Sylvester–Habicht polynomials (cf. Gonzalez *et al.*, 1990, 1994, 1998) rather than the usual sub-resultants. The corresponding factor of proportionality $(-1)^{(d-j)(d-j-1)/2}$ is accomplished by the above permutation of the BX^s-rows in the definition of the jth Sylvester matrix. Thus for a d-couple (A,B), the Sylvester–Habicht sequence results from the sub-resultant sequence by multiplying the two starting sub-resultants A and B by $+1$, the next two by -1 (no matter whether non-defective, defective, or vanishing), and so on. Furthermore, this permutation of the rows has organizational advantages when Syl_{j-1} is considered as a sub-matrix of Syl_j; one only has to add a first and a last row in order to obtain Syl_j.

(2) For reasons of uniformity in the degree of B (and simpler recursions) we consider throughout the Sylvester–Habicht polynomials with respect to a degree pattern $(d, d-1)$ (cf. Remark 4.1).

(3) The initializing definition $h_d = 1$ is classical and will be used throughout. This however produces the appearance of the cumbersome flipping a_d^{-1} rather than $h_d = 1$ instead. All formulæ become uniform with the alternative definitions $H_d = a_d^{-2} \cdot A$ and $h_d = \mathrm{lc}\, H_d$, however considerations will not remain within $\mathrm{D}[X]$ (cf. Lickteig and Roy, 1996).

Remark 4.4. Let $\Sigma_j = \Sigma_j(A,B)$ be the $(2d-1-2j) \times (2d-2-2j)$ east block of the matrix Syl_j of the columns of $X^{2d-2-j}, X^{2d-3-j}, \ldots, X^{j+2}, X^{j+1}$. The matrix Σ_j defines

a linear form $\sigma_j = \sigma_j(A,B)$ as $\sigma_j(\xi) = \det(\Sigma_j, \xi)$ for $\xi \in \mathrm{D}^{2d-1-2j}$ which is orthogonal to these columns. This linear form σ_j is non-zero if and only if the rank of Σ_j takes its maximal value $2d-2-2j$; in this case its extension to $\mathrm{K}^{2d-1-2j}$ is uniquely determined up to a non-zero factor in K by this orthogonality property. The coefficients $\mathrm{cf}_\nu(H_j)$ of H_j are the values of σ_j on the X^ν-column. Therefore,

$$\begin{aligned} H_j &= \sum_{\ell=0}^{j} \det(\mathrm{Syl}_{j,\ell}) X^\ell = \sum_{\ell=0}^{2d-2-j} \det(\mathrm{Syl}_{j,\ell}) X^\ell \\ &= \sum_{r=0}^{d-2-j} u_{j,r} \cdot AX^r + \sum_{t=0}^{d-1-j} v_{j,t} \cdot BX^t \\ &= \left(\sum_{r=0}^{d-2-j} u_{j,r} X^r \right) \cdot A + \left(\sum_{t=0}^{d-1-j} v_{j,t} X^t \right) \cdot B \\ &= U_j \cdot A + V_j \cdot B \in (A,B)\mathrm{D}[X] \end{aligned}$$

where the coefficients $u_{j,r} = u_{j,r}(A,B)$ and $v_{j,t} = v_{j,t}(A,B)$ of the polynomials $U_j = U_j(A,B)$, $V_j = V_j(A,B) \in \mathrm{D}[X]$ of the above Bézout relation for H_j are, up to sign, the maximal minors of Σ_j (that is, the coefficients of the linear form σ_j).

Now we are going to examine the relation between the Sylvester–Habicht polynomials and the remainders. The main property of the Sylvester–Habicht polynomials is the following Structure Theorem which is a refinement of the well-known Sub-resultant Theorem (cf. Habicht, 1948; Collins, 1967; Brown, 1971; Brown and Traub, 1971; Loos, 1982; Gonzalez *et al.*, 1990; Ducos, 1996; Lazard, 1998; Quitté, 1998).

THEOREM 4.1. (STRUCTURE THEOREM) *For a d-couple (A,B) of polynomials in $\mathrm{D}[X]$, D a domain with quotient field K, the polynomials in the Sylvester–Habicht sequence $H_d, \ldots, H_0$ are either K-proportional to the polynomials in the signed remainder sequence $R_0, \ldots, R_w$ or zero. Denoting for i, $0 \le i \le w = w(A,B)$, $j = \deg R_i$ and $k = \deg R_{i+1}$ one has the K-proportionalities*

$$R_i \sim_{\mathrm{K}} H_j,$$
$$R_{i+1} \sim_{\mathrm{K}} H_{j-1} \sim_{\mathrm{K}} H_k.$$

Furthermore, denoting $c_{j-1} = \mathrm{cf}_k(H_{j-1})$ the leading coefficient of H_{j-1}, the following relations hold:

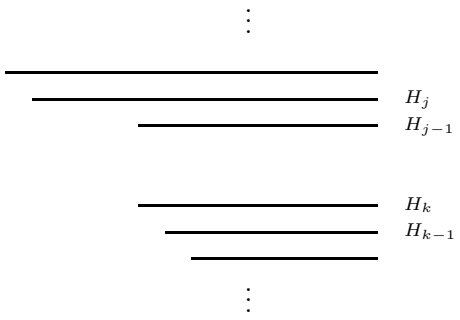
(1) $h_k = (-1)^{(j-k)(j-k-1)/2} \cdot c_{j-1} \cdot \left(\dfrac{c_{j-1}}{t_j} \right)^{j-k-1}$,

(2) $H_\ell = 0$ *for* $k < \ell < j-1$,

(3) (a) for $k \ge 0$, $h_j^2 \cdot H_{k-1} = -\mathrm{Rem}\,(h_k \cdot c_{j-1} \cdot H_j, H_{j-1})$, *and (b) this is an exact signed Euclidean division in* $\mathrm{D}[X]$.

REMARK 4.5. (1) The values of j with $h_j \neq 0$ are precisely the degrees of the polynomials in the signed Euclidean remainder sequence. The vanishing of the intermediate

Sylvester–Habicht polynomials is the famous gap structure, graphically displayed by the following diagram of Habicht lines.



