SPECIALISATION DE LA SUITE DE STURM ET SOUS-RESULTANTS

Laureano GONZALEZ
Mathématiques
Université de Santander
Santander ESPAGNE

Henri LOMBARDI
Mathématiques
UFR des Sciences et des Techniques
Université de Franche Comté
25030 Besançon CEDEX

Tomas RECIO
Mathématiques
Université de Santander
Santander ESPAGNE

Marie-Françoise ROY
IRMAR
Université de Rennes I CEDEX
35042 Rennes CEDEX

Résumé

Le but de cet article est de présenter et de comparer les différents algorithmes pour compter le nombre de racines réelles d'un polynôme et leurs généralisations. La clé pour comprendre les relations entre les diverses méthodes est l'étude de la suite de Sturm-Habicht, qui repose sur la théorie des polynômes sous-résultants.

Dans le §1 nous donnons le théorème de Sturm et sa généralisation. Dans le §2 nous donnons une légère généralisation de la notion de polynôme sous-résultant de deux polynômes; ceci permet de simplifier les démonstrations concernant les polynômes sous-résultants, de préciser les algorithmes pour les calculer, et de traiter de manière agréable les problèmes de spécialisation, même lorsqu'il y a chute du degré (d'un ou même parfois des deux polynômes). Dans le § 3 nous définissons et étudions la suite de Sturm-Habicht. Dans le § 4 nous décrivons et comparons différentes méthodes pour compter le nombre de racines réelles d'un polynôme.

Mots clé

Sous-résultants, algorithme des sous-résultants, suite de Sturm, suite de Sturm-Habicht, spécialisation, nombre de racines réelles

Introduction

Nous présentons dans le § 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 d'un polynôme P . Dans le cas général on détermine la différence entre le nombres 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, sont classiques (cf [Syl]). Nous indiquons ensuite les difficultés rencontrées lorsque on cherche à spécialiser ce calcul.

Dans le § 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 § 2.c ; en outre, les preuves de plusieurs résultats sont simplifiées.

Dans le § 2. c , nous indiquons comment se spécialisent ces polynômes sous-résultants.

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

Dans le § 3 , 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 Sturm pour compter le nombre de racines réelles d'un polynôme P (ou pour déterminer la différence entre le nombres 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 § 4 , nous présentons la méthode d'Hermite pour déterminer le nombres 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.

Une version abrégée de cet article est à paraître en deux parties dans ([GLRR1]). Les résultats étaient annoncés dans [GLRR2].

Plan de l'article

1) Suite de Sturm de deux polynômes
   a) Définitions et notations
   b) Propriétés de la suite de Sturm
   c) Problèmes de spécialisation

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

3) Suite de Sturm-Habicht et spécialisation
   a) Suite de Habicht
   b) Suite de Sturm-Habicht
   c) Spécialisation de la suite de Sturm-Habicht

4) Les différentes méthodes pour calculer le nombre de racines réelles d'un polynôme (et généralisation)
   a) Méthode d'Hermite
   b) Bezoutiens et coefficients sous-résultants
   c) Mineurs principaux et signature d'une forme quadratique
   d) De la méthode de Sturm-Habicht à la méthode de Hermite
   e) Conclusions et remarques

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 **Rst**(P,S) le reste de la division euclidienne de P par S dans **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 $j \leq \sup(d(P),d(S)+1)$ .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 $0 < j < t-1$:

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

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 2.b et 2.c .

Remarque 1 :

Si un point a d'une extension de **K** n'est pas racine de P , il ne peut être racine de deux restes successifs. En effet le PGCD de deux restes successifs coincide avec le PGCD de P et S .

Suite des restes signés de P et S

Etant donnés deux polynômes P et S nous appelerons:

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 :

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

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

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 $0 < j < t-1$:

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

Suite de Sturm

Etant donnés deux polynômes P et Q nous appellerons:

suite de Sturm de P et Q

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

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

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

Nous notons de même

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

Si $Q = 1$ on note $\mathbf{Stu}^m(P,Q)$ et $\mathbf{Stu}_j(P,Q)$ respectivement $\mathbf{Stu}^m(P)$ et $\mathbf{Stu}_j(P)$, on a $\mathbf{Stu}^0(P) = P$, $\mathbf{Stu}^1(P) = P'$, $\mathbf{Stu}^{m+1}(P) = -\,\mathbf{Rst}(\,\mathbf{Stu}^{m-1}(P),\,\mathbf{Stu}^m(P))$ et on retrouve la notion classique de **suite de Sturm de P**.

Nombre de changements de signes

Toutes les définitions précécentes 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 $\leq$, 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** $V(a_0,...,a_n)$ dans une suite $(a_0,...,a_n)$ d'éléments de **K** par récurrence sur n :

$V(a_0) = 0$,

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

$V(a_0,...,a_{n+1}) = V(a_0,...,a_n) + 1$ sinon.

Si $f = [f_0,f_1,...,f_n]$ est une suite de polynômes et si a et b sont deux éléments de $K \cup \{+\infty\} \cup \{-\infty\}$ on appelera **nombre de changements de signes de $f_0,f_1,...,f_n$ en x** et on notera $V(f_0,f_1,...,f_n ; x)$ ou même $V(f ; x)$ la quantité $V(f_0(x),f_1(x),...,f_n(x))$; on appellera **différence des changements de signe dans la suite $f_0,f_1,...,f_n$ entre a et b** et on notera $V(f_0,f_1,...,f_n ; a,b)$ la quantité $V(f_0,f_1,...,f_n ; a) - V(f_0,f_1,...,f_n ; b)$.

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.

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

$V_{Rss}(P,S ; a)$	le nombre de changements de signes dans la suite des restes signés de P et S en a,
$V_{Rss}(P,S ; a,b)$	$:= V_{Rss}(P,S ; a) - V_{Rss}(P,S ; b)$
$V_{Rss}(P,S)$	$:= V_{Rss}(P,S ; -\infty) - V_{Rss}(P,S ; +\infty)$
$V_{Stu}(P,Q ; a)$	$:= V_{Rss}(P,R ; a)$, où $R = Rst(P'Q,P)$
$V_{Stu}(P,Q ; a,b)$	$:= V_{Rss}(P,R ; a,b)$
$V_{Stu}(P,Q)$	$:= V_{Rss}(P,R)$.
$V_{Stu}(P ; a)$	$:= V_{Stu}(P,1 ; a)$
$V_{Stu}(P ; a,b)$	$:= V_{Stu}(P)$

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

$c_\varepsilon(P,Q;a,b)$	le nombre d'éléments de : $\{u \in]a, b[\ / \ P(u) = 0 , signe(Q(u)) = \varepsilon\}$
$c_\varepsilon(P,Q)$	$:= c_\varepsilon(P,Q;-\infty,+\infty)$
$c(P;a,b)$	$:= c_+(P,1;a,b)$
$c(P)$	$:= c_+(P,1)$

b) Propriétés de la suite de Sturm

Théorème 1 (voir Sylvester [Syl] pour un résultat analogue) :

Soit un corps $\mathbf{K}$, soit $\leq$ un ordre sur $\mathbf{K}$ et soit $\mathbf{R}$ la clôture réelle de $\mathbf{K}$ muni de l'ordre $\leq$. Soient P et Q deux polynômes quelconques à coefficients dans $\mathbf{K}$ et a et b (avec $a < b$) des points de $\mathbf{K}$ qui ne sont pas racines de P. Alors:

(i) $V_{Stu}(P,Q;a,b) = c_+(P,Q;a,b) - c_-(P,Q;a,b)$.

(ii) $V_{Stu}(P,Q) = c_+(P,Q) - c_-(P,Q)$.

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 $f_m = \mathbf{Stu}^m(P,Q)/\ \mathbf{Stu}^n(P,Q)$.

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 $\mathbf{R}$ 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 et distinct de c .

démonstration du lemme 1:

Précisons d'abord l'énoncé.

Soit c une racine de g_i et a_1 et b_1 des éléments de $\mathbf{R}$ tels que

(1) $a_1 < c < b_1$

(2) aucun g_i $(i = 0,...,s-1)$ ne s'annule sur $]\ a_1,c\ [$ ni sur $]\ c,b_1\ [$,

alors pour tout x de $]\ a_1,b_1\ [- \{c\}$ il y a exactement un changement de signe dans la suite $(\ g_{i-1}(x)\ ,\ g_i(x)\ ,\ g_{i+1}(x)\ )$.

Soit donc x un élément de $]\ a_1,b_1\ [- \{c\}$. On a nécessairement $g_{i-1}(c)$ et $g_{i+1}(c)$ tous les deux différents de zéro, puisque le PGCD de g_i et de g_{i-1} (resp. g_{i+1}) est $g_s = 1$. D'après la définition de g , g_{i+1} est l'opposé du reste de g_{i-1} divisé par g_i , et on a donc $g_{i+1}(c).g_{i-1}(c) < 0$. Les signes de g_{i-1} et g_{i+1} en x coincident avec les signes de g_{i-1} et g_{i+1} en c . Ceci montre que quelque soit le signe de $g_i(x)$ le nombre de changements de signes dans la suite $(\ g_{i-1}(x)\ ,\ g_i(x)\ ,\ g_{i+1}(x)\ )$ est 1.

