Real algebraic geometry and computations, an intricated history

Marie-Françoise Roy
Université de Rennes 1

POEMA

November 26, 2020

Introduction

- POEMA
- polynomials
- moments
- sums of squares
- extremal points
- real reals

Topics

- real root counting and generalizations (moments)
- quantifier elimination
- positivity and sums of squares: non-constructive proof of Hilbert 17th problem (sums of squares)
- effectivity and complexity
- critical point method and applications (extremal points)
- elementary recursive solution to Hilbert 17th problem
- discussion : Coq, real reals

Topics

- **real root counting and generalizations**
- quantifier elimination
- positivity and sums of squares: non-constructive proof of Hilbert 17th problem
- effectivity and complexity
- critical point method and applications
- elementary recursive solution to Hilbert 17th problem
- discussion : Coq , real reals

Real root counting

- How many roots for a real polynomial ?
- A basic algorithmic problem
- real means with coefficients in a real closed field **R** with algebraic closure $\mathbf{R}[i] = \mathbf{C}$. Real closed = totally ordered with Intermediate Value Theorem (IVT) for polynomials.
- Descartes's law of sign, upper bound
- Sturm using euclidean division of P and P'
- Hermite using the signature of a quadratic form with entries the Newton sums (moments)

Hermite's quadratic form (moments)

P univariate monic polynomial,

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

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

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

Hermite's quadratic form

Proposition

$P = a_p X^p + a_{p-1} X^{p-1} + \cdots + a_1 X + a_0$, $a_p = 1$. Then for any i

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

with the convention $a_i = N_i = 0$ for $i < 0$.

Proposition

The signature of the Hermite quadratic defined by $\mathrm{Herm}(P)$ is the number of real roots of P.

Hint : complex conjugate roots contribute for a difference of two squares.
Note: the determinant of the Hermite matrix is the discriminant of P.

Tarsky query

- what is the Tarski query ?

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

- difference between the number of (real) roots where Q is positive and the number of (real) roots where Q is negative
- number of real roots is a special case (take $Q = 1$)
- signature of generalized Hermite using the signature of a quadratic form with entries linear combinations of the Newton sums

Generalized 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.
$\mathrm{Herm}(P,Q)_{i,j} = N_{i+j-2}(P,Q)$ and $\mathrm{Herm}(P,Q)$ the associated quadratic form. Entries are linear combinations of moments using the coefficients of Q.

Proposition

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

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

Hint : complex conjugate roots contribute for a difference of two squares.

Computation of Tarski query

- Determined by the signs of the principal minors of $\mathrm{Herm}(P, Q)$.
- In general, the signature is NOT determined by the signs of the principal minors but Hermite matrix is special
- can be computed in quasi linear time ($\tilde{O}(d)$ where d is a estimating the degree), with bit size well controlled, using subresultants and remainders rather than minors

Sign determination

- computing 3 Tarsk-queries

$$\mathrm{TaQu}(P, 1), \mathrm{TaQu}(P, Q), \mathrm{TaQu}(P, Q^2)$$

one can easily compute 3 quantities :

  - the number of roots of P where $Q > 0$,
  - the number of roots of P where $Q < 0$,
  - the number of roots of P where $Q = 0$.

Gives in particular the list of signs of Q realized at the roots of P

- base for naive sign determination: compute the list of realizable sign conditions of a family of polynomials $Q_1, \ldots, Q_s$ at the roots of P by an algorithm using Tarski queries of all products of the Q_i and Q_i^2
- sign determination can be improved, using Tarski queries of a few products of the Q_i and Q_i^2 (and not all of them)

Topics

- real root counting and generalizations
- **quantifier elimination**
- positivity and sums of squares: non-constructive proof of Hilbert 17th problem
- effectivity and complexity
- critical point method and applications
- elementary recursive solution to Hilbert 17th problem
- discussion : Coq , real reals

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 $\mathbb{R}$, is true in $\mathbb{R}$!
- Valid for any formula, due to Tarski
- eliminate one variable after the other
- "parametric sign determination" : compute the sign conditions on the parameters fixing the realizable sign conditions of a list of (parametric) polynomials $Q_1, \ldots, Q_s$ at the roots of (a parametric polynomial) P, using Tarski queries of all products of the Q_i and Q_i^2.

