Effectivité et complexité du 17ème problème de Hilbert

Marie-Françoise Roy
Université de Rennes

Séminaire Philosophie et Mathématique
4 Mai, 2026

Positivité et sommes de carrés

- Un polynôme à coefficients réels qui prend toujours des valeurs positives ou nulles est-il une somme de carrés de polynômes?
- L'écriture comme somme de carrés est un certificat de positivité.
- Oui si le nombre de variables est 1.
- Indication : décomposer le polynôme en produit de facteurs irréductibles: les facteurs de degré deux (correspondant aux racines complexes) sont sommes de carrés, les facteurs de degré 1 (correspondant aux racines réelles) sont à une puissance paire. Les produits de sommes de carrés sont des sommes de carrés
- Oui si le degré est 2 et le nombre de variables quelconque.
- Indication: une forme quadratique prenant seulement des valeurs positives ou nulles est une somme de carrés de polynômes linéaires.

Positivité et sommes de carrés

- Un polynôme à coefficients réels qui prend toujours des valeurs positives ou nulles est-il une somme de carrés de polynômes?
- Oui si le nombre de variables est 1.
- Oui si le degré est 2 et le nombre de variables quelconque.
- Aussi si le nombre de variable est 2 et le degré est 4 (Hilbert).
- Non dans tous les autres cas.
- Premier contre-exemple explicite Motzkin 69

$$1 + X^4Y^2 + X^2Y^4 - 3X^2Y^2$$

prend des valeurs positives ou nulles et n'est pas somme de carrés de polynômes.

- C'est Olga Taussky-Todd qui en a fait la remarque, Théodore Motzkin ne s'en était pas aperçu.

Olga Taussky-Todd (1906-1995)

Contre exemple de Motzkin (degré 6, 2 variables)

$$M = 1 + X^4Y^2 + X^2Y^4 - 3X^2Y^2$$

- M prend seulement des valeurs positives ou nulles. Indication: la moyenne arithmétique est toujours au moins égale à la moyenne géométrique.
- M n'est pas une somme de carrés de polynômes. Indication : essayer de l'écrire comme une somme de carrés de polynômes de degré 3 et vérifier que c'est impossible.
- Exemple: le monome X^3 ne peut pas apparaitre dans la somme de carrés. Etc ...

Le 17ème problème de Hilbert

- Reformulation proposée par Hermann Minkowski.
- Question David Hilbert Congrès de Paris, 1900.
- Un polynôme à coefficients réels qui prend toujours des valeurs positives ou nulles est-il une somme de carrés de fractions rationnelles?
- Aussi un certificat de positivité
- Artin 27: Réponse affirmative. Preuve non-constructive.

Le Nullstellensatz

Certificat exprimant qu'un ensemble algébrique est vide.
K un corps, C une extension algébriquement close de K,

$$P_1, \ldots, P_s \in \mathrm{K}[x_1, \ldots, x_k]$$
$$P_1 = \ldots = P_s = 0 \text{ n'a pas de solution dans } \mathrm{C}^k$$
$$\Longleftrightarrow$$
$$\exists \quad (A_1, \ldots, A_s) \in \mathrm{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$$

Grete Hermann (1901-1984)

Le Nullstellensatz

Principe de la preuve: par récurrence sur le nombre de variables.
On introduit une variable annexe U et on considère le résultant de P_1 et $P_2 + UP_3 + \ldots + U^{s-2}P_s$ par rapport X_k; ses coefficients en U sont des polynômes en $X_1, \ldots, X_{k-1}$ qui appartiennent à l'idéal engendré par $P_1, \ldots, P_s$ et ont une racine commune dans C^{k-1} si et seulement si $P_1, P_2, \ldots, P_s$ ont une racine dans C^k.
En éliminant les variables une à une : s'il n'y a pas de zéros communs, 1 est dans l'idéal engendré par $P_1, \ldots, P_s$.
Et on peut tracer les degrés des polynômes calculés en fonction de la complexité de l'entrée (degrés, nombre de polynômes et nombre de variables). Donne des bornes doublement exponentielles dans le nombre de variables puisque le degré des coefficients du résultant est quadratique par rapport au degré des polynômes de départ.
Travail fondateur de la complexité en calcul formel.

Schéma de la preuve d'Artin

- Supposons que P n'est pas une somme de carrés de fractions rationnelles.
- Les sommes de carrés forment un cone propre du corps des fractions rationnelles qui ne contient pas P (un cone contient les carrés et est clos par addition et multiplication, un cone propre ne contient pas -1).
- En utilisant le lemme de Zorn, on obtient un cone propre maximal du corps des fractions rationnelles qui ne contient pas P. Un tel cone maximal correspond à un ordre total $(\star)$ sur le corps des fractions rationnelles pour lequel P est négatif.

Schéma de la preuve d'Artin

- Supposons que P n'est pas une somme de carrés de fractions rationnelles.
- Les sommes de carrés forment un cone propre du corps des fractions rationnelles.
- Par Zorn, on obtient un ordre total $(\star)$ sur le corps des fractions rationnelles où P est négatif.
- Un cops réel clos est un corps totalement ordonné où TVI est valide (Théorème des Valeurs Intermédiaires pour les polynômes). Par exemple le corps $\mathbb{R}$ des nombres réels.
- Tout corps totalement ordonné a une clôture réelle.
- En prenant la clôture réelle du corps des fractions rationnelles pour l'ordre $(\star)$, on obtient un corps dans lequel P prend une valeur négative (quand on l'évalue au "point générique" $=$ le point $(X_1, \ldots, X_k)$).