□

Lemme 2 : (notations du début de la preuve du théorème 1)

(i) f_0 a pour racines les racines de P non racines de Q,

(ii) $V(f ; x) = V_{Stu}(P,Q ; x)$ pour x non zéro de P,

(iii) le nombre $V(f ; x)$ 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 $V(f ; x)$ ne change pas quand on passe à droite d'une racine de f_i $(i = 1,...,n)$ non racine de f_0.

démonstration du lemme 2:

(i) et (ii) sont immédiats d'après la définition de **f**.

Reformulons plus précisément (iii) et (iv) :

(iii') Soit c une racine de f_0 et a_1 et b_1 des éléments de **R** tels que

(1) $a_1 < c < b_1$

(2) aucun f_i $(i = 0,...,n-1)$ ne s'annule sur $]a_1,c[$ ni sur $]c,b_1[$.

Alors, pour tout x de $]a_1,c[$ et pour tout y de $]c,b_1[$ la différence entre $V(f ; x)$ et $V(f ; y)$ est -1 si Q(c) est positif et 1 si Q(c) est négatif.

(iv') Soit c une racine de f_i non racine de f_0 et a_1 et b_1 des éléments de **R** tels que

(1) $a_1 < c < b_1$

(2) aucun f_i $(i = 0,...,n-1)$ ne s'annule sur $]a_1,c[$ ni sur $]c,b_1[$.

Alors, pour tout x de $]a_1,c[$ et pour tout y de $]c,b_1[$, $V(f ; x)$ et $V(f ; y)$ sont égaux.

Démontrons (iii'):

Soient c avec $f_0(c) = 0$, a_1 et b_1 des éléments de **R** tels que

(1) $a_1 < c < b_1$

(2) aucun f_i $(i = 0,...,n)$ ne s'annule sur $]a_1,c[$ ni sur $]c,b_1[$.

Soient x un élément de $]a_1,c[$ et y un élément de $]c,b_1[$.

Si c est aussi racine d'un f_i, $i \in \{1,...,n-1\}$, le nombre de changements de signes dans la suite $(f_{i-1}(x), f_i(x), f_{i+1}(x))$ et dans la suite $(f_{i-1}(y), f_i(y), f_{i+1}(y))$ est 1 d'après le lemme 1 appliqué à P et R.

Que c soit ou non racine d'un f_i, $i \in \{1,...,n-1\}$, le nombre de changements de signes dans la suite $(f_i(x))_{i \in \{1,...,n-1\}}$ coincide donc avec le nombre de changements de signes dans la suite $(f_i(y))_{i \in \{1,...,n-1\}}$.

Regardons maintenant ce qui se passse pour f_0 et f_1.

Soit k la multiplicité de c dans P, d'après (i) c est racine dans **R** d'ordre k−1 de P'Q. $\mathbf{Stu}^n(P,Q)$ qui est le PGCD de P et P'Q est donc égal $(x-c)^{k-1}$ h avec $h(c) \neq 0$. Si $P = (x-c)^k P_1$, avec $P_1(c) \neq 0$, on a $f_0 = (x-c) P_1 / h$ et $f_1 = R_1 / h$ où R_1 est le reste de la division de $(k.P_1 + (x-c).P'_1).Q$ par $(x-c).P_1$.

Soit ε le signe de P_1 / h en c. Le signe de R_1 en c coincide avec le signe de

$n.P_1(c).Q(c)$, donc le signe de f_1 en c est le signe de $\varepsilon.Q(c)$.

Le polynôme f_1 est non nul en c et ne s'annule pas sur $]\, a_1,c\,[$ ni sur $]\, c,b_1\,[$, il a donc sur tout $]\, a_1,b_1\,[$ le même signe qu'en c , à savoir ε si $Q(c) > 0$ et $-\varepsilon$ si $Q(c) < 0$.

Si $Q(c) > 0$, alors sur $]\, a_1,c\,[$, f_0 et f_1 sont de signes opposés, et sur $]\, c,b_1\,[$, f_0 et f_1 sont de mêmes signes.

Si $Q(c) < 0$, alors sur $]\, a_1,c\,[$, f_0 et f_1 sont de mêmes signes, et sur $]\, c,b_1\,[$, f_0 et f_1 sont de signes opposés.

On en déduit la propriété (iii') annoncée.

Démontrons maintenant (iv') : Si $f_0(c)$ est non nul, on a immédiatement la propriété (iv') à partir du lemme 1 appliqué à P et R . ❑

démonstration du théorème:

(i) Il suffit de mettre bout à bout les lemmes 1 et 2 .

(ii) est un cas particulier de (i). ❑

Corollaire 1 (théorème de Sturm [Stu]) :

Si a et b ne sont pas racines de P , $V_{Stu}(P;a,b)$ est le nombre de racines dans **R** de P entre a et b .

En particulier $V_{Stu}(P)$ est le nombre de racines dans **R** de P .

démonstration du corollaire 1:

On applique le théorème à P et à 1. ❑

Corollaire 2:

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

démonstration du corollaire 2 :

On applique le théorème à P et à Q^2. ❑

Corollaire 3 On a donc les égalités :

$$V_{Stu}(P;a,b) = c_0(P,Q;a,b) + c_+(P,Q;a,b) + c_-(P,Q;a,b),$$
$$V_{Stu}(P,Q^2;a,b) = c_+(P,Q;a,b) + c_-(P,Q;a,b),$$
$$V_{Stu}(P,Q;a,b) = c_+(P,Q;a,b) - c_-(P,Q;a,b)$$

qui permettent de calculer $c_0(P,Q;a,b)$, $c_+(P,Q;a,b)$ et $c_-(P,Q;a,b)$ connaissant $V_{Stu}(P;a,b)$, $V_{Stu}(P,Q^2;a,b)$ et $V_{Stu}(P,Q;a,b)$.

Remarque 2 :

Dans l'article [Syl] , Sylvester étudie le nombre $V_{Rss}(P, S)$ 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'entrecroisements entre les racines de P et celles de S . Nous pouvons donner

l'interprétation suivante pour le nombre $V_{Rss}(P,S ; a,b)$: on suppose que $P(a).P(b) \neq 0$, on ne tient compte que des racines α de P sur l'intervalle dont l'ordre est supérieur d'un nombre impair à leur ordre en tant que racine de S ; en outre on compte cette racine avec le coefficient +1 ou −1 selon que P'S est ≥ 0 ou ≤ 0 au voisinage de la racine. Lorsque P n'a que des racines simples, cela revient à affecter à chaque racine de P un coefficient égal au signe de P'S . 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 $V_{Stu}(P,Q;a,b)$ 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 de Sylvester 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** (ceci résulte par exemple des résultats de [CoR]).

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 $A = \mathbb{Z}[Y]$ et $A' = \mathbb{Z}[\xi]$ 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 apparait 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 coincident 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 § 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 au § 3 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 ,

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

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

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

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

$$\mathbf{Stu}^2(P) = -\ (1/4)\ (\ 2pX^2 + 3qX + 4r)$$

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

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

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 subsituant 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 obtenur la suite de Sturm de P .

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

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

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

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

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

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 [Loo]. Nous serons cependant en désaccord avec lui sur certains points de détail. Pour la théorie des sous-résultants voir également [Br], [BroT], [Col] et [Hab]. Pour l'expression des sous-résultants en fonction des racines (point que nous n'abordons pas) voir [Syl], [Bor], [Las], [Cha].

a) Définitions

Nous rappelons dans ce § 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 $d(P) \leq p$, $d(S) \leq s$ et $j < \inf(p,s)$, nous notons $\mathbf{Sylv_j}(P,p,S,s)$ la j-ème 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 $P = a_p X^p + a_{p-1} X^{p-1} + \ldots + a_0$, $S = b_s X^s + b_{s-1} X^{s-1} + \ldots + b_0$, (avec éventuellement les premiers coefficients de P et S nuls), $\mathbf{Sylv_j}(P,p,S,s)$ est la matrice

$$
\begin{array}{cccccccccccccc}
a_p & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a_0 & 0 & \cdot & \cdot & 0 \\
0 & a_p & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a_0 & 0 & \cdot & 0 \\
 & & & & & & & & & & & & & \\
0 & \cdot & \cdot & 0 & a_p & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a_0 & 0 \\
0 & \cdot & \cdot & \cdot & 0 & a_p & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a_0 \\
b_s & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b_0 & 0 & \cdot & \cdot & \cdot & 0 \\
0 & b_s & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b_0 & 0 & \cdot & \cdot & 0 \\
0 & 0 & b_s & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b_0 & 0 & \cdot & 0 \\
 & & & & & & & & & & & & & \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & \cdot & \cdot & \cdot & 0 & b_s & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b_0 & 0 \\
0 & \cdot & \cdot & \cdot & \cdot & 0 & b_s & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b_0
\end{array}
$$

s-j lignes de P

p-j lignes de S

p+s-j colonnes

Par définition, le **déterminant polynomial d'une matrice** possédant N lignes et M colonnes, avec $M \geq N$ 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 (considérés 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.-à-d. 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 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.

