Algorithmes de la
Géométrie Algébrique Réelle

Marie-Françoise Roy
CNRS, Université de Rennes, France
FRISCO (Projet Esprit CEE)

Systèmes d'équations polynomiales

Exemple très simple
cubique $y^2 = x^3 - x$; droite $x = t$
complexe, toujours deux points d'intersection sauf pour $t = -1, 0, 1$ (tangence)
réel, plus compliqué
a) pas toujours d'intersection
b) invariant: la parité du nombre d'intersections (sauf si tangence)
c) les t pour lesquels il y a intersection

$$x^3 - x \geq 0$$

Systèmes d' inégalités polynomiales

Trois grand problèmes

I Décider l'existence de solutions pour des égalités et des inégalités

(pour les entiers : indécidable
10-ème problème de Hilbert,
NON, Y. Mattiassevitch, 1973).

pour les réels, décidable
Tarski 1939 .

II 16-ème problème de Hilbert

équation $P(X,Y)$ de degré d,
types topologiques possibles
des zéros de P
(connu jusqu'au degré 7)

17-ème problème de Hilbert

un polynôme positif est-il somme de carrés ?
pas somme de carrés de polynômes,
somme de carrés de fractions rationnelles
Artin 1925

Concepts clés en algorithmique

effectivité
existence d'un algorithme

complexité
taille du calcul en fonction de la taille des entrées

efficacité
jusqu'à quelle taille des entrées ca marche

Dans cette série d'exposés

Compter le nombre de racines réelles

Calculer la topologie d'une courbe plane

Décider l'existence de solutions pour des égalités et des inégalités

Retour sur les sommes de carrés

Dans les exposé complémentaires

Constructions de courbes algébriques réelles
Ilia Itenberg

Calculs efficaces
Fabrice Rouillier

-

Compter le nombre de racines réelles

$$A = a_1 X^{d(1)} + \ldots + a_\ell X^{d(\ell)}$$

$(d(1) > \ldots > d(\ell),\ a_i \neq 0)$

nombre de racines positives
(avec multiplicités) :
plus petit que le nombre
de changements de signes
dans les coefficients de A,
égal module 2

pas de calculs
réponse très partielle

si peu de monômes,
peu de racines réelles

méthode d'isolation

Méthode d'isolation (Uspensky)

ramener les racine positives sur $[0,1]$ (homothétie), faire le changement de variable $X \mapsto X/2$, puis le changement de variables $X \mapsto X+1$

tant que le nombre de changements de signes dans les coefficients du nouveau polynôme n'est pas 0 ou 1, continuer

le processus s'arrête (théorème de Vincent)

si c'est 0, pas de racine sur $[0,1]$, si c'est 1,une racine

en revenant au polynôme de départ on a décidé l'existence d'une racine sur un sous-intervalle

Dichotomie (archimédianité)

Sturm (1837)
et la division euclidienne avec signe

Algorithme St
Initialisation:

$$St^0 := A, St^1 := A'$$

Etape suivante:

$$Sy^i = -\mathrm{Rem}(St^{i-2}, St^{i-1})$$

Fin: L'algorithme termine avec St^w, le PGCD (signé) de A et A'.

Nombre de racines réelles = différence entre les nombres de variations de signes en $-\infty$ et $+\infty$

$$x^3 - ax$$

$$3x^2 - a$$

$$2ax$$

$$a$$

Si $a > O$

$$-\infty : -, +, -, +$$

$$+\infty : +, +, +, +$$

3-0=3 racines.

Si $a < O$

$$-\infty : -, +, +, -$$

$$+\infty : +, +, -, -$$

2-1=1 racine.

Si $a = 0$

$$-\infty : -, +, 0, 0$$

$$+\infty : +, +, 0, 0$$

1-0=1 racine

Autres problèmes similaires

Nombre de racines
avec contraintes polynomiales

nombre de racines de A où C est positif- nombre de racines de A où C est négatif

Domaine de stabilité

nombre de racines complexes avec partie rélle négative

Signature d'une matrice de Haenkel

Indice de Cauchy

nombre de sauts de $\frac{B}{A}$ de $-\infty$ à $+\infty$
- nombre de sauts de $+\infty$ à $-\infty$

$B = A'$ nombre de racines réelles,

$B = A'C$, contraintes polynomiales

A et B parties réelles et imaginaires de $P(it)$: domaine de stabilité

Algorithm Sy

Initialisation:

$$Sy^0 := A, Sy^1 := B$$

Etape suivante:

$$Sy^i = -\mathrm{Rem}(Sy^{i-2}, Sy^{i-1})$$

Fin: L'algorithme termine avec St^w, le PGCD (signé) de A et B.

indice de Cauchy= différence
des nombres de variations de signes
en $-\infty$ et $+\infty$ dans cette suite