Schéma de la preuve d'Artin

- Supposons que P n'est pas une somme de carrés de fractions rationnelles.
- Les sommes de carrés forment un cone propre du corps des fractions rationnelles.
- Par Zorn, on obtient un ordre total $(\star)$ sur le corps des fractions rationnelles où P est négatif.
- En prenant la clôture réelle du corps des fractions rationnelles pour l'ordre $(\star)$, on obtient un corps dans lequel P prend une valeur négative (quand on l'évalue au "point générique" $=$ le point $(X_1, \ldots, X_k)$).
- Alors P prend des valeurs négatives sur les nombres réels Premier exemple du principe de transfert en géométrie algébrique réelle.

Principe de Transfert

- Soit R un corps réel clos.
- Un énoncé faisant intervenir des éléments de R qui est vrai dans un corps réel clos contenant R est vrai dans R.
- Par exemple la clôture réelle de $\mathbb{R}(X_1, \ldots, X_k)$ pour l'ordre total $(\star)$, qui contient $\mathbb{R}$.
- Pas tout énoncé, seulement un "énoncé de la logique du premier ordre".
- Exemple d'un tel énoncé

$$\exists x_1 \ \ldots \ \exists x_k \ P(x_1, \ldots, x_k) < 0$$

est vrai dans un corps réel clos R' contenant R si et seulement si il est vrai dans R.

- Cas particulier d'élimination des quantificateurs.

Qu'est ce que l'élimination des quantificateurs ?

Déjà vu au lycée

$$\exists \quad x \quad ax^2 + bx + c = 0, a \neq 0$$

$$\Longleftrightarrow$$

$$b^2 - 4ac \geq 0, a \neq 0$$

Si a, b, c sont des nombres, la formule est vraie ou fausse suivant le signe de $b^2 - 4ac$.
Si a, b, c sont des paramètres, on a trouvé une condition de signe sur les paramètres qui remplace la formule. Le quantificateur est éliminé.
Valide pour toute formule, dû à Tarski.

Soit K un corps ordonné et R un corps réel clos contenant K Soit $P \in \mathrm{K}[X]$, unitaire, avec $\deg P = p \geq 1$. On note $\mathrm{Tra}(A)$ la trace de l'application linéaire de la multiplication by $A \in \mathrm{K}[X]$ dans le R-espace vectoriel $\mathrm{K}[X]/P$.

Définition (matrice d'Hermite)

La matrice d'Hermite $\mathrm{Her}(P;1) \in \mathrm{K}^{p\times p}$ *correspond à la forme quadratique associant à* $(f_0, f_1, \ldots, f_{p-1})$

$$\mathrm{Tra}((f_0 + f_1X + \ldots + f_{p-1}X^{p-1})^2).$$

La matrice d'Hermite se calcule facilement à partir des coefficients de P, ses entrées correspondent aux sommes de Newton (moments) de P.
Son déterminant est le discriminant de P.

Définition (matrice d'Hermite généralisée)

Soient $P, Q \in \mathrm{K}[X]$ *avec* $\deg P = p \geq 1$, P *unitaire. La matrice d'Hermite généralisée* $\mathrm{Her}(P;Q) \in \mathrm{K}^{p\times p}$ *correspond à la forme quadratique associant à* $(f_0, f_1X, \ldots, f_{p-1})$

$$\mathrm{Tra}(Q(X)(f_0 + f_1X + \ldots + f_{p-1}X^{p-1})^2).$$

La matrice d'Hermite généralisée se calcule facilement à partir des coefficients de P et Q, ses entrées correspondent à des combinaisons linéaires des sommes de Newton (moments) de P. Son déterminant est le discriminant de P mutiplié par le résultant de P et Q.

La méthode d'Hermite

Théorème (Théorie d'Hermite)

Soient $P, Q \in \mathrm{K}[X]$ *avec* $\deg P = p \geq 1$, P *unitaire. Alors*

$$\mathrm{TaQu}(P, Q) = \mathrm{Si}(\mathrm{Her}(P; Q))$$

où

$$\mathrm{TaQu}(P, Q) := \sum_{x \in \mathrm{R} \mid P(x)=0} \mathrm{sign}(Q(x)),$$

est la requête de Tarski et $\mathrm{Si}(\mathrm{Her}(P; Q))$ *est la signature de la matrice symétrique* $\mathrm{Her}(P; Q)$.

Indication de preuve: pour $\mathbb{R}$ faire intervenir les racines complexes. Egalement vrai pour un corps réel clos quelconque, voir détails plus tard.

La méthode d'Hermite

Notation

Soient $P, Q \in \mathrm{K}[X]$ *avec* $\deg P = p \geq 1$, P *unitaire. Pour* $0 \leq j \leq p-1$, *on note* $\mathrm{HMi}_j(P;Q)$ *le* $(p-j)$*-ème mineur principal de* $\mathrm{Her}(P;Q)$, *avec* $\mathrm{HMi}_p(P;Q) = 1$. *On note* $\mathrm{HMi}(P;Q)$ *la liste*

$$[\mathrm{HMi}_0(P;Q), \ldots, \mathrm{HMi}_p(P;Q)] \subset \mathrm{R}.$$

Les signes des $\mathrm{HMi}(P;Q)$ (qui sont dans K) déterminent la signature, et donc la requête de Tarski.
Les calculs sont dans K, les informations obtenues dans R.