(2) When H_{j-1} is non-defective, that is, when $k = j-1$, then $h_{j-1} = c_{j-1} = h_k$ and the exact signed Euclidean division 3 becomes Habicht's generic division formula $h_j^2 \cdot H_{j-2} = -\mathrm{Rem}\,(h_{j-1}^2 \cdot H_j, H_{j-1})$ (cf. Habicht, 1948).
(3) When H_{j-1} is defective, the preceeding result is a strict improvement of the famous Sub-resultant Theorem (cf. Habicht, 1948; Collins, 1967; Brown, 1971; Brown and Traub, 1971; Loos, 1982; Gonzalez *et al.*, 1990; Ducos, 1996; Lazard, 1998; Quitté, 1998)

REMARK 4.6. This new structure theorem gives a new classical style algorithm with $O(d^2)$ arithmetic operations for computing the Sylvester–Habicht polynomials, all intermediate computations being performed on integers of bit size $O(\tau d)$ in case of integer input polynomials of bit size $\tau > \log(d+1)$ without using modular techniques. A regular couple (H_j, H_{j-1}) being computed, the algorithm passes to the next regular couple (H_k, H_{k-1}) in the following way.

Starting from t_j and c_{j-1}, compute h_k successively as

$$t_j = \frac{h_j^2}{\mathrm{lc}\, H_j}, \ldots, t_{\ell-1} = t_\ell \cdot \frac{(-1)^{j-\ell} c_{j-1}}{t_j}, \ldots, t_k$$

and take $h_k = t_k$.
Compute H_k by multiplying H_{j-1} by h_k and dividing the result by c_{j-1}.
Compute H_{k-1} through exact Euclidean division of $-h_k \cdot c_{j-1} \cdot H_j$ by H_{j-1} and dividing the resulting remainder by h_j^2.

The fact that the t_ℓ, $\ell = j, j-1, \ldots, k$, belong to D can already be found in (Ducos, 1996), Lazard (1998) and (Quitté, 1998) and will be proved in Lemma 8.

Apart from statement 3 (b) on the exact signed Euclidean division, which we shall prove at the end of this section, the proof of the Structure Theorem 4.1 will follow from the subsequent two lemmas. For technical reasons we modify the remainder of the Euclidean division

$$A = \mathrm{Quo}\,(A, B) \cdot B + \mathrm{Rem}\,(A, B)$$

of a couple (A, B) of non-zero polynomials in $\mathrm{K}[X]$ with $\deg A \geq \deg B$ by multiplying this equation by $-\frac{\mathrm{lc}\, B}{\mathrm{lc}\, A}$. The *Gaussian remainder* $\mathrm{Gau}\,(A, B)$ is defined as

$$\begin{aligned}\mathrm{Gau}\,(A, B) &= \left(-\frac{\mathrm{lc}\, B}{\mathrm{lc}\, A}\right) \cdot \mathrm{Rem}\,(A, B) \\ &= \left(-\frac{\mathrm{lc}\, B}{\mathrm{lc}\, A} \cdot A\right) + \left(\frac{\mathrm{lc}\, B}{\mathrm{lc}\, A} \cdot \mathrm{Quo}\,(A, B)\right) \cdot B.\end{aligned}$$

Note that

$$\mathrm{Gau}\,(aA, bB) = b \cdot \mathrm{Gau}\,(A, B) \qquad \text{for non-zero } a, b \in \mathrm{K} \tag{4.1}$$

(while $\mathrm{Rem}\,(aA, bB) = a \cdot \mathrm{Rem}\,(A, B)$ for non-zero $a, b \in \mathrm{K}$) and that the cofactor of B in the above Bézout relation for the Gaussian remainder is monic. The latter property is characteristic for the *Gaussian remainder sequence* $G_0, \ldots, G_w$ recursively defined as $G_{i+1} = G_{i+1}(A, B) = \mathrm{Gau}\,(G_{i-1}, G_i)$ starting with $G_0 = A$ and $G_1 = B$.

Lemma 4.1. *Let (A, B) be a d-couple of non-zero polynomials in $\mathrm{K}[X]$ with Gaussian remainder sequence $G_0, \ldots, G_w$. Then there is a polynomial $A_i \in \mathrm{K}[X]$ of degree $d_1 - d_i$ and a monic polynomial $B_i \in \mathrm{K}[X]$ of degree $d_0 - d_i$ (where $d_i = \deg R_i = \deg G_i$) such that*

$$G_{i+1} = A_i \cdot A + B_i \cdot B$$

for $i = 1, \ldots, w = w(A, B)$.

Proof. Induction on i. □

The monic cofactor of B in the above Bézout relation for G_{i+1} allows us to perform a unimodular row manipulation with determinant one in the matrix Syl_ℓ which replaces some of the BX^s-rows by certain $G_{i+1}X^t$-rows. Since the maximal minors of Syl_ℓ remain unchanged this will allow us to analyze conveniently the coefficients of the Sylvester–Habicht polynomials in the gap situation and to bridge the gap.

Lemma 4.2. *Assume that $\deg H_j = j > \deg H_{j-1} = k$ and $d_i \geq j > d_{i+1} = \deg G_{i+1}$. Then the following hold:*

(1) $H_{j-1} = a_d \cdot t_j \cdot G_{i+1}$ (so $d_{i+1} = k$ and $\mathrm{lc}\, G_{i+1} = \frac{c_{j-1}}{a_d \cdot t_j}$),
(2) $H_\ell = 0$ for $k < \ell < j - 1$,
(3) $H_k = (-1)^{(j-k)(j-k-1)/2} \cdot a_d^{j-k} \cdot t_j \cdot (\mathrm{lc}\, G_{i+1})^{j-k-1} \cdot G_{i+1}$,
(4) defining $t_\ell = (-1)^{(j-\ell)(j-\ell-1)/2} \cdot c_{j-1} \cdot \left(\frac{c_{j-1}}{t_j}\right)^{j-\ell-1}$, then t_ℓ is a maximal minor of Syl_ℓ for $\ell = j-1, \ldots, k$, and $t_k = h_k$ (in accordance with the preliminary definition of t_k).

