SOUS-RESULTANTS , SUITE DE STURM , SPECIALISATION

SUBRESULTANT POLYNOMIALS, STURM SEQUENCE SPECIALISATION

Abstract

We give a slight generalisation of subresultant polynomials of two polynomials in A[X] where A is an integral domain.

This allows to simplify proofs related to subresultant polynomials, specialisations of subresultant polynomials and algorithms to compute them.

We give explicit relations between the remainder sequence ans the subresultant sequence of two polynomials, and discuss the polynomial time computability of the remainder sequence.

We prove that the formal version of the Sturm sequence of two polynomials (here called the Sturm-Habicht sequence) is as good as the Sturm sequence for computing the number of real roots of a polynomial on an interval, but it is necessary to introduce a special counting rule for the number of changes of signs of the Sturm-Habicht sequence at a real root of a defective subresultant polynomial.

We study the polynomial time computability of a complete Bezout relation for a list of polynomials.

Key-Words

Subresultant polynomials, subresultant algorithm, Sturm sequence, formal Sturm sequence, complete Bezout relation, Smith normal form, polynomial time computability

SOUS-RESULTANTS , SUITE DE STURM , SPECIALISATION

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

Résumé

Nous donnons une légère généralisation de la notion de *polynôme sous-résultant* (ou *sous-pgcd*) de 2 polynômes de A[X] où A est un anneau intègre.

Ceci permet de simplifier les démonstrations concernant les sous-pgcd, de préciser les algorithmes pour les calculer, et de traiter de manière agréable les problèmes de *spécialisation* (c.-à-d. lorsqu'on transforme les coefficients par un homomorphisme d'anneaux), même lorsqu'il y a chute du degré (d'un ou même parfois des deux polynômes), en particulier dans le cas de la *suite de Sturm* et de ses généralisations.

Nous explicitons les relations entre suite des restes et suite des sous-pgcd, et discutons la question de la calculabilité en temps polynomial de la suite des restes.

Nous démontrons que la version formelle de la suite de Sturm, que nous appelons *suite de Sturm-Habicht,* fonctionne aussi bien que la suite de Sturm pour le comptage des racines réelles sur un intervalle, à condition d'introduire une règle particulière pour évaluer le nombre de changements de signes de la suite de Sturm-Habicht lorsqu'on est en un zéro d'un polynôme sous-résultant défectueux.

Nous étudions la calculabilité en temps polynomial d'une *relation de Bezout complète* entre plusieurs polynômes, qui est un cas particulier de la réduction de Smith d'une matrice.

Mots clé

Sous-résultants, sous-pgcd, algorithme des sous-résultants, suite de Sturm, suite de Sturm formelle, spécialisation, relation de Bezout, forme normale de Smith, calculabilité en temps polynomial

Remerciements

Je remercie vivement Marie-Françoise Roy et Laureano Gonzalez. Sans les longues discussions que nous avons eues et les éclaircissements qu'elles m'ont apportés, cet article n'aurait pas vu le jour.

Introduction

Nous donnons une légère généralisation de la notion de *polynômes sous-résultants* de 2 polynômes (cf **[Hab]**, **[Loos]**), polynômes que nous appelons également des *sous-pgcd*. L'utilité de cette généralisation s'avère lorsque nous étudions les problèmes liés à la spécialisation (§ 4 notamment) , en outre, les preuves de plusieurs résultats sont simplifiées.

La suite de polynômes sous-résultants est en quelque sorte une version formelle de la suite des restes, beaucoup plus facile à calculer, notamment pour les raisons suivantes:

– lorsque nous travaillons dans un anneau intègre **A** où les divisions exactes sont relativement aisées, on peut utiliser des algorithmes de calcul des sous-pgcd qui n'utilisent que des additions, multiplications et divisions exactes dans l'anneau **A** , et les coefficients obtenus restent polynomialement majorés si les déterminants sont polynomialement majorés dans **A** (par exemple avec $\mathbf{A} = \mathbb{Z}[X_1, ..., X_n]$)

– les sous-pgcd se spécialisent bien : si les divisions exactes dans un autre anneau **A'** ne sont pas aisées, on peut utiliser un algorithme de calcul des sous-pgcd dans **A** puis une *spécialisation* (i.e. un homomorphisme d'anneaux) de **A** vers **A'** (par exemple avec $\mathbf{A'} = \mathbb{Z}[\xi_1, ..., \xi_n]$ où les ξ_i sont des nombres algébriques).

– 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 prop 8).

Supposons maintenant que le corps des fractions de **A** est muni d'un ordre.

Le nombre de changements de signes dans la suite des restes (convenablement modifiée) intervient dans le théorème de Sturm et dans des généralisations du théorème de Sturm (cf par exemple **[Syl]**). Il s'avère en fait que la suite des sous-pgcd fait presque aussi bien l'affaire que la suite des restes pour calculer, à une constante près, le nombre de changements de signes. Ceci peut se déduire de résultats de Habicht, comme l'a montré Laureano Gonzalez (cf **[Gon]**). Nous en donnons dans cet article une preuve "directe".

Nous étudions dans le § 2 la suite des sous-pgcd par une méthode qui n'utilise pas de calculs de déterminants et se généralise au cas de n polynômes (cf § 9). Cela suffit à établir des résultats généraux concernant la calculabilité en temps polynomial de la suite des restes "à facteurs multiplicatifs non nuls près".

Nous établissons dans le § 3 les formules reliant explicitement la suite des restes à la suite des sous-pgcd. Nous retrouvons en les précisant les résultats du § précédent. Nous discutons la question de la calculabilité en temps polynomial de la suite des restes.

Dans le § 4 , étant donnée une spécialisation Sp: $\mathbf{A} \to \mathbf{A'}$, nous étudions la possibilité de calculer "facilement" les polynômes sous-résultants de Sp(P) et Sp(Q) lorsqu'on connaît les polynômes sous-résultants de P et Q .

Dans le § 5 , nous donnons différentes variantes de l'algorithme des sous-résultants de Habicht-Loos (donné dans **[Ha]** et modifié dans **[Loos]**). Nous sommes en désaccord avec **[Loos]** sur certains points de détail.

Dans le § 6 , nous définissons la *suite des restes signés* de 2 polynômes (qui est la suite des restes avec des signes modifiés selon une convention à la Sturm), puis la *suite de*

Habicht de 2 polynômes qui est une version formelle de la suite des restes signés. Nous démontrons par une méthode directe un résultat de Laureano Gonzalez qui montre que la suite de Habicht fait aussi bien l'affaire que la suite des restes signés dans le théorème de Sturm ou dans ses généralisations. Nous étudions les problèmes liés à la spécialisation d'une suite de Habicht.

Dans le § 7 , nous définissons *suite de Sturm-Habicht d'un polynôme* et indiquons comment elle se spécialise lorsque le degré du polynôme chute de 1 par spécialisation

Dans le § 8 , nous indiquons comment la suite de Habicht est calculée lors du traitement de la matrice de Sylvester (convenablement présentée) par la méthode du pivot améliorée à la Bareiss.

