Quantifier elimination versus Hilbert's 17 th problem

Marie-Françoise Roy
Université de Rennes 1, France

based in part on a collaboration with
Henri Lombardi
Université de Franche-Comté, France
Daniel Perrucci
Universidad de Buenos Aires, Argentina

7 september 2018 *EWM General Meeting*

Hilbert's 17th Problem

- To write a polynomial (in one or several variables) as a sum of squares gives an immediate proof that this polynomial cannot take a negative value.
- Algebraic certificate of positivity

Sums of squares of polynomials

- If a positive polynomial a sum of squares of polynomials ?
- Yes if the number of variables is 1.
- Indication : decompose the polynomial in powers of irreducible polynomials: the factors of degree 2 (corresponding to complex roots) are sums of squares, the factors of degree 1 (corresponding to real roots) appear with an even exponent, product of sums of squares is a sum of squares.

Positivity and sum of squares

- If a positive polynomial a sum of squares of polynomials ?
- Yes if the number of variables is 1.
- Yes if the degree is 2.
- A quadratic form taking only positive values is a sum of squares of linear polynomials.

Positivité et sommes de carrés

- If a positive polynomial a sum of squares of polynomials ?
- Yes if the number of variables is 1.
- Yes if the degree is 2.
- No in general.
- First explicit counter-example Motzkin '69

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

is positive and is not a square of polynomials.

The counter example

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

- M is positive. Indication: the arithmetic mean is always at least the geometric mean .
- M is not a sum of squares of polynomials. Indication : try to write it as a sum of squares of polynomials of degree 3 and verify that it is t impossible.
- Starting point: no monomial X^3 can appear in the sum of squares. Etc ...

Hilbert’s 17-th problem

- Reformulation proposed after discussing with Minkowski.
- Question Hilbert ’1900.
- Is a positive polynomial a sum of squares of rational functions?
- Artin ’27: Positive answer. Non-constructive proof.

Hilbert's 17-th problem

- Reformulation proposed after discussing with Minkowski.
- Question Hilbert '1900.
- Is a positive polynomial a sum of squares of rational functions?
- Artin '27: Positive answer. Non-constructive proof.

Scheme of Artin's proof

- Suppose that P is not a sum of squares of rational functions.
- Sums of squares form a proper cone of the field of rational functions and do not contain du P (a cone contains squares and is closed by addition and multiplication, a proper cone does not contain -1).

Scheme of Artin's proof

- Suppose that P is not a sum of squares of rational functions.
- Sums of squares form a proper cone of the field of rational functions and do not contain du P (a cone contains squares and is closed by addition and multiplication, a proper cone does not contain -1).

Scheme of Artin's proof

- Suppose that P is not a sum of squares of rational functions.
- Sums of squares form a proper cone of the field of rational functions and do not contain du P
- Using Zorn's lemma, we get a maximal proper cone of the field of rational functions that does not contain P. Such a maximal proper cone defines a total order on the field of rational functions with P negative.

Scheme of Artin's proof

- Suppose that P is not a sum of squares of rational functions.
- Sums of squares form a proper cone of the field of rational functions and do not contain du P
- Using Zorn's lemma, we get a maximal proper cone of the field of rational functions that does not contain P. Such a maximal proper cone defines a total order on the field of rational functions with P negative.

Scheme of Artin's proof

- Suppose that P is not a sum of squares of rational functions.
- Sums of squares form a proper cone of the field of rational functions and do not contain du P
- Using Zorn's lemma, we get a total order on the field of rational functions with P negative. $(\star)$.
- A real closed field is a totally ordered field where positive elements are squares and every polynomial of odd degree has a root.
- Every ordered field has a real closure.
- Taking the real closure of the field of rational functions for the order obtained in $(\star)$, we get a field where P takes nagative value (evaluating at the "generic point" = point $(X_1, \ldots, X_k)$).