Détermination de Signe

- K un corps ordonné (ex: $\mathbb{Q}$), R un corps réel clos le contenant (ex: $\mathbb{R}$, $\mathbb{R}_{\mathrm{alg}}$)
- un polynôme non nul en une variable P et une liste d'autres polynômes $Q_1, \ldots, Q_s$ tous dans $\mathrm{K}[X]$
- trouver la liste des conditions de signes non vides (i.e. des éléments de $\{0, 1, -1\}^s$) saisfaites par $Q_1, \ldots, Q_s$ aux racines réelles de P (i.e. racines dans R)

Cas particulier 1: compter les racines

- un polynôme non nul en une variable $P \in \mathrm{K}[X]$
- décider si P a une racine réelle (i.e. une racine dans R) ou pas
- variante: compter aussi le nombre de racines de P dans R
- par Hermite avec $Q = 1$.

Cas particulier 2: un seul polynôme

- un polynôme non nul en une variable $P \in \mathrm{K}[X]$ et un autre polynôme $Q \in \mathrm{K}[X]$
- décider les signes de Q aux racines de P dans R (variante: compter le nombre de ces racines)
- outil : requête de Tarski

$$\mathrm{TaQu}(P, Q) := \sum_{x \in \mathrm{R} \mid P(x)=0} \mathrm{sign}(Q(x))$$

Cas particulier 2: un seul polynôme

$c(P = 0, Q = 0)$ est le nombre de racines de P dans R où $Q = 0$ etc

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} c(P = 0, Q = 0) \\ c(P = 0, Q > 0) \\ c(P = 0, Q < 0) \end{bmatrix} = \begin{bmatrix} \mathrm{TaQu}(P, 1) \\ \mathrm{TaQu}(P, Q) \\ \mathrm{TaQu}(P, Q^2) \end{bmatrix}$$

La matrice est celle des signes de $1, Q_1, Q_1^2$ lorsque Q_1 est nul, positif ou négatif.
Calculer trois requêtes de Tarski, calculer trois cardinalités et décider quelles sont les conditions de signes non vides.

Cas particulier 3: deux polynômes

Avec $s = 2$, la matrice des signes est

$$\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & -1 & -1 & -1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 \\
0 & 0 & 0 & 0 & 1 & -1 & 0 & -1 & 1 \\
0 & 0 & 0 & 0 & 1 & -1 & 0 & 1 & -1 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & -1 & -1 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1
\end{bmatrix}$$

et est inversible.

Calculer 9 requêtes de Tarski en déduire les cardinalités des 9 conditions de signe. Voir lesquelles sont non vides.

Cas général

- calculer les requêtes de Tarski de P et des produits des Q_i ou de leurs carrés (en utilisant la méthode d'Hermite)
- résoudre un système linéaire sur K, ce qui donne les cardinalités des conditions de signes aux racines de P dans R,
- donc les conditions de signes non vides

Le fait que la matrice est inversible se prouve par induction sur s.
Le nombre des requêtes de Tarski à calculer est exponentiel en s.

Détermination de signe et élimination des quantificateurs

- $P[u][X], Q_1[u][X], \ldots, Q_s[u][X]$ sont des polynômes dans les paramètres u et la variable principale X
- Calculer des polynômes en u dont les signes fixent la liste des conditions de signe non-vides réalisées par $Q_1[u][X], \ldots, Q_s[u][X]$, aux racines de $P[u][X]$ (mineurs de matrices de Hermite)
- éliminer une variable correspond à la détermination de signes avec des paramètres.
- Quand il n'y a que des signes stricts on rajoute comme égalité la dérivée du produit.

L'algorithme d'élimination des quantificateurs de Tarski est essentiellement la détermination de signes avec paramètres [BPR] .

Primitif récursif/élémentairement récursif

- fonctions primitives récursives obtenues à partir de 0, successeur, choix d'un coordonnée, composition and récursion
- exemple: addition à partir de successeur, multiplication à partir de l'addition, exponentiation à partir de la multiplication en utilisant la récursion
- exemple: la fonction associant à n une tour d'exponentielle de hauteur n. $f(0) = 2$, $f(1) = 2^2$, $f(2) = 2^{2^2}$ ... facile à construire en utilisant la récursion
- fonctions élémentairement récursives obtenues à partir de l' addition, la multiplication, la soustraction et la division par choix d'une coordonnée, composition, sommes et produits finis. Typiquement: fonction exponentielle 2^n, doublement exponentielle 2^{2^n}, tour d'exponentielle de hauteur fixée (exemple: 4 ou 5).

Primitif récursif/élémentairement récursif

Nous avons vu deux exemples

- complexité doublement exponentielle (donc élémentairement récursive) pour la preuve effective du Nullstellensat par Grete Hermann: quand on élimine une variable le degré passe de d à d^2.
- complexité primitive récursive pour l'élimination des quantificateurs de Tarski: quand on élimine une variable le nombre de polynômes passe de s à 3^s.

