INFORMATIQUE THÉORIQUE ET APPLICATIONS

L. GONZÁLEZ-VEGA
H. LOMBARDI
T. RECIO
M.-F. ROY

Spécialisation de la suite de Sturm et sous-résultants (I)

Informatique théorique et applications, tome 24, n° 6 (1990), p. 561-588

<http://www.numdam.org/item?id=ITA_1990__24_6_561_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 24, n° 6, 1990, p. 561 à 588)

SPÉCIALISATION DE LA SUITE DE STURM ET SOUS-RÉSULTANTS (I) (*)

par L. GONZÁLEZ-VEGA (1), H. LOMBARDI (2), T. RECIO (1)
et M.-F. ROY (3)

Communiqué par L. BERSTEL

Résumé. – *Nous présentons et comparons les différents algorithmes pour compter le nombre de racines réelles d'un polynôme et leurs généralisations. Ces méthodes sont reliées par la suite de Sturm-Habicht, qui repose sur la théorie des polynômes sous-résultants.*

Dans cette première partie, nous donnons le théorème de Sturm et sa généralisation. Une légère généralisation de la notion de polynôme sous-résultant de deux polynômes permet de simplifier les démonstrations, de préciser les algorithmes et de traiter de manière agréable les problèmes de spécialisation, même lorsqu'il y a chute du degré.

Dans la deuxième partie, nous étudierons la suite de Sturm-Habicht, puis comparerons différentes méthodes pour compter le nombre de racines réelles d'un polynôme.

Abstract. – *We describe and compare the existing algorithms for computing the number of real roots of a polynomial and its extensions. These methods are related through the sequence of Sturm-Habicht, which itself relies on the theory of subresultant polynomials.*

In this first part of the paper, we give Sturm's theorem and its generalization; a slight generalization of the notion of subresultant polynomial allows us to simplify the proofs, to give more concise algorithms, and to deal in a clean way with the problems of specialization, even if the degree decreases.

In the second part of the paper, we will study the sequence of Sturm-Habicht, and compare several methods for counting the number of real roots of a polynomial.

INTRODUCTION

Nous présentons dans le I.1 une notion générale de suite de Sturm de deux polynômes P et Q et donnons ses propriétés. Si $Q=1$, on retrouve le théorème de Sturm qui permet de déterminer le nombre de racines réelles

(*) Reçu janvier 1989, version finale décembre 1989.

(1) Mathématiques, Université de Santander, Espagne.
(2) Mathematiques, Université de Franche-Comté, 25030 Besançon Cedex, France.
(3) IRMAR, Université de Rennes, 35042 Rennes Cedex, France.

Informatique théorique et Applications/Theoretical Informatics and Applications
0988-3754/90/06 561 28/$4.80/

d'un polynôme P. Dans le cas général on détermine la différence entre le nombre de racines réelles de P rendant Q (strictement) positif et le nombre de racines réelles de P rendant Q (strictement) négatif. Ces résultats, quoique peu connus, ont des sources classiques (*cf.* [18]). Nous indiquons ensuite les difficultés rencontrées lorsque on cherche à spécialiser ce calcul.

Dans le I.2, nous étudions les polynômes sous-résultants. Nous donnons les résultats classiques de cette théorie, et nous précisons les relations entre la suite des sous-résultants et la suite des restes pour la division euclidienne. Nous introduisons une légère généralisation de la notion de polynôme sous-résultant. L'utilité de cette généralisation s'avère lorsque nous étudions les problèmes liés à la spécialisation dans le I.2 (*c*); en outre, les preuves de plusieurs résultats sont simplifiées.

Dans le I.2 (*c*), nous indiquons comment se spécialisent ces polynômes sous-résultants.

Dans le I.2 (*d*), nous donnons différentes variantes de l'algorithme des sous-résultants de Habicht-Loos.

Dans II.1 nous définirons et étudierons la suite de Sturm-Habicht, puis dans le II.2 nous décrirons et comparerons différentes méthodes pour compter le nombre de racines réelles d'un polynôme [9]. Quelques détails supplémentaires (dans les preuves, ou sur quelques points historiques) peuvent être trouvés dans [11].

Plan de la partie I

I.1. Suite de Sturm de deux polynômes

(*a*) Définitions et notations

(*b*) Propriétés de la suite de Sturm

(*c*) Problèmes de spécialisation

I.2. Polynômes sous-résultants

(*a*) Définitions

(*b*) Polynômes sous-résultants, suites des restes et PGCD

(*c*) Spécialisation des polynômes sous-résultants

(*d*) Algorithmes de calcul et complexité

I.1. SUITE DE STURM DE DEUX POLYNÔMES

(a) Définitions et notations

Suite des restes

Soient un anneau intègre **A** et son corps de fractions **K**. Nous noterons :

- $d(P)$: le degré d'un polynôme P;
- $cd(P)$: son coefficient dominant;

$\mathbf{cf}_j(P)$: son coefficient de degré j (égal à 0 si j est $> d(P)$).

Soient P et S deux polynômes à coefficients dans **A**. Nous noterons $\mathbf{Rst}(P, S)$ le reste de la division euclidienne de P par S dans $\mathbf{K}[X]$. On a la relation :

$$\mathbf{Rst}(a.P, b.S) = a.\mathbf{Rst}(P, S).$$

Nous considérons maintenant la **suite des restes de l'algorithme d'Euclide,** démarrant avec le numéro 0, et définie de manière récurrente par :

$$\mathbf{Rst}^0(P, S) := P, \qquad \mathbf{Rst}^1(P, S) := S,$$
$$\mathbf{Rst}^{m+1}(P, S) := \mathbf{Rst}(\mathbf{Rst}^{m-1}(P, S), \mathbf{Rst}^m(P, S)).$$

On arrête la suite au plus petit entier n tel que $\mathbf{Rst}^{n+1}(P, S) = 0$.

Le polynôme $\mathbf{Rst}^m(P, S)$ est le **m-ième reste** de P et S.

Nous noterons par ailleurs $\mathbf{Rst}_j(P, S)$ le reste de degré j (avec $j < \inf(d(P), d(S))$, s'il existe, dans la suite des restes de l'algorithme d'Euclide. Nous prolongeons cette notation comme suit pour toutes les valeurs de $j \leqq \sup(d(P), d(S)+1)$. Nous posons $t = \sup(d(P), d(S)+1)$, et nous définissons :

$$\mathbf{Rst}_t(P, S) := P, \qquad \mathbf{Rst}_{t-1}(P, S) := S$$

et, pour $0 < j < t-1$:

$$\mathbf{Rst}_j(P, S) := \begin{cases} \mathbf{Rst}^m(P, S) & \text{si } j = d(\mathbf{Rst}^m(P, S)) \quad (m \geqq 1) \\ \mathbf{Rst}^{m+1}(P, S) & \text{si } j+1 = d(\mathbf{Rst}^m(P, S)) \quad (m \geqq 1) \\ 0 & \text{si ni } j \text{ ni } j+1 \text{ n'est le degré} \\ & \text{d'un reste } \mathbf{Rst}^m(P, S) \quad (m \geqq 1), \end{cases}$$

On remarquera que si $j+1$ et j sont les degrés de deux restes consécutifs, la définition reste cohérente. L'intérêt de cette définition-convention apparaîtra en I.2 (*b*) et I.2 (*c*).

Remarque 1 : Si un point a d'une extension de $\mathbf{K}$ n'est pas racine de P, il ne peut être racine de deux restes successifs. En effet le PGCD de deux restes successifs coïncide avec le PGCD de P et S.

Suite des restes signés de P et S

Étant donnés deux polynômes P et S nous appellerons :

suite des restes signés de P et S

la suite des restes de l'algorithme d'Euclide (démarrant avec P et S) avec des modifications de signes convenables comme suit :

$$\mathbf{Rss}^m(P, S) := (-1)^{(m(m-1))/2}\, \mathbf{Rst}^m(P, S)$$

de sorte qu'on ait la relation de récurrence :

$$\mathbf{Rss}^{m+1}(P, S) = -\mathbf{Rst}(\mathbf{Rss}^{m-1}(P, S), \mathbf{Rss}^m(P, S)).$$

avec l'initialisation :

$$\mathbf{Rss}^0(P, S) := P, \qquad \mathbf{Rss}^1(P, S) := S.$$

En posant $t = \sup(d(P), d(S)+1)$, nous notons également

$$\mathbf{Rss}_t(P, S) := P, \qquad \mathbf{Rss}_{t-1}(P, S) := S$$

et, pour $0 < j < t-1$:

$$\mathbf{Rss}_j(P, S) := \begin{cases} \mathbf{Rss}^m(P, S) & \text{si } j = d(\mathbf{Rss}^m(P, S)) \quad (m \geqq 1) \\ \mathbf{Rss}^{m+1}(P, S) & \text{si } j+1 = d(\mathbf{Rss}^m(P, S)) \quad (m \geqq 1) \\ 0 & \text{si ni } j \text{ ni } j+1 \text{ n'est le degré} \\ & \text{d'un reste } \mathbf{Rss}^m(P, S) \quad (m \geqq 1). \end{cases}$$

Suite de Sturm

Étant donnés deux polynômes P et Q nous appellerons :

suite de Sturm de P et Q

la suite des restes signés de P et $R := \mathbf{Rst}(P' Q, P)$:

$$\mathbf{Stu}^m(P, Q) := \mathbf{Rss}^m(P, R)$$

de sorte qu'on ait la relation de récurrence :

$$\mathbf{Stu}^{m+1}(P, Q) = -\mathbf{Rst}(\mathbf{Stu}^{m-1}(P, Q), \mathbf{Stu}^m(P, Q)).$$

avec l'initialisation

$$\mathbf{Stu}^0(P, Q) = P, \qquad \mathbf{Stu}^1(P, Q) = \mathbf{Rst}(P' Q, P).$$

Nous notons de même

$$\mathbf{Stu}_j(P, Q) := \mathbf{Rss}_j(P, R) \qquad \text{pour} \quad j \leqq d(P)$$

Si $Q = 1$ on note $\mathbf{Stu}^m(P, Q)$ et $\mathbf{Stu}_j(P, Q)$ respectivement $\mathbf{Stu}^m(P)$ et $\mathbf{Stu}_j(P)$ et on retrouve la notion classique de **suite de Sturm de P.**

Nombre de changements de signes

Toutes les définitions précédentes ont été faites en utilisant seulement la structure de corps de **K**. Nous allons maintenant introduire des notions qui nécessitent que le corps **K** soit muni d'un ordre. Supposons donc qu'on a fixé un ordre, noté $\leqq$, sur le corps **K** et notons **R** la clôture réelle de **K**. Si **K** est réel clos, **R** coïncide avec **K**.