---

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

Proposition 1 :

Nous supposons $d(P) \leq p$, $d(S) \leq s$, $j < \inf(p,s)$

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

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

c) Si $s' \geq s$ 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:

a) la première colonne de $\mathbf{Sylv}_j(P,p,\ S,s)$ est nulle.

b) cela revient à calculer le signe d'une permutation.

c) (i) la nouvelle matrice est obtenue à partir de l'ancienne en rajoutant $s'-s$ colonnes nulles à gauche, puis $s'-s$ lignes au dessus, chacune portant le polynôme P décalé à chaque fois d'un cran. Les déterminants intervenant dans le calculs des $\mathbf{Sres}_j$ sont donc tous multipliés par $cd(P)^{s'-s}$.

c) (ii) on applique c) (i) et 2 fois b). ❑

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 $s \geq d(S)$.

Proposition 2 :

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

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

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

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

démonstration:

a) et b) : observer le dessin de la matrice $\mathbf{Sylv}_j(P,p,\ S,p-1)$

c) c'est la proposition 1c. ❑

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

Nous établissons dans ce § 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 $p = d(P) \geq s = d(S)$, le polynôme $cd(S)^{p-s+1}.\mathbf{Rst}(P,S)$ est appelé le **pseudo-reste** de la division de P par S, et nous le noterons **Prst(P,S)** . Le pseudo-reste est donc proportionel (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 § nous noterons (H) l'hypothèse suivante :

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

Nous commençons par une proposition qui sert de base aux calculs qui suivent[1]:

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 :

(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 $\mathbf{Sylv}_j(R,p,S,s)$.

(ii) même démonstration ❑

Proposition 4 : Lorsque $p = d(P) \geq s = d(S)$, 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 $p' \geq p$ 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:

(i) on applique la proposition 3 (ii) avec $j = s-1$, la matrice $\mathbf{Sylv}_{s-1}(S,s,R,p)$ obtenue est surtriangulaire, on développe les déterminants suivant la diagonale :

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

---

[1] En fait, tous les résultats des § b et c sont basés sur l'utilisation systématique des propositions 1 , 2 , 3 et 4 , qui sont toutes très élémentaires

(ii) on applique la proposition 2 c) avec $j = s-1$:

$\mathbf{Sres}_{s-1}(P,p, S,p-1) = cd(P)^{p-s-1}\ \mathbf{Sres}_{s-1}(P,p, S,s)$ et on remarque que :

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

(la première égalité par (i) , la deuxième en appliquant proposition 1 b) .

(iii) la première égalité résulte de 1) c (i), la deuxième du (i) ci-dessus, et la dernière de la défintion du pseudo-reste. ❑

Le cas ordinaire

C'est le cas où les degrés dans la suite des restes baissent 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 $j < s-1$

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:

$\mathbf{Sres}_j(P,p, S,s) = (c(s).c(s-1)...c(j+1))^2\ \mathbf{Rst}_j(P,S)$ 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 5a est un cas particulier de la proposition 4 (i) . La proposition 5b s'obtient en appliquant la proposition 3 puis les propositions 1b et 1c(i) . ❑

Le théorème de Habicht

Nous redémontrons maintenant le "théorème de Habicht" dans [Loo] par un calcul direct.

Théorème 2 (**théorème de Habicht** [Hab]) :

Nous supposons $d(P) \le p = s+1$, $d(S) \le s$.

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

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

(i) Alors, pour $0 \le h < j \le s$, 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 $d(S_j) = j \le s$, on obtient:

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

démonstration:[1]

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

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

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

et $S_h = \gamma(h).R_h$ ❑

Le cas défectueux

Proposition 7 : Supposons (H) . On a:

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

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

b) On en déduit

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

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

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

démonstration :

a) (i) en effet: $\mathbf{Sres}_{s-1}(S,s,\ P,p) = \mathbf{Prst}\ (P,S)$ (proposition 4 (i)) et
$\mathbf{Sres}_{s-1}(P,p,\ S,s) = (-1)^{p-s+1}\ \mathbf{Sres}_{s-1}(S,s,\ P,p)$ (prop 1b)

a) (ii) on a
$$\begin{aligned}\mathbf{Sres}_j(P,p,\ S,s) &= \mathbf{Sres}_j(R,p,\ S,s) && \text{(prop 3)}\\ &= (-1)^{(p-j)(s-j)}\ \mathbf{Sres}_j(S,s,\ R,p) && \text{(prop 1b)}\\ &= (-1)^{(p-j)(s-j)}\ \mathrm{cd}(S)^{p-s+1}\ \mathbf{Sres}_j(S,s,\ R,s-1) && \text{(prop 1c (i))}\end{aligned}$$

b) (i) on applique a) (ii) puis la proposition 2 a) à $\mathbf{Sres}_j(S,s,\ R,s-1)$

b) (ii) si $r = s-1$, c'est trivial. Sinon a) (ii) donne

$$\begin{aligned}\mathbf{Sres}_r(P,p,\ S,s) &= (-1)^{(s-r)(p-s+1)}\ \mathrm{cd}(S)^{p-s+1}\ \mathbf{Sres}_r(S,s,\ R,s-1)\\ &= (-1)^{(s-r)(p-s+1)}\ \mathrm{cd}(S)^{p-s+1}\ (\mathrm{cd}(R)\ \mathrm{cd}(S))^{s-r-1}\ R \quad \text{(prop 2 b)}\end{aligned}$$

enfin a) (i) donne

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

---

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

b) (iii) si $r = s - 1$ c'est simplement a) (ii), sinon on applique a) (ii) et

$\mathbf{Sres}_j(S,s, R,s-1) = (cd(S))^{s-r-1}\ \mathbf{Sres}_j(S,s, R,r)$ (prop 2 c) ❑

Proposition 8 :

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

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

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

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

où $\varepsilon_i = 1$ si $\Sigma_{0\le k\le i}(1+ d_k - d_i).e_k$ 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 recurrence fonctionne grâce à b) (iii). ❑

Sous-résultants et restes

Théorème 3 (sous-résultants et restes [Hab] [Loo]):

a) Supposons (H) . Soit $j < s$. Le polynôme $\mathbf{Sres}_j(P,p,S,s)$ est égal , à un facteur non nul près dans **K** , à $\mathbf{Rst}_j(P,S)$ [1].

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

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 $j < \inf(d(P),d(S))$. Par ailleurs, si $d(P) = p > s > j \ge d(S)$, on a

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

$= 0$ si $d(S) < j < p - 1$ (prop 2 a)

$(cd(P)\ cd(S))^{p-s-1}\ S$ si $j=d(S)$ (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.-à-d. $\mathbf{Sres}_{s-1}(P,p, S,s) \neq 0$) . Alors le dernier sous-résultant non nul $\mathbf{Sres}_n(P,p,S,s)$ est de degré n (c.-à-d.: non défectueux). Il est égal au PGCD de P et S dans **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 . ❑

---

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

Le théorème des sous-résultants

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

Théorème 4 (théorème des sous-résultants [Hab], [Loo]) :

Nous supposons $d(P) \leq p = s+1$, $d(S) \leq s$, l'une des 2 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) $\quad cd(S_j)^{(j-k)}\, S_j = cd(S_{j+1})^{(j-k)}\, S_k$.

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

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

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 th 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 prop 2b : $\mathbf{Sres}_k(S_{j+1}, j+1, S_j, j) = (cd(S_j).cd(S_{j+1}))^{j-k}\, S_j$

b) (iii) le th 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 prop 2 a) . ❑

c) Spécialisation des polynômes sous-résultants

Nous venons de voir que la suite des sous-résultants nous donne la suite des restes. Etant donnée une spécialisation (i.e. un homomorphisme d'anneaux) $Sp: A \to A'$, 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 $A[X]$). 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.

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.

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

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

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

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

3ème 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 $Sp(a) = 0$. Plus précisément nous écrivons:

$P = a.c_p\, X^p + a_{p-1}\, X^{p-1} + \ldots$, $S = a.d_s\, X^s + b_{s-1}\, X^{s-1} + \ldots$ et nous supposons que le déterminant $\boxed{d = c_p\, b_{s-1} - d_s\, a_{p-1}}$ se spécialise non nul.

Cette situation se rencontre notamment dans l'important cas particulier où S est égal à la dérivée de P et où $d(Sp(P)) = d(P) - 1$.

Proposition 9 : Avec les hypothèses ci-dessus, et $p \geq s$

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

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

pour $j < s-1$

démonstration:

Nous notons P_1 et S_1 les polynômes P et S tronqués de leur coefficient dominant. On a évidemment $Sp(P) = Sp(P_1)$ et $Sp(S) = Sp(S_1)$. Nous posons $P_2 := c_p.X^p + P_1$, $S_2 := d_s.X^s + S_1$. Le polynôme $\mathbf{Sres}_j(P,p,S,s)/a$ est le déterminant polynomial de la matrice M_j dont les vecteurs lignes successifs sont $P_2.X^{s-j-1}$, $P.X^{s-j-2}$,..., P.X, P, $S_2.X^{p-j-1}$, $S.X^{p-j-2}$,..., S.X, S.

cas j= s-1 : Après spécialisation la matrice M_j est de la forme:

$Sp(c_p)$ $Sp(a_{p-1})$ $Sp(d_s)$ $Sp(b_{s-1})$	
0	matrice surtriangulaire dont les vecteurs lignes sont des polynômes $X^i S_1$

D'où le résultat a)

cas j < s-1 : Si on regroupe en haut les deux lignes portant $P_2.X^{q-j-1}$ et $S_2.X^{p-j-1}$, et si on spécialise, on obtient une matrice de la forme

$Sp(c_p)$ $Sp(a_{p-1})$ $Sp(d_s)$ $Sp(b_{s-1})$	
0	$\mathbf{Sylv_j(Sp(P_1),p-1,Sp(S_1),s-1)}$

D'où le résultat 9b) si on tient compte de la parité de la permutation de lignes effectuée.❑

4ème 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 Sp(S), P_p:= P tronqué au dessus du degré de 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: [1]

Nous supposons $d(P) = p = n+1$, $d(S) = s \leq n$.