Les questions qui restent

- Preuve d'Artin très indirecte (par contraposition, usage de Zorn).
- Aucune indication sur les dénominateurs: quelles sont les bornes sur les degrés?
- Emil Artin note que l'efficacité est désirable mais difficile.
- Problème de décidabilité : Y a t-il un algorithme qui décide si un polynôme ne prend que des valeurs négatives ? Oui grâce à un algorithme d'élimination des quantificateurs.
- Problème d'effectivité : Pouvons nous utiliser cet algorithme pour obtenir une représentation comme somme de carrés?
- Problème de complexité : Quelles bornes sur les degrés ?

Positivstellensatz (Krivine 64, Stengle 74)

Il est utile de généraliser.

- Trouver des identités algébriques certifiant qu'un système de conditions de signe n'a pas de solutions.
- On a déjà vu le Nullstellensatz.
  K un corps, C une extension algébriquement close de K,
  $P_1, \ldots, P_s \in \mathrm{K}[x_1, \ldots, x_k]$

$$P_1 = \ldots = P_s = 0 \text{ n'a pas de solution dans } \mathrm{C}^k$$

$$\Longleftrightarrow$$

$$\exists \quad (A_1, \ldots, A_s) \in \mathrm{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$$

- Pour les inégalités, l'énoncé est plus compliqué.

Positivstellensatz

- K un corps ordonné, R un corps réel clos extension de K,
- $P_1, \ldots, P_s \in \mathrm{K}[x_1, \ldots, x_k]$,
- $I_{\neq}, I_{\geq}, I_{=} \subset \{1, \ldots, s\}$,

$$\begin{cases} P_i(x) \neq 0 & \text{pour} \quad i \in I_{\neq} \\ P_i(x) \geq 0 & \text{pour} \quad i \in I_{\geq} \\ P_i(x) = 0 & \text{pour} \quad i \in I_{=} \end{cases}$$ n'a pas de solution dans R^k

$$\Longleftrightarrow$$

$$\exists \quad S = \prod_{i \in I_{\neq}} P_i^{2e_i}, \qquad N = \sum_{I \subset I_{\geq}} \Big(\sum_j k_{I,j} Q_{I,j}^2\Big) \prod_{i \in I} P_i \quad (k_{I,j} > 0),$$

$$Z \in \langle P_i \mid i \in I_{=} \rangle \subset \mathrm{K}[x$$

tel que $$\underbrace{S}_{>0} + \underbrace{N}_{\geq 0} + \underbrace{Z}_{=0} = 0.$$

Incompatibilités

$$\mathcal{H}(x): \begin{cases} P_i(x) & \neq & 0 & \text{pour} & i \in I_{\neq} \\ P_i(x) & \geq & 0 & \text{pour} & i \in I_{\geq} \\ P_i(x) & = & 0 & \text{pour} & i \in I_{=} \end{cases}$$

$$\downarrow \mathcal{H} \downarrow : \quad \underbrace{S}_{>0} + \underbrace{N}_{\geq 0} + \underbrace{Z}_{=0} = 0$$

avec

$S \in \left\{ \prod_{i \in I_{\neq}} P_i^{2e_i} \right\}$ $\leftarrow$ monoide associé à $\mathcal{H}$

$N \in \left\{ \sum_{I \subset I_{\geq}} \left(\sum_j k_{I,j} Q_{I,j}^2 \right) \prod_{i \in I} P_i \right\}$ $\leftarrow$ cone associé à $\mathcal{H}$

$Z \in \langle P_i \mid i \in I_{=} \rangle$ $\leftarrow$ idéal associé à $\mathcal{H}$

le Positivstellensatz implique le 17ème problème de Hilbert

$$P \geq 0 \text{ dans } \mathbb{R}^k \iff P(x) < 0 \text{ pas de solution}$$

$$\iff \begin{cases} P(x) \neq 0 \\ -P(x) \geq 0 \end{cases} \text{ pas de solution}$$

$$\iff \underbrace{P^{2e}}_{>0} + \underbrace{\textstyle\sum_i Q_i^2 - (\sum_j R_j^2)P}_{\geq 0} = 0$$

$$P = \frac{P^{2e} + \sum_i Q_i^2}{\sum_j R_j^2} = \frac{(P^{2e} + \sum_i Q_i^2)(\sum_j R_j^2)}{(\sum_j R_j^2)^2}.$$

Positivstellensatz: preuves

- Preuves classiques du Positivstellensatz basées sur l'Algèbre Moderne.
- Lemme de Zorn, clôture réelle et principe de Tranfert, très similaire à la preuve d'Artin du 17ème problème de Hilbert.
- Preuves non-constructives,
- pas de bornes sur les degrés

Les questions qui restent

- Pour le 17ème problème d'Hilbert comme pour le Positivtellensatz
- Usage de Zorn
- Aucune indication pour les bornes sur les degrés
- Problème de décidabilité' : Pouvons nous décider si un système d'inégalités n'a pas de solutions ? Oui en utilisant un algorithme d'élimination des quantificateurs.
- Problème d'effectivité' : Pouvons nous utiliser un algorithme d'élimination des quantificateurs pour fabriquer des incompatibilités dans le Positivstellensatz?
- Problème de complexité' : Quelles bornes sur les degrés ?

On a généralisé le problème, on ne l'a pas résolu.

Positivstellensatz: preuves

Stratégie dûe à Henri Lombardi

- Pour chaque système de conditions de signes sans solution, trouver une preuve algorithmique la plus algébrique possible du fait qu'il n'y a pas de solution, en utilisant une méthode bien choisie d'élimination des quantificateurs.
- Utiiser cette preuve pour construire une incompatibilité et controler les degrés du Positivstellensatz.

