New structure theorem for subresultants *

Henri Lombardi, Marie-Françoise Roy and Mohab Safey El Din

November 10, 1999

Abstract

We give a new structure theorem for subresultants precising their gap structure and derive from it a new algorithm for computing them. If d is a bound on the degrees and τ a bound on the bitsize of the minors extracted from Sylvester matrix, our algorithm has $O(d^2)$ arithmetic operations and size of intermediate computations 2τ. The key idea is to precise the relations between the successive Sylvester matrix of A and B in one hand and of A and XB on the other hand, using the notion of G-remainder we introduce. We also compare our new algorithm with another algorithm with the same characteristics already appeared in [4].

Introduction

Let A and B be two univariate polynomials with degree $\leq d$. Subresultants are polynomials having as coefficients minors extracted from the Sylvester matrix of A and B. So it is possible to compute them using Jordan-Bareiss method, with $O(d^3)$ arithmetic operations. If τ is the maximal bitsize of the coefficients of the subresultants of A and B (in the case of integer coefficients), Jordan-Bareiss's method produces intermediate results of bitsize 2τ.

On the other hand, the classical subresultant algorithm, which uses more fully the special structure of Sylvester matrix and the connections between subresultants and polynomials in the remainder sequence of A and B, computes the subresultants in $O(d^2)$ arithmetic operations, which is optimal since the size of the output is $O(d^2)$. Unfortunately, when there are gaps in degrees in the remainder sequence, the size of the integers in the intermediate computations of the classical subresultant algorithm are not in $O(\tau)$. Even when there are no gaps of degrees, the size of the integers in the intermediate computations of the classical subresultant algorithm is bounded by 3τ rather than 2τ.

In this paper we describe an algorithm which, neglecting linear factors, performs $2d^2$ arithmetic operations with size of intermediate computations at most $2\tau + 1$. The key idea is to precise the relations between the successive Sylvester matrix of A and B in one hand and of A and XB on the other hand, using the notion of G-remainder (see Section 1). We establish a new structure theorem describing these relations, a new gap structure, and deduce from it a new algorithm. We also compare our new algorithm with another algorithm with the same characteristics already appeared in [4].

*second and third author supported in part by the project ESPRIT-LTR 21.024 FRISCO.

1 Some linear algebra on polynomials

Let $\mathbf{D}$ be a domain and $\mathbf{K}$ its fraction field. Consider the $\mathbf{K}$-vector space $\mathcal{F}$ of polynomials of degree $< n$ equipped with the basis $\mathcal{E} = [X^{n-1}, \ldots, X, 1]$. A sequence of polynomials $\mathcal{A} = [A_1, \ldots, A_m]$, with $m \leq n$ can be seen as a matrix whose rows are the coordinates of the A_i's on the basis $\mathcal{E}$. The polynomial A_i is identified with the row vector of its coefficients in the basis $\mathcal{E}$. So we shall speak of the *degree of a row* and the *leading coefficient* of a row using this identification. We suppose that the coefficients of the A_i belong to $\mathbf{D} \subset \mathbf{K}$.

Elementary row replacements and r-reduced forms
An *elementary row replacement* of $\mathcal{A}$ is the replacement of a row A_i by a row $A_i + \Sigma_{j<i}\alpha_{i,j}A_j$ ($\alpha_{i,j} \in \mathbf{K}$). We denote $\mathcal{A} \sim_r \mathcal{A}'$ to indicate that $\mathcal{A}'$ is obtained from $\mathcal{A}$ by a finite sequence of elementary row replacements and say that $\mathcal{A}$ is r-equivalent to $\mathcal{A}'$. Note that $\sim_r$ is indeed an equivalence relation.

A *reverse* sequence of elementary row replacements has the following form: first, an elementary row replacement transforming the last row; second, an elementary row replacement transforming the $(m-1)$-th row, ... Any sequence of elementary row replacements can be easily replaced by a reverse sequence of elementary row replacements.

A matrix is *r-reduced* is all its non zero rows have distinct degrees. An *r-reduced form* of $\mathcal{A}$ is a matrix r-equivalent to $\mathcal{A}$ which is r-reduced. An elementary row replacement does not change the rank of the matrix. So the number of non zero polynomials in an r-reduced form of $\mathcal{A}$ is equal to the rank of $\mathcal{A}$.

Proposition 1.1 *Let $\mathcal{A}'$ and $\mathcal{A}''$ be two r-reduced forms of $\mathcal{A} = [A_1, \ldots, A_m]$. Call A'_i, A''_i the row of index i in $\mathcal{A}', \mathcal{A}''$.*
a) The rows of $\mathcal{A}'$ and the rows of $\mathcal{A}''$ have same degrees and same leading coefficients. The leading coefficients of the non zero rows of $\mathcal{A}'$ and $\mathcal{A}''$ are called the r-pivots *of $\mathcal{A}$. The corresponding degree is called the degree of the r-pivot.*
b) The rows of smallest degree of $\mathcal{A}'$ and $\mathcal{A}''$ are equal.
c) More generally, two non zero rows A'_i and A''_i have equal coefficients from the leading one (of degree d_i) down to the one of degree $k+1$ where k is the biggest degree of r-pivots with degree $< d_i$ in the previous rows.
d) These coefficients are – up to signs – quotients of minors extracted from $\mathcal{A}$.

Proof: Elementary row replacements do not change the following property: the i-th row is a linear combination of the previous ones. On the other hand, in an r-reduced matrix, the i-th row is zero if and only if it is a linear combination of the previous ones. So, $A'_i = 0 \iff A''_i = 0$. Now, without loss of generality, consider a reverse sequence of elementary row replacements transforming $\mathcal{A}'$ in $\mathcal{A}''$. When transforming A'_i (of degree d_i) in A''_i we can only modify coefficients of degrees $\leq k$, where k is the biggest degree of pivots with degree $< \deg(A'_i)$ in the previous rows. So $\deg(A''_i) = \deg(A'_i)$, d_i is well defined and a), b) and c) are clear.

d) First remark that rows that are r-reduced to 0 are not needed in elementary row replacements: replace, in an elementary row replacement involving one of these rows, the row by a suitable linear combination of preceeding rows. So we assume w.l.o.g. that $\mathcal{A}$ has full rank m. Remark also that elementary row replacements do not change $(s \times s)$-minors involving the first s rows and any choice for the s columns. So we can consider minors of $\mathcal{A}'$. Call p_ℓ the pivot on the row A'_ℓ. Then the product $\prod_{k=1}^{i-1} p_k$ is equal, up to sign, to the suitable minor involving the

columns of degrees $d_1, \ldots, d_{i-1}$. Let j a degree $\in \{i, \ldots, k+1\}$ with i and k as in d). Let α be the corresponding coefficient of A'_i. Then the product $\alpha \times \prod_{k=1}^{i-1} p_k$ is equal, up to sign, to the suitable minor involving the columns of degrees $d_1, \ldots, d_{i-1}, j$. So the result is clear. □

Note that this proof doesn't use commutativity (except for d)): it works when replacing $\mathbf{K}$ by a division ring. It gives a constructive theory of dimension for finitely generated sub(left)modules of a free (left) module over a division ring.

Definition 1.2 *The* least degree polynomial generated by $\mathcal{A} = [A_1, \ldots, A_m]$, *denoted by* $\mathrm{ldPol}(\mathcal{A})$ *is the polynomial of smallest degree in an r-reduced form of* $\mathcal{A}$, *i.e. the zero polynomial if one row is zero, the polynomial corresponding to the least degree row otherwise.*
The deviation *of* $\mathcal{A}$, *denoted by* $\delta(\mathcal{A})$ *is the difference between* m *and the index of the row of* $\mathrm{ldPol}(\mathcal{A})$ *in any r-reduced form of* $\mathcal{A}$ *(if* $\mathrm{ldPol}(\mathcal{A})$ *is zero, the difference between* m *and the smallest index of a zero vector in an r-reduced form of* $\mathcal{A}$*).*
The minor extracted on the first $m-1$ *columns of* $\mathcal{A}$ *and the* $m-1$ *rows obtained by removing the row of index* $m - \delta(\mathcal{A})$ *is denoted by* $\mu(\mathcal{A})$.
The matrix $\mathcal{A}$ *is said to be* non defective *if* $\mathrm{ldPol}(\mathcal{A})$ *has degree* $n-m$, *i.e., if the* $m \times m$*-minor extracted on the first columns is non zero.*

Note that $\mathrm{ldPol}(\mathcal{A})$ is always of degree $\leq n-m$ since when $\mathrm{ldPol}(\mathcal{A}) \neq 0$ an r-reduced form of $\mathcal{A}$ has no two rows of same degrees.

Remark that if $m < n$ claiming $\mathcal{A}$ to be non defective is stronger than "$\mathcal{A}$ has full rank m". In case of a square matrix ($m = n$) we get the usual notion of a regular square matrix.

As proved in Proposition 1.1, if $\mathcal{A} \sim_r \mathcal{A}'$ then $\mathrm{ldPol}(\mathcal{A}) = \mathrm{ldPol}(\mathcal{A}')$, $\delta(\mathcal{A}) = \delta(\mathcal{A}')$ and $\mu(\mathcal{A}) = \mu(\mathcal{A}')$

If $\mathcal{A} = [A_1, \ldots, A_m]$ and $\mathcal{B} = [B_1, \ldots, B_k]$, the notation $\mathcal{A}, \mathcal{B}$ means $[A_1, \ldots, A_m, B_1, \ldots, B_k]$. The following lemma is clear,

Lemma 1.3 *Let* $\mathcal{A} = [A_1, \ldots, A_m]$ *be a non-defective matrix, and consider* $\mathcal{B} = [B_1, \ldots, B_k]$ *such that* $m + k \leq n$ *and* $\deg(B_i) \leq n - m$, *then*

$$\mathrm{ldPol}(\mathcal{A}, \mathcal{B}) = \mathrm{ldPol}(\mathrm{ldPol}(\mathcal{A}), \mathcal{B}).$$

Moreover if $\deg(B_i) < n - m$,

$$\mathrm{ldPol}(\mathcal{A}, \mathcal{B}) = \mathrm{ldPol}(\mathcal{B}).$$

Polynomial determinants

Definition 1.4 *Let* $\mathcal{A} = [A_1, \ldots, A_m]$ *be polynomials in the basis* $X^{n-1}, \ldots, 1$ *with* $m \leq n$. *Denote by* μ_j *the* $m \times m$ *minor extracted on the columns* $1, \ldots, m-1, n-j$. *The* polynomial determinant *of* $\mathcal{A}$ *denoted by* $\mathrm{DetPol}(\mathcal{A})$ *is the polynomial defined by:*

$$\mathrm{DetPol}(\mathcal{A}) := \sum_{j \leq n-m} \mu_j X^j$$

Note that elementary row replacements do not change the polynomial determinant.

The following holds:

Lemma 1.5 *Let $\mathcal{A} = [A_1, \ldots, A_m]$. Let $\mathcal{M}$ be the $m \times m$ matrix whose $m-1$ first columns are the $m-1$ first columns of $\mathcal{A}$ and the elements of the last column are the polynomials $A_1, \ldots, A_m$. Then*

$$\mathrm{DetPol}(\mathcal{A}) = \mathrm{Det}(\mathcal{M}).$$

Proof: It is clear that $\mathrm{Det}(\mathcal{M}) := \sum_{j \leq n} \mu_j X^j$ where μ_j is the $m \times m$ minor obtained taking the columns of index $1, \ldots, m-1, n-j$ of $\mathcal{A}$ for $j = 1, \ldots, n$. For $j > n-m$, $\mu_j = 0$ since it is the determinant of a matrix with two equal columns. □

Lemma 1.5 shows that $\mathrm{DetPol}(\mathcal{A})$ is a linear combination of the A_i with coefficients equal (up to sign) to minors $(m-1) \times (m-1)$ extracted on the $m-1$ first columns of $\mathcal{A}$. It is thus a polynomial of the **D**-module generated by the A_i's.

