RAIRO. INFORMATIQUE THÉORIQUE ET APPLICATIONS

LAUREANO GONZÁLEZ-VEGA
HENRI LOMBARDI
TOMAS RECIO
MARIE-FRANÇOISE ROY

Spécialisation de la suite de Sturm

RAIRO. Informatique théorique et applications, tome 28, n° 1 (1994), p. 1-24

<http://www.numdam.org/item?id=ITA_1994__28_1_1_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 28, n° 1, 1994, p. 1 à 24)

SPÉCIALISATION DE LA SUITE DE STURM (*)

par Laureano González-Vega (1), Henri Lombardi (2), Tomas Recio (1)
et Marie-Françoise Roy (3)

Communiqué par J. 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 la première partie, nous avons donné le théorème de Sturm et sa généralisation puis avons légèrement généralisé la notion de polynômes sous-résultants de deux polynômes. Dans cette partie, nous définissons et étudions la suite de Sturm-Habicht, puis nous décrivons et comparons différentes méthodes pour compter le nombre de racines réelles d'un polynôme.

Abstract. – *We describe and present 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 the first part we have described the theorem of Sturm and its generalization, and we have slightly generalized the concept of subresultant polynomials of two polynomials,

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

INTRODUCTION

Cet article fait suite à [GLRR1], paru dans ce même journal. Quelques détails supplémentaires (dans les preuves, ou sur quelques points historiques) peuvent être trouvés dans [GLRR3].

Dans le chapitre 1, nous définissons la suite de Sturm-Habicht de deux polynômes qui est une sorte de suite de Sturm formelle. Nous démontrons par une méthode directe les résultats de Habicht et les améliorons, obtenant ainsi que la suite de Sturm-Habicht fait aussi bien l'affaire que la suite de

(*) Reçu en janvier 1989, accepté en janvier 1990.
(1) Mathématiques, Université de Santander, Espagne.
(2) Mathématiques, UFR des Sciences et Techniques, 25030 Besançon cedex, Université de Franche-Comté, France.
(3) IRMAR, Université de Rennes, 35042 Rennes cedex, France.

Informatique théorique et Applications/Theoretical Informatics and Applications
0988-3754/94/01/$4.00/

Sturm pour compter le nombre de racines réelles d'un polynôme P (ou pour déterminer 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). Nous indiquons comment se spécialise la suite de Sturm-Habicht et donnons un algorithme de calcul.

Dans le chapitre 2, nous présentons la méthode d'Hermite pour déterminer le nombre de racines réelles de P. Nous établissons un lien direct, purement algébrique, entre les résultats obtenus par cette méthode et ceux obtenus par la méthode de Sturm. La suite de Sturm-Habicht est la clé pour comprendre la situation. C'est aussi elle qui donne les calculs les plus généraux et les plus simples.

1. SUITE DE STURM-HABICHT ET SPÉCIALISATION

1.1. Suite de Habicht

Le nombre de changements de signes dans la suite des restes signés permet, comme nous l'avons vu dans les théorèmes de Sturm et de Sylvester, de calculer le nombre de racines dans $\mathbf{R}$ d'un polynôme P (éventuellement «rendant le polynôme $Q>0$»), sur un intervalle $[a, b]$. Il s'avère en fait que la suite des sous-résultants (modifiée par des changements de signe convenables) fait aussi bien l'affaire que la suite des restes et permet d'obtenir les mêmes résultats. Ceci peut se déduire de résultats de Habicht (*cf.* [Gon] et [GLRR4]). Nous en donnons ici une preuve directe.

Nous considérons dans ce paragraphe une version formelle de la suite des restes signés, que nous appelons *la suite de Habicht*. Nous démontrons que les différences de changements de signes dans la suite des restes signés et dans la suite de Habicht coïncident.

DÉFINITION : *Soit P un polynôme de degré p et S un polynôme de degré s, $v := \sup(p, s+1)$.*

La suite de Habicht est la suite formée des

$$\mathbf{Ha}_j(P, S) := (-1)^{k(k-1)/2}\,\mathbf{Sres}_j(P, v, S, s)\ (j+k=v) \text{ pour } j \text{ variant de } 0 \text{ à } v.$$

On prend donc la suite des sous-résultants de P (considéré comme de degré v) et S qu'on modifie en multipliant les deux premiers polynômes par $+1$, les deux suivants par -1, etc., *de manière automatique* (sans tenir compte du fait que les polynômes sous-résultants sont éventuellement défectueux ou nuls).

Les polynômes de la suite de Habicht sont donc des multiples des polynômes de la suite $[\mathbf{Rss}^k(P, S)]_{k=0,1,\ldots}$ des restes signés, avec des dédoublements et des changements de signes, ou sont nuls. Plus précisément, en appliquant le théorème 3 de [GLRR1], et vues les conventions concernant les $\mathbf{Rss}_j(P, S)$ et les $\mathbf{Ha}_j(P, S)$ pour $j \geqq \inf(d(P), d(S))$, on voit que :

Pour tout $j \leqq \sup(d(P), d(S)+1)$ les polynômes $\mathbf{Ha}_j(P, S)$
et $\mathbf{Rss}_j$(P, S) sont égaux, à un facteur non nul près

Supposons que $\mathbf{K}$ est muni d'un ordre $\leqq$ et soit $\mathbf{R}$ sa clôture réelle pour cet ordre.

On définit

$$\mathbf{V}_{\mathbf{Ha}}(P, S; a) = V([\mathbf{Ha}_j(P, S)]_{j=v, v-1, \ldots, 0}; a)$$
$$\mathbf{V}_{\mathbf{Ha}}(P, S; a, b) = V([\mathbf{Ha}_j(P, S)]_{j=v, v-1, \ldots, 0}; a, b)$$

En fait, nous avons besoin d'introduire une convention particulière pour le décompte du nombre de changements de signes en a dans le cas de la suite de Habicht lorsqu'un polynôme sous-résultant défectueux s'annule en a. D'où les deux définitions qui suivent :

DÉFINITION : *Soient* $\mathbf{K}$ *un corps ordonné,* $a \in \mathbf{K} \cup \{+\infty\} \cup \{-\infty\}$, $[f_0, f_1, \ldots, f_n]$ *une liste de polynômes de* $\mathbf{K}[X]$. *On note* $V'(f_0, f_1, \ldots, f_n; a)$ *le nombre entier défini comme suit :*

– *on extrait tout d'abord la suite* $[g_0, g_1, \ldots, g_m] = [f_{j_0}, f_{j_1}, \ldots, f_{j_m}]$ *formée des polynômes non identiquement nuls,*

– *on compte ensuite le nombre de changements de signes dans la suite* $[g_0(a), g_1(a), \ldots, g_m(a)]$ en adoptant les conventions suivantes concernant les 0 :

* *comptent pour* 1 *changement de signe les segments suivants*

$$-, 0, + \quad ou \quad +, 0, - \quad ou \quad +, 0, 0, - \quad ou \quad -, 0, 0, +$$

* *comptent pour* 2 *changements de signe les segments suivants*

$$+, 0, 0, + \quad ou \quad -, 0, 0, -$$

Le nombre $V'(f_0, f_1, \ldots, f_n; a)$ *reste donc non défini pour des suites comportant des segments avec des* 0 *non couverts par la convention ci-dessus. Il est cependant clair qu'il est défini lorsque* $f_0, f_1, \ldots, f_n$ *est une suite de restes signés (un* 0 *est toujours isolé et entouré de* 2 *signes opposés) ou une suite de*

Habicht (*les* 0 *isolés sont entourés de* 2 *signes opposés, et il n'y a pas de* 0 *triples*).

DÉFINITION : *Soient* $\mathbf{K}$ *un corps ordonné, P et S des polynômes de* $\mathbf{K}[X]$, *a et* $b \in \mathbf{K} \cup \{+\infty\} \cup \{-\infty\}$, *non racines du pgcd de P et S, on définit*

$$\mathbf{V}'_{\mathbf{Ha}}(P, S; a) := V'([\mathbf{Ha}_j(P, S)]_{j=v, v-1, \ldots, 0}; a)$$
$$\mathbf{V}'_{\mathbf{Ha}}(P, S; a, b) := \mathbf{V}'_{\mathbf{Ha}}(P, S; a) - \mathbf{V}'_{\mathbf{Ha}}(P, S; b)$$

NB: On a $\mathbf{V}'_{\mathbf{Ha}}(P, S) := \mathbf{V}_{\mathbf{Ha}}(P, S)$, plus généralement $\mathbf{V}'_{\mathbf{Ha}}(P, S; a, b)$ ne diffère de $\mathbf{V}_{\mathbf{Ha}}(P, S; a, b)$ que dans le cas où un polynôme sous-résulant défectueux s'annule en *a ou en b*.

THÉORÈME 1 ([Hab]) : *En tous points a et b de* $\mathbf{R}$ *non racines du pgcd de P et S on a l'égalité* :

$$\mathbf{V}'_{\mathbf{Ha}}(P, S; a, b) = \mathbf{V}_{\mathbf{Rss}}(P, S; a, b).$$

Démonstration: Le théorème 1 est une conséquence immédiate du lemme suivant :

LEMME 1 : *Sous les hypothèses du théorème il existe une constante c qui dépend seulement de P et S telle que* :

$$\mathbf{V}'_{\mathbf{Ha}}(P, S; a) = \mathbf{V}_{\mathbf{Rss}}(P, S; a) + c.$$

La preuve du lemme 1 utilise le lemme 2 suivant :

LEMME 2 : *Si* $v \geqq j = d(\mathbf{Rss}_j(P, S)) > 0$, *alors*

$$\frac{\mathbf{Ha}_{j-1}(P, S)}{\mathbf{Rss}_{j-1}(P, S)} \cdot \frac{\mathbf{Ha}_j(P, S)}{\mathbf{Rss}_j(P, S)} \text{ est un carré dans } \mathbf{K}.$$

Notations: $t = \sup(d(P), d(S)+1)$, $q = d(S)$, $T_j = \mathbf{Sres}_j(P, t, S, q)$, $R_j = \mathbf{Rst}_j(P, S)$, $\mathbf{Rss}_j = \mathbf{Rss}_j(P, S)$, $\mathbf{Ha}_j = \mathbf{Ha}_j(P, S)$, $T_j/R_j = r_j$.

Montrons tout d'abord que le lemme 1 *résulte du lemme* 2.

Si $j = t$ ou est le degré d'un reste $\mathbf{Rss}^m$, alors $\mathbf{Rss}_j$ et $\mathbf{Rss}_{j-1}$ sont deux polynômes successifs dans la suite des restes signés (les $\mathbf{Rss}^m$). Par ailleurs, tout polynôme non identiquement nul dans la suite de Habicht est de la forme $\mathbf{Ha}_j$ ou $\mathbf{Ha}_{j-1}$ avec j comme ci-avant. D'après le lemme 2, en un point a où tous les $\mathbf{Rss}_j(P, S)(a)$ sont non nuls, il y a changement de signe entre $\mathbf{Rss}_j$ et $\mathbf{Rss}_{j-1}$ si et seulement si il y a changement de signe entre $\mathbf{Ha}_j$ et $\mathbf{Ha}_{j-1}$. Dans la suite de Habicht, s'ajoutent d'éventuels changements de signes entre $\mathbf{Ha}_{j-1}$ et $\mathbf{Ha}_h$ si $h = d(\mathbf{Ha}_{j-1}) < j-1$: mais les deux polynômes étant

proportionnels, ce changement de signe «supplémentaire» éventuel a lieu indépendamment du point a où sont évalués les polynômes.

Voyons maintenant le cas où l'un des polynômes, non défectueux dans la suite de Habicht, s'annule en a: par exemple $d(\mathbf{Ha}_j)=j$, $d(\mathbf{Ha}_{j-1})=j-1$, et $\mathbf{Ha}_{j-1}(a)=0$. On sait alors que $\mathbf{Rss}_j(a).\mathbf{Rss}_{j-2}(a)<0$, ce qui compte pour un changement de signe dans la suite des restes signés.

En outre, pour a' suffisamment proche de a et distinct de a, on a $\mathbf{V}_{\mathbf{Rss}}(P, S, a)=\mathbf{V}_{\mathbf{Rss}}(P, S, a')$ et tous les $\mathbf{Rss}^j(P, S)(a')$ sont non nuls.

En appliquant deux fois le lemme 2 on voit que $\mathbf{Ha}_{j-2}/\mathbf{Rss}_{j-2}.\mathbf{Ha}_j/\mathbf{Rss}_j$ est un carré dans $\mathbf{K}$, et on obtient donc également un changement de signe dans la suite de Habicht. Et pour a' suffisamment proche de a, on a $\mathbf{V}_{\mathbf{Ha}}(P, S, a)=\mathbf{V}_{\mathbf{Ha}}(P, S, a')$.

Donc $\mathbf{V}_{\mathbf{Ha}}(P, S, a)=\mathbf{V}_{\mathbf{Rss}}(P, S, a)+c$ avec la même valuer de c en a qu'en a'.

Voyons enfin le cas où l'un des polynômes défectueux dans la suite de Habicht, s'annule en a. Soit donc j avec $\mathbf{Ha}_{j+1}$ non défecteux (de degré $j+1$), $\mathbf{Ha}_j$ défectueux de degré $h<j$ et tel que $\mathbf{Ha}_j(a)=0$. D'après le lemme 2

$$\frac{\mathbf{Ha}_j}{\mathbf{Rss}_j}.\frac{\mathbf{Ha}_{j+1}}{\mathbf{Rss}_{j+1}} \quad \text{est un carré dans } \mathbf{K}$$

et

$$\frac{\mathbf{Ha}_h}{\mathbf{Rss}_h}.\frac{\mathbf{Ha}_{h-1}}{\mathbf{Rss}_{h-1}} \quad \text{est un carré dans } \mathbf{K}.$$

Ceci signifie que les polynômes $\mathbf{Ha}_{j+1}.\mathbf{Ha}_j.\mathbf{Ha}_h.\mathbf{Ha}_{h-1}$ et $\mathbf{Rss}_{j+1}.\mathbf{Rss}_j.\mathbf{Rss}_h.\mathbf{Rss}_{h-1}$ sont de même signe en tout point a' non racine de $\mathbf{Ha}_j$. Or $\mathbf{Rss}_j=\mathbf{Rss}_h$, et $\mathbf{Rss}_{j+1}$ et $\mathbf{Rss}_{h-1}$ sont de signe opposé en a. Si on considère donc un point a' non racine de $\mathbf{Ha}_j$ et suffisamment proche de a (tel qu'il n'y ait aucune racine d'un polynôme de la suite des restes signés de P et Q entre a et a'), le polynôme $\mathbf{Ha}_{j+1}.\mathbf{Ha}_j.\mathbf{Ha}_h.\mathbf{Ha}_{h-1}$ est négatif en a' et le nombre des changements de signe dans la suite $\mathbf{Ha}_{j+1}$, $\mathbf{Ha}_j$, $\mathbf{Ha}_h$, $\mathbf{Ha}_{h-1}$ en a' vaut 2 si $\mathbf{Ha}_{j+1}.\mathbf{Ha}_{h-1}>0$, 1 si $\mathbf{Ha}_{j+1}.\mathbf{Ha}_{h-1}<0$.

On a donc $\mathbf{V}'_{\mathbf{Ha}}(P, S; a)=\mathbf{V}'_{\mathbf{Ha}}(P, S; a')=\mathbf{V}_{\mathbf{Rss}}(P, S; a')$ □

Voyons maintenant la preuve du lemme 2.

Lorsque $j=t$, le lemme 2 est trivial:

$$P=T_j=R_j=\mathbf{Rss}_j=\mathbf{Ha}_j \qquad \text{et} \qquad S=T_{j-1}=R_{j-1}=\mathbf{Rss}_{j-1}=\mathbf{Ha}_{j-1}.$$

On utilise ensuite l'algorithme généralisé des polynômes sous-résultants et on regarde comment les choses évoluent lors de «étape suivante», lorsqu'on passe de $j+1, j$ à $h, h-1$. Si on pose $c_{j+1} := \mathbf{sr}_{j+1}(P, t, S, q)$ et $c_j := \mathbf{cd}(T_j)$, on trouve:

$$\frac{r_h}{r_{h-1}} = \frac{r_j}{r_{j+1}} \cdot \left(\frac{c_{j+1}}{c_j}\right)^2 \cdot (-1)^{j-h}$$

Comme $\mathbf{Rss}_{j+1}$, $\mathbf{Rss}_j = \mathbf{Rss}_h$ et $\mathbf{Rss}_{h-1}$ sont 3 restes successifs on a:

$$(\mathbf{Rss}_{j+1}/\mathrm{R}_{j+1}) \cdot (\mathbf{Rss}_j/\mathrm{R}_j) \cdot (\mathbf{Rss}_h/\mathbf{R}_h) \cdot (\mathbf{Rss}_{h-1}/\mathrm{R}_{h-1}) = -1$$

Enfin, on a:

$$(\mathbf{Ha}_{j+1}/\mathrm{T}_{j+1}) \cdot (\mathbf{Ha}_j/\mathrm{T}_j) \cdot (\mathbf{Ha}_h/\mathrm{T}_h) \cdot (\mathbf{Ha}_{h-1}/\mathrm{T}_{h-1}) = (-1)^{j-h+1}$$

Ce qui montre le lemme 2 en $h, h-1$ s'il était vrai en $j+1, j$. □

Contre-exemple: Avec $\mathbf{V}_{\mathbf{Ha}}$ au lieu de $\mathbf{V}'_{\mathbf{Ha}}$ le théorème ne serait plus valable si un des deux points a ou b annule un polynôme sous-résultant défectueux. Considérons en effet les polynômes suivants:

$$\mathrm{P} = \mathrm{X}^5 + 2X + 2$$
$$S = X^4 + 1$$

La suite de Habicht est alors

$$\mathbf{Ha}_5(P, S) = X^5 + 2X + 2 \qquad \mathbf{Ha}_4(P, S) = X^4 + 1 \qquad \mathbf{Ha}_3(P, S) = -X - 2$$
$$\mathbf{Ha}_2(P, S) = 0 \qquad \mathbf{Ha}_1(P, S) = X + 2 \qquad \mathbf{Ha}_0(P, S) = 17$$

et choisissons $a = -2$, $b = -1$. on a $\mathbf{V}_{\mathbf{Ha}}(P, S; -2, -1) = 2$.

Or la suite des restes signés est:

$$\mathbf{Rss}^0(P, S) = X^5 + 2X + 2 \qquad \mathbf{Rss}^1(P, S) = X^4 + 1$$
$$\mathbf{Rss}^2(P, S) = -X - 2 \qquad \mathbf{Rss}^3(P, S) = -17$$

et $\mathbf{V}_{\mathbf{Rss}}(P, S; -2, -1) = 0$.

1.2. Suite de Sturm-Habicht

Rappelons que nous avons défini en 1.1. la suite de Sturm de P et Q à partir des restes signés de P et de R (reste de la division de $P'Q$ par P).

Nous donnons maintenant des définitions et notations analogues, concernant cette fois-ci la suite de Habicht. Nous obtenons ainsi un analogue formel

de la suite de Sturm, appelée suite de Sturm-Habicht. Nous montrerons que les variations de signes dans la suite de Sturm-Habicht donnent aussi la différence entre le nombre de racines dans **R** de P rendant Q positif et le nombre de racines dans **R** de P rendant Q négatif. Nous avons simplifié les définitions données dans [GLRR2], mais elles ne sont pas substantiellement différentes.

Nous définissons la **suite de Sturm-Habicht de P et Q** en séparant différents cas :

DÉFINITION : *On note* $p := d(P)$, $q := d(Q)$, $\mathrm{R} := \mathrm{Rst}(P'Q, P)$, $r := d(\mathrm{R})$. *La suite de Sturm-Habicht est définie pour les indices* $j = p, p-1, \ldots, 0$.

- *si* $cd(P) = 1$ (*cas où P est unitaire*)

$$\mathbf{StHa}_j(P, Q) := \mathbf{Ha}_j(P, R) = (-1)^{(p-j)(p-j-1)/2}\,\mathbf{Sres}_j(P, p, R, r).$$

- *si* $cd(P) \neq 1$ (*cas où P n'est pas unitaire*)
- *si* $q = d(Q) \geqq 1$

$$\mathbf{StHa}_p(P, Q) := cd(P)^{(q+1) \bmod 2} . P$$

et pour $j < p$

$$\begin{aligned}\mathbf{StHa}_j(P, Q) &:= (-1)^{(p-j)(p-j-1)/2}\,\mathbf{Sres}_j(P, p, P'Q, p+q-1)/cd(P)\\ &= (-1)^{(p-j)(p-j+2q-1)/2}\,\mathbf{Sres}_j(P'Q, p+q-1, P, p)/cd(P)\end{aligned}$$

- *si* $Q = 1$ *on note* $\mathbf{StHa}_j(P)$ *pour* $\mathbf{StHa}_j(P, 1)$ *et on définit* :

$$\mathbf{StHa}_p(P) := cd(P) . P$$

$$\mathbf{StHa}_{p-1}(P) := cd(P) . P'$$

et pour $j < p-1$

$$\mathbf{StHa}_j(P) := \mathbf{Ha}_j(P, P')/cd(P) = (-1)^{(p-j)(p-j-1)/2}\,\mathbf{Sres}_j(P, p, P', p-1)/cd(P)$$

Remarque 1 : Si P est unitaire, les définitions données pour le cas P non unitaire coïncident avec celles données pour le cas P unitaire. Si on appliquait la définition du cas P non unitaire $q \geqq 1$ pour le cas $Q = 1$ on retrouverait la même chose sauf pour $\mathbf{StHa}_{p-1}(P)$ (P' serait divisé par $cd(P)$ au lieu d'être multiplié par $cd(P)$ et on risquerait de quitter l'anneau des coefficients).

Lorsque P est unitaire la suite de Sturm-Habicht de P et Q est tout simplement la suite de Habicht de P et R. Les complications techniques qui se présentent dans les autres cas sont dues au fait que l'on veut

– que les coefficients des polynômes de la suite de Sturm-Habicht soient dans l'anneau des coefficients de P et Q,

– que la suite de Sturm-Habicht se comporte bien par spécialisation, même dans certains cas où il y a chute du degré de P ou de Q,

– que la suite de Sturm-Habicht soit calculée par un algorithme aussi performant que possible.

DÉFINITION : *On appellera* **coefficient de Sturm-Habicht** *et on notera* $\mathbf{sth}_j(P, Q)$ *le coefficient de* X^j *dans* $\mathbf{StHa}_j(P, Q)$. *On dira que* $\mathbf{StHa}_j(P, Q)$ *est* défectueux *s'il est de degré* $<j$, *c'est-à-dire si* $\mathbf{sth}_j(P, Q)$ *est nul.*

Enfin, on appellera **suite de Sturm-Habicht du polynôme** P *la suite de Sturm-Habicht de* P *et* 1.

Définitions et notations: Si $\mathbf{K}$ est muni d'un ordre $\leqq$ et si a et b sont deux éléments de $\mathbf{K} \cup \{+\infty\} \cup \{-\infty\}$ on note:

$$\mathbf{V}_{\mathbf{StHa}}(P, Q; a) := \mathrm{V}([\mathbf{StHa}_j(P, Q)]_{j=p, p-1, \ldots, 0}; a)$$

$$\mathbf{V}_{\mathbf{stHa}}(P, Q; a, b) := \mathbf{V}_{\mathbf{StHa}}(P, Q; a) - \mathbf{V}_{\mathbf{StHa}}(P, Q; b)$$

$$\mathbf{V}_{\mathbf{StHa}}(P, Q) := \mathbf{V}_{\mathbf{StHa}}(P, Q, -\infty) - \mathbf{V}_{\mathbf{StHa}}(P, Q, +\infty).$$

Soient $\mathbf{K}$ un corps ordonné, P et Q des polynômes de $\mathbf{K}[X]$, de degrés p et q a et $b \in \mathbf{K} \cup \{+\infty\} \cup \{-\infty\}$, non racines du *pgcd* de P et Q, on définit

$$\mathbf{V}'_{\mathbf{StHa}}(P, Q; a) := V'([\mathbf{StHa}_j(P, Q)]_{j=p, p-1, \ldots, 0}; a)$$

$$\mathbf{V}'_{\mathbf{StHa}}(P, Q; a, b) := \mathbf{V}'_{\mathbf{StHa}}(P, Q; a) - \mathbf{V}'_{\mathbf{StHa}}(P, Q; b).$$

Principales propriétés

Les définitions des $\mathbf{StHa}_j(P, Q)$ ci-dessus sont choisies de manière à ce que soit vérifiée la proposition suivante.

PROPOSITION 1 (étude du cas où P n'est pas unitaire) : *a) Si* $d(R) = p - 1$, *les polynômes* $\mathbf{StHa}_j(P, Q)$ *et* $\mathbf{Ha}_j(P, R)$ *(où* $R = \mathbf{Rst}(P'Q, P)$*) sont proportionnels dans un facteur de signe constant (même résultat si* $p - 1 - d(R)$ *est pair).*

b) Dans tous les cas, il existe une constante c' *qui ne dépend que de* P *et* Q *telle que*:

$$\mathbf{V}'_{\mathbf{Ha}}(P, R; a) = \mathbf{V}'_{\mathbf{StHa}}(P, Q; a) + c'$$

Démonstration: Si $Q = 1$ le résultat est trivial. Reste à voir avec $d(Q) = q \geqq 1$. Les propositions et remarques citées dans la suite de la preuve sont dans [GLRR1].

On a $\mathbf{Ha}_j(P, R) = (-1)^{(p-j)(p-j-1)/2} \mathbf{Sres}_j(P, p, R, r)$, avec en particulier $\mathbf{Ha}_p(P, R) = P$ et $\mathbf{Ha}_{p-1}(P, R) = R$.

On a $\mathbf{StHa}_j(P, Q) := (-1)^{(p-j)(p-j-1)/2} \mathbf{Sres}_j(P, p, R, p+q-1)/cd(P)$ pour $j \leqq p-1$, par application de la proposition 3.

Pour $j < p-1$ on a, d'après la proposition 1 *c* (i) et la remarque 5 :

$$\mathbf{Sres}_j(P, p, R, p+q-1) = (cd(P))^{p+q-1-r} \mathbf{Sres}_j(P, p, R, r)$$

Enfin, on voit facilement que $\mathbf{Sres}_{p-1}(P, p, R, p+q-1) = ((cd(P))^q R$.

Ainsi, lorsque $r = p-1$, on a pour tout $j \leqq p-1$

$$\mathbf{StHa}_j(P, Q) = (cd(P))^{q-1} \mathbf{Ha}_j(P, R), \text{ d'où le résultat } a).$$

Lorsque $r < p-1$, on a pour tout $j < p-1$

$$\mathbf{StHa}_j(P, Q) = (cd(P))^{p+q-2-r} \mathbf{Ha}_j(P, R)$$

et le polynôme proportionnel à R est dédoublé dans les deux suites considérées : une fois avec l'indice $p-1$, l'autre fois avec l'indice r. Avant le dédoublement (sur le morceau P, R) les deux suites sont proportionnelles à un facteur près de signe constant : le même que celui de $cd(P)^{q-1}$. Après le dédoublement (2e occurrence de R et jusqu'à la fin), les deux suites sont proportionnelles au facteur constant près : $(cd(P))^{p+q-2-r}$. D'où le *b*). □

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

$$P = X^4 + pX^2 + qX + r.$$

La suite de Sturm-Habicht de P et P', calculée dans $\mathbb{Z}[p, q, r][X]$ est

$$\mathbf{StHa}_4(P) = X^4 + pX^2 + qX + r \qquad \mathbf{StHa}_3(P) = 4X^3 + 2pX + q$$

$$\mathbf{StHa}_2(P) = -4(2pX^2 + 3qX + 4r)$$

$$\mathbf{StHa}_1(P) = -4((2p^3 - 8pr + 9q^2)X + p^2q + 12qr)$$

$$\mathbf{StHa}_0(P) = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3$$

A des carrés de $\mathbb{Q}(p, q, r)$ près, elle coïncide avec la suite de Sturm générique (voir exemple 1 de [GLRR1]).

Si $p=0$, la suite de Sturm-Habicht de $P=X^4+qX+r$, obtenue en substituant 0 à p dans la suite de Sturm-Habicht de P est donc:

$$\mathbf{StHa}_4(P)=X^4+qX+r \qquad \mathbf{StHa}_3(P)=4X^3+q$$
$$\mathbf{StHa}_2(P)=-4(3qX+4r) \qquad \mathbf{StHa}_1(P)=-12q(3qX+4r)$$
$$\mathbf{StHa}_0(P)=27q^4+256r^3$$

Comparer avec ce qu'on obtenait dans l'exemple 1 du paragraphe 1 de [GLRR1]: la suite de Sturm-Habicht est formée de multiples des polynômes de la suite de Sturm, avec certains changements de signes et répétitions.

Nous donnons maintenant des résultats concernant le cas P unitaire qui nous seront utiles par la suite.

PROPOSITION 2 : *Soient P et Q deux polynômes à coefficients dans un anneau intègre A, avec P unitaire.*

(i) *Si*

$$\mathbf{sth}_j(P,Q)\neq 0, \quad \mathbf{sth}_{j-1}(P,Q)=\ldots=\mathbf{sth}_{j-h}(P,Q)=0, \quad \mathbf{sth}_{j-h-1}(P,Q)\neq 0$$

alors $\mathbf{StHa}_j(P,Q)$ *est de degré* j, $\mathbf{StHa}_{j-1}(P,Q)$ *est défectueux de degré* $j-h-1$ *et tous les* $\mathbf{StHa}_k(P,Q)$, $j-h\leq k<j-1$, *sont nuls.*

(ii) *Sous la même hypothèse nous avons, en notant* $c_{j-h-1}:=cd(\mathbf{StHa}_{j-1})$,

$$\mathbf{sth}_j(P,Q)^h\,\mathbf{StHa}_{j-h-1}=(-1)^{h(h+1)/2}(c_{j-h-1})^h\,\mathbf{StHa}_{j-1}.$$

(iii) $\mathbf{StHa}_p(P,Q)=P$, $\mathbf{StHa}_{p-1}(P,Q)=R=\mathbf{Rst}(P'Q,P)$, et pour $j<p-1$, $k=p-j$:

$$\mathbf{StHa}_j(P,Q)=(-1)^{k(k-1)/2}\,\mathbf{Sres}_j(P,p,R,d(R))$$
$$=(-1)^{k(k-1)/2}\,\mathbf{Sres}_j(P,p,R,p-1)$$

En conséquence la suite de Sturm-Habicht est invariante par spécialisation.

Démonstration: Immédiate d'après le théorème 4 de [GLRR1] et la définition de la suite de Sturm-Habicht.

La suite de Sturm-Habicht est la version formelle de la suite de Sturm. Dans le cas ordinaire, où P est unitaire et où les degrés descendent de 1 en 1 dans la suite de Sturm, les deux suites sont formées des mêmes polynômes, à des facteurs carrés près. Dans les cas défectueux la suite de Sturm de P et Q possède moins de termes que la suite de Sturm-Habicht. La suite de Sturm-Habicht est beaucoup plus facile à calculer que la suite de Sturm. Le théorème analogue au théorème 1 s'avère donc fort utile: c'est le théorème 2 suivant.

THÉORÈME 2 ([Hab]) : *Soient P et Q deux polynômes quelconques à coefficients dans un corps ordonné* $\mathbf{K}$ *et a et b (avec $a<b$) des points de* $\mathbf{K}$ *non racines de P.*

(i) *On a l'égalité* $\mathbf{V}'_{\mathbf{StHa}}(P, Q; a, b) = \mathbf{V}_{\mathbf{Stu}}(P, Q; a, b)$.

(ii) *On a l'égalité* $\mathbf{V}_{\mathbf{StHa}}(P, Q) = \mathbf{V}_{\mathbf{Stu}}(P, Q)$.

Démonstration: Notons $p := d(P)$, $q := d(Q)$, $R := \mathbf{Rst}(P, P' Q)$, $r := d(R)$.

Le (ii) résulte du (*i*).

Voyons le (i). D'après le théorème 1, on a le résultat suivant :

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

On conclut par la proposition 1. □

COROLLAIRE : *Soient P et Q deux polynômes quelconques à coefficients dans un corps ordonné* $\mathbf{K}$ *de clôture réelle* $\mathbf{R}$ *et a et b (avec $a<b$) des points de* $\mathbf{R}$ *non racines de P.*

(i) *On a l'égalité* $\mathbf{V}'_{\mathbf{StHa}}(P, Q, a, b) = \mathbf{c}_+(P, Q, a, b) - c_-(P, Q, a, b)$.

(ii) *On a l'égalité* $\mathbf{V}_{\mathbf{StHa}}(P, Q) = \mathbf{c}_+(P, Q) - \mathbf{c}_-(P, Q)$.

Démonstration: Résulte du théorème 2, et du théorème 1 de [GLRR1]. □

Algorithmes

Les $\mathbf{StHa}_j(P, Q)$ peuvent être calculés au moyen des algorithmes donnés au paragraphe 1.2 de [GLRR1] :

Si P est unitaire on utilisera l'algorithme généralisé des polynômes sous-résultants (algorithme 3).

Si P n'est pas unitaire on utilisera l'algorithme 5 avec, dans le cas $d(Q) \geqq 1$, la deuxième formule donnée dans la définition.

1.3. Spécialisation de la suite de Sturm-Habicht

On considère deux polynômes P et Q à coefficients dans un anneau $\mathbf{A}$, un homomorphisme Sp de $\mathbf{A}$ dans $\mathbf{A}'$ où $\mathbf{A}'$ est un anneau intègre de corps de fractions $\mathbf{K}'$. On considère un ordre $\leqq$ sur $\mathbf{K}'$ et la clôture réelle $\mathbf{R}'$ de $\mathbf{K}'$ pour cet ordre.

On note $p = d(P)$, $q = d(Q)$, $P_1 = \mathrm{Sp}(P)$, $Q_1 = \mathrm{Sp}(Q)$, $p_1 = d(P_1)$, $q_1 = d(Q_1)$.

1er cas : $p_1 = p$, $q \geqq 1$

PROPOSITION 3 (Notations ci-dessus) : *Supposons* $p_1 = p$, $q \geqq 1$.

a) Si P est unitaire, on a $\mathrm{Sp}(\mathbf{StHa}_j(P, Q)) = \mathbf{StHa}_j(P_1, Q_1)$.

b) Dans tous les cas, la différence des changements de signes dans la suite obtenue par spécialisation de la suite de Sturm-Habicht de P et Q entre a et b coïncide avec la différence des changements de signes dans la suite de Sturm-Habicht de $\mathrm{Sp}(P)$ *et* $\mathrm{Sp}(Q)$ *entre a et b (a et b sont des éléments de* $\mathbf{K}' \cup \{+\infty\} \cup \{-\infty\}$).

Autrement dit, on a l'égalité :

$$\mathbf{V}'_{\mathbf{StHa}}(P_1, Q_1; a, b) = V'([\mathrm{Sp}(\mathbf{StHa}_j(P, Q))]_{j=p, p-1, \ldots, 0}; a, b)$$

Démonstration : Si P est unitaire, a) est donné par la proposition 2 (iii), *b)* s'en déduit

Si P n'est pas unitaire, on remarque que le théorème 2 se déduit de la proposition 1 et du théorème 1. Mais dans la proposition 1, la preuve utilise seulement $q \geqq d(Q)$ et non pas $q = d(Q)$. □

2e cas : $p_1 = p - 1$, $q_1 = q$:

On applique la proposition 9 de [GLRR1]. Les démonstrations résultent de calculs immédiats.

PROPOSITION 4 : *Nous supposons* $p_1 = p - 1$, $q_1 = q \geqq 1$

On a alors pour $j < p_1$, *l'égalité* :

$$\mathrm{Sp}(\mathbf{StHa}_j(P, Q)) = (-1)^q \cdot cd(P_1)^2 \cdot cd(Q_1) \cdot \mathbf{StHa}_j(P_1, Q_1)$$

PROPOSITION 5 : *Nous supposons* $p_1 = p - 1$.

On a alors pour $j < p_1 - 1$, *l'égalité* :

$$\mathrm{Sp}(\mathbf{StHa}_j(P)) = cd(P_1)^2 \cdot \mathbf{StHa}_j(P_1).$$

Il sera donc facile, dans les deux cas envisagés, de calculer des polynômes égaux, à un facteur constant près, à ceux de la suite de Sturm-Habicht de $\mathrm{Sp}(P)$ et $\mathrm{Sp}(Q)$. (On prendra garde seulement à l'initialisation de la suite, à calculer directement).

3e cas : $p_1 < p - 1$, ou $p_1 = p - 1$, $q_1 < q$,

On a $\mathrm{Sp}(\mathbf{StHa}_j(P, Q)) = 0$. Si on veut calculer la suite de Sturm-Habicht avant spécialisation, on doit faire un nouveau calcul : on considère les poly-

nômes

$$P_p := \text{« } P \text{ tronqué au-delà du degré } d(\mathrm{Sp}(P))\text{ »},$$

$$Q_q := \text{« } Q \text{ tronqué au-delà du degré } d(\mathrm{Sp}(Q))\text{ »}$$

on a $\mathrm{Sp}(P)=\mathrm{Sp}(P_p)$, $\mathrm{Sp}(Q)=\mathrm{Sp}(Q_q)$. On calcule alors les $\mathbf{StHa}_j(P_p, Q_q)$.

2. LES DIFFÉRENTES MÉTHODES POUR CALCULER LE NOMBRE DE RACINES RÉELLES D'UN POLYNÔME (ET GÉNÉRALISATION)

On a déjà vu la méthode de Sturm et la méthode de Sturm-Habicht, qui s'en déduit si on connait la théorie des sous-résultants. Une autre méthode d'inspiration *a priori* très différente, due à Hermite, utilise la signature d'une forme quadratique. Nous allons expliquer cette méthode d'Hermite avant d'indiquer les relations entre les différentes méthodes, qui se comprennent bien en utilisant la suite de Sturm-Habicht. Pour les paragraphes *a*) et *c*) de cette section, nous avons utilisé abondamment l'excellent article [KrN] qui nous a été signalé par E. Becker.

Dans tous le chapitre 2 le polynôme P sera *unitaire*.

2.1. Méthode d'Hermite

On considére toujours un anneau intègre **A** de corps de fraction **K**.

Soit $P=X^p+a_{p-1}X^{p-1}+\ldots+a_0$ un polynôme unitaire à coefficients dans **A** et $Q=b_qX^q+b_{q-1}X^{q-1}+\ldots+b_0$ un polynôme à coefficient dans **A**. On note $(\alpha_i)_{i=1,\ldots,p}$ les racines de P dans une clôture algébrique **C** de **K**.

On définit une forme quadratique à p variables $x_0, x_1, \ldots, x_{p-1}$, $B(P, Q)$, par :

$$B(P, Q)=\sum_{i=1,\ldots,p} Q(\alpha_i)(x_0+x_1\alpha_i+\ldots+x_{p-1}\alpha_i^{p-1})^2.$$

Il est clair que $B(P, Q)$ est à coefficients dans **A**, puisque l'expression est symétrique en les α_i.

En désignant par $s(P, Q)_k$, pour $k=0, \ldots, 2p-2$ la somme $\sum_{i=1,\ldots,p} Q(\alpha_i)\alpha_i^k$ on a :

$$B(P, Q)=\sum_{k=0,\ldots,p-1;\, j=0,\ldots,p-1} s(P, Q)_{k+j}x_kx_j.$$

Lorsque $Q=1$, on note $B(P)$ la forme $B(P, 1)$; on a

$$B(P)=\sum_{i=1,\ldots,p}(x_0+x_1\alpha_i+\ldots+x_{p-1}\alpha_i^{p-1})^2.$$

En désignant par s_k la somme de Newton $\sum_{i=1,\ldots,p}\alpha_i^k$ on a:

$$B(P)=\sum_{k=0,\ldots,p-1;\, j=0,\ldots,p-1} s_{k+j}x_k x_j.$$

Si $\leqq$ est un ordre sur $\mathbf{K}$ on note $\mathbf{R}$ la clôture réelle de $\mathbf{K}$ pour l'ordre $\leqq$. Rappelons qu'on note $\mathbf{c}_+(P, Q)$ le nombre de racines de P dans $\mathbf{R}$ avec $Q>0$, $\mathbf{c}_-(P, Q)$ le nombre de racines de P dans $\mathbf{R}$ avec $Q<0$, $\mathbf{c}(P)$ le nombre de racines de P dans $\mathbf{R}$. La forme quadratique $B(P, Q)$ a une signature dans le corps $\mathbf{R}$ (cette signature dépend du choix de l'ordre $\leqq$ sur $\mathbf{K}$). On prend alors pour corps $\mathbf{C}$ le corps $\mathbf{R}[i]$ (avec $i^2=-1$). On appelera *racines réelles* celles qui sont dans $\mathbf{R}$ et *racines complexes* celles qui sont dans $\mathbf{C}-\mathbf{R}$.

THÉORÈME 3 (méthode d'Hermite [Her]) : *Avec les notations ci-dessus,*

(i) *le rang de $B(P, Q)$ est égal au nombre de racines distinctes de P non racines de Q dans* $\mathbf{C}$.

(ii) *la signature de $B(P, Q)$ est égale à $\mathbf{c}_+(P, Q)-\mathbf{c}_-(P, Q)$.*

Démonstration: La démonstration est élémentaire (voir [Gan] ou [KrN] ou [GLRR3]). □

COROLLAIRE : *Avec les notations précédentes, la signature de $B(P)$ est égale à $\mathbf{c}(P)$.*

2.2. Bezoutiens et coefficients sous-résultants

DÉFINITION ET NOTATION : *On appelle* **bezoutiens** *et on note $b(P, Q)_k$ les mineurs principaux* (1) *de la matrice symétrique*

$$A=(s(P, Q)_{i+j-2})_{i=1,\ldots,p;\, j=1,\ldots,p}$$

associée à la forme quadratique $B(P, Q)$.

Considérons le développement en $1/X$ de la fonction rationnelle $P'Q/P$. Si $P=\prod_{i=1,\ldots,p}(X-\alpha_i)$ on a $P'/P=\sum_{i=1,\ldots,p}1/(X-\alpha_i)$, et en posant

(1) Définition donnée au début du paragraphe 2.3 qui suit.

$Q = Q(\alpha_i) + (X - \alpha_i) A_i \quad P'Q/P = \sum_{i=1,\ldots,p} A_i + \sum_{i=1,\ldots,p} Q(\alpha_i)/(X - \alpha_i)$. On en déduit que le coefficient de $1/X^k$ dans le développement de $P'Q/P$ en $1/X$ est, avec les notations précédentes $s(P, Q)_{k-1}$.

Par ailleurs, si R est le reste de la division de $P'Q$ par P, R/P est la partie fractionnaire de la fraction rationnelle $P'Q/P$ de sorte que $s(P, Q)_{k-1}$ est le coefficient de $1/X^k$ dans le développement en $1/X$ de R/P.

On a donc: (*) $R/P = \sum_{i=1,\ldots,p} Q(\alpha_i)/(X - \alpha_i)$.

Tout ceci permet d'établir par identification du membre gauche et du membre droit de (*) des relations entre les $s(P, Q)_k$, les coefficients de $P = X^p + a_{p-1} X^{p-1} + \ldots + a_0$ et ceux de $R = c_{p-1} X^{p-1} + \ldots + c_0$ (c_{p-1} éventuellement nul), à savoir:

$s(P, Q)_0 = c_{p-1}$

$s(P, Q)_1 + a_{p-1} s(P, Q)_0 = c_{p-2}$

$\ldots$

$s(P, Q)_{p-1} + \ldots\ldots\ldots + a_1 s(P, Q)_0 = c_0$

$s(P, Q)_{n-1} + \ldots\ldots\ldots + a_1 s(P, Q)_{n-p} = 0$ pour $n > p$.

On désignera les relations précédentes par (**) dans la suite.

PROPOSITION 6 : *Soient P et Q deux polynômes avec*:

$$P = X^p + a_{p-1} X^{p-1} + \ldots + a_0 \qquad Q = b_q X^q + b_{q-1} X^{q-1} + \ldots + b_0$$

En notant $\mathbf{sth}_j(P, Q))$ *le coefficient en degré j de* $\mathbf{StHa}_j(P, Q)$ *on a pour tout $k = 1, \ldots, p$*:

$$\mathbf{sth}_{p-k}(P, Q) = b(P, Q)_k$$

Démonstration: Notons $R = c_{p-1} X^{p-1} + \ldots + c_0$ le reste de la division euclidienne de P par $P'Q$. D'après la définition de la suite de Sturm-Habicht et la proposition 2 (iii):

$$\mathbf{sth}_{p-k}(P, Q)) = (-1)^{k(k-1)/2} \mathbf{sr}_{p-k}(P, p, R, p-1).$$

Rappelons la définition de $\mathbf{sr}_{p-k}(P, p, R, p-1)$, noté $\mathbf{sr}_{p-k}$.

$$\mathbf{sr}_{p-k}=\begin{vmatrix} 1 & a_{p-1} & \cdots & a_{p-2k+2} \\ 0 & 1 & a_{p-1} & \cdots & a_{p-2k+3} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 1 & a_{p-1} & \cdots & a_{p-k} \\ c_{p-1} & c_{p-2} & \cdots & \cdots & c_{p-2k+1} \\ 0 & c_{p-1} & c_{p-2} & \cdots & c_{p-2k+2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & c_{p-1} & \cdots & c_{p-1-k} \end{vmatrix}$$

Les équations de (**) permettent d'écrire, en notant $s'_k := s(P, Q)_k$:

$$\mathbf{sr}_{p-k}=\begin{vmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ s'_0 & s'_1 & \cdots & s'_{k-1} & \cdots & \cdots & s'_{2k-2} \\ 0 & s'_0 & s'_1 & \cdots & \cdots & \cdots & s'_{2k-3} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & s'_0 & s'_1 & \cdots & s'_{k-1} \end{vmatrix} \begin{vmatrix} 1 & a_{p-1} & \cdots & \cdots & a_{p-2k+2} \\ 0 & 1 & a_{p-1} & \cdots & a_{p-2k-2} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 1 & a_{p-1} & \cdots & a_{p-k} \\ 0 & \cdots & \cdots & 0 & 1 & \cdots & a_{p-k+1} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \end{vmatrix}$$

d'où

$$\mathbf{sr}_{p-k}=\begin{vmatrix} s'_{k-1} & \cdots & \cdots & s'_{2k-2} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ s'_0 & s'_1 & \cdots & s'_{k-1} \end{vmatrix}$$

et enfin, en tenant compte de la permutation des lignes,

$$\mathbf{sr}_{p-k}=(-1)^{k(k-1)/2}\, b(P, Q)_k. \quad \square$$

2.3. Mineurs principaux et signature d'une forme quadratique

On appelle **mineurs principaux d'une matrice** $A=(a_{i,j})_{i=1,\ldots,p,\ j=1,\ldots,p}$ les déterminants $\det(A_k)$ des matrices $A_k=(a_{i,j})_{i=1,\ldots,k,\ j=1,\ldots,k}$ pour $k=1, \ldots, p$.

Si A est une matrice symétrique à coefficients dans un corps ordonné on a le résultat suivant dû à Jacobi.

PROPOSITION 7 (**théorème de Jacobi**) : *Avec les notations précédentes, si les* $\det(A_k)$ *sont tous non nuls, la signature de la forme quadratique associée à une matrice symétrique A est égale à la différence entre le nombre d'éléments positifs et le nombre d'éléments négatifs dans la suite* $(1, (\det(A_k))_{k=1,\ldots,p})$.

Si des mineurs principaux de la matrice s'annulent il n'est plus vrai en général que les mineurs principaux de la matrice symétrique déterminent la signature de la forme quadratique (pour tout ceci voir [Gan], chap. 10).

Il est possible de généraliser le théorème de Jacobi et d'obtenir la signature grâce aux seuls signes des mineurs principaux dans le cas particulier des formes de Hankel. Les **formes de Hankel** sont les formes quadratiques du type $B = \sum_{k=0,\ldots,p-1;\ 1=0,\ldots,p-1} c_{k+1}\, x_k\, x_1$. La matrice symétrique $A=[a_{i,j}]_{i=1,\ldots,p;\ j=1,\ldots,p}$ qui est associée à B est définie par $a_{i,j}=c_{i+j-2}$.

Faisons tout d'abord une remarque: considérons une suite $(a_0, \ldots, a_n)$ d'éléments tous non nuls de **K**. Rappelons qu'on note $V(a_0, \ldots, a_n)$ le nombre de changements de signes dans $(a_0, \ldots, a_n)$. On définit maintenant le **nombre de permanences de signes** $\Pi(a_0, \ldots, a_n)$ dans $(a_0, \ldots, a_n)$ par récurrence sur n:

$\Pi(a_0)=0$,

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

$\Pi(a_0, \ldots, a_{n+1})=\Pi((a_0, \ldots, a_n)$ sinon.

On a alors la relation suivante.

Remarque 2: Si les éléments de $(a_0, \ldots, a_n)$ sont tous non nuls, alors on a

$$\Pi(a_0, \ldots, a_n)=V((-1)^n a_0, (-1)^{n-1} a_1, \ldots, -a_{n-1}, a_n).$$

La différence $C(a_0, \ldots, a_n)$ entre le nombre d'éléments positifs et le nombre d'éléments négatifs dans la suite $(a_0, \ldots, a_n)$ est égale à $\Pi(a_0, \ldots, a_n)-V(a_0, \ldots, a_n)$ si $a_0>0$.

On peut donc réénoncer ainsi le théorème de Jacobi:
Avec les notations précédentes, si les $\det(A_k)$ sont tous non nuls, la signature de la forme quadratique associée à une matrice symétrique A est égale à $C(1, (\det(A_k))_{k=1,\ldots,p})$.

La proposition suivante indique comment se généralise le théorème de Jacobi. On doit tout d'abord généraliser la définition du nombre $C(a_0, \ldots, a_n)$ au cas d'une suite comportant des zéros.

DÉFINITION : *On définit la quantité* $C(a_0, \ldots, a_n)$ *où* $(a_0, \ldots, a_n)$ *est une suite d'éléments de* $\mathbf{K}$ *et* $a_0 \neq 0$ *de la manière suivante*:

– *faisons apparaître les éléments nuls de* $(a_0, \ldots, a_n)$

$$(a_0, \ldots, a_n) = (a_0, \ldots, a_{i(1)}, 0, \ldots, 0, a_{i(1)+k(1)+1}, \ldots,$$
$$a_{i(2)}, 0, \ldots, 0, a_{i(2)+k(2)+1}, \ldots,$$
$$a_{i(t-1)+k(t-1)}, 0, \ldots, 0, a_{i(t-1)+k(t-1)+1}, \ldots, a_{i(t)}, 0, \ldots, 0)$$

(*tous les éléments* a_j, *tels que* $i(h-1)+k(h-1) < j \leqq i(h)$, $h = 1, \ldots, t$ *sont non nuls*),

– *définissons*

$$C(a_0, \ldots, a_n) := \sum_{h=1,\ldots,t} C(a_{i(t-1)+k(t-1)+1}, \ldots, a_{i(t)}) + \sum_{h=1,\ldots,t} \varepsilon_h$$

avec $\varepsilon_h = 0$ *si* $k(h)$ *est impair,* $(-1)^{k(h)/2} \operatorname{signe}(a_{i(h)+k(h)+1} \cdot a_{i(h)})$ *si* $k(h)$ *est pair.*

PROPOSITION 8 : *Avec les notations précédentes, la signature d'une forme de Hankel dont la matrice symétrique associée est* A, *est égale à* $C(1, (\det(A_k))_{k=1,\ldots,p})$.

Démonstration: Due à Frobenius [Fro]. Il semble difficile d'exposer ceci plus clairement que [Gan], chapitre 10. □

Les résultats précédents nous permettent d'énoncer la proposition suivante:

PROPOSITION 9 : *La signature* $\mathbf{S_B}(P, Q)$ *de* $B(\mathrm{P}, Q)$ *est égale à la quantité* $C(1, (b(P, Q)_k)_{k=1,\ldots,p})$.

Démonstration: On utilise la proposition 8 et le fait que la matrice associée à $B(P, Q)$ est une matrice de Hankel. □

Remarque 3: A cause de la relation entre bezoutiens et coefficients sous-résultants, il est clair que si le rang de la forme quadratique $B(P, Q)$ est r, alors le bezoutien $b(P, Q)_r$ est non nul (utiliser le corollaire du théorème 3 de [GLRR1]). Ceci permet d'obtenir plus facilement la proposition 8 dans le cas particulier de $B(P, Q)$ (on n'a pas besoin du théorème 23 p. 344 de [Gan]).

THÉORÈME 4 (méthode des bezoutiens [Her], [Syl]) : *La quantité* $C(1, (b(P, Q)_k)_{k=1,\dots,p})$ *est égale à* $\mathbf{c}_+(P, Q) - \mathbf{c}_-(P, Q)$.

Démonstration : On applique le théorème 3 et la proposition 9. □

Remarque 4 : 1) Les calculs des $(b(P, Q)_k)_{k=1,\dots,p}$ se font dans l'anneau **A**. La quantité $C(1, (b(P, Q)_k)_{k=1,\dots,p})$ dépend évidemment du choix de l'ordre sur **K**.

2) Considérons maintenant un homomorphisme d'anneau Sp de **A** dans **A'**. Les $b(\mathrm{Sp}(P), \mathrm{Sp}(Q))_k$ sont les spécialisés des $b(P, Q)_k$. Il faut recalculer $C(1, (b(\mathrm{Sp}(P), \mathrm{Sp}(Q))_k)_{k=1,\dots,p})$ en évaluant les signes des $b(\mathrm{Sp}(P), \mathrm{Sp}(Q))_k$ et en utilisant la définition de C.

Notons que dans toute la théorie de Hermite et des bezoutiens il est essentiel que le degré de P soit fixé.

2.4. De la méthode de Sturm-Habicht à la méthode d'Hermite

Nous allons maintenant indiquer comment calculer $\mathbf{V}_{\mathbf{StHa}}(P, Q)$ à partir des coefficients $\mathbf{sth}_k(P, Q)_{k=1,\dots,p}$, en l'absence des polynômes $\mathbf{StHa}_k(P, Q)$, ce qui finira d'expliciter le rapport entre la méthode de Sturm et la méthode d'Hermite.

PROPOSITION 10 : $\mathbf{V}_{\mathbf{StHa}}(P, Q)$ *est égal à* $C((\mathbf{sth}_{p-k}(P, Q))_{k=0,\dots,p})$.

Ce résultat reste valable même si P n'est pas unitaire.

Démonstration : *Voyons le cas où P est unitaire.*

Il est clair que si tous les $\mathbf{sth}_{p-k}(P, Q)$ sont non nuls on a :

$$\mathbf{V}_{\mathbf{StHa}}(P, Q; +\infty) = V(\mathbf{sth}_{p-k}(P, Q)_{k=0,\dots,p})$$

$$\mathbf{V}_{\mathbf{StHa}}(P, Q; -\infty) = V((-1)^{p-k}\mathbf{sth}_{p-k}(P, Q)_{k=0,\dots,p})$$

$$= \Pi(\mathbf{sth}_{p-k}(P, Q)_{k=0,\dots,p}) \quad \text{en utilisant la remarque 2,}$$

d'où :

$$\mathbf{V}_{\mathbf{StHa}}(P, Q) = \mathbf{V}_{\mathbf{StHa}}(P, Q; -\infty) - \mathbf{V}_{\mathbf{StHa}}(P, Q; +\infty)$$

$$= C(\mathbf{sth}_{p-k}(P, Q)_{k=0,\dots,p}).$$

d'où :

$$\mathbf{V}_{\mathbf{StHa}}(P, Q) = \mathbf{V}_{\mathbf{StHa}}(P, Q; -\infty) - \mathbf{V}_{\mathbf{StHa}}(P, Q; +\infty)$$

$$= C(\mathbf{sth}_{p-k}(P, Q)_{k=0,\dots,p}).$$

Le cas non trivial est celui d'un polynôme défectueux dans la suite de Sturm-Habicht car alors il y a un zéro de plus dans la suite des $\mathbf{sth}_{p-k}(P, Q)$ $(k=0, \ldots, p)$ que dans la suite de Sturm-Habicht.

Rappelons (proposition 2) que si

$$\mathbf{sth}_j(P, Q)\neq 0, \qquad \mathbf{sth}_{j-1}(P, Q)=\ldots=\mathbf{sth}_{j-h}(P, Q)=0, \qquad \mathbf{sth}_{j-h-1}(P, Q)\neq 0$$

alors $\mathbf{StHa}_j(P, Q)$ est de degré j, $\mathbf{StHa}_{j-1}(P, Q)$ est défectueux de degré $j-h-1$ et tous les $\mathbf{StHa}_k(P, Q)$, $j-h\leqq k<j-1$, sont nuls.

Nous allons montrer, en notant $\mathbf{StHa}_j(P, Q)$, $\mathbf{StHa}_{j-1}(P, Q)$ et $\mathbf{StHa}_{j-h-1}(P, Q)$ respectivement $\mathbf{StHa}_j$, $\mathbf{StHa}_{j-1}$ et $\mathbf{StHa}_{j-h-1}$ que

$$V((\mathbf{StHa}_j, \mathbf{StHa}_{j-1}, \mathbf{StHa}_{j-h-1}); -\infty) - V((\mathbf{StHa}_j, \mathbf{StHa}_{j-1}, \mathbf{StHa}_{j-h-1}); +\infty)=\varepsilon_h$$

avec $\varepsilon_h=0$ si h est impair, $\varepsilon_h=(-1)^{h/2}$ signe $(\mathbf{sth}_j(P, Q)\ \mathbf{sth}_{j-h-1}(P, Q))$ sinon.

D'après la proposition 2 nous avons, en notant c_{j-h-1} le coefficient dominant de $\mathbf{StHa}_{j-1}$,

$$\mathbf{sth}_j(P, Q)^h\,\mathbf{StHa}_{j-h-1}=(-1)^{h(h+1)/2}(c_{j-h-1})^h\,\mathbf{StHa}_{j-1},$$

d'où

$$\mathbf{sth}_j(P, Q)^h\,\mathbf{sth}_{j-h-1}(P, Q)=(-1)^{h(h+1)/2}(c_{j-h-1})^{h+1}\ (***).$$

Il est maintenant facile de voir avec (***) que

– si h est impair et $(-1)^{(h+1)/2}=1$ alors

$$V(\mathbf{StHa}_j, \mathbf{StHa}_{j-1}, \mathbf{StHa}_{j-h-1}; -\infty) - V(\mathbf{StHa}_j, \mathbf{StHa}_{j-1}, \mathbf{StHa}_{j-h-1}; +\infty)=0$$

– si h est impair et $(-1)^{(h+1)/2}=-1$ alors

$$V(\mathbf{StHa}_j, \mathbf{StHa}_{j-1}, \mathbf{StHa}_{j-h-1}; -\infty) - V(\mathbf{StHa}_j, \mathbf{StHa}_{j-1}, \mathbf{StHa}_{j-h-1}; +\infty)=0$$

– si h est pair et $(-1)^{h/2}=1$ alors

$$V(\mathbf{StHa}_j, \mathbf{StHa}_{j-1}, \mathbf{StHa}_{j-h-1}; -\infty) - V(\mathbf{StHa}_j, \mathbf{StHa}_{j-1}, \mathbf{StHa}_{j-h-1}; +\infty)=1$$

– si h est pair et $(-1)^{h/2} = -1$ alors

$$V(\mathbf{StHa}_j, \mathbf{StHa}_{j-1}, \mathbf{StHa}_{j-h-1}; -\infty) - V(\mathbf{StHa}_j, \mathbf{StHa}_{j-1}, \mathbf{StHa}_{j-h-1}; +\infty) = -1$$

et de vérifier que dans les quatre cas le résultat est égal à ε_h.

Le cas où P n'est pas unitaire se déduit du cas P unitaire et de la proposition 1. □

THÉORÈME 5 : *Les deux nombres* $\mathbf{V}_{\mathbf{StHa}}(P, Q)$ *et* $\mathbf{S}_{\mathbf{B}}(P, Q)$ *coïncident.*

Démonstration: Mettre bout à bout les propositions 6, 9 et 10. □

2.5. Conclusions et remarques

Résumé des résultats obtenus

On peut résumer dans le théorème suivant les résultats obtenus

THÉORÈME 6 : *a*) (i) *Les* 2 *nombres* $\mathbf{V}_{\mathbf{Stu}}(P, Q; a, b)$, $\mathbf{V}'_{\mathbf{StHa}}(P, Q; a, b)$ *coïncident.* (ii) *Ils sont égaux à* $\mathbf{c}_+(P, Q; a, b) - \mathbf{c}_-(P, Q; a, b)$.

b) (i) *Les* 3 *nombres* $\mathbf{V}_{\mathbf{Stu}}(P, Q)$, $\mathbf{V}_{\mathbf{StHa}}(P, Q)$, $C((\mathbf{sth}_{p-k}(P, Q))_{k=0,\ldots,p})$ *coïncident, et coïncident avec* $\mathbf{S}_{\mathbf{B}}(P, Q)$ *lorsque P est unitaire.* (ii) *Ils sont égaux à* $\mathbf{c}_+(P, Q) - \mathbf{c}_-(P, Q)$.

