Élimination des quantificateurs versus 17ème problème de Hilbert

Marie-Françoise Roy

Université de Rennes 1, France

basé en partie sur des travaux en commun avec

Henri Lombardi

Université de Franche-Comté, France

Daniel Perrucci

Universidad de Buenos Aires, Argentina

Journées en l'honneur d'Hourya Benis Sinaceur

15 juin 2017

Le 17-ème de Hilbert

- Écrire un polynôme (en une ou plusieurs variables) comme une somme de carrés donne une preuve algébrique que le polynôme ne prend jamais de valeur négative.
- Certificat algébrique de positivité

Le 17-ème de Hilbert

- Écrire un polynôme (en une ou plusieurs variables) comme une somme de carrés donne une preuve algébrique que le polynôme ne prend jamais de valeur négative.
- Certificat algébrique de positivité

Somme de carrés de polynômes

- Un polynôme positif est-il une somme de carrés de polynômes ?
- Oui si le nombre de variables est 1.
- Indication : décomposer le polynôme en puissances de facteurs irréductibles: les facteurs de degrés deux (correspondant aux racines réelles) sont des sommes de carrés, les facteurs de degré 1 (correspondant aux racines réelles) apparaissent avec un exposant pair, le produit de sommes de carrés est une somme de carrés.

Somme de carrés de polynômes

- Un polynôme positif est-il une somme de carrés de polynômes ?
- Oui si le nombre de variables est 1.
- Indication : décomposer le polynôme en puissances de facteurs irréductibles: les facteurs de degrés deux (correspondant aux racines réelles) sont des sommes de carrés, les facteurs de degré 1 (correspondant aux racines réelles) apparaissent avec un exposant pair, le produit de sommes de carrés est une somme de carrés.

Somme de carrés de polynômes

- Un polynôme positif est-il une somme de carrés de polynômes ?
- Oui si le nombre de variables est 1.
- Indication : décomposer le polynôme en puissances de facteurs irréductibles: les facteurs de degrés deux (correspondant aux racines réelles) sont des sommes de carrés, les facteurs de degré 1 (correspondant aux racines réelles) apparaissent avec un exposant pair, le produit de sommes de carrés est une somme de carrés.

Positivité et sommes de carrés

- Un polynôme positif est-il une somme de carrés de polynômes ?
- Oui si le nombre de variables est 1.
- Oui si le degré est 2.
- Une forme quadratique prenant seulement des valeurs positives est une somme de carrés de polynômes linéaires.

Positivité et sommes de carrés

- Un polynôme positif est-il une somme de carrés de polynômes ?
- Oui si le nombre de variables est 1.
- Oui si le degré est 2.
- Une forme quadratique prenant seulement des valeurs positives est une somme de carrés de polynômes linéaires.

Positivité et sommes de carrés

- Un polynôme positif est-il une somme de carrés de polynômes ?
- Oui si le nombre de variables est 1.
- Oui si le degré est 2.
- Non en général.
- Premier contre-exemple explicite Motzkin '69

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

est positif et n'est pas une somme de carrés de polynômes.

Positivité et sommes de carrés

- Un polynôme positif est-il une somme de carrés de polynômes ?
- Oui si le nombre de variables est 1.
- Oui si le degré est 2.
- Non en général.
- Premier contre-exemple explicite Motzkin '69

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

est positif et n'est pas une somme de carrés de polynômes.

Le contre-exemple

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

- M est positif. Indication: la moyenne arithmétique est toujours au moins la moyenne géométrique.
- M n'est pas une somme de carrés. Indication : tenter de l'écrire comme une sommes de carrés de polynômes de degré 3 et vérifier que c'est impossible.
- Point de départ: aucun monôme en X^3 ne peut apparaître dans la somme de carrés. Etc ...

Le contre-exemple

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

- M est positif. Indication: la moyenne arithmétique est toujours au moins la moyenne géométrique.
- M n'est pas une somme de carrés. Indication : tenter de l'écrire comme une sommes de carrés de polynômes de degré 3 et vérifier que c'est impossible.
- Point de départ: aucun monôme en X^3 ne peut apparaître dans la somme de carrés. Etc ...

Le contre-exemple

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

- M est positif. Indication: la moyenne arithmétique est toujours au moins la moyenne géométrique.
- M n'est pas une somme de carrés. Indication : tenter de l'écrire comme une sommes de carrés de polynômes de degré 3 et vérifier que c'est impossible.
- Point de départ: aucun monôme en X^3 ne peut apparaître dans la somme de carrés. Etc ...

Le 17-ème problème de Hilbert

- Reformulation proposée par Minkowski.
- Question Hilbert '1900.
- Est-ce qu'un polynôme positif est une somme de carrés de fractions rationnelles?
- Artin '27: Réponse positive. Preuve non-constructive.

Le 17-ème problème de Hilbert

- Reformulation proposée par Minkowski.
- Question Hilbert '1900.
- Est-ce qu'un polynôme positif est une somme de carrés de fractions rationnelles?
- Artin '27: Réponse positive. Preuve non-constructive.

Schéma de la preuve d'Artin

- Supposons que P n'est pas une sommes de carrés de fractions rationnelles.
- Les sommes de carrés forment un cône propre du corps des fractions rationnelles et ne contiennent pas P (un cône propre contient les carrés et est clos par addition et multiplication, un cône propre ne contient pas -1).

Schéma de la preuve d'Artin

- Supposons que P n'est pas une sommes de carrés de fractions rationnelles.
- Les sommes de carrés forment un cône propre du corps des fractions rationnelles et ne contiennent pas P (un cône propre contient les carrés et est clos par addition et multiplication, un cône propre ne contient pas -1).

Schéma de la preuve d'Artin

- Supposons que P n'est pas une sommes de carrés de fractions rationnelles.
- Les sommes de carrés forment un cône propre du corps des fractions rationnelles et ne contiennent pas P.
- En utilisant le lemme de Zorn, on obtient un cône propre maximal du corps des fractions rationnelles qui ne contient pas P. Un tel cône propre maximal définit un ordre total sur le corps des fractions rationnelles.

Schéma de la preuve d'Artin

- Supposons que P n'est pas une sommes de carrés de fractions rationnelles.
- Les sommes de carrés forment un cône propre du corps des fractions rationnelles et ne contiennent pas P.
- En utilisant le lemme de Zorn, on obtient un cône propre maximal du corps des fractions rationnelles qui ne contient pas P. Un tel cône propre maximal définit un ordre total sur le corps des fractions rationnelles.

Schéma de la preuve d'Artin

- Supposons que P n'est pas une sommes de carrés de fractions rationnelles.
- Les sommes de carrés forment un cône propre du corps des fractions rationnelles et ne contiennent pas P.
- En utilisant le lemme de Zorn, on obtient un ordre total sur le corps des fractions rationnelles qui ne contient pas P $(\star)$.
- Un corps réel clos est un corps totalement ordoné où les éléments positifs sont les carrés et où tout polynôme de degré impair a une racine.
- Tout corps ordonné a une clôture réelle.
- En prenant la clôture réelle du corps des fractions rationnelles pour l'ordre obtenu en $(\star)$, on obtient un corps où P prend des valeurs négatives (on évalue au "point générique" = le point $(X_1, \ldots, X_k)$).

Schéma de la preuve d'Artin

- Supposons que P n'est pas une sommes de carrés de fractions rationnelles.
- Les sommes de carrés forment un cône propre du corps des fractions rationnelles et ne contiennent pas P.
- En utilisant le lemme de Zorn, on obtient un ordre total sur le corps des fractions rationnelles qui ne contient pas P $(\star)$.
- Un corps réel clos est un corps totalement ordoné où les éléments positifs sont les carrés et où tout polynôme de degré impair a une racine.
- Tout corps ordonné a une clôture réelle.
- En prenant la clôture réelle du corps des fractions rationnelles pour l'ordre obtenu en $(\star)$, on obtient un corps où P prend des valeurs négatives (on évalue au "point générique" = le point $(X_1, \ldots, X_k)$).

