Un algorithme de factorisation absolue des polynomes en deux variables

Guillaume CHEZE

Définition et notations

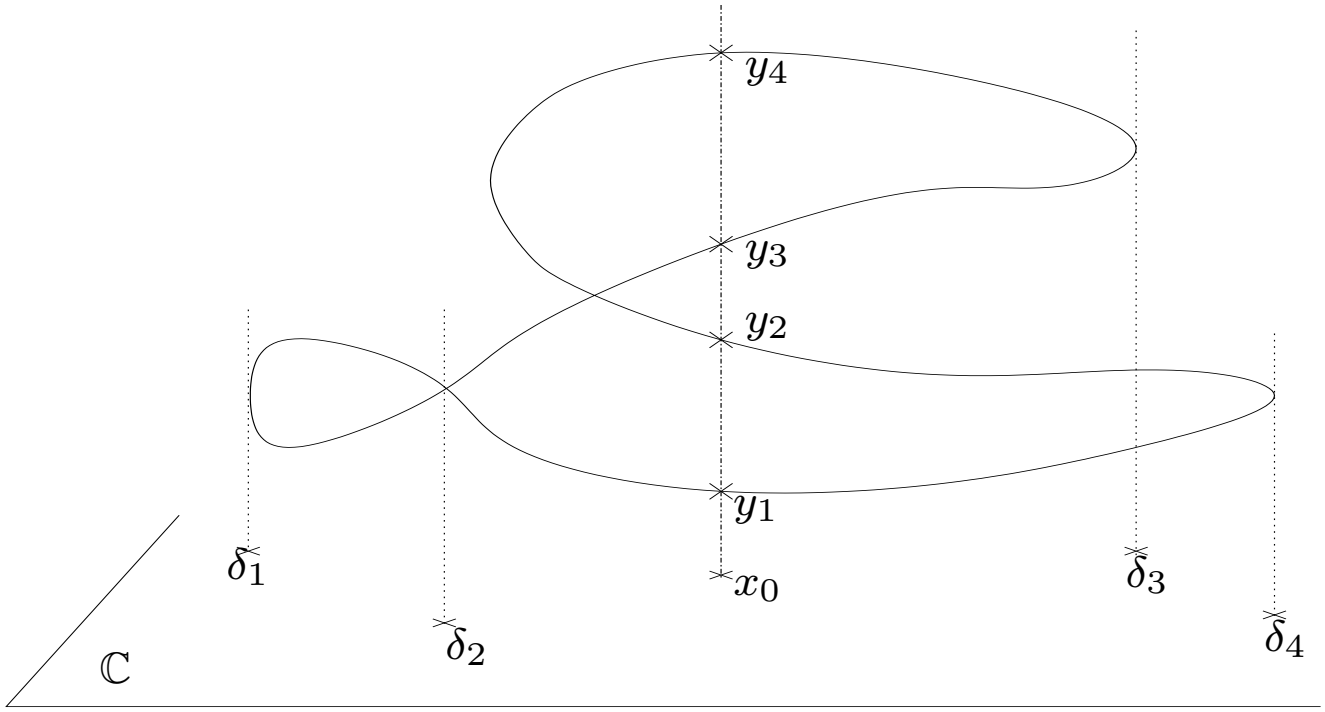
DEFINITION : Soit $P(X,Y) \in \mathbb{Q}[X,Y]$, la factorisation absolue de P est la décomposition $P = P_1 \cdots P_s$ en produits de polynomes irréductibles dans $\mathbb{C}[X,Y]$.

Notations :

- $P(X,Y) = Y^n + a_1(X)Y^{n-1} + ... + a_n(X)$ où $a_i(X) \in \mathbb{Q}[X]$ et $\deg(a_i(X)) \leq i$.
- $P(X,Y)$ est irréductible dans $\mathbb{Q}[X,Y]$.

Objectif : Trouver les facteurs P_i.

L'IDÉE



Soit $x_0 \notin \Delta = \{x \in \mathbb{C} \,|\, Res_Y(P, \partial_Y P)(x) = 0\}$.

Théorème des fonctions implicites $\Rightarrow \begin{cases} \varphi_i(x_0) = y_i(x_0) \\ P(X, \varphi_i(X)) = 0 \end{cases}$

L'IDÉE

$P(X,Y) = \prod_{i=1}^{n}(Y - \varphi_i(X))$
$\Rightarrow P_1(X,Y) = \prod_{k=1}^{m}(Y - \varphi_{i_k}(X)) = Y^m + (AX+B)Y^{m-1} + \cdots + c_m(X)$

Développement de Taylor de $\varphi_i(X)$:
$\varphi_i(X) = y_i + a_i(X - x_0) + b_i(X - x_0)^2 + \cdots$

Relations racines-coefficients $\Rightarrow \sum_{k=1}^{m} \varphi_{i_k}(X) = -(AX+B)$
$\Rightarrow \sum_{k=1}^{m} b_{i_k} = 0$

Caractérisation des facteurs

Théorème 1 (GaRup, SVW) *Soit $Q(X,Y) \in \mathbb{Q}[X,Y]$, irréductible dans $\mathbb{Q}[X,Y]$. Soit $P(X,Y) = Q(X + \lambda Y, Y)$. Alors pour presque toutes les spécialisations (x_0, λ_0) de (X, λ) nous avons :*
$\sum_I b_i = 0 \Longleftrightarrow \prod_I (Y - \varphi_i(X))$ *est un facteur polynomial de P.*

Objectif : Trouver les sommes minimales (i.e. $\sum_I b_i = 0$ et $\sum_{J \subsetneq I} b_i \neq 0$), elles correspondent aux facteurs absolument irréductibles.