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 $\quad (0 \leq j \leq s)$

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 : {$1 \leq j \leq s-1$, 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 $h < k < j$: $\quad S_k := 0$ (7)
- $j := h-1$

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

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

démonstration:

(0) par la proposition 4 (i)

(1) par la proposition 2 b)

(2) par la proposition 4 (ii)

(3) par la proposition 2 a)

(4) par le théorème de Habicht puisque $cd(S_{j+1}) = \mathbf{cf}_{j+1}(S_{j+1})$

(5) (6) (7) par le théorème 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)

---

[1] 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 [Loo] 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 $n = p-1 \geq s$, il est par contre incorrect lorsque $p \leq s$. (Cf la 3ème note bas de page au sujet de l'algorithme n°3 : ici c'est la note 1 page 25)

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) ≤ 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 ≤ n.

Nous posons $S_p := P$, $S_n := S$, $S_s := cd(S)^{n-s} S$, $S_j := \mathbf{Sres}_j(P,p,S,s)$ pour j < s. **entrées** : les polynômes P et S

sortie : la suite des sous-résultants standards S_j (0 ≤ j ≤ s)

initialisation :

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

étape suivante et **fin** : comme dans l'algorithme n°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 ≥ d(P) , s = d(S) et p > s, on pose:

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

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

$\mathbf{Sres}_k(P,p,S,s) := 0$ si s < k < p-1 ,

$\mathbf{sr}_p(P,p,S,s) := 1$, $\mathbf{sr}_j(P,p,S,s) := \mathbf{cf}_j(\mathbf{Sres}_j(P,p,S,s))$ si 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 $p < j = s - 1 < s < s'$ [1]

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

Algorithme 3 : Algorithme généralisé des polynômes sous-résultants [2]

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

Nous posons pour $j \leq p$: $S_j := \mathbf{Sres}_j(P,p,S,s)$, $t_j := \mathbf{sr}_j(P,p,S,s)$

entrées : les polynômes P et S , l'entier $p \geq d(P)$

sortie : la suite des polynômes sous-résultants S_j $(0 \leq j \leq p)$

initialisation :

– $S_p := P$; $t_p := 1$

– $S_{p-1} := S$

– $j := p - 1$

étape suivante : { $1 \leq j \leq n$, 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 $h = j$ $S_{h-1} := \mathbf{Sres}_{h-1}(S_j, h, S_{j+1}, j+1) / t_{j+1}^2$; (4)

– si $h < j$ $S_h := S_j . \mathbf{cf}_h(S_j)^{j-h} / t_{j+1}^{j-h}$; (5) (*)

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

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

– $j := h - 1$; $t_{j+1} := \mathbf{cf}_{j+1}(S_{j+1})$ [3]

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

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

---

[1] Ainsi la convention concernant $\mathbf{Sres}_s(P,p,S,s)$ pour $s = d(S) < p$ tient correctement la route par rapport aux égalités générales données dans la prop 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 $\mathbf{Sres}_p(P,p,S,s)$.

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

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

N B : 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[1] 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 $p > s = d(S)$, $p \geq d(P)$, 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: $\mathbf{Sres}_{h-1}(S_j,h, S_{j+1},j+1) = \mathbf{cf}_h(S_j)^{j-h+2}\,\mathbf{Rst}(S_{j+1},S_j)$

démonstration:
Tout d'abord, si $p = d(P) > s = d(S)$, il s'agit d'une simple reformulation de l'algorithme précédent, tenu compte de la définition-convention. Ensuite on remarque que l'algorithme écrit sous cette forme généralisée peut être vu comme une suite d'identités algébriques sous conditions (les conditions sont celles qui forcent les égalités $d(S_j) = h$, c'est-à-dire l'annulation de certains déterminants extraits de la matrice $\mathbf{Sylv}_0(P,p, S,s)$). Il est donc encore valable si $d(P) < p$ (le coefficient dominant de P n'intervient pas dans l'algorithme). ❑

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 $d(S) = d(P)$)

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 $\quad (0 \leq j < s)$

initialisation :

- $S_{s-1} := \mathbf{Prst}\,(S,P)$, $t := d(S_{s-1})$ (1)
- si $t = s-1$ $S_{s-2} := \mathbf{Prst}\,(P, S_{s-1}) / cd(P)$ (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 n°1

---

[1] Dans le Subresultant Theorem et le Subresultant Chain Algorithm de [Loo] , c'est toujours $\mathbf{Prst}(S_{j+1},S_j)$ qui intervient. Or ce polynôme n'est défini que pour $d(S_{j+1}) \geq d(S_j)$. 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 [Loo] de définition explicite des $\mathbf{Sres}_j(P,n+1, S,s)$ lorsque $n > j \geq s$

démonstration:

On pose pour $j < s$: $\Sigma_j := \mathbf{Sres}_j(S,s+1, P,s)$. Par la proposition 1 on obtient : $\Sigma_j = cd(P).S_j$.

(1) par la proposition 4

(2) par le théorème de Habicht on a: $\Sigma_{s-2} = \mathbf{Prst}\,(P,\Sigma_{s-1})/cd(P)^2$.

Par ailleurs $\mathbf{Prst}\,(P,S_{s-1}) = \mathbf{Prst}\,(P,\Sigma_{s-1})/cd(P)^2$ parce que $S_{s-1} = \Sigma_{s-1}/cd(P)$

(1 bis) On remplace dans le théorème de Habicht j par s-1 et r par t , on obtient:

$$cd(P)^{2(s-1-t)} . \Sigma_t = \mathbf{Sres}_t(P,s, \Sigma_{s-1},s-1).$$

Par ailleurs $\mathbf{Sres}_t(P,s, \Sigma_{s-1},s-1) = \mathbf{Sres}_t(P,s, S_{s-1},s-1).cd(P)^{s-t}$ (il y a s-t lignes "portant S_{s-1}" dans la matrice correspondante). La proposition 2b donne de plus:

$$\mathbf{Sres}_t(P,s, S_{s-1},s-1) = (cd(P).cd(S_{s-1}))^{s-1-t}. S_{s-1} .$$

Fin du calcul: élémentaire.

(2 bis) Par le théorème de Habicht on a: $cd(P)^{2(s-t)} . \Sigma_{t-1} = \mathbf{Sres}_{t-1}(P,s, \Sigma_{s-1},s-1)$

Par ailleurs $\mathbf{Sres}_{t-1}(P,s, \Sigma_{s-1},s-1) = \mathbf{Sres}_{t-1}(P,s, S_{s-1},s-1).cd(P)^{s-t+1}$ (même argument que ci-dessus). La proposition 2d donne de plus:

$$\mathbf{Sres}_{t-1}(P,s, S_{s-1},s-1) = (-cd(P))^{s-t-1}\,\mathbf{Prst}\,(P, S_{s-1}) .$$ Fin du calcul: élémentaire.

(4) , (5) , (6), (7) : vu le caractère homogène de ces formules, elles se déduisent des formules analogues pour les Σ_j , obtenues par l'algorithme généralisé des sous-résultants standards. ❑

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

Algorithme n°5 :

(cas $d(S) < d(P)$, cd(P) et cd(S) divisibles par un même élément c)

Nous supposons $d(P) = p = n+1$, $d(S) = s \le n$, 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 ($0 \le j \le n-1$)

initialisation :

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

- $S_s := \chi^{n-s} . c^{n-s-1} . S$ (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)

2ème cas : d(S) + 1 = d(P) (c.-à-d. p = s+1)

- $S_s := S$
- $S_{s-1} := \mathbf{Prst}(P,S) / c$ (1)
- $t := d(S_{s-1})$
- si $t = s-1$ $S_{s-2} := \mathbf{Prst}(S, S_{s-1}) / (c.\chi^2)$ (2)
- si $t < s-1$ on calcule S_t et S_{t-1} comme suit

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

  $S_{t-1} := (-1)^{p-t} . \mathbf{Prst}(S, S_{s-1}) / (c.\chi^{p-t})$ (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 n°1

démonstration :

On pose pour $j < s$: $\Sigma_j := \mathbf{Sres}_j(P,p,S,s)$. On a $\Sigma_j = c.S_j$ pour $j < p-1$. On regarde comment se modifie l'algorithme n°2 lorsqu'il traite les S_j au lieu des Σ_j, ce qui donne l'initialisation. Dès qu'on a obtenu S_{j+1} de degré $j+1 < p-1$ et S_j on peut se brancher sur "étape suivante" en raison du caractère homogène des formules. ❑

Comparaison des différents algorithmes proposés

Les algorithmes n°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 n°3 avec $p = d(P) > s = d(S)$ peut remplacer le n°2 (il effectue exactement les mêmes calculs) et est plus facile à écrire. L'algorithme n°5 est une amélioration de l'algorithme n°2, pour les deux raisons suivantes : primo, si le facteur c qu'on connait 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 n°5 peut s'avérer utile tandis que celle calculée par l'algorithme n°2 serait inutilisable (cf la proposition 9)

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

L'algorithme n°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 5 § 3 a par exemple) reposer sur la correction de cet algorithme n°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 $A = \mathbb{Z}$ ou $A = \mathbb{Z}[X_1, ..., X_n]$),

– 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 [Lom]).