Schéma de la preuve d'Artin

- Supposons que P n'est pas une sommes de carrés de fractions rationnelles.
- Les sommes de carrés forment un cône propre du corps des fractions rationnelles et ne contiennent pas P.
- En utilisant le lemme de Zorn, on obtient un ordre total sur le corps des fractions rationnelles qui ne contient pas P $(\star)$.
- Un corps réel clos est un corps totalement ordoné où les éléments positifs sont les carrés et où tout polynôme de degré impair a une racine.
- Tout corps ordonné a une clôture réelle.
- En prenant la clôture réelle du corps des fractions rationnelles pour l'ordre obtenu en $(\star)$, on obtient un corps où P prend des valeurs négatives (on évalue au "point générique" = le point $(X_1, \dots, X_k)$).

Schéma de la preuve d'Artin

- Supposons que P n'est pas une sommes de carrés de fractions rationnelles.
- Les sommes de carrés forment un cône propre du corps des fractions rationnelles et ne contiennent pas P.
- En utilisant le lemme de Zorn, on obtient un ordre total sur le corps des fractions rationnelles qui ne contient pas P $(\star)$.
- Un corps réel clos est un corps totalement ordoné où les éléments positifs sont les carrés et où tout polynôme de degré impair a une racine.
- Tout corps ordonné a une clôture réelle.
- En prenant la clôture réelle du corps des fractions rationnelles pour l'ordre obtenu en $(\star)$, on obtient un corps où P prend des valeurs négatives (on évalue au "point générique" = le point $(X_1, \ldots, X_k)$).

Schéma de la preuve d'Artin

- Supposons que P n'est pas une sommes de carrés de fractions rationnelles.
- Les sommes de carrés forment un cône propre du corps des fractions rationnelles et ne contiennent pas P.
- En utilisant le lemme de Zorn, on obtient un textcolorcelesteordre total sur le corps des fractions rationnelles qui ne contient pas P $(\star)$.
- En prenant la clôture réelle du corps des fractions rationnelles pour l'ordre obtenu en $(\star)$, on obtient un corps où P prend des valeurs négatives (on évalue au "point générique" = le point $(X_1, \ldots, X_k)$).
- Alors P prend des valeurs négatives sur les nombres réels. Premier exemple d'un principe de trasfert en géométrie algébrique réelle. Basé sur le théorème de Sturm's, ou la forme quadratique d'Hermite.

Schéma de la preuve d'Artin

- Supposons que P n'est pas une sommes de carrés de fractions rationnelles.
- Les sommes de carrés forment un cône propre du corps des fractions rationnelles et ne contiennent pas P.
- En utilisant le lemme de Zorn, on obtient un textcolorcelesteordre total sur le corps des fractions rationnelles qui ne contient pas P $(\star)$.
- En prenant la clôture réelle du corps des fractions rationnelles pour l'ordre obtenu en $(\star)$, on obtient un corps où P prend des valeurs négatives (on évalue au "point générique" = le point $(X_1, \ldots, X_k)$).
- Alors P prend des valeurs négatives sur les nombres réels. Premier exemple d'un principe de trasfert en géométrie algébrique réelle. Basé sur le théorème de Sturm's, ou la forme quadratique d'Hermite.

Principe de transfert

- Un énoncé portant sur des éléments de $\mathbb{R}$ qui est vrai dans un corps réel clos contenant $\mathbb{R}$ (tel que la clôture réelle du corps de fractions rationnelles sur l'ordre choisi en $(\star)$) est vrai dans $\mathbb{R}$.
- Pas n'importe quel énoncé, un "énoncé de 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 contenant $\mathbb{R}$ si et seulement si il et vrai dans $\mathbb{R}$
- Cas particulier de l' élimination des quantificateurs.

Principe de transfert

- Un énoncé portant sur des éléments de $\mathbb{R}$ qui est vrai dans un corps réel clos contenant $\mathbb{R}$ (tel que la clôture réelle du corps de fractions rationnelles sur l'ordre choisi en ($\star$)) est vrai dans $\mathbb{R}$.
- Pas n'importe quel énoncé, un "énoncé de 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 contenant $\mathbb{R}$ si et seulement si il et vrai dans $\mathbb{R}$
- Cas particulier de l' élimination des quantificateurs.

Elimination des quantificateurs

- Qu'est-ce que l' élimination des quantificateurs ?
- Mathématiques du lycée

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

$$\iff$$

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

- Si c'est vrai dans un corps réel clos contenant $\mathbb{R}$, c'est vrai dans $\mathbb{R}$!
- Vrai pour toute formule, résultat de Tarski, utiliise des généralisations du théorème de Sturm's, ou la forme quadratique d'Hermite.

Elimination des quantificateurs

- Qu'est-ce que l' élimination des quantificateurs ?
- Mathématiques du lycée

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

$$\Longleftrightarrow$$

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

- Si c'est vrai dans un corps réel clos contenant $\mathbb{R}$, c'est vrai dans $\mathbb{R}$!
- Vrai pour toute formule, résultat de Tarski, utiliise des généralisations du théorème de Sturm's, ou la forme quadratique d'Hermite.

Elimination des quantificateurs

- Qu'est-ce que l' élimination des quantificateurs ?
- Mathématiques du lycée

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

$\Longleftrightarrow$

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

- Si c'est vrai dans un corps réel clos contenant $\mathbb{R}$, c'est vrai dans $\mathbb{R}$!
- Vrai pour toute formule, résultat de Tarski, utiliise des généralisations du théorème de Sturm's, ou la forme quadratique d'Hermite.

- Qu'est-ce que l' élimination des quantificateurs ?
- Mathématiques du lycée

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

$$\iff$$

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

- Si c'est vrai dans un corps réel clos contenant $\mathbb{R}$, c'est vrai dans $\mathbb{R}$!
- Vrai pour toute formule, résultat de Tarski, utiliise des généralisations du théorème de Sturm's, ou la forme quadratique d'Hermite.

Forme quadratique d'Hermite

$$N_i = \sum_{x \in \mathrm{Zer}(P,\mathbf{C})} \mu(x) x^i,$$

où $\mu(x)$ est la multiplicité de x.

$$\mathrm{Herm}(P) = \begin{bmatrix} N_0 & N_1 & \iddots & & \iddots & N_{p-1} \\ N_1 & \iddots & & \iddots & N_{p-1} & N_p \\ \iddots & & \iddots & N_{p-1} & N_p & \iddots \\ & \iddots & N_{p-1} & N_p & \iddots & \\ \iddots & N_{p-1} & N_p & \iddots & & \iddots \\ N_{p-1} & N_p & \iddots & & \iddots & N_{2p-2} \end{bmatrix}$$

Forme quadratique d'Hermite

$$a \neq 0, P(x) = ax^2 + bx + c == a(x - x_1)(x - x_2)$$

$$N_0 = x_1^0 + x_2^0 = 2$$

$$N_1 = x_1 + x_2 = -\frac{b}{a}$$

$$N_2 = x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1x_2 = \frac{b^2}{a^2} - 2\frac{c}{a} = \frac{b^2 - 2ac}{a^2}$$

$$\mathrm{Herm}(P) = \begin{bmatrix} N_0 & N_1 \\ N_1 & N_2 \end{bmatrix} = \begin{bmatrix} 2 & -\frac{b}{a} \\ -\frac{b}{a} & \frac{b^2 - 2ac}{a^2} \end{bmatrix}$$

$$\det(\mathrm{Herm}(P)) = \frac{b^2 - 4ac}{a^2} = \frac{\Delta}{a^2}$$

La signature de la forme quadratique $\mathrm{Herm}(P)$ est

- 2 si $\Delta > 0$ (2 racines réelles)
- 1 si $\Delta = 0$ (1 racine réelle)
- 0 si $\Delta < 0$ (pas de racine réelle)

Forme quadratique d'Hermite

Proposition

$P = a_p X^p + a_{p-1} X^{p-1} + \cdots + a_1 X + a_0$. Alors pour tout i i

$$(p-i)a_{p-i} = a_p N_i + \cdots + a_0 N_{i-p}, \tag{1}$$

avec la convention $a_i = N_i = 0$ for $i < 0$.