Topics

- real root counting and generalizations
- quantifier elimination
- **positivity and sums of squares: non-constructive proof of Hilbert 17th problem**
- effectivity and complexity
- critical point method and applications
- elementary recursive solution to Hilbert 17th problem
- discussion : Coq , real reals

Positivity and sums of squares

- Is a polynomial with real coefficients taking only non negative values a sum of squares of polynomials?
- Yes if the number of variables is 1.
- Hint : decompose the polynomial in powers of irreducible factors: degree two factors (corresponding to complex roots) are sums of squares, degree 1 factors (corresponding to real roots appear with even degree)
- Yes if the degree is 2.
- Hint: a quadratic form taking only non negative values is a sum of squares of linear polynomials

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.
- Also if the number of variables is 2 and the degree is 4
- No in general.
- First explicit counter-example Motzkin '69

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

takes only non negative values and is not a sum of square of polynomials.

Motzkin's counter-example (degree 6, 2 variables)

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

- M takes only non negative values. Hint: arithmetic mean is always at least geometric mean.
- M is not a sum of squares. Hint : try to write it as a sum of squares of polynomials of degree 3 and check that it is impossible.
- Example: no monomial X^3 can appear in the sum of squares. Etc ...

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 do not contain P (a cone contains squares and is closed under addition and multiplication, a proper cone does not contain -1).
- 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.
- A real closed field is a totally ordered field where IVT holds (Intermediate Value Theorem for polynomials)
- Every totally ordered field has a real closure.
- 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 "generic point" = the point $(X_1, \ldots, X_k)$).

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 real closed field in which P takes negative values (when evaluated at the "generic point" = the point $(X_1, \ldots, X_k)$).
- 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.

Transfer principe

- A statement involving elements of **R** which is true in a real closed field containing **R** (such as the real closure of the field of rational functions for a chosen total order) is true in **R**.
- Not any statement, only ”first order logic statement”.
- Example of such statement

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

  is true in a real closed field containing **R** if and only if it is true in **R**
- Special case of quantifier elimination.

Topics

- real root counting and generalizations
- quantifier elimination
- positivity and sums of squares: non-constructive proof of Hilbert 17th problem
- **effectivity and complexity**
- critical point method and applications
- elementary recursive solution to Hilbert 17th problem
- discussion : Coq , real reals

What about computations ?

Existence of effective procedures ?

- real root counting and Tarski queries (by Hermite): YES

  sign determination by Tarski queries : YES

- quantifier elimination : YES, parametric sign determination (Tarski's paper was supported by the Rand corporation)
- Hilbert 17 th problem : NO
  - checking whether a given polynomial is everywhere nonnegative : YES (by quantifier elimination)
  - providing a representation as a sum of squares: NO (Artin notes that his proof is very indirect, that effectivity is desirable but difficult).

Note the ordered base field must be "discrete": it is possible to decide the sign of an element, i.e. not over the "real" reals !

What about computations ?

Complexity bounds ?

- real root counting and Tarski queries quasi linear in the degree
- sign determination is polynomial in d and s
- Tarski's quantifier elimination : primitive recursive.

Real algebraic numbers: Thom's encodings

- a real root of a polynomaial is characterized by the signs taken by the derivatives at the root
- signed determination can be used to compute the Thom encodings taking for $Q_1, \ldots, Q_s$ the derivatives

Cylindrical decomposition

- Collins Cylindrical Algebraic Decomposition : doubly exponential in number of variables, polynomial in degre and number of polyomials. Use of subresultants controls degree growth and combinatorial explosion.
- doubly exponential is big! Computations are impractical for significant examples in more than two variables
- The proof uses the continuity of the roots and the notion of connected component
- recent variant of CAD [PR] using Thom encoding and sign determination. The proof is purely algebraic.

