Calcul polynomial

Bruno Salvy

INRIA

Exemple de polynôme

$$t^3 \log 2 + \frac{1}{y} + z^n - z^3 + \pi \log u + v$$

n'est pas un polynôme en z.

C'est un polynôme en

$$t, v$$

$$\pi, \log 2.$$

Types de problèmes

- Décision :
  - simplification et test d'égalité d'expressions faisant intervenir des racines de polynômes ;
  - questions de signe (nombre de racines réelles, ou dans un intervalle) ;
- Efficacité, généralité :
  - éviter la factorisation de polynômes (trop coûteuse) ;
  - chercher des algorithmes indépendants du corps de base.

I. Pgcd

Division euclidienne

$$A, B \in \mathbb{K}[x], \qquad \mathbb{K} \text{ corps}$$

$$\to A = BQ + R, \qquad \deg R < \deg B.$$

$Q := 0; R := A;$

Tant que $R \neq 0$ et

$\delta := \deg(R) - \deg(B) \geq 0$

  $T := \mathrm{lc}(R)/\mathrm{lc}(B)\, x^{\delta};$

  $Q := Q + T;\ R := R - TB;$

Renvoyer (Q, R).

Si $B(\alpha) = 0$, alors pour tout $P \in \mathbb{K}[x]$

$$P(\alpha) \in \bigoplus_{i=0}^{\deg B - 1} \mathbb{K} \cdot \alpha^i$$

espace vectoriel de dimension finie $\to$ forme normale, test d'égalité, …

Algorithme d'Euclide

$$A, B \in \mathbb{K}[x] \longrightarrow U, V, G \in \mathbb{K}[x],$$
$$AU + BV = G = \mathrm{pgcd}(A, B), \qquad \text{(Bézout)}$$

$\deg G$ maximal, $\deg U < \deg B$, $\deg V < \deg A$.

On va trouver (u_i, v_i) tels que

$$a_0 u_i + a_1 v_i = a_i$$

Lors d'une division euclidienne

$$\begin{aligned} a_{i+2} &= a_i - q_{i+1} a_{i+1}, \\ &= a_0(u_i - q_{i+1} u_{i+1}) + a_1(v_i - q_{i+1} v_{i+1}). \end{aligned}$$

→ fractions rationnelles (forme normale) ;

→ nombres algébriques (forme normale).

Factorisation sans carrés

$\mathbb{A}$ anneau factoriel de caractéristique 0.

$$P = Q_1^1 Q_2^2 \cdots Q_m^m$$

$Q_i \wedge Q_j = 1$ et Q_i sans facteurs multiples.
Faible complexité

→ partie sans carré du polynôme ;

→ groupe les racines par multiplicité.

$$\text{Idée : } G := \gcd(P, P') = \prod_{i=1}^{m} Q_i^{i-1}.$$

L'algorithme de Yun

$$W := P/G = \prod_{i=1}^{m} Q_i$$

$$Y := P'/G = Q_1'Q_2 \cdots Q_m + \cdots + mQ_1 \cdots Q_{m-1}Q_m'$$

$$Z := Y - W' = Q_1[Q_2' \cdots Q_m + \cdots + (k-1)Q_2 \cdots Q_m']$$

$$Q_1 = \gcd(W, Z).$$

Puis on itère :

$$W := W/Q_i, \quad Y := Z/Q_i, \quad Z := Y - W', \quad Q_i = \gcd(W, Z).$$

Un exemple

$$A = x^8 + 6x^6 + 12x^4 + 8x^2$$

G	W	Y	Z	A_i
$x^5 + 4x^3 + 4x$	$x^3 + 2x$	$8x^2 + 4$	$5x^2 + 2$	1
	$x^3 + 2x$	$5x^2 + 2$	$2x^2$	x
	$x^2 + 2$	$2x$	0	$x^2 + 2$

$$A = x^2(x^2 + 2)^3$$

Bézout et les nombres algébriques

$$AU + BV = G$$

Inverses : si $A(\alpha) = 0$ et $G = 1$,

$$\frac{1}{B(\alpha)} = V(\alpha), \qquad V \in \mathbb{K}[\alpha]$$

Plus généralement, si $P \in \mathbb{K}[x]$ est irréductible, $P(\alpha) = 0$,

$$\mathbb{K}(\alpha) \simeq \bigoplus_{i=0}^{\deg P - 1} \mathbb{K} \cdot \alpha^i$$

espace vectoriel de dimension finie $\rightarrow$ forme normale, test à zero.