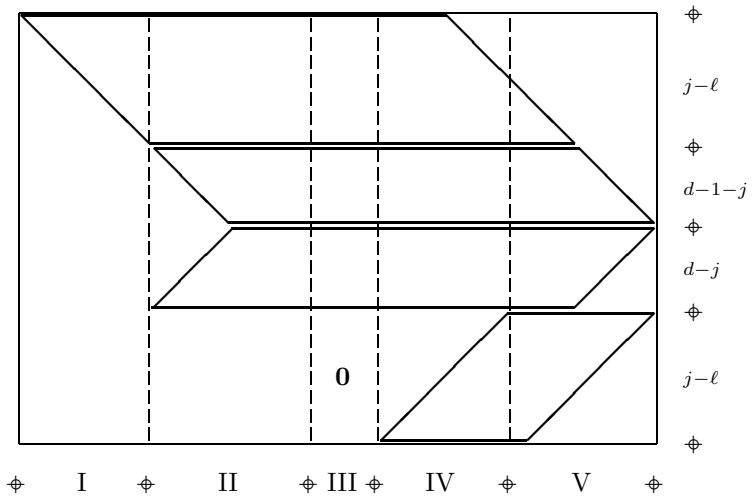
Proof. Assume first that $d > j$; then $t_j = h_j$. We consider the ℓth Sylvester matrix Syl_ℓ for $j \geq \ell \geq k$ and replace the rows of

$$BX^{d-j}, BX^{d-j+1}, \ldots, BX^{d-2-\ell}, BX^{d-1-\ell}$$

by the rows of $G_{i+1}, G_{i+1}X, \ldots, G_{i+1}X^{j-2-\ell}, G_{i+1}X^{j-1-\ell}$. By Lemma 4.1 this new matrix results from Syl_ℓ through a unimodular rows manipulation with determinant one (adding successively linear combinations of previous rows to the rows of

$$BX^{d-j}, BX^{d-j+1}, \ldots, BX^{d-2-\ell}, BX^{d-1-\ell}$$

of Syl_ℓ) and has the following shape



where the top parallelogram comprises the rows of

$$AX^{d-2-\ell}, AX^{d-3-\ell}, \ldots, AX^{d-j}, AX^{d-1-j},$$

the two middle parallelograms together correspond to the jth Sylvester matrix Syl_j and comprise the rows of

$$AX^{d-2-j}, AX^{d-3-j}, \ldots, AX, A$$

and of

$$B, BX, \ldots, BX^{d-2-j}, BX^{d-1-j},$$

and finally the bottom parallelogram comprises the rows of

$$G_{i+1}, G_{i+1}X, \ldots, G_{i+1}X^{j-2-\ell}, G_{i+1}X^{j-1-\ell};$$

furthermore for the vertical bands,

I is the block of the columns of $X^{2d-2-\ell}, X^{2d-3-\ell}, \ldots, X^{2d-j}, X^{2d-1-j}$,
II is the block of the columns of $X^{2d-2-j}, X^{2d-3-j}, \ldots, X^{j+2}, X^{j+1}$,
III is the block of the columns of $X^{j}, X^{j-1}, \ldots, X^{j-(\ell-k)+1}, X^{j-(\ell-k)}$,
IV is the block of the columns of $X^{j-(\ell-k)-1}, X^{j-(\ell-k)-2}, \ldots, X^{k+1}, X^{k}$,
V is the block of the columns of $X^{k-1}, X^{k-2}, \ldots, X, 1$.

Note that the upper triangular $(j-\ell)\times(j-\ell)$ north block of band I always has on its diagonal the element a_d, the middle $(2d-1-2j)\times(2d-2-2j)$ block of band II is the matrix Σ_j (see Remark 4.4), band III has a $(j-\ell)\times(\ell-k+1)$ null south block, and that the $(j-\ell)\times(j-\ell)$ south block of IV always has on its anti-diagonal the element $\mathrm{lc}\, G_{i+1}$.

(1) For $j-\ell=1$, the linear form $\sigma_\ell=\sigma_{j-1}$ is non-zero since $a_d\cdot h_j\neq 0$, and we find from the shape of the above matrix that $H_{j-1}=a_d\cdot h_j\cdot G_{i+1}$, which can only be zero if $G_{i+1}=0$, that is, if $i=w$, or in other words, if $k=d_{i+1}=-1$.
If $k=-1$ all linear forms σ_ℓ are null for $\ell<j$ since the bottom parallelogram of the above matrix is null, so we assume $k\geq 0$ in what follows.

(2) For $j-\ell\geq 2$ and $\ell-k+1\geq 2$, the null south block of III shows that the columns of I, II, and the first two of III (that is, the columns of X^j, X^{j+1}) are linearly dependent. Thus the same columns of Σ_ℓ are dependent, and the linear form σ_ℓ is zero. Hence $H_\ell=0$ for $k<\ell<j-1$.

(3) For $\ell=k$, band III just consists of the X^j-column and the shape of the above matrix shows that $H_k=(-1)^{(j-k)(j-k-1)/2}\cdot a_d^{j-k}\cdot h_j\cdot(\operatorname{lc} G_{i+1})^{j-k-1}\cdot G_{i+1}$.

(4) By the first statement $c_{j-1}/h_j=a_d\cdot\operatorname{lc} G_{i+1}$, so t_ℓ is the minor of the columns of band I, band II, the first column of band III (the X^j-column), and the columns of band IV of the above matrix, and hence its coincides with the same minor of Syl_ℓ.

The case $j=d$ is similar and left to the reader; one considers Syl_ℓ directly. □

Proof of the Structure Theorem 4.1. The degree inequality $d_i\geq j$ assumed in Lemma 4.2 is an equality for $j=d=d_0$, so by induction this is always an equality under the assumption $j>d_{i+1}$. Thus it remains to show the third item in the Structure Theorem 4.1. Using Lemma 4.2 and relation (4.1) for the Gaussian remainder we find that

$$\begin{aligned}
H_{k-1}&=a_d\cdot h_k\cdot G_{i+2}=a_d\cdot h_k\cdot\operatorname{Gau}(G_i,G_{i+1})\\
&=\frac{h_k}{t_j}\cdot\operatorname{Gau}(G_i,a_d\cdot t_j\cdot G_{i+1})\\
&=\frac{h_k}{t_j}\cdot\operatorname{Gau}(H_j,H_{j-1})\\
&=-\frac{h_k\cdot c_{j-1}}{h_j^2}\cdot\operatorname{Rem}(H_j,H_{j-1})\\
&=-h_j^{-2}\cdot\operatorname{Rem}(h_k\cdot c_{j-1}\cdot H_j,H_{j-1}),
\end{aligned}$$

thus $h_j^2\cdot H_{k-1}=-\operatorname{Rem}(h_k\cdot c_{j-1}\cdot H_j,H_{j-1})$. The fact that this is an exact signed Euclidean division in $\mathrm{D}[X]$ will be shown at the end of this section (Corollary 4.3). □