Topics

- real root counting and generalizations
- quantifier elimination
- positivity and sums of squares: non-constructive proof of Hilbert 17th problem
- effectivity and complexity
- critical point method and applications
- **critical point method and applications**
- elementary recursive solution to Hilbert 17th problem
- discussion : Coq , real reals

Better complexity bounds ?

quantifier elimiation: project blocks of variables in one step using the critical point method initiated by [GV]

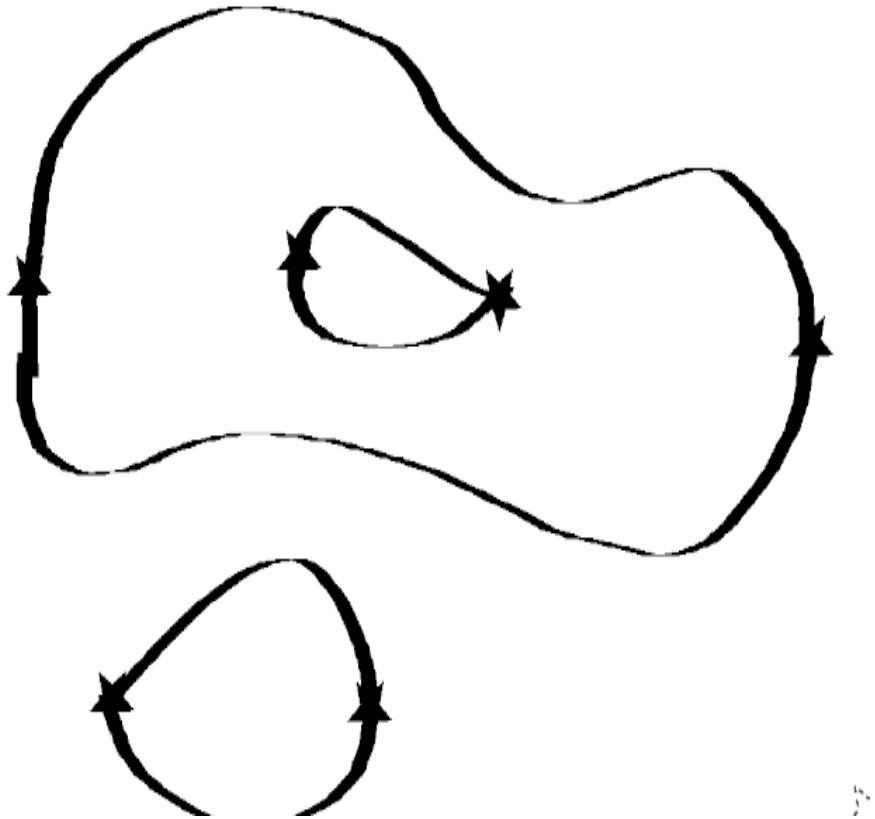

Figure: Critical points in the X-direction

The critical point method

- RUR given a finite number of points in $\mathbf{R}^k$ is is possible to express them as the values of a rational function at the roots of a univariate polynomial (for which we can use Thom encodings)
- given a smooth and bounded hypersurface, a sweeping family of parallel hyperplanes touches the hyoersurface in a finite single exponential number of points
- need to introduce (a fixed number of) infinitesimals to treat singular cases ! Computations are impractical except in "generic situations".
- An infinitesimal should not be consider as an extra variable in the computations..

Applications of the critical point method

- quantifier elimination method follows: parametric block elimination, doubly exponential in the number of blocks
- existential theory of the reals, single exponential (only one block of existential quantifiers)
- sampling: find a point (at least) in every semi-algebraically connected component
- road map algorithm (including ”baby step giant step” see [BRSS], ”divide and conquer” roadmap [SS],[BR])
- covering by contractible sets: parametrized road map
- description of connected components
- quantitative curve selection lemma

Curve selection lemma

- find a curve entering from a point of the closure of $\bar{S}$ inside S
- quantitative version s, d, k a bound on the number, the degree and the number of variables of the polynomials describing a semi-algebraic set S and a point x in $\bar{S}$, construct a semi-algebraic path starting at x and entering in S with a description of degree $(O(d)^{3k+3}, O(d)^k)$, improvement on previous results by [JK]
- strategy: "same thing" as finding a point in a semi-algebraic set !

Curve selection lemma

- classical proof: take a sphere of infinitesimal radius ε around x, intersect it with S,pick up a point $x(\varepsilon)$, replace ε by a small enough t_0 and get a little path $x(t)$ defined on $(0, t_0]$ starting from x and entering S
- quantitative version: do the same, finding the point by the (critical point) sampling algorithm, estimating the degree of the point $x(\varepsilon)$ also with respect to the variable ε see [BR1]

Topics

- real root counting and generalizations
- quantifier elimination
- positivity and sums of squares: non-constructive proof of Hilbert 17th problem
- effectivity and complexity
- critical point method and applications
- **elementary recursive solution to Hilbert 17th problem**
- discussion : Coq , real reals

Hilbert's 17th problem made effective

Two kinds of degree bounds

- primitive recursive degree bounds. Starting from 0 and successor, the recursion scheme makes it possible to build successively $+$, $\times$, $f_1(n) = 2^n$,then $f_2(n) = 2^{2^n}$...
  $g(n) = f_n(2)$ (no fixed level of exponentiations).
- elementary recursive degree bounds: only functions with a fixed level of exponentiations. Single exponential (one level), doubly exponential (two levels)... five levels of exponentials ...

