Elementary recursive bounds for Hilbert's 17-th problem: why 5 levels of exponentials ?

by Marie-Françoise Roy

IRMAR
CNRS/Université de Rennes 1

This talk is based on joint work with Henri Lombardi (Besançon, France) and Daniel Perrucci (Buenos Aires, Argentina). Follows a first talk by Daniel.

1 Sums of squares

Hilbert's question (1900), $X = (X_1, \ldots X_k)$: is it true that

$$P \in R[X] \text{ is non negative if and only if } P \in \sum R(X)^2$$

sum of squares of rational function (with denominators)

Artin's positive answer (1927): abstract algebra

Result about the reals, method of proof uses much more abstract objects : real closures of the field of rational functions.

Outline of Artin's proof:

- Start from P which is not a sum of squares of rational functions.
- Sums of squares do not contain P and form a proper cone.
- Using Zorn's lemma, obtain a maximal proper cone which does not contain P. Such a maximal cone is a total order.
- Taking the real closure of the field of rational functions for this order, get a field in which P takes negative values (the images of the variables).
- If P takes negative values in a real closed field containing the reals, P takes negative values over the reals. This is the first instance of a **transfer principle** in real algebraic geometry. Based on Sturm's theorem.

"quite indirect" : by contradiction + use of Zorn

Many problems after Artin's proof.

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?

Former results (see Daniel's talk for references to former work): primitive recursive degree bounds.

Our work [LPR] gives *elementary recursive* degree, precisely (d degree, k number of variables of the input polynomial)

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

Strategy For every unrealizable $\mathcal{H}$, construct an algebraic identity $\downarrow\mathcal{H}\downarrow$ and control the degrees for the Positivstellensatz. Hilbert 17 th problem follows (cf talk by Daniel).

Principle of the proof Translate a (very elementary) proof that $\mathcal{H}$ is *unrealizable* into an *incompatibility* (algebraic identity) $\downarrow\mathcal{H}\downarrow$.

Method already used by Lombardi in 1990 [Lom] to give primitive recursive bounds : the construction of the impossibility follows the proof of unrealizability based on the very elementary proof produced by the quantifier elimination method of Hormander [Hor],[BCR].

`primitive recursive degree bounds coming from Hormander's quantifier elimination algorithm`.

Here the construction of the incompatibility uses more sophisticated tools that can be used to prove the unrealizability

1. a real polynomial of odd degree has a real root
2. a real polynomial has a complex root (algebraic proof due to Laplace)
3. number of real roots given by the signature of Hermite's quadratic form (moment matrix (!)) which is also determined by sign conditions on principal minors
4. Sylvester's inertia law: the signature of a quadratic form is well defined
5. cylindrical decomposition : realizable sign conditions for $\mathcal{P} \subset R[X_1, ..., X_k]$ fixed by list of non empty sign conditions for $\mathrm{Proj}_{X_k}(\mathcal{P}) \subset R[X_1, ..., X_{k-1}]$. $\mathrm{Proj}_{X_k}(\mathcal{P})$ contains minors of several Hermite quadratic forms (using Thom's encoding of real roots by sign of derivatives)

necessary to construct the corresponding incompatibilities, `controling the degrees`.
main concept : weak inference (see Daniel's talk)
basic tools: algebraic identities, case by case reasoning (see Daniel' talk)

1.1 Base case: univariate polynomial (with parameters

A polynomial of odd degree has a real root

$P(u, y)$ polynomial monic with respect to y, of odd degree in y (with parameters u (many))

Since P has a root in R for every $u \in R^k$ it is clear that, for every system of sign conditions $\mathcal{H}$ ("context")

$$\text{if } \mathcal{H} \wedge P(u,t) = 0 \text{ is unrealizable, then } \mathcal{H} \text{ is unrealizable}$$

We need to prove

$$\vdash \ \exists t\, P(u,t) = 0$$

i.e. give a construction of $\downarrow\mathcal{H}\downarrow$ starting from $\downarrow\mathcal{H}, P(u,t) = 0\downarrow$

"goes from right to left"

Artin-Shreier's [AS] : in a maximally real field (-1 is not a sum of squares but in every algebraic extension -1 a sum of squares), every polynomial of odd degree has a root: proof is by induction on the degree p, using euclidean division.

Theorem 1. *Let $P(u,y) \in K[u,y]$ monic with respect to y of odd degree p in y. Then*

$$\vdash \ \exists t\, P(u,t) = 0$$

Suppose we have an initial incompatibility $\downarrow \mathcal{H}, P(u,t) = 0 \downarrow$ in variables (v,t), where $v \supset u$ and $t \notin v$, with degree in v bounded by δ_v and degree in t bounded by δ_t. The final incompatibility $\downarrow \mathcal{H} \downarrow$ has degree in v bounded by $3\mathrm{g}_1(p)\,(\delta_v + \delta_t \deg_u(P))$, where

$$\mathrm{g}_1(p) = 2^{3 \cdot 2^{p-1}}\, p^p.$$

`Degree: adds two level of exponentials`

A polynomial with real coefficients has a complex root [Lap]

$P(u,t)$ a polynomial monic and of degree p with respect to T.