0-1 VECTEURS

$\sum_I b_i = 0 \Longleftrightarrow \sum_I x_i b_i = 0$
où $x_i = 1$ pour $i \in I$ et $x_i = 0$ pour $i \notin I$.

Nous cherchons donc des 0-1 vecteurs dans $\mathbb{Z}^n$, $v_1, v_2, \ldots, v_l$ tels que :
$< v_i, b >= 0$ où $b = (b_1, \ldots, b_n) \in \mathbb{C}^n$.

DEFINITION : Soit $V = \mathbb{Z}(v_1, \ldots, v_l) \subset \mathbb{Z}^n$ le réseau engendré par $v_1, \ldots, v_l$.

Objectif : Trouver V.

La deuxième idée

"Construire une suite décroissante de réseaux $\mathcal{L}_i$ convergeant vers V." [vHoe]

$V \subset \mathcal{L}_{i+1} \subset \mathcal{L}_i \subset \mathcal{L}_0 = \mathbb{Z}^n$

$$\mathcal{L}'_0 = \mathbb{Z}(v'_1, \ldots, v'_n)\,, \begin{pmatrix} v'_1 \\ \vdots \\ v'_n \end{pmatrix} = \begin{pmatrix} 1 & 0 & \ldots & 0 & \Re(b_1) & \Im(b_1) \\ 0 & 1 & \ldots & 0 & \Re(b_2) & \Im(b_2) \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & \Re(b_n) & \Im(b_n) \end{pmatrix}$$

Soit $\nu_1, \ldots, \nu_n$ une base LLL réduite de $\mathcal{L}'_0$.

$\nu_1 = \sum_{i=1}^n \lambda_i v'_i = (\lambda_1, \ldots, \lambda_n, \sum_{i=1}^n \lambda_i \Re(b_i), \sum_{i=1}^n \lambda_i \Im(b_i))$ où $\lambda_i \in \mathbb{Z}$.

Objectif : Trouver des vecteurs du type $(1, 1, 0, 1, 0, \ldots, 1, 0, \mathbf{0,0})$.
Donc des vecteurs ν_i tels que $\|\nu_i\| \leq n$.

Nancy's Lemma Soit $\mathcal{L}' = \mathbb{Z}(\nu_1, \ldots, \nu_n)$ un réseau, M une constante et $\nu_1^*, \ldots, \nu_n^*$ les vecteurs donnés par l'orthogonalisation de Gram-Schmidt de $\{\nu_1, \ldots, \nu_n\}$. S'il existe un indice k_0 tel que :
$\forall k \geq k_0, \|\nu_k^*\| > M$,
alors $\{x \in \mathcal{L}' / \|x\| \leq M\} \subset \mathbb{Z}(\nu_1, \ldots, \nu_{k_0-1})$.

Dans notre cas $M = n$, et on pose :
$\mathcal{L}'_1 = \mathbb{Z}(\nu_1, \ldots, \nu_{k_0-1}) \subset \mathcal{L}'_0$.
$\mathcal{L}_1 = \pi_{\mathbb{Z}^n}(\mathcal{L}'_1) \subset \mathcal{L}_0$.

Test d'arrêt

Remarque : La matrice M_V des coordonnées des 0-1 vecteurs $v_i \in V$ a la propriété :
($\star$) Chaque colonne de M a une coordonnée égale à 1 et toutes les autres sont nulles.

Test d'arrêt : Si $RREF(\mathcal{L}_i)$ a la propriété ($\star$) alors on arrête le calcul de la suite $(\mathcal{L}_i)_{i\in\mathbb{N}}$.

L'ALGORITHME

1. Calculer les y_i, a_i, b_i.
2. Trouver V.
3. On a $P_k(X,Y) = \prod_{I_k}(Y - y_i - a_i(X-x_0) - b_i(X-x_0)^2) \mod (X-x_0)^3$.
   Retrouver P_k à l'aide d'une remontée de Hensel.

Conclusion

Détails cachés :

1. Nous avons des valeurs approchées pour y_i, a_i, b_i...
2. Etudier $\Re(b_i)$ permet de réduire la taille du réseau...

Un exemple :

Cet algorithme a permis de factoriser un polynome $P(X, Y)$ tel que :
$tdeg(P) = 120$,
P a 1268 monomes,
taille moyenne des coefficients : 5.10^7,
taille maximum des coefficients : 3.10^9.