Scheme of Artin's proof

- Suppose that P is not a sum of squares of rational functions.
- Sums of squares form a proper cone of the field of rational functions and do not contain du P
- Using Zorn's lemma, we get a total order on the field of rational functions with P negative. $(\star)$.
- A real closed field is a totally ordered field where positive elements are squares and every polynomial of odd degree has a root.
- Every ordered field has a real closure.
- Taking the real closure of the field of rational functions for the order obtained in $(\star)$, we get a field where P takes nagative value (evaluating at the "generic point" = point $(X_1, \ldots, X_k)$).

Scheme of Artin's proof

- Suppose that P is not a sum of squares of rational functions.
- Sums of squares form a proper cone of the field of rational functions and do not contain du P
- Using Zorn's lemma, we get a total order on the field of rational functions with P negative. $(\star)$.
- Taking the real closure of the field of rational functions for the order obtained in $(\star)$, we get a field where P takes nagative value (evaluating at the "generic point" = point $(X_1, \ldots, X_k)$)
- Finally P takes negative values at a real point. First example of a transfer principle in real algebraic geometry. Based on Sturm's theorem, or Hermite's quadratic form.

Transfer principle

- A statement about elements of $\mathbb{R}$ which is true in a real closed field containing $\mathbb{R}$ (such that the real closure of the field of rational functions on the order chosen in $(\star)$) is true in $\mathbb{R}$.
- Not any statement, a "statement of the first order logic".
- Example of such a statement

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

  is true in a real closed field containing $\mathbb{R}$ if and only if it is true in $\mathbb{R}$.
- Exactly what we need to finish Artin's proof.
- Special case of quantifier elimination.

Quantifier elimination

- What is quantifier elimination ?
- High school mathematics.

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

$$\Longleftrightarrow$$

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

- If true in a real closed field containing $\mathbb{R}$, true in $\mathbb{R}$!
- True for any formula, resultat of Tarski, uses generalisations of Sturm's theorem, or Hermite's quadratic form.

Quantifier elimination

- What is quantifier elimination ?
- High school mathematics.

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

$$\Longleftrightarrow$$

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

- If true in a real closed field containing $\mathbb{R}$, true in $\mathbb{R}$!
- True for any formula, resultat of Tarski, uses generalisations of Sturm's theorem, or Hermite's quadratic form.

Quantifier elimination

- What is quantifier elimination ?
- High school mathematics.

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

$$\Longleftrightarrow$$

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

- If true in a real closed field containing $\mathbb{R}$, true in $\mathbb{R}$!
- True for any formula, resultat of Tarski, uses generalisations of Sturm's theorem, or Hermite's quadratic form.

Quantifier elimination

- What is quantifier elimination ?
- High school mathematics.

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

$$\Longleftrightarrow$$

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

- If true in a real closed field containing $\mathbb{R}$, true in $\mathbb{R}$!
- True for any formula, resultat of Tarski, uses generalisations of Sturm's theorem, or Hermite's quadratic form.

Hermite's quadratic form

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

where $\mu(x)$ is the multiplicity of x.

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

Hermite's quadratic form

$$a \neq 0, P(x) = ax^2 + bx + c == a(x - x_1)(x - x_2)$$
$$N_0 = x_1^0 + x_2^0 = 2$$
$$N_1 = x_1 + x_2 = -\frac{b}{a}$$
$$N_2 = x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1 x_2 = \frac{b^2}{a^2} - 2\frac{c}{a} = \frac{b^2 - 2ac}{a^2}$$
$$\mathrm{Herm}(P) = \begin{bmatrix} N_0 & N_1 \\ N_1 & N_2 \end{bmatrix} = \begin{bmatrix} 2 & -\frac{b}{a} \\ -\frac{b}{a} & \frac{b^2-2ac}{a^2} \end{bmatrix}$$
$$\det(\mathrm{Herm}(P)) = \frac{b^2 - 4ac}{a^2} = \frac{\Delta}{a^2}$$

The signature of $\mathrm{Herm}(P)$ is

- 2 if $\Delta > 0$ (2 real roots)
- 1 if $\Delta = 0$ (1 real root)
- 0 if $\Delta < 0$ (no real root)

Hermite's quadratic form

Proposition

The signature of Hermite's quadratic form $\mathrm{Herm}(P)$ *is the number of real roots of* P*.*

Indication : conjugate complex roots contribute for a difference of two squares.
Moreover the signature can be computed within the base field.

