Effectivity Issues and Results for Hilbert 17 th Problem

Marie-Françoise Roy
Université de Rennes 1, France

joint work with

Henri Lombardi
Université de Franche-Comté, France

and

Daniel Perrucci
Universidad de Buenos Aires, Argentina

Berkeley - September 26, 2014

Positivity and sums of squares

- Is a non-negative 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 non negative and is not a sum of square of polynomials.

Hilbert 17th problem

- Reformulation proposed by Minkowski.
- Question Hilbert '1900.
- Is a a non-negative polynomial a sum of squares of rational functions ?
- Artin '27: Affirmative answer. Non-constructive.

Outline of Artin's proof

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

Outline of Artin's proof

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

Outline of Artin's proof

- Suppose P is not a sum of squares of rational functions.
- Sums of squares form a proper cone of the field of rational functions, and does not contain P .
- Using Zorn, get a total order on the field of rational functions which does not contain P.
- Taking the real closure of the field of rational functions for this order, get a field in which P takes negative values (when evaluated at the variables, which are elements of the real closure).
- Then P takes negative values over the reals. First instance of a transfer principle in real algebraic geometry. Based on Sturm's theorem, or Hermite quadratic form.

Remaining problems

- Very indirect proof (by contraposition, uses Zorn).
- Artin notes effectivity is desirable but difficult.
- No hint on denominators: what are the degree bounds ?
- Effectivity problems : is there an algorithm checking whether a given polynomial is everywhere nonnegative and if so provides a representation as a sum of squares?
- Complexity problems : what are the best possible bounds on the degrees of the polynomials in this representation ?

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

• Our work '14: another constructive proof $\rightsquigarrow$ elementary recursive degree bound:

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

Positivstellensatz

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

Positivstellensatz

- Find algebraic identities certifying that a system of sign condition is empty.
- In the spirit of Farkas Lemma.
  K a, ordered field, **R** a real closed extension of **K**,

  $$\sum A_{ij}x_j + b_i \geq 0, \sum C_{nj}x_j + d_n = 0$$

  no solution in $\mathbf{R}^k$

  $$\Longleftrightarrow \exists\ \lambda_i \geq 0, \mu_k$$

  $$1 + \sum \lambda_i(\sum A_{ij}x_j + b_i) + \sum \mu_n(\sum C_{nk}x_k + d_n) = 0.$$

- For real numbers and arbitrary degrees, statement more complicated.

Positivstellensatz =SOS proof of impossibility

- **K** an ordered field, **R** a real closed extension of **K**,
- $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$,
- $I_{\neq}, I_{\geq}, I_{=} \subset \{1, \ldots, s\}$,

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

there exist S, N, Z, deduced from $\mathcal{H}(x)$ using SOS proofs such that

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

Positivstellensatz (Krivine '64, Stengle '74)

More precisely

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

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

with

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

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

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

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

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

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:

$$\left\{\begin{array}{rcl} x & \neq & 0 \\ y - x^2 - 1 & \geq & 0 \\ xy & = & 0 \end{array}\right. \quad \text{no solution in } \mathbb{R}^2$$

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

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

The degree of this is incompatibility is 4.

Positivstellensatz: proofs

- Classical proofs of Positivstellensatz based on Zorn's lemma and Tranfer principle, very similar to Artin's proof for Hilbert 17th problem [BPR].
- Constructive proofs use quantifier elimination over the reals.
- What is quantifier elimination ?
- You know it from high school
  ... in a special case !

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

$$\iff$$

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

- True for any formula, due to Tarski, use generalizations of Sturm's theorem, or Hermite quadratic form [BPR].

Positivstellensatz: Constructive proofs

- Classical proofs of Positivstellensatz based on Zorn's lemma and Transfer principle, very similar to Artin's proof for Hilbert's 17 th problem [BCR].
- Constructive proofs use quantifier elimination over the reals.
- Transform a proof that a system of sign conditions is empty, based on a quantifier elimination method, into an incompatibility.