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 $A = \mathbb{Z}$ ou $A = \mathbb{Z}[X_1, ..., X_k]$ d'après l'inégalité d'Hadamard ([Mig]). Supposons enfin que ces déterminants se calculent en temps polynomial en m : c'est le cas pour les anneaux $A = \mathbb{Z}$ ou $A = \mathbb{Z}[X_1, ..., X_k]$ d'après la complexité des opérations arithmétiques dans ces aneaux et la méthode du pivot améliorée à la Bareiss[1] ([Bar] ou [Loo] ou [Ait]). Alors il est clair d'après la définition des polynômes sous-résultants comme déterminants polynomiaux que ceux-ci sont calculables en temps polynomial.

---

[1] En fait l'algorithme de Bareiss remonte au moins à [Ait] 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 2 déterminants extraits de la matrice de départ. Dans [Gan] 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 ([Ait]) signale "en passant" comment obtenir une triangulation entièrement dans $\mathbb{Z}$ en utilisant des divisions exactes (produit en croix divisé par le pivot précédent) ... cad par la méthode de Bareiss.

Si n est une borne sur les degrés de P et S le nombre d'opérations arithmétiques sur $A = \mathbb{Z}$ ou $A = \mathbb{Z}[X_1, ..., X_k]$ 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 arithmétriques sur 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 A est alors en $O(n^2)$, les tailles des éléments de A à considérer étant de même nature dans les deux calculs[1]. Par exemple si $A = \mathbb{Z}$ 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.

---

[1] 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 [Lom]) . C'est néanmoins en $O(n^3)$ opérations élémentaires (additions, multiplications, divisions exactes dans A) , donc plus coûteux que les algorithmes à la Habicht .

3) Suite de Sturm-Habicht et spécialisation

a) 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 **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]) . 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

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

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

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

Supposons que **K** est muni d'un ordre ≤ et soit **R** sa clôture réelle pour cet ordre.

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

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

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 2 définitions qui suivent :

Définition:

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

- on extrait tout d'abord la suite $[g_0,g_1,...,g_m] = [f_{j0},f_{j1},...,f_{jm}]$ formée des polynômes non identiquement nuls
- on compte ensuite le nombre de changements de signes dans la suite $[g_0(a),g_1(a),...,g_m(a)]$ *en adoptant les conventions suivantes concernant les 0 :*
  - * comptent pour 1 changement de signe les segments suivants
    $-,0,+$ ou $+,0,-$ ou $+,0,0,-$ ou $-,0,0,+$
  - * comptent pour 2 changements de signe les segments suivants
    $+,0,0,+$ ou $-,0,0,-$

Le nombre $V'(f_0,f_1,...,f_n ; a)$ 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 $f_0,f_1,...,f_n$ 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 **K** un corps ordonné, P et S des polynômes de **K[X]** ,
a et $b \in K \cup \{+\infty\} \cup \{-\infty\}$, non racines du pgecd de P et S , on définit

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

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

Théorème 5 ([Hab])

En tous points a et b de **R** non racines du pgcd de P et S on a l'égalité :

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

démonstration :

Le théorème 5 est une conséquence immédiate du lemme suivant :

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

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

La preuve du lemme 1 utilise le lemme 2 suivant :

Lemme 2 :

Si $v \geq j = d(Rss_j(P,S) > 0$, alors

$$\frac{Ha_{j-1}(P,S)}{Rss_{j-1}(P,S)} \cdot \frac{Ha_j(P,S)}{Rss_j(P,S)}$$ est un carré dans **K** .

Notations: $t = \sup(d(P)\ ,\ d(S)+1)$, $q = d(S)$, $T_j = Sres_j(P,t,S,q)$, $R_j = Rst_j(P,S)$, $Rss_j = Rss_j(P,S)$, $Ha_j = Ha_j(P,S)$, $T_j / R_j = r_j$.

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

Si $j = t$ ou est le degré d'un reste Rss^m , alors Rss_j et Rss_{j-1} sont deux polynômes successifs dans la suite des restes signés (les Rss^m). Par ailleurs, tout polynôme non identiquement nul dans la suite de Habicht est de la forme Ha_j ou Ha_{j-1} avec j comme ci-avant. D'après le lemme 2, en un point a où tous les $Rss_j(P,S)(a)$ sont non nuls, il y a changement de signe entre Rss_j et Rss_{j-1} si et seulement si il y a changement de signe entre Ha_j et Ha_{j-1} . Dans la suite de Habicht, s'ajoutent d'éventuels changements de signes entre Ha_{j-1} et Ha_h si $h = d(Ha_{j-1}) < j-1$: mais les deux polynômes étant proportionnels, ce changement de signe "supplémentaire" éventuel a lieu indépendamment du point a où sont évalués les polynômes. *Ceci démontre le lemme 1 dans le cas où tous les* $Rss^j(P,S)(a)$ *sont non nuls.*

Voyons maintenant le cas où l'un des polynômes, non défectueux dans la suite de Habicht, s'annule en a : par exemple $d(Ha_j) = j$, $d(Ha_{j-1}) = j-1$, et $Ha_{j-1}(a) = 0$. On sait alors que $Rss_j(a).Rss_{j-2}(a) < 0$, 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 $V_{Rss}(P,S,a) = V_{Rss}(P,S,a')$ et tous les $Rss^j(P,S)(a')$ sont non nuls .

En appliquant deux fois le lemme 2 on voit que $\frac{Ha_{j-2}}{Rss_{j-2}} \cdot \frac{Ha_j}{Rss_j}$ est un carré dans **K** , et on obtient donc également un changement de signe dans la suite de Habicht. Et pour a' suffisamment proche de a , on a $V_{Ha}(P,S,a) = V_{Ha}(P,S,a')$.

Donc $V_{Ha}(P,S,a) = V_{Rss}(P,S,a) + c$ avec la même valeur 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 Ha_{j+1} non défectueux (de degré j+1), Ha_j défectueux de degré $h < j$ et tel que $Ha_j(a) = 0$. D'après le lemme 2

$\frac{Ha_j}{Rss_j} \cdot \frac{Ha_{j+1}}{Rss_{j+1}}$ est un carré dans K et

$\frac{Ha_h}{Rss_h} \cdot \frac{Ha_{h-1}}{Rss_{h-1}}$ est un carré dans K.

Ceci signifie que les polynômes $Ha_{j+1} \cdot Ha_j \cdot Ha_h \cdot Ha_{h-1}$ et $Rss_{j+1} \cdot Rss_j \cdot Rss_h \cdot Rss_{h-1}$ sont de même signe en tout point a' non racine de Ha_j. Or $Rss_j = Rss_h$, et Rss_{j+1} et Rss_{h-1} sont de signe opposé en a. Si on considère donc un point a' non racine de 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 $Ha_{j+1} \cdot Ha_j \cdot Ha_h \cdot Ha_{h-1}$ est négatif en a' et le nombre des changements de signe dans la suite $Ha_{j+1}, Ha_j, Ha_h, Ha_{h-1}$ en a' vaut 2 si $Ha_{j+1} \cdot Ha_{h-1} > 0$, 1 si $Ha_{j+1} \cdot Ha_{h-1} < 0$.
On a donc $V'_{Ha}(P,S; a) = V'_{Ha}(P,S; a') = V_{Rss}(P,S; a')$ ❑

Voyons maintenant la preuve du lemme 2.
Lorsque $j = t$, le lemme 2 est trivial :

$$P = T_j = R_j = Rss_j = Ha_j \quad \text{et} \quad S = T_{j-1} = R_{j-1} = Rss_{j-1} = Ha_{j-1}.$$

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 $c_{j+1} := sr_{j+1}(P,t,S,q)$ et $c_j := cd(T_j)$, 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 $Rss_{j+1}, Rss_j = Rss_h$ et Rss_{h-1} sont 3 restes successifs on a :

$$(Rss_{j+1}/R_{j+1}).(Rss_j/R_j).(Rss_h/R_h).(Rss_{h-1}/R_{h-1}) = -1$$

Enfin, on a:

$$(Ha_{j+1}/T_{j+1}).(Ha_j/T_j).(Ha_h/T_h).(Ha_{h-1}/T_{h-1}) = (-1)^{j-h+1}$$

Ce qui montre le lemme 2 en h, h−1 s'il était vrai en j+1, j. ❑

Contre-exemple:

Avec V_{Ha} au lieu de V'_{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:

$$P = X^5 + 2X + 2$$
$$S = X^4 + 1$$

La suite de Habicht est alors

$Ha_5(P,S) = X^5 + 2X + 2$ $\quad Ha_4(P,S) = X^4 + 1$ $\quad Ha_3(P,S) = -X - 2$

$Ha_2(P,S) = 0$ $\quad Ha_1(P,S) = X + 2$ $\quad Ha_0(P,S) = 17$

et choisissons $a = -2$, $b = -1$. On a $V_{Ha}(P,S; -2, -1) = 2$.
Or la suite des restes signés est:

$Rss^0(P,S) = X^5 + 2X + 2$ $\quad Rss^1(P,S) = X^4 + 1$

$Rss^2(P,S) = -X - 2$ $\quad Rss^3(P,S) = -17$

et $V_{Rss}(P,S; -2, -1) = 0$.

b) Suite de Sturm-Habicht

Rappelons que nous avons défini au §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 telle que les variations de signes dans la suite de Sturm-Habicht donnent 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.