Dans le § 9 , nous étudions la calculabilité d'une *relation de Bezout complète entre plusieurs polynômes*, à titre de prolongement naturel des § 2 et 8 .

Plan de l'article

1) Matrice de Sylvester , polynômes sous-résultants et suite des restes: notations, premiers résultats

Nous donnons dans ce § une légère généralisation de la notion de polynôme sous-résultant. 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 un anneau intègre **A** et son corps de fractions **K** .

Notations

Polynômes, suite des restes

Nous noterons $d(P)$ le degré d'un polynôme P , $cd(P)$ son coefficient dominant et $\mathbf{cf}_j(P)$ son coefficient de degré j (égal à 0 si j est > d(P)).

Si R est le reste de la division de P par Q dans **K**[X], on note

$$\mathbf{Rst}(P,Q) := R ,$$

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

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

On arrête la suite au premier reste nul. Le pgcd de P et Q est le dernier reste non nul.

En posant $t := \sup(d(P),d(Q)+1)$, nous noterons

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

(pour $-1 < j < t-1$) $\mathbf{Rst}_j(P,Q)$ le reste de plus fort degré inférieur ou égal à j dans la suite des restes $\mathbf{Rst}^m(P,Q)$ avec $m \geq 1$.

Matrice de Sylvester

Si P et Q sont dans **A**[X], p , q , et j des entiers avec $d(P) \leq p$, $d(Q) \leq q$ et $j < \inf(p,q)$, nous notons $\mathbf{Sylv}_j(P,p, Q,q)$ la j-ème matrice extraite de "*la matrice de Sylvester de P et Q considérés comme étant de degrés p et q*" :

sur la base $X^{p+q-j-1},..., X^2, X, 1,$ les vecteurs lignes successifs de cette matrice sont : $P.X^{q-j-1},..., P.X, P, Q.X^{p-j-1},..., Q.X, Q$.

Cette matrice possède $Nl = p+q-2j$ lignes et $Nc = p+q-j$ colonnes.

Nous noterons $\mathbf{Esylv}_j(P,p, Q,q)$ le sous espace de **K**[X] engendré par les polynômes $P.X^{q-j-1},..., P.X, P, Q.X^{p-j-1},..., Q.X, Q$ (lignes de la matrice $\mathbf{Sylv}_j(P,p, Q,q)$).

Définitions

Polynôme associé à une matice

Par définition, le **polynôme associé à une matrice** possédant Nl lignes et Nc colonnes, où $Nc = Nl + j$, est un polynôme de degré $\leq j$: son coefficient de degré d est le déterminant extrait de cette matrice sur les colonnes 1,2,...,Nl-1,Nc-d .

Polynômes sous-résultants (ou sous-pgcd) de deux polynômes

Les **polynômes sous-résultants** (ou encore : **les sous-pgcd**) (de P et Q considérés comme étant de degrés p et q) sont les polynômes associés aux matrices

$\mathbf{Sylv}_j(P,p,\ Q,q)$.
Ils seront notés $\mathbf{Sres}_j(P,p,\ Q,q)$ $\quad j < \inf(p,q)$
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**.

Si $p = d(P) \geq q = d(Q)$, on appelle le **pseudo-reste** de la division de P par Q le polynôme à coefficients dans **A** :

$$\mathbf{Prst}(P,Q) := \mathbf{Sres}_{q-1}(Q,q,\ P,p) = cd(Q)^{p-q+1}\ .\ \mathbf{Rst}(P,Q)$$

La **suite des polynômes sous-résultants** est la liste des $\mathbf{Sres}_j(P,p,\ Q,q)$ pour j descendant de $\inf(p,q)-1$ à 0 .

Nous appellerons **polynôme sous-résultant standard** un sous-pgcd $\mathbf{Sres}_j(P,p,\ Q,q)$ où $d(P) = p$ et $d(Q) = q \leq p$.

Coefficients sous-résultants de deux polynômes

Les **coefficients sous-résultants** (ou encore les **sous-résultants**) (de P et Q considérés comme étant de degrés p et q) sont les coefficients suivants:

$$\mathbf{sr}_j(P,p,\ Q,q) := \mathbf{cf}_j(\mathbf{Sres}_j(P,p,\ Q,q)) \qquad j < \inf(p,q)$$

Remarques

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

(b) On a les relations $\mathbf{Sres}_j(a.P,p,\ b.Q,q) = a^{q-j}.b^{p-j}.\mathbf{Sres}_j(P,p,\ Q,q)$
$\mathbf{Rst}(a.P,b.Q) = a.\mathbf{Rst}(P,Q)$ et
$\mathbf{Prst}(a.P,b.Q) = a.b^{p-q+1}.\mathbf{Prst}(P,Q)$.

(c) Les polynômes sous-résultants définis dans [**Loos**] p. 118 sont les sous-pgcd standards.

Autres définitions et notations

Nous donnons au § 5 p 18 une extension "raisonnable" de la suite des sous-pgcd en la faisant démarrer à $j = p$, du moins lorsque $p > q = d(Q)$. Cette définition est utilisée au début du § 6 p. 23 dans la définition de la **suite de Habicht** de 2 polynômes. On trouve au début du § 6 p. 23 la définition de la **suite des restes signés** de 2 polynômes ainsi que les notations et conventions concernant le nombre de changements de signes dans une suite. Au début du § 7 p. 29 on trouve les définitions de la **suite de Sturm** et de la **suite de Sturm-Habicht** d'un polynôme

Relations entre sous-pgcd généraux et sous-pgcd standards

Ordinairement on calcule les sous-pgcd standards. Mais après spécialisation, il se peut que le degré de P ou celui de Q se retrouve diminué, aussi est-il intéressant d'étudier le comportement des sous-pgcd dans le cas où l'un des 2 degrés est plus petit que le degré annoncé. Si les 2 degrés sont trop petits, tous les sous-pgcd sont nuls.

Les autres sous-pgcd peuvent tous être facilement calculés à partir des sous-pgcd standards (ou vice-versa si l'autre sous-pgcd n'est pas identiquement nul), en appliquant la proposition suivante (pour plus de détails cf § 4) :

Proposition 1 :

Nous supposons $d(P) \le p$, $d(Q) \le q$, $j < \inf(p,q)$

a) Si $d(P) < p$ et $d(Q) < q$, alors

$$\mathbf{Sres}_j(P,p,Q,q) = 0$$

b) $$\mathbf{Sres}_j(P,p,Q,q) = (-1)^{(p-j)(q-j)}\ \mathbf{Sres}_j(Q,q,P,p)$$

c) Si $q' \ge q$ et $d(P) = p$ alors

$$\mathbf{Sres}_j(P,p,Q,q') = cd(P)^{q'-q}\ .\ \mathbf{Sres}_j(P,p,Q,q)$$

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

preuve>

a) la première colonne de $\mathbf{Sylv}_j(P,p,Q,q)$ est nulle

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

c1) la nouvelle matrice est obtenue à partir de l'ancienne en rajoutant q'-q colonnes nulles à gauche, puis q'-q 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 $cd(P)^{q'-q}$.

c2) on applique c1) et 2 fois b) ❑

NB : Lorsque P est unitaire, la proposition 1 c1) montre que le polynôme sous-résultant $\mathbf{Sres}_j(P,p,Q,q)$ ne dépend pas du choix de $q \ge d(Q)$.