Corollary 4.1. *For a d-couple (A,B) in $\mathrm{D}[X]$ and $j\neq\deg\gcd(A,B)-1$, $j\leq d-1$,*

$$H_j=0\iff\sigma_j=0\iff\operatorname{rank}\Sigma_j<2d-2-2j.$$

For $j=\deg\gcd(A,B)-1$, $H_j=0$ and $\sigma_j\neq 0$.

Next we remark that the Bézout relations for non-zero H_j in Remark 4.4 are uniquely determined through a certain degree condition on the cofactors U_j and V_j; we shall call them *the* polynomials of *the* jth Bézout relation, that is to say with definite articles.

PROPOSITION 4.1. *For a d-couple* (A, B) *of polynomials in* $\mathrm{D}[X]$ *the polynomials* U_j *and* V_j *in* $\mathrm{D}[X]$ *in the* j*th Bézout relation*

$$H_j = U_j \cdot A + V_j \cdot B$$

are uniquely determined by the degree restriction $\deg V_j \leq d-1-j$ *for all* j *such that* $H_j(A, B) \neq 0$. *One has* $\deg V_j = d-1-j$ *if and only if* $j = d$ *or* H_{j+1} *is non-defective.*

PROOF. This is clear for $j = d$. For $j < d$, $\deg V_j \leq d-1-j$ implies the validity of the additional degree bound $\deg U_j \leq d-2-j$. $H_j \neq 0$ always implies that $\sigma_j \neq 0$. Any such degree restricted Bézout relation for any non-zero polynomial of degree $\leq j$ uniquely corresponds to a linear form that is K-proportional to σ_j (see Remark 4.4). If this polynomial coincides with H_j the factor of proportionality is one. (In any case, if $\sigma_j \neq 0$, the pair (U_j, V_j) is uniquely determined up to K-proportionality by the conditions $\deg V_j \leq d-1-j$ and $\deg(U_j \cdot A + V_j \cdot B) \leq j$.) □

Corresponding conditions make transition matrices unique; analogously as above we shall speak of *the* transition matrices.

COROLLARY 4.2. *Let* $0 \leq j \leq d$, (A, B) *be a d-couple and* (C, D) *be a* j*-couple of polynomials in* $\mathrm{K}[X]$. *Assume* (C, D) *to be element-wise* K*-proportional to a couple of two consecutive signed Euclidean remainders of* (A, B), *and let*

$$M = \begin{pmatrix} I & J \\ K & L \end{pmatrix} \in \mathrm{K}[X]^{2\times 2}$$

be a transition matrix, that is,

$$\begin{pmatrix} C \\ D \end{pmatrix} = M \cdot \begin{pmatrix} A \\ B \end{pmatrix}.$$

Then the conditions $\deg J \leq d-1-j$ *and* $\deg L \leq d-j$ *make the transition matrix* $M = M(C, D; A, B)$ *unique,* M *is unimodular, and* $\deg L = d-j$, *provided that* $D \neq 0$.

If $D = 0$, *an additional non-zero calibration of* $\det M$ *makes* M *unique with these properties.*

PROOF. By the Structure Theorem 4.1 we may assume by a monomial scaling that $(C, D) = (H_j, H_{j-1})$. Then if $H_{j-1} \neq 0$,

$$M = \begin{pmatrix} U_j & V_j \\ U_{j-1} & V_{j-1} \end{pmatrix}, \tag{4.2}$$

by Proposition 4.1, and another monomial scaling and the comparison with the unimodular signed Euclidean transition matrix shows that M is unimodular with $\deg V_{j-1} = d-j$ (cf. Lemma 3.1 or consider the linear form σ_{j-1}).

If $H_{j-1} = 0$ the second row of M in (4.2) may be scaled arbitrarily. Passing to the generic situation first shows that in any case $\det M \in \mathrm{K}$ (a constant polynomial), and $H_j \neq 0$ shows $\det M \neq 0$. (For $j = 0$ pass first to the generic situation of $(d+1)$-couples and consider $j = 1$.) □

We fix a d-couple (A, B) of polynomials in $\mathrm{D}[X]$ and study the transition between two regular couples of Sylvester–Habicht polynomials (H_j, H_{j-1}) and (H_k, H_{k-1}), that is to say, both regular and $0 \le k \le j \le d$. Moreover, if $H_{j-1} \sim_{\mathrm{K}} H_k$, then the pair of regular couples of Sylvester–Habicht polynomials is said to be *consecutive*.

For such a pair (k, j), $0 \le k \le j \le d$, we define the *Sylvester–Habicht transition matrix*

$$N_{k,j} = N_{k,j}(A, B) = \begin{pmatrix} U_{1,k,j} & V_{1,k,j} \\ U_{2,k,j} & V_{2,k,j} \end{pmatrix} \in \mathrm{K}[X]^{2\times 2}$$

such that

$$\begin{pmatrix} H_k \\ H_{k-1} \end{pmatrix} = N_{k,j} \cdot \begin{pmatrix} H_j \\ H_{j-1} \end{pmatrix}$$

defined by Corollary 4.2 as $N_{k,j} = M(H_k, H_{k-1}; H_j, H_{j-1})$ with the calibrating $\det N_{k,j} = h_k^2/h_j^2$ if $H_{k-1} = 0$ (motivated by the non-final transition; see Lemma 4.3, Proposition 4.2, and Proposition 4.3). Note that $U_{1,k,j} = 0$ in the consecutive case. Generally, $N_{k,j}$ is the product of all the intermediate consecutive Sylvester transition matrices.

We have the following lemma.