Proposition

La signature de la forme quadratique d'Hermite $\mathrm{Herm}(P)$ est le nombre de racines réelles de P.

Indication : les racines complexes conjuguées contribuent pour une différence de deux carrés.

Forme quadratique d'Hermite généralisée

$$N_i(P,Q) = \sum_{x \in \mathrm{Zer}(P,\mathbf{C})} \mu(x) Q(x) x^i,$$

où $\mu(x)$ est la multiplicité de x.
$\mathrm{Herm}(P,Q)_{i,j} = N_{i+j-2}(P,Q)$

Proposition

La signature de la forme quadratique d'Hermite généralisée associée à $\mathrm{Herm}(P,Q)$ est la donnée de Tarski de P et Q :

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

Indication : les racines complexes conjuguées contribuent pour une différence de deux carrés.

Elimination des quantificateurs

- La plupart des méthodes éliminent les variables l'un après l'autre : méthode de projection
- les conditions de signes non vides pour $\mathcal{P} \subset \mathbf{K}[x_1, \ldots, x_k]$ sont fixées par les conditions de signes non vides pour $\mathrm{Proj}(\mathcal{P}) \subset \mathbf{K}[x_1, \ldots, x_{k-1}]$
- méthode de Tarski purement algébrique (basée sur les données de Tarski) mais primitive récursive. $\mathrm{Proj}(\mathcal{P})$ est une liste de mineurs de formes d'Hermite généralisée entre produits d'éléments de $\mathcal{P}$
- même complexité pour Cohen-Hormander et Seidenberg
- la méthode de projection peut être rendue efficace = élémentairement récursive
- décomposition cylindrique classique (Collins) utilise la notion géométrique de composante connexe
- nouvelle méthode de projection basée uniquement sur l'algèbre (utilisant le codage de Thom des racines réelles par le signe des dérivées et la détermination de signe)

Outils pour l'élimination des quantificateurs élémentairement récursive basée seulement sur l'algèbre

- codage à la Thom : une racine réelle x d'un polynôme en une variable P est identifié par les signes en x des dérivées de P
- détermination de signe : calculer aux racines de P les signes d'une liste de polynômes $Q_1, \ldots, Q_s$ par un algorithme rapide utilisant des données de Tarski de P et de produits de peu parmi les Q_i
- la détermination de signe est utilisée pour calculer les codages à la Thom
- donne une élimination des quantificateurs élémentairement récursive
- la meilleure complexité connue utilise la projection par blocs (mais n'est pas purement algébrique)

Le 17ème problème: preuve d'Artin

- Supposons que P n'est pas une sommes de carrés de fractions rationnelles.
- Les sommes de carrés forment un cône propre du corps des fractions rationnelles et ne contiennent pas P.
- En utilisant le lemme de Zorn, on obtient un ordre total sur le corps des fractions rationnelles qui ne contient pas P $(\star)$.
- En prenant la clôture réelle du corps des fractions rationnelles pour l'ordre obtenu en $(\star)$, on obtient un corps où P prend des valeurs négatives (on évalue au "point générique" = le point $(X_1, \ldots, X_k)$).
- Alors P prend des valeurs négatives sur les nombres réels. Premier exemple d'un principe de trasfert en géométrie algébrique réelle. Basé sur le théorème de Sturm's, ou la forme quadratique d'Hermite.

Le 17ème problème: ce qui reste à faire

- Preuve très indirecte (par contraposition, utilise Zorn, la clôture réelle).
- Artin note qu'une construction effective est désirable mais difficile.
- Aucune indication sur les dénominateurs : bornes sur les degrés ?
- Problème d'effectivité : y a-t-il un algorithme qui vérifie si un polynôme ne prend que des valeurs positives ?
- L'élimination des quantificateurs décide si le polynôme est partout positif avec complexité élémentairement récursive.
- Mais comment construire la représentation ?
- Problème de complexité : quels sont les meilleures bornes sur les degrés dans la représentation ?

Le 17ème problème: ce qui reste à faire

- Preuve très indirecte (par contraposition, utilise Zorn, la clôture réelle).
- Artin note qu'une construction effective est désirable mais difficile.
- Aucune indication sur les dénominateurs : bornes sur les degrés ?
- Problème d'effectivité : y a-t-il un algorithme qui vérifie si un polynôme ne prend que des valeurs positives ?
- L'élimination des quantificateurs décide si le polynôme est partout positif avec complexité élémentairement récursive.
- Mais comment construire la représentation ?
- Problème de complexité : quels sont les meilleures bornes sur les degrés dans la représentation ?

Le 17ème problème: ce qui reste à faire

- Preuve très indirecte (par contraposition, utilise Zorn, la clôture réelle).
- Artin note qu'une construction effective est désirable mais difficile.
- Aucune indication sur les dénominateurs : bornes sur les degrés ?
- Problème d'effectivité : y a-t-il un algorithme qui vérifie si un polynôme ne prend que des valeurs positives ?
- L'élimination des quantificateurs décide si le polynôme est partout positif avec complexité élémentairement récursive.
- Mais comment construire la représentation ?
- Problème de complexité : quels sont les meilleures bornes sur les degrés dans la représentation ?

Le 17ème problème: ce qui reste à faire

- Preuve très indirecte (par contraposition, utilise Zorn, la clôture réelle).
- Artin note qu'une construction effective est désirable mais difficile.
- Aucune indication sur les dénominateurs : bornes sur les degrés ?
- Problème d'effectivité : y a-t-il un algorithme qui vérifie si un polynôme ne prend que des valeurs positives ?
- L'élimination des quantificateurs décide si le polynôme est partout positif avec complexité élémentairement récursive.
- Mais comment construire la représentation ?
- Problème de complexité : quels sont les meilleures bornes sur les degrés dans la représentation ?

Le 17ème problème: ce qui reste à faire

- Preuve très indirecte (par contraposition, utilise Zorn, la clôture réelle).
- Artin note qu'une construction effective est désirable mais difficile.
- Aucune indication sur les dénominateurs : bornes sur les degrés ?
- Problème d'effectivité : y a-t-il un algorithme qui vérifie si un polynôme ne prend que des valeurs positives ?
- L'élimination des quantificateurs décide si le polynôme est partout positif avec complexité élémentairement récursive.
- Mais comment construire la représentation ?
- Problème de complexité : quels sont les meilleures bornes sur les degrés dans la représentation ?

Le 17ème problème: ce qui reste à faire

- Preuve très indirecte (par contraposition, utilise Zorn, la clôture réelle).
- Artin note qu'une construction effective est désirable mais difficile.
- Aucune indication sur les dénominateurs : bornes sur les degrés ?
- Problème d'effectivité : y a-t-il un algorithme qui vérifie si un polynôme ne prend que des valeurs positives ?
- L'élimination des quantificateurs décide si le polynôme est partout positif avec complexité élémentairement récursive.
- Mais comment construire la représentation ?
- Problème de complexité : quels sont les meilleures bornes sur les degrés dans la représentation ?

Le 17ème problème: ce qui reste à faire

- Preuve très indirecte (par contraposition, utilise Zorn, la clôture réelle).
- Artin note qu'une construction effective est désirable mais difficile.
- Aucune indication sur les dénominateurs : bornes sur les degrés ?
- Problème d'effectivité : y a-t-il un algorithme qui vérifie si un polynôme ne prend que des valeurs positives ?
- L'élimination des quantificateurs décide si le polynôme est partout positif avec complexité élémentairement récursive.
- Mais comment construire la représentation ?
- Problème de complexité : quels sont les meilleures bornes sur les degrés dans la représentation ?