Note that if $\mathcal{A} \sim_r \mathcal{A}'$, $\mathrm{DetPol}(\mathcal{A}) = \mathrm{DetPol}(\mathcal{A}')$. So considering an r-reduced form $\mathcal{A}'$ of $\mathcal{A}$, we get:

Lemma 1.6 *Let $\mathcal{A} = [A_1, \ldots, A_m]$.*

a) We have the following identity

$$\mathrm{DetPol}(\mathcal{A}) = (-1)^{\delta(\mathcal{A})} \mu(\mathcal{A}) \, \mathrm{ldPol}(\mathcal{A}).$$

b) The polynomial $\mathrm{DetPol}(\mathcal{A})$ *is zero in the two following cases: either* $\mathrm{ldPol}(\mathcal{A}) = 0$ *or* $\mu(\mathcal{A}) = 0$.

c) The matrix $\mathcal{A}$ is non defective if and only if any r-reduced form contains a polynomial in each degree $n-m, ..., n$. This is also equivalent to $\deg(\mathrm{ldPol}(\mathcal{A})) = n-m$.

d) If $\mathcal{B} = [A_1, \ldots, A_{m-1}]$ is non defective, then the deviation of $\mathcal{A}$ equals 0,

$$\mathrm{DetPol}(\mathcal{A}) = \mu(\mathcal{A}) \, \mathrm{ldPol}(\mathcal{A})$$

and $\mu(\mathcal{A})$ equals the coefficient of degree $n-m+1$ of $\mathrm{DetPol}(\mathcal{B})$.

e) The matrix $\mathcal{A}$ has full rank m if and only if $\mathrm{ldPol}(\mathcal{A}) \neq 0$.

G-remainder of two polynomials.
Let A and B be two polynomials of degree p and q ($q \leq p$) with leading coefficients a and b and $\mathrm{Rem}(A, B)$ their remainder. If $\mathcal{B}$ is the matrix $[B, XB, \ldots, X^{p-q}B, A]$ then it is clear that the matrix $[B, XB, \ldots, X^{p-q}B, \mathrm{Rem}(A, B)]$ is an r-reduced form of $\mathcal{B}$, so $\mathrm{ldPol}(\mathcal{B}) = \mathrm{Rem}(A, B)$. In a similar way we give the following definition.

Definition 1.7 *Let A and B be two polynomials of degree p and q ($q \leq p$). Let $\mathcal{A} = [A, B, XB, \ldots, X^{p-q}B]$. The* G-remainder of A divided by B, *denoted by* $\mathrm{GRem}(A, B)$, *is the least degree polynomial generated by $\mathcal{A}$,* $\mathrm{ldPol}(\mathcal{A})$.

It is clear that $G = \mathrm{GRem}(A, B)$ is characterized by the equality $cA = QB - G$ with Q monic, $c \in \mathbf{K}$ and $\deg(G) < q$. Thus

$$a\mathrm{GRem}(A, B) = -b\mathrm{Rem}(A, B).$$

Note that $\mathrm{Rem}(\alpha A, \beta B) = \alpha \mathrm{Rem}(A, B)$ and $\mathrm{GRem}(\alpha A, \beta B) = \beta \mathrm{GRem}(A, B)$.

Denote by $\mathrm{PRem}(A, B) = \mathrm{Rem}(b^{p-q+1}A, B)$ the *pseudo-remainder* of A and B. The polynomial determinant of $\mathcal{A} = [A, B, XB, \ldots, X^{p-q}B]$ is $\varepsilon_{p-q+1}\mathrm{PRem}(A, B)$ and the polynomial determinant of $\mathcal{B} = [B, XB, \ldots, X^{p-q}B, A]$ is $\varepsilon_{p-q}\mathrm{PRem}(A, B)$, where $\varepsilon_m = (-1)^{m(m+1)/2}$.

Example 1.8 Suppose

$$\begin{aligned} A &= a_5X^5 + a_4X^4 + \cdots \qquad \ldots + a_0 \\ B &= b_3X^3 + b_2X^2 + \cdots \qquad \ldots + b_0 \end{aligned}$$

An r-reduced form of

$$\mathcal{A} = \begin{bmatrix} a_5 & a_4 & \cdot & \cdot & \cdot & a_0 \\ 0 & 0 & b_3 & b_2 & \cdot & b_0 \\ 0 & b_3 & b_2 & \cdot & b_0 & 0 \\ b_3 & b_2 & \cdot & b_0 & 0 & 0 \end{bmatrix} \begin{matrix} A \\ B \\ XB \\ X^2B \end{matrix}$$

is

$$\begin{bmatrix} a_5 & a_4 & \cdot & \cdot & \cdot & a_0 \\ 0 & 0 & b_3 & b_2 & \cdot & b_0 \\ 0 & b_3 & b_2 & \cdot & b_0 & 0 \\ 0 & 0 & 0 & c_2 & c_1 & c_0 \end{bmatrix} \begin{matrix} A \\ B \\ XB \\ C \end{matrix}$$

with $C = \mathrm{GRem}(A, B)$.

Note that in G-remainder, G comes from "Gauss pivoting", which is in fact an old chinese technique. But to call it "chinese remainder" would be in conflict with the tradition (Chinese Remainder Theorem).

2 First structure theorem

Let A and B be two polynomials of degrees p and q. Denote by a the leading coefficient of A and b the leading coefficient of B. We define the Sylvester-Habicht matrices associated to A and B, the signed subresultants of A and B and some related notions.

Notation 2.1 Let A and B be two polynomials of degrees p and q. Let $0 \leq j \leq \inf(p, q) - 1$.
The *j-th Sylvester-Habicht matrix* of A and B, denoted by $\mathcal{H}_j(A, B)$ or $\mathcal{H}_j$ is the matrix associated to $[X^{q-j-1}A, \ldots, A, B, \ldots, X^{p-j-1}B]$. It has $p+q-2j$ rows and $p+q-j$ columns,
The least degree polynomial generated by $\mathcal{H}_j$ is denoted by G_j, and g_j is its leading coefficient.
The minor $\mu(\mathcal{H}_j)$ is denoted by μ_j and the deviation of $\mathcal{H}_j$ is denoted by δ_j.
The *j-th signed subresultant of A and B*, denoted by $H_j(A, B)$ or H_j is the polynomial determinant of $\mathcal{H}_j$. The polynomial H_j is of degree $\leq j$.
The *j-th signed subresultant coefficient of A and B*, denoted by $h_j(A, B)$ or h_j is the coefficient of degree j of H_j, $\mathrm{coef}_j(H_j)$. If H_j is defective, $h_j = 0$.
The leading coefficient of $H_j \neq 0$, $\mathrm{lc}(H_j)$ is denoted by $\overline{h}_j$. If H_j is non defective, $\overline{h}_j = h_j$.

In order to make things more visible see the following picture (to be compared with the picture corresponding to the definition of usual non signed subresultants)

$$\begin{aligned} A &= a_pX^p + a_{p-1}X^{p-1} + a_{p-2}X^{p-2} + \cdots + a_0, \\ B &= b_qX^q + b_{q-1}X^{q-1} + \cdots + b_0 \end{aligned}$$

then if $p = q + 1$ the matrix $\mathcal{H}_j$ has the shape

$$\mathcal{H}_j = \underbrace{\begin{pmatrix} a_p & \cdots & \cdots & \cdots & \cdots & a_0 & & \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & a_p & \cdots & \cdots & \cdots & \cdots & a_0 \\ & & & b_q & \cdots & \cdots & \cdots & b_0 \\ & & b_q & \cdots & \cdots & \cdots & b_0 & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & & \\ b_q & \cdots & \cdots & \cdots & b_0 & & & \end{pmatrix}}_{p+q-j} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\end{matrix}}\right\} q-j \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\end{matrix}}\right\} p-j \end{matrix}$$

and is a submatrix of the full Sylvester-Habicht matrix $\mathcal{H}_0$.

The matrix $\mathcal{H}_j$ is non defective if and only if $h_j \neq 0$. In this case, G_j is of degree j.

We complete these "usual" definitions by a useful convention for index $\inf(p, q)$.

Convention 2.2 Let $\varepsilon_m = (-1)^{m(m+1)/2}$.
If $p > q$ we let $\mathcal{H}_q = [B, \ldots, X^{p-1-q}B]$, so $G_q = B$, $H_q = \varepsilon_{p-1-q} b_q^{p-1-q} B$ (note that $\mathcal{H}_q$ is non defective and $h_q = \varepsilon_{p-1-q} b_q^{p-q}$).
If $p = q$ we let $G_q = B$, $H_q = b_q^{-1}B$ and we let "$\mathcal{H}_q$ is non defective, $h_q = 1$".
If $p < q$ we let $\mathcal{H}_p = [X^{q-1-p}A, \ldots, A]$, so $G_p = A$, $H_p = a_p^{q-1-p}A$ (note that $\mathcal{H}_p$ is non defective and $h_p = a_p^{q-p}$).

We have the following Bezout identity for G_j.

Lemma 2.3 *Let $0 \leq j \leq \inf(p, q) - 1$. Let δ_j be the deviation of $\mathcal{H}_j$. There is an identity*

$$G_j = U_j A + V_j B$$

with U_j of degree equal to $q - j - 1 - \delta_j$ and V_j monic of degree equal to $p - j - 1 - \delta_j$.

Proof If the deviation of $\mathcal{H}_j$ is δ_j, G_j is on the row of index $p + q - 2j - \delta_j$ corresponding to the polynomial $X^{p-j-1-\delta_j}B = X^{k_0}B$. So we may delete the rows that follow, but also the first rows $X^m A$ corresponding to lines of too high degree ($> q + k_0$). So there are $\beta_k \in \mathbf{K}$, for $k < p - j - 1 - \delta_j$ and $\alpha_k \in \mathbf{K}$, $k \leq q - j - 1 - \delta_j$ with

$$G_j = X^{p-j-1-\delta_j}B + \sum_{k<p-j-1-\delta_j} \beta_k X^k B + \sum_{k\leq q-j-1-\delta_j} \alpha_k X^k A$$

We take $U_j = \sum_{k\leq q-j-1-\delta_j} \alpha_j X^j$, $V_j = X^{p-j-1-\delta_j} + \sum_{k<p-j-1-\delta_j} \beta_k X^k$. We see that U_j has exactly degree $d = q - j - 1 - \delta_j$: $\alpha_d = -b/a$. □

The results in the following proposition 2.5 relate the least degree polynomial generated by Sylvester matrices and the G-remainders.

In order to best understand what happens, we show first an example.

Example 2.4 (see notations 2.1). Suppose that A is of degree 8 and of leading coefficient a, B of degree 7 and of leading coefficient b. We have $\mathcal{H}_7 = [B], H_7 = G_7 = B, h_7 = b$.

The polynomial $\mathrm{GRem}(A, B)$ is of expected degree 6, suppose that in fact $\mathrm{GRem}(A, B)$ is of degree 4. The matrix $\mathcal{H}_6$ associated to $[A, B, XB]$ has as r-reduced form

$$\mathcal{G}_6 = \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot \end{bmatrix} \begin{matrix} A \\ B \\ \mathrm{GRem}(A, B) \end{matrix}$$

with $G_6 = \mathrm{GRem}(A, B) = g_6X^4 + \cdots$. Also $\mu_6 = ab$, $\delta_6 = 0$ and $H_6 = abG_6$, $\overline{h}_6 = abg_6$.