Définitions

Nous définissons la

suite de Sturm-Habicht de P et Q

en séparant différents cas :

Définition :

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

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

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

- *si* $cd(P) \neq 1$ (cas où P n'est pas unitaire)

  - *si* $q = d(Q) \geq 1$

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

et pour $j < p$

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

  - *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 $j < p-1$

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

Remarque 6 :

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 $q \geq 1$ 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 **K** est muni d'un ordre $\leq$ et si a et b sont deux éléments de $\mathbf{K} \cup \{+\infty\} \cup \{-\infty\}$ on note :

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

Soient **K** un corps ordonné, P et Q des polynômes de **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

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

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

démonstration : Si $Q = 1$ le résultat est trivial. Reste à voir avec $d(Q) = q \geq 1$.

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

On a $\mathbf{StHa}_j(P,Q) := (-1)^{\frac{(p-j)(p-j-1)}{2}} \mathbf{Sres}_j(P,p,R,p+q-1) / cd(P)$ pour $j \leq p-1$, 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 $j \leq p-1$ $\mathbf{StHa}_j(P,Q) = ((cd(P))^{q-1} \mathbf{Ha}_j(P,R)$, 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 ($2^{ème}$ 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 2 :

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).

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:

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

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

$\mathbf{StHa}_1(P) = -12\,q\,(3\,q\,X+4\,r)$
$\mathbf{StHa}_0(P) = 27\,q^4+256\,r^3$

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

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

Proposition 11 :

Soient P et Q deux polynômes à coeffients dans un anneau intègre A , avec P unitaire.

(i) Si $\mathbf{sth}_j(P,Q) \neq 0$, $\mathbf{sth}_{j-1}(P,Q) = \ldots = \mathbf{sth}_{j-h}(P,Q) = 0$, $\mathbf{sth}_{j-h-1}(P,Q) \neq 0$ 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 $j < p-1$, $k = p-j$:

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

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

démonstration:

(i) et (ii) Immédiat d'après le théorème 4 et la définition de la suite de Sturm-Habicht.

(iii) la deuxième égalité (ligne 2) résulte de la proposition 2 c). Par spécialisation P donne un polynôme unitaire de même degré et R donne le reste (dans la proposition 4 (iii) remplacer S et P par P et P'Q) ❑

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 5 s'avère donc fort utile: c'est le théorème 6 suivant.

Théorème 6 ([Hab]):

Soient P et Q deux polynômes quelconques à coefficients dans un corps ordonné K et a et b (avec a < b) des points de K non racines de P .

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

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

démonstration:

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

Le (ii) résulte du (i) puisque les points $+\infty$ et $-\infty$ sont toujours ordinaires.

Voyons le (i). D'après le théorème 5, on a le résultat suivant :

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

On conclut par la proposition 10 . ❑

Corollaire:

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

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

(ii) On a l'égalité $V_{\mathbf{StHa}}(P,Q) = c_+(P,Q) - c_-(P,Q)$.

démonstration:

Résulte des théorèmes 6 et 1. ❑

Algorithmes

Les $\mathbf{StHa}_j(P,Q)$ peuvent être calculés au moyen des algorithmes donnés au § 2 :

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 $d(Q) \geq 1$, la deuxième formule donnée dans la définition.

c) Spécialisation de la suite de Sturm-Habicht

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

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

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

Proposition 12 : (Notations ci-dessus) Supposons $p_1 = p$, $q \geq 1$.

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

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 Sp(P) et 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 :

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

démonstration:

Si P est unitaire ,

a) est donné par la prop 11 (iii), b) s'en déduit

Si P n'est pas unitaire

on remarque que théorème 6 se déduit de la proposition 10 et du théorème 5. Mais dans la proposition 10, la preuve utilise seulement $q \geq d(Q)$ et non pas $q = d(Q)$. ❑

2ème cas : $p_1 = p - 1$, $q_1 = q$:

On applique la proposition 9 .

Proposition 13 : Nous supposons $p_1 = p - 1$, $q_1 = q \geq 1$.

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

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

démonstration

On utilise la deuxième forme dans la définition de $\mathbf{StHa}_j(P,Q))$ et on remarque que le déterminant d de la proposition 9 se spécialise en $cd(P_1).cd(Q_1)$. ❑

Proposition 14 : Nous supposons $p_1 = p - 1$

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

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

démonstration

On remarque que le déterminant d de la proposition 9 se spécialise en $cd(P_1)$. ❑

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 la suite de Sturm-Habicht de Sp(P) et Sp(Q). (on prendra garde seulement à l'initialisation de la suite, à calculer directement).

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

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

P_p := "P tronqué au delà du degré d(Sp(P))",

Q_q := "Q tronqué au delà du degré d(Sp(Q))"

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

4) 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 tout le § 4 le polynôme P sera *unitaire* .

a) Méthode d'Hermite

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

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

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

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

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, ..., 2p − 2 la somme $\Sigma_{i=1,...,p}\, Q(\alpha_i)\, \alpha_i^k$ on a :

$$B(P,Q) = \Sigma_{k=0,...,p-1;j=0,...,p-1}\, s(P,Q)_{k+j}\, x_k\, x_j .$$

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

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

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_k la somme de Newton $\Sigma_{i=1,...,p}\, \alpha_i^k$ on a :

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

Si ≤ est un ordre sur **K** on note **R** la clôture réelle de **K** pour l'ordre ≤ . Rappelons qu'on note $c_+(P,Q)$ le nombre de racines de P dans **R** avec Q > 0 , $c_-(P,Q)$ le nombre de racines de P dans **R** avec Q < 0 , c(P) le nombre de racines de P dans **R** . La forme quadratique B(P,Q) a une signature dans le corps **R** (cette signature dépend du choix de l'ordre ≤ sur **K**). On prend alors pour corps **C** le

corps $\mathbf{R}[i]$ (avec $i^2 = -1$) . On appellera *racines réelles* celles qui sont dans $\mathbf{R}$ et *racines complexes* celles qui sont dans $\mathbf{C} - \mathbf{R}$.

Théorème 7 (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 $c_+(P,Q) - c_-(P,Q)$.

démonstration :

Notons $\beta_1,...,\beta_n$ les racines réelles (distinctes) de P , $\mu_1,...,\mu_n$ leurs multiplicités, γ_1 , $\overline{\gamma_1}$, .. , γ_m , $\overline{\gamma_m}$ les racines complexes (distinctes) de P , $\omega_1,...,\omega_m$ leurs multiplicités. Pour $\alpha \in \mathbf{C}$, soit ψ la forme linéaire sur $\mathbf{C}^n$ définie par :

$$\psi(\alpha,x) := x_0 + x_1\,\alpha + ... + x_{p-1}\,\alpha^{p-1} \ , \quad \text{et soit} \quad \varphi(\alpha,x) := \psi(\alpha,x)^2$$

La forme quadratique $B(P,Q)$ s'écrit donc comme

$$B(P,Q) = \Sigma_{j=1,..,n}\ \mu_j\ Q(\beta_j)\ \varphi(\beta_j,x) + \Sigma_{j=1,...,m}\ \omega_j\ (\ Q(\gamma_j)\ \varphi(\gamma_j,x) + Q(\overline{\gamma_j})\ \varphi(\overline{\gamma_j},x)\ )$$

Les formes linéaires $\psi(\beta_j,x)$, $\psi(\gamma_h,x)$, $\psi(\overline{\gamma_k},x)$ sont linéairement indépendantes (on a choisi les racines distinctes et il suffit de considérer un déterminant de van der Monde). Ceci donne (i).

En écrivant $Q(\gamma_j) = \delta_j^2$ et en décomposant $\delta_j\ \psi(\gamma_j,x)$ sous forme $P_j + i\ Q_j$ avec P_j et Q_j des formes linéaires réelles , il est clair que $Q(\gamma_j)\ \varphi(\gamma_j,x) + Q(\overline{\gamma_j})\ \varphi(\overline{\gamma_j},x)$ est une différence de carrés de formes linéaires réelles.

La signature de $B(P,Q)$ ne dépend alors que des n premiers termes de la somme et est donc égale à $c_+(P,Q) - c_-(P,Q)$. ❑

Corollaire:

Avec les notations précédentes, la signature de $B(P)$ est égale à $c(P)$. ❑

b) 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 $A = (s(P,Q)_{i+j-2})_{i=1,...,p;j=1,...,p}$ associée à la forme quadratique $B(P,Q)$.

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

---

[1] définition donnée au début du §c qui suit

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 : (*) $R/P = \Sigma_{i=1,...,p}\ Q(\alpha_i)/(X-\alpha_i)$.

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 $P = X^p + a_{p-1}X^{p-1} + ... + a_0$ et ceux de $R = c_{p-1}X^{p-1} + ... + c_0$ (c_{p-1} éventuellement nul), à savoir :

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

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

$s(P,Q)_2 + a_{p-1}\ s(P,Q)_1 + a_{p-2}\ s(P,Q)_0 = c_{p-3}$

...

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

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

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

Proposition 15:

Soient P et Q deux polynômes avec :

$P = X^p + a_{p-1}X^{p-1} + ... + a_0$

$Q = b_q X^q + b_{q-1}X^{q-1} + ... + b_0$

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

démonstration:

Notons $R = c_{p-1}X^{p-1} + ... + c_0$ le reste de la division euclidienne de P par P'Q.

D'après la définition de la suite de Sturm-Habicht et la proposition 11 (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 $\mathbf{sr}_{p-k}$.

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

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

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

$$\text{d'où} \quad sr_{p-k} = \begin{vmatrix} s'_{k-1} & \dots & s'_{2k-2} \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ s'_0 & s'_1 & \dots\ s'_{k-1} \end{vmatrix}$$

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

$$sr_{p-k} = (-1)^{k(k-1)/2}\, b(P,Q)_k \ . \qquad \square$$

c) Mineurs principaux et signature d'une forme quadratique

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

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

Proposition 16 (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 $(1, (\det(A_k))_{k=1,\dots,p})$.

Si des mineurs principaux de la matrice s'annnulent 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] tome I 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 $B = \Sigma_{k=0,\dots,p-1;l=0,\dots,p-1}\, c_{k+l}\, x_k\, x_l$. La matrice symétrique $A = [a_{i,j}]_{i=1,\dots,p;j=1,\dots,p}$ qui est associée à B est définie par $a_{i,j} = c_{i+j-2}$.

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

$\Pi(a_0) = 0$,

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

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

On a alors la relation suivante.

Remarque 7 :

Si les éléments de $(a_0,...,a_n)$ sont tous non nuls, alors on a

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

La différence $C(a_0,...,a_n)$ entre le nombre d'éléments positifs et le nombre d'éléments négatifs dans la suite $(a_0,...,a_n)$ est égale à $\Pi(a_0,...,a_n) - V(a_0,...,a_n)$ 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 $C(1 , (\det(A_k))_{k=1,...,p})$.

La proposition suivante indique comment se généralise le théorème de Jacobi.

On doit tout d'abord généraliser la définition du nombre $C(a_0,...,a_n)$ au cas d'une suite comportant des zéros.

Définition

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

- faisons apparaître les éléments nuls de $(a_0,...,a_n)$

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

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

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

  avec $\varepsilon_h = 0$ si $k(h)$ est impair

  $(-1)^{k(h)/2}$ signe$(a_{i(h)+k(h)+1} \cdot a_{i(h)})$ si $k(h)$ est pair .

Proposition 17

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

démonstration:
due à Frobenius [Fro] . Il semble difficile d'exposer ceci plus clairement que [Gan], tome 1, chapitre 10 . ❑

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

Proposition 18:

La signature $S_B(P,Q)$ de $B(P,Q)$ est égale à $C(1 , (b(P,Q)_k)_{k=1,...,p})$.

démonstration:
On utilise la proposition 17 et le fait que la matrice associée à $B(P,Q)$ est une matrice de Hankel. ❑

Remarque 8:
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). Ceci permet d'obtenir plus facilement la proposition 17 dans le cas particulier de $B(P,Q)$ (on n'a pas besoin du théorème 23 page 344 de [Gan]).

Théorème 8 (méthode des bezoutiens [Her], [Syl]):

La quantité $C(1 , (b(P,Q)_k)_{k=1,...,p})$ est égale à $c_+(P,Q) - c_-(P,Q)$.

démonstration:
On applique le théorème 7 et la proposition 18 . ❑

Remarque 9

1) Les calculs des $(b(P,Q)_k)_{k=1,...,p}$) se font dans l'anneau A . La quantité $C(1, (b(P,Q)_k)_{k=1,...,p})$ dépend évidemment du choix de l'ordre sur K .
2) Considérons maintenant un homomorphisme d'anneau Sp de A dans A' .
   Les $b(Sp(P),Sp(Q))_k$ sont les spécialisés des $b(P,Q)_k$
   Il faut recalculer $C(1, (b(Sp(P),Sp(Q))_k)_{k=1,...,p})$ en évaluant les signes des $b(Sp(P),Sp(Q))_k$ 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.

d) De la méthode de Sturm-Habicht à la méthode d'Hermite

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

Proposition 19 :

$V_{StHa}(P,Q)$ est égal à $C((sth_{p-k}(P,Q))_{k=0,...,p})$.

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

démonstration:

voyons d'abord le cas où P est unitaire

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

$V_{StHa}(P,Q; +\infty) = V(sth_{p-k}(P,Q)_{k=0,...,p})$

$V_{StHa}(P,Q; -\infty) = V((-1)^{p-k} sth_{p-k}(P,Q)_{k=0,...,p})$

$= \Pi(sth_{p-k}(P,Q)_{k=0,...,p})$ en utilisant la remarque 7,

d'où : $V_{StHa}(P,Q) = V_{StHa}(P,Q; -\infty) - V_{StHa}(P,Q; +\infty) = C(sth_{p-k}(P,Q)_{k=0,...,p})$.

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 $sth_{p-k}(P,Q)$ (k=0,...,p) que dans la suite de Sturm-Habicht.

Rappelons (proposition 11) que si

$sth_j(P,Q) \neq 0$, $sth_{j-1}(P,Q) = ... = sth_{j-h}(P,Q) = 0$, $sth_{j-h-1}(P,Q) \neq 0$

alors $StHa_j(P,Q)$ est de degré j , $StHa_{j-1}(P,Q)$ est défectueux de degré j-h-1 et tous les $StHa_k(P,Q)$, $j-h \leq k < j-1$, sont nuls.

Nous allons montrer, en notant $StHa_j(P,Q)$, $StHa_{j-1}(P,Q)$ et $StHa_{j-h-1}(P,Q)$ respectivement $StHa_j$, $StHa_{j-1}$ et $StHa_{j-h-1}$ que

$V((StHa_j,StHa_{j-1},StHa_{j-h-1}) ; -\infty) - V((StHa_j,StHa_{j-1},StHa_{j-h-1}) ; +\infty) = \varepsilon_h$

avec $\varepsilon_h = 0$ si h est impair,

$\varepsilon_h = (-1)^{h/2}$ signe($sth_j(P,Q)\, sth_{j-h-1}(P,Q)$) sinon .

D'après la proposition 11 nous avons, en notant c_{j-h-1} le coefficient dominant de $StHa_{j-1}$,

$sth_j(P,Q)^h\, StHa_{j-h-1} = (-1)^{h(h+1)/2} (c_{j-h-1})^h\, StHa_{j-1}$,

d'où $sth_j(P,Q)^h\, sth_{j-h-1}(P,Q) = (-1)^{h(h+1)/2} (c_{j-h-1})^{h+1}$ (***) .

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

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

$V(StHa_j, StHa_{j-1}, StHa_{j-h-1} ; -\infty) - V(StHa_j, StHa_{j-1}, StHa_{j-h-1} ; +\infty) = 0$

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

$V(StHa_j, StHa_{j-1}, StHa_{j-h-1} ; -\infty) - V(StHa_j, StHa_{j-1}, StHa_{j-h-1} ; +\infty) = 0$

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

$V(StHa_j, StHa_{j-1}, StHa_{j-h-1} ; -\infty) - V(StHa_j, StHa_{j-1}, StHa_{j-h-1} ; +\infty) = 1$

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

$V(StHa_j, StHa_{j-1}, StHa_{j-h-1} ; -\infty) - V(StHa_j, StHa_{j-1}, StHa_{j-h-1} ; +\infty) = -1$

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

On en déduit donc l'égalité annoncée.

Voyons maintenant le cas où P n'est pas unitaire

Soient c l'inverse du coefficient dominant de P , et $R = \mathbf{Rst}(P'Q,P)$.

On a $c\,R = \mathbf{Rst}((c\,P)'Q, c\,P)$.

Donc en prenant $A = K$ on a : $\mathbf{StHa}_j(c\,P, Q) = \mathbf{Ha}_j(c\,P, c\,R)$ (c P est unitaire).

Supposons tout d'abord $p-1-r$ pair :

$\mathbf{Ha}_j(c\,P, c\,R) = c^{p+r-2j}\,\mathbf{Ha}_j(P, R)$ et, par la proposition 10 a)

$\mathbf{StHa}_j(P, Q) / \mathbf{Ha}_j(P, R)$ est de signe constant

donc $\mathbf{StHa}_j(P, Q) / \mathbf{StHa}_j(c\,P, Q)$ est de signe constant

donc $\mathbf{V}_{\mathbf{StHa}}(P , Q) = \mathbf{V}_{\mathbf{StHa}}(c\,P, Q)$

(ce qui était d'ailleurs évident via les théorèmes 6 et 1 (ii))

et aussi $\mathbf{sth}_j(P, Q) / \mathbf{sth}_j(c\,P, Q)$ est de signe constant

donc $C((\mathbf{sth}_{p-k}(P,Q))_{k=0,\ldots,p}) = C((\mathbf{sth}_{p-k}(c\,P,Q))_{k=0,\ldots,p})$

on conclut en utilisant le résultat déjà obtenu puisque c P est unitaire.