Positivstellensatz (Krivine '64, Stengle '74)

- Trouver des identités algébriques certificant qu'un système de conditions de signes est vide.
- Dans l'esprit du Nullstellensatz de Hilbert.
  K un corps, **C** une extension algébriquement close de **K**,
  $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$
  $P_1 = \ldots = P_s = 0$ n'a pas de solution dans $\mathbf{C}^k$
  $\Longleftrightarrow$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$

Positivstellensatz (Krivine '64, Stengle '74)

- Trouver des identités algébriques certificant qu'un système de conditions de signes est vide.
- Dans l'esprit du Nullstellensatz de Hilbert.

  K un corps, **C** une extension algébriquement close de **K**,
  $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$
  $P_1 = \ldots = P_s = 0$ n'a pas de solution dans $\mathbf{C}^k$
  $\Longleftrightarrow$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$

Positivstellensatz (Krivine '64, Stengle '74)

- Trouver des identités algébriques certificant qu'un système de conditions de signes est vide.
- Dans l'esprit du Nullstellensatz de Hilbert.
  K un corps, **C** une extension algébriquement close de **K**,
  $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$
  $P_1 = \ldots = P_s = 0$ n'a pas de solution dans $\mathbf{C}^k$
  $\iff$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$

Positivstellensatz (Krivine '64, Stengle '74)

- Trouver des identités algébriques certificant qu'un système de conditions de signes est vide.
- Dans l'esprit du Nullstellensatz de Hilbert.
  K un corps, **C** une extension algébriquement close de **K**,
  $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$
  $P_1 = \ldots = P_s = 0$ n'a pas de solution dans $\mathbf{C}^k$
  $\Longleftrightarrow$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$

Nullstellensatz quantitatif

- **K** un corps, **C** une extension algébriquement close de **K**, $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$
  $P_1 = \ldots = P_s = 0$ n'a pas de solution dans $\mathbf{C}^k$
  $\Longleftrightarrow$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- Quels sont les degrés des A_i ?
- en utilisant des résultants (Grete Hermann 1925): degrés doublement exponentiels en k
- plus récemment (Brownawell 1987 (méthodes analytiques),..., Kollar (méthodes algébriques), ... degrés simplement exponentiel en k, ne peut pas être amélioré

Nullstellensatz quantitatif

- **K** un corps, **C** une extension algébriquement close de **K**,
  $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$
  $P_1 = \ldots = P_s = 0$ n'a pas de solution dans $\mathbf{C}^k$
  $\Longleftrightarrow$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- Quels sont les degrés des A_i ?
- en utilisant des résultants (Grete Hermann 1925): degrés doublement exponentiels en k
- plus récemment (Brownawell 1987 (méthodes analytiques),..., Kollar (méthodes algébriques), ... degrés simplement exponentiel en k, ne peut pas être amélioré

Nullstellensatz quantitatif

- **K** un corps, **C** une extension algébriquement close de **K**, $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$
  $P_1 = \ldots = P_s = 0$ n'a pas de solution dans $\mathbf{C}^k$
  $\Longleftrightarrow$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- Quels sont les degrés des A_i ?
- en utilisant des résultants (Grete Hermann 1925): degrés doublement exponentiels en k
- plus récemment (Brownawell 1987 (méthodes analytiques),..., Kollar (méthodes algébriques), ... degrés simplement exponentiel en k, ne peut pas être amélioré

Nullstellensatz quantitatif

- **K** un corps, **C** une extension algébriquement close de **K**, $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$ $P_1 = \ldots = P_s = 0$ n'a pas de solution dans $\mathbf{C}^k$
  $\Longleftrightarrow$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- Quels sont les degrés des A_i ?
- en utilisant des résultants (Grete Hermann 1925): degrés doublement exponentiels en k
- plus récemment (Brownawell 1987 (méthodes analytiques),..., Kollar (méthodes algébriques), ... degrés simplement exponentiel en k, ne peut pas être amélioré

Nullstellensatz quantitatif

- **K** un corps, **C** une extension algébriquement close de **K**,
  $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$
  $P_1 = \ldots = P_s = 0$ n'a pas de solution dans $\mathbf{C}^k$
  $\Longleftrightarrow$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- Quels sont les degrés des A_i ?
- en utilisant des résultants (Grete Hermann 1925): degrés doublement exponentiels en k
- plus récemment (Brownawell 1987 (méthodes analytiques),..., Kollar (méthodes algébriques), ... degrés simplement exponentiel en k, ne peut pas être amélioré

Plus compliqué dans le cas réel

• **K** un corps ordonné (pour simplifier : où tous les positifs sont des carrés), **R** un corps réel clos extension de **K**,

• $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$, • $I_{\neq}, I_{\geq}, I_{=} \subset \{1, \ldots, s\}$,

$$\mathcal{H}(x) : \left\{ \begin{array}{llll} P_i(x) & \neq & 0 & \text{for} \quad i \in I_{\neq} \\ P_i(x) & \geq & 0 & \text{for} \quad i \in I_{\geq} \\ P_i(x) & = & 0 & \text{for} \quad i \in I_{=} \end{array} \right. \quad \text{sans solution dans } \mathbf{R}^k$$

$\Longleftrightarrow$

$\exists \quad S, N, Z$ avec $S(x) > 0, N(x) \geq 0, Z(x) = 0$ sous les hypothèses $\mathcal{H}(x)$ et

$$S + N + Z = 0.$$

Ce qu'on note

$$\downarrow \mathcal{H} \downarrow$$

Positivstellensatz

Plus compliqué dans le cas réel

- **K** un corps ordonné (pour simplifier : où tous les positifs sont des carrés), **R** un corps réel clos extension de **K**,

- $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$,
- $I_{\neq}, I_{\geq}, I_{=} \subset \{1, \ldots, s\}$,

$$\mathcal{H}(x) : \begin{cases} P_i(x) & \neq & 0 & \text{for} & i \in I_{\neq} \\ P_i(x) & \geq & 0 & \text{for} & i \in I_{\geq} \\ P_i(x) & = & 0 & \text{for} & i \in I_{=} \end{cases} \quad \text{sans solution dans } \mathbf{R}^k$$

$\Longleftrightarrow$

$\exists \quad S, N, Z$ avec $S(x) > 0, N(x) \geq 0, Z(x) = 0$ sous les hypothèses $\mathcal{H}(x)$ et

$$S + N + Z = 0.$$

Ce qu'on note

$$\downarrow \mathcal{H} \downarrow$$

Positivstellensatz

Plus compliqué dans le cas réel

- **K** un corps ordonné (pour simplifier : où tous les positifs sont des carrés), **R** un corps réel clos extension de **K**,

- $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$, • $I_{\neq}, I_{\geq}, I_{=} \subset \{1, \ldots, s\}$,

$$\mathcal{H}(x) : \begin{cases} P_i(x) & \neq & 0 & \text{for} & i \in I_{\neq} \\ P_i(x) & \geq & 0 & \text{for} & i \in I_{\geq} \\ P_i(x) & = & 0 & \text{for} & i \in I_{=} \end{cases} \quad \text{sans solution dans } \mathbf{R}^k$$

$\Longleftrightarrow$

$\exists \quad S, N, Z$ avec $S(x) > 0, N(x) \geq 0, Z(x) = 0$ sous les hypothèses $\mathcal{H}(x)$ et

$$S + N + Z = 0.$$

Ce qu'on note

$$\downarrow \mathcal{H} \downarrow$$

Incompatibilités

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

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

avec

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

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

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

Degré d'une incompatibilité

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

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

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

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 d'incompatibilité

$P < 0, P \geq 0$ n'a pas de solution dans $\mathbb{R}^k$

$\downarrow\ P \neq 0, -P \geq 0, P \geq 0\ \downarrow$

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

Le degré de cette incompatibilié est $2\deg(P)$.

Exemple d'incompatibilité

$P < 0, P \geq 0$ n'a pas de solution dans $\mathbb{R}^k$

$$\downarrow \; P \neq 0, -P \geq 0, P \geq 0 \; \downarrow$$

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

Le degré de cette incompatibilié est $2\deg(P)$.