Quelles méthodes pour l'élimination des quantificateurs ?

- Plusieurs méthodes
- Les plus anciennes ont une complexité primitive récursive dans le nombre de variables : Tarski (celle qu'on a esquissée), Seidenberg, Cohen-Hormander.
- Celle choisie par Henri Lombardi pour une preuve constructive du Positivstellensatz est l'algorithme de Cohen-Hormander sous la forme donnée dans [BCR].

Degré d'une incompatibilité

$$\mathcal{H}(x): \begin{cases} P_i(x) & \neq & 0 & \text{pour} & i \in I_{\neq} \\ P_i(x) & \geq & 0 & \text{pour} & i \in I_{\geq} \\ P_i(x) & = & 0 & \text{pour} & i \in I_{=} \end{cases}$$

$$\downarrow \mathcal{H} \downarrow : \qquad \underbrace{S}_{>0} + \underbrace{N}_{\geq 0} + \underbrace{Z}_{=0} = 0$$

$$S = \prod_{i \in I_{\neq}} P_i^{2e_i}, \qquad N = \sum_{I \subset I_{\geq}} \Big(\sum_j k_{I,j} Q_{I,j}^2\Big) \prod_{i \in I} P_i, \qquad Z = \sum_{i \in I_{=}} Q_i P_i$$

Le degré de $\mathcal{H}$ est le degré maximum de

$$S = \prod_{i \in I_{\neq}} P_i^{2e_i}, \qquad Q_{I,j}^2 \prod_{i \in I} P_i \ \ (I \subset I_{\geq}, j), \qquad Q_i P_i \ \ (i \in I_{=}).$$

Exemple:

$$\begin{cases} x & \neq & 0 \\ y - x^2 - 1 & \geq & 0 \\ xy & = & 0 \end{cases} \quad \text{pas de solution dans } \mathbb{R}^2$$

$\downarrow \; x \neq 0, \quad y - x^2 - 1 \geq 0, \quad xy = 0 \; \downarrow$:

$$\underbrace{x^2}_{>0} + \underbrace{x^2(y - x^2 - 1) + x^4}_{\geq 0} + \underbrace{(-x^2 y)}_{=0} = 0.$$

Le degré de cette incomptabilité est 4.

Concept clé (Lombardi) l'inférence faible

$\mathcal{F}(u), \mathcal{G}_1(u), \mathcal{G}_2(u)$ systèmes de conditions de signes $\mathrm{K}[u]$. Une inférence faible (définition légèrement simplifiée adaptée à l'exemple qui suit)

$$\mathcal{F}(u) \quad \vdash \quad \mathcal{G}_1(u) \quad \vee \quad \mathcal{G}_2(u)$$

est une construction qui pour tout système de conditions de signe $\mathcal{H}$ dans $\mathrm{K}[v]$ où $v \supset u$ et toutes incompatibilités de départ

$$\downarrow \mathcal{G}_1(u),\ \mathcal{H}(v) \downarrow, \downarrow \mathcal{G}_2(u),\ \mathcal{H}(v) \downarrow$$

produit une incompatibilité

$$\downarrow \mathcal{F}(u),\ \mathcal{H}(v) \downarrow .$$

De droite à gauche.

Construction ? voir exemple qui suit.

Inférence faible: raisonnement cas par cas

$$A \neq 0 \quad \vdash \quad A < 0 \quad \vee \quad A > 0, A \in \mathrm{K}[u]$$

$\downarrow \mathcal{H}, \quad A < 0 \downarrow \leftarrow$ degré δ_1

$$\underbrace{A^{2e_1} S_1}_{>0} + \underbrace{N_1 - N_1' A}_{\geq 0} + \underbrace{Z_1}_{=0} = 0$$

$\downarrow \mathcal{H}, \quad A > 0 \downarrow \leftarrow$ degré δ_2

$$\underbrace{A^{2e_2} S_2}_{>0} + \underbrace{N_2 + N_2' A}_{\geq 0} + \underbrace{Z_2}_{=0} = 0$$

$$A^{2e_1} S_1 + N_1 + Z_1 = N_1' A \qquad A^{2e_2} S_2 + N_2 + Z_2 = -N_2' A$$

$$A^{2e_1+2e_2} S_1 S_2 + N_3 + Z_3 = -N_1' N_2' A^2$$

$$\underbrace{A^{2e_1+2e_2} S_1 S_2}_{>0} + \underbrace{N_1' N_2' A^2 + N_3}_{\geq 0} + \underbrace{Z_3}_{=0} = 0$$

Inférence faibles raisonnement cas par cas

Partant de deux incompatibilités

$\downarrow \mathcal{H},\ A<0 \downarrow \leftarrow$ degré δ_1 $\qquad$ $\downarrow \mathcal{H},\ A>0 \downarrow \leftarrow$ degré δ_2

$$\underbrace{A^{2e_1}S_1}_{>0}+\underbrace{N_1-N_1'A}_{\geq 0}+\underbrace{Z_1}_{=0}=0 \qquad \underbrace{A^{2e_2}S_2}_{>0}+\underbrace{N_2+N_2'A}_{\geq 0}+\underbrace{Z_2}_{=0}=0$$

nous avons construit (en faisant un produit) un nouvelle incompatibilité

$$\underbrace{A^{2e_1+2e_2}S_1S_2}_{>0}+\underbrace{N_1'N_2'A^2+N_3}_{\geq 0}+\underbrace{Z_3}_{=0}=0$$

$$\downarrow \mathcal{H},\ A\neq 0 \downarrow \leftarrow \text{degré } \delta_1+\delta_2$$