$P(u,a+i\,b)=0$ is an abbreviation for the two equalities

$$P_{\mathrm{Im}}(u,a,b)=0, P_{\mathrm{Re}}(u,a,b)=0$$

expressing that the real and imaginary part of

$$P(u,a+i\,b)$$

are zero.

Since P has a root in $R[i]$ for every $\upsilon\in R^k$, it is clear that if $\mathcal{H}\wedge P(u,a+i\,b)=0$ is unrealizable then $\mathcal{H}$ is unrealizable.

Need to prove

$$\vdash\ \exists z\,[\,P(z)=0\,]$$

i.e. to give a construction of $\downarrow\mathcal{H}\downarrow$ from $\downarrow\mathcal{H}, P(u,a+i\,b)=0\downarrow$

"goes from right to left"

Based on the algebraic proof of the fundamental theorem of algebra (Laplace). Proof by induction on the exponent of 2 in the degree p, constructs a polynomial of odd degree $\leqslant p^p$, which has a real root, then a complex root of P by successive quadratic extensions.

Theorem 2. *Let $P(y) \in K[u, y]$ monic with respect to y, of degree p in y, $p = 2^r\, o \geq 1$, with o odd. Then ($z = a + i\, b$)*

$$\vdash \ \exists z \, [\, P(z) = 0 \,]$$

Suppose we have an initial incompatibility $\downarrow\mathcal{H}$, $P(u, a + i\ b) = 0\downarrow$ in $K[v, a, b]$, where $v \supset v$ and $a, b \notin v$, degree in v bounded by δ_v and degree in (a, b) bounded by δ_z. The final incompatibility $\downarrow\mathcal{H}\downarrow$ has degree in v bounded by $g_2(p)\,(\delta_v + \delta_z \deg_u(P))$ where

$$g_2(p) = 2^{2^{3(\frac{p}{2})^{2^r}}}$$

`Degree: adds three level of exponentials`

Factorization into irreducible real factors of degree 1 and 2 as incompabilities, with degree bounds.

$$\mathrm{Fact}^{\mu,\nu}(t,z)$$

describes the factorization of P into $\#\mu$ distinct real factors of degree 1 with multiplities $\mu_1,...,\mu_{\#\mu}$ and $\#\nu$ distinct irreducible real factors of degree 2

$$(t_k+a_k)^2+b_k^2$$

with multiplities $\nu_1,...,\nu_{\#\nu}$, $t=(t_1,...,t_{\#\mu})$ and $z=(z_1,...,z_{\#\nu})$, $z_k=a_k+i\,b_k, b_k\neq 0$.

That two quadratic factors are distinct is expressed by

$$\mathrm{Res}_y\big((y-a)^2+b^2,(y-a')^2+b'^2\big)=((a-a')^2+(b-b')^2)\cdot((a-a')^2+(b+b')^2)\neq 0$$

where Res_y is the resutant polynomial in the variable y.

`Degree: adds three level of exponentials`

Hermite's method [Her], [BPR]
$P(u,t)$ a polynomial monic in t of degree p.
Hermite's quadratic form, using Newton sums

$$\mathrm{Her}(P)(u) = \sum_{t \in Z(P(u),R[i])} \mu(t)(f_1 + f_2\, t + \cdots + f_p\, t^{p-1})^2,$$

Hermite's theory

$$\begin{aligned} \mathrm{Rk}(\mathrm{Her}(P)(u)) &= \text{number of complex roots of } P(u,t) \\ \mathrm{Si}(\mathrm{Her}(P)(u)) &= \text{number of real roots of } P(u,t) \end{aligned}$$

Complex conjugate roots give a difference of two squares, only real roots contribute to the signature.

fixing the number of distinct real and complex roots with multiplicities of P by (μ, ν), get a value $(\mathrm{Rk}_{\mathrm{Fact}}(\mu,\nu), \mathrm{Si}_{\mathrm{Fact}}(\mu,\nu))$ of the rank and signature of Hermite's quadratic form.

fixing a sign condition $\tau \in \{-1, 0, 1\}^{0,\ldots,p-1}$ on the principal minors of Hermite's quadratic form, get a value $(\mathrm{Rk}_{\mathrm{HMi}}(\tau), \mathrm{Si}_{\mathrm{HMi}}(\tau))$ of its rank and signature.