Generailized Hermite's quadratic form

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

where$\mu(x)$ is the multiplicity of x, $\mathrm{Herm}(P,Q)_{i,j} = N_{i+j-2}(P,Q)$.

Proposition

The signature of generalized Hermite's quadratic form $\mathrm{Herm}(P,Q)$ *is the Tarski's query of P and Q :*

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

Indication : conjugate complex roots contribute for a difference of two squares.
We can then determine thanks to several Tarski queries the number of roots of P whiere $Q > 0$ etc ... without approximating the roots ..

Quantifier elimination

- Most quantifier elimination methods eliminate variables one after the other : projection method.
- non-empty sign conditions for $\mathcal{P} \subset \mathbf{K}[x_1, \ldots, x_k]$ are fixed by non-empty sign conditions for $\mathrm{Proj}(\mathcal{P}) \subset \mathbf{K}[x_1, \ldots, x_{k-1}]$
- Tarski's original method purely algebraic (based on Tarskis data) but primitive recursive. $\mathrm{Proj}(\mathcal{P})$ is a list of minors of generalized Hermite's quadratic form between products of elements of $\mathcal{P}$
- the projection method can be made more efficient = elementary recursive
- the correctness proof of the classical cylindrical decomposition (Collins) uses the geometric notion of connected component
- new elementary recursive projection method based only on algebra, smaller $\mathrm{proj}(\mathcal{P})$.

Tools for elementary quantifier elimination based only on algebra

- Thom's encoding : a real root x of a univariate polynomial P is identified by the signs at x of the derivatives of P
- sign determination : compute at the roots of P the signs of the list of polynomials $Q_1, \ldots, Q_s$ by a quick algorithm using Tarski data of P and products of "few" of the Q_i,
- sign determination is used to compute Thom's encodings
- "small" $\mathrm{proj}(\mathcal{P})$
- gives a quantifier elimination method elementary recursive

Even better complexity using block projection (but not purely algebraic)

Scheme of Artin's proof

- Suppose that P is not a sum of squares of rational functions.
- Sums of squares form a proper cone of the field of rational functions and do not contain du P
- Using Zorn's lemma, we get a total order on the field of rational functions with P negative. $(\star)$.
- Taking the real closure of the field of rational functions for the order obtained in $(\star)$, we get a field where P takes nagative value (evaluating at the "generic point" = point $(X_1, \ldots, X_k)$)
- Finally P takes negative values at a real point. First example of a transfer principle in real algebraic geometry. Based on generalized Hermite's quadratic form.

Hilbert's 17 th problem: what remains to be done

- Very indirect proof (by contraposition, uses Zorn, real closure).
- Artin notes that an effective construction is desirable but difficult.
- No indication on the denominators : bounds on the degrees ?
- Effectivity Problem : is there an algorithm deciding whether a polynomial takes only positive value?
- This can be decided by quantifier elimination by a purely algebraic method and an elementary recursive complexity.
- But how to construct the representation as sums of squares ?
- Complexity Problem : what are the best degree bounds on the derees in the representation ?

Hilbert's 17 th problem: what remains to be done

- Very indirect proof (by contraposition, uses Zorn, real closure).
- Artin notes that an effective construction is desirable but difficult.
- No indication on the denominators : bounds on the degrees ?
- Effectivity Problem : is there an algorithm deciding whether a polynomial takes only positive value?
- This can be decided by quantifier elimination by a purely algebraic method and an elementary recursive complexity.
- But how to construct the representation as sums of squares ?
- Complexity Problem : what are the best degree bounds on the derees in the representation ?