Exemple d'incompatibilité

Avec $\Delta = b^2 - 4ac$,

$$\begin{cases} ax^2 + bx + c & = & 0 \\ \Delta & < & 0 \end{cases}$$ n'a pas de solution dans $\mathbb{R}^2$

(les racines sont complexes quand $\Delta < 0$)

$$\downarrow\ \Delta \neq 0, -\Delta \geq 0, ax^2 + bx + c = 0,\ \downarrow$$

$$\underbrace{\Delta^2}_{>0} + \underbrace{(-\Delta)(2ax+b)^2}_{\geq 0} + \underbrace{4a\Delta(ax^2+bx+c)}_{=0} = 0.$$

Le degré de cette incompatibilité est 4 (si a, b, c, x sont des variables).

Exemple d'incompatibilité

Avec $\Delta = b^2 - 4ac$,

$$\left\{ \begin{array}{rcl} ax^2 + bx + c & = & 0 \\ \Delta & < & 0 \end{array} \right. \quad \text{n'a pas de solution dans } \mathbb{R}^2$$

(les racines sont complexes quand $\Delta < 0$)

$$\downarrow \ \Delta \neq 0, -\Delta \geq 0, ax^2 + bx + c = 0, \ \downarrow$$

$$\underbrace{\Delta^2}_{>0} + \underbrace{(-\Delta)(2ax+b)^2}_{\geq 0} + \underbrace{4a\Delta(ax^2+bx+c)}_{=0} = 0.$$

Le degré de cette incompatibilité est 4 (si a, b, c, x sont des variables).

Exemple d'incompatibilité

Avec $\Delta = b^2 - 4ac$,

$$\left\{\begin{array}{ccc} ax^2+bx+c & = & 0 \\ \Delta & < & 0 \end{array}\right. \quad \text{n'a pas de solution dans } \mathbb{R}^2$$

(les racines sont complexes quand $\Delta < 0$)

$$\downarrow\ \Delta \neq 0, -\Delta \geq 0, ax^2+bx+c=0,\ \downarrow$$

$$\underbrace{\Delta^2}_{>0} + \underbrace{(-\Delta)(2ax+b)^2}_{\geq 0} + \underbrace{4a\Delta(ax^2+bx+c)}_{=0} = 0.$$

Le degré de cette incompatibilité est 4 (si a, b, c, x sont des variables).

Positivstellensatz: preuves

- Les preuves classiques du Positivstellensatz sont basées sur le lemme de Zorn et le principe de tranfert, très similaire à la preuve d'Artin's pour le 17ème problème de Hilbert.
- Les preuves constructives utilisent l' élimination des quantificateurs.
- Principe: transformer une preuve du fait qu'un système de conditions de signe est vide, utilisant une méthode d'élimination quantificateurs, en une incompatibilité.
- Quelle méthode d' l'élimination des quantificateurs ?

Positivstellensatz: preuves

- Les preuves classiques du Positivstellensatz sont basées sur le lemme de Zorn et le principe de tranfert, très similaire à la preuve d'Artin's pour le 17ème problème de Hilbert.
- Les preuves constructives utilisent l' élimination des quantificateurs.
- Principe: transformer une preuve du fait qu'un système de conditions de signe est vide, utilisant une méthode d'élimination quantificateurs, en une incompatibilité.
- Quelle méthode d' l'élimination des quantificateurs ?

Positivstellensatz: preuves

- Les preuves classiques du Positivstellensatz sont basées sur le lemme de Zorn et le principe de tranfert, très similaire à la preuve d'Artin's pour le 17ème problème de Hilbert.
- Les preuves constructives utilisent l' élimination des quantificateurs.
- Principe: transformer une preuve du fait qu'un système de conditions de signe est vide, utilisant une méthode d'élimination quantificateurs, en une incompatibilité.
- Quelle méthode d' l'élimination des quantificateurs ?

Positivstellensatz: preuves

- Les preuves classiques du Positivstellensatz sont basées sur le lemme de Zorn et le principe de tranfert, très similaire à la preuve d'Artin's pour le 17ème problème de Hilbert.
- Les preuves constructives utilisent l' élimination des quantificateurs.
- Principe: transformer une preuve du fait qu'un système de conditions de signe est vide, utilisant une méthode d'élimination quantificateurs, en une incompatibilité.
- Quelle méthode d' l'élimination des quantificateurs ?

Positivstellensatz: bornes sur les degrés

- Lombardi '90:
bornes sur les degrés primitives récursives en k,
$d = \max \deg P_i$ et $s = \#P_i$.

Basé sur l'algorithme de Cohen-Hörmander d' élimination des quantificateurs:

- tour d'exponentielles de hauteur $k+4$,
- $d\log(d) + \log\log(s) + c$ en haut.

- Nos résultalts: Basé sur notre méthode de projection efficace basée uniquement sur l'algèbre (utilisant le codage à la Thom des racines réeles et la détermination de signe) .
bornes sur les degrés élémentairement récursive en k, d et s:

$$2^{2^{2^{\max\{2,d\}^{4^k}} + s^{2^k} \max\{2,d\}^{16^k \mathrm{bit}(d)}}}.$$

Positivstellensatz: bornes sur les degrés

- Lombardi '90:

bornes sur les degrés primitives récursives en k,
$d = \max \deg P_i$ et $s = \# P_i$.

Basé sur l'algorithme de Cohen-Hörmander d' élimination des quantificateurs:

- tour d'exponentielles de hauteur $k + 4$,
- $d \log(d) + \log \log(s) + c$ en haut.

- Nos résultalts: Basé sur notre méthode de projection efficace basée uniquement sur l'algèbre (utilisant le codage à la Thom des racines réeles et la détermination de signe) .

bornes sur les degrés élémentairement récursive en k, d et s:

$$2^{2^{2^{\max\{2,d\}^{4^k}} + s^{2^k} \max\{2,d\}^{16^k \mathrm{bit}(d)}}}.$$

Positivstellensatz: bornes sur les degrés

• Lombardi '90:
bornes sur les degrés primitives récursives en k,
$d = \max \deg P_i$ et $s = \# P_i$.

Basé sur l'algorithme de Cohen-Hörmander d' élimination des quantificateurs:

- tour d'exponentielles de hauteur $k+4$,
- $d\log(d) + \log\log(s) + c$ en haut.

• Nos résultalts: Basé sur notre méthode de projection efficace basée uniquement sur l'algèbre (utilisant le codage à la Thom des racines réeles et la détermination de signe) .
bornes sur les degrés élémentairement récursive en k, d et s:

$$2^{2^{2^{\max\{2,d\}^{4^k}}+s^{2^k}\max\{2,d\}^{16^k \mathrm{bit}(d)}}}.$$

Positivstellensatz: bornes sur les degrés

- Lombardi '90:
bornes sur les degrés primitives récursives en k,
$d = \max \deg P_i$ et $s = \# P_i$.

Basé sur l'algorithme de Cohen-Hörmander d' élimination des quantificateurs:

- tour d'exponentielles de hauteur $k + 4$,
- $d \log(d) + \log\log(s) + c$ en haut.