By Sylvester's inertia law,hese two values of the rank and signature cannot be different.

Theorem 3. *$P(u, y) \in K[u, y]$monic with respect to y of degree p in y.*

If $(\mathrm{Rk}_{\mathrm{HMi}}(\tau), \mathrm{Si}_{\mathrm{HMi}}(\tau)) \neq (\mathrm{Rk}_{\mathrm{Fact}}(\mu,\nu), \mathrm{Si}_{\mathrm{Fact}}(\mu,\nu))$, we have

$$\downarrow \mathrm{sign}(\mathrm{HMi}P)) = \tau, \mathrm{Fact}(P)^{\mu,\nu}(t, z) \downarrow$$

with degree bounded by $g_H(p) \deg_{t,z}(P)$, with

$$g_H(p) = 21 \cdot 2^{7p+1}\, p^{5p+6}\, 3^{4p+2}.$$

`Degree: one level of exponentials`

Similar result (statement would be more technical) for a useful generalization (sign determination) [BPR]

Hermite's quadratic form $\mathrm{Her}(P,Q)$

$$\begin{aligned}
\mathrm{Her}(P,Q) &= \sum_{t\in \mathrm{Zer}(P,R[i])} \mu(t)Q(t)(f_1+f_2\,t+\cdots+f_p\,t^{p-1})^2 \\
\mathrm{Rank}(\mathrm{Her}(P,Q)) &= \#\{x\in \mathrm{Zer}(P,R[i])|\ Q(x)\neq 0\} \\
\mathrm{Sign}(\mathrm{Her}(P,Q)) &= \#\{x\in \mathrm{Zer}(P,R)|\ Q(x)>0\}-\#\{x\in \mathrm{Zer}(P,R)|\ Q(x)<0\}
\end{aligned}$$

also determined by signs of principal minors

1.2 Removing one variable: cylindrical decomposition

$\mathcal{P}$ s polynomials in k variables, cylindrical decomposition produces $\mathrm{Proj}_{X_k}(\mathcal{P})$ in $k-1$ variables (minors of Hermite quadratic forms associated to products of (few) polynomials of $\mathcal{P}$). To every realizable sign condition τ on $\mathrm{Proj}_{X_k}(\mathcal{P})$ is associated the list $\mathrm{Sign}(\tau, \mathcal{P})$ of realizable sign conditions on $\mathcal{P}$ implied by τ.

Uses subresultants, sign determination, Thom encodings ...

If $\mathcal{H}$ is such that for every $\sigma \in \mathrm{Sign}(\tau, \mathcal{P})$, $\mathcal{H} \wedge \mathrm{sign}(\mathcal{P}) = \sigma$ is unrealizable, then $\mathcal{H} \wedge \mathrm{sign}(\mathrm{Proj}_{X_k}(\mathcal{P})) = \tau$ is unrealizable. Need to construct, given incompatibilities $\downarrow\mathcal{H} \wedge \mathrm{sign}(\mathcal{P}) = \sigma\downarrow$ for every $\sigma \in \mathrm{Sign}(\tau, \mathcal{P})$, an incompatibility $\downarrow\mathcal{H} \wedge \mathrm{sign}(\mathrm{Proj}_{X_k}(\mathcal{P})) = \sigma\downarrow$ which is the meaning of

$$(\star) \quad \mathrm{sign}(\mathrm{Proj}_{X_k}(\mathcal{P})) = \tau \vdash \bigvee_{\sigma \in \mathrm{Sign}(\tau, \mathcal{P})} \mathrm{sign}(\mathcal{P}) = \sigma$$

"goes from right to left"

`Degree: adds three level of exponentials`

induction on the number of variables: the degree produced at the end (univariate polynomials) $\mathrm{Proj}_{X_2}(...\mathrm{Proj}_{X_k}(\mathcal{P}))$ are d^{4^k}

1.3 Back to effective Hilbert 17 th problem

If it is true that $P \geqslant 0$ everywhere, want to construct an incompatibility $\downarrow\mathcal{H}\downarrow$ where $\mathcal{H}_{\neq} = \{P\}, \mathcal{H}_{\geq} = \{-P\}, \mathcal{H}_{=} = \emptyset$ (expressing that $P < 0$ is empty)

start from incompatibility between $P > 0$ and $\mathcal{H}$

$$P^2 + (-P)\, P = 0 \,(1)$$

and incompatibility between $P = 0$ and $\mathcal{H}$

$$P^2 + (-P)\, P = 0 \,(2)$$

using the inference $(\star)$ for $\mathrm{Proj}_{X_k}(\{P\})$, we get an incompatibility between $\mathcal{H}$ and every relizable sign condition on $\mathrm{Proj}_{X_k}(\{P\})$

using the inference $(\star)$ for $\mathrm{Proj}_{X_k}(\{P\})$, we get an incompatibility between $\mathcal{H}$ and every relizable sign condition on $\mathrm{Proj}_{X_{k-1}}(\mathrm{Proj}_{X_k}(\{P\}))$