Liste des énoncés nécessaires sous forme d'inférence faible

- Beaucoup d'inférences faibles simples comme la précédente sont combinées pour obtenir des inférences faibles plus intéressantes.
- En particuler: TVI : Théorème des Valeurs Intermédiaires pour les polynômes qui est essentiel dans l'élimination des quantificateurs de Cohen-Hörmander.
- Finalement Henri Lombardi a obtenu des bornes sur les degrés primitives récursives pour le Positivstellensatz, donc aussi pour le 17ème problème de Hilbert Lombardi 90.
- Concernant le 17ème problème seul, il y a d'autres résultats. Kreisel 57 - Daykin 61 - Schmid 00: preuves constructives, bornes sur les degrés primitives récursives en k et $d = \deg P$.

Complexité de l'élimination des quantificateurs

Il y existe aussi des méthodes élémentairement récursives.

- La décomposition algébrique cylindrique a une complexité doublement exponentielle
- Polynomiale quand le nombre de variables est fixée
- Utilise la continuité des racines et la notion de connexité

Des méthodes plus récentes sont doublement exponentielles dans le nombre d'alternances de quantificateurs et simplement exponentielles quand il y a un seul bloc de quanificateurs. Utilisent encore plus de géométrie (points critiques...).
On veut une méthode élémentairement récursive et purement algébrique.

Détermination de Signe

- K un corps ordonné (ex: $\mathbb{Q}$), R un corps réel clos le contenant (ex: $\mathbb{R}$, $\mathbb{R}_{\mathrm{alg}}$)
- un polynôme non nul en une variable P et une liste d'autres polynômes $Q_1, \ldots, Q_s$ tous dans $\mathrm{K}[X]$
- trouver la liste des conditions de signes non vides (i.e. des éléments de $\{0, 1, -1\}^s$) saisfaites par $Q_1, \ldots, Q_s$ aux racines réelles de P (i.e. racines dans R)

Détermination de Signe améliorée

- Le nombre de conditions de signes non vides est au plus le nombre $r \leq d$ de racines réelles
- Retirer les conditions de signe vides à chaque étape de l'induction
- Utiliser la structure spéciale de la matrice pour résoudre le système linéaire en temps quadratique
- **Montrer que les $Q_1^{\alpha_1} \ldots, Q_s^{\alpha_s}$ dont les requêtes de Tarski sont calculées dan l'algorithme ont au plus $\log_2 d$ α_i non nuls**.

Complexité

- Le nombre total de requêtes de Tarski calculées est $3sd$ (linéaire en s plutôt qu'exponentiel)
- La boîte noire de requête de Tarski est utilisée par P et des polynômes de degré au plus $2d \log_2 d$

(avec Aviva Szpirglas)

Nombres réels algébriques

- (avec Michel Coste) Les nombres réels algébriques peuvent être caractérisés par les signes qu'ils donnent à leurs dérivées successives (codage à la Thom) : facile par induction sur le degré
- Les codages à la Thom peuvent être calculés par détermination de signe
- Aucune approximation numérique, valable dans tout corps réel close
- Une fois les codages à la Thom connus, la détermination de signe est simplifiée, seuls des produits de (peu de) dérivées et d'un autre polynôme (ou de son carré) sont nécessaires.

Détermination de signe et élimination des quantificateurs

- On obtient ainsi une nouvelle méthode purement algébrique d'élimination des quantificateurs en utilisant la détermination de signe améliorée et les codages à la Thom (avec Daniel Perrucci)
- Complexité élémentairement récursive
- Polynomiale dans le nombre de polynômes quand le nombre de variables est fixé mais **PAS** dans le degré des polynômes
- Ne nécessite pas la notion de composante connexe d'une condition de signe

Bornes de degrés élémentairement récursives pour le Positivstellensatz

- stratégie: transformer une preuve alébrique qu'un système d'inégalités n'a pas de solution en construction d'une identité algébrique
- transformer tous les ingrédients précédents : calcul de la signature de la forme quadratique d'Hermite, codage à la Thom, détermination de signe, en constructions d'identités algébriques
- controler le degré de ces identités

(Travail en commun avec Daniel Perrucci et Henri Lombardi)

Corps réels clos: TVI et TFA

Théorème

R *corps totalement ordonné. Les conditions suivantes sont équivalentes*

1. *TVI: le théorème des valeurs intermédiaires pour les polynômes : si* $P \in \mathrm{R}[X]$,

$$a < b, P(a)P(b) < 0 \implies \exists c \in (a, b)\, P(c) = 0.$$

2. *TFA:* $\mathrm{C} = \mathrm{R}[i] = \mathrm{R}[T]/(T^2 + 1)$ *est un corps algébriquement clos.*

TFA implique TVI: factorisation de P en facteurs linéaires et quadratiques.