Hilbert's 17 th problem: what remains to be done

- Very indirect proof (by contraposition, uses Zorn, real closure).
- Artin notes that an effective construction is desirable but difficult.
- No indication on the denominators : bounds on the degrees ?
- Effectivity Problem : is there an algorithm deciding whether a polynomial takes only positive value?
- This can be decided by quantifier elimination by a purely algebraic method and an elementary recursive complexity.
- But how to construct the representation as sums of squares ?
- Complexity Problem : what are the best degree bounds on the derees in the representation ?

Hilbert's 17 th problem: what remains to be done

- Very indirect proof (by contraposition, uses Zorn, real closure).
- Artin notes that an effective construction is desirable but difficult.
- No indication on the denominators : bounds on the degrees ?
- Effectivity Problem : is there an algorithm deciding whether a polynomial takes only positive value?
- This can be decided by quantifier elimination by a purely algebraic method and an elementary recursive complexity.
- But how to construct the representation as sums of squares ?
- Complexity Problem : what are the best degree bounds on the derees in the representation ?

Positivstellensatz (Krivine '64, Stengle '74)

- Find algebraic identities certifiying that a system of sign conditions is empty.
- In the spirit of Hilbert's Nullstellensatz.
  K a field, **C** an algebraic closed extension of **K**,
  $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$
  $P_1 = \ldots = P_s = 0$ has no solution in $\mathbf{C}^k$
  $\iff$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$

Positivstellensatz (Krivine '64, Stengle '74)

- Find algebraic identities certifiying that a system of sign conditions is empty.
- In the spirit of Hilbert's Nullstellensatz.
  K a field, **C** an algebraic closed extension of **K**,
  $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$
  $P_1 = \ldots = P_s = 0$ has no solution in $\mathbf{C}^k$
  $\Longleftrightarrow$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$

Quantitative Nullstellensatz

- **K** a field, **C** an algebraic closed extension of **K**, $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$
  $P_1 = \ldots = P_s = 0$ has no solution in $\mathbf{C}^k$
  $\iff$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- What are the degrees of the A_i ?
- using resultants (Grete Hermann 1925): doubly exponential degrees in k
- more recently (Brownawell 1987 (analytic methods),..., Kollar (algebraic methods), ... singly exponential degrees in k, cannot be improved

Quantitative Nullstellensatz

- **K** a field, **C** an algebraic closed extension of **K**,
  $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$
  $P_1 = \ldots = P_s = 0$ has no solution in $\mathbf{C}^k$
  $\Longleftrightarrow$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- What are the degrees of the A_i ?
- using resultants (Grete Hermann 1925): doubly exponential degrees in k
- more recently (Brownawell 1987 (analytic methods),..., Kollar (algebraic methods), ... singly exponential degrees in k, cannot be improved

Quantitative Nullstellensatz

- **K** a field, **C** an algebraic closed extension of **K**,
  $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$
  $P_1 = \ldots = P_s = 0$ has no solution in $\mathbf{C}^k$
  $\Longleftrightarrow$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- What are the degrees of the A_i ?
- using resultants (Grete Hermann 1925): doubly exponential degrees in k
- more recently (Brownawell 1987 (analytic methods),...,
  Kollar (algebraic methods), ... singly exponential degrees in k, cannot be improved

Positivstellensatz

More complicated in the real case

- **K** an ordered field (to simplify statement :where all the positives are squares), **R** a real closed field extension of **K**,

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

$$\mathcal{H}(x) : \begin{cases} P_i(x) & \neq & 0 & \text{for} & i \in I_{\neq} \\ P_i(x) & \geq & 0 & \text{for} & i \in I_{\geq} \\ P_i(x) & = & 0 & \text{for} & i \in I_{=} \end{cases} \quad \text{no solution in } \mathbf{R}^k$$

$\Longleftrightarrow$

$\exists \quad S, N, Z$ with $S(x) > 0, N(x) \geq 0, Z(x) = 0$ under the hypothesis $\mathcal{H}(x)$ and

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

This is noted

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

Incompatibilities

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

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

with

$S \in \left\{\prod_{i \in I_{\neq}} P_i^{2e_i}\right\}$ $\leftarrow$ monoid associated to $\mathcal{H}$

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

$Z \in \langle P_i \mid i \in I_{=} \rangle$ $\leftarrow$ ideal associated to $\mathcal{H}$

Degree of an incompatibility

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

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

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

the degree of $\mathcal{H}$ is the maximum degree of

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

Example of incompatibility

$$P < 0, P \geq 0 \text{ has no solution in } \mathbb{R}^k$$

$$P \neq 0, -P \geq 0, P \geq 0 \text{ has no solution in } \mathbb{R}^k$$

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

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

The degree of this incompatibility is $2\deg(P)$.

Example of incompatibility

$$P < 0, P \geq 0 \text{ has no solution in } \mathbb{R}^k$$

$$P \neq 0, -P \geq 0, P \geq 0 \text{ has no solution in } \mathbb{R}^k$$

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

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

The degree of this incompatibility is $2\deg(P)$.

Positivstellensatz: proofs

- Positivstellensatz's classical proofs are based Zorn's lemma and transfer principal , very similar to Artin's proof for Hilbert's 17 th problem.
- Constructive proofs use quantifier elimination.
- Principle: transform a proof of the fact that a system of sign conditions is empty, using a quantifier elimination method, into an incompatibility.

$$P \geq 0 \text{ in } \mathbb{R}^k \iff P(x) < 0 \quad \text{has no solution}$$

$$\iff \begin{cases} P(x) & \neq & 0 \\ -P(x) & \geq & 0 \end{cases} \quad \text{has no solution}$$

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

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

Positivstellensatz implies Hilbert's 17 th probleme

$$P \geq 0 \text{ in } \mathbb{R}^k \iff P(x) < 0 \quad \text{has no solution}$$

$$\iff \begin{cases} P(x) & \neq & 0 \\ -P(x) & \geq & 0 \end{cases} \quad \text{has no solution}$$

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

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

Our strategy

- For every empty sign condition, construct an incompatibility and controll the degree.
- Find Hilbert's 17th problem as a particular case
- Using the notions introduced by Lombardi '90
- Key concept: weak inference.

Weak Inférence

(in the particular case we need)

Definition (weak inference)

$\mathcal{F}, \mathcal{G}$ systems of sign conditions $\mathbf{K}[u]$ and $\mathbf{K}[u,t]$. A weak inference

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

is a construction which for every system of sign condition $\mathcal{H}$ in $\mathbf{K}[v]$ with $v \supset u$ not containing t and every incompatibility

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

produces an incompatibility

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

From right to left.

Construction ? an example !

Example of a weak inference : positive elements are squares

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

$A(u)$ any polynomial in several variables

$$\downarrow \mathcal{H}, A(u) = t^2 \downarrow \quad \longrightarrow \quad \begin{cases} \mathcal{H}(v) \\ A(u) = t^2 \end{cases} \text{has no solution}$$

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

$$\downarrow \mathcal{H}(v),\ \ A(u) \geq 0 \downarrow \quad \longrightarrow \quad \begin{cases} \mathcal{H}(v) \\ A(u) \geq 0 \end{cases} \text{has no solution}$$

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

From right to left.

Example of a weak inference : positive elements are squares

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

$A(u)$ any polynomial in several variables

$$\downarrow \mathcal{H}, A(u) = t^2 \downarrow \quad \longrightarrow \quad \left\{ \begin{array}{c} \mathcal{H}(v) \\ A(u) = t^2 \end{array} \right. \quad \text{has no solution}$$

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

$$\downarrow \mathcal{H}(v),\ \ A(u) \geq 0 \downarrow \quad \longrightarrow \quad \left\{ \begin{array}{c} \mathcal{H}(v) \\ A(u) \geq 0 \end{array} \right. \quad \text{has no solution}$$

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

From right to left.

The construction

Start from incompatibility

$$S + \sum_i V_i^2(t) \cdot N_i + \sum_j W_j(t) \cdot Z_j + W(t) \cdot (t^2 - A) = 0 \qquad (1)$$

$V_{i1} \cdot t + V_{i0}$ remainder of $V_i(t)$ in the division by $t^2 - A$
$W_{j1} \cdot t + W_{j0}$ remainder of $W_j(t)$ in the division by $t^2 - A$
there exists $W'(t) \in \mathbf{K}[v][t]$ such that

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

which is rewritten in

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

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

The construction (end)

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

Examining degrees in t, we obtain $W''(t) = 0$, then $W''' = 0$
This ends the proof since

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

is the incompatibility we are looking for.
On we can keep track of the degrees with respect to the variabbles

Construction ?

- Procedure which makes it possible to construct a new incompatibility starting from an initial one.
- In our example :
  - Perform euclidean division.
  - Grouper terms differently.
  - Deduce that some pieces are zero by degree identification.
  - Keep track of the degree with respect to various variables.

List of statements that we need to translate into weak inferences

- Tools from classical algebra to modern computer algebra
- a positive polynomial has a real root (axiom)
- a real polynomials has a complex root (algebraic proof due to Laplace)

List of statements that we need to translate into weak inferences

- a positive polynomial has a real root
- a real polynomial has a complex root
- the signature of generalized Hermite's quadratic form is equal to the Tarski query and can be computed by sign conditions on principal minors
- Sylvester's inertia law: the signature of a quadratic form is well defined

List of statements that we need to translate into weak inferences

- a positive polynomial has a real root
- a real polynomial has a complex root
- the signature of generalized Hermite's quadratic form is equal to the Tarski query and can be computed by sign conditions on principal minors
- Sylvester's inertia law
- non empty sign conditions for a family of polynomials at the roots of a polynomial determined by the signs of minors of several generalized Hermite's quadratic forms (using Thom's encoding and sign determination)
- finally: non-empty sign conditions for $\mathcal{P} \subset \mathbf{K}[x_1, \ldots, x_k]$ deteremined by non empty sign conditions for $\mathrm{proj}(\mathcal{P}) \subset \mathbf{K}[x_1, \ldots, x_{k-1}]$: using the elementary recursive projection method using only algebra

List of statements that we need to translate into weak inferences

- a positive polynomial has a real root
- a real polynomial has a complex root
- the signature of generalized Hermite's quadratic form is equal to the Tarski query and can be computed by sign conditions on principal minors
- Sylvester's inertia law
- non empty sign conditions for a family of polynomials at the roots of a polynomial determined by the signs of minors of several generalized Hermite's quadratic forms (using Thom's encoding and sign determination)
- finally: non-empty sign conditions for $\mathcal{P} \subset \mathbf{K}[x_1, \ldots, x_k]$ deteremined by non empty sign conditions for $\mathrm{proj}(\mathcal{P}) \subset \mathbf{K}[x_1, \ldots, x_{k-1}]$: using the elementary recursive projection method using only algebra

How to produce the sum of squares?

Suppose tat P takes only positive values. The proof by quantifier elimination that

$$P \geq 0$$

is transformed, step by step, in the proof of the weak inference

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

Which means that is we have an incompatibility of $\mathcal{H}$ with $P \geq 0$, we can construct an incompatibility of $\mathcal{H}$

From right to left.

How to produce the sum of squares?

$P < 0$, i.e. $P \neq 0, -P \geq 0$, is incompatible with $P \geq 0$, since

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

This is the incompatibility of the system $P \geq 0, P \neq 0, -P \geq 0$ we are starting from!
So, using the weak inference

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

we know how to construct an incompatibility of $P \neq 0, -P \geq 0$
...

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

This is the incompatibility we are looking for !!
We have expressed P as a sum of squares of rational functions !!!

Hilbert's 17 th problem degree bounds

• Kreisel '57 - Daykin '61 - Lombardi '90 - Schmid '00:
Constructive proofs $\rightsquigarrow$ primitives recursive degree bounds k and $d = \deg P$.

• Our results '14: based on purely algebraic and elementary recursive quantifier elimination $\rightsquigarrow$ elémentary recursive degree bounds

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

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).

(with more references)