Since the matrix $\mathcal{H}_5$ associated to $[XA, A, B, XB, X^2B]$ contains the matrices $\mathcal{H}_6$ and $X\mathcal{H}_6$ it gives by elementary row replacements the following r-reduced matrix

$$\mathcal{G}_5 = \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot & 0 \end{bmatrix} \begin{matrix} XA \\ A \\ B \\ G_6 \\ XG_6 \end{matrix}$$

and $G_5 = G_6$. We have $\mu_5 = 0$, $H_5 = 0$.

Since the matrix $\mathcal{H}_4$ associated to $[X^2A, XA, A, B, XB, X^2B, X^3B]$ contains the matrices $\mathcal{H}_6$, $X\mathcal{H}_6$ and $X^2\mathcal{H}_6$ it gives by elementary row replacements the following r-reduced matrix

$$\mathcal{G}_4 = \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot & 0 & 0 \end{bmatrix} \begin{matrix} X^2A \\ XA \\ A \\ B \\ G_6 \\ XG_6 \\ X^2G_6 \end{matrix}$$

and $G_4 = G_6$. We have $\mu_4 = -a^3bg_6^2$. Note that $h_4 = -a^3bg_6^3$, $\delta_4 = 2$, $H_4 = -a^2g_6^2H_6$ and the matrix $\mathcal{H}_4$ is non defective.

Since the matrix $\mathcal{H}_3$ associated to $[X^3A, \ldots, A, B, \ldots, X^4B]$ contains the matrices $\mathcal{H}_6$, $X\mathcal{H}_6$, $X^2\mathcal{H}_6$ and $X^3\mathcal{H}_6$, it gives by elementary row replacements the following matrix

$$\begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & 0 & 0 \\ 0 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & 0 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 0 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot & 0 & 0 & 0 \end{bmatrix} \begin{matrix} X^3A \\ X^2A \\ XA \\ A \\ B \\ G_6 \\ XG_6 \\ X^2G_6 \\ X^3G_6 \end{matrix}$$

So it has as r-reduced form

$$\mathcal{G}_3 = \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & 0 & 0 \\ 0 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & 0 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 0 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & g_3 & \cdot & \cdot & \cdot \end{bmatrix} \begin{matrix} X^3A \\ X^2A \\ XA \\ A \\ B \\ G_6 \\ XG_6 \\ X^2G_6 \\ \mathrm{GRem}(B, G_6) \end{matrix}$$

with $\mathrm{GRem}(B, G_6) = g_3X^3 + \cdots = G_3$. Observe that $H_3 = ah_4G_3$.

We denote by $[P, \mathcal{L}, Q]$ the sequence obtained from the sequence $\mathcal{L}$ and elements P and Q adding P at the head and Q at the tail.

Proposition 2.5 *(Notations 2.1 and convention 2.2) Let $0 \leq j \leq \inf(p, q)$. Supppose that $\mathcal{H}_j$ is non defective (in particular this works for $j = \inf(p, q)$).*

a) $H_{j-1} = ah_jG_{j-1}$, $\overline{h}_{j-1} = ah_jg_{j-1}$, $\mu_{j-1} = ah_j$, $\delta_{j-1} = 0$

b) If G_{j-1} is zero then G_j is a GCD of A and B.

c) If $G_{j-1} \neq 0$ is of degree k then $\mathcal{H}_k$ is non defective and

i) $G_{k-1} = \mathrm{GRem}(G_j, G_{j-1})$

Moreover if $k < j - 1$,

ii) $G_{j-1} = G_{j-2} = \ldots = G_{k+1} = G_k$

iii) $\mu_{j-2} = \ldots = \mu_{k+1} = 0$, $\mu_k = \varepsilon_{j-k-2}a^{j-k}h_jg_{j-1}^{j-1-k}$

iv) $\delta_{j-2} = 1$, $\delta_{j-3} = 2, \ldots,$ $\delta_k = j - 1 - k$

d) If $p \geq q$ then $G_{q-1} = \mathrm{GRem}(A, B)$. If $p \leq q$ then $G_{p-1} = \mathrm{Rem}(B, A)$.

Proof:
a) If $j = q = p$, by convention $h_q = 1$. In the other cases, since $\mathcal{H}_j$ is non defective and $\mathcal{H}_{j-1} = [X^{q-j-1}A, \mathcal{H}_j, X^{p-j-1}B]$, the deviation of $\mathcal{H}_{j-1}$ is 0, $\mu_{j-1} = ah_j$ and $H_{j-1} = ah_jG_{j-1}$ (see lemma 1.6 d) and example 2.4).

b) Since h_j is non zero, G_j is non zero (see lemma 1.6 a)). From lemma 2.3 we see that $\mathrm{GCD}(A, B)$ divides G_j and $\deg(\mathrm{GCD}(A, B)) \geq j$. The polynomial G_{j-1} is zero or of degree $\leq j - 1$. If G_{j-1} is zero, lemma 2.3 says that $U_{j-1}A = -V_{j-1}B$ with U_{j-1} of degree equal to $q-j$ and V_{j-1} monic of degree equal to $p-j$. The LCM of A and B is thus of degree $\leq p+q-j$. So the GCD of A and B is of degree j and equal to G_j.

c) Suppose now that G_{j-1} is non zero of degree $k \leq j - 1$.
The matrix $\mathcal{H}_{k-1}$ is r-equivalent to

$$[X^{q-k}A, \ldots, X^{q-j}A, \mathcal{H}_j, G_{j-1}, \ldots, X^{j-k}G_{j-1}],$$

thus

$$G_{k-1} = \mathrm{ldPol}(\mathcal{H}_{k-1}) =$$
$$\mathrm{ldPol}(X^{q-k}A, \ldots, X^{q-j}A, \mathcal{H}_j, G_{j-1}, \ldots, X^{j-k}G_{j-1}).$$

According to Lemma 1.3,

$$\mathrm{ldPol}(X^{q-k}A, \ldots, X^{q-j}A, \mathcal{H}_j, G_{j-1}, \ldots, X^{j-k}G_{j-1}) =$$
$$\mathrm{ldPol}(\mathrm{ldPol}(X^{q-k}A, \ldots, X^{q-j}A, \mathcal{H}_j), G_{j-1}, \ldots, X^{j-k}G_{j-1})$$
$$= \mathrm{GRem}(G_j, G_{j-1})$$

So

$$G_{k-1} = \mathrm{GRem}(G_j, G_{j-1}).$$

A simple computation shows that $\mu_k = \varepsilon_{j-k-2}a^{j-k}h_jg_j^{j-k-1}$.

If $k < j-1$, for $\delta = 0, \ldots, j-k-1$, the matrix $\mathcal{H}_{j-1-\delta}$ associated to

$$[X^{q-j-\delta}A, \ldots, X^{q-j}A, \mathcal{H}_j, G_{j-1}, \ldots, X^{\delta}G_{j-1}]$$

is r-equivalent to$\mathcal{H}_{j-1-\delta}$. So it is clear that the G-polynomial $\mathcal{G}_{j-1-\delta}$ is G_{j-1} and that the deviation of $\mathcal{G}_{j-1-\delta}$ is δ.
For every $\delta = 1, \ldots, j-k-2$, the row of index $p+q-2j+1+\delta$ in the matrix whose determinant is $\mu_{j-1-\delta}$ is zero, hence $\mu_{j-2} = \ldots = \mu_{k+1} = 0$.
d) This is clear. □

Algorithmic comment 2.6 In the preceeding proposition, since $\mathcal{H}_k$ is non defective as is $\mathcal{H}_j$ in the hypothesis we see that b), c) and d) allow to compute all the G_j's ($\inf(p,q) \geq j \geq 0$) from inputs A and B by using only the successive G-remainders.

Corollary 2.7 (size of Euclid's remainders [9]) *Assume $p \geq q$. When running the successive G-remainders algorithm, one gets polynomials $A = \widetilde{G}_1$, $B = \widetilde{G}_2$, $\widetilde{G}_3$, ..., $\widetilde{G}_s = \mathrm{GCD}(A,B)$, whose coefficients are equal to quotients of minors extracted form the Sylvester Matrix. Let $d_j = \deg(\widetilde{G}_j)$. In case of integer polynomials, let $\lambda_j = 2(p+q-2d_j)$ and τ be a bound for the size of $\| A \|_2$ and $\| B \|_2$. Then the size of each coefficient of $\widetilde{G}_j$ is bounded by $\lambda_j\tau$ which is an $\mathrm{O}((p-d_j)\tau)$,*
Let us denote $\widetilde{g}_j$ the leading coefficient of $\widetilde{G}_j$. When running Euclidean algorithm (successive remainders algorithm), one gets polynomials A, B, $\widetilde{R}_3$, ..., $\widetilde{R}_s$. We have for $k \geq 1$

$$\widetilde{R}_{2k+1} = \frac{\widetilde{g}_1 \cdots \widetilde{g}_{2k-1}}{\widetilde{g}_2 \cdots \widetilde{g}_{2k}} \widetilde{G}_{2k+1}$$

and

$$\widetilde{R}_{2k+2} = \frac{\widetilde{g}_2 \cdots \widetilde{g}_{2k}}{\widetilde{g}_3 \cdots \widetilde{g}_{2k+1}} \widetilde{G}_{2k+2}$$

In case of integer polynomials, the size of each coefficient of $\widetilde{R}_j$ is bounded by $2(j(p+q)-2(d_1+\cdots+d_j))\tau$ which is an $\mathrm{O}((p-d_j)^2\tau)$.

Proof Easy consequence of propositions 1.1 and 2.5 and of the relation between a remainder and a G-remainder. □

The first structure theorem of subresultants [9], which is a refinement of the famous Subresultant Theorem (cf. [1, 2, 3, 4, 5, 7, 8, 10, 11]), is the following one.

Theorem 2.1 (First structure theorem) *We use notations 2.1 and convention 2.2. Let $0 \leq j \leq \inf(p,q)$. Supppose that $\mathcal{H}_j$ is non defective (in particular this works for $j = \inf(p,q)$).*

a) If H_{j-1} is zero then H_j is a GCD of A and B.

b) If $H_{j-1} \neq 0$ is of degree k then $\mathcal{H}_k$ is non defective and

i) $h_j^2 H_{k-1} = -\mathrm{Rem}(\overline{h}_{j-1}h_k H_j, H_{j-1})$.

More precisely,

$$h_j^2 H_{k-1} = -\overline{h}_{j-1}h_k H_j - C_j H_{j-1},$$

with $C_j \in \mathbf{D}[X]$.

Moreover if $k < j-1$,

ii) $H_{j-2} = \ldots = H_{k+1} = 0$

iii) $h_k = \varepsilon_{j-k-1}\frac{\overline{h}_{j-1}^{j-k}}{h_j^{j-k-1}}$, $\overline{h}_{j-1}H_k = h_k H_{j-1}$, *i.e.* $H_k = \varepsilon_{j-k-1}\left(\frac{\overline{h}_{j-1}}{h_j}\right)^{j-k-1} H_{j-1}$

c) If $p \geq q$ *then* $h_q = \varepsilon_{p-q-1} b^{p-q}$ *and* $H_{q-1} = a h_q G_{q-1} = \mathrm{GRem}(A, a h_q B) = \mathrm{DetPol}(\mathcal{H}_{q-1})$.
If $p < q$ *then* $h_p = a^{q-p}$ *and* $H_{p-1} = a h_p G_{p-1} = \mathrm{Rem}(a h_p B, A) = \mathrm{DetPol}(\mathcal{H}_{p-1})$.