On définit le **nombre de changements de signes** $V(a_0, \ldots, a_n)$ dans une suite $(a_0, \ldots, a_n)$ d'éléments de **K** par récurrence sur n :

$$V(a_0) = 0,$$

$V(a_0, \ldots, a_{n+1}) = V(a_0, \ldots, a_n)$ si $(a_0, \ldots, a_n) = (0, \ldots, 0)$ ou si a_{n+1} a le même signe que le dernier élément non nul de $(a_0, \ldots, a_n)$

$$V(a_0, \ldots, a_{n+1}) = \mathrm{V}(a_0, \ldots, a_n) + 1 \quad \text{sinon.}$$

Si $\mathbf{f} = [f_0, f_1, \ldots, f_n]$ est une suite de polynômes et si a et b sont deux éléments de $\mathbf{K} \cup \{+\infty\} \cup \{-\infty\}$ on appellera **nombre de changements de signes de $[\mathbf{f_0}, \mathbf{f_1}, \ldots, \mathbf{f_n}]$ en x** et on notera :

$$V(f_0, f_1, \ldots, f_n; x) = V(\mathbf{f}; x) := V(f_0(x), f_1(x), \ldots, f_n(x)).$$

On appelera **différence des changements de signe dans la suite $\mathbf{f_0}, \mathbf{f_1}, \ldots, \mathbf{f_n}$ entre a et b** la quantité :

$$V(f_0, f_1, \ldots, f_n; a, b) := V(f_0, f_1, \ldots, f_n; a) - V(f_0, f_1, \ldots, f_n; b).$$

NB : si $x = +\infty$ ou $-\infty$, le signe d'un polynôme $g(x)$ est donné par le signe du coefficient dominant de g et la parité de l'exposant correspondant.

Soit $a < b$ deux éléments de $\mathbf{K} \cup \{+\infty\} \cup \{-\infty\}$, on note :

$$\mathbf{V}_{\mathbf{Rss}}(P, S; a)$$

le nombre de changements de signes dans la suite des restes signés de P et S en a,

$$\mathbf{V}_{\mathbf{Rss}}(P, S; a, b) := \mathbf{V}_{\mathbf{Rss}}(P, S; a) - \mathbf{V}_{\mathbf{Rss}}(P, S; b)$$

$$\mathbf{V}_{\mathbf{Rss}}(P, S) := \mathbf{V}_{\mathbf{Rss}}(P, S; -\infty) - \mathbf{V}_{\mathbf{Rss}}(P, S; +\infty)$$

$$\mathbf{V}_{\mathbf{Stu}}(P, Q; a) := \mathbf{V}_{\mathbf{Rss}}(P, R; a), \qquad \text{où} \quad R = \mathbf{Rst}(P' Q, P)$$

$$\mathbf{V}_{\mathbf{Stu}}(P, Q; a, b) := \mathbf{V}_{\mathbf{Rss}}(P, R; a, b)$$

$$\mathbf{V}_{\mathbf{Stu}}(P, Q) := \mathbf{V}_{\mathbf{Rss}}(P, R)$$

$$\mathbf{V}_{\mathbf{Stu}}(P; a) := \mathbf{V}_{\mathbf{Stu}}(P, 1; a)$$

$$\mathbf{V}_{\mathbf{Stu}}(P; a, b) := \mathbf{V}_{\mathbf{Stu}}(P, 1; a, b)$$

$$\mathbf{V}_{\mathbf{Stu}}(P) := \mathbf{V}_{\mathbf{Stu}}(P, 1)$$

Soient $a<b$ comme ci-dessus et $\varepsilon \in \{+, 0, -\}$, on note :

$$\mathbf{c}_{\varepsilon}(P, Q; a, b)$$

le nombre d'éléments de :

$$\{u \in]a, b[/ P(u) = 0, \text{ signe } (Q(u)) = \varepsilon\}$$

$$\mathbf{c}_{\varepsilon}(P, Q) := \mathbf{c}_{\varepsilon}(P, Q; -\infty, +\infty)$$

$$\mathbf{c}(P; a, b) := \mathbf{c}_{+}(P, 1; a, b)$$

$$\mathbf{c}(P) := \mathbf{c}_{+}(P, 1)$$

(b) Propriétés de la suite de Sturm

THÉORÈME 1 (*voir* Sylvester [18] pour un résultat analogue) : *Soit un corps* **K**, *soit* $\leqq$ *un ordre sur* **K** *et soit* **R** *la clôture réelle de* **K** *muni de l'ordre* $\leqq$. *Soient P et Q deux polynômes quelconques à coefficients dans* **K** *et a et b (avec* $a<b$*) des points de* **K** *qui ne sont pas racines de P. Alors :*

(i) $\mathbf{V}_{\mathbf{Stu}}(P, Q; a, b) = \mathbf{c}_{+}(P, Q; a, b) - \mathbf{c}_{-}(P, Q; a, b)$.

(ii) $\mathbf{V}_{\mathbf{Stu}}(P, Q) = \mathbf{c}_{+}(P, Q) - \mathbf{c}_{-}(P, Q)$.

Démonstration : Soit $n+1$ la longueur de la suite de Sturm de P et Q, $\mathbf{Stu}^n(P, Q)$ est donc le dernier élément de cette suite et le PGCD de P et $P' Q$. Soit **f** la suite définie par $f_m = \mathbf{Stu}^m(P, Q)/\mathbf{Stu}^n(P, Q)$. La démonstration du théorème 1 est une conséquence immédiate des lemmes suivants, qu'il est facile de démontrer avec la stratégie classique pour la preuve du théorème de Sturm. □

LEMME 1 : *Soient P et S deux polynômes quelconques à coefficients dans un corps ordonné* **K**. *Soit* $n+1$ *la longueur de la suite des restes signés de P et S;* $\mathbf{Rss}^n(P, S)$ *est donc le dernier élément de cette suite et le PGCD de P et S. Soit* **g** *la suite définie par* $g_m = \mathbf{Rss}^m(P, S)/\mathbf{Rss}^n(P, S)$.

Si c est une racine dans **R** *de* g_i, $i \neq 0$, *il y a exactement un changement de signe dans la suite* $(g_{i-1}(x), g_i(x), g_{i+1}(x))$ *pour tout x suffisamment proche de c.*

LEMME 2 : (i) f_0 *a pour racines les racines de P non racines de Q,*

(ii) $V(\mathbf{f}; x) = \mathbf{V}_{\mathbf{Stu}}(P, Q; x)$ *pour x non zéro de P,*

(iii) *le nombre* $V(\mathbf{f}; x)$ *diminue de* 1 *quand on passe à droite d'une racine de* f_0 *avec Q positif et augmente de* 1 *quand on passe à droite d'une racine de* f_0 *avec Q négatif,*

(iv) *le nombre* $V(\mathbf{f}; x)$ *ne change pas quand on passe à droite d'une racine de* f_i $(i = 1, \ldots, n)$ *non racine de* f_0.

COROLLAIRE 1 (théorème de Sturm [17]) : *Si a et b ne sont pas racines de P,* $\mathbf{V}_{\mathbf{Stu}}(P; a, b)$ *est le nombre de racines dans* **R** *de P entre a et b. En particulier* $\mathbf{V}_{\mathbf{Stu}}(P)$ *est le nombre de racines dans* **R** *de P.*

COROLLAIRE 2 : *Si a et b ne sont pas racines de P,* $\mathbf{V}_{Stu}(P, Q^2; a, b)$ *est le nombre de racines dans* **R** *de P non racines de Q entre a et b.*

COROLLAIRE 3 : *On a donc les égalités :*

$$\mathbf{V}_{Stu}(P; a, b) = \mathbf{c_0}(P, Q; a, b) + \mathbf{c}_+(P, Q; a, b) + \mathbf{c}_-(P, Q; a, b),$$
$$\mathbf{V}_{Stu}(P, Q^2; a, b) = \mathbf{c}_+(P, Q; a, b) + \mathbf{c}_-(P, Q; a, b),$$
$$\mathbf{V}_{Stu}(P, Q; a, b) = \mathbf{c}_+(P, Q; a, b) - \mathbf{c}_-(P, Q; a, b),$$

qui permettent de calculer $\mathbf{c_0}(P, Q; a, b)$, $\mathbf{c}_+(P, Q; a, b)$ *et* $\mathbf{c}_-(P, Q; a, b)$ *connaissant* $\mathbf{V}_{\mathbf{Stu}}(P; a, b)$, $\mathbf{V}_{\mathbf{Stu}}(P, Q^2; a, b)$ *et* $\mathbf{V}_{\mathbf{Stu}}(P, Q; a, b)$.

Remarque 2 : Dans l'article [18], Sylvester étudie le nombre $\mathbf{V}_{\mathbf{Rss}}(P, S)$ de changements de signe dans la suite des restes signés de deux polynômes P et S, au moins dans le cas où P et S sont sans facteurs carrés et sans racine commune, en termes du nombre d'entrecroissements entre les racines de P et celles de S. Nous pouvons donner l'interprétation suivante pour le nombre $\mathbf{V}_{\mathbf{Rss}}(P, S; a, b)$ lorsque P n'a que des racines simples sur l'intervalle : on suppose que $P(a).P(b) \neq 0$, on compte les racines de P sur l'intervalle en affectant à chaque racine de P un coefficient égal au signe de $P'S$. Le nombre trouvé est égal à $\mathbf{V}_{\mathbf{Rss}}(P, S; a, b)$. La preuve est essentiellement la même que celle du théorème 1.