1 : calculs algébriques.
2 : discussions de signes .

valable dans un corps réel clos quelconque
(tout nombre positif est un carré, tout polynôme de degré impair a une racine)
(pas forcément archimédien)

calculs rationnels (dans le corps des coefficients du polynôme, pas dans le corps où on compte les racines)

on calcule sur les entiers on a une réponse sur les réels

pas de problème d'effectivité

Taille de la sortie
tous les restes successifs
A et B de degré d
Sortie de taille $O(d^2)$

Complexité de l'algorithme
$O(d^2)$ opérations arithmétiques

Problèmes
Tailles d'entiers
Spécialisation

Exemple

$$\mathrm{Stu}^0(A) = X^4 + pX^2 + qX + r$$
$$\mathrm{Stu}^1(A) = 4X^3 + 2pX + q$$
$$\mathrm{Stu}^2(A) = \frac{-(2pX^2 + 3qX + 4r)}{4}$$
$$\mathrm{Stu}^3(A) = \frac{1}{p^2} - ((2p^3 - 8pr + 9q^2)X + \\ + p^2q + 12qr)$$
$$\mathrm{Stu}^4(A) = \frac{p^2}{4(2p^3 - 8pr + 9q^2)^2} \cdot \\ \cdot (16p^4r - 4p^3q^2 - \\ -128p^2r^2 + 144pq^2r - 27q^4 + 256r^3)$$

Si $p = 0$, calcul à refaire.

$$\mathrm{Stu}^0(A) = X^4 + qX + r$$
$$\mathrm{Stu}^1(A) = 4X^3 + q$$
$$\mathrm{Stu}^2(A) = \frac{-(3qX + 4r)}{4}$$
$$\mathrm{Stu}^3(A) = \frac{-(27q^4 - 256r^3)}{27q^3}$$

Pas obtenue en faisant $p = 0$ dans la suite de Sturm .

Sous résultants (Sylvester-Habicht) dans le cas usuel (degrés baissent de 1 en 1), petite modification de Sylvester.

Algorithme SyHaUsuel (Habicht 1948)

Initialisation: $d := \deg(A)$,

$$H_d := A, H_{d-1} := B$$

$$H_{d-2} = -\mathrm{Rem}(h_{d-1}^2 H_d, H_{d-1})$$

Prochaine étape ($j < d$):

$$H_{j-2} = -\frac{1}{h_j^2}\mathrm{Rem}(h_{j-1}^2 H_j, H_{j-1})$$

Fin: H_0

Plus de dénominateurs

Tailles d'entiers raisonnables

Bonnes propriétés de spécialisation

$$\begin{aligned}
\mathrm{StHa}_4(A) &= X^4 + pX^2 + qX + r\\
\mathrm{StHa}_3(A) &= 4X^3 + 2pX + q\\
\mathrm{StHa}_2(A) &= -4(2pX^2 + 3qX + 4r)
\end{aligned}$$

$$\mathrm{StHa}_1(A) =$$
$$-4((2p^3 - 8pr + 9q^2)X + +p^2q + 12qr)$$
$$\mathrm{StHa}_0(A) = 16p^4r - 4p^3q^2 -$$
$$-128p^2r^2 + +144pq^2r - 27q^4 + 256r^3$$

Si $p = 0$, pas besoin de refaire les calculs

$$\begin{aligned}
\mathrm{StHa}_4(A) &= X^4 + qX + r\\
\mathrm{StHa}_3(A) &= 4X^3 + q\\
\mathrm{StHa}_2(A) &= -4(3qX + 4r)\\
\mathrm{StHa}_1(A) &= -12q(3qX + 4r)\\
\mathrm{StHa}_0(A) &= -27q^4 + 256r^3
\end{aligned}$$

cas général, structure de saut
(Habicht 1948)

Algorithme SyHa
(Lickteig R 1996)
Initialisation:

$$H_d := A, H_{d-1} := B,$$

$$\bar{h}_d := {a_d}^{-1}$$

Prochaine etape:

$$H_\ell = 0$$

pour $j-2 \leq \ell \leq k+1$
Si $k = j-1$, rien à calculer.
Si $k < j-1$, c_{j-1} coefficient dominant de H_{j-1}.

$$\bar{h}_{j-1} = c_{j-1},$$

$$\ldots,$$

$$\bar{h}_\ell = (-1)^{j-\ell-1} \cdot \frac{\bar{h}_{\ell+1} c_{j-1}}{\bar{h}_j}, \ldots .$$

$$H_k = \frac{\bar{h}_k H_{j-1}}{c_{j-1}}$$

$$H_{k-1} =$$

$$= -\frac{1}{h_j \bar{h}_j} \mathrm{Rem}(c_{j-1} h_k H_j, H_{j-1}).$$

Fin: H_0

indice de Cauchy= différence
des nombres de variations de signes
en $-\infty$ et $+\infty$ dans cette suite

Clair dans le cas usuel
(proportionnel à Sylvester avec des carrés)
aussi vrai en général

Complexité en nombres d'opérations arithmétiques

$O(d^2)$

Taille d'entiers controlée:
le déterminant d'une matrice de taille $O(d)$ avec entrées de tailles binaires τ est de taille binaire $O(d(\tau + log(d))$ (inégalité d'Hadamard)

Linéaire en d

Conséquence dans la suite des restes
Taille quadratique en d
(Lickteig R 1997)

restes non nécessaires.
signes des restes :
taille de la sortie $0(d)$.