LEMMA 4.3. *Let (A, B) be a regular d-couple of polynomials in $\mathrm{D}[X]$, and (H_j, H_{j-1}) and (H_k, H_{k-1}) be two consecutive regular couples of its Sylvester–Habicht polynomials, $0 \le k < j \le d$. Then the anti-diagonal entries of the consecutive Sylvester–Habicht transition matrix*

$$N_{k,j} = \begin{pmatrix} 0 & V_{1,k,j} \\ U_{2,k,j} & V_{2,k,j} \end{pmatrix}$$

are

$$V_{1,k,j} = \frac{h_k}{c_{j-1}}, \qquad U_{2,k,j} = -\frac{h_k \cdot c_{j-1}}{h_j^2};$$

so

$$\det N_{k,j} = \frac{h_k^2}{h_j^2}.$$

Moreover, $\deg V_{2,k,j} = j - k$.

PROOF. This is an immediate consequence of points 2 and 3 (a) of the Structure Theorem 4.1. □

Let $d = d_0 > d_1 > \cdots > j = d_i > \cdots > d_w$ denote the degree sequence in the remainder sequence of the d-couple (A, B). We now consider the Sylvester–Habicht transition matrix $N_{j,d} = N_{j,d}(A, B)$,

$$N_{j,d} = N_{d_i,d_{i-1}} \cdots N_{d_1,d_0}$$

of an "absolute transition" satisfying

$$\begin{pmatrix} H_j \\ H_{j-1} \end{pmatrix} = N_{j,d} \cdot \begin{pmatrix} H_d \\ H_{d-1} \end{pmatrix} = N_{j,d} \cdot \begin{pmatrix} A \\ B \end{pmatrix}.$$

PROPOSITION 4.2. *Let (A, B) be a d-couple of polynomials in $\mathrm{D}[X]$, $0 \le j \le d$, and*

(H_j, H_{j-1}) be a regular couple of its Sylvester–Habicht polynomials. Then

$$N_{j,d} = \begin{pmatrix} U_j & V_j \\ U_{j-1} & V_{j-1} \end{pmatrix}$$

where $U_j, V_j, U_{j-1}, V_{j-1} \in \mathrm{D}[X]$ are the polynomials of the jth and $(j-1)$th Bézout relations.

Proof. By Proposition 4.1 and Corollary 4.2. □

For a "relative transition" one has the following.

Proposition 4.3. *Let (A, B) be a d-couple of polynomials in $\mathrm{D}[X]$, and (H_j, H_{j-1}) and (H_k, H_{k-1}) be two regular couples of its Sylvester–Habicht polynomials, $0 \le k \le j \le d$. Then*

$$\det N_{k,j} = \frac{h_k^2}{h_j^2},$$
$$h_j^2 \cdot N_{k,j} = \begin{pmatrix} U_k & V_k \\ U_{k-1} & V_{k-1} \end{pmatrix} \cdot \begin{pmatrix} V_{j-1} & -V_j \\ -U_{j-1} & U_j \end{pmatrix},$$

and therefore the elements of this scaled matrix lie in $\mathrm{D}[X]$.

Proof. The matrix $N_{k,j}$ is the product of all intermediate consecutive Sylvester–Habicht transition matrices; so by the multiplicativity of determinants and Lemma 4.3, $\det N_{k,j} = h_k^2/h_j^2$.

The factorizations of $N_{k,j}$ and of $N_{j,d}$ as the products of the respective consecutive ones shows that we can in fact write $N_{k,j} = N_{k,d} \cdot N_{j,d}^{-1}$; so by Proposition 4.3 and $\det N_{j,d} = h_j^2$ the scaled matrix is in fact denominator free. □

Next we deduce the exact divisibility stated in the Structure Theorem 4.1. In the consecutive case we have for the Sylvester–Habicht transition matrix

$$N_{k,j} = \begin{pmatrix} 0 & V_{1,k,j} \\ U_{2,k,j} & V_{2,k,j} \end{pmatrix}$$

the explicit representations

$$V_{1,k,j} = \frac{h_k}{c_{j-1}} = \frac{h_k \cdot t_j \cdot c_{j-1}^{-1}}{t_j} = \frac{(-1)^{j-k-1} \cdot t_{k+1}}{t_j} = \frac{h_k \cdot h_j^2 \cdot c_{j-1}^{-1}}{h_j^2},$$

where the element t_{k+1} lies in D for $k+1 < d$ $\left(t_j = \frac{h_j^2}{\mathrm{lc}\, H_j}\right.$, as in Lemma 4.2$\left.\right)$, and

$$(-1)^{j-k-1} \cdot t_{k+1} \cdot (\mathrm{lc}\, H_j) = h_k \cdot h_j^2 \cdot c_{j-1}^{-1} = -U_k(0) \cdot V_j(0) + V_k(0) \cdot U_j(0),$$
$$U_{2,k,j} = -\frac{h_k \cdot c_{j-1}}{h_j^2},$$

and

$$V_{2,k,j} = \frac{1}{h_j^2} \cdot (-U_{k-1} \cdot V_j + V_{k-1} \cdot U_j).$$

This shows that instead of the usual exact Euclidean divisibility via the pseudo-remainder, one also has the following exact signed Euclidean division announced in the Structure Theorem 4.1.3. (b).

COROLLARY 4.3. *Notations as above, one has for $j \leq d$ and the entries of a consecutive Sylvester–Habicht transition matrix*

$$N_{k,j} = \begin{pmatrix} 0 & V_{1,k,j} \\ U_{2,k,j} & V_{2,k,j} \end{pmatrix}$$

the numerator-denominator representations

$$V_{1,k,j} = \frac{-U_k(0) \cdot V_j(0) + V_k(0) \cdot U_j(0)}{h_j^2} = \frac{(-1)^{j-k-1} \cdot t_{k+1}}{t_j}$$

where $t_{k+1} \in \mathrm{D}$ for $k+1 < d$,

$$U_{2,k,j} = -\frac{h_k \cdot c_{j-1}}{h_j^2},$$

and

$$V_{2,k,j} = \frac{-U_{k-1} \cdot V_j + V_{k-1} \cdot U_j}{h_j^2}.$$

As a consequence,

$$-h_k \cdot c_{j-1} \cdot H_j = (U_{k-1} \cdot V_j - V_{k-1} \cdot U_j) \cdot H_{j-1} + h_j^2 \cdot H_{k-1}$$

is an exact signed Euclidean division.