Remark 2.8 The proportionality between H_{j-1} and H_k and the identity

$$h_j^2 H_{k-1} = -\mathrm{Rem}(\overline{h}_{j-1} h_k H_j, H_{j-1}),$$

is the only ingredient necessary to establish the connection between the H_j and the Cauchy index which is the basis of all the results needed for real root counting by using Sturm-Habicht sequences (see [6]).

Proof
c) If $p \geq q$, since $G_{q-1} = \mathrm{GRem}(A, B)$ and $H_{q-1} = a h_q G_{q-1}$ we get $H_{q-1} = \mathrm{GRem}(A, a h_q B)$. Similar computation in the other case.
a) follows from proposition 2.5 a) and b).
b) i) According to proposition 2.5

$$G_{k-1} = \mathrm{GRem}(G_j, G_{j-1})$$

and H_k is of degree k. Multiplying both sides by $a h_j^2 h_k$ which is non zero, noting that

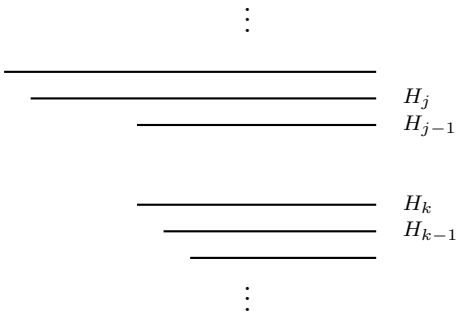
$$H_{j-1} = a h_j G_{j-1}, \quad H_{k-1} = a h_k G_{k-1},$$

and using the relationship between remainder and G-remainder we get

$$h_j^2 H_{k-1} = \mathrm{GRem}(H_j, h_k h_j H_{j-1}) = -\mathrm{Rem}(\overline{h}_{j-1} h_k H_j, H_{j-1}).$$

The fact that the quotient of the division of $\overline{h}_{j-1} h_k H_j$ by H_{j-1} belongs to $\mathbf{D}[X]$ is proved in [9], see also [6].
ii) For $\delta = 1, \ldots, j-k-2$ we have $H_{j-1-\delta} = 0$ since $\mu_{j-1-\delta} = 0$.
iii) This is a consequence of the preceeding results since $a h_j g_{j-1} = \mu_{j-1} g_{j-1} = \overline{h}_{j-1}$.
□

The signed subresultants present the famous *gap structure*, graphically displayed by the following diagram of Habicht lines: H_{j-1} and H_k are proportional, of degree k, $H_{j-2}, \ldots, H_{k+1}$ are zero.



Remark 2.9 In the non defective case, theorem 2.1 is the classical subresultant theorem (except for the signs). In the defective case the improvement with respect to the classical subresultant theorem comes from the fact that the quotient of the division of $\overline{h}_{j-1} h_k H_j$ by H_{j-1} belongs to $\mathbf{D}[X]$ ([9], see also [6]).

The following proposition due to Lazard [8] will give when $k < j-1$ an improved way of computing H_k starting from H_{j-1}.

Proposition 2.10 *Let $\mathcal{H}_j$ be non defective. Let k be the degree of H_{j-1} and assume $k < j-1$. Define*

$$\overline{H}_{j-2} = -\frac{\overline{h}_{j-1} \cdot H_{j-1}}{h_j},$$
$$\overline{H}_{j-\delta-1} = (-1)^{\delta} \frac{\overline{h}_{j-1} \cdot \overline{H}_{j-\delta}}{h_j}, \quad \text{for } \delta = 2, \ldots, j-k-1,$$

then all these polynomials are in $\mathbf{D}[X]$ and $H_k = \overline{H}_k$

Proof : Remark that $\overline{h}_{j-1}/h_j = a g_{j-1}$. Replace the δ last rows of $\mathcal{H}_{j-1-\delta}$ by G_{j-1}, XG_{j-1}, $\ldots$, $X^{\delta-1}G_{j-1}$ and add $j-k-1-\delta$ rows $X^{k+\delta+1}, \ldots, X^j$ to obtain a matrix $\overline{\mathcal{H}}_{j-1-\delta}$. It is easy to see that the polynomial determinant of $\overline{\mathcal{H}}_{j-1-\delta}$ is $\overline{H}_{j-1-\delta}$. □

Example 2.11 Following example 2.4 the matrix $\mathcal{H}_5$ has as r-reduced form of the matrix

$$\mathcal{G}_5 = \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot & 0 \end{bmatrix} \begin{matrix} XA \\ A \\ B \\ G_6 \\ XG_6 \end{matrix}$$

The matrix $\overline{\mathcal{H}}_5$ is

$$\begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{matrix} XA \\ A \\ B \\ G_6 \\ XG_6 \\ X^6 \end{matrix}$$

$\overline{H}_5 = -(\overline{h}_6/b)H_6 = -(ag_6)H_6 = -(ag_6)(abG_6) = \mathrm{DetPol}(\overline{\mathcal{H}}_5)$

¿From Theorem 2.1, Remark 2.9 and Proposition 2.10, it is easy to produce an algorithm [9] computing the signed subresultants with $O(d^2)$ arithmetic operations and size of intermediate computations (in the case of polynomials with integer coefficients) bounded by 3τ, where τ is the maximal bit size of a minor extracted from Sylvester matrix, which is an improvement of the classical subresultant algorithm in the defective case.

Improved Subresultant Algorithm

Input A and B two polynomials of degrees p and q

Output Subresultants H_j (notations 2.1, and convention 2.2).

Initialization

- If $p > q$ let $j \leftarrow q$, $h_q \leftarrow \varepsilon_{p-q-1} b^{p-q}$, $H_q \leftarrow \varepsilon_{p-q-1} b^{p-q-1} B$, $H_{q-1} \leftarrow -\mathrm{Rem}(bh_q A, B)$.
- If $p = q$ let $j \leftarrow q$, $h_q \leftarrow 1$, $H_{q-1} \leftarrow -\mathrm{Rem}(bA, B)$.
- If $p < q$ let $j \leftarrow p$, $h_p \leftarrow a^{q-p}$, $H_p \leftarrow a^{q-p-1} A$, $H_{p-1} \leftarrow \mathrm{Rem}(ah_p B, A)$.

- If $H_{j-1} = 0$ the computation is over, else let $k \leftarrow \deg(H_{j-1})$

Main loop

- Input : $h_j \neq 0$, H_j of degree j, H_{j-1} of degree $k \leq j$
- Output : $h_k \neq 0$, H_k, of degree k, H_{k-1} of degree $\leq k-1$.
- If $k = j-1$ let $H_{k-1} \leftarrow -\mathrm{Rem}(h_{j-1}^2 H_j, H_{j-1})/h_j^2$
  (if $p = q = j$ $H_{q-2} \leftarrow -\mathrm{Rem}(h_{q-1}^2 B, H_{q-1})/b$)
  { H_k is known since $k = j-1$ }
- If $k < j-1$
  - $\overline{h}_{j-1} \leftarrow \mathrm{lc}(H_{j-1})$
  - Computation of h_k :
    - For δ from 1 to $j-k-1$: $\overline{h}_{j-\delta-1} \leftarrow (-1)^\delta(\overline{h}_{j-1} \cdot \overline{h}_{j-\delta})/h_j$,
    - $h_k \leftarrow \overline{h}_k$
  - Computation of H_k : $H_k \leftarrow (h_k \cdot H_{j-1})/\overline{h}_{j-1}$
  - Computation of H_{k-1} : $H_{k-1} \leftarrow -\mathrm{Rem}(\overline{h}_{j-1} h_k H_j, H_{j-1})/h_j^2$
    (if $p = q = j$ $H_{k-1} \leftarrow -\mathrm{Rem}(\overline{h}_{q-1} h_k B, H_{j-1})/b$)
- If $H_{k-1} = 0$ the algorithm is over. Otherwise let $j \leftarrow k$, $k \leftarrow \deg(H_{k-1})$.

3 Second structure theorem

The second structure theorem presented in this section will improve the subresultant algorithm also in the non defective case.

The main idea is to consider also the Sylvester-Habicht matrices of A and XB

Notation 3.1 Let $0 \leq j \leq \inf(p-1, q)$. We denote by $\mathcal{H}_j^\star$ the matrix associated to $[X^{q-j}A, \ldots, A, XB, \ldots, X^{p-j}B]$.
We denote by $G_j^\star$ the least degree polynomial generated by $\mathcal{H}_j^\star$ and $g_j^\star$ its leading coefficient. The matrix $\mathcal{H}_j^\star$ has $p+q-2j+1$ rows and $p+q-j+1$ columns, its polynomial determinant $H_j^\star$ is of degree $\leq j$. We denote by $h_j^\star$ the coefficient of degree j of $H_j^\star$. If $H_j^\star$ is defective, $h_j^\star = 0$. The leading coefficient of $H_j^\star \neq 0$, $\mathrm{lc}(H_j^\star)$ is denoted by $\overline{h}_j^\star$. If $H_j^\star$ is non defective, $\overline{h}_j^\star = h_j^\star$.

We make moreover the following convention.

Convention 3.2 If $p > q$ then we let $\mathcal{H}_q = [B, \ldots, X^{p-1-q}B]$ as in convention 2.2. Moreover we let $h_{q+1}^\star = 1$ (so "$H_{q+1}^\star$ is non defective").
If $p \leq q$ then we let $\mathcal{H}_p^\star = [X^{q-p}A, \ldots, A]$ as in convention 2.2, so $G_p^\star = A$, $H_p^\star = a^{q-p}A$ and $h_p^\star = a^{q-p+1}$. Moreover we let $h_p = 1$ (so "H_p is non defective")

Remark that in this convention, $h_p = 1$ may disagree with the convention 2.2.

When $\mathcal{H}_j$ is defined, write $\mathcal{H}_j = [\mathcal{A}_j, \mathcal{B}_j]$ with $\mathcal{A}_j$ the submatrix made of the $X^k A$'s and $\mathcal{B}_j$ the submatrix made of the $X^k B$'s. In a similar way, write $\mathcal{H}_j^\star = [\mathcal{A}_j^\star, \mathcal{B}_j^\star]$. It is clear that

$$\mathcal{H}_{j-1} = [\mathcal{A}_j^\star, B, \mathcal{B}_j^\star] = [X^{q-j}A, \mathcal{H}_j, X^{p-j}B]$$

i.e., $\mathcal{H}_{j-1}$ is associated to the list of polynomals in $\mathcal{H}_j^\star$, with B inserted at the right place, and

$$\mathcal{H}_{j-1}^\star = [X\mathcal{A}_{j-1}, A, X\mathcal{B}_{j-1}] = [X^{q-j+1}A, \mathcal{H}_j^\star, X^{p-j+1}B]$$

i.e., $\mathcal{H}^\star_{j-1}$ is associated to the list of polynomals in $\mathcal{H}_{j-1}$ multiplied by X, with A inserted at the right place.
So we see that the sequence $\mathcal{H}_{j-1}$ contains as extracted sequences $\mathcal{H}^\star_j$ and $\mathcal{H}_j$. Similarly, the sequence $\mathcal{H}^\star_{j-1}$ contains as extracted sequences $\mathcal{H}^\star_j$ and $X\mathcal{H}_{j-1}$.