....

using k times the inference $(\star)$ we get an incompability between $\mathcal{H}$ and ... nothing .. because all the variables have been eliminated

as seen before (talk of Daniel) an incompatibility of $\downarrow\mathcal{H}\downarrow$ where $\mathcal{H}_{\neq}=\{P\}$, $\mathcal{H}_{\geq}=\{-P\}, \mathcal{H}_{=}=\emptyset$ (expressing that $P<0$ is empty) is of the form

$$P^{2e}+\sum Q_i^2-\sum R_j^2\,P=0$$

$$P=\frac{\sum R_j^2\,P^2}{P^{2e}+\sum Q_i^2}=\frac{\sum R_j^2\,P^2\,(P^{2k}+\sum Q_i^2)}{(P^{2e}+\sum Q_i^2)^2},$$

degree of the last eliminating family doubly exponential d^{4^k}, to plug in a tower with already three level of exponents: we get five !

2 Discussion

Classical Nullstellensatz: single exponential bounds [Bro].

Existential theory of the reals: single exponential bounds (when based on critical point method, not on CAD, use infinitesimal deformation) [BPR].

Why not single exponential certificate for Hilbert 17th problem ?

Trade-off: "elementary proof' correspond to' "long certificate", "more sophisticated proof" correspond to "shorter certificate".

Projects for the near future: finalize the paper (75 pages), first talk announcing the result in NY in jan 1991 (23 years ago)

Projects for the future

- use another algebraic proof of the existence of complex roots (`two exponentials rather than three`) (recent work of M. Eisermann)

- use critical point method rather than projection variable after variable (`one exponential rather than two`)

Bibliography

[A] E. ARTIN, *Über die Zerlegung definiter Funktionen in Quadrate*, Hamb. Abh. **5**, 100-115 (1927). The collected papers of Emil Artin, 273-288. Reading: Addison-Wesley (1965).

[AS] E. ARTIN, O. SCHREIER, *Algebraische Konstruktion reeller Körper*, Hamb. Abh. 5 8(-99 (1925). The collected papers of Emil Artin, 258-271. Addison-Wesley (1965).

[BPR] S. BASU, R. POLLACK, M.-F. ROY, *Algorithms in real algebraic geometry*, Springer-Verlag, second edition (2006). Revised version of the first edition on line at http://perso.univ-rennes1.fr/marie-francoise.roy/

[BCR] J. BOCHNAK, M. COSTE, M.-F. ROY, *Real algebraic geometry*, Springer-Verlag, second edition in english (1998)

[Col] G. E. COLLINS,. *Quantifier elimination for real closed fields by cylindric algebraic decomposition*. In *Second GI Conference on Automata Theory and Formal Languages*, volume 33 of *Lecture Notes in Computer Science*, pages 134–183, Berlin, 1975. Springer-Verlag.

[E] M. EISERMANN, *The Fundamental Theorem of Algebra made effective: an elementary real-algebraic proof via Sturm chains*, The American Mathematical Monthly 119(9): 715-752 (2012) (arXiv:0808.0097v4 [math.AG]).

[Her] C. HERMITE, *Remarque sur le théorème de M. Sturm.*, Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences, 36, pp. 294-297 (1853)

[Hor] L. HÖRMANDER, *The analysis of linear partial differential operators*, vol. 2, Springer-Verlag, Berlin, Heidelberg, New York (1983)

[Kr] G. KREISEL, *Hilbert's 17-th problem.* in Summaries of talks presented at the Summer Inst. of Symbolic Logic at Cornell Univ (1957)

[Kri] J.-L. KRIVINE, *Anneaux préordonnés*, J. Analyse Math., 12, 307-326 (1964)

[Lom] H. LOMBARDI, *Une borne sur les degrés pour le Théorème des zéros réel effectif.* 323–345. In: Real Algebraic Geometry. Proccedings, Rennes 1991, Lecture Notes in Mathematics no 1524. Eds.: Coste, Mahe, Roy. (Springer-Verlag, 1992).

[LPR] H. LOMBARDI, D. PERRUCCI, M.-F. ROY, *Elementary recursive bounds for positivstellenzatz*, in preparation.

[Sch] J. SCHMID, *On the degree complexity of Hilbert's 17th problem and the Real Nullstellensatz*, Habilitation, University of Dortmund, n° 70, Seminar of logic, Paris 7, (2000).

[Ste] G. STENGLE, *A Nullstellensatz and a Positivstellensatz in semialgebraic geometry*, Mathematische Annalen, 207, 87-97 (1974)