Résultant et applications

Préparation agrégation, option C

05/06

Le résultant est un outil de calcul que l'on rencontre dans divers domaines des mathématiques, ce texte présente quelques méthodes de calcul du résultant plus ou moins efficaces selon les cas, puis des applications.

1 Calcul du résultant

Le calcul des résultants non triviaux est très vite intensif, on essaie donc d'utiliser des algorithmes efficaces, nous en présentons quelques uns.

1.1 Méthode du sous-résultant.

Pour calculer le résultant de A et B, on peut réduire le déterminant correspondant en faisant apparaitre par des combinaisons linéaires de lignes le reste de la division euclidienne de A par B. On suit ainsi l'algorithme d'Euclide. On peut donc améliorer l'efficacité de cette méthode de la même manière que pour le calcul du PGCD, en effectuant des pseudo-divisions (pour éviter d'introduire des dénominateurs), en simplifiant par le PGCD des coefficients, et même en utilisant la méthode du sous-résultant qui évite le calcul du PGCD des coefficients en calculant à priori un facteur commun du reste.

1.2 Méthodes de calcul de déterminant.

On peut "oublier" l'origine polynomiale du résultant et le calculer comme n'importe quel déterminant. On peut ainsi utiliser des méthodes modulaires par exemple lorsque les coefficients sont entiers (cf. infra) ou la méthode de Laplace, plus particulièrement efficace pour des polynomes creux ou à coefficients symboliques. Cette méthode consiste à calculer tout d'abord tous les mineurs 2,2 des 2 premières colonnes du déterminant, puis tous les mineurs 3,3 des 3 premères colonnes en les développant par rapport à la 3ème colonne et en utilisant les mineurs 2,2 précédents, ainsi de suite jusqu'au déterminant lui-même qu'on développe par rapport à la dernière colonne.

1.3 Méthodes modulaires.

Si les polynômes sont à coefficients entiers, on peut calculer le déterminant modulo plusieurs nombres premiers et reconstruire le résultat par le théorème des restes chinois

en utilisant la représentation symétrique des entiers. Il faut une majoration de la valeur absolue du déterminant à calculer, ce qu'on obtient facilement par la majoration de Hadamard.

Lorsque les polynômes dépendent polynomialement de paramètres, on peut donner des valeurs entières à ces paramètres et reconstruire le résultat par interpolation de Lagrange. Il faut ici une majoration sur le degré du résultant. On peut majorer par la somme des degrés partiels de A et B par rapport à cette variable multiplié par le degré total par rapport aux autres variables. Dans certains cas on peut améliorer cette majoration, par exemple si les polynomes considérés sont homogènes par rapport à un groupe de variables et si on calcule le résultant par rapport à une de ces variables, le degré total du résultant par rapport aux variables restantes est majoré par le produit des degrés totaux des deux polynômes de départ, c'est ce qui permet de montrer par exemple que l'intersection de deux courbes algébriques de degrés totaux n et m a au plus nm points (théorème de Bézout).

2 Exemples d'applications

Dans cette section, on présente quelques exemples importants d'application du résultant. Il ne s'agit en aucun cas d'une liste exhaustive d'applications !

2.1 Systèmes polynomiaux

Le résultant sert tout d'abord à éliminer une variable lorsqu'on résout plusieurs équations polynomiales faisant intervenir cette variable. Si A et B sont deux polynômes premiers entre eux à coefficients dans un anneau de polynômes, on peut écrire une version améliorée de l'identité de Bézout lorsque le second membre est le résultant de A et B : il existe deux polynomes U et V à coefficients dans l'anneau de polynomes tels que

$$AU + BV = \text{resultant}(A, B)$$

Ainsi, si A et B s'annulent alors le résultant de A et B s'annulera aussi.