Remarque 3 : Le calcul de la suite de Sturm se fait uniquement avec les opérations de corps de **K**. Le calcul du nombre $\mathbf{V}_{\mathbf{Stu}}(P, Q; a, b)$ pour a et b deux éléments de **K** (et même le fait que $a<b$) dépendent du choix de l'ordre sur **K**. Le résultat obtenu concerne le nombre de racines dans le corps réel clos **R** entre a et b.

D'un point de vue algorithmique, ceci signifie que la suite de Sturm est calculable dès que les opérations de **K** le sont. La détermination du nombre des racines dans **R** entre a et b (a et b deux éléments de **K** non racines de P avec $a<b$ pour l'ordre choisi) s'obtient ensuite par un nombre fini de tests de signes portant sur des éléments de **K**, il est calculable dès que l'ordre sur **K** l'est (c'est-à-dire qu'il y a un algorithme exact pour déterminer le signe d'un élément). Tous les calculs et tests se déroulent donc dans **K**.

On peut en outre également appliquer le théorème 1 si a et b sont des éléments de $\mathbf{R} \cup \{+\infty\} \cup \{-\infty\}$ et il est encore possible de déterminer exactement les signes dans **R** des polynômes de la suite de Sturm par des calculs dans **K** si a et b sont convenablement codés dans **K** (*cf.* par exemple [8]).

Le résultat du calcul dépend naturellement de l'ordre choisi sur **K** : considérons par exemple le polynôme $P = Y^2 - X$ de $\mathbb{Q}(X)[Y]$. Si l'ordre choisi sur $\mathbb{Q}(X)$ est celui qui rend X positif et plus petit que tout rationnel strictement positif, P a deux racines dans la clôture réelle de $\mathbb{Q}(X)$ pour cet ordre, alors que si l'ordre choisi sur $\mathbb{Q}(X)$ est celui qui rend X négatif et plus grand que tout rationnel strictement négatif, P n'a aucune racine dans la clôture réelle de $\mathbb{Q}(X)$ pour cet ordre.

(c) Problèmes de spécialisation

Soient **A** un anneau intègre, **K** son corps de fractions, P et Q des polynômes de **K** $[X]$. Supposons qu'on ait effectué le calcul de la suite de Sturm dans le corps **K**, et qu'on spécialise les coefficients de P et Q, c'est-à-dire qu'on considère un morphisme Sp de **A** dans un anneau intègre **A'** et les images Sp (P) et Sp (Q) de P et Q dans l'anneau **A'** $[X]$. Un exemple typique de cette situation est $\mathbf{A} = \mathbb{Z}[Y]$ et $\mathbf{A}' = \mathbb{Z}[\xi]$ où ξ est un nombre algébrique.

La suite de Sturm associée à Sp (P) et Sp (Q) ne peut pas s'obtenir facilement à partir de celle de P et Q parce que dans le processus de division euclidienne de P et Q, il apparaît des éléments de **A** au dénominateur, et que ces éléments peuvent très bien se spécialiser à 0. Dans ce cas, la suite de Sturm de Sp (P) et Sp (Q) ne s'obtient pas en spécialisant la suite de Sturm de P et Q, et les degrés des polynômes de la suite de Sturm de Sp (P) et

Sp (Q) ne coïncident pas avec ceux de la suite de Sturm de P et Q. Il faut en principe recommencer tout le calcul.

Nous allons voir dans le paragraphe suivant que grâce à la théorie des sous-résultants on peut obtenir la suite des restes par un algorithme qui se spécialise bien. On pourra ainsi définir en II.1 la suite de Sturm-Habicht, qui permettra aussi de compter les racines dans **R** d'un polynôme et se comportera bien par spécialisation.

Exemple 1 : Considérons l'exemple du polynôme général de degré 4,

$$P = X^4 + p X^2 + q X + r.$$

La suite de Sturm de P et P', calculée dans $Q(p, q, r)[X]$ est

$$\mathbf{Stu}^0(P) = X^4 + p X^2 + q X + r$$

$$\mathbf{Stu}^1(P) = 4 X^3 + 2 p X + q$$

$$\mathbf{Stu}^2(P) = -(1/4)(2 p X^2 + 3 q X + 4 r)$$

$$\mathbf{Stu}^3(P) = -\frac{4((2.p^3 - 8.pr + 9.q^2).X + p^2 q + 12.qr)}{p^2}$$

$$\mathbf{Stu}^4(P) = \frac{p^2.(16.p^4 r - 4.p^3 q^2 - 128.p^2 r^2 + 144.pq^2 r - 27.q^4 + 256.r^3)}{4.(2.p^3 - 8.pr + 9.q^2)^2}.$$

Lorsqu'on choisit des valeurs particulières p, q, r pour p, q, r la suite de Sturm de $P = X^4 + p.X^2 + q.X + r$ s'obtient en général en substituant dans la suite de Sturm de P la valeur de P. Toutefois lorsqu'un des dénominateurs s'annule en p, q, r cette substitution n'a plus de sens et il faut faire un nouveau calcul pour obtenir la suite de Sturm de P.

C'est ainsi que si $p = 0$, la suite de Sturm de $P = X^4 + q X + r$ est

$$\mathbf{Stu}^0(P) = X^4 + q X + r$$

$$\mathbf{Stu}^1(P) = 4 X^3 + q$$

$$\mathbf{Stu}^2(P) = \frac{3 q X + 4 r}{4}$$

$$\mathbf{Stu}^3(P) = \frac{-(27 q^4 + 256 r^3)}{27 q^3}.$$

I.2. POLYNÔMES SOUS-RÉSULTANTS

Il est clair qu'on ne peut plus parler de sous-résultants sans s'inspirer de l'article de synthèse de [15]. Nous serons cependant en désaccord avec lui sur certains points de détail. Pour la théorie des sous-résultants voir également [4, 5, 7, 12]. Pour l'expression des sous-résultants en fonction des racines (point que nous n'abordons pas) voir [18, 3, 13, 6].

(a) Définitions

Nous rappelons dans ce paragraphe la notion de polynôme sous-résultant et en donnons une légère généralisation. L'utilité de cette généralisation s'avèrera lorsque nous étudierons les problèmes liés à la spécialisation.

Nous établissons en outre les relations liant polynômes sous-résultants « ordinaires » et « généralisés ».

On considère toujours un anneau intègre **A** et son corps de fractions **K**.

Si P et S sont dans **A** $[X]$, p, s, et j des entiers avec $d(P) \leqq p$, $d(S) \leqq s$ et $j < \inf(p, s)$, nous notons $\mathbf{Sylv}_j(P, p, S, s)$ la j-ième matrice extraite de la matrice de Sylvester de P et S (considérés comme étant de degrés p et s) : sur la base $X^{p+s-j-1}, \ldots, X^2, X, 1$, les vecteurs lignes successifs de cette matrice sont : $P.X^{s-j-1}, \ldots, P.X, P, S.X^{p-j-1}, \ldots, S.X, S$. Cette matrice possède $p+s-2j$ lignes et $p+s-j$ colonnes.

Si $P = a_p X^p + a_{p-1} X^{p-1} + \ldots + a_0$, $S = b_s X^s + b_{s-1} X^{s-1} + \ldots + b_0$, $\mathbf{Sylv}_j(P, p, S, s)$ est donc la matrice :

$$\mathbf{Sylv}_j(P, p, S, s) = \underbrace{\begin{bmatrix} a_p & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_p & \cdots & a_0 & 0 & \cdots & 0 \\ \vdots & \ddots & & & \ddots & & \vdots \\ 0 & \cdots & 0 & a_p & \cdots & a_0 & 0 \\ 0 & \cdots & \cdots & 0 & a_p & \cdots & a_0 \\ b_s & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & b_s & \cdots & b_0 & 0 & \cdots & 0 \\ \vdots & \ddots & & & \ddots & & \vdots \\ 0 & \cdots & 0 & b_s & \cdots & b_0 & 0 \\ 0 & \cdots & \cdots & 0 & b_s & \cdots & b_0 \end{bmatrix}}_{p+s-j \text{ colonnes}} \left.\begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix}\right\} \begin{matrix} s-j \text{ lignes de P} \\ \\ \\ \\ \\ p-j \text{ lignes de S} \\ \\ \\ \\ \\ \end{matrix} \Big\} p+s-2j \text{ lignes}$$

Par définition, le **déterminant polynomial d'une matrice** possédant N lignes et M colonnes, avec $M \geqq N$ est un polynôme de degré inférieur ou égal à

$j = M - N$: son coefficient de degré d est le déterminant extrait de cette matrice sur les colonnes 1, 2, ..., $N-1$, $M-d$.

Les **polynômes sous-résultants** de P et S (considéré comme étant de degrés p et s) sont les déterminants polynomiaux des matrices $\mathbf{Sylv}_j(P, p, S, s)$ et ils seront notés :

$$\mathbf{Sres}_j(P, p, S, s).$$

On a la relation :

$$\mathbf{Sres}_j(a.P, p, b.S, s) = a^{s-j}.b^{p-j}.\mathbf{Sres}_j(P, p, S, s).$$

Il est clair que les polynômes sous-résultants sont à coefficients dans **A** et que $\mathbf{Sres}_j(P, p, S, s)$ est de degré inférieur ou égal à j. Si $\mathbf{Sres}_j(P, p, S, s)$ est de degré $<j$ on dit qu'il est **défectueux**.

Les **coefficients sous-résultants** de P et S (considérés comme étant de degrés p et s) sont les :

$$\mathbf{sr}_j(P, p, S, s) := \mathbf{cf}_j(\mathbf{Sres}_j(P, p, S, s)).$$

Le coefficient sous-résultant $\mathbf{sr}_j(P, p, S, s)$ est nul si et seulement si le degré de $\mathbf{Sres}_j(P, p, S, s)$ est $<j$ (c'est-à-dire si le polynôme sous-résultant est défectueux).