TVI implies TFA

Preuve algébrique de Laplace. TVI implique que tous les nombres positifs ont une racine carrée et que tous les polynômes de degré impair ont une racine. TFA se montre par induction dans l'exposant de 2 dans le degré, et construit finalement un polynôme de degré impair très élevé (exponentiel en d).
Indication : $P \in \mathrm{R}[X]$ de degré $d = 2^k s$ avec s ipair, P a une racine dans C par induction sur k. Si $k = 0$, d est impair et P a une racine dans $\mathrm{R} \subset \mathrm{C}$. Sinon, définir pour $h \in \mathbb{Z}$,

$$Q_h(X_1, \ldots, X_d, X) = \prod_{\lambda<\mu} (X - X_\lambda - X_\mu - hX_\lambda X_\mu)$$

$\deg_X(Q_h) = d(d-1)/2 = 2^{k-1}s'$ avec s' impair.
Polynôme symétrique, substituer les fonctions symétriques élémentaires: coeffcients dans R. Hypotèse d'induction, principe des tiroirs, calcul des racines complexes des polynômes de degré 2

Construire des identités algébrique pour les faits suivants

- un polynôme réel de degré impair a une racine réelle
- un polynôme réel a une racine complexe (par Laplace)
- requêtes de Tarski par la méthode d'Hermite (on avait besoin de TFA pour prouver Hermite)
- loi d'inertie de Sylvester pour les formes quadratiques
- conditions de signes non vides fixées par les mineurs de formes quadratiques d'Hermite de degré controlés (utilise le codage à la Thom et la détermination de signe améliorée),
- conditions de signes réalisables par $\mathcal{P} \subset \mathrm{K}[x_1, \ldots, x_k]$ fixées par les conditions de signes sur une famille $\mathrm{Proj}(\mathcal{P}) \subset \mathrm{K}[x_1, \ldots, x_{k-1}]$: projection efficace par des méthodes purement algébriques

et à la fin produire une somme de carrés avec une complexité élémentairement récursive (tour de cinq exponentielles) !

Comment est produite la somme de carrés ?

Supposons que P ne prend que des valeurs positives ou nulles. La preuve que

$$P \geq 0$$

est transformée, étape par étape, en une preuve de l'inférence faible

$$\vdash \quad P \geq 0.$$

Ce qui signifie que si nous avons une incompatibilité initiale de $\mathcal{H}$ avec $P \geq 0$, nous savons comment construire une incompatibilité finale de $\mathcal{H}$ lui même, en controlant les degrés.

De droite à gauche.

Comment est produite la somme de carrés ?

En particulier $P < 0$, i.e. $P \neq 0, -P \geq 0$, est incompatible avec $P \geq 0$, puisque

$$\underbrace{P^2}_{>0} + \underbrace{P \times (-P)}_{\geq 0} = 0$$

est une incompatibilité de départ de $P \geq 0, P \neq 0, -P \geq 0$!
Donc prenant $\mathcal{H} = [P \neq 0, -P \geq 0]$ nous savons construire une incompatibilite de $\mathcal{H}$ elle même (en controlant les degrés)!

$$\underbrace{P^{2e}}_{>0} + \underbrace{\sum_i Q_i^2 - (\sum_j R_j^2)P}_{\geq 0} = 0$$

qui est l'incompatibilité finale cherchée !!
Nous avons exprimé P comme une somme de fractions rationnelles !!!

17ème problème de Hilbert élémentairement récursif

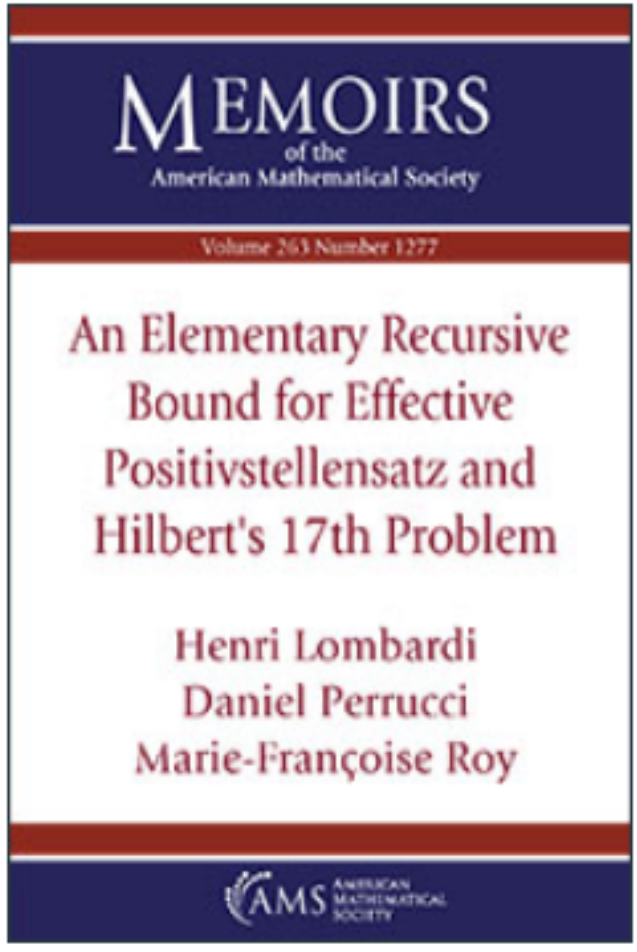
Un polynôme de degré d en k variables qui prend uniquement des valeurs positives ou nulles peut être représenté comme une somme de carrés de fractions rationnelle avec des bornes de degré élémentairement récursives:

$$2^{2^{2^{d^{4^k}}}}.$$

[LPR]
et des résultats similaires pour le Positivstellensatz

Discussion

- Pourquoi une tour de cinq exponentielles ?
- C'est ce que donne notre méthode, il n'y a pas d'autre raison
- existence d'une racine réelle pour un polynôme de degré impair d: construction d'identités algébriques avec deux niveaux d'exponentielle
- preuve de Laplace pour un polynôme de degré d; polynôme de degré impair d^d, triple exponentielle pour le théorème fondamental de l'algèbre
- méthode de projection basée seulement sur l'algèbre: polynomes de degré doublement exponentiels (éliminant les variables l'une après l'autre avec les mineurs d'Hermite)
- finalement : une tour de 5 exponentielles
- long article, dans les Memoirs of the AMS ...