Proposition 2 :

Soient P et Q des polynômes de degrés p et $q < p-1$, alors :

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

b) $\mathbf{Sres}_q(P,p,Q,p-1) = (cd(P)\, cd(Q))^{p-q-1}\ Q$

c) $\mathbf{Sres}_j(P,p,Q,p-1) = cd(P)^{p-q-1}\ \mathbf{Sres}_j(P,p,Q,q)$ pour $j < q$

d) $\mathbf{Sres}_{q-1}(P,p,Q,p-1) = (-cd(P))^{p-q-1}\ \mathbf{Prst}(P,Q)$

preuve> a) et b) : faire un dessin de la matrice $\mathbf{Sylv}_j$: par exemple

avec $p = 6$, $q = 3$, $j = 4$

```
x x x x x x x      (les . représentent les 0 de la matrice)
• • y y y y .      (les • sont les coeffs 0 de Q au dessus du degré)
. • • y y y y      (les x représentent les coeffs de P )
                   (les y représentent les coeffs de Q )
```

avec $p = 6$, $q = 3$, $j = 3$

```
x x x x x x x .
. x x x x x x x
• • y y y y . .
. • • y y y y .
. . • • y y y y
```

c) c'est la prop 1c

d) on applique c) avec $j = q-1$ et on remarque que

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

(la 1ère égalité par définition, la 2ème en appliquant prop 1 b)) .❑

2) Un peu d'algèbre linéaire: conséquences pour la complexité

Nous étudions dans ce § la suite des sous-pgcd *dans le cas standard* par une méthode utilisant uniquement des arguments de dimension, sans faire appel à des calculs de déterminants. Cela suffit à établir des résultats généraux concernant la calculabilité en temps polynomial de la suite des restes *à facteurs multiplicatifs non nuls près.*

On considère 2 polynômes P et Q , de degrés p et q avec $p \geq q$, à coefficients dans l'anneau intègre **A** de corps des fractions **K** .

Notations :
On note pour abréger Rst_j au lieu de $Rst_j(P,Q)$, $Sylv_j$ au lieu de $Sylv_j(P,p,Q,q)$, $Esylv_j$ au lieu de $Esylv_j(P,p,Q,q)$.

Proposition 3 :

Soient 2 polynômes P et Q , de degrés p et q avec $p \geq q$.

Soient $j_1 \leq q$ et $j_2 \geq 0$ les degrés de 2 restes successifs (dans l'algorithme des divisions successives démarrant avec P et Q). Alors:

a) la matrice $\mathbf{Sylv}_{j_1-1}$ est de rang maximum (c.-à-d.: égal au nombre de ses lignes)

b) l'espace $\mathbf{Esylv}_{j_1-1}$ possède une base qui commence par $\mathbf{Rst}_{j_2}$, $\mathbf{Rst}_{j_1}$, et se poursuit par des polynômes dont les degrés augmentent régulièrement de 1 , tous de la forme $X^i.\mathbf{Rst}_j$ (avec $j \geq j_1$)

c) si $j_1 > j_2 + 1$, la matrice $\mathbf{Sylv}_{j_2}$ est de rang maximum (c.-à-d.: égal au nombre de ses lignes) et: l'espace $\mathbf{Esylv}_{j_2}$ possède une base qui commence par $\mathbf{Rst}_{j_2}$ et se poursuit par des polynômes dont les degrés augmentent régulièrement de 1 , tous de la forme $X^i.\mathbf{Rst}_j$ (avec $j \geq j_2$)

Avec les hypothèses $j_1 > 0$ et $\mathbf{Rst}_{j_2} = 0$ (degré = -1), on obtient :

a') la matrice $\mathbf{Sylv}_{j_1-1}$ est de rang égal au nombre de ses lignes moins 1

b') l'espace $\mathbf{Esylv}_{j_1-1}$ possède une base qui commence par $\mathbf{Rst}_{j_1}$, et se poursuit par des polynômes dont les degrés augmentent régulièrement de 1 , tous de la forme $X^i.\mathbf{Rst}_j$ (avec $j \geq j_1$)

preuve>

- On amorce la pompe avec $j_1 = q$, les résultats a) et b) (ou a') et b')) se montrent sans difficulté (diviser P par Q)
- On a la relation de récurrence $\mathbf{Esylv}_{m-1} = \mathbf{Esylv}_m + X.\mathbf{Esylv}_m$.

Par ailleurs $\mathbf{Sylv}_{m-1}$ possède 2 lignes de plus que $\mathbf{Sylv}_m$.

- Soient $j > k > h$ les degrés de 3 restes successifs. Supposons les résultats a) et b) démontrés avec $j_1 = j$ et $j_2 = k$. Supposons pour fixer les idées $j = k+3$.

Soit $\mathbf{Rst}_k$, $\mathbf{Rst}_j$, R_1, R_2,... R_n une base de $\mathbf{Esylv}_{j-1}$ comme décrite en b). Le nombre de lignes de $\mathbf{Sylv}_{j-1}$ est donc égal à $n + 2$.

- Vue la relation de récurrence l'espace $\mathbf{Esylv}_{j-2}$ contient les $n + 4$ polynômes $\mathbf{Rst}_k$, $X.\mathbf{Rst}_k$, $\mathbf{Rst}_j$, $X.\mathbf{Rst}_j$, $X.R_1$, $X.R_2$,... , $X.R_n$ dont les degrés sont strictement

croissants. Cela implique que la matrice $\mathbf{Sylv}_{j-2}$ est de rang maximum, (elle possède en effet $n+4$ lignes) et que les polynômes ci-dessus sont une base de $\mathbf{Esylv}_{j-2}$.
- De même, l'espace $\mathbf{Esylv}_k = \mathbf{Esylv}_{j-3}$ contient les $n+6$ polynômes