Un exemple simple d'application est le passage d'équations paramétriques rationnelles d'une courbe à son équation cartésienne. On commence par transformer en un système de 2 équations polynomiales en t (le paramètre), x et y (les coordonnées), dont on élimine t en en prenant le résultant. En géométrie analytique, on peut représenter les objets usuels (droites, cercles) par des équations paramétriques rationnelles, et calculer les intersections, perpendiculaires, etc. de manière paramétrique, ce qui permet par exemple de calculer l'équation cartésienne d'un lieu géométrique.

On peut aussi calculer l'intersection de deux courbes algébriques par cette méthode, ou les points singuliers d'une courbe.

Plus généralement, on peut résoudre des systèmes polynomiaux de cette manière en éliminant au fur et à mesure les variables jusqu'à obtenir une équation en une variable. Cette méthode est toutefois moins efficace que l'utilisation des bases de Groebner : il s'agit de bases particulières d'un idéal engendré par des polynômes, telles que la réduction par "divisions" successives (en restant dans l'anneau) par les éléments de la base renvoie 0 si et seulement si le polynome est dans l'idéal. Le calcul des bases

de Groebner fait intervenir un ordre moins dissymétrique entre les variables, cette souplesse permet des gains en efficacité.

2.2 Fractions rationnelles (intégration)

C'est plutot l'identité de Bézout qui permet de décomposer des fractions rationnelles en éléments simples que l'on utilise pour calculer des primitives de fractions rationnelles, mais le résultant intervient à la fin.

On commence par factoriser le polynôme sous forme "square-free" (en produit de puissances de polynômes premiers entre eux et sans racine multiple), on décompose avec Bézout

$$\frac{N}{\prod_j P_j^j} = \sum_j \frac{N_j}{P_j^j}$$

on élimine les multiplicités en utilisant Bézout pour P_j et P_j', si $1 < k \leq j$:

$$\int \frac{N}{P_j^k} = \int \frac{AP_j + BP_j'}{P_j^k} = \int \frac{A}{P_j^{k-1}} + \int B\frac{P'}{P_j^k}$$

pour la dernière intégrale, on effectue une intégration par parties, ce qui permet de diminuer la puissance du dénominateur de 1, on se ramène ainsi à un dénominateur sans racine multiple (à la puissance 1).

L'étape finale consiste à intégrer une fraction dont le dénominateur n'a que des racines simples. C'est ici qu'intervient le résultant, si on souhaite exprimer cette intégrale en minimisant les extensions algébriques (nécessaires à la factorisation du dénominateur), en regroupant les logarithmes correspondant au même coefficient, on montre que :

$$\int \frac{N}{D} = \sum_{t/\text{resultant}(N-tD',D)=0} t \ln(\gcd(N - tD', D))$$

2.3 Extensions algébriques

Le résultant sert également à calculer le polynome minimal d'une extension algébrique contenant deux extensions algébriques. Si x a comme polynome minimal $P(x)$ de degré p irréductible sur $\mathbb{Q}[X]$ et y a comme polynome minimal $Q(y)$ de degré q, irréductible sur $\mathbb{Q}(x)[X]$, alors il existe un entier k tel que $kx + y$ engendre une extension algébrique contenant x et y, et le polynome minimal de $x + ky$ est de degré pq (en général on peut prendre $k = 1$). Pour calculer le polynome minimal de $kx + y$, on calcule le résultant par rapport à x de P et de $Q(z - kx)$, on le factorise par rapport à z, on doit obtenir un polynome de degré pq (sinon on change de k), en effet $P(x) = 0$ et si $z = kx + y$, alors $Q(z - kx) = Q(y) = 0$.

Le résultant sert également à factoriser des polynomes à coefficients dans une extension algébrique de $\mathbb{Q}$ (cf. par exemple Cohen).

3 Suggestions de développement

- Description d'un algorithme complet de calcul de primitives de fraction rationnelle.
- Applications en géométrie, par exemple calcul de lieu géométrique.
- Etude locale des courbes algébriques.
- Illustration de l'utilisation du résultant pour les extensions algébriques.
- Autre(s) exemple(s) d'application(s) du résultant et/ou de Bézout.
- Intérêt des algorithmes modulaires.
- Comparaison d'algorithmes de calcul de déterminant