MEMOIRS
of the
American Mathematical Society
Volume 263 Number 1277
An Elementary Recursive Bound for Effective Positivstellensatz and Hilbert's 17th Problem
Henri Lombardi
Daniel Perrucci
Marie-Françoise Roy
AMS

Ce qu'on peut espérer ?

- Nullstellensatz : borne supérieures et inférieures simplement exponentielles (..., Kollar, ...), en utilisant plus de géométrie algébrique qu'à l'époque de Grete Hermann.
- Meilleures bornes inférieures pour le 17ème problème de Hilbert: degré linéaire en k (Bleckerman et coauteurs) !
- Positivstellensatz: bornes inférieures simplement exponentielles Grigorev-Vorobjov
- Décider qu'un système d'inégalités n'a pas de solutions : simplement exponentiel Grigorev-Vorobjov, plus sophistiqué que projeter les variables une à une
- Espoir actuel: faire la théorie d'Hermite sans racines complexes, en utlisant plutôt la règle de Descartes, nous avons une preuve algébrique satisfaisnte mais pas (encore ?) les identités algébriques ... Donnerait 4 niveaux d'exponentielle ...

References

[BGP] Blekherman G., Gouveia J. and Pfeiffer J. Sums of Squares on the Hypercube Manuscript. arXiv:1402.4199.

[BCR] J. Bochnak , M. Coste , M.-F. Roy. Real algebraic geometry. Second edition in english.Ergebnisse der Mat., vol. 36. Berlin Heidelberg New York: Springer (1998)

[BPR] S. Basu, R. Pollack, M.-F. Roy, Algorithms in real algebraic geometry, Algorithms and Computation in Mathematics, 10, Second edition. *Springer-Verlag, Berlin*, 2006.

[PR] D. Perrucci, M.-F. Roy. Elementary recursive quantifier elimination based on Thom encoding and sign determination. Annals of Pure and Applied Logic, Volume 168, Issue 8, August 2017, Pages 1588-1604 (preliminary version, arXiv:1609.02879v2)¡;

[LPR] H. Lombardi, D. Perrucci, M.-F. Roy, *An elementary recursive bound for effective Positivstellensatz and Hilbert 17-th problem* (preliminary version, arXiv:1404.2338).

(avec beaucoup d'autres références)

Grete Hermann, Olga Taussky-Todd

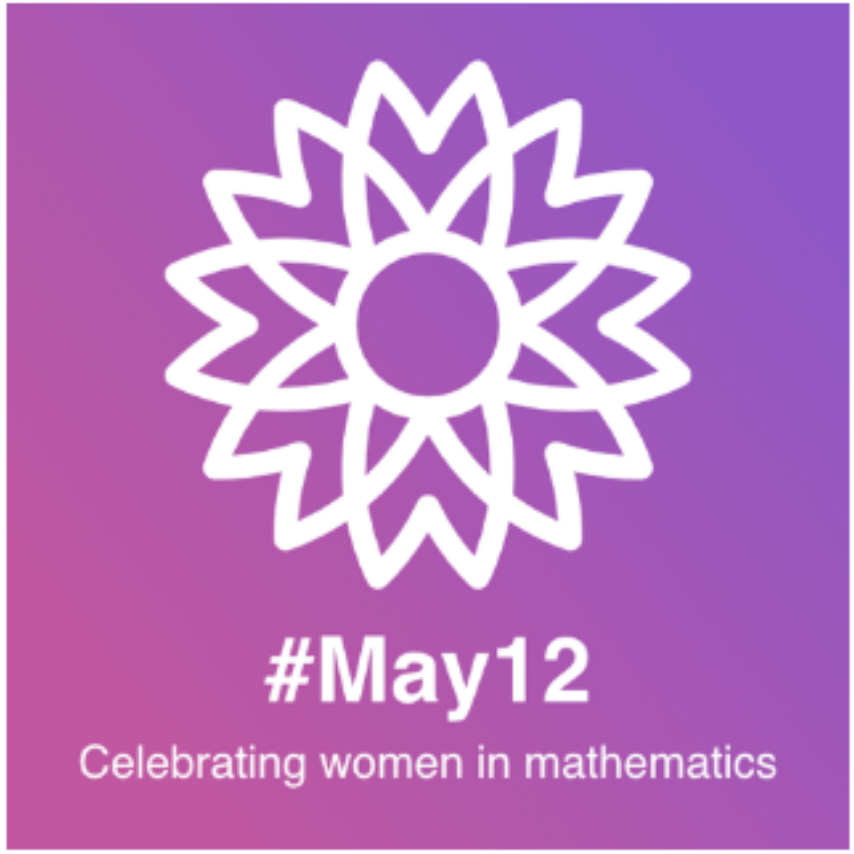


Figure: May 12 Celebrating Women in Mathematics