The Sylvester–Habicht sequences gives the Cauchy index in a similar way as the remainder sequence using the subsequent definition of modified sign changes.

DEFINITION 4.1. Let $\mathcal{P} = [P_0, P_1, \ldots, P_n]$ be an arbitrary sequence of polynomials and a be an element of $\mathrm{R} \cup \{-\infty, +\infty\}$. Then $W(\mathcal{P}; a)$, the *number of modified sign changes* of $\mathcal{P}$ at a, is the number defined as follows.

(1) Delete from $\mathcal{P}$ those polynomials which are identically 0 to obtain the list of polynomials $[p_0, \ldots, p_s]$ in $\mathrm{D}[X]$.
(2) Take $W(\mathcal{P}; a)$ as the number of sign changes in the list of values $[p_0(a), \ldots, p_s(a)]$, the usual definition being modified only for groups of two zeros in the following way:

count *one* sign variation for the groups $[+, 0, 0, -]$ and $[-, 0, 0, +]$,
count *two* sign variations for the groups $[+, 0, 0, +]$ and $[-, 0, 0, -]$.

We denote by $W(a)$ the number of modified sign changes of the Sylvester–Habicht sequence of (A, B) at a.

THEOREM 4.2. (GONZALEZ *et al.*, 1998) *Let (A, B) be d-couple of polynomials in $\mathrm{D}[X]$, and $a < b$ elements in $\mathrm{R} \cup \{-\infty, +\infty\}$ and $A(a) \cdot A(b) \neq 0$. Then,*

$$I(B/A;]a, b[) = W(a) - W(b).$$

Note that the existing proofs of this result (Gonzalez *et al.*, 1998; Roy, 1996) are based on the classical Sub-resultant Theorem. These proofs can be slightly simplified using the new Structure Theorem 4.1.

5. Bit Size and Sylvester–Habicht Transition Matrices

In this section we assume $\mathrm{D} = \mathbb{Z}$. In the following for a pair (k, j), $0 \le k < j \le d$, we denote the list of all intermediate consecutive Sylvester–Habicht transition matrices by $\mathcal{N}_{k,j}(A, B)$; their product (in the right order) is $N_{k,j}(A, B)$.

We fix a number D and now define, in the spirit of Section 3, the task $\mathcal{T}(D, \sigma; d, \ell)$ for $\ell \le D$. The inputs are now regular couples (R, S) of integer polynomials such that there exists a D-couple (A, B) with $(R, S) = (H_\delta(A, B), H_{\delta-1}(A, B))$ for some $\delta \le d$, (A, B) satisfying the requirement that the coefficients of all the determinants and (determinantal) polynomials associated to (A, B) appearing in Remark 4.4, Theorem 4.1, Proposition 4.1, Proposition 4.3, and Corollary 4.3 have bit size bounded by σ. In this case we say that (A, B) satisfies the (D, σ)-*requirement*. If D-couples (A, B) of bit size at most $\tau > \log(D + 1)$ are considered, $\sigma = \sigma(D, \tau) = O(D\tau)$ will be sufficiently big by Hadamard's bound.

The task $\mathcal{T}(D, \sigma; d, \ell)$ for $d \le D$, using the target number r as defined in Section 3, is the following.

Input: a regular couple $(R, S) = (H_\delta(A, B), H_{\delta-1}(A, B))$ with $\delta \le d$, (A, B) satisfying the (D, σ)-requirement.
Output: the list $(\mathcal{N}_{r,\delta}(A, B); N_{r,\delta}(A, B); H_r(A, B), H_{r+1}(A, B))$ with $r = r(d, \ell, R, S)$.

We first recall polynomial multiplication in the bit complexity model.

THEOREM 5.1. (SCHÖNHAGE, 1982) *Multiplication of two integer polynomials of degrees at most d and (coefficient) bit size bounded by $\tau \ge \log(d+1)+2$ is possible on a multi-tape Turing machine in time (number of bit operations)*

$$\mathcal{M}(d, \tau) = O(d\tau \cdot \log(d\tau) \cdot \log\log(d\tau)).$$

Using the usual modular tricks with respect to coefficients, an exact Euclidean division of integer polynomials can be done within the same time provided the quotient and remainder are known to satisfy the same bit size bounds.

COROLLARY 5.1. *An exact division of two integer polynomials of degrees bounded by d and (coefficient) bit size bounded by $\tau \ge \log(d+1)+2$ having a quotient and a remainder of bit size bounded by τ as well is possible on a multi-tape Turing machine in time*

$$O(\mathcal{M}(d, \tau)) = O(d\tau \cdot \log(d\tau) \cdot \log\log(d\tau)).$$

THEOREM 5.2. *For numbers $\ell \le d < D$ and bit size bound $\sigma \ge \log(d + 1)$, task $\mathcal{T}(D, \sigma; d, \ell)$ can be solved on a multi-tape Turing machine in time*

$$O(\mathcal{M}(d, \sigma) \cdot \log(d)).$$

PROOF. The design with respect to the degree descent is analogous to the one in Section 3, replacing signed remainders by Sylvester–Habicht polynomials and quotients by Sylvester–Habicht transition matrices, according to the results of the two previous sections. For the multiplication and (signed) Euclidean division of integer polynomials one uses the above-mentioned results. □

If a couple (A, B) of degree at most d and bit size τ is given, a choice $D = O(d)$ and a choice $\sigma(D, \tau) = O(d\tau)$ is sufficient by Remark 4.1 and Hadamard's bound for computing the Cauchy index. Thus we have the following corollary.

COROLLARY 5.2. *Computation of the Cauchy index of a couple of integer polynomials (A, B) of degree at most d of bit size bounded by τ between two rational numbers a and b of numerator and denominator bit size at most τ as well (including $a = -\infty$ or $b = +\infty$) can be performed on a multi-tape Turing machine in time*

$$O(d^2\tau \cdot \log(d\tau) \cdot \log\log(d\tau) \cdot \log(d)).$$

The same bound holds for the computation of the Sylvester–Habicht transition matrices and the last non-zero Sylvester–Habicht polynomial.

For computing the signature of a non-singular (over $\mathbb{Q}$) Hankel matrix we have the following result improving on Gemignani (1991 and 1994).