- Nos résultalts: Basé sur notre méthode de projection efficace basée uniquement sur l'algèbre (utilisant le codage à la Thom des racines réeles et la détermination de signe) .
bornes sur les degrés élémentairement récursive en k, d et s:

$$2^{2^{2^{\max\{2,d\}^{4^k}} + s^{2^k} \max\{2,d\}^{16^k \operatorname{bit}(d)}}}.$$

Le positivstellensatz implique le 17ème problème de Hilbert

$P \geq 0$ in $\mathbb{R}^k$ $\iff$ $P(x) < 0$ n'a pas de solution

$\iff \left\{ \begin{array}{rcl} P(x) & \neq & 0 \\ -P(x) & \geq & 0 \end{array} \right.$ n'a pas de solution

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

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

Le positivstellensatz implique le 17ème problème de Hilbert

$$P \geq 0 \ \text{ in } \ \mathbb{R}^k \iff P(x) < 0 \quad \text{n'a pas de solution}$$

$$\iff \left\{ \begin{array}{rcl} P(x) & \neq & 0 \\ -P(x) & \geq & 0 \end{array} \right. \quad \text{n'a pas de solution}$$

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

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

Le positivstellensatz implique le 17ème problème de Hilbert

$$P \geq 0 \text{ in } \mathbb{R}^k \iff P(x) < 0 \quad \text{n'a pas de solution}$$

$$\iff \left\{ \begin{array}{rcl} P(x) & \neq & 0 \\ -P(x) & \geq & 0 \end{array} \right. \quad \text{n'a pas de solution}$$

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

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

Le positivstellensatz implique le 17ème problème de Hilbert

$$P \geq 0 \text{ in } \mathbb{R}^k \iff P(x) < 0 \quad \text{n'a pas de solution}$$

$$\iff \left\{ \begin{array}{rcl} P(x) & \neq & 0 \\ -P(x) & \geq & 0 \end{array} \right. \quad \text{n'a pas de solution}$$

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

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

Le positivstellensatz implique le 17ème problème de Hilbert

$$P \geq 0 \text{ in } \mathbb{R}^k \iff P(x) < 0 \quad \text{n'a pas de solution}$$

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

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

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

Notre stratégie

- Pour chaque système de conditions de signe sans solution, construire une incompatiblité algébrique et contrôler le degrés pour le Positivstellensatz.
- Retrouver le 17ème problème de Hilbert's comme un cas particulier
- Utiliser les notions introduites dans Lombardi '90
- Concept clé: inférence faible.

Inférence faible

(dans le cas particulier dont nous aurons besoin)

Definition (inférence faible)

$\mathcal{F}, \mathcal{G}$ systèmes de condition de signes dans $\mathbf{K}[u]$ et $\mathbf{K}[u,t]$. Une inférence faible

$$\mathcal{F}(u) \quad \vdash \quad \exists\, t\; \mathcal{G}(u,t)$$

est une construction qui pour tout système de conditions de signes $\mathcal{H}$ dans $\mathbf{K}[v]$ avec $v \supset u$ ne contenant pas t et toute incompatibilité

$$\downarrow \mathcal{G}(u,t),\ \mathcal{H}(v) \downarrow_{\mathbf{K}[v,t]}$$

produit une incompatibilité

$$\downarrow \mathcal{F}(u),\ \mathcal{H}(v) \downarrow_{\mathbf{K}[v]} .$$

De la droite vers la gauche.

Construction ? un exemple !

Inférence faible

(dans le cas particulier dont nous aurons besoin)

Definition (inférence faible)

$\mathcal{F}, \mathcal{G}$ systèmes de condition de signes dans $\mathbf{K}[u]$ et $\mathbf{K}[u, t]$. Une inférence faible

$$\mathcal{F}(u) \quad \vdash \quad \exists\, t\, \mathcal{G}(u, t)$$

est une construction qui pour tout système de conditions de signes $\mathcal{H}$ dans $\mathbf{K}[v]$ avec $v \supset u$ ne contenant pas t et toute incompatibilité

$$\downarrow \mathcal{G}(u, t),\ \mathcal{H}(v) \downarrow_{\mathbf{K}[v,t]}$$

produit une incompatibilité

$$\downarrow \mathcal{F}(u),\ \mathcal{H}(v) \downarrow_{\mathbf{K}[v]} .$$

De la droite vers la gauche.

Construction ? un exemple !

Exemple d'inférence faible: les éléments positifs sont des carrés

$$A(u) \geq 0 \quad \Longrightarrow \exists t \; A(u) = t^2$$

$A(u)$ est n'importe quel polynôme en plusieurs variables, $\mathcal{H}(v)$ n'importe quel système de condition de signe

$$\downarrow \mathcal{H}, A(u) = t^2 \downarrow \quad \longrightarrow \quad \left\{ \begin{array}{c} \mathcal{H}(v) \\ A(u) = t^2 \end{array} \right. \quad \text{n'a pas de solution}$$

$$\downarrow \qquad\qquad\qquad\qquad \downarrow$$

$$\downarrow \mathcal{H}(v), \;\; A(u) \geq 0 \downarrow \quad \longrightarrow \quad \left\{ \begin{array}{c} \mathcal{H}(v) \\ A(u) \geq 0 \end{array} \right. \quad \text{n'a pas de solution}$$

$$A(u) \geq 0 \quad \vdash \quad \exists \; t \; A(u) = t^2$$

De la droite vers la gauche.

Exemple d'inférence faible: les éléments positifs sont des carrés

$$A(u) \geq 0 \quad \Longrightarrow \exists t \; A(u) = t^2$$

$A(u)$ est n'importe quel polynôme en plusieurs variables, $\mathcal{H}(v)$ n'importe quel système de condition de signe

$$\begin{array}{ccccc} \downarrow \mathcal{H}, A(u) = t^2 \downarrow & \longrightarrow & \left\{ \begin{array}{c} \mathcal{H}(v) \\ A(u) = t^2 \end{array} \right. & \text{n'a pas de solution} \\ \downarrow & & \downarrow \\ \downarrow \mathcal{H}(v), \;\; A(u) \geq 0 \downarrow & \longrightarrow & \left\{ \begin{array}{c} \mathcal{H}(v) \\ A(u) \geq 0 \end{array} \right. & \text{n'a pas de solution} \end{array}$$

$$A(u) \geq 0 \quad \vdash \quad \exists \; t \; A(u) = t^2$$

De la droite vers la gauche.

Exemple d'inférence faible: les éléments positifs sont des carrés

$$A(u) \geq 0 \quad \Longrightarrow \exists t\ A(u) = t^2$$

$A(u)$ est n'importe quel polynôme en plusieurs variables, $\mathcal{H}(v)$ n'importe quel système de condition de signe

$$\downarrow \mathcal{H}, A(u) = t^2 \downarrow \quad \longrightarrow \quad \left\{ \begin{array}{c} \mathcal{H}(v) \\ A(u) = t^2 \end{array} \right. \quad \text{n'a pas de solution}$$

$$\downarrow \qquad\qquad\qquad\qquad \downarrow$$

$$\downarrow \mathcal{H}(v), \ \ A(u) \geq 0 \downarrow \quad \longrightarrow \quad \left\{ \begin{array}{c} \mathcal{H}(v) \\ A(u) \geq 0 \end{array} \right. \quad \text{n'a pas de solution}$$

$$A(u) \geq 0 \quad \vdash \quad \exists\ t\ A(u) = t^2$$

De la droite vers la gauche.

Exemple d'inférence faible: les éléments positifs sont des carrés

$$A(u) \geq 0 \quad \Longrightarrow \exists t\ A(u) = t^2$$

$A(u)$ est n'importe quel polynôme en plusieurs variables, $\mathcal{H}(v)$ n'importe quel système de condition de signe

$$\begin{array}{ccc} \downarrow \mathcal{H}, A(u) = t^2 \downarrow & \longrightarrow & \left\{ \begin{array}{c} \mathcal{H}(v) \\ A(u) = t^2 \end{array} \right. \text{ n'a pas de solution} \\ \downarrow & & \downarrow \\ \downarrow \mathcal{H}(v), \ \ A(u) \geq 0 \downarrow & \longrightarrow & \left\{ \begin{array}{c} \mathcal{H}(v) \\ A(u) \geq 0 \end{array} \right. \text{ n'a pas de solution} \end{array}$$

$$A(u) \geq 0 \quad \vdash \quad \exists\ t\ A(u) = t^2$$

De la droite vers la gauche.

On part de l'incompatibilité

$$S+\sum_i V_i^2(t)\cdot N_i+\sum_j W_j(t)\cdot Z_j+W(t)\cdot(t^2-A)=0 \qquad (2)$$

$V_{i1}\cdot t+V_{i0}$ le reste de $V_i(t)$ dans la division par t^2-A
$W_{j1}\cdot t+W_{j0}$ le reste de $W_j(t)$ dans la division par t^2-A
il existe $W'(t)\in \mathbf{K}[v][t]$ tel que

$$S+\sum_i (V_{i1}\cdot t+V_{i0})^2\cdot N_i+\sum_j (W_{j1}\cdot t+W_{j0})\cdot Z_j+W'(t)\cdot(t^2-A)=0.$$

ce qui est réecrit en

$$S+\sum_i (V_{i1}^2\cdot A+V_{i0}^2)\cdot N_i+\sum_j W_{j0}\cdot Z_j+W'''\cdot t+W''(t)\cdot(t^2-A)=0.$$

avec $W'''\in \mathbf{K}[v]$ et $W''(t)\in \mathbf{K}[v][t]$.

La construction (fin)

On en était à

$$S+\sum_i (V_{i1}^2 \cdot A + V_{i0}^2)\cdot N_i + \sum_j W_{j0}\cdot Z_j + W''' \cdot t + W''(t)\cdot(t^2 - A) = 0.$$

En examinant les degrés e t, on trouve que $W''(t) = 0$, puis que $W''' = 0$
Ceci termine la démonstration puisque

$$S + \sum_i (V_{i1}^2 \cdot A + V_{i0}^2) \cdot N_i + \sum_j W_{j0} \cdot Z_j = 0.$$

est l'incompatibilité cherchée.
Et on peut suivre les degrés par rapport aux variabbles

Construction ?

- Procédé qui permet de fabriquer une incompatibilité á partir d'une autre incompatibilité.
- Dans notre exemple
- Faire une division euclidienne.
- Regrouper différemment les termes.
- Déduire que certains morceaux sont nuls en identifiant les degrés.
- Garder une trace des degrés par rapport aux différentes variables.

Liste des énoncés à traduite en inférences faibles

- Combiner beaucoup d'inférences faibles simples pour en obtenir des plus intéressantes.
- Outils de l'algèbre classique au calcul formel moderne

un polynôme de degré impair a une racine réelle

un polynôme réel a une racine complexe (preuve algébrique due à Laplace)

Liste des énoncés à traduite en inférences faibles

- Combiner beaucoup d'inférences faibles simples pour en obtenir des plus intéressantes.
- Outils de l'algèbre classique au calcul formel moderne

  un polynôme de degré impair a une racine réelle

  un polynôme réel a une racine complexe (preuve algébrique due à Laplace)

Liste des énoncés à traduite en inférences faibles

- Combiner beaucoup d'inférences faibles simples pour en obtenir des plus intéressantes.
- Outils de l'algèbre classique au calcul formel moderne

  un polynôme de degré impair a une racine réelle

  un polynôme réel a une racine complexe (preuve algébrique due à Laplace)

Liste des énoncés à traduite en inférences faibles

- un polynôme de degré impair a une racine réelle
- un polynôme réel a une racine complexe
- la signature de la forme quadratique d'Hermite généralisée est égale à la donnése de Tarski et se calcule par des conditions de signe sur les mineurs principaux
- loi d'inertie de Sylvester: la signature d'une forme quadratique est bien définie

Liste des énoncés à traduite en inférences faibles

- un polynôme de degré impair a une racine réelle
- un polynôme réel a une racine complexe
- la signature de la forme quadratique d'Hermite généralisée est égale à la donnése de Tarski et se calcule par des conditions de signe sur les mineurs principaux
- loi d'inertie de Sylvester: la signature d'une forme quadratique est bien définie

Liste des énoncés à traduite en inférences faibles

- un polynôme de degré impair a une racine réelle
- un polynôme réel a une racine complexe
- signature de la forme quadratique d'Hermite généralisée
- loi d'inertie de Sylvester
- conditions de signes non vides pour une famille de polyômes aux racines d'un polynôme fixée par les signes des mineurs de plusieurs formes quadratiques d' Hermite (utiliser les codages à a Thom et la détermination de signe)
- finalement: les conditions de signes non vides pour $\mathcal{P} \subset \mathbf{K}[x_1, \ldots, x_k]$ sont fixées par les conditions de signes non vides pour $\mathrm{Proj}(\mathcal{P}) \subset \mathbf{K}[x_1, \ldots, x_{k-1}]$: méthode de projection efficace utilisant seulement l'algèbre

Liste des énoncés à traduite en inférences faibles

- un polynôme de degré impair a une racine réelle
- un polynôme réel a une racine complexe
- signature de la forme quadratique d'Hermite généralisée
- loi d'inertie de Sylvester
- conditions de signes non vides pour une famille de polyômes aux racines d'un polynôme fixée par les signes des mineurs de plusieurs formes quadratiques d' Hermite (utiliser les codages à a Thom et la détermination de signe)
- finalement: les conditions de signes non vides pour $\mathcal{P} \subset \mathbf{K}[x_1, \ldots, x_k]$ sont fixées par les conditions de signes non vides pour $\mathrm{Proj}(\mathcal{P}) \subset \mathbf{K}[x_1, \ldots, x_{k-1}]$: méthode de projection efficace utilisant seulement l'algèbre

Comment produire la somme de carrés?

Supposons que P prend seulement des valeurs positives. La preuve que

$$P \geq 0$$

est transformée, pas à pas, en une preuve de l'inférence faible

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

Ce qui veut dire que si nous avons une incompatibilité de $\mathcal{H}$ avec $P \geq 0$, nous savons construire une incompatibilité de $\mathcal{H}$ lui même

De la droite vers la gauche.

Comment produire la somme de carrés?

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

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

C'est l'incompatibilité du système $P \geq 0, P \neq 0, -P \geq 0$ dont nous partons!

Donc, partant $\mathcal{H} = [P \neq 0, -P \geq 0]$ et utilisant l'inférence faible

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

nous savons construire une incompatibilité de $\mathcal{H}$ lui-même !

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

qui est l'incompatibilité finale que nous cherchons !!

Nous avons exprimé P comme une somme de carrés de fractions rationnelles !!!

Degrés pour le 17-ème problème de Hilbert

• Kreisel '57 - Daykin '61 - Lombardi '90 - Schmid '00: Preuves constructive $\rightsquigarrow$ bornes sur les degrés primitives récursives en k et $d = \deg P$.

• Notre travail '14: basé sur l'élimination des quantificateurs purement algébrique et élémentairement récursive $\rightsquigarrow$ bornes sur les degrés élémentairement récursives

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

Degrés pour le 17-ème problème de Hilbert

• Kreisel '57 - Daykin '61 - Lombardi '90 - Schmid '00: Preuves constructive $\rightsquigarrow$ bornes sur les degrés primitives récursives en k et $d = \deg P$.

• Notre travail '14: basé sur l'élimination des quantificateurs purement algébrique et élémentairement récursive $\rightsquigarrow$ bornes sur les degrés élémentairement récursives

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

Discussion

- Pourquoi une tour de cinq exponentielles ?
- c'est ce que donne notre méthode aucune autre raison ...
- l'existence d'une racine réelle pour un polynôme en une variable de degré d donne déjà une inférence faible qui fait intervenir un degré doublement exponentiel en d
- la preuve de Laplace part d'un polynôme de degré d et produit un polynôme de degré impair d^d : une tour de trois exponentielles pour l'inférence faible correspondant au théorème fondamental de l'algèbre
- notre méthode de projection basée uniquement sur l'algèbre donne des polynômes en une variable de degré doublement exponentiel
- donc : une tour de 5 exponentielles
- nous avons la chance que les autres étapes n'empirent pas cette borne
- long papier (128 pages) ...

Discussion

- Pourquoi une tour de cinq exponentielles ?
- c'est ce que donne notre méthode aucune autre raison ...
- l'existence d'une racine réelle pour un polynôme en une variable de degré d donne déjà une inférence faible qui fait intervenir un degré doublement exponentiel en d
- la preuve de Laplace part d'un polynôme de degré d et produit un polynôme de degré impair d^d : une tour de trois exponentielles pour l'inférence faible correspondant au théorème fondamental de l'algèbre
- notre méthode de projection basée uniquement sur l'algèbre donne des polynômes en une variable de degré doublement exponentiel
- donc : une tour de 5 exponentielles
- nous avons la chance que les autres étapes n'empirent pas cette borne
- long papier (128 pages) ...

Discussion

- Pourquoi une tour de cinq exponentielles ?
- c'est ce que donne notre méthode aucune autre raison ...
- l'existence d'une racine réelle pour un polynôme en une variable de degré d donne déjà une inférence faible qui fait intervenir un degré doublement exponentiel en d
- la preuve de Laplace part d'un polynôme de degré d et produit un polynôme de degré impair d^d : une tour de trois exponentielles pour l'inférence faible correspondant au théorème fondamental de l'algèbre
- notre méthode de projection basée uniquement sur l'algèbre donne des polynômes en une variable de degré doublement exponentiel
- donc : une tour de 5 exponentielles
- nous avons la chance que les autres étapes n'empirent pas cette borne
- long papier (128 pages) ...

Discussion

- Pourquoi une tour de cinq exponentielles ?
- c'est ce que donne notre méthode aucune autre raison ...
- l'existence d'une racine réelle pour un polynôme en une variable de degré d donne déjà une inférence faible qui fait intervenir un degré doublement exponentiel en d
- la preuve de Laplace part d'un polynôme de degré d et produit un polynôme de degré impair d^d : une tour de trois exponentielles pour l'inférence faible correspondant au théorème fondamental de l'algèbre
- notre méthode de projection basée uniquement sur l'algèbre donne des polynômes en une variable de degré doublement exponentiel
- donc : une tour de 5 exponentielles
- nous avons la chance que les autres étapes n'empirent pas cette borne
- long papier (128 pages) ...

Discussion

- Pourquoi une tour de cinq exponentielles ?
- c'est ce que donne notre méthode aucune autre raison ...
- l'existence d'une racine réelle pour un polynôme en une variable de degré d donne déjà une inférence faible qui fait intervenir un degré doublement exponentiel en d
- la preuve de Laplace part d'un polynôme de degré d et produit un polynôme de degré impair d^d : une tour de trois exponentielles pour l'inférence faible correspondant au théorème fondamental de l'algèbre
- notre méthode de projection basée uniquement sur l'algèbre donne des polynômes en une variable de degré doublement exponentiel
- donc : une tour de 5 exponentielles
- nous avons la chance que les autres étapes n'empirent pas cette borne
- long papier (128 pages) ...

Discussion

- Pourquoi une tour de cinq exponentielles ?
- c'est ce que donne notre méthode aucune autre raison ...
- l'existence d'une racine réelle pour un polynôme en une variable de degré d donne déjà une inférence faible qui fait intervenir un degré doublement exponentiel en d
- la preuve de Laplace part d'un polynôme de degré d et produit un polynôme de degré impair d^d : une tour de trois exponentielles pour l'inférence faible correspondant au théorème fondamental de l'algèbre
- notre méthode de projection basée uniquement sur l'algèbre donne des polynômes en une variable de degré doublement exponentiel
- donc : une tour de 5 exponentielles
- nous avons la chance que les autres étapes n'empirent pas cette borne
- long papier (128 pages) ...

Discussion

- Pourquoi une tour de cinq exponentielles ?
- c'est ce que donne notre méthode aucune autre raison ...
- l'existence d'une racine réelle pour un polynôme en une variable de degré d donne déjà une inférence faible qui fait intervenir un degré doublement exponentiel en d
- la preuve de Laplace part d'un polynôme de degré d et produit un polynôme de degré impair d^d : une tour de trois exponentielles pour l'inférence faible correspondant au théorème fondamental de l'algèbre
- notre méthode de projection basée uniquement sur l'algèbre donne des polynômes en une variable de degré doublement exponentiel
- donc : une tour de 5 exponentielles
- nous avons la chance que les autres étapes n'empirent pas cette borne
- long papier (128 pages) ...

Discussion

- Qu'est ce qu'on peut espérer?
- Positivstellensatz: bornes inférieures simplement exponentielles (Grigorev Vorobjov)
- Meilleure borne inférieure pour le 17ème problème de Hilbert : degré linéaire en k (résultat récent de Bleckerman et cie) !
- Bornes supérieures
- Nullstellensatz : simplement exponentiel (..., Kollar, ...).
- Décider qu'un système de conditions de signes est vide (en projetant les variables "par bloc") : simplement exponentiel: résultats de Grigori'ev-Vorobjov, est ce qu'on peut s'en servir ?

Discussion

- Qu'est ce qu'on peut espérer?
- Positivstellensatz: bornes inférieures simplement exponentielles (Grigorev Vorobjov)
- Meilleure borne inférieure pour le 17ème problème de Hilbert : degré linéaire en k (résultat récent de Bleckerman et cie) !
- Bornes supérieures
- Nullstellensatz : simplement exponentiel (..., Kollar, ...).
- Décider qu'un système de conditions de signes est vide (en projetant les variables "par bloc") : simplement exponentiel: résultats de Grigori'ev-Vorobjov, est ce qu'on peut s'en servir ?

Discussion

- Qu'est ce qu'on peut espérer?
- Positivstellensatz: bornes inférieures simplement exponentielles (Grigorev Vorobjov)
- Meilleure borne inférieure pour le 17ème problème de Hilbert : degré linéaire en k (résultat récent de Bleckerman et cie) !
- Bornes supérieures
- Nullstellensatz : simplement exponentiel (..., Kollar, ...).
- Décider qu'un système de conditions de signes est vide (en projetant les variables "par bloc") : simplement exponentiel: résultats de Grigori'ev-Vorobjov, est ce qu'on peut s'en servir ?

Discussion

- Qu'est ce qu'on peut espérer?
- Positivstellensatz: bornes inférieures simplement exponentielles (Grigorev Vorobjov)
- Meilleure borne inférieure pour le 17ème problème de Hilbert : degré linéaire en k (résultat récent de Bleckerman et cie) !
- Bornes supérieures
- Nullstellensatz : simplement exponentiel (..., Kollar, ...).
- Décider qu'un système de conditions de signes est vide (en projetant les variables "par bloc") : simplement exponentiel: résultats de Grigori'ev-Vorobjov, est ce qu'on peut s'en servir ?

Discussion

- Qu'est ce qu'on peut espérer?
- Positivstellensatz: bornes inférieures simplement exponentielles (Grigorev Vorobjov)
- Meilleure borne inférieure pour le 17ème problème de Hilbert : degré linéaire en k (résultat récent de Bleckerman et cie) !
- Bornes supérieures
- Nullstellensatz : simplement exponentiel (..., Kollar, ...).
- Décider qu'un système de conditions de signes est vide (en projetant les variables "par bloc") : simplement exponentiel: résultats de Grigori'ev-Vorobjov, est ce qu'on peut s'en servir ?

References

[HS] Sinaceur H. *Corps et modèles*, Mathesis, Vrin, 1991.
[BGP] Blekherman G., Gouveia J. and Pfeiffer J. *Sums of Squares on the Hypercube* Manuscript. arXiv:1402.4199.

[GV1] D. Grigoriev, N. Vorobjov, *Solving systems of polynomial inequalities in subexponential time*, Journal of Symbolic Computation, 5, 1988, 1-2, 37-64.

[GV2] D. Grigoriev, N. Vorobjov, *Complexity of Null- and Positivstellensatz proofs*, Annals of Pure and Applied Logic 113 (2002) 153-160.

[PR] D. Perrucci, M.-F. Roy, *Elementary recursive quantifier elimination based on Thom encoding and sign determination*, to appear in Annals of Pure and Applied Logic (arXiv:1609.02879v2).

[LPR] H. Lombardi, D. Perrucci, M.-F. Roy, *An elementary recursive bound for effective Positivstellensatz and Hilbert 17-th problem* ,to appear in Memoirs of the AMS (arXiv:1404.2338v3).

(avec toutes les autres références)