When $p > q$ we get the following increasing sequence of matrices extracted from $\mathcal{H}^\star_0$.

$$\mathcal{H}_q \subset \mathcal{H}^\star_q \subset \mathcal{H}_{q-1} \subset \mathcal{H}^\star_{q-1} \subset \mathcal{H}_{q-2} \subset \cdots \subset \mathcal{H}^\star_1 \subset \mathcal{H}_0 \subset \mathcal{H}^\star_0.$$

E.g., if $p = q + 1$ this takes the following form

$$[B] \subset [A, XB] \subset [A, B, XB] \subset [XA, A, XB, X^2B] \subset [XA, A, B, XB, X^2B] \subset \cdots \subset \mathcal{H}_0 \subset \mathcal{H}^\star_0$$

So there is a natural succession of polynomials :

$$H_q,\ H^\star_q,\ H_{q-1},\ H^\star_{q-1},\ H_{q-2},\ \ldots,\ H^\star_1,\ H_0,\ H^\star_0$$

When $p \leq q$ we get the following increasing sequence of matrices extracted from $\mathcal{H}^\star_0$.

$$\mathcal{H}^\star_p \subset \mathcal{H}_{p-1} \subset \mathcal{H}^\star_{p-1} \subset \mathcal{H}_{p-2} \subset \cdots \subset \mathcal{H}^\star_1 \subset \mathcal{H}_0 \subset \mathcal{H}^\star_0$$

E.g. if $p = q$ this takes the following form

$$[A] \subset [A, B] \subset [XA, A, XB] \subset [XA, A, B, XB] \subset \cdots \subset \mathcal{H}^\star_1 \subset \mathcal{H}_0 \subset \mathcal{H}^\star_0.$$

Example 3.3 We consider the successive matrices and their r-reduced forms in the non defective case. E.g., with $q = 3$.

$$\mathcal{H}_3 \subset \mathcal{H}^\star_3 \subset \mathcal{H}_2 \subset \mathcal{H}^\star_2 \subset \mathcal{H}_2 \subset \mathcal{H}^\star_1 \subset \mathcal{H}_0 \subset \mathcal{H}^\star_0$$

We begin with

$$h^\star_4 = 1,\ H_3 = B$$

$$\mathcal{H}^\star_3 = \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot \\ b & \cdot & \cdot & \cdot & 0 \end{bmatrix} \begin{matrix} A \\ XB \end{matrix} \sim_r \mathcal{G}^\star_3 = \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot \\ 0 & g^\star_3 & \cdot & \cdot & \cdot \end{bmatrix} \begin{matrix} A \\ \mathrm{GRem}(A, XB) \end{matrix}$$

Thus $G^\star_3 = \mathrm{GRem}(A, XB)$.

$$\mathcal{H}_2 = \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot \\ 0 & b & \cdot & \cdot & \cdot \\ b & \cdot & \cdot & \cdot & 0 \end{bmatrix} \begin{matrix} A \\ B \\ XB \end{matrix} \sim_r \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot \\ 0 & b & \cdot & \cdot & \cdot \\ 0 & g^\star_3 & \cdot & \cdot & \cdot \end{bmatrix} \begin{matrix} A \\ B \\ G^\star_3 \end{matrix} \sim_r \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot \\ 0 & b & \cdot & \cdot & \cdot \\ 0 & 0 & g_2 & \cdot & \cdot \end{bmatrix} \begin{matrix} A \\ B \\ \mathrm{GRem}(B, G^\star_3) \end{matrix}$$

So $G_2 = \mathrm{GRem}(B, G^\star_3)$.

$$\mathcal{H}^\star_2 = \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & a & \cdot & \cdot & \cdot & \cdot \\ 0 & b & \cdot & \cdot & \cdot & 0 \\ b & \cdot & \cdot & \cdot & 0 & 0 \end{bmatrix} \begin{matrix} XA \\ A \\ XB \\ X^2B \end{matrix} \sim_r \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & a & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & g^\star_3 & \cdot & \cdot & \cdot \\ 0 & 0 & g_2 & \cdot & \cdot & 0 \end{bmatrix} \begin{matrix} XA \\ A \\ G^\star_3 \\ XG_2 \end{matrix} \sim_r \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & a & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & g^\star_3 & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & g^\star_2 & \cdot & \cdot \end{bmatrix} \begin{matrix} XA \\ A \\ G^\star_3 \\ G^\star_2 \end{matrix}$$

So $G^\star_2 = \mathrm{GRem}(G^\star_3, XG_2)$.

In the *non defective case* we have the following results.

Proposition 3.4 *When $p = q + 1$ and for all $j \leq q$ the H_j and $H_j^\star$ are of degree j,*

$$G_{j-1} = \mathrm{GRem}(G_j, G_j^\star)$$
$$G_{j-1}^\star = \mathrm{GRem}(G_j^\star, XG_{j-1}).$$

Proposition 3.5 *When $p = q + 1$ and for all $j \leq q$ the H_j and $H_j^\star$ are of degree j,*

$$h_{j+1}^\star H_{j-1} = \mathrm{GRem}(H_j, h_j H_j^\star) = -\mathrm{Rem}(h_j^\star H_j, H_j^\star)$$
$$h_j H_{j-1}^\star = \mathrm{GRem}(H_j^\star, h_j^\star X H_{j-1}) = -\mathrm{Rem}(h_{j-1} H_j^\star, X H_{j-1}).$$

They are easy to prove in the spirit the example above, and are particular cases of Proposition 3.7 and Theorem 3.1 that we prove later.

The following algorithm due to C. Quitté [11] follows from the proposition and the conventions. It is particularly simple and improves the subresultant algorithm in the non defective case.

Non defective FlipFlop Algorithm
Let $H_q \leftarrow B$, $H_q^\star \leftarrow aXB - bA, h_{q+1}^\star \leftarrow 1$, ,
Knowing H_j, $H_j^\star$ and $h_{j+1}^\star$

$$H_{j-1} \leftarrow -(h_j^\star H_j - h_j H_j^\star)/h_{j+1}^\star$$

Knowing $H_j^\star$, H_{j-1} and h_j

$$H_{j-1}^\star \leftarrow -(h_{j-1} H_j^\star - h_j^\star X H_{j-1})/h_j.$$

We shall get a general version of this algorithm at the end of the paper.

In order to understand better what happens, in the defective case, we show first an example.

Example 3.6 Suppose that A is of degree 8 and of leading coefficient a, B of degree 7 and of leading coefficient b. First we have by conventions.

$$\mathcal{H}_7 = [\ b\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ ]\ \ B = G_7$$

Then the matrix

$$\mathcal{H}_7^\star = \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \end{bmatrix} \begin{matrix} A \\ XB \end{matrix}$$

has as r-reduced form, if $\mathrm{GRem}(A, XB)$ is of degree 7,

$$\mathcal{G}_7^\star = \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & g_7^\star & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix} \begin{matrix} A \\ G_7^\star = \mathrm{GRem}(G_8^\star, XG_7) \end{matrix}$$

Then $\mathcal{H}_6$ is associated to $[A, B, XB]$

$$\mathcal{H}_6 = \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \end{bmatrix} \begin{matrix} A \\ B \\ XB \end{matrix}$$

It gives by an elementary row replacement

$$\begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & g_7^\star & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix} \begin{matrix} A \\ B \\ G_7^\star \end{matrix}$$

Assume that G_6 is of degree 5, this gives the r-reduced form

$$\mathcal{G}_6 = \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix} \begin{matrix} A \\ B \\ G_6 = \mathrm{GRem}(B, G_7^\star) \end{matrix}$$

Since $\mathcal{H}_6^\star = [XA, A, XB, X^2B]$ contains the matrices $\mathcal{H}_7^\star$ and $X\mathcal{H}_6$, it has as r-reduced form

$$\mathcal{G}_6^\star = \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & g_7^\star & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \end{bmatrix} \begin{matrix} XA \\ A \\ G_7^\star \\ XG_6 = G_6^\star \end{matrix}$$

Since $\mathcal{H}_5 = [XA, A, B, XB, X^2B]$ contains $\mathcal{H}_6$ and $X\mathcal{H}_6$, it gives by elementary row replacements the following r-reduced form

$$\mathcal{G}_5 = \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \end{bmatrix} \begin{matrix} XA \\ A \\ B \\ G_6 = G_5 \\ XG_6 \end{matrix}$$

Suppose now that $G_5^\star = \mathrm{GRem}(G_7^\star, XG_6)$, of expected degree 5, is in fact of degree 4 : $G_5^\star = g_5^\star X^4 + \cdots$. Then $\mathcal{H}_5^\star = [X^2A, XA, A, XB, X^2B, X^3B]$ gives after some elementary row replacements the matrix

$$\mathcal{G}_5^\star = \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & g_7^\star & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & g_5^\star & \cdot & \cdot & \cdot & \cdot \end{bmatrix} \begin{matrix} X^2A \\ XA \\ A \\ G_7^\star \\ XG_6 \\ G_5^\star = \mathrm{GRem}(G_7^\star, XG_6) \end{matrix}$$

The matrix $\mathcal{H}_4 = [X^3A, X^2A, XA, A, B, XB, X^2B, X^3B]$ contains the matrices $\mathcal{H}_5$ and $\mathcal{H}_5^\star$, so it has as r-reduced form

$$\mathcal{G}_4 = \begin{bmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & g_6 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & g_5^\star & \cdot & \cdot & \cdot & \cdot \end{bmatrix} \begin{matrix} X^2A \\ XA \\ A \\ B \\ G_6 \\ XG_6 \\ G_5^\star = G_4 \end{matrix}$$

Proposition 3.7 *(notations 2.1 and 3.1, conventions 3.2).*

1) Let $0 \leq j \leq \inf(p-1, q)$. Suppose that $\mathcal{H}_{j+1}^\star$ and $\mathcal{H}_j$ are non defective. In particular this is the case if $j = q < p$ with $G_q^\star = \mathrm{GRem}(A, XB)$.

a) If $G_j^\star = 0$, then G_j is the GCD of A and B and XG_j is the GCD of A and XB.

b) If $G_j^\star \neq 0$ is of degree $k \leq j$, then

i) $G_{k-1} = \mathrm{GRem}(G_j, G_j^\star)$

Moreover if $k < j$

ii) $G_j^\star = G_{j-1} = G_{j-1}^\star = \ldots = G_k = G_k^\star$

Remark that (in case $k = j$ as in case $k < j$) $\mathcal{H}_k$ and $\mathcal{H}_k^\star$ are non defective, and we are thus in the situation 2) underneath.

2) Let $0 \leq j \leq \inf(p, q)$. Suppose that $\mathcal{H}_j^\star$ and $\mathcal{H}_j$ are non defective. In particular this is the case if $j = p \leq q$ with $G_{p-1} = \mathrm{Rem}(B, A)$.

a) If $G_{j-1} = 0$, then $G_j^\star$ is the GCD of A and B, and it is also the GCD of A and XB.

b) If $G_{j-1} \neq 0$ is of degree $k \leq j-1$, then

i) $G_k^\star = \mathrm{GRem}(G_j^\star, XG_{j-1})$

Moreover if $k < j-1$

ii) $G_{j-1} = \ldots = G_k$

$G_{j-1}^\star = \ldots = G_{k+1}^\star = XG_{j-1}$

Remark that (in case $k = j-1$ as in case $k < j-1$) $\mathcal{H}_{k+1}^\star$ and $\mathcal{H}_k$ are non defective, and we are thus in the situation 1) above.