COROLLARY 5.3. *Computation of the signature of a non-singular integer $d \times d$ Hankel matrix of bit size bounded by τ can be performed on a multi-tape Turing machine in time*

$$O(d^2\tau \cdot \log(d\tau) \cdot \log\log(d\tau) \cdot \log(d)).$$

PROOF. Given $h = (h_0, \ldots, h_{2d-1})$, let $\mathrm{Han}_d(h)$ be the associated Hankel matrix. By Jacobi's criterion (cf. Gantmacher, 1966, Chapter 10) the signature of $\mathrm{Han}_d(h)$ is determined by the sequence of signs of the successive principal minors $1, h_0, h_0h_2 - h_1^2, \ldots$ of $\mathrm{Han}_d(h)$. In the same way it is also determined by the sequence of signs of the successive reverse principal minors $1, h_{2d-2}, h_{2d-4}h_{2d-2} - h_{2d-3}^2, \ldots$. Consider the polynomials T^{2d} and $C = \sum_{k=0}^{2d-1} h_k T^k$ as in the proof of Theorem 3.4, and assume for simplicity that $h_0 \neq 0$. Consider, furthermore, the segment $H_{2d-1}(T^{2d}, C), \ldots, H_{d-1}(T^{2d}, C)$ of the Sylvester–Habicht polynomials. Up to factors $\pm h_0$, the constant terms of these coincide with the successive reverse principal minors $1, h_{2d-2}, h_{2d-4}h_{2d-2} - h_{2d-3}^2, \ldots$ of $\mathrm{Han}_d(h)$. One can compute these within the stated time bound by using the algorithm of Theorem 5.2 and a Horner scheme-like backward evaluation as in Remark 3.1. (For $H_{2d-i}(T^{2d}, C)(0)$ the factor is $(-1)^{i-1}h_0$.) □

6. Remainders

We are now going to prove the following result which surprisingly seems to be new.

THEOREM 6.1. *The coefficients of the polynomials of the remainder sequence of a d-couple (A, B) of integer polynomials of bit size at most $\tau \geq \log(d + 1)$ possess integer numerator-denominator representations of bit size $O(\tau d^2)$.*

The proof is an immediate consequence of the subsequent proposition.

PROPOSITION 6.1. *Let (A, B) be a d-couple of polynomials in* $\mathrm{D}[X]$, D *a domain with quotient field* K, $R_0, \ldots, R_w$ *its signed remainder sequence of degrees* $d_0, \ldots, d_w$ *and* $H_d, \ldots, H_0$ *its Sylvester–Habicht sequence. Then the factors of proportionality* $\lambda_i, \mu_i \in \mathrm{K}^\times$ *in*

$$R_i = \lambda_i \cdot H_{d_i},$$
$$R_{i+1} = \mu_i \cdot H_{d_i - 1}$$

satisfy the recursion

$$\begin{pmatrix} \lambda_{i+1} \\ \mu_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & V_{1,d_{i+1},d_i}^{-1} \\ -U_{2,d_{i+1},d_i}^{-1} & 0 \end{pmatrix} \cdot \begin{pmatrix} \lambda_i \\ \mu_i \end{pmatrix}$$

where V_{1,d_{i+1},d_i} *and* U_{2,d_{i+1},d_i} *are the anti-diagonal entries of the consecutive Sylvester–Habicht transition matrix* N_{d_{i+1},d_i}.

PROOF. We consider the next couple

$$R_{i+1} = \lambda_{i+1} \cdot H_{d_{i+1}},$$
$$R_{i+2} = \mu_{i+1} \cdot H_{d_{i+1}-1}.$$

With the notations of Corollary 4.3 we have

$$\begin{pmatrix} R_{i+1} \\ R_{i+2} \end{pmatrix} = \begin{pmatrix} \lambda_{i+1} & 0 \\ 0 & \mu_{i+1} \end{pmatrix} \cdot \begin{pmatrix} 0 & V_{1,d_{i+1},d_i} \\ U_{2,d_{i+1},d_i} & V_{2,d_{i+1},d_i} \end{pmatrix} \cdot \begin{pmatrix} \lambda_i^{-1} & 0 \\ 0 & \mu_i^{-1} \end{pmatrix} \cdot \begin{pmatrix} R_i \\ R_{i+1} \end{pmatrix}.$$

By the uniqueness of the signed Euclidean transition matrix (cf. Corollary 4.2) we have in fact $\lambda_{i+1} \cdot V_{1,d_{i+1},d_i} \cdot \mu_i^{-1} = 1$ and $\mu_{i+1} \cdot U_{2,d_{i+1},d_i} \cdot \lambda_i^{-1} = -1$, as asserted. □

Thus in the integer polynomials situation of Theorem 6.1, for every i the factors $\lambda_i, \mu_i \in \mathbb{Q}$, possess a numerator-denominator representation with both numerator and denominator each being a product of at most d integers having size at most $O(d\tau)$, by Corollary 4.3.

Note that the sub-resultant polynomials, being defined through determinants, have integer coefficients of bit size at most $O(d\tau)$. This implies immediately that in the Gaussian remainder sequence all the coefficients of the polynomials in the sequence possess a numerator-denominator representation with numerator and denominator having size at most $O(d\tau)$, by point 1 of Lemma 4.2. In a monic remainder sequence as well (when the coefficients of the remainder are divided by the leading coefficient), the polynomials in the sequence possess as well a numerator-denominator representation with numerator and denominator having size at most $O(d\tau)$. In contrast, in the ordinary Euclidean remainder sequence the coefficients of the remainders possess a numerator-denominator representation with numerator and denominator having size at most $O(d^2\tau)$, and this is the quadratic behavior observed in practice.