II. Suites de restes

Pseudo-division euclidienne

Les coefficients appartiennent à un anneau intègre.

Pseudo-division :

$$\alpha A = BQ + R.$$

Remarque : dans la division euclidienne, on divise toujours par $\mathrm{lc}(B)$.

Algorithme : on divise $\mathrm{lc}(B)^{\deg(A)-\deg(B)+1} A$ par B.

Suite de restes :

$$R_0 = A, \qquad R_1 = B, \qquad \alpha_i R_i = R_{i+1} Q_i + R_{i+2}.$$

L'algorithme des sous-résultants

On pose $\beta_1 = -1$, $\alpha_1 = (-1)^{\delta_1+1}$,

$$\begin{cases} \delta_i = \deg(R_{i-1}) - \deg(R_i), \\ \beta_{i+1} = (-\operatorname{lc}(R_i))^{\delta_i}\beta_i^{1-\delta_i}, \\ \alpha_{i+1} = -\operatorname{lc}(R_i)\beta_{i+1}^{\delta_i+1}. \end{cases}$$

Théorème [Collins, Brown]. Ça donne bien une suite de restes.

PGCD par sous-résultants: exemple

$$\begin{array}{ll}
F_0 = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5 & \\
F_1 = 3x^6 + 5x^4 - 4x^2 - 9x + 21 & \alpha_1 = -1 \\
F_2 = 15x^4 - 3x^2 + 9 & \alpha_2 = -243 \\
F_3 = 65x^2 + 125x - 245 & \alpha_3 = -9375 \\
F_4 = 9326x - 12300 & \alpha_4 = 10985 \\
F_5 = 260708 &
\end{array}$$

$$\mathrm{Res}(F_0, F_1) = F_4.$$

Nombres algébriques réels

$$P \in \mathbb{Q}[x], \qquad a, b \in \mathbb{R} \cup \{\pm\infty\},$$

Nombre de racines de P dans $]a, b[$? ($P(a) \neq 0$, $P(b) \neq 0$).

Def. Suite de Sturm. $P_0 = P$, $P_1 = P'$, $P_{i+1} = -\operatorname{rem}(P_{i-1}, P_i)$.

Th.[Sturm] Le nombre de racines de P entre a et b est $V(P; a) - V(P; b)$.

Le calcul des P_i peut se faire par sous-résultants (en faisant attention au signe).

Permet l'isolation des racines réelles en temps polynomial.

III. Résultants

Un exemple

$$A = 3tx^2 - t^3 - 4$$

$$B = x^2 + t^3x - 9$$

On élimine x entre A et B :

$$C = A - 3tB = -3t^4x - t^3 - 4 + 27t$$

$$D = 3t^4B + xC = (3t^7 - t^3 + 27t - 4)x - 27t^4$$

$$E = 3t^4D + \mathrm{lc}(D)C = -3t^{10} - 12t^7 + t^6 - 54t^4 + 8t^3 + 729t^2 - 216t + 16$$

Définition

$$A, B \in \mathbb{A}[x], \qquad \mathbb{A} \text{ anneau intègre}$$

Soient α_i et β_j les racines de A et B (dans la clôture algébrique du corps des fractions de $\mathbb{A}$)