$\mathbf{Rst}_k$, X. $\mathbf{Rst}_k$, X^2. $\mathbf{Rst}_k$, $\mathbf{Rst}_j$, X.$\mathbf{Rst}_j$, X^2.$\mathbf{Rst}_j$, $X^2.R_1$, $X^2.R_2$,... $X^2.R_n$ dont les degrés croissent régulièrement de 1 en 1 . Cela implique que la matrice $\mathbf{Sylv}_k$ est de rang maximum, et que les polynômes ci-dessus sont une base de $\mathbf{Esylv}_k$. Ceci montre le c) pour $j_1 = j$ et $j_2 = k$.
- enfin l'espace $\mathbf{Esylv}_{k-1}$ contient les $n+8$ polynômes
$\mathbf{Rst}_k$, X.$\mathbf{Rst}_k$, X^2.$\mathbf{Rst}_k$, X^3.$\mathbf{Rst}_k$, $\mathbf{Rst}_j$, X.$\mathbf{Rst}_j$, X^2.$\mathbf{Rst}_j$, X^3.$\mathbf{Rst}_j$, $X^3.R_1$, $X^3.R_2$, $X^3.R_n$. Les 5 premiers polynômes engendrent le même espace que les polynômes $\mathbf{Rst}_h$, $\mathbf{Rst}_k$, X.$\mathbf{Rst}_k$, X^2.$\mathbf{Rst}_k$, X^3.$\mathbf{Rst}_k$: diviser $\mathbf{Rst}_j$ par $\mathbf{Rst}_k$. Et $\mathbf{Esylv}_{k-1}$ contient donc les polynômes $\mathbf{Rst}_h$, $\mathbf{Rst}_k$, X.$\mathbf{Rst}_k$, X^2.$\mathbf{Rst}_k$, X^3.$\mathbf{Rst}_k$, X.$\mathbf{Rst}_j$, X^2.$\mathbf{Rst}_j$, X^3.$\mathbf{Rst}_j$, $X^3.R_1$, $X^3.R_2$,... $X^3.R_n$ dont les degrés sont strictement croissants.
Si $\mathbf{Rst}_h$ est non nul, cela prouve donc a) et b) pour $j_1 = k$ et $j_2 = h$.
Si $\mathbf{Rst}_h$ est nul avec $k > 0$, nous voulons montrer a') et b') pour $j_1 = k$ et $j_2 = h$: nous connaissons déjà $n+7$ polynômes linéairement indépendants convenables dans le sous-espace $\mathbf{Esylv}_{k-1}$; il suffit donc de voir que la matrice $\mathbf{Sylv}_{k-1}$ ne peut pas être de rang maximum, et ceci se déduit du fait que tous les polynômes de $\mathbf{Esylv}_{k-1}$ sont multiples de $\mathbf{Rst}_k$ (pgcd de P et Q) et ont leur degré convenablement majoré. ❑

On en déduit immédiatement:

Théorème 1

a) Pour $j < q$ le sous-pgcd $\mathbf{Sres}_j$ est proportionnel au reste $\mathbf{Rst}_j$
b) Si $j_1 \leq q$ et j_2 sont les degrés de 2 restes successifs , les polynômes $\mathbf{Sres}_{j_1-1}$ et $\mathbf{Sres}_{j_2}$ sont multiples de $\mathbf{Rst}_{j_2}$ avec des facteurs non nuls
c) Si $j_1 - 1 > j > j_2$, alors $\mathbf{Sres}_j$ est identiquement nul

preuve>

* Si la matrice $\mathbf{Sylv}_j$ n'est pas de rang maximum, le sous-pgcd est identiquement nul. Ceci se produit lorsque $\mathbf{Rst}_{j_1}$ est le dernier reste non nul, avec $j < j_1$. En effet, les lignes de la matrice représentent des polynômes tous multiples de $\mathbf{Rst}_{j_1}$, ce qui donne la dimension de $\mathbf{Sylv}_j$: $p - q - j - j_1$. Or la matrice possède plus de lignes: $p - q - 2j$. Ceci prouve a) lorsque j est plus petit que le degré du dernier reste non nul, ainsi que b) et c) lorsque $j_2 = -1$

* Voyons b) et c) lorsque $j_2 \geq 0$ et $j_1 - 1 \geq j \geq j_2$: la matrice $\mathbf{Sylv}_j$ est alors de rang maximum. Une base de $\mathbf{Esylv}_j$ est donnée dans la proposition 3 (ou dans sa preuve). Or, lorsqu'on remplace les vecteurs lignes, supposés indépendants, d'une matrice, par une autre base de l'espace engendré, les polynômes associés aux deux matrices sont proportionnels avec pour rapport le déterminant d'une matrice de passage. Nous pouvons donc raisonner avec la matrice ayant pour vecteurs lignes la base de $\mathbf{Esylv}_j$ fournie à la proposition 3 (ou dans sa preuve). Cette matrice est sur-triangulaire et son polynôme associé est immédiatement calculé: c'est un multiple de $\mathbf{Rst}_{j_2}$, le facteur étant non nul juste pour $j = j_1 - 1$ ou $j = j_2$. ❑

Corollaire

a) Si **A** est un anneau intègre où les déterminants sont calculables en temps polynomial[1], on peut calculer en temps polynomial une suite de

[1] Voir la remarque qui suit

polynômes de A[X] égaux, à des facteurs non nuls près, aux polynômes de la suite des restes de P et Q

b) Si en outre le corps des fractions K de A est muni d'un ordre tel que le signe d'un élément de A soit calculable en temps polynomial, alors on peut calculer en temps polynomial une suite de polynômes de A[X] égaux, à des facteurs strictement positifs près, aux polynômes de la suite des restes de P et Q

preuve>

a) immédiat

b) Il s'agit de multiplier chacun des sous-pgcd par le facteur +1 ou -1. Il faut voir que ces facteurs peuvent être déterminés en temps polynomial. On procède de proche en proche, en calculant, pour 2 sous-pgcd successifs, leur pseudo-reste, ce qui permet en utilisant les signes des différents coefficients dominants obtenus, de décider le "vrai signe" du reste correspondant. ❑

Remarque :

La phrase "les déterminants sont calculables en temps polynomial dans A" signifie précisément ceci: A est dénombrable et est codé de manière que l'on ait à la fois :

- l'égalité (dans A de 2 mots du code) est testable en temps polynomial, et
- les déterminants sont calculables en temps polynomial.

Dans l'anneau $A = \mathbb{Z}[X_1, \ldots, X_n]$ les déterminants sont calculables en temps polynomial. Les méthodes les plus performantes semblent être actuellement les méthodes modulaires (cf [**Col**]).

Le plus souvent , on peut obtenir la calculablilité en temps polynomial des déterminants par utilisation de la méthode de Bareiss : grosso modo : si dans A (convenablement codé) les additions, multiplications, divisions exactes, tests d'égalité sont en temps polynomial et si la taille des déterminants est polynomialement majorée, alors le calcul des déterminants est en temps polynomial. Une étude générale de la calculabilité des déterminants en temps polynomial est donnée dans [**Lom**].

3) Sous-pgcd et vrais restes : des formules explicites

Nous établissons dans ce § les formules reliant explicitement la suite des restes à la suite des sous-pgcd standards. Nous retrouvons en les précisant les résultats du § précédent. Nous discutons la question de la calculabilité en temps polynomial de la suite des restes.