Two kinds of degree bounds

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

- Our work Lombardi, Perrucci, R. '14: another constructive proof $\rightsquigarrow$ elementary recursive degree bound:

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

Construct specific algebraic identities expressing that

- a real polynomial of odd degree has a real root
- a real polynomial has a complex root (by Laplace's proof)
- Tarski queries computed by Hermite quadratic forms
- the Sylvester's inertia law for quadratic forms is valid
- realizable sign conditions for a family of univariate polynomials at the roots of a polynomial, fixed by sign of minors of Hermite quadratic forms (uses subresultants Thom's encoding, and sign determination),
- realizable sign conditions for $\mathcal{P} \subset \mathbf{K}[X_1, \ldots, X_k]$ are fixed by list of non empty sign conditions for $\mathrm{Proj}(\mathcal{P}) \subset \mathbf{K}[X_1, \ldots, X_{k-1}]$: efficient projection method using only algebra

and at the end produce a sum of squares, with elementary recursive complexity (tower of five exponentials) !

Topics

- real root counting and generalizations
- quantifier elimination
- positivity and sums of squares: non-constructive proof of Hilbert 17th problem
- effectivity and complexity
- critical point method and applications
- elementary recursive solution to Hilbert 17th problem
- **discussion: Coq, real reals**

Discussion: Coq

- Proving in Coq that the theorems in [BPR] Chapter 2 are correct, Cyril Cohen found little mistakes in proofs, and even a non-constructive proof. More interestingly, his work led us to simplify several proofs (simpler base case for induction on remainder sequence), and make (improved) sign determination much more explicit.
- Working group on constructive real algebraic geometry with Assia Mahboubi, Henri Lombardi, Cyril Cohen, Michel Coste, and (most often not attending) Thierry Coquand, Daniel Perrucci and Saugata Basu. No paper in common at that point but papers by subgroups.

Discussion: real reals

- Main open problem (Henri Lombardi is insisting): how to do real real algebraic geometry (over the real numbers)
- in particular trichotomy is not valid
- impossible to find the number of real roots of $X^2 + \varepsilon$ if the sign of ε is not known

References

[BPR] S. Basu, R. Pollack, M.-F. Roy, Algorithms in real algebraic geometry, Algorithms and Computation in Mathematics, 10, Second edition. *Springer-Verlag, Berlin*, 2006. Updated version (2016) https://perso.univ-rennes1.fr/marie-francoise.roy/bpr-ed2-posted3.html

[BR] S. Basu, M.-F. Roy, Divide and Conquer Roadmaps for Algebraic sets, Discrete and Computational Geometry Volume 52 Issue 2 (September 2014) Pages 278-343 (preliminary version, arXiv:1305.3211)

[BR1] S. Basu, M.-F. Roy, Quantitative Curve Selection Lemma (preliminary version, arXiv:1803.00505)

[BRSS] S. Basu, M.-F. Roy, M. Safey El Din, E. Schost. A baby step-giant step roadmap algorithm for general algebraic sets, Foundation of Computational Mathematics : Volume 14, Issue 6 (2014), Page 1117-1172 (preliminary version, arXiv:1201.6439).

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

[GV1] Z. Jelonek, K. Kurdyka,Reaching generalized critical values of a polynomial,Math. Z.276(2014), no. 1-2, 557–570

[LPR] H. Lombardi, D. Perrucci, M.-F. Roy, *An elementary recursive bound for effective Positivstellensatz and Hilbert 17-th problem* Memoirs of the AMS, Vol 263, Number 1277, January 2020. (arXiv:1404.2338)

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

[SS] M. Safey El Din, E. Schost, A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets, Journal of the ACM, Vol. 63(6), 2017.

(and many other references not listed and available in this book and papers)