Proof:
1a) and 2a) Let $G = \mathrm{GCD}(A, B)$, $G^\star = \mathrm{GCD}(A, XB)$. We have $G^\star = G$ or $G^\star = XG$ (up to constants). In case (1a) we know that $G^\star = G_{j+1}^\star$ and G divides G_j. So $\deg(G) < \deg(G^\star)$. It follows that $G^\star = XG$ and $G = G_j$ (up to a constant). In case (2a) we know that $G = G_j$ and $G^\star$ divides $G_j^\star$. So $\deg(G) = \deg(G^\star)$. It follows that $G_j^\star = G^\star = G$ (up to a constant).
1b) Using proposition 2.5, it is enough to prove
(1α) $G_{k-1} = \mathrm{GRem}(G_j, G_j^\star)$ and
(1β) if $k < j$ then $G_{j-1} = G_j^\star$.

The matrix $\mathcal{H}_{k-1}$ is r-equivalent to

$$[X^{q-k}A, \ldots, X^{q-j}A, \mathcal{H}_j, G_j^\star, \ldots, X^{j-k}G_j^\star],$$

thus

$$G_{k-1} = \mathrm{ldPol}(\mathcal{H}_{k-1}) =$$
$$\mathrm{ldPol}(X^{q-k}A, \ldots, X^{q-j}A, \mathcal{H}_j, G_j^\star, \ldots, X^{j-k}G_j^\star).$$

According to Lemma 1.3,

$$\mathrm{ldPol}(X^{q-k}A, \ldots, X^{q-j}A, \mathcal{H}_j, G_j^\star, \ldots, X^{j-k}G_j^\star) =$$
$$\mathrm{ldPol}(\mathrm{ldPol}(X^{q-k}A, \ldots, X^{q-j}A, \mathcal{H}_j), G_j^\star, \ldots, X^{j-k}G_j^\star)$$
$$= \mathrm{GRem}(G_j, G_j^\star)$$

So

$$G_{k-1} = \mathrm{GRem}(G_j, G_j^\star).$$

If $k < j$, the matrix $\mathcal{H}_{j-1}$ associated to

$$[X^{q-j}A, \mathcal{H}_j, G_j^\star]$$

is r-equivalent to $\mathcal{H}_{j-1}$. So it is clear that the G-polynomial $\mathcal{G}_{j-1}$ is $G_j^\star$.
2b) Using proposition 2.5, it is enough to prove
(2α) $G_k^\star = \mathrm{GRem}(G_j^\star, XG_{j-1})$ and
(2β) if $k < j$ then $G_{j-1}^\star = XG_{j-1}$.

The matrix $\mathcal{H}_k^\star$ is r-equivalent to

$$[X^{q-k}A, \ldots, X^{q-j}A, \mathcal{H}_j^\star, XG_{j-1}, \ldots, X^{j-k}G_{j-1}],$$

thus

$$G_k^\star = \mathrm{ldPol}(\mathcal{H}_k^\star) = \mathrm{ldPol}(X^{q-k}A, \ldots, X^{q-j}A, \mathcal{H}_j^\star, XG_{j-1}, \ldots, X^{j-k}G_{j-1}).$$

According to Lemma 1.3,

$$\begin{aligned}\mathrm{ldPol}(X^{q-k}A, \ldots, X^{q-j}A, \mathcal{H}_j^\star, XG_{j-1}, \ldots, X^{j-k}G_{j-1}) = \\ \mathrm{ldPol}(\mathrm{ldPol}(X^{q-k}A, \ldots, X^{q-j}A, \mathcal{H}_j^\star), XG_{j-1}, \ldots, X^{j-k}G_{j-1}) \\ = \mathrm{GRem}(G_j^\star, XG_{j-1})\end{aligned}$$

So

$$G_k^\star = \mathrm{GRem}(G_j^\star, XG_{j-1}).$$

If $k < j-1$, the matrix $\mathcal{H}_{j-1}^\star$ associated to

$$[X^{q-j}A, \mathcal{H}_j^\star, XG_{j-1}]$$

is r-equivalent to $\mathcal{H}_{j-1}^\star$. So it is clear that the G-polynomial $\mathcal{G}_{j-1}^\star$ is XG_{j-1}. □

We are now ready for the general structure theorem.

Theorem 3.1 **(Second structure theorem)** *We use notations 2.1, 3.1 and convention 3.2.*

1) Let $0 \le j \le \inf(p-1, q)$. Assume $\mathcal{H}_{j+1}^\star$ and $\mathcal{H}_j$ non defective. In particular this is the case if $j = q < p$ with $h_{q+1}^\star = 1$, $H_q = \varepsilon_{p-q-1} b^{p-q-1} B$.

Let i be the largest index such that H_{i-1} is of degree j. (if $j = q < p$ then $i = j+1$)

a) If $H_j^\star = 0$ then H_j is the GCD of A and B and XH_j is the GCD of A and XB.

b) If $H_j^\star \neq 0$ is of degree k then

i) $h_i^\star \cdot H_{k-1} = (-1)^{i-k}\mathrm{Rem}(h_k^\star H_{i-1}, H_j^\star)$

Moreover if $k < j$, we have

ii) $H_j^\star$, H_{j-1}, H_k, and $H_k^\star$ are proportional. Precisely:

iii) $\overline{h}_{j-1} = \frac{h_j \overline{h}_j^\star}{h_{j+1}^\star}$, $h_k = \varepsilon_{j-k-1} \frac{h_j \overline{h}_j^{\star\, j-k}}{h_{j+1}^{\star\, j-k}}$, $h_k^\star = (-1)^{j-k} \frac{h_k \overline{h}_j^\star}{h_j}$,

iv) $H_{j-1}^\star = H_{j-2} = \ldots = H_{k+1} = H_{k+1}^\star = 0$

Remark that (in case $k = j$ as in case $k < j$) $\mathcal{H}_k$ and $\mathcal{H}_k^\star$ are non defective, and we are thus in the situation 2) underneath.

2) Let $0 \leq j \leq \inf(p,q)$. Assume $\mathcal{H}_j$ and $\mathcal{H}_j^\star$ non defective. In particular this is the case if $j = p \leq q$ with $h_p = 1$, $H_p^\star = a^{q-p}A$.

Let i be the largest index such that $H_i^\star$ is of degree j (if $j = p \leq q$ then $i = j$)

a) If $H_{j-1} = 0$ then $H_j^\star$ is the GCD of A and B and it is also the GCD of A and XB.

b) If $H_{j-1} \neq 0$ is of degree k then

i) $h_i H_k^\star = (-1)^{i-k}\mathrm{Rem}(h_k H_i^\star, XH_{j-1})$

Moreover if $k < j-1$ we have

ii) XH_{j-1}, $H_{j-1}^\star$, $H_{k+1}^\star$ and XH_k are proportional. Precisely:

iii) $\overline{h^\star}_{j-1} = \frac{h_j^\star \bar{h}_{j-1}}{h_j}$, $h_{k+1}^\star = \varepsilon_{j-k-2}\frac{h_j^\star \bar{h}_{j-1}^{j-k-1}}{h_j^{j-k-1}}$, $h_k = (-1)^{j-k-1}\frac{h_{k+1}^\star \bar{h}_{j-1}}{h_j}$,

iv) $H_{j-2} = H_{j-2}^\star = \ldots = H_{k+1} = 0$,

Remark that (in case $k = j-1$ as in case $k < j-1$) $\mathcal{H}_{k+1}^\star$ and $\mathcal{H}_k$ are non defective, and we are thus in the situation 1) above.

Proof:
1a) and 2a) are deduced from analogous results in proposition 3.7.
1b ii), iii) and iv) follow from Theorem 2.1 and proposition 3.7 when remarking that

$$ag_{j-1} = ag_j^\star = \frac{\overline{h_j^\star}}{h_{j+1}^\star} = \frac{\overline{h}_{j-1}}{h_j}$$

(following proposition 2.5 a)) and that

$$h_k = \varepsilon_{j-k-1}\frac{\overline{h}_{j-1}{}^{j-k}}{h_j{}^{j-k-1}},\ h_k^\star = \varepsilon_{j-k}\frac{\overline{h_j^\star}^{j-k+1}}{h_{j+1}^\star{}^{j-k}}$$

2b ii), iii) and iv) follow from Theorem 2.1 and proposition 3.7 when remarking that

$$ag_{j-1}^\star = ag_{j-1} = \frac{\overline{h}_{j-1}}{h_j} = \frac{\overline{h_{j-1}^\star}}{h_j^\star}$$

(following proposition 2.5 a)) and that

$$h_{k+1}^\star = \varepsilon_{j-k-2}\frac{\overline{h_{j-1}^\star}^{j-k-1}}{h_j^{\star j-k-2}},\ h_k = \varepsilon_{j-k-1}\frac{\overline{h}_{j-1}{}^{j-k}}{h_j{}^{j-k-1}}.$$

1b i) Using proposition 3.7:

$$G_{k-1} = \mathrm{GRem}(G_j, G_j^\star),$$

multiplying both sides by $ah_k h_{j+1}^\star$ and noting that

$$H_{k-1} = ah_k G_{k-1},\ H_j^\star = ah_{j+1}^\star G_j^\star,$$

we get $h_{j+1}^\star \cdot H_{k-1} = \mathrm{GRem}(H_j, h_k H_j^\star)$. Using the relationship between remainder and G-remainder, we obtain :

$$h_{j+1}^\star H_{k-1} = (-1)^{j-k+1}\mathrm{Rem}(h_k^\star H_j, H_j^\star)$$

Finally, using 2b iii), we have the proportionality between H_i and H_j ((i,j) replacing (j,k))

$$h_i^\star H_j = (-1)^{(i-j-1)} h_{j+1}^\star H_{i-1}$$

Using this relation, we obtain as expected :

$$h_i^\star H_{k-1} = (-1)^{i-k} \mathrm{Rem}(h_k^\star H_{i-1}, H_j^\star)$$

Remark that 2b iii) is also true at the initialisation and in the non defective case.
2b i) Same computation. First using proposition 3.7 we get $h_j H_k^\star = \mathrm{GRem}(H_j^\star, h_{k+1}^\star X H_{j-1})$. Then the relationship between remainder and G-remainder gives :

$$h_j H_k^\star = (-1)^{j-k} \mathrm{Rem}(h_k H_j^\star, X H_{j-1})$$

Finally, using 1b iii), we have the proportionality between $H_i^\star$ and $H_j^\star$:

$$h_i H_j^\star = (-1)^{i-j} h_j H_i^\star$$

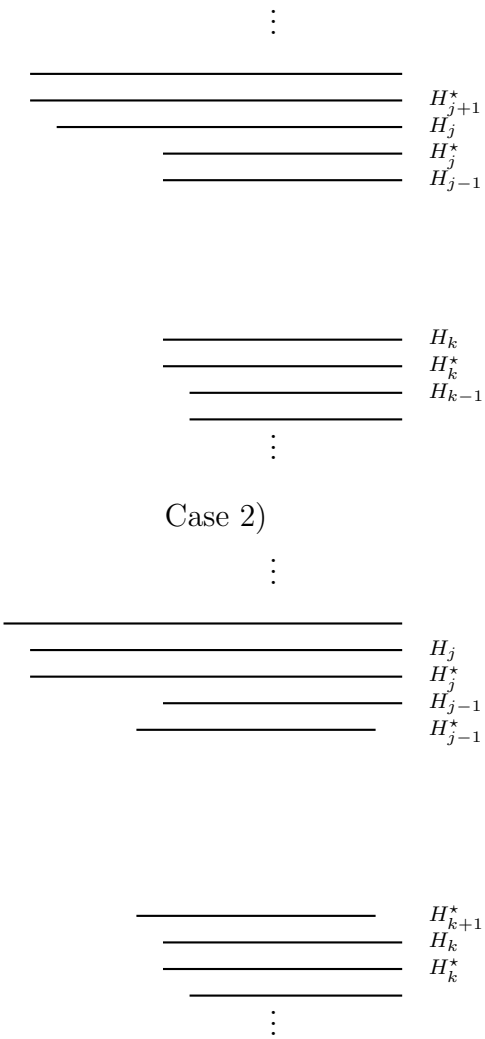
Using this relation, we obtain as expected :

$$h_i H_k^\star = (-1)^{i-k} \mathrm{Rem}(h_k H_i^\star, X H_{j-1})$$

□

The corresponding *gap structure* can be graphically displayed as follows.

Case 1)



Case 2)

4 Algorithm

Contrarily to what could be hoped, in the defective case, the divisions in the right hand side of the equalities $h_i^\star \cdot H_{k-1} = (-1)^{i-k}\mathrm{Rem}(h_k^\star H_{i-1}, H_j^\star)$ and $h_i H_k^\star = (-1)^{i-k}\mathrm{Rem}(h_k H_i^\star, XH_{j-1})$ do not give always quotients a with coefficients in $\mathbf{D}$.

Example 4.1 *Consider the polynomials* $A = 3X^5 + X + 1$ *and* $B = 2X^4 + X - 3$. *We have :*

$$H_4 = B \quad H_4^\star = \mathrm{PRem}(A, XB) = -6X^2 + 22X + 4$$

So using relations in 3.1, $h_2^\star = -6$. *Then we find*

$$\mathrm{Quo}(h_2^\star H_4, H_4^\star) = 12X^2 + 44X + 508/3$$

The following proposition due to Lionel Ducos [4] will be used to perform the divisions of $h_k^\star H_{i-1}$ by $H_j^\star$ (resp. of $h_k H_i^\star$ by XH_{j-1}) without computing the quotient.

Proposition 4.2 *Let* $\mathcal{H}_j$ *be non defective. Let* k *be the degree of* H_{j-1} *and assume* $k < j - 1$. *Then we get for* $\delta = 0, \ldots, j - 1 - k$

$$\mathrm{Rem}(h_k X^{k+\delta}, H_{j-1}) \in \mathbf{D}[X]$$

Proof : Add the row $X^{k+\delta}$ to $\mathcal{H}_k$ to obtain a matrix $\mathcal{M}_{k,\delta}$. By elementary row replacements we can replace the $j - k$ last rows of $\mathcal{H}_k$ by $G_{j-1}, \ldots, X^{j-k-1}G_{j-1}$ and, by new elementary row replacements the last row $X^{k+\delta}$ by $\mathrm{Rem}(X^{k+\delta}, G_{j-1})$, since the least degree polynomial generated by $[G_{j-1}, \ldots, X^{j-k-1}G_{j-1}, X^{k+\delta}]$ is $\mathrm{Rem}(X^{k+\delta}, G_{j-1})$. So $\mathrm{ldPol}(\mathcal{M}_{k,\delta}) = \mathrm{Rem}(X^{k+\delta}, G_{j-1})$. Since $\mathcal{H}_k$ is non defective, we can apply lemma 1.6 d) to $\mathcal{M}_{k,\delta}$: $\mathrm{DetPol}(\mathcal{M}_{k,\delta}) = h_k\mathrm{Rem}(X^{k+\delta}, G_{j-1}) = \mathrm{Rem}(h_k X^{k+\delta}, H_{j-1})$. □

Note that the pseudoremainder of A and B can be computed as follows.

Pseudo Remainder computation

Input A and B of degrees p and q $(q \leq p)$

Output $\mathrm{PRem}(A, B)$

Initialization $R_q \leftarrow b^{p-q+1}X^q - b^{p-q}B$, $r_q \leftarrow \mathrm{coef}_q(R_q)$

Loop For δ from 0 to $p - q - 1$: $r_{q+\delta} \leftarrow \mathrm{coef}_q(R_{q+\delta})$, $R_{q+\delta+1} \leftarrow XR_{q+\delta} - (r_{q+\delta}B/b)$,

Final step Denoting by a_ℓ the coefficient of degree ℓ of A, let

$$D \leftarrow \sum_{\ell<q} a_\ell \cdot b^{p-q+1}X^\ell + \sum_{p\geq\ell\geq q} a_\ell \cdot R_\ell.$$

{ Thus $D = \mathrm{PRem}(A, B)$}.

This technique will be used in the initialization phase of the following algorithm. A similar technique will be used later to compute H_{k-1} (resp. $H_k^\star$) in the defective case.

FlipFlop Algorithm

Input A and B two polynomials of degrees p and q

Output Subresultants H_j and $H_j^\star$ (notations 2.1, 3.1 and convention 3.2).

Initialization

- If $p > q$ let $j \leftarrow q$, $h_{q+1}^\star \leftarrow 1$, $i \leftarrow q+1$,
  $H_q \leftarrow \varepsilon_{p-q-1} b^{p-q-1} B$,
  $H_q^\star \leftarrow \varepsilon_{p-q+1}\mathrm{PRem}(A, XB)$ { $= \mathrm{DetPol}(\mathcal{H}_q^\star)$ },
  $k \leftarrow \deg(H_q^\star)$.
  If $H_q^\star = 0$ the computation is over. Otherwise go to Part 1).
- If $p \leq q$ let $j \leftarrow p$, $h_p \leftarrow 1$, $i \leftarrow p$
  $H_p^\star \leftarrow a^{q-p} A$,
  $H_{p-1} \leftarrow \mathrm{PRem}(B, A)$ { $= \mathrm{DetPol}(\mathcal{H}_{p-1})$ },
  $k \leftarrow \deg(H_{p-1})$.
  If $H_{p-1} = 0$ the computation is over. Otherwise go to Part 2).

Part 1)

- Input : i, j, k, H_{i-1}, $H_j^\star$, $h_i^\star$, $h_{j+1}^\star$, h_j
  $\{\mathcal{H}_{j+1}^\star$ and $\mathcal{H}_j$ are non defective, i is the largest index such that H_{i-1} is of degree j, $k = \deg(H_j^\star)\}$
- Output : $H_j^\star$, H_{k-1}, h_j, h_k, $h_k^\star$. Moreover i, j, k get new values and in the defective case the missing subresultants are computed as extra outputs (that are not needed in order to run the algorithm).
- If $k = j$ let $H_{k-1} \leftarrow -(h_j^\star H_{i-1} - h_{i-1} H_j^\star)/h_i^\star$
  { $h_k^\star$ and h_k are known since $k = j$ }
- If $k < j$
  - Computation of h_k :
    - $\overline{h_j} \leftarrow h_j$
    - For δ from 0 to $j-k-1$: $\overline{h}_{j-\delta-1} \leftarrow (-1)^\delta \overline{h}_{j-\delta} \bar{h}_j^\star / h_{j+1}^\star$
    - $h_k \leftarrow \overline{h_k}$
  - Computation of $h_k^\star$: $h_k^\star = (-1)^{j-k} h_k \bar{h}_j^\star / h_j$
  - Computation of H_{k-1} :
    - Initialization :
      $R_k \leftarrow h_k^\star X^k - (h_k^\star H_j^\star / \overline{h_j^\star})$ $\{= \mathrm{Rem}(h_k^\star \cdot X^k, H_j^\star)\}$
    - For δ from 0 to $j-k-1$:
      $r_{k+\delta} \leftarrow \mathrm{coef}_k(R_{k+\delta})$, $R_{k+\delta+1} \leftarrow XR_{k+\delta} - (r_{k+\delta} H_j^\star / \overline{h_j^\star})$
      $\{R_{k+\delta+1} = \mathrm{Rem}(XR_{k+\delta}, H_j^\star).\}$
    - Denoting by $h_{i-1,m}$ the coefficient of degree m of H_{i-1}, let

      $$D \leftarrow \sum_{m<k} h_{i-1,m} \cdot h_k^\star X^m + \sum_{j \geq m \geq k} h_{i-1,m} \cdot R_m.$$

      { Thus $D = \mathrm{Rem}(h_k^\star H_{i-1}, H_j^\star)$, hence $h_i^\star \cdot H_{k-1} = (-1)^{i-k} D$ } and

      $$H_{k-1} \leftarrow (-1)^{i-k} D / h_i^\star$$

  - Computation of extra outputs :
    $H_{j-1} \leftarrow h_j H_j^\star / h_{j+1}^\star$,
    $H_k \leftarrow h_k H_j^\star / \overline{h_j^\star}$,
    $H_k^\star \leftarrow h_k^\star H_j^\star / \overline{h_j^\star}$
    $H_{j-1}^\star = H_{j-2}^\star = \ldots = H_{k+1} = H_{k+1}^\star \leftarrow 0$,
- If $H_{k-1} = 0$, let all the subresultants H_ℓ and $H_\ell^\star$ with $0 \leq \ell < k$ be $= 0$ and stop the algorithm. Otherwise let $(i, j, k) \leftarrow (j, k, \deg(H_{k-1}))$ and enter Part 2)

Part 2)

- Input : i, j, k, $H_i^\star$, H_{j-1}, h_i, h_j, $h_j^\star$,
  $\{$ $\mathcal{H}_j$ and $\mathcal{H}_j^\star$ are non defective, i is the largest index such that $H_i^\star$ is of degree j, $k = \deg(H_{j-1})$ $\}$
- Output : H_{j-1}, $H_k^\star$, $h_j^\star$, $h_{k+1}^\star$, h_k. Moreover i, j, k get new values and in the defective case the missing subresultants are computed as extra outputs (that are not needed in order to run the algorithm).
- If $k = j-1$ let $H_k^\star \leftarrow -(h_{j-1}H_i^\star - h_j^\star X H_{j-1})/h_i$
  $\{\, h_k$ and $h_{k+1}^\star$ are known since $k = j-1 \,\}$
- If $k < j-1$
  - Computation of $h_{k+1}^\star$:
    - $\overline{h}_j^\star \leftarrow h_j^\star$
    - For δ from 0 to $j-k-2$: $\overline{h}_{j-1-\delta}^\star \leftarrow (-1)^\delta \overline{h}_{j-\delta}^\star \bar{h}_{j-1}/h_j$
    - $h_{k+1}^\star \leftarrow \overline{h}_{k+1}^\star$
  - Computation of h_k : $h_k = (-1)^{j-k-1} h_{k+1}^\star \bar{h}_{j-1}/h_j^\star$
  - Computation of $H_k^\star$:
    - Initialization :
      $R_{k+1}^\star \leftarrow h_k X^{k+1} - (h_k X H_{j-1}/\overline{h}_{j-1})$ $\{= \mathrm{Rem}(h_k X^{k+1}, X H_{j-1})\}$
    - For δ from 1 to $j-k-1$:
      $r_{k+\delta}^\star \leftarrow \mathrm{coef}_k(R_{k+\delta}^\star)$, $R_{k+\delta+1}^\star \leftarrow X R_{k+\delta}^\star - (r_{k+\delta}^\star H_{j-1}/\overline{h}_{j-1})$
      $\{R_{k+\delta+1}^\star = \mathrm{Rem}(X R_{k+\delta}^\star, H_{j-1})\}$
    - Denoting by $h_{i,m}^\star$ the coefficient of degree m of $H_i^\star$, let

      $$D^\star \leftarrow \sum_{m<k} h_{i,m}^\star \cdot h_k X^m + \sum_{j \geq m \geq k} h_{i,m}^\star \cdot R_m^\star$$

      $\{$ Thus $D^\star = \mathrm{Rem}(h_k H_i^\star, X H_{j-1})$, hence $h_i \cdot H_k^\star = (-1)^{i-k} D^\star$ $\}$ and

      $$H_k^\star \leftarrow (-1)^{i-k} D^\star / h_i$$

  - Computation of extra outputs :
    $H_{j-1}^\star \leftarrow h_j^\star X H_{j-1}/h_j$,
    $H_{k+1}^\star \leftarrow h_{k+1}^\star X H_{j-1}/\overline{h}_{j-1}$,
    $H_k \leftarrow h_k H_{j-1}/\overline{h}_{j-1}$
    $H_{j-2} = H_{j-2}^\star = \ldots = H_{k+1} = 0$,
- If $H_k^\star = 0$, let all the subresultants $H_{\ell-1}$ and $H_\ell^\star$ with $0 \leq \ell \leq k$ be $= 0$ and stop the algorithm. Otherwise let $(i, j, k) \leftarrow (j, k, \deg(H_k^\star))$ and enter Part 1)

The fact that the algorithm is correct follows from theorem 3.1 and propositions 2.10 and 4.2.