7. Summary

After defining the Cauchy index and recalling the quotient boot method for evaluating quickly the remainder sequence at a point, we considered Sylvester–Habicht polynomials

which are a signed version of sub-resultants. We improved the classical Sub-resultant Theorem by proving a new exact divisibility result for Sylvester–Habicht polynomials and studied in detail the Sylvester–Habicht transition matrices. We then adapted the quotient boot method to the Sylvester–Habicht transition matrices, obtaining new algorithms for computing the Cauchy index of a rational function, and the signature of a non-singular Hankel matrix, in a fast and also storage efficient way. Over the integers our algorithms have bit complexity $O(\mathcal{M}(d,\sigma)\cdot\log(d))$ with $\sigma = O(d\tau)$ where $\mathcal{M}(d,\sigma) = O(d\sigma\cdot\log(d\sigma)\cdot\log\log(d\sigma))$ is Schönhage's bound for multiplication of integer polynomials of degrees bounded by d and bit size bounded by σ in the multi-tape Turing machine model. Thus our bound is $O(d^2\tau\cdot\log(d\tau)\cdot\log\log(d\tau)\cdot\log(d))$. We also proved that the size of coefficients in the ordinary remainder sequence is quadratic in d.

References

Brent, R. P., Gustavson, F. G., Yun, D. Y. Y. (1980). Fast solution of toeplitz systems of equations and computation of Padé approximants. *J. Algorithms*, **1**, 259–295.

Brown, W. S. (1971). On Euclid's algorithm and the computation of polynomial greatest common divisor. *J. A. C. M.*, **18**, 476–504.

Brown, W. S., Traub, J. F. (1971). On Euclid's algorithm and the theory of sub-resultants. *J. A. C. M.*, **18**, 505–524.

Collins, G. E. (1967). Subresultants and reduced polynomial remainder sequence. *J. A. C. M.*, **14**, 128–142.

Ducos, L. (1996). Algorithme de Bareiss, algorithmes des sous-résultants. *Informatique théorique et applications*, **30**, 319–347.

Frobenius, F. G. (1884). Über das Trägheitsgesetz der quadratischen Formen, *Sitzungsberichte der Preuss. Akad. der Wiss.* (März 1984 und Mai 1884), pp. 241–256.

Gantmacher, F. R. (1966). *Théorie des matrices, tome* **I**, Dunod 1966 and New York, Springer-Verlag 1986.

Gemigniani, L. (1991). Computing the inertia of Bézout and Hankel matrices. *Calcolo*, **28**, 267–274.

Gemigniani, L. (1994). Solving Hankel systems over the integers. *J. Symb. Comput.*, **18**, 573–584.

Gonzalez, L., Lombardi, H., Recio, T., Roy, M.-F. (1990). Spécialisation de la suite de Sturm et sous-résultants I. *Informatique théorique et applications*, **24**, 561–588.

Gonzalez, L., Lombardi, H., Recio, T., Roy, M.-F. (1994). Spécialisation de la suite Sturm. *Informatique théorique et applications*, **28**, 1–24.

Gonzalez, L., Lombardi, H., Recio, T., Roy, M.-F. (1998). Sturm-Habicht sequence, determinants and real roots of univariate polynomials. In Caviness, B., Johnson, J. eds, *Quantifier Elimination and Cylindrical Algebraic Decomposition*, *Texts and Monographs in Symbolic Computation*, New York, Springer-Verlag.

Habicht, W. (1948). Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens. *Comm. Math. Helvetici*, **21**, 99–116.

Henrici, P. (1970). Upper bounds for the abscissa of stability of a stable polynomial. *SIAM J. Num. Anal.*, **7**, 538–544.

Henrici, P. (1974). *Applied and Computational Complex Analysis*, volume 1, New York, J. Wiley.

Ho, C.-H., Yap, C. K. (1996). Pseudo-subresultants. *J. Symb. Comput.*, **21**, 1–14.

Knebusch, M., Scheiderer, C. (1989). *Einführung in die reelle Algebra*, Vieweg-Studium 63, Vieweg, Aufbaukurs Mathematik.

Krein, M. G., Naimark, M. A. (1936). The method of symmetric and hermitian forms in the theory of separation of roots of algebraic equation. Kharkov 1936 (in Russian). English translation. *Linear and Multi-linear Algebra (1981)*, **10**, 265–308.

Kung, H. T. (1974). On computing reciprocals of power series. *Numer. Math.*, **22**, 341–348.

Lazard, D. (1998). Sous-résultant. Unpublished manuscript.

Lickteig, T., Roy, M.-F. (1996). Cauchy index computation. *Calcolo*, **33**, 337–351.

Loos, R. (1982). Generalized polynomial remainder sequences. In *Computer Algebra, Symbolic and Algebraic Computation*, Berlin, Springer-Verlag.

Moenck, R. T. (1973). Fast computation of GCDs. *Proceedings STOC '73*, 142–151.

Quitté, C. (1998). Une démonstration de l'algorithme de Bareiss par l'algèbre extérieur. Unpublished manuscript, Université de Poitier.

Reischert, D. (1997). Asymptotically fast computation of resultants. *Proceedings of ISSAC '97, Hawaii*. pp. 233–240. ACM Press.

Roy, M.-F. (1996). Basic algorithms in real algebraic geometry and their complexity: from Sturm's theorem to the existential theory of reals. In *Lectures on Real Geometry in Memoriam of Mario Raimondo*, de Gruyter Expositions in Mathematics, **23**, 1–67.
Schönhage, A. (1971). Schnelle Berechnung von Kettenbruchentwicklungen. *Acta Informatica*, **1**, 139–144.
Schönhage, A. (1982). Asymptotical fast algorithms for the numerical multiplication and division of polynomials with complex coefficients. In *Proceedings, EUROCAM '82*, Marseille.
Schönhage, A., Strassen, V. (1971). Schnelle Multiplikation großer Zahlen. *Computing*, **7**, 281–292.
Sieveking, M. (1972). An algorithm for division of power series. *Computing*, **10**, 153–156.
Strassen, V. (1983). The computational complexity of continued fractions. *SIAM J. Comp.*, **12/1**, 1–27.
Sturm, C. (1835). Mémoire sur la résolution des équations numériques. *Inst. France Sc. Math. Phys.*, **6**.
Sylvester, J. J. (1835). On a theory of syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's function. *Trans. Roy. Soc. London*.
Thull, K., Yap, C. K. (1990). A Unified Approach to HGCD Algorithms for Polynomials and Integers. Preprint: `http://cs.nyu.edu/yap/papers`.
Yap, C. K. (1999). *Fundamental Problems in Algorithmic Algebra*, Oxford, Oxford University Press.

Originally Received 1 December 1997
Accepted 25 August 2000
Published electronically 24 January 2001