Dans tout le § nous utiliserons souvent l'hypothèse suivante, notée (H) :

(H) $\quad p = d(P) \geq q = d(Q)$, $R = \mathbf{Rst}(P,Q)$, et $r = d(R)$

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

Proposition 4 : Supposons (H) et $j < q$, alors:

$\mathbf{Sres}_j(P,p,Q,q) = \mathbf{Sres}_j(R,p,Q,q)$ et $\mathbf{Sres}_j(Q,q,P,p) = \mathbf{Sres}_j(Q,q\,R,p)$

preuve> Chaque ligne $P.X^k$ de la matrice $\mathbf{Sylv}_j(P,p,Q,q)$ peut être remplacée par la ligne $R.X^k$ en lui rajoutant des lignes $-c_m.Q.X^{k+m}$, en choisissant pour c_m les coefficients du polynôme B dans l'identité de la division euclidienne: $P = B.Q + R$. Ces manipulations

élémentaires ne modifient pas les déterminants extraits.
Or, la nouvelle matrice obtenue n'est autre que $\mathbf{Sylv}_j(R,p,Q,q)$
NB: cette dernière matrice, à coefficients dans **K** , admet donc un polynôme associé à coefficients dans **A** ❑

Le cas générique *(les degrés dans la suite des restes décroissent de 1 en 1)*

Proposition 5 : Supposons (H) et $p = q+1$. Alors nous avons:

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

b) $\mathbf{Sres}_j(P,p,Q,q) = cd(Q)^2\ \mathbf{Sres}_j(Q,q,R,q-1)$ pour $j < q-1$

Théorème 2 : Supposons (H) , et que les degrés dans la suite des restes décroissent de 1 en 1 (en commençant au polynôme P).
Posons $c(q) := cd(Q)$ et , pour $j < q$, $c(j) := cd(\mathbf{Rst}_j(P,Q))$. Alors:

$$\mathbf{Sres}_j(P,p,Q,q) = (\,c(q).c(q-1)...c(j+1)\,)^2\ \mathbf{Rst}_j(P,Q) \quad \text{pour } j < q$$

En particulier, si on est dans un corps ordonné, chaque sous-pgcd a "même signe" que le reste correspondant.

preuve> Le théorème résulte immédiatement de la proposition 5. La prop 5a résulte de l'égalité pour le pseudo-reste et de la prop 1c. La prop 5b résulte de la prop 4 et des prop 1c et 1b . ❑

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

Théorème de Habicht :
Nous supposons $d(P) \le p = q+1$, $d(Q) \le q$ [1].
Nous posons $S_p := P$, $S_q := Q$, $S_j := \mathbf{Sres}_j(P,p,Q,q)$ pour $j < q$, $C(j) := \mathbf{cf}_j(S_j)$ pour $j \le q$, $C(p) := 1$. Alors, pour $0 \le h < j \le q$, on a :

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

En particulier, lorsque $d(S_{j+1}) = j+1$ et $d(S_j) = j$, on obtient:

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

preuve> Le cas particulier résulte de l'égalité générale, avec $h = j-1$, et de la définition du pseudo-reste. Les égalités générales à démontrer sont des identités algébriques. On peut donc supposer que les coefficients de P et Q sont des *variables indépendantes*. On applique alors les résultats du théorème 2 . Les 2 membres de l'égalité à établir sont des multiples de $\mathbf{Rst}_h(P,Q)$. Les calculs sont simples. Nous les explicitons en reprenant les notations du théorème 2 .

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

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 $S_h = \gamma(h).R_h$ ❑

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

Théorème de Habicht : (2ème version)

Nous supposons $d(P) \le p$, $d(Q) = q$, $p > q$.

Nous posons $T_q := cd(Q)^{p-1-q} Q$, $T_j := \mathbf{Sres}_j(P,p,Q,q)$ pour $j < q$. Alors, pour $0 \le h < j < q$, on a :

$$\mathbf{cf}_j(T_j)^{2(j-h)} T_h = \mathbf{Sres}_h(T_{j+1}, j+1, T_j, j)$$

En particulier, lorsque $d(T_{j+1}) = j+1$ et $d(T_j) = j$, on obtient :

$$\mathbf{cf}_{j+1}(T_{j+1})^2 T_{j-1} = \mathbf{Prst}(T_{j+1}, T_j)$$

preuve> Le cas particulier résulte de l'égalité générale, avec $h = j - 1$, et de la définition du pseudo-reste. Les égalités générales à démontrer sont des identités algébriques. On peut donc supposer que les coefficients de P et Q sont des *variables indépendantes*.
Si $q = p - 1$, on retrouve la 1ère version du théorème de Habicht. Si $q < p - 1$, on pose $S_j := \mathbf{Sres}_j(P,p,Q,p-1)$ pour $j \le q$, de sorte qu'on a pour tout $j \le q$, $S_j = cd(P)^{p-1-q} T_j$ (en appliquant les prop 1 c1) et 2 b)), et on termine en remarquant que l'égalité du théorème de Habicht est homogène, donc passe des S_j aux T_j . ❑

Le cas défectueux

Proposition 6 : Supposons (H) . On a:

a) $\mathbf{Sres}_{q-1}(P,p,Q,q) = (-cd(Q))^{p-q+1} R = (-1)^{p-q+1} \mathbf{Prst}(P,Q)$

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

b) On en déduit

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

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

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

Corollaire :

a) Supposons (H). Le polynôme $\mathbf{Sres}_j(P,p,Q,q)$ est ou bien nul, ou bien égal, à un facteur non nul près dans **K** , à $\mathbf{Rst}_j(P,Q)$.
Le cas "facteur non nul" se produit lorsque j ou j+1 est le degré d'un reste, et pour $j = d(Q) - 1$.

b) Ce résultat reste vrai si $d(P) \le p$, $d(Q) \le q$, l'une des 2 inégalités étant une égalité, et $j < \inf(d(P),d(Q))$

Théorème 3 :

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

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

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

$$\mathbf{Sres}_{d_i - 1}(P,p,Q,q) = \varepsilon_i \cdot c_0^{f_0} \cdot c_1^{f_1} \cdots c_{i-1}^{f_{i-1}} \cdot c_i^{e_i} \cdot R_{i+1}$$

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

Corollaire

Si **A** est un anneau intègre où les déterminants sont calculables en temps polynomial, on peut calculer en temps polynomial une suite de polynômes de

A[X] égaux, à des facteurs carrés non nuls près dans **A** , aux polynômes de la suite des restes de P et Q

preuves>

Proposition 6

a1) en effet : $\mathbf{Sres}_{q-1}(Q,q,\ P,p) = cd(Q)^{p-q+1}\ R = \mathbf{Prst}(P,Q)$ et
$\mathbf{Sres}_{q-1}(P,p,\ Q,q) = (-1)^{p-q+1}\ \mathbf{Sres}_{q-1}(Q,q,\ P,p)$

a2) on a $\mathbf{Sres}_j(P,p,\ Q,q) = \mathbf{Sres}_j(R,p,\ Q,q)$ (prop 4)
$= (-1)^{(p-j)(q-j)}\ \mathbf{Sres}_j(Q,q,\ R,p)$ (prop 1b)
$= (-1)^{(p-j)(q-j)}\ cd(Q)^{p-q+1}\ \mathbf{Sres}_j(Q,q,\ R,q-1)$ (prop 1 c1)

b3) si $r = q - 1$ c'est simplement a2), sinon on applique la prop 2c) à $\mathbf{Sres}_j(Q,q,\ R,q-1)$

b1) on applique a2) puis la prop 2a) à $\mathbf{Sres}_j(Q,q,\ R,q-1)$

b2) si $r = q - 1$ c'est trivial, sinon on applique a2) puis la prop 2 b) à $\mathbf{Sres}_j(Q,q,\ R,q-1)$ et on utilise a1) .