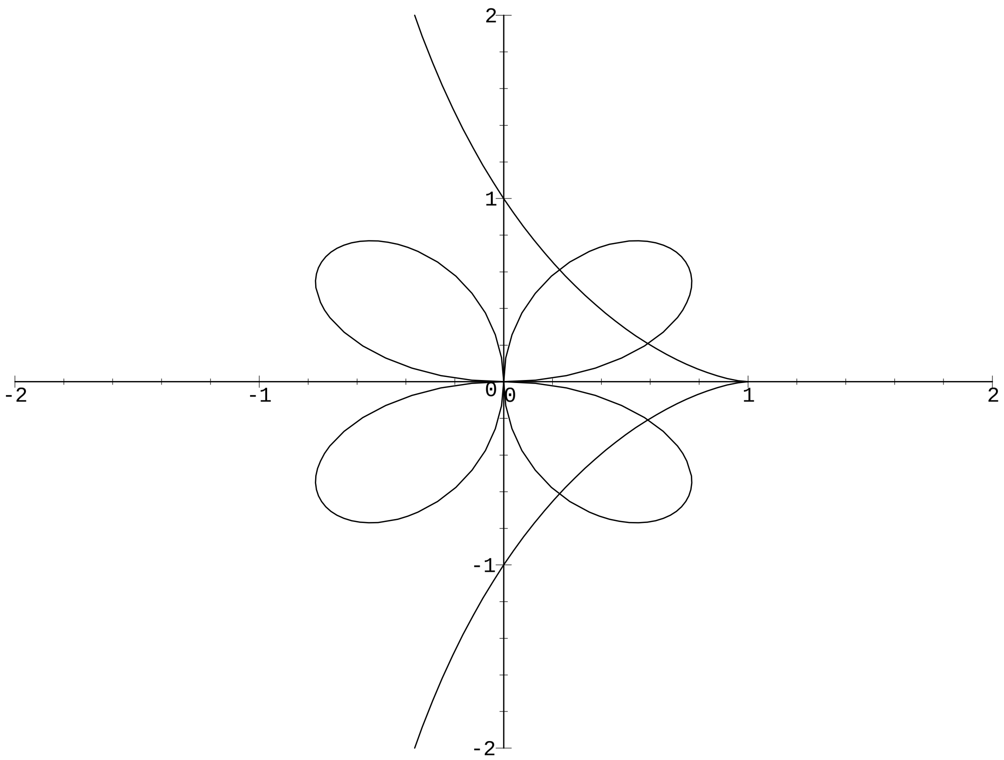
$$\mathrm{Res}_x(A, B) := \mathrm{lc}(A)^m \, \mathrm{lc}(B)^n \prod_{i,j} (\alpha_i - \beta_j).$$

Propriétés :

- $\mathrm{Res}_x(A, B) \in \mathbb{A}$;
- $\mathrm{Res}_x(A, B) = 0 \iff \deg(\mathrm{pgcd}(A, B)) > 0.$

x est éliminé entre A et B

Exemple



$$\begin{cases} (x^2+y^2)^3 - 4x^2y^2 = 0, \\ y^2(1+x) - (1-x)^3 = 0. \end{cases}$$

Opérations de corps dans $\overline{\mathbb{K}}$

$$P(\alpha) = 0, \quad Q(\beta) = 0$$

$$R(\alpha + \beta) = 0 \text{ avec } R(x) = \operatorname{Res}_y(P(x-y), Q(y)),$$

$$R(\alpha \cdot \beta) = 0 \text{ avec } R(x) = \operatorname{Res}_y(y^{\deg(P)} P(x/y), Q(y)),$$

$$R(\alpha / \beta) = 0 \text{ avec } R(x) = \operatorname{Res}_y(P(xy), Q(y)).$$

Croissance des degrés.

Calcul du résultant

$$A = a_0x^n + \cdots + a_{n-1}x + a_n \in \mathbb{A}[x], \quad a_0 \neq 0$$
$$B = b_0x^m + \cdots + b_{m-1}x + b_m \in \mathbb{A}[x], \quad b_0 \neq 0.$$

Prop. [Habicht]: Le $j$ème sous-résultant $S_j(A,B)$ est le déterminant de la matrice $(n+m-2j)\times(n+m-2j)$:

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_n & 0 & 0 & x^{n-j-1}A(x) \\ & a_0 & a_1 & \ddots & & \vdots & \vdots \\ & & & a_0 & \cdots & a_{n-j-1} & A(x) \\ b_0 & b_1 & \cdots & b_m & 0 & 0 & x^{m-j-1}B(x) \\ & b_0 & b_1 & \ddots & & \vdots & \vdots \\ & & & b_0 & \cdots & b_{m-j-1} & B(x) \end{pmatrix}.$$

$$\mathrm{Res}(A,B) = S_0(A,B).$$

Autres algorithmes sur les polynômes univariés

1. Méthodes modulaires ($\rightarrow$ pgcd)
2. Hensel lifting ($\rightarrow$ factorisation)
3. Théorie de Galois ($\rightarrow$ résolution par radicaux, denesting)

Plus de détails en filière calcul formel.