Le sous-résultant $\mathbf{Sres}_0(P, p, S, s) = \mathbf{sr}_0(P, p, S, s)$ est le résultant de P et S si $p = d(P)$ et $s = d(S)$.

La **suite des sous-résultants** est la liste des $\mathbf{Sres}_j(P, p, S, s)$ pour j descendant de $\inf(p, s) - 1$ à 0. Nous donnerons en 2 (*c*) une extension « raisonnable » de la suite des sous-résultants en la faisant démarrer à $j = p$, du moins lorsque $p > s = d(S)$.

Nous appellerons **polynôme sous-résultant standard** un polynôme sous-résultant $\mathbf{Sres}_j(P, p, S, s)$ où $d(P) = p$ et $d(S) = s \leq p$. Ordinairement les sous-résultants calculés seront les sous-résultants standards [1] avec $p = d(P)$ et $s = d(S)$. Mais après spécialisation, il se peut que le degré de P ou celui de S se retrouve diminué, aussi est-il intéressant d'étudier le comportement des sous-résultants dans le cas où l'un des deux degrés est plus petit que le degré annoncé. Si les deux degrés sont trop petits, tous les polynômes sous-résultants sont nuls. Les autres polynômes sous-résultants peuvent tous être facilement

[1] Les polynômes sous-résultants définis dans [15], p. 118, sont les polynômes sous-résultants standards.

calculés à partir des polynômes sous-résultants standards (ou vice versa si l'autre polynôme sous-résultant n'est pas identiquement nul). Les relations entre polynômes sous-résultants standards et polynômes sous-résultants découlent de la proposition suivante.

PROPOSITION 1 : *Nous supposons* $d(P) \leqq p$, $d(S) \leqq s$, $j < \inf(p, s)$

(*a*) *Si* $d(P) < p$ *et* $d(S) < s$, *alors*

$$\mathbf{Sres}_j(P, p, S, s) = 0$$

(*b*) $\mathbf{Sres}_j(P, p, S, s) = (-1)^{(p-j)(s-j)} \mathbf{Sres}_j(S, s, P, p)$ *et en particulier*

$$\mathbf{Sres}_j(P, p, S, p-1) = \mathbf{Sres}_j(S, p-1, P, p) \qquad (d(S) \leqq p-1)$$

(*c*) *Si* $s' \geqq s$ *et* $d(P) = p$ *alors*

(i) $\mathbf{Sres}_j(P, p, S, s') = cd(P)^{s'-s} . \mathbf{Sres}_j(P, p, S, s)$,

(ii) $\mathbf{Sres}_j(S, s', P, p) = ((-1)^{p-j} cd(P))^{s'-s} . \mathbf{Sres}_j(S, s, P, p)$.

Démonstration : Utiliser la définition des polynômes sous-résultants avec des propriétés élémentaires des déterminants. □

NB : lorsque P est unitaire de degré p, la proposition 1 (*c*) (i) montre que le polynôme sous-résultant $\mathbf{Sres}_j(P, p, S, s)$ ne dépend pas du choix de $s \geqq d(S)$.

PROPOSITION 2 : *Soient* P *et* S *des polynômes de degrés* p *et* $s < p-1$, *alors :*

(*a*) $\mathbf{Sres}_j(P, p, S, p-1) = 0$ *si* $s < j < p-1$,

(*b*) $\mathbf{Sres}_s(P, p, S, p-1) = (cd(P)\, cd(S))^{p-s-1} S$,

(*c*) $\mathbf{Sres}_j(P, p, S, p-1) = cd(P)^{p-s-1} \mathbf{Sres}_j(P, p, S, s)$ *pour* $j < s$.

Démonstration : Utiliser la définition de polynômes sous-résultants avec des propriétés élémentaires des déterminants □

(b) Polynômes sous-résultants, suite des restes et PGCD

Nous établissons dans ce paragraphe les formules reliant explicitement la suite des restes à la suite des polynômes sous-résultants standards.

Rappelons que l'on note **Rst** (P, S) le reste de la division de P par S. Lorsque $p = d(P) \geqq s = d(S)$, le polynôme $cd(S)^{p-s+1}$. **Rst** (P, S) est appelé le **pseudo-reste** de la division de P par S, et nous le noterons **Prst** (P, S). Le pseudo-reste est donc proportionnel (par un élément de **A**) au reste, et il est à coefficients dans **A** (cela résulte par exemple de la proposition 4 infra). On

a la relation :

$$\mathbf{Prst}\ (a.P,\ b.S) = a.b^{p-s+1}.\mathbf{Prst}\ (P,\ S).$$

Dans tout le paragraphe nous noterons (H) l'hypothèse suivante :

(H) $\quad p = d\ (P) \geqq s = d\ (S), \quad R = \mathbf{Rst}\ (P,\ S) \quad$ et $\quad r = d\ (R)$

Nous commençons par une proposition qui sert de base aux calculs qui suivent ([2]) :

PROPOSITION 3 : *Supposons* (H) *et* $j < s$, *alors :*

(i) $\mathbf{Sres}_j\ (P,\ p,\ S,\ s) = \mathbf{Sres}_j\ (R,\ p,\ S,\ s)$,

(ii) $\mathbf{Sres}_j\ (S,\ s,\ P,\ p) = \mathbf{Sres}_j\ (S,\ s,\ R,\ p)$.

Démonstration : par exemple (i). Chaque ligne $P.X^k$ de la matrice $\mathbf{Sylv}_j\ (P,\ p,\ S,\ s)$ peut être remplacée par la ligne $R.X^k$ en lui rajoutant des lignes $-c_m.S.X^{k+m}$, en choisissant pour c_m les coefficients du polynôme B dans l'identité de la division euclidienne : $P = B.S + R$. Ces manipulations élémentaires ne modifient pas les déterminants extraits. Or, la nouvelle matrice obtenue n'est autre que $\mathbf{Sylv}_j$ (R, p, S, s). □

PROPOSITION 4 : *Lorsque* $p = d\ (P) \geqq s = d\ (S)$, *on a les égalités*

(i) $\mathbf{Sres}_{s-1}\ (S,\ s,\ P,\ p) = \mathbf{Prst}\ (P,\ S)$,

(ii) $\mathbf{Sres}_{s-1}\ (P,\ p,\ S,\ p-1) = (-cd\ (P))^{p-s-1}\ \mathbf{Prst}\ (P,\ S)$,

(iii) *Si* S *est unitaire et* $p' \geqq p$ *on a :*

$$\mathbf{Sres}_{s-1}\ (S,\ s,\ P,\ p') = \mathbf{Sres}_{s-1}\ (S,\ s,\ P,\ p) = \mathbf{Prst}\ (P,\ S) = \mathbf{Rst}(P,\ S).$$

Démonstration : Utiliser les résultats des propositions 1, 2 et 3. □

Le cas ordinaire

C'est le cas où les degrés dans la suite des restes baisssent de un en un.

PROPOSITION 5 : *Supposons* (H) *et* $p = s + 1$. *Alors nous avons :*

(*a*) $\mathbf{Sres}_{s-1}\ (P,\ p,\ S,\ s) = cd\ (S)^2\ R = \mathbf{Prst}\ (P,\ S)$,

(*b*) $\mathbf{Sres}_j\ (P,\ p,\ S,\ s) = cd\ (S)^2\ \mathbf{Sres}_j\ (S,\ s,\ R,\ s-1)$ *pour* $j < s-1$.

([2]) En fait, tous les résultats des paragraphes (*b*) et (*c*) sont basés sur l'utilisation systématique des propositions 1, 2, 3 et 4, qui sont toutes trois élémentaires.

PROPOSITION 6 : *Supposons* (H), *et que les degrés dans la suite des restes décroissent de un en un (en commençant au polynôme P). Posons* $c(s) := cd(S)$ *et, pour* $j<s$, $c(j) := cd(\mathbf{Rst}_j)$. *Alors :*

$$\mathbf{Sres}_j(P, p, S, s) = (c(s).c(s-1)\ldots c(j+1))^2\ \mathbf{Rst}_j(P, S)$$

pour $j<s$.

En particulier, chaque polynôme sous-résultant est égal, à un carré dans **K** près, au reste correspondant.

Démonstration des propositions 5 *et* 6 *:* La proposition 6 résulte de la proposition 5, par induction sur j. La proposition 5 (a) est un cas particulier de la proposition 4 (i). La proposition 5 (b) s'obtient en appliquant la proposition 3 puis les propositions 1 (b) et 1 (c) (i). □

Le théorème de Habicht

Nous redémontrons maintenant le « théorème de Habicht » dans [15] par un calcul direct.

THÉORÈME 2 (théorème de Habicht [12]) : *Nous supposons* $d(P)\leqq p=s+1$, $d(S)\leqq s$.

Nous posons

$$S_p := P, \qquad S_s := S, \qquad S_j := \mathbf{Sres}_j(P, p, S, s) \qquad pour \quad j<s,$$

$$C(p) := 1, \qquad C(j) := \mathbf{cf}_j(S_j) \qquad pour \quad j\leqq s.$$

(i) *Alors, pour* $0\leqq h<j\leqq s$, *on a :*

$$C(j+1)^{2(j-h)}S_h = \mathbf{Sres}_h(S_{j+1}j+1, S_j, j).$$

(ii) *En particulier, lorsque* $j<s$ *on obtient*

$$\mathbf{sr}_{j+1}(P, p, S, s)^{2(j-h)}S_h = \mathbf{Sres}_h(S_{j+1}, j+1, S_j, j)$$

(iii) *Si* $d(S_{j+1})=j+1$ *et* $d(S_j)=j\leqq s$, *on obtient :*

$$C(j+1)^2 S_{j-1} = \mathbf{Prst}(S_{j+1}, S_j).$$

Démonstration ([3]) :

(ii) est la même chose que (i);

(iii) résulte de (i), avec $h=j-1$, et de la proposition 4 (i).

(i) Les égalités à démontrer sont des identités algébriques. On peut donc supposer que les coefficients de P et S sont des *variables indépendantes*. On applique alors les résultats de la proposition 6. Les deux membres de l'égalité à établir sont des multiples de $\mathbf{Rst}_h$. Les calculs sont simples. Nous les explicitons en reprenant les notations de la proposition 6.

Nous posons

$$R_j := \mathbf{Rst}_j(\mathbf{P}, \mathbf{S}), \qquad \gamma(j) := (c(s).c(s-1)\ldots c(j+1))^2 = C(j)/c(j).$$

On a donc

$$C(j+1)^2 = \gamma(j).\gamma(j+1), \qquad S_j = \gamma(j).R_j.$$

Par ailleurs

$$\begin{aligned}\mathbf{Sres}_h(S_{j+1}, j+1, S_j, j) &= \gamma(j+1)^{j-h}.\gamma(j)^{j-h+1}\,\mathbf{Sres}_h(R_{j+1}, j+1, R_j, j)\\ &= \gamma(j+1)^{j-h}.\gamma(j)^{j-h+1}.(c(j).c(j-1)\ldots c(h+1))^2 R_h\\ &= \gamma(j+1)^{j-h}.\gamma(j)^{j-h}.\gamma(h).R_h\end{aligned}$$

et

$$S_h = \gamma(h).R_h. \quad \square$$

Le cas défectueux

PROPOSITION 7 : *Supposons* (H). *On a :*

(*a*) (i) $\mathbf{Sres}_{s-1}(P, p, S, s) = (-cd(S))^{p-s+1} R = (-1)^{p-s+1}\,\mathbf{Prst}(P, S)$,

(ii) $\mathbf{Sres}_j(P, p, S, s) = ((-1)^{s-j} cd(S))^{p-s+1}\,\mathbf{Sres}_j(S, s, R, s-1)$ *pour* $j<s-1$.

(*b*) *On en déduit*

(i) $\mathbf{Sres}_j(P, p, S, s) = 0$ *si* $r<j<s-1$,

(ii) $\mathbf{Sres}_r(P, p, S, s) = ((-1)^{p-s-1} cd(S).cd(R))^{s-r-1}\,\mathbf{Sres}_{s-1}(P, p, S, s)$,

(iii) $\mathbf{Sres}_j(P, p, S, s) = (-1)^{(p-s-1)(s-j)} cd(S)^{p-r}\,\mathbf{Sres}_j(S, s, R, r)$ *pour* $j<r$.

([3]) Pour que le théorème affirme autre chose que des égalités $0=0$, il faut que l'on ait $d(P)=p$ ou $d(S)=s$.

Démonstration : Les égalités de (*a*) et (*b*) sont conséquences des propositions 1, 2 et 3. □

PROPOSITION 8 : *Supposons* (H), *et définissons* $R_{-1} := P$, $R_0 := S$, $R_i := \mathbf{Rst}^{i+1}(P, S)$

$$d_i = d(R_i), \qquad e_i = d_{i-1} - d_i + 1, \qquad f_i = d_{i-1} - d_{i+1}, \qquad c_i = cd(R_i)$$

alors, pour tout degré $d_i < s$, *on a :*

$$R_{i+1} = \mathbf{Sres}_{d_i - 1}(P, p, S, s)/(\varepsilon_i . c_0^{f_0} . c_1^{f_1} \ldots c_{i-1}^{f_{i-1}} . c_i^{e_i})$$

où $\varepsilon_i = 1$ *si* $\sum_{0 \leq k \leq i} (1 + d_k - d_i) . e_k$ *est pair,* -1 *sinon.*

Démonstration : Se démontre par récurrence sur j en utilisant la proposition 7. On amorce la pompe avec (*a*) (i) et la récurrence fonctionne grâce à (*b*) (iii). □

Sous-résultants et restes

THÉORÈME 3 (sous-résultants et restes [12], [15]) : (*a*) *Supposons* (H). *Soit* $j < s$. *Le polynôme* $\mathbf{Sres}_j(P, p, S, s)$ *est égal, à un facteur non nul près dans* $\mathbf{K}$, *à* $\mathbf{Rst}_j(P, S)$ (4).

(*b*) *Ce résultat reste vrai si* $d(P) \leqq p$, $d(S) \leqq s$, *l'une des deux inégalités étant une égalité, et* $j < \inf(d(P), d(S))$, *ou encore si* $d(P) = p > s > j \geqq d(S)$.

Démonstration : (*a*) c'est vérifié pour $j = s-1, \ldots, r$ d'après la proposition 7, alinéas (*b*) (i) et (*b*) (ii). Pour $j < r$ on utilise l'alinéa (*b*) (iii) qui nous ramène au cas de la suite des restes démarrant avec S et R (preuve par induction sur le degré de P donc).

(*b*) la proposition 1 (*c*) montre que $\mathbf{Sres}_j(P, p, S, s)$ et $\mathbf{Sres}_j(P, d(P), S, d(S))$ sont proportionnels avec un facteur non nul pour $j < \inf(d(P), d(S))$.

(4) On notera ici l'utilité de la définition conventionnelle de certains $\mathbf{Rst}_j(P, S)$ comme égaux à 0.

Par ailleurs, si $d(P)=p>s>j\geqq d(S)$, on a

$$cd(P)^{p-s-1}\,\mathbf{Sres}_j(P, p, S, s)$$

$$=\mathbf{Sres}_j(P, p, S, p-1) \quad \text{[prop. 1 (c) (i)]}$$

$$=0 \qquad \text{si} \quad d(S)<j<p-1 \quad \text{[prop. 2 (a)]}$$

$$(cd(P)\,cd(S))^{p-s-1}\,S \text{ si } j=d(S) \quad \text{[prop. 2 (b)]}$$

(et par définition on a $\mathbf{Rst}_{d(S)}(P, S)=S$) □.

COROLLAIRE : *Supposons que $s=d(S)$ ou $p=d(P)$, et que S ne divise pas P (c'est-à-dire* $\mathbf{Sres}_{s-1}(P, p, S, s)\neq 0$*). Alors le dernier sous-résultant non nul* $\mathbf{Sres}_n(P, p, S, s)$ *est de degré n (c'est-à-dire non défectueux). Il est égal au PGCD de P et S dans* $\mathbf{K}[X]$.

Démonstration : Cela résulte du théorème 3 et du fait que le dernier reste non nul dans la suite des restes est le PGCD de P et S. □

Le théorème des sous-résultants

Le théorème suivant complète le théorème de Habicht dans le cas défectueux.

THÉORÈME 4 (théorème des sous-résultants [12], [15]) : *Nous supposons $d(P)\leqq p=s+1$, $d(S)\leqq s$, l'une des deux inégalités étant une égalité.*

(a) Si $j<s-1$ avec $\mathbf{Sres}_{j+1}(P, p, S, s)$ *non défectueux et* $\mathbf{Sres}_j(P, p, S, s)$ *défectueux, de degré k, alors* $\mathbf{Sres}_k(P, p, S, s)$ *est proportionnel à* $\mathbf{Sres}_j(P, p, S, s)$ *avec un facteur non nul, (en particulier* $\mathbf{Sres}_k(P, p, S, s)$ *n'est pas défectueux).*

(b) Plus précisément, avec les mêmes hypothèses, en notant $S_h := \mathbf{Sres}_h(P, p, S, s)$ $(h<s)$ on a les relations :

(i) $cd(S_j)^{(j-k)}\,S_j=cd(S_{j+1})^{(j-k)}\,S_k$.

(ii) $S_{k+1}=\ldots=S_{j-1}=0 \qquad (si\ k<j-1)$.

(iii) $(-cd(S_{j+1}))^{(j-k+2)}\,S_{k-1}=\mathbf{Prst}(S_{j+1}, S_j)$.

Démonstration : (*a*) et (*b*) (ii) : déjà énoncés (sous une autre forme) dans le théorème 3 lorsqu'on est dans l'une des hypothèses de ce théorème. De manière générale, le (*a*) résulte du (*b*) qui se démontre directement à partir

du théorème de Habicht comme suit :

(*b*) (i) le théorème de Habicht nous donne :

$$cd(S_{j+1})^{2(j-k)} S_k = \mathbf{Sres}_k(S_{j+1}, j+1, S_j, j),$$

et la proposition 2 (*b*) :

$$\mathbf{Sres}_k(S_{j+1}, j+1, S_j, j) = (cd(S_j) . cd(S_{j+1}))^{j-k} S_j,$$

(*b*) (iii) le théorème de Habicht nous donne :

$$cd(S_{j+1})^{2(j-k+1)} S_{k-1} = \mathbf{Sres}_{k-1}(S_{j+1}, j+1, S_j, j),$$

et la proposition 4 (ii) :

$$\mathbf{Sres}_{k-1}(S_{j+1}, j+1, S_j, j) = (-cd(S_{j+1}))^{j-k} \mathbf{Prst}(S_{j+1}, S_j),$$

(*b*) (ii) on applique le théorème de Habicht comme ci-dessus et on conclut par la proposition 2 (*a*). □

(c) Spécialisation des polynômes sous-résultants

Nous venons de voir que la suite des sous-résultants nous donne la suite des restes. Étant donnée une spécialisation (*i.e.* un homomorphisme d'anneaux) Sp : $\mathbf{A} \to \mathbf{A}'$, nous étudions la possibilité de calculer « facilement » les polynômes sous-résultants standards de Sp (*P*) et Sp (*S*) lorsqu'on connaît les polynômes sous-résultants standards de *P* et *S* (polynômes de $\mathbf{A}[X]$). La situation typique de spécialisation que nous avons en tête est naturellement l'application définie par l'évaluation de certaines variables indépendantes en des nombres algébriques. On aura ainsi la suite des restes dans la situation spécialisée sans avoir besoin de refaire un nouveau calcul.