Corollaire de la proposition 6

a) c'est vérifié pour $j = q - 1, \ldots, r$ d'après la proposition 6 , alinéas b1) et b2) . Pour $j < r$ on utilise l'alinéa b3) qui nous ramène au cas de la suite des restes démarrant avec Q et R . (preuve par induction sur le degré de P donc) .

b) la proposition 1c montre que $\mathbf{Sres}_j(P,p,\ Q,q)$ et $\mathbf{Sres}_j(P,d(P),\ Q,d(Q))$ sont proportionnels dans un facteur non nul pour $j < \inf(d(P),d(Q))$

Théorème 3

Se démontre par récurrence sur i en utilisant la proposition 6 . On amorce la pompe avec a1) et la recurrence fonctionne grâce à b3).

Corollaire du théorème

Posons $s_{i+1} := cd(\mathbf{Sres}_{d_i-1}(P,p,\ Q,q))$

La formule du théorème appliquée aux coefficients dominants donne:

$$s_{i+1} := \varepsilon_i \cdot {c_0}^{f_0} \cdot {c_1}^{f_1} \ldots\ldots {c_{i-1}}^{f_{i-1}} \cdot {c_i}^{e_i} \cdot c_{i+1}$$

et on voit qu'on a un polynôme V_{i+1} égal à R_{i+1} *à un facteur carré non nul près* qui est de la forme :

$$V_{i+1} := \alpha_i \cdot {s_0}^{g_{0,i}} \cdot {s_1}^{g_{1,i}} \ldots\ldots {s_{i-1}}^{g_{i-1,i}} \cdot {s_i}^{g_{i,i}} \cdot \mathbf{Sres}_{d_i-1}(P,p,\ Q,q)$$

avec les $g_{k,i}$ égaux à 0 ou 1 , et $\alpha_i = \pm 1$ qui peuvent être calculés de proche en proche

❑

Discussion sur le temps de calcul de la suite des restes

Nous établissons maintenant des formules plus explicites lorsque les degrés descendent de 1 en 1 et lorsqu'ils descendent de 3 en 3. Dans le premier cas, on conclut que la suite des restes (pour deux polynômes de départ à coefficients entiers) est calculable en temps polynomial. Le deuxième cas a été choisi parce qu'apparaît alors dans les formules la possibilité d'une explosion exponentielle de la taille des coefficients de la suite $\mathbf{Rst}_j$. Nous n'avons cependant pas d'exemple explicite d'explosion, et nous laissons donc la question ouverte.

Proposition 7 : Nous reprenons les hypothèses du théorème 2, et nous définissons: $c(j) := cd(\mathbf{Rst}_j)$, $C(j) := cf_j(\mathbf{Sres}_j)$ $C(q) := c(q) := cd(Q)$

Alors les c(j) et les C(j) sont liés par les relations: (pour $0 \le j < q$)

$C(j) = (\ c(q).c(q-1)...c(j+1)\ )^2\ c(j)$

$C(j)\ /\ C(j+1) = c(j+1).c(j)$

$c(q).c(q-1)...c(q-2i) = C(q).C(q-2)....C(q-2i) \,/\, C(q-1).C(q-3)....C(q-2i+1)$

$c(q).c(q-1)...c(q-2i-1) = C(q-1).C(q-3)...C(q-2i-1) \,/\, C(q).C(q-2)...C(q-2i)$

En particulier, si les déterminants sont calculables en temps polynomial dans **A**, les $\mathbf{Rst}_j$ peuvent être calculés en temps polynomial.

Proposition 8 : Nous supposons (H), $q = p-1$, et que les degrés successifs dans la suite des restes descendent de 3 en 3 (à partir de q). Nous reprenons les notations du théorème 3 et nous définissons en outre:

$S_0 = R_0 = Q$, $S_{i+1} := \mathbf{Sres}_{d_i - 1}$, $C_i := cd(S_i)$.

On obtient alors les relations:

$S_0 = R_0$, $S_1 = c_0^2.R_1$, $S_2 = c_0^4.c_1^4.R_2$

$S_{i+1} = c_0^4.(c_1....c_{i-1})^6 . c_i^4 . R_{i+1}$ $(i \geq 2)$

$C_{i+1} = c_0^4.(c_1....c_{i-1})^6 . c_i^4 . c_{i+1}$ $(i \geq 2)$

$C_0 = c_0$, $C_1 = c_0^2.c_1$

$C_{i+1} / C_i = c_{i-1}^2 \, c_i^3 \, c_{i+1}$ $(i \geq 1)$

$c_i \cdot c_{i+1} = C_{i+1} / (C_i \cdot (c_{i-1} c_i)^2)$ $(i \geq 1)$

$c_{i+1} \cdot c_{i+2} = (c_{i-1} c_i)^4 . C_{i+2}. C_i^2 / C_{i+1}^3$ $(i \geq 1)$

$c_0. c_1 = C_1 / C_0$

$c_2. c_3 = C_3.C_1 / C_2^3.C_0^4$

$c_4. c_5 = C_5.C_3^6.C_1^{24} / C_4^3.C_2^{12}.C_0^{16}$ et plus généralement

$$c_{2i}. c_{2i+1} = C_{2i+1} \cdot \Big(\prod_{t=0}^{i-1} C_{2i-2t-1}^{6.4^t}\Big) / \Big(\prod_{t=0}^{i-1} C_{2i-2t}^{3.4^t}\Big) C_0^{4^i}$$

preuve> on applique le théorème 2 pour la proposition 7 et le théorème 3 pour la proposition 8 ❑

Question ouverte : La proposition 8 incline en faveur de l'affirmation suivante:
Lorsque $\mathbf{A} = \mathbb{Z}$, les coefficients des polynômes de la suite des restes de 2 polynômes P et Q ne sont pas polynomialement majorés en taille à partir de la taille des données (qui sont les listes des coefficients de P et Q)
Soit en effet v une valuation p-adique (ou le logarithme de la valeur absolue archimédienne); on considère l'égalité :

$$c_{i+1} \cdot c_{i+2} = (c_{i-1} c_i)^4 . C_{i+2}. C_i^2 / C_{i+1}^3$$

on pose $i = 2k+1$, $\gamma_k = c_{2k}.c_{2k+1}$ et on obtient

$$v(\gamma_{k+1}) = 4.v(\gamma_k) + v(C_{2k+3}) + 2.v(C_{2k+1}) - 3.v(C_{2k+2})$$