Positivstellensatz: Constructive proofs

• Lombardi '90:
Primitive recursive degree bounds on k, $d = \max \deg P_i$ and $s = \# P_i$.

Based in Cohen-Hörmander algorithm for quantifier elimination [BCR]:

- exponential tower of height $k+4$,
- $d\log(d) + \log\log(s) + c$ on the top.

• Our work: Based on (a variant of) cylindrical decomposition [BPR].
Elementary recursive degree bound in k, d and s:

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

Positivstellensatz implies Hilbert 17th problem

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

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

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

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

Our strategy

- For every system of sign conditions with no solution, construct an algebraic incompatibility and control the degrees for the Positivstellensatz.
- Uses notions introduced in Lombardi '90
- Key concept : weak inference.

Weak inferences: first example

$$A > 0, \quad B \geq 0 \quad \Longrightarrow \quad A + B > 0.$$

Let $\mathcal{H}$ be any system of sign conditions.

$$\downarrow \mathcal{H}, \ \ A + B > 0 \downarrow \quad \longrightarrow \quad \begin{cases} \mathcal{H}(x) & \\ A(x) + B(x) & > \quad 0 \end{cases} \quad \text{no solution}$$

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

$$\downarrow \mathcal{H}, \ \ A > 0, \ \ B \geq 0 \downarrow \quad \longleftarrow \quad \begin{cases} \mathcal{H}(x) & & \\ A(x) & > & 0 \\ B(x) & \geq & 0 \end{cases} \quad \text{no solution}$$

$$A > 0, \quad B \geq 0 \quad \vdash \quad A + B > 0.$$

Weak inferences go from right to left.

$$A > 0, \quad B \geq 0 \qquad \vdash \qquad A + B > 0$$

$$\downarrow \mathcal{H}, \; A + B > 0 \downarrow \quad \rightarrow \quad \downarrow \mathcal{H}, \; A + B \neq 0, \; A + B \geq 0 \downarrow$$

$$\underbrace{(A+B)^{2e} S}_{> 0} \; + \; \underbrace{N + N'(A+B)}_{\geq 0} \; + \; \underbrace{Z}_{= 0} \; = \; 0$$

$$\downarrow$$

$$\underbrace{A^{2e} S}_{> 0} \; + \; \underbrace{\sum_{i=0}^{2e-1} \binom{2e}{i} A^i B^{2e-1} S + N + N'A + N'B}_{\geq 0} \; + \; \underbrace{Z}_{= 0} \; = \; 0$$

$$\downarrow \mathcal{H}, \; A \neq 0, \; A \geq 0, \; B \geq 0 \downarrow \quad \rightarrow \quad \downarrow \mathcal{H}, \; A > 0, \; B \geq 0 \downarrow$$

$$A > 0, \quad B \geq 0 \qquad \vdash \qquad A + B > 0$$

What about degrees?

$$\underline{(A+B)^{2e}S} + \underline{N} + \underline{N'(A+B)} + \underline{Z} = 0$$

$$\downarrow$$

$$\underline{A^{2e}S} + \sum_{i=0}^{2e-1} \underline{\binom{2e}{i} A^i B^{2e-1} S} + \underline{N} + \underline{N'A} + \underline{N'B} + \underline{Z} = 0$$

initial incompatibility
degree

$\rightarrow$

final incompatibility
degree

$$\delta$$

$$\delta + \max\{1, 2e\} \cdot (\max\{\deg A, \deg B\} - \deg\{A+B\})$$

Symbolic degree !!

Weak inferences: case by case reasoning

$$A \neq 0 \quad \Longrightarrow \quad A < 0 \quad \vee \quad A > 0$$

Let $\mathcal{H}$ be any system of sign conditions.

$$\downarrow \mathcal{H},\ \ A < 0 \downarrow \quad \longrightarrow \quad \begin{cases} \mathcal{H}(x) & \\ A(x) & < \quad 0 \end{cases} \quad \text{no solution}$$

$$\downarrow \mathcal{H},\ \ A > 0 \downarrow \quad \longrightarrow \quad \begin{cases} \mathcal{H}(x) & \\ A(x) & > \quad 0 \end{cases} \quad \text{no solution}$$

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

$$\downarrow \mathcal{H},\ \ A \neq 0 \downarrow \quad \longleftarrow \quad \begin{cases} \mathcal{H}(x) & \\ A(x) & \neq \quad 0 \end{cases} \quad \text{no solution}$$

$$A \neq 0 \quad \vdash \quad A < 0 \quad \vee \quad A > 0$$

Again, from right to left.

$$A \neq 0 \quad \vdash \quad A < 0 \quad \vee \quad A > 0$$

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

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

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

$$A^{2e_1} S_1 + N_1 + Z_1 = N_1' A$$

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

$$A^{2e_2} S_2 + N_2 + Z_2 = -N_2' A$$

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

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

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

List of statements needed into weak inferences form

- Many simple weak inferences of that kind are combined to obtain more interesting weak inferences.
- Tools from classical algebra to modern computer algebra

  a real polynomial of odd degree has a real root

  a real polynomial has a complex root (using an algebraic proof due to Laplace) [BPR]

List of statements needed into weak inferences form

- a real polynomial of odd degree has a real root
- a real polynomial has a complex root
- signature of Hermite's quadratic form determined by the number of real roots of a polynomial and also by sign conditions on principal minors [BPR]
- Sylvester's inertia law: the signature of a quadratic form is well defined

List of statements into weak inferences form

- a real polynomial of odd degree has a real root
- a real polynomial has a complex root
- signature of Hermite's quadratic form
- Sylvester's inertia law
- realizable sign conditions for a family of univariate polynomials fixed by sign of minors of several Hermite quadratic form (using Thom's encoding of real roots by sign of derivatives) [BPR]
- realizable sign conditions for $\mathcal{P} \subset \mathbf{K}[x_1, \ldots, x_k]$ fixed by list of non empty sign conditions for $\mathrm{Proj}(\mathcal{P}) \subset \mathbf{K}[x_1, \ldots, x_{k-1}]$ (cylindrical decomposition) [BPR]

How is produced the sum of squares ?

Suppose that P takes always non negative values. The proof that

$$P \geq 0$$

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

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

Which means that if we have an initial incompatibility of $\mathcal{H}$ with $P \geq 0$, we know how to construct a final incompability of $\mathcal{H}$ it self

Going right to left.

How is produced the sum of squares ?

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

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

is an initial incompatibility of $P \geq 0, P \neq 0, -P \geq 0$!
Hence we know how to construct an incompatibility of $P \neq 0, -P \geq 0$

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

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

Why a tower of five exponentials ?

- outcome of our method ... no other reason ...
- cylindrical decomposition gives univariate polynomials of doubly exponential degrees
- dealing with univariate polynomials of degree d (real root for odd degree, complex root by Laplace) already gives three level of exponentials
- we are lucky enough that all the other steps do not spoil this bound
- long paper (85 pages) ... currently under review.

What can be hoped for ? ?

- Nullstellensatz : single exponential (..., Kollar, Jelonek, ...).
- Nullstellensatz: single exponential lower bounds (...,Philippon , ...).
- Positivstellensatz: single exponential lower bounds [GV].
- Best lower bound for Hilbert 17th problem : degree linear in k (recent result by [BGP]) !
- Deciding emptyness for the reals (critical point method : more sophisticated than cylindrical decomposition) : single exponential [BPR].

References

[BPR] Basu S., Pollack R. and Roy M.-F. *Algorithms in Real Algebraic Geometry*. Springer-Verlag, Berlin.
http://perso.univ-rennes1.fr/marie-francoise.roy/bpr-ed2-posted2.html
(Revised and completed 2013)

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

[BCR] Bochnak J., Coste M. and Roy M.-F. *Géométrie Algébrique Réelle* (*Real Algebraic Geometry*), Springer-Verlag, Berlin, 1987 (1998).

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

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

(and all other references there)

Thanks!