Comment calculer les signes des restes sans calculer les restes ?

Idée (Schoenhage, Monk):
botte des quotients et PGCD
quotients et PGCD : seulement $0(d)$ coefficients, les valeurs des restes en un point (donc les signes) se calculent facilement grâce aux GCD et aux quotients

Comment calculer les quotients sans calculer les restes?

Idée: le quotient de A et B dépend seulement des termes dominants de A et B : on peut appliquer un algorithme de diviser pour régner: $d\log(d)^2$ opérations arithmétiques. Controle de la taille des coefficients dans l'algorithme (linéaire)

Adaptation de l'idée de Schoenhage et Monk aux sous-résultants (Lickteig R 96)
Matrices de transition pour les sous résultants

Bornes inférieures ?

Strassen : botte des quotients et PGCD $O(d\log(d))$ au moins (arguments de degré, beauoup de schémas possible pour les chutes de degrés)

Lickteig R signes des restes $O(d\log(d))$ nécessaires 1996 (adaptation de Strassen aux inégalités, utilise le spectre réel (algèbre réelle abstraite)

assez satisfaisant $d\log^2 d$ d'un côté, $d\log(d)$ de l'autre

-

Calcul de la topologie d'une courbe
Collins 1975
El Kahoui, Gonzalez-Vega, 1996

Idée : décomposer l'axe des X en segments et points ou rien de change
Décomposition algébrique cylindrique

$D(X)$: éliminer Y entre
$P(X,Y)$ et $\dfrac{\partial P}{\partial Y}(X,Y)$:
déterminant de la matrice de Sylvester
$P_x(Y) = P(x,Y)$
$D(x) \neq 0$ si et seulement si

$$PGCD(P_x, \left(\frac{\partial P}{\partial Y}\right)_x) = 1$$

$D(x) = 0$ si et seulement si $P_x(Y)$ a une racine double

géométriquement au dessus de x
existence d'un point spécial
* soit un point critique

$$P_x(y) = \left(\frac{\partial P}{\partial Y}\right)_x(y) = O$$
$$\left(\frac{\partial P}{\partial X}\right)_x(y) \neq O$$

* soit un point singulier

$$P_x(y) = \left(\frac{\partial P}{\partial Y}\right)_x(y) = \left(\frac{\partial P}{\partial X}\right)_x(y) = O$$

Si la courbe est bien placée (position générale), un seul point spécial au dessus d'une racine de D

Comment caractériser les racines

Première possibilité (archimédien)
méthode d'Uspenski

Deuxième possibilité (toujours)
Lemme de Thom
Soit x un élément de R
et $\sigma(x) = (\sigma_0, \sigma_1, \ldots, \sigma_{d-1)}$
la suite des signes de

$$A, A', \ldots, A^{(i)}, \ldots, A^{(d-1)}$$

en x
Si x est racine de A et $y \neq x$, $\sigma(y) \neq \sigma(x)$

Codage à la Thom
Calculer les conditions de signes non vides portant sur

$$A, A', \ldots, A^{(d-1)}$$

en calculant diverses suites de Sylvester-Habicht de A et $A'C$ où C est un produit de dérivées de A (contraintes polynomiales)

Déterminer le signe d'un autre polynôme en une racine de A encore Sylvester-Habicht

Etape 1 Position générale ?
Calculer la suite de Sturm- Habicht de $P(X, Y)$
dernier polynôme: discriminant D
position générale si et seulement si pour toute racine x de D,

$$B_x(Y) = PGCD(P_x, \left(\frac{\partial P}{\partial Y}\right)_x)$$

est de la forme $(Y - u(x))^\mu$
$B_x(Y)$ est le dernier polynôme non nul de la suite de Sturm-Habicht
Si pas en position générale, changer les axes
Au hasard ca marche,
Borner le nombre d'essais.