On en déduit que :

si $v(\gamma_0) \geq 1$, et pour tout k $3.v(C_{2k+2}) \leq 2^k + v(C_{2k+3}) + 2.v(C_{2k+1})$

alors pour tout k $v(\gamma_k) \geq 2^k$

Si on arrive à réaliser les inégalités ci-dessus, ainsi que les annulations de déterminants qui forcent la suite des degrés des restes à descendre 3 en 3, avec des polynômes P et Q de degrés arbitrairement grands et ayant des coefficients majorés en taille par une fonction polynôme du degré, on aura établi l'affirmation en italique ci-dessus.
Si cette conjecture est vraie, cela signifie que la méthode des divisions successives ne doit pas être appliquée "telle quelle" dans les calculs de PGCD dans $\mathbb{Q}[X]$, et a fortiori dans les calculs

de base standard pour des idéaux de $\mathbb{Q}[X,Y]$ (par exemple), ou dans le calcul d'une forme réduite de Smith d'une matrice à coefficients dans $\mathbb{Q}[X]$.

4) Spécialisation

Etant donnée une spécialisation (i.e. un homomorphisme d'anneaux) Sp: $\mathbf{A} \to \mathbf{A'}$, nous étudions la possibilité de calculer "facilement" les polynômes sous-résultants standards de Sp(P) et Sp(Q) lorsqu'on connaît les polynômes sous-résultants standards de P et Q (polynômes de A[X]). Ceci est important car il est fréquent d'avoir un algorithme de division exacte facile dans **A** , et beaucoup plus difficile (voire impossible) dans **A'**. Or les algorithmes rapides de calculs des sous-pgcd utilisent des divisions exactes (cf § 5 et § 8).

1er cas : *les degrés de P et Q 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 2 degrés de P ou Q s'abaisse au cours d'une spécialisation*

Nous supposons que les divisions exactes se font "facilement" dans **A**.

Supposons que nous connaissions, par exemple par l'algorithme n°1 donné au § 5 , les polynômes sous-résultants $\mathbf{Sres}_j(P,p, Q,p-1)$.

Si $d(Sp(P)) = d(P)$, on obtient en spécialisant ces sous-pgcd des sous-pgcd non nuls, même si $d(Sp(Q)) < d(Q)$.

Par contre, si $d(Sp(Q)) = d(Q) = q < p-1$ et $d(Sp(P)) < d(P)$, on a $Sp(\mathbf{Sres}_j(P,p, Q,p-1)) = 0$. Il suffit cependant de calculer $\mathbf{Sres}_j(P,p, Q,q)$ à partir de $\mathbf{Sres}_j(P,p, Q,p-1)$ pour obtenir par spécialisation des sous-pgcd non nuls. De manière générale, il est utile de savoir calculer les sous-pgcd standards à partir d'autres sous-pgcd. Ceci est possible si les divisions exactes dans l'anneau considéré sont "faciles". On utilisera les résultats suivants, conséquences immédiates de la proposition 1.

Proposition 9 : Nous supposons $d(P) = p$, $d(Q) = q$, $j < \inf(p,q)$

a) Si $q \geq p$ alors

$\mathbf{Sres}_j(Q,q, P,q) = (-1)^{q-j}\, \mathbf{Sres}_j(P,q, Q,q) = \mathbf{Sres}_j(P,q+1, Q,q) / cd(Q)$

b) Si $p \geq q' > q$ alors

$\mathbf{Sres}_j(P,p, Q,q) = \mathbf{Sres}_j(P,p, Q,q') / cd(P)^{q'-q}$

$= \mathbf{Sres}_j(P,p, Q,p-1) / cd(P)^{p-q-1}$

c) Si $p' > p \geq q$ alors

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

d) Si $p' \geq q \geq p$ alors

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

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

Nous supposons que cd(P) et cd(Q) s'écrivent respectivement: $cd(P) = a.c_p$ et $cd(Q) = a.c_q$ avec $Sp(a) = 0$. Plus précisément nous écrivons:

$P = a.c_p\, X^p + a_{p-1}\, X^{p-1} + \ldots$, $Q = a.c_q\, X^q + b_{q-1}\, X^{q-1} + \ldots$ et nous supposons que le déterminant $\boxed{det = c_p\, b_{q-1} - c_q\, a_{p-1}}$ se spécialise non nul.

Proposition 10 : Avec les hypothèses ci-dessus, et $p \geq q$

a) $Sp(\mathbf{Sres}_{q-1}(P,p,Q,q) / a) = Sp(\det . b_{q-1}^{p-q-1} . Q)$.

b) $Sp(\mathbf{Sres}_j(P,p,Q,q) / a) = (-1)^{q-j+1}.Sp(\det).\ \mathbf{Sres}_j(Sp(P),p-1, Sp(Q),q-1)$

pour $j < q-1$

preuve> Nous notons P_1 et Q_1 les polynômes P et Q tronqués de leur coefficient dominant. On a évidemment $Sp(P) = Sp(P_1)$ et $Sp(Q) = Sp(Q_1)$. Nous posons $P_2 := c_p.X^p + P_1$, $Q_2 := c_q.X^q + Q_1$.

Le polynôme $\mathbf{Sres}_j(P,p,Q,q)/a$ est le polynôme associé à la matrice M_j dont les vecteurs lignes successifs sont $P_2.X^{q-j-1}$, $P.X^{q-j-2}$,..., P.X, P, $Q_2.X^{p-j-1}$, $Q.X^{p-j-2}$,..., Q.X, Q

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

$Sp(c_p)$ $Sp(a_{p-1})$ $Sp(c_q)$ $Sp(b_{q-1})$	
0	matrice surtriangulaire dont les vecteurs lignes sont des polynômes $X^i\ Q_1$

D'où le résultat a)

cas j < q-1 : Si on regroupe en haut les 2 lignes portant $P_2.X^{q-j-1}$ et $Q_2.X^{p-j-1}$, et si on spécialise, on obtient une matrice de la forme

$Sp(c_p)$ $Sp(a_{p-1})$ $Sp(c_q)$ $Sp(b_{q-1})$	
0	$\mathbf{Sylv}_j(Sp(P_1),p-1,Sp(Q_1),q-1)$

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

4ème cas : *les degrés de P et Q 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

Q_q := Q tronqué au dessus du degré de Sp(Q),

P_p := P tronqué au dessus du degré de Sp(P),

à calculer les sous-pgcd de P_p et Q_q, et spécialiser pour terminer.