Dans le cas $p-1-r$ impair, l'argument doit être légèrement modifié : le signe de $\mathbf{sth}_j(P, Q) / \mathbf{sth}_j(c\,P, Q)$ n'est sûrement constant à partir de $j = r$ (cf la preuve de la proposition 10) mais fort heureusement les 2 suites commencent par un coefficient non nul suivi d'un nombre impair de zéros, ce qui implique que le début de la suite n'intervient pas dans le compte du nombre $C(\ldots)$[1]. ❑

Théorème 9

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

démonstration:

mettre bout à bout les proposions 15 , 18 et 19 . ❑

e) Conclusions et remarques

Résumé des résultats obtenus

On peut résumer dans le théorème suivant les résultats obtenus

Théorème 10

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 $c_+(P,Q;a,b) - c_-(P,Q;a,b)$.

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 $c_+(P,Q) - c_-(P,Q)$.

---

[1] Ceci ressemble à un petit miracle, comme le b) de la proposition 10 , d'ailleurs. La meilleure explication est sans doute que les $\mathbf{StHa}_j(P, Q)$ sont égaux, à un facteur de signe constant près, aux $\mathbf{Ha}_j(P'Q, -P)$, et que le théorème de Sturm-Sylvester peut aussi être énoncé avec la suite des restes signés démarrant avec P'Q et -P en comptant le nombre de changements de signes à partir de -P .

démonstration:

a) (i) voir le théorème 6

a) (ii) voir le théorème 1 (i)

b) (i) voir les théorèmes 6 et 9 et la proposition 19

b) (ii) : a) et au choix le théorème 1(ii) ou le théorème 7. ❑

Dans la démonstration du point b) on a donc produit une démonstration du point (ii) du théorème 1 (théorème de Sylvester, cas où l'intervalle est **R** tout entier) à partir du théorème 7 (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) et du théorème 7 on a produit une preuve de la proposition 18 sans utiliser les résultats de Frobenius sur les formes de Hankel.

Discussion

En définitive, quelle est donc la meilleure méthode pour calculer $c_+(P,Q) - c_-(P,Q)$?

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).

Etant 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 9) .

Si 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

§ 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 $c_+(P,Q;a,b) - c_-(P,Q;a,b)$.

– les propriétés de spécialisation de la suite de Stum-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 $c_+(P,Q) - c_-(P,Q)$, il faut noter que *la méthode la plus rapide est la suivante: calculer la suite des polynômes sous-résultants par un des algorithmes du § 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 19* . (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 10

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 cele 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 Stum-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.

Une dernière remarque, concernant un article de Van Vleck (datant de 1899-1900)

Dans un article récent ([Akr]), Akritas signale un article de Van Vleck qui affirme en substance que ce que nous appelons la suite de Sturm-Habicht d'un polynôme est une "suite de Sturm", c.-à-d. peut être utilisée pour le comptage des zéros réels d'un polynôme sur un intervalle. Les polynômes considérés par Van Vleck sont exactement nos polynômes de Habicht $\mathbf{Ha}_j(P,S)$. Il sont définis comme des polynômes associés à des matrices extraites de la matrice de Sylvester de P et S après qu'on ait convenablement réordonné les lignes. A ce titre, on pourrait aussi bien les appeler des polynômes de Van Vleck.
Néanmoins, les théorèmes de Van Vleck sont incorrects lorsque la suite des coefficients sous-résultants comporte plusieurs zéros consécutifs, c.-à-d. lorsqu'il y a une chute de degré supérieure à 2 dans la suite des restes.
Ceci n'est pas étonnant dans la mesure où la démonstration de Van Vleck n'est faite que dans le cas d'une chute de degré égale à 1 ou 2 et uniquement pour le comptage de *toutes* les racines réelles.
En particulier Van Vleck semble ignorer qu'en cas d'une chute de degré supérieure à 2, les polynômes sous résultants intermédiaires sont identiquement nuls. Et il ne donne pas la règle de comptage nécessaire lorsqu'il y a plusieurs zéros consécutifs dans la suite des coefficients sous-résultants (notre proposition 19), règle de comptage qui diffère de celle utilisée avec les "suites de Surm". De même, il n'indique aucune règle de comptage particulière pour le cas de l'évaluation en un réel a fini qui serait racine d'un polynôme défectueux dans la suite de Habicht (notre $V'(f_0,f_1,...,f_n ; a)$ dans la définition p. 31).
Signalons enfin que le "programme de travail" esquissé par Van Vleck est mené à bien (sans erreur ni omission) dans [Gon].
Par ailleurs, voici quelques remarques sur l'article d'Akritas. La méthode de Bareiss appliquée à la matrice de Sylvester (convenablement réordonnée) est certes une méthode uniforme et facile à exposer pour le calcul de la suite de Habicht de 2 polynômes. Il y a cependant quelques bonnes raisons de ne pas se limiter à cette méthode.

- tout d'abord les raffinements nécessaires pour la démonstration de la nouvelle règle de comptage dans le cas défectueux, semblent compliquer inévitablement tout exposé de

la théorie des sous-résultants. Seules les insuffisances de la preuve de Van Vleck pouvaient laisser penser le contraire.

- les sous-résultants "améliorés" que nous calculons dans l'algorithme n°5 offrent des avantages évidents tant pour le temps de calcul que pour les problèmes de spécialisation.
- les 5 algorithmes que nous proposons (issus de [Loos] et [Hab]) sont plus rapides (d'un facteur O(n)) que celui donné par la méthode de Bareiss (cf note bas de page n°2 p 29).

Laureano GONZALEZ	Henri LOMBARDI	Marie-Françoise ROY
Tomas RECIO	Mathématiques	I R M A R
Mathématiques	UFR des Sciences et Techniques	Université de Rennes
Université de Santander	Université de Franche-Comté	35 042 Rennes cédex
Espagne	25 030 Besançon cédex	France
	France	

Nous remercions Mr. Jouanolou pour nous avoir signalé les références [Bor] et [Akr] dans la bibliographie qui suit.

Bibliographie

[Ait] Aitken A. C. : On the evaluation of determinants, the formation of their adjugates, and the practical solution of simultaneous linear equations. Proc. Edinburgh Math. Soc. ser 2 III , 207-219 , (1932)

[Akr] Akritas A. G. : A New Method for Computing G.C.D. and Polynomial Remainder Sequences. Numer. Math. 52, 119-127 (1988).

[Bar] Bareiss E. H. : Sylvester's identity and multistep integer preserving Gaussian elimination. Math. Comp. 22, 565-578 (1968).

[Bor] Borchardt : Zur Theorie der Elimination und Kettenbruch-Entwichlung. Math. Abh. der Akad. der Wissenschaften zu Berlin, 1878, p 1-17.

[Bro] Brown W. S. : On Euclid's Algorithm and the Computation of Polynomial Greatest Common Divisors. JACM 18, 476-504 (1971)

[BroT] Brown W. S., Traub J. F. : On Euclid's Algorithm and the Theory of Subresultants. JACM 18, 505-514 (1971)

[Col] Collins G.E. Subresultants and Reduced Polynomial Remainder Sequences. JACM 14, 128-142 (1967)

[CoR] Coste M., Roy M.-F. : Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets. J. Symbolic Computation 5 , 121-129 (1988).

[Fro] Frobenius : Uber das Traegheitsgesetz des quadratishen Formen, S-B Pruss. Akad. Wiss. 241-256 (Marz 1984) und 403-431 (Mai 1984)

[Gan] Gantmacher Fr. :Théorie des matrices, tome I. Dunod 1966.

[GLRR1] Gonzalez L., Lombardi H., Recio T., Roy M.-F. : spécialisation de la suite de Sturm et sous-résultants (I) et (II). A paraître au RAIRO Informatique théorique.

[GLRR2] Gonzalez L., Lombardi H., Recio T., Roy M.-F. : Sturm-Habicht sequences. Proceedings ISSAC 1989 pages 136-146 .

[Gon] Gonzalez Laureano. The proof of the Sylvester Theorem through Habicht's sequence. prépublication . Université de Santander (Espagne). 1988

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

[Her] Hermite C. : Remarques sur le théorème de Sturm, C. R. Acad. Sci. Paris 36 , 52-54 (1853).

[KrN] Krein M. G. Naimark M.A. : The method of symmetric and hermitian forms on the theory of the separation of the roots of algebraic equations . Originalement publié à Kharkov (1936). Lin. Multilinear algebra 1981, 10 265-308 (1981).

[Lom] Lombardi Henri : Sous-résultants, suite de Sturm, spécialisation Prépublication. Besançon. 1988.

[Loos] Loos R. : Generalized poynomial reaminder sequences. Dans Computer Algebra, Symbolic and Algebraic Computation 115-138. Edité par Buchberger, Collins, Loos . Springer Verlag 1982.

[Mig] Mignotte M.: Some useful bounds. Dans Computer Algebra, Symbolic and Algebraic Computation 259-263. Edité par Buchberger, Collins, Loos . Springer Verlag 1982.

[Stu] Sturm C.: Mémoire sur la résolution des équations numériques. Inst. France Sc. Math. Phys. 6 (1835)

[Syl] Sylvester J. J. : 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] Vallibouze A.: Fonctions symétriques et changements de base, Thèse, Université Paris VI, 1987.

[VV] Van Vleck, E. B., : On the determination of a series of Sturm's functions by the calculation of a single determinant. Ann. Math. (Second Series) 1, 1-13 (1899-1900).