Complexity of the algorithms

We are going to compare the Improved subresultant algorithm, the FlipFlop algorithm and Ducos's algorithm from [4].

In order to give a hint of the computations made by the Ducos's algorithm, we describe it in the non defective case (see [4] for the defective case).

We denote by $h_{j+1,j}$ the coefficient of X^j in H_{j+1} and by k_j the coefficient of degree j of K_j.

Non defective Ducos's Algorithm

$$K_q \leftarrow aXB - bA,$$
$$H_{q-1} \leftarrow -(k_q B - h_q K_q).$$

Knowing H_{j+1}, H_j and h_{j+1}

$$K_j \leftarrow -XH_j - (h_{j+1,j}H_j - h_j H_{j+1})/h_{j+1},$$
$$H_{j-1} \leftarrow (k_j H_j - h_j K_j)/h_{j+1}.$$

It is not complicated to check that in the three algorithms we compare the non defective case involves more arithmetic operations and bit operations.

In order to go from H_j to H_{j-1}

- in the Improved subresultant algorithm we perform $3j$ multiplications between coefficients of bit size $2\tau + 1$ and τ, $2j - 1$ additions between coefficients of bit size $3\tau + 1$, j exact divisions between coefficients of bit size $3\tau + 2$ and 2τ,
- in the FlipFlop algorithm we perform $4j + 1$ multiplications between coefficients of bit size τ, and $2j - 1$ additions of bit size 2τ, $2j + 1$ exact divisions between coefficients of bit size $2\tau + 1$ and τ.
- in the Ducos's algorithm we perform $4j$ multiplications between coefficients of bit size τ, and $3j$ additions of bit size 2τ, $2j+1$ exact divisions between coefficients of bit size $2\tau+1$ and τ.

In the case of polynomials of degree d with integer coefficients of bit size t, the maximum bit size τ of a minor extracted from Sylvester matrix is $O(d(t + \log(d))$.

Neglecting linear factors, the three algorithms perform $2d^2$ arithmetic operations, in the Improved subresultant algorithm the size of intermediate computations is at most $3\tau+2$, while in the FlipFlop algorithm and Ducos's algorithm the size of intermediate computations is at most $2\tau + 1$.

Using naive arithmetic operations, the bit complexity of the Improved subresultant algorithm is dominated by $6\tau^2 d^2$, the the bit complexity of the FlipFlop and Ducos's algorithm is dominated by $4\tau^2 d^2$.

Using fast arithmetic operations, and neglecting log factors, the bit complexity of the Improved subresultant algorithm is dominated by $(15/2)\tau d^2$, the bit complexity of the FlipFlop algorithm is dominated by $6\tau d^2$, and the complexity of Ducos's algorithm is dominated by $7\tau d^2$.

Experimental results

The FlipFlop algorithm has been implemented in Aldor. We have tested it and compared with implementations in the same language of the improved subresultant algorithm, and Ducos's algorithm for univariate polynomials and multivariate polynomials. In the experimentation, we have distinguished the non defective case, i.e. the case where there are no gaps of degrees in the remainder sequence, and the defective case where there are gaps of degrees in the remainder sequence. Note that the non defective case is generic and that in this case the improved and classical subresultant algorithm coincide.

1) For univariate polynomials, the algorithms have been performed on a PC Pentium II, 300 Mhz with 64 Meg of RAM. The computing times are given in seconds.

- a) In the non defective case, we have taken random polynomials. Here are the computation times in seconds :

degree	FlipFlop	Ducos	Improved
100	10,2	10,1	12,5
150	46,8	46,7	57,4
200	139,0	139,0	170,0
250	329,0	327,7	397,8
300	662	663	798
350	1200	1201	1435

- b) The test suite we used to compare the algorithms in the defective case is the following:

	$x^{30} + ax^{20} + 2ax^{10} + 3a$
	$x^{25} + 4bx^{15} + 5bx^5$
P30-25/a	$a = 10^{240}$ $b = 2 \cdot 10^{240}$
P30-25/b	$a = 10^{726}$ $b = 2 \cdot 10^{726}$
P30-25/c	$a = 10^{1726}$ $b = 2 \cdot 10^{1726}$
	$(a + x)^{90}$ $(a - x)^{60}$
P90-60/a	$a = 2$
P90-60/b	$a = 10$
	$x^{120} + ax^{100} + 2ax^{80} + 3ax^{70} + 2ax^{50} + 3ax^{20} + ax^5 + 2a$
	$x^{115} + 4bx^{85} + 5bx^{65} - x^{35} + 4bx^{25} + 5bx^{15}$
P120-115/a	$a = 10^{126}$ $b = 2.10^{126}$
P120-115/b	$a = 10^{226}$ $b = 2.10^{226}$

Here are the computation times :

degree	FlipFlop	Ducos	Improved
P30-25/a	0,69	0,49	1,1
P30-25/b	5,6	4,1	8,4
P30-25/c	32,2	24,1	44,1
P90-60/a	5,9	5,6	7,0
P90-60/b	21,2	20,1	25,2
P120-115/a	75,0	68,0	161,4
P120-115/b	249,0	224,0	489,0

The couples P30-25 are such that there are gaps of degrees in all the successive remainders. We notice that Ducos's algorithm is the best, the FlipFlop Algorithm is good and they are both better than the Improved subreultant Algorithm.

The couples P90-60 are such that there is only one big gap of degree at the beginning of the computation. We notice that there is little difference in computation times between the different algorithms.

The couples P120-115 are intermediate examples.

From these experiments, it appears that the FlipFlop Algorithm and Ducos's algorithm are better in terms of computation times than the Improved Subresultant Algorithm. In the generic

(non defective) case, the computation times are equivalent for FlipFlop Algorithm and Ducos's algorithm. In the defective case, Ducos's algorithm is the best, but FlipFlop Algorithm is not so far.

2) For multivariate polynomials, we used a PC Bi-Pentium II 400 Mhz with 512 Meg of RAM of the UMS Medicis.

- a) For testing the non defective case, we have taken random polynomials whose coefficients are univariate polynomials. Here are the computing times in seconds :

degree	FlipFlop	Ducos	Improved
10	3,8	3,5	7,4
15	32,4	32,7	64,1
20	160	171	329
25	616	731	1303

  Here the FlipFlop Algorithm gives slightly better computation times than the Ducos's algorithm. During the computations with multivariate polynomials, we have observed bigger coefficients for Ducos's algorithm than for FlipFlop Algorithm.

  On the other hand, the FlipFlop Algorithm and Ducos's algorithm are significantly better than the Improved Subresultant Algorithm for multivariate polynomials.

- b) For the defective cases, in order to observe what happens when there are gaps in degrees, we have constructed artificially the following examples.

	$x^{30} + ax^{20} + 2ax^{10} + 3a$
	$x^{25} + 4bx^{15} + 5bx^5$
P30-25/a	$a = (y^2+1)^3 \qquad b = (y^3+y^2+1)^2$
P30-25/b	$a = (y^2+1)^9 \qquad b = (y^3+y^2+1)^6$
P30-25/c	$a = (y^2+1)^{12} \qquad b = (y^3+y^2+1)^8$
	$(a+x)^{15} \qquad (a-x)^{10}$
P90-60/a	$a = (y^2+1)^3$
P90-60/b	$a = (y^2+1)^6$
	$ax^{100} + 2ax^{80} + 3ax^{70} + 2ax^{50} + 3ax^{20} + ax^5 + 2a$
	$4bx^{85} + 5bx^{65} - x^{35} + 4bx^{25} + 5bx^{15}$
P100-85/a	$a = y^2 + 1 \qquad b = y^3 + y^2 + 1$

  Here wegive the computation times :

degree	FlipFlop	Ducos	Improved
P30-25/a	5,9	4,4	19,7
P30-25/b	87,6	66,2	922,6
P30-25/c	211,6	160,5	2704
P90-60/a	67,2	48,2	100,7
P90-60/b	633	449	894
P100-85/a	739	671	> 6000

The couples P30-25 are such that during the computation there are always gaps of degrees in the remainder sequence. The couples P90-60 are such that there is only one big gap of degree at the beginning of the computation. The couples P100-85 are intermediate examples. Ducos's algorithm is slightly better for the defective case.

The little difference between the algorithms observed for the first test-suite is due to the fact that the gap in degree comes early in the computation. Thus, the size of the subresultant coefficients is no tbig enough to observe the better growth of the coefficients in FlipFlop and Ducos's algorithms.

One can conclude that for the multivariate case, the FlipFlop and Ducos's algorithms bring significant improvements to the Improved Subresultant Algorithm even in the non defective cases.

References

[1] Brown, W. S. *On Euclid's algorithm and the computation of polynomial greatest common divisors*. J. Assoc. Comput. Machin. 18, 478-504 (1971) 9

[2] Brown, W. S., Traub, J.F. *On Euclid's algorithm and the theory of subresultants*. J. Assoc. Comput. Machin. 18, 505-514 (1971) 9

[3] Collins, G. E. *Subresultants and reduced polynomial remainder sequences*. J. Assoc. Comput. Mach. 14, 128-142 (1967) 9

[4] Ducos L. *Optimizations of the subresultant algorithm*, to appear in Journal of Pure and Applied Algebra. 1, 9, 20, 22

[5] L. Gonzalez, H. Lombardi, T. Recio, and M.-F. Roy, *Spécialisation de la suite de Sturm et sous-résultants I*, Informatique théorique et applications **24** (1990), 561- 588. 9

[6] L. González-Vega, F. Rouillier, M.-F. Roy, G. Trujillo Symbolic Recipes for Real Solutions, In: Some tapas of computer algebra, A. Cohen et al. ed. Algorithms and Computation in Mathematics, vol. 4, 121-167, Springer. 10

[7] W. Habicht, *Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens,* Comm. Math. Helvetici **21** (1948), 99-116. 9

[8] D. Lazard, *Sous-résultants*, Manuscrit non publié. 9, 11

[9] Lickteig, T., Roy, M.-F. *Cauchy Index computation*. Calcolo, 33, 337-351 (1996) 9, 10, 11

[10] R. Loos, *Generalized polynomial remainder sequences*, in: Computer algebra, symbolic and algebraic computation, Springer-Verlag, Berlin (1982). 9

[11] C. Quitté, *Une démonstration de l'algorithme de Bareiss par l'algèbre extérieure*, Manuscrit non publié. 9, 14

Contents