Démonstration: *a*) (i) voir le théorème 2.

a) (ii) Voir le théorème 1 (i) de [GLRR1],

b) (i) voir les théorèmes 2 et 5 et la proposition 10.

b) (ii): *a*) et au choix le théorème 1 (ii) de [GLRR1], ou le théorème 3. □

Dans la démonstration du point *b*) on a donc produit une démonstration du point (ii) du théorème 1 de [GLRR1] (théorème de Sylvester, cas où l'intervalle est **R** tout entier) à partir du théorème 3 (méthode d'Hermite), ou inversement, et ceci essentiellement par des méthodes d'algèbre linéaire. Il est intéressant de noter que les preuves – toutes deux élémentaires – de ces deux théorèmes reposent sur des principes distincts: théorème des valeurs intermédiaires dans un cas, existence de racines complexes conjuguées dans l'autre. On pourrait aussi considérer qu'à partir des théorèmes 1 (ii) de [GLRR1] et du théorème 3 on a produit une preuve de la proposition 9 sans utiliser les résultats de Frobenius sur les formes de Hankel.

Discussion

En définitive, quelle est donc la meilleure méthode pour calculer $\mathbf{c}_+(P, Q) - \mathbf{c}_-(P, Q)$?

La méthode de Sturm-Sylvester n'a que des inconvénients par rapport à la méthode de Sturm-Habicht : calculs dans un corps plutôt que dans un anneau, défauts de spécialisation, temps de calcul plus long. La méthode de Sturm-Habicht est en temps polynomial (si on travaille sur les entiers naturels, ou plus généralement sur un anneau où les déterminants se calculent en temps polynomial).

Étant obtenue par des changements de signes automatiques à partir de la suite des sous-résultants, la suite de Sturm-Habicht peut, elle aussi, se calculer par des méthodes modulaires.

La méthode d'Hermite donne elle aussi un algorithme (la méthode de réduction des formes quadratiques de Gauss donne naissance à des calculs explicites); il est toutefois plus intéressant de calculer la signature de $B(P, Q)$ par la méthode des bezoutiens. En utilisant alors la méthode de Bareiss pour calculer les déterminants on a alors affaire (sur les entiers ou sur un anneau où les déterminants se calculent en temps polynomial) à un algorithme en temps polynomial. Du point de vue des spécialisations, rappelons que la méthode des bezoutiens se spécialise bien à condition qu'on travaille toujours en degré fixé pour P (voir remarque 4).

Si l'on compare maintenant la méthode de Sturm-Habicht à celle des bezoutiens, on observe que la méthode de Sturm-Habicht donne des calculs plus rapides :

– en utilisant les relations entre sous-résultants et restes on donne un algorithme de calcul de toute la suite des sous-résultants plus rapide que le calcul d'un seul coefficient sous-résultant par la méthode de Bareiss (voir le point « complexité » dans le chapitre 2), donc également plus rapide que le calcul des bezoutiens (qui est essentiellement le même que celui des sous-résultants). De plus la méthode de Sturm-Habicht s'applique au cas où P n'est pas unitaire et permet de calculer directement $\mathbf{c}_+(P, Q; a, b) - \mathbf{c}_-(P, Q; a, b)$.

– les propriétés de spécialisation de la suite de Sturm-Habicht sont meilleures : on peut en particulier traiter le cas où le degré de P baisse exactement de 1 alors que celui de Q ne change pas.

– Pour calculer $\mathbf{c}_+(P, Q) - \mathbf{c}_-(P, Q)$, il faut noter que *la méthode la plus rapide est la suivante : calculer la suite des polynômes sous-résultants par un des algorithmes du chapitre* 2, *en déduire la suite de Sturm-Habicht par des changements de signes automatiques, et évaluer les signes des seuls coefficients de Sturm-Habicht et appliquer la proposition* 10 (valable même pour P non unitaire). Ce qui donne un calcul en $O(n^2)$ opérations arithmétiques suivies de n évaluations de signes.

Dans l'état actuel des choses, on peut donc conclure en général à la supériorité de la méthode de Sturm-Habicht. La méthode des bezoutiens pourra toutefois peut-être s'avérer plus efficace dans certains cas, car elle repose sur les sommes de Newton qui sont des fonctions symétriques de calcul rapide (*voir* [Val]).

Remarque 5 : On vient de voir que les calculs pour trouver le nombre de racines de P (resp. la différence entre le nombre de racines de P rendant $Q>0$ et le nombre de racines de P rendant $Q<0$) sont essentiellement les mêmes dans la méthode d'Hermite (plus précisément celle des bezoutiens) et celle de Sturm (plus précisément celle de Sturm-Habicht).

Une différence essentielle entre la méthode d'Hermite (ou la méthode des bezoutiens) et celle de Sturm (ou de Sturm-Habicht) est que dans la méthode d'Hermite on traite globalement toutes les racines et qu'on ne peut étudier avec les seuls polynômes P et Q ce qui se passe sur un intervalle $]a, b[$. Une manière de pallier à cet inconvénient est d'introduire les polynômes $(a-x)Q$, $(b-x)Q$.

Nous allons voir sur un exemple que ces différents calculs donnent des résultats différents, et que les résultats les plus simples sont obtenus pour la suite de Sturm-Habicht de P et P'.

Exemple 3 : Comparons donc les différents calculs qui permettent de déterminer la condition (C) pour que le nombre de racines réelles comprises strictement entre -1 et 1 d'un polynôme du troisième degré $P=x^3+px+q$ sans racines doubles soit égale à trois :

1) calcul de la suite de Sturm-Habicht de P et évaluation en -1 et 1 : on trouve que (C) est équivalente à :

$$p+q+1>0, \quad q-p-1<0, \quad p+3>0, \quad 2p+3q<0, \quad -2p+3q>0,$$
$$4p^3+27q^2<0,$$

2) calcul des suites de Sturm-Habicht de x^3+px+q et $1-x$, puis de x^3+px+q et $-1-x$ (ou méthode des bezoutiens pour x^3+px+q et $1-x$, puis pour x^3+px+q et $-1-x$) :
on trouve que (C) est équivalente à :

$$4p^2+6p-9q<0, \quad 4p^2+6p+9q<0, \quad (p+q+1)(4p^3+27q^2)<0,$$
$$(q-p-1)(4p^3+27q^2)>0,$$

Il n'est pas immédiat que ces systèmes d'inégalités soient équivalents. Le résultat 1) est le plus simple, et ne peut être obtenu par la méthode des bezoutiens.

Note : Dans l'article précédent [GLRR1], la proposition 8 p. 576 est valable pour tout degré $d_i \leqq s$ et donne donc la relation explicite complète liant les sous-résultants et les restes.

BIBLIOGRAPHIE

[Fro] FROBENIUS, Uber das Traegheitsgesetz des quadratishen Formen, *S-B Pruss. Akad. Wiss.*, Marz 1984, 241-256; Mai 1984, 403-431.

[Gan] Fr. GANTMACHER, *Théorie des matrices*, t. I, Dunod 1966.

[GLRR1] L. GONZALEZ, H. LOMBARDI, T. RECIO, M.-F. ROY, Spécialisation de la suite de Sturm et sous-résultants (I), *Inf. Théorique et Appl.*, 1990, *6*, 561-588.

[GLRR2] L. GONZALEZ, H. LOMBARDI, T. RECIO et M.-F. ROY, *Sturm-Habicht sequences*, Proceedings ISSAC, 1989.

[GLRR3] L. GONZALEZ, H. LOMBARDI, T. RECIO, M.-F. ROY, *Spécialisation de la suite de Sturm et sous-résultants*, Version détaillée, dans CALSYF (journées du GRECO de Calcul Formel) 1989.

[GLRR4] L. GONZÁLEZ-VEGA, H. LOMBARDI, T. RECIO, M.-F. ROY, *Determinants and real roots of univariate polynomials.* A paraître dans : Special volume of the series "Texts and Monographs in Symbolic Computation" (Springer-Verlag) ayant pour titre : 25 *years of Quantifier Elimination and Cylindrical Algebraic Decomposition*, (Compte-rendus du Symposium on quantifier elimination and cylindrical algebraic decomposition. Linz. 6-8 oct. 93).

[Gon] L. GONZALEZ, *The Proof of the Sylvester Theorem Through Habicht Sequences*, Preprint, Université de Santander, 1988.

[Hab] W. HABICHT, Eine Verallgemeinerung des Sturmschen Wurzel zählverfahrens, *Comm. Math. Helvetici*, 1948, *21*, 99-116.

[Her] C. HERMITE, Remarques sur le théorème de Sturm, *C.R. Acad. Sci. Paris*, 1853, *36*, 52-54.

[KrN] M. G. KREIN, M. A. NAIMARK, The Method of Symmetric and Hermitian Forms on the Theory of the Separation of the Roots of Algebraic Equations, Originairement publié à Kharkov (1936), *Lin. Multilinear algebra*, 1981, *10*, 265-308.

[Syl] 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.
Reprint dans : Sylvester, Collected Math. Papers, Chelsea Pub. Comp. NY, 1983, vol. 1, 429-586.

[Val] A. VALLIBOUZE, *Fonctions symétriques et changements de base*, Thèse, Université Paris-VI, 1987.