2 *En position générale*

On a déjà Sturm-Habicht

On caractérise les racines de D et on les ordonne

Au dessus de chaque racine, point spécial

calcul des autres racines au dessus de x- toutes simples

ordonner avec point spécial

Entre deux racines de D combien de racines de $P(X,Y)$ par Sturm-Habicht

On recolle l'information pour avoir la topoloige

Complexité polynomiale en d et τ

Marche pour de gros exemples

Théorie Existentielle des Réels

s polynômes

$\mathcal{P} = \{P_1, P_2, \ldots, P_s\}$

k variables, $X_1, \ldots, X_k$

degrés au plus d

coefficients dans $D \subset R$

Théore Existentielle des Réels

$\exists (X_1, \ldots, X_k) F(P_1, \ldots, P_s)$

$F(P_1, \ldots, P_s)$ sans quantificateurs

OUI ou NON.

Tarski: dédicable.

Calculs dans l'anneau D.

Exemple $X^4 + pX^2 + qX + r$ a 4 racines réelles si et seulement si il y a 4 variations en $-\infty$ et O en $+\infty$ dans le suite de Sturm ce qui signifie

$$p < 0$$
$$(2p^3 - 8pr + 9q^2) < 0$$
$$16p^4r - 4p^3q^2 - 128p^2r^2 +$$
$$144pq^2r - 27q^4 + 256r^3 > 0$$

De même pour 0 et 2 racines, on peut écrire les conditions.
On s'est ramené à des conditions de signes portant sur une variable de moins.

Trouver des points tests

$$\mathcal{P} = \{P_1, \ldots, P_s\}$$
condition de signe $\sigma \in \{-1, 0, 1\}$ non-vide
$$\exists x \in R^k$$
$$(\mathbf{sign} P_1(x), \ldots, \mathbf{sign} P_s(x)) = \sigma.$$

Calculer la liste
des conditions de signes non vides.
Calculer un point dans chaque
composante connexe
de chaque condition de signe non vide.

Décomposition Algébrique Cylinrique
Tarski pour montrer la décidabilité de TER.
Améliorée plus tard par Collins avec les sous-resultants

Eliminer les variables une à une.
Très simple en principe

Point faible:
degrés dans les paramètres.
Du degré d au degré $2d^2$.
Doublement exponentiel
dans le nombre des variables.
Marche bien pour les courbes (deux variables).

Combien de composantes connexes de conditions de signes non vides ?

a priori 3^s
Cas linéaire $\binom{0(s)}{k}$
En général $\binom{0(s)}{k}0(d)^k$

Warren, Allon, Canny, Renegar
Pollack-R
Simplement exponentiel.

Position générale
nombre maximum de cas
en utilisant des déformations
infinitésimales

$k + 1$ polynômes
en position générale
n'ont pas de zéros en commun

Considérer seulement
des ensembles algébriques

Proposition

C composante connexe de
$P_1 = \ldots = P_m = 0,$
$P_{m+1} \geq 0, \ldots, P_s \geq 0$

$\exists\ \ell_{m+1} \ldots \ell_{m'}$
$\exists\ D$ composante connexe de
$P_1 = \ldots = P_m = 0,$
$P_{\ell_{m+1}} = \ldots, P_{\ell_{m'}} = 0$

$D \subset C$

Compter les composantes connexes
d'ensembles algébriques
Petrowsky, Oleinik, Thom, Milnor
degré d, k variables

$$O(d)^k$$

Méthode des points critiques
théorème de Bezout

Nombre de cas
(position générale)

$$\binom{0(s)}{k}$$

Algorithme pour trouver despoints

complexité

$$\binom{O(s)}{k} d^{O(k)}$$

(Basu-Pollack-R)

utilise
des déformations infinitésimales
la méthode des points critiques
la résolution des systèmes polynomiaux
le comptage des racines réelles

Sur une sous-variété de dimension k'
Nombre $\binom{0(s)}{k'} 0(d)^k$
Complexité
$$\binom{O(s)}{k'} d^{O(k)}$$
(Basu-Pollack-R)

Problèmes
Elimination des quantificateurs
Décision pour la connexité
Composantes connexes

Problèmes ouverts (complexité)
Calcul de dimension réelle
Calcul d'une stratification

Retour sur les sommes de carrés
Positivstellensatz (Stengle 1974)

$$A_i > 0, B_j = 0, C_k \geq 0$$

n'a pas de solutions si et seulement si il existe A, B, C avec A produit de A_i, B dans l'idéal des B_j, C dans le cone engendré par B_j, C_k
(cone: stable par addition et multiplication, contient les carrés)

$$A + B + C = 0$$

certificat algébrique d'impossiblité effectif (Lombardi 1992)
Redonne: positif est somme de carrés de fraction rationnelles

Complexité du Positivstellensatz ?
Lombardi, R (travail en cours)
Tour d'exponentielle de hauteur 5

Programme de travail dans le futur:
le cas p-adique
Equivalent de la décomposition algébrique cylindrique : Cohen
Equivalentdu 17-ème problème de Hilbert, Kochen