Comportement des polynômes sous-résultants par spécialisation

1er cas : *les degrés de P et S sont conservés au cours d'une spécialisation*

Les polynômes sous-résultants standards se spécialisent en les polynômes sous-résultants standards.

2e cas : *un seul des deux degrés de P ou S s'abaisse au cours d'une spécialisation*

Supposons que nous ayons déjà calculé les polynômes sous-résultants $\mathbf{Sres}_j(P, p, S, p-1)$.

Si $d(\mathrm{Sp}(P))=d(P)$, on obtient en spécialisant ces polynômes sous-résultants une suite de polynômes sous-résultants non tous nuls, même si $d(\mathrm{Sp}(S))<d(S)$.

Par contre, si $d(\mathrm{Sp}(S))=d(S)=s<p-1$ et $d(\mathrm{Sp}(P))<d(P)$, on a, pour tout j, $\mathrm{Sp}(\mathbf{Sres}_j(P, p, S, p-1))=0$. Il suffit cependant de calculer $\mathbf{Sres}_j(P, p, S, s)$ à partir se $\mathbf{Sres}_j(P, p, S, p-1)$ en utilisant la proposition 1 pour obtenir par spécialisation des polynômes sous-résultants non nuls.

3e cas : *les degrés de P et S s'abaissent de* 1 *pour une raison commune*

Nous supposons que $cd(P)$ et $cd(S)$ s'écrivent respectivement : $cd(P)=a.c_p$ et $cd(S)=a.d_s$ avec $\mathrm{Sp}(a)=0$. Plus précisément nous écrivons :

$$P=a.c_pX^p+a_{p-1}X^{p-1}+\ldots, \qquad S=a.d_sX^s+b_{s-1}X^{s-1}+\ldots$$

et nous supposons que le déterminant

$$d=c_pb_{s-1}-d_sa_{p-1}$$

se spécialise non nul.

Cette situation se rencontre souvent dans l'important cas particulier où S est égal à la dérivée de P [lorsque $\mathrm{Sp}(a_p)=0$ et $\mathrm{Sp}(a_{p-1})\neq 0$].

PROPOSITION 9 : *Avec les hypothèses ci-dessus, et* $p\geqq s$

(*a*) $\mathrm{Sp}(\mathbf{Sres}_{s-1}(P, p, S, s)/a)=\mathrm{Sp}(d.b_{s-1}^{p-s-1}.S)$.

(*b*) $\mathrm{Sp}(\mathbf{Sres}_j(P, p, S, s)/a)=(-1)^{s-j+1}.\mathrm{Sp}(d).\mathbf{Sres}_j(\mathrm{Sp}(P), p-1, \mathrm{Sp}(S), s-1)$ *pour* $j<s-1$.

Démonstration : L'étude détaillée de la structure des matrices $\mathbf{Sylv}_{s-1}(P, p, S, s)$ et $\mathbf{Sylv}_j(P, p, S, s)$ après spécialisation donne les égalités (*a*) et (*b*). □

4e cas : *les degrés de P et S s'abaissent de manière « incontrôlée »*

On n'obtient rien par spécialisation « directe ».

Néanmoins, si les divisions exactes sont nettement plus faciles dans **A** que dans **A'**, on aura intérêt à poser $S_s:=S$ tronqué au-dessus du degré de $\mathrm{Sp}(S)$, $P_p:=P$ tronqué au dessus du degré de $\mathrm{Sp}(P)$, à calculer les polynômes sous-résultants de P_p et S_s, et spécialiser pour terminer.

(d) Algorithmes de calculs et complexité

Algorithmes de calcul

Présentons maintenant les algorithmes de calculs qui se déduisent des résultats précédents. *Ces algorithmes utilisent uniquement des calculs de pseudo-restes et des divisions exactes.*

Nous commençons par un algorithme qui se déduit directement du théorème de Habicht et du théorème des sous-résultants (théorème 4) :

ALGORITHME 1 ([5]) : Nous supposons $d(P)=p=n+1$, $d(S)=s\leqq n$.

Nous posons $S_{n+1} := P$, $S_n := S$, et $S_j := \mathbf{Sres}_j(P, n+1, S, n)$ pour $j<n$.

entrées : les polynômes P et S

sortie : la suite des sous-résultants $S_j (0\leqq j\leqq s)$

initialisation :

- si $s=n$ $\quad S_{s-1} := \mathbf{Prst}(P, S)$; $\quad S_s := S$ (0)
- si $s<n$ $\quad S_s := (cd(P)\, cd(S))^{n-s} S$ (1)

  $S_{s-1} := (-cd(P))^{n-s} . \mathbf{Prst}(P, S)$ (2)

  en outre si $s<n-1$ et $s<k<n$: $S_k := 0$ (3)
- $j := s-1$

étape suivante : $\{1\leqq j\leqq s-1$, S_{j+1} et S_j sont supposés déjà calculés, avec $d(S_{j+1})=j+1$ et $h=d(S_j)$. On va calculer les S_k manquants jusqu'à $S_{h-1}\}$

- $h := d(S_j)$
- si $h=j$ $\quad S_{h-1} := \mathbf{Prst}(S_{j+1}, S_j)/cd(S_{j+1})^2$ (4)
- si $h<j$ $\quad S_h := S_j . cd(S_j)^{j-h}/cd(S_{j+1})^{j-h}$ (5) (*)

  $S_{h-1} := \mathbf{Prst}(S_{j+1}, S_j)/(-cd(S_{j+1}))^{j-h+2}$ (6) (*)

  en outre si $h<j-1$ et $h<k<j$: $S_k := 0$ (7)
- $j := h-1$

fin : l'algorithme se termine lorsqu'on a calculé S_0 c'est-à-dire lorsque $j\leqq 0$

([5]) Cet algorithme calcule les polynômes sous-résultants $\mathbf{Sres}_j(P, n+1, S, n)$ lorsque $d(P)=n+1>d(S)$. Le Subresultant Theorem, p. 122, de [15] semble, en première lecture, concerner ces sous-résultants, puisque p. 121, ce sont ces sous-résultants (obtenus par spécialisation d'une suite où P et S sont formellement de degrés $n+1$ et n) qui sont considérés... En fait le Subresultant Theorem est correct avec les $\mathbf{Sres}_j(P, n+1, S, s)$ lorsque $n=p-1\geqq s$, il est par contre incorrect lorsque $p\leqq s$. (*Cf.* la note bas de page n° 9.)

(*) (5) n'est pas exécuté si $h=-1$, (6) n'est pas exécuté si $h\leqq 0$.

Démonstration : L'initialisation est conséquence des propositions 2 et 4 et la suite des théorèmes de Habicht et des sous-résultants. □

Remarque 4 : Si $j=h$ l'affectation (5) donnerait $S_j := S_j$. Et l'affectation (6) produirait le même effet que la (4).

On remarque maintenant que les formules récurrentes (4), (5), (6), (7) sont homogènes. Si, en dessous d'un certain degré k, on sait que les S_j sont tous multiples d'une constante c de **A**, les formules sont encore valables si on remplace les polynômes S_j par les S_j/c. Nous en déduisons, lorsque $p=d(P)$, $s=d(S)\leqq n=p-1$, un algorithme pour calculer les sous-résultants standards $\mathbf{Sres}_j(P, p, S, s)=\mathbf{Sres}_j(P, p, S, n)/cd(P)^{n-s}$ [*cf.* proposition 1 (*c*)]. On notera que l'algorithme ne diffère du précédent que lorsque $s<n$, et seulement dans la partie « initialisation ».

ALGORITHME 2 : **Calcul des polynômes sous-résultants standards** (cas $d(S)<d(P)$).

Nous supposons $d(P)=p=n+1$, $d(S)=s\leqq n$. Nous posons $S_p := P$, $S_n := S$, $S_s := cd(S)^{n-s}S$, et $S_j := \mathbf{Sres}_j(P, p, S, s)$ pour $j<s$.
entrées : les polynômes P et S
sortie : la suite des sous-résultants standards $S_j (0\leqq j\leqq s)$
initialisation :

- $p := d(P)$, $\quad s := d(S)$, $\quad n := p-1$,
- $S_s := cd(S)^{n-s}S$ (1)
- $S_{s-1} := (-1)^{n-s}.\mathbf{Prst}(P, S)$ (2)
- $j := s-1$

étape suivante et **fin :** comme dans l'algorithme 1.

On peut maintenant essayer de faire rentrer les affectations (1) et (2) dans le moule : (5) et (6). C'est possible en prenant $j=n$, $h=s$, et en faisant l'affectation $cd(S_{n+1}) := 1$ (qui est « fausse »). Avec cette philosophie, la suite des sous-résultants commence à $S_{n+1}=P$ et il faut poser $S_k := 0$ si $s<k<p-1$. L'avantage est que les seules initialisations sont : $S_{n+1} := P$, $S_n := S$, « $cd(S_{n+1}) := 1$ ». Et on passe directement à « étape suivante ».

Aussi ferons-nous désormais la convention suivante :

DÉFINITION (convention) : Si $p \geqq d(P)$, $s = d(S)$ et $p > s$, on pose :

$$\mathbf{Sres}_p(P, p, S, s) := P, \qquad \mathbf{Sres}_{p-1}(P, p, S, s) := S,$$
$$\mathbf{Sres}_s(P, p, S, s) := cd(S)^{p-1-s}.S,$$
$$\mathbf{Sres}_k(P, p, S, s) := 0 \qquad \text{si} \quad s < k < p-1,$$
$$\mathbf{sr}_p(P, p, S, s) := 1,$$
$$\mathbf{sr}_j(P, p, S, s) := \mathbf{cf}_j(\mathbf{Sres}_j(P, p, S, s)) \qquad \text{si} \quad j < p.$$

Remarque 5 : On notera qu'avec cette convention, de nombreux « cas distincts » dans les propositions établies précédemment « fusionnent » :

- proposition 2 : (*a*) et (*b*) sont des cas particuliers de (*c*);
- proposition 5 : (*a*) est un cas particulier de (*b*);
- théorème de Habicht : définition « uniforme » pour les S_j et les $C(j)$;
- proposition 7 : (*a*) (i) est un cas particulier de (*a*) (ii), (*b*) (i) et (*b*) (ii) sont des cas particuliers de (*b*) (iii);
- proposition 9 : (*a*) est un cas particulier de (*b*).

En outre remarquons que :

- la proposition 1 (*c*) (i) reste vraie dans les cas $j = s = d(S) < p$ et $d(S) = s < j < \inf(s', p-1)$;
- la proposition 1 (*c*) (ii) reste vraie dans le cas $j = p < s$ mais serait fausse pour $p < j = s < s'$ ou $p < j = s-1 < s < s'$ ([6]).

Nous donnons maintenant une généralisation de l'algorithme précédent, conformément à la définition-convention ci-dessus.

ALGORITHME 3 : **Algorithme généralisé des polynômes sous-résultants** ([7]).

Nous supposons $p \geqq d(P)$, $s = d(S)$ et $p > s$.

([6]) Ainsi la convention concernant $Sres_s(P, p, S, s)$ pour $s = d(S) < p$ tient correctement la route par rapport aux égalités générales données dans la proposition 1. Il en va de même avec les polynômes sous-résultants identiquement nuls pour $s < j < p-1$. La lecture des propositions 1 (*c*) et 2 (*a*) et (*b*) pouvait d'ailleurs inciter à poser ces conventions au tout début de l'article. Il en va tout différemment en ce qui concerne la convention $\mathbf{Sres}_{p-1}(P, p, S, s) = S$. Supposons en effet $p = d(P)$, $s = d(S)$, $p > s+1$: l'égalité $\mathbf{Sres}_{p-1}(P, p, S, p) = cd(P)\,S$ inciterait à poser, vue la proposition 1 (*c*) (i), $\mathbf{Sres}_{p-1}(P, p, S, s) := S/cd(P)^{p-s-1}$ tandis que l'égalité $\mathbf{Sres}_{p-1}(P, p+1, S, s) = 0$ inciterait à poser, elle, vue 1 (*c*) (ii), $\mathbf{Sres}_{p-1}(P, p, S, s) := 0$. La même critique vaut pour la convention concernant le sous-résultants $\mathbf{Sres}_p(P, p, S, s)$.

([7]) Le Subresultant Chain Algorithm dans [15] est celui-ci lorsque $p = d(P) > d(S)$.

Nous posons pour $j \leqq p$: $S_j := \mathbf{Sres}_j(P, p, S, s)$, $t_j := \mathbf{sr}_j(P, p, S, s)$.
entrées : les polynômes P et S, l'entier $p \geqq d(P)$
sortie : la suite des polynômes sous-résultants $S_j (0 \leqq j \leqq p)$
initialisation :

- $S_p := P$; $\quad t_p := 1$
- $S_{p-1} := S$
- $j := p-1$

étape suivante : $\{ 1 \leqq j \leqq n$, S_{j+1}, t_{j+1} et S_j sont supposés déjà calculés, S_{j+1} et t_{j+1} non nuls, avec $h = d(S_j)$. On va calculer les S_k manquants jusqu'à $S_{h-1} \}$

- $h := d(S_j)$
- si $h = j$ $\quad S_{h-1} := \mathbf{Sres}_{h-1}(S_j, h, S_{j+1}, j+1)/t_{j+1}^2$; (4)
- si $h < j$ $\quad S_h := S_j . \mathbf{cf}_h(S_j)^{j-h}/t_{j+1}^{j-h}$; (5) (*)

$$S_{h-1} := \mathbf{Sres}_{h-1}(S_j, h, S_{j+1}, j+1)/(-t_{j+1})^{j-h+2} \quad (6)\ (*)$$

en outre si $h < j-1$ et $h < k < j$: $S_k := 0$ (7)

- $j := h-1$; $\quad t_{j+1} := \mathbf{cf}_{j+1}(S_{j+1})$ ([8])

fin : l'algorithme se termine lorsqu'on a calculé S_0 c'est-à-dire lorsque $j \leqq 0$.

(*) (5) n'est pas exécuté si $h = -1$, (6) n'est pas exécuté si $h \leqq 0$.

NB : On notera que dans (4) et (6) on peut toujours remplacer $\mathbf{Sres}_{h-1}(S_j, h, S_{j+1}, j+1)$ par $\mathbf{Prst}(S_{j+1}, S_j)$ sauf lors du premier passage ([9]) si $d(P) < p$. En particulier, si $d(P) = p > s = d(S)$, le théorème 4 (théorème des sous-résultants) reste vrai avec tout $j < p$ (au lieu de $j < s-1$). Dans le cas $p > s = d(S)$, $p \geqq d(P)$, le théorème 4 reste vrai à condition de remplacer dans (*b*) (iii) $\mathbf{Prst}(S_{j+1}, S_j)$ par $\mathbf{Sres}_{h-1}(S_j, h, S_{j+1}, j+1)$.

En outre, on a toujours l'égalité : $\mathbf{Sres}_{h-1}(S_j, h, S_{j+1}, j+1) = \mathbf{cf}_h(S_j)^{j-h+2}\, \mathbf{Rst}(S_{j+1}, S_j)$.

([8]) Cette affectation pourrait aussi s'écrire $t_h := \mathbf{cf}_h(S_h)$.

([9]) Dans le Subresultant Theorem et le Subresultant Chain Algorithm de [15], c'est toujours $\mathbf{Prst}(S_{j+1}, S_j)$ qui intervient. Or ce polynôme n'est défini que pour $d(S_{j+1}) \geqq d(S_j)$. En conséquence le Subresultant Theorem et le Subresultant Chain Algorithm sont « illisibles » pour $d(P) < d(S)$ et incorrects pour $d(P) = d(S)$. On notera également que l'on ne trouve pas dans [15] de définition explicite des $\mathbf{Sres}_j(P, n+1, S, s)$ lorsque $n > j \geqq s$.

On peut déduire de l'algorithme précédent un algorithme pour les sous-résultants standards dans le cas où $d(P)=d(S)$. Il ne diffère de celui donné pour le cas $d(P)>d(S)$ que dans la partie « initialisation ».

ALGORITHME 4 : **Calcul des polynômes sous-résultants standards** [cas où $d(S)=d(P)$].

Nous supposons $d(P)=d(S)=s$.

Nous posons $S_j := \mathbf{Sres}_j(P, s, S, s)$ pour $j<s$.

entrées : les polynômes P et S

sortie : la suite des sous-résultants standards $S_j (0 \leqq j < s)$

initialisation :

- $S_{s-1} := \mathbf{Prst}(S, P), \qquad t := d(S_{s-1})$ (1)
- si $t=s-1$ $\quad S_{s-2} := \mathbf{Prst}(P, S_{s-1})/cd(P)$ (2)
- si $t<s-1$ on calcule S_t et S_{t-1} comme suit

  $S_t := cd(S_{s-1})^{s-1-t} . S_{s-1}$ (1 *bis*)

  $S_{t-1} := (-1)^{s-1-t} . \mathbf{Prst}(P, S_{s-1})/cd(P)$ (2 *bis*)

  en outre si $t<s-2$ et $t<k<s-1 : S_k := 0$ (3)
- $j := t-1$

étape suivante et **fin :** comme dans l'algorithme 1.

Nous présentons enfin un algorithme qui constitue une amélioration de l'algorithme 2 lorsque $cd(P)$ et $cd(S)$ sont divisibles par un même élément c de **A**.

ALGORITHME 5 : [cas $d(S)<d(P)$, $cd(P)$ et $cd(S)$ divisibles par un même élément c de **A**].

Nous supposons $d(P)=p=n+1$, $d(S)=s \leqq n$, $cd(P)$ et $cd(S)$ divisibles par un même élément c de **A** : $cd(P)=c.\gamma$, $cd(S)=c.\chi$.

Nous posons $S_j := \mathbf{Sres}_j(P, p, S, s)/c$ pour $j<n$.

entrées : les polynômes P et S

sortie : la suite des S_j définis ci-dessus $(0 \leqq j \leqq n-1)$

initialisation :

1er cas : d(S)+1<d(P) (c'est-à-dire $p>s+1$)

- $S_s := \chi^{n-s} . c^{n-s-1} . S$ (1)
- $S_{s-1} := (-1)^{n-s} . \mathbf{Prst}(P, S)/c$ (2)
- $j := s-1$

– si $s<p-2$ et $s<k<p-1$: $S_k := 0$ (3)

2e cas : d (S) + 1 = d (P) (c'est-à-dire $p=s+1$)

– $S_s := S$

– $S_{s-1} := \mathbf{Prst}(P, S)/c$ (1)

– $t := d(S_{s-1})$

– si $t=s-1$ $S_{s-2} := \mathbf{Prst}(S, S_{s-1})/(c \cdot \chi^2)$ (2)

– si $t<s-1$ on calcule S_t et S_{t-1} comme suit

$S_t := cd(S_{s-1})^{s-1-t} \cdot S_{s-1}/\chi^{s-1-t}$ (1 *bis*)

$S_{t-1} := (-1)^{p-t} \cdot \mathbf{Prst}(S, S_{s-1})/(c \cdot \chi^{p-t})$ (2 *bis*)

en outre si $t<s-2$ et $t<k<s-1$: $S_k := 0$ (3)

– $j := t-1$

étape suivante et **fin :** comme dans l'algorithme 1.

Comparaison des différents algorithmes proposés

Les algorithmes 2 et 4 sont ceux qu'on utilisera en pratique pour calculer les sous-résultants. En effet les sous-résultants généraux sont des multiples des sous-résultants standards : ils occupent en général plus de place et occasionnent des calculs plus longs. Notons cependant que l'algorithme 3 avec $p=d(P)>s=d(S)$ peut remplacer le 2 (il effectue exactement les mêmes calculs) et est plus facile à écrire. L'algorithme 5 est une amélioration de l'algorithme 2, pour les deux raisons suivantes : *primo*, si le facteur c qu'on connaît dans $cd(P)$ et $cd(S)$ est « grand » (du point de vue de la taille occupée), les calculs seront *a priori* plus rapides avec les coefficients divisés par ce facteur commun; *secundo*, si le facteur c s'annule par spécialisation, la suite calculée par l'algorithme 5 peut s'avérer utile tandis que celle calculée par l'algorithme 2 serait inutilisable (*cf.* la proposition 9).

L'algorithme 1 est une sorte d'algorithme intermédiaire qui permet de démontrer facilement les algorithmes 2 et 4 à partir du théorème de Habicht.

L'algorithme 3 est sans doute celui qui éclaire le mieux la question des sous-résultants : les polynômes P et S font partie ici de la suite des sous-résultants de manière tout à fait naturelle, et l'étape d'initialisation est réduite au strict minimum. Il n'est donc pas étonnant de voir dans la suite certaines démonstrations (celle du théorème 1, § II. 1 (*a*) par exemple) reposer sur la correction de cet algorithme 3.

Complexité

Une suite de sous-résultants est beaucoup plus facile à calculer que la suite des restes, notamment pour les raisons suivantes :

– le calcul des sous-résultants n'utilise que des additions, multiplications et divisions exactes dans l'anneau **A**, et les coefficients obtenus restent de taille polynomiale si les déterminants sont de taille polynomiale dans **A** (par exemple avec $\mathbf{A}=\mathbb{Z}$ ou $\mathbf{A}=\mathbb{Z}[X_1, \ldots, X_n]$);

– les sous-résultants se spécialisent bien : si les divisions exactes dans **A'** ne sont pas aisées, on peut utiliser l'algorithme des sous-résultants avant spécialisation;

– si on essaye de calculer la suite des restes directement dans le corps des fractions de **A**, on est confronté à l'alternative suivante : ou bien ne pas simplifier les fractions obtenues au fur et à mesure, mais alors la taille des coefficients explose presque à tout coup, ou bien simplifier les fractions obtenues, mais cela exige un calcul de *pgcd* dans **A** (en général nettement plus coûteux qu'une division exacte dans **A**), et on n'est même pas prémuni contre une possible explosion de la taille des fractions réduites (*cf.* [14]).

Si on désire vraiment avoir les restes sans facteur multiplicatif, le mieux sera en général de calculer la suite des sous-résultants puis de retrouver les restes en utilisant la proposition 8.

Supposons qu'on a une notion de taille pour les éléments de **A**, et que les déterminants de matrices formées d'éléments de **A** sont de taille polynomiale en m, qui est un majorant de la dimension de la matrice et des tailles des coefficients de **A**. C'est le cas pour les anneaux $\mathbf{A}=\mathbb{Z}$ ou $\mathbf{A}=\mathbb{Z}[X_1, \ldots, X_k]$ d'après l'inégalité d'Hadamard [16]. Supposons enfin que ces déterminants se calculent en temps polynomial en m : c'est le cas pour les anneaux $\mathbf{A}=\mathbb{Z}$ ou $\mathbf{A}=\mathbb{Z}[X_1, \ldots, X_k]$ d'après la complexité des opérations arithmétiques dans ces anneaux et la méthode du pivot améliorée à la Bareiss ([10]) [2, 15, 1].Alors

([10]) En fait l'algorithme de Bareiss remonte au moins à [1] de 1932. La méthode du pivot améliorée à la Bareiss est basée sur l'étude des valeurs des coefficients successifs obtenus lors d'une triangulation par la méthode du pivot : tout coefficient obtenu est le quotient de deux déterminants extraits de la matrice de départ. Dans son livre (tome 1, chap. 2), Gantmacher met clairement en évidence comment l'analyse détaillée de la méthode du pivot permet une démonstration simple des identités de Sylvester concernant les déterminants, identités qui garantissent la possibilité d'opérer les divisions exactes dans **A** qui interviennent dans la méthode de Bareiss. Notons qu'en 1932, Aitken [1], signale « en passant » comment obtenir une triangulation entièrement dans $\mathbb{Z}$ en utilisant des divisions exactes (produit en croix divisé par le pivot précédent)... c'est-à-dire par la méthode de Bareiss.

il est clair d'après la définition des polynômes sous-résultants comme déterminants polynomiaux que ceux-ci sont calculables en temps polynomial.

Si n est une borne sur les degrés de P et S, le nombre d'opérations arithmétiques sur $\mathbf{A}=\mathbb{Z}$ ou $\mathbf{A}=\mathbb{Z}[X_1, \ldots, X_k]$ pour calculer les polynômes sous-résultants comme déterminants polynomiaux est alors en $O(n^5)$ [n polynômes sous-résultants, avec pour chacun d'entre eux n calculs de déterminants (leurs coefficients), chaque calcul de déterminant étant en n^3 opérations arithmétiques sur $\mathbf{A}$ par la méthode de Bareiss].

Il est toutefois plus efficace de les calculer en utilisant un des algorithmes précédents, car le nombre d'opérations arithmétiques sur $\mathbf{A}$ est alors en $O(n^2)$, les tailles des éléments de $\mathbf{A}$ à considérer étant de même nature dans les deux calculs ([11]). Par exemple si $\mathbf{A}=\mathbb{Z}$ et si $t=\sup(\log(\Sigma a_i^2), \log(\Sigma b_j^2))$, la complexité totale du calcul est en $O(n^4 t^2)$.

Le seul calcul du résultant par la méthode de Bareiss appliquée à la matrice de Sylvester est plus coûteux que le calcul de toute la suite des sous-résultants faite en utilisant un des algorithmes précédents.

Si on le souhaite, les polynômes sous-résultants peuvent être calculés en utilisant des méthodes modulaires puisque leurs coefficients sont des déterminants.

Remarquons enfin qu'on utilise le fait que les coefficients des polynômes sous-résultants sont des déterminants pour les majorer en taille, mais qu'on les calcule par une autre méthode. Ce phénomène est fréquent en calcul formel.

BIBLIOGRAPHIE

1. A. C. Aitken, On te Evaluation of Determinants, the Formation of their Adjugates, and the Practical Solution of Simultaneous Linear Equations, *Proc. Edinburgh Math. Soc.*, série 2, III, 1932, p. 207-219.
2. E. H. Bareiss, Sylvester's Identity and Multistep Integer Preserving Gaussian Elimination, *Math. Comp.*, *22*, 565-578 (1968).
3. Borchardt, Zur Theorie der Elimination und Kettenbruch-Entwichlung, *Math. Abh. der Akad. der Wissenschaften zu Berlin*, 1878, p. 1-17.

([11]) En fait, si on réordonne convenablement les lignes de la matrice de Sylvester, le calcul de son déterminant par la méthode de Bareiss fournit, en cours de route, tous les coefficients de tous les polynômes sous-résultants (*cf.* [14]). C'est néanmoins en $O(n^3)$ opérations élémentaires (additions, multiplications, divisions exactes dans $\mathbf{A}$), donc plus coûteux que les algorithmes à la Habicht.

4. W. S. Brown, On Euclid's Algorithm and the Computation of Polynomial Greatest Common Divisors, *J.A.C.M.*, 1971, *18*, p. 476-504.
5. W. S. Brown et J. F. Traub, On Euclid's Algorithm and the Theory of Subresultants, *J.A.C.M.*, 1971, *18*, p. 505-514.
6. M. Chardin, Un algorithme pour le calcul du résultant de trois polynômes homogènes en trois variables, *Centre de Mathématiques et Laboratoire d'informatique, École Polytechnique*, 91128 Palaiseau Cedex (prépublication).
7. G. E. Collins, Subresultants and Reduced Polynomial Remainder Sequences, *J.A.C.M.*, 1967, *14*, p. 128-142.
8. M. Coste et M.-F. Roy, Thom's Lemma, the Coding of Real Algebraic Numbers and the Computation of the Topology of Semi-Algebraic Sets, *J. Symbolic Computations*, 1988, *5*, p. 121-129.
9. L. Gonzalez, H. Lombardi, T. Recio et M.-F. Roy, Spécialisation de la suite de Sturm et sous-résultants (II), *R.A.I.R.O.*, 1990, , p.000-000.
10. L. Gonzalez H. Lombardi T. Recio et M.-F. Roy, Sturm-Habicht Sequences, *Proceedings I.S.S.A.C.*, 1989, p. 136-146.
11. L. Gonzalez, H. Lombardi, T. Recio et M.-F. Roy, Spécialisation de la suite du Sturm et sous-résultants, version détaillée, *CALSYF, Journées du GRECO de Calcul Formel*, 1989.
12. W. Habicht, Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens, *Comm. Math. Helvetici*, 1948, *21* p. 99-116.
13. A. Lascoux, La résultante de deux polynômes, *Séminaire d'Algèbre M. P. Malliavin, Lecture Notes in Math.*, 1984-1985.
14. H. Lombardi, Sous-résultants, suite de Sturm, spécialisation, Publications Mathématiques de Besançon (Théorie des Nombres). 1988-89, fascicule 2.
15. R. Loos, Generalized Polynomial Reaminder Sequences, *Computer Algebra, Symbolic and Algebraic Computation*, Buchberger, Collins, Loos éd., Springer-Verlag, 1982, p. 115-138.
16. M. Mignotte, Some useful bounds, *Computer Algebra, Symbolic and Algebraic Computation*, Buchberger, Collins, Loos éd., Springer-Verlag, 1982, p. 259-263.
17. C. Sturm, Mémoire sur la résolution des équations numériques, *Inst. France Sc. Math. Phys.*, 1835, *6*.
18. J. J. Sylvester, 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*, 1853; repris dans *Sylvester : Collected Math Papers*, Chelsea Pub. Comp. NY, 1983, *1*, p. 429-586.

Nous remercions M. Jouanolou pour nous avoir signalé la référence 3.