5) Algorithmes de calcul de polynômes sous-résultants

Nous présentons 5 algorithmes de calculs des sous-pgcd de 2 polynômes. Les relations entre ces algorithmes seront discutées à la fin du paragraphe

Algorithme n°1 (1)

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

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

Les S_j peuvent alors être calculés par la méthode suivante (utilisant uniquement des calculs de pseudo-restes et des divisions exactes):

entrées : les polynômes P et Q

sortie : la suite des sous-pgcd S_j $\quad (0 \leq j \leq n-1)$

initialisation :

– si $q = n$	$S_{q-1} := \mathbf{Prst}(P,Q)$	(0)	
– si $q < n$	$S_q := (cd(P)\, cd(Q))^{n-q}\, Q$	(1)	
	$S_{q-1} := (-cd(P))^{n-q}\, .\, \mathbf{Prst}(P,Q)$	(2)	
	en outre si $q < n-1$ et $q < k < n$: $S_k := 0$	(3)	
–	$j := q-1$		

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

–	$s := d(S_j)$		
– si $j = s$	$S_{s-1} := \mathbf{Prst}(S_{j+1}, S_j) \,/\, cd(S_{j+1})^2$	(4)	
– si $s < j$	$S_s := S_j .\, cd(S_j)^{j-s} \,/\, cd(S_{j+1})^{j-s}$	(5)	(*)
	$S_{s-1} := \mathbf{Prst}(S_{j+1}, S_j) \,/\, (-cd(S_{j+1}))^{j-s+2}$	(6)	(*)
	en outre si $s < j-1$ et $s < k < j$: $S_k := 0$	(7)	
–	$j := s-1$		

fin : l'algorithme se termine lorsqu'on a calculé S_0 cad lorsque $j \leq 0$

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

preuve>

(0) par la définition du pseudo-reste

(1) par la prop 2 b)

(2) par la prop 2 d)

(3) par la prop 2 a)

(4) par le th de Habicht puisque $cd(S_{j+1}) = cf_{j+1}(S_{j+1})$

(5) le th de Habicht nous donne : $cd(S_{j+1})^{2(j-s)} .\, S_s = \mathbf{Sres}_s(S_{j+1}, j+1, S_j, j)$, et la prop 2b : $\mathbf{Sres}_s(S_{j+1}, j+1, S_j, j) = (cd(S_j).cd(S_{j+1}))^{j-s}\, S_j$

(6) le th de Habicht nous donne : $cd(S_{j+1})^{2(j-s+1)} .\, S_{s-1} = \mathbf{Sres}_{s-1}(S_{j+1}, j+1, S_j, j)$, et la

---

1 Cet algorithme calcule les sous-pgcd $\mathbf{Sres}_j(P,n+1, Q,n)$ lorsque $d(P) = n+1 > d(Q)$.

Le Subresultant Theorem p 122 de [**Loos**] semble, en première lecture, concerner ces sous-pgcd, puisque p 121, ce sont ces sous-pgcd (obtenus par spécialisation d'une suite où P et Q sont formellement de degrés n+1 et n) qui sont considérés ... En fait le Subresultant Theorem est correct avec les $\mathbf{Sres}_j(P,n+1, Q,q)$ lorsque $n = p-1 \geq q$, il est par contre incorrect lorsque $p \leq q$. (Cf la dernière note bas de page au sujet de l'algorithme n°3)

prop 2d : $\mathbf{Sres}_{s-1}(S_{j+1}, j+1, S_j, j) = (-cd(S_{j+1}))^{j-s}\ \mathbf{Prst}(S_{j+1},S_j)$
(7) on applique le th de Habicht comme ci dessus et on conclut par la prop 2a. ❑

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 $\mathbf{A}$, les formules sont encore valables si on remplace les polynômes S_j par les S_j / c. Nous en déduisons, lorsque $p = d(P)$, $q = d(Q) \le n = p - 1$, un algorithme pour calculer les sous-résultants standards $\mathbf{Sres}_j(P,p,Q,q) = \mathbf{Sres}_j(P,p,Q,n) / cd(P)^{n-q}$ (cf proposition 1 c)). On notera que l'algorithme ne diffère du précédent que lorsque $q < n$, et seulement dans la partie "initialisation". Nous n'avons réécrit *étape suivante* et *fin* qu'à cause du changement de notation (T_j au lieu de S_j).

Algorithme n°2 :

(algorithme des polynômes sous-résultants standards dans le cas $d(Q) < d(P)$)

Nous supposons $d(P) = p = n+1$, $d(Q) = q \le n$.

Nous posons $T_p := P$, $T_n := Q$, $T_q := cd(Q)^{n-q}.Q$, et $T_j := \mathbf{Sres}_j(P,p,Q,q)$ pour $j < q$. Les T_j peuvent alors être calculés par la méthode suivante (utilisant uniquement des calculs de pseudo-restes et des divisions exactes):

entrées : les polynômes P et Q,

sortie : la suite des sous-pgcds standards T_j $\quad (0 \le j \le q)$

initialisation :

- $p := d(P)$, $q := d(Q)$, $n := p - 1$
- $T_q := cd(Q)^{n-q}\ Q$ (1)
- $T_{q-1} := (-1)^{n-q}\ .\ \mathbf{Prst}(P,Q)$ (2)
- $j := q - 1$

étape suivante : { $1 \le j \le q-1$, T_{j+1} et T_j sont supposés déjà calculés, avec $j+1 = d(T_{j+1})$ et $s = d(T_j)$. On va calculer les T_k manquants jusqu'à T_{s-1} }

- $s := d(T_j)$
- si $j = s$ $\quad T_{s-1} := \mathbf{Prst}(T_{j+1}, T_j) / cd(T_{j+1})^2$ (4)
- si $s < j$ $\quad T_s := T_j.\ cd(T_j)^{j-s} / cd(T_{j+1})^{j-s}$ (5) (*)
  $\quad T_{s-1} := \mathbf{Prst}(T_{j+1}, T_j) / (-cd(T_{j+1}))^{j-s+2}$ (6) (*)
  $\quad$ en outre si $s < j-1$ et $s < k < j$: $T_k := 0$ (7)
- $j := s - 1$

fin : l'algorithme se termine lorsqu'on a calculé T_0 cad lorsque $j \le 0$

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

Remarques:

1) si $j = s$ l'affectation (5) donnerait $T_j := T_j$. Et l'affectation (6) produirait le même effet que la (4)

2) on peut essayer de faire rentrer les affectations (1) et (2) dans le moule: (5) et (6). C'est possible en prenant $j = n$, $s = q$, et en faisant l'affectation $cd(T_{n+1}) := 1$ (qui est "fausse"). Avec cette philosophie, la suite des sous-pgcd commence à $T_{n+1} = P$ et il faut poser $T_k := 0$ si $q < k < p-1$. L'avantage est que les seules initialisations sont : $T_{n+1} := P$, $T_n := Q$, "$cd(T_{n+1}) := 1$". Et on passe directement à "étape suivante". Aussi ferons nous désormais la convention suivante: