Elementary recursive complexity results in real algebraic geometry

Marie-Françoise Roy
Université de Rennes 1

Women in Mathematics (Japan), 7 september 2022

June 21, 2022

Real algebraic geometry

- solution of polynomial equalities and inequalities in R^k
- R: real closed field, totally ordered field, positive elements are square, IVT: Intermediate Value Theorem. If $P \in \mathrm{R}[X]$ $P(a)P(b) < 0, a < b$ then $\exists c \quad P(c) = 0$
- examples of real closed field : (such as $\mathbb{R}$ field of real numbers, $\mathbb{R}_{\mathrm{alg}}$ field of real algebraic numbers , and also and also non archimedean models such as $\mathbb{R}\langle\epsilon\rangle$ the field of Puiseux series
- $\mathrm{R}[i]$ is algebraically closed, using an algebraic proof due to Laplace of the Fundamental Theorem of Algebra.

Definitions
Modern algebra: non constructive proofs
Proof theory: primitive recursive degree bounds
Computer algebra: elementary recursive degree bounds
Discussion

Primitive recursive/elementary recursive

- primitive recursive functions obtained from 0, successor, chosing one coordinate, composition and recursion
- example: addition from successor, multiplication from addition, exponentiation from multiplication using recursion
- example: associate to n a tower of exponential whose height is n. $f(0) = 2$, $f(1) = 2^2$, $f(2) = 2^{2^2}$ ... easy to construct using recursion
- elementary recursive functions are functions obtained from addition, multiplication, substraction and division using chosing one coordinate, composition, finite summation and product. Typically: exponential function 2^n, doubly exponential function 2^{2^n}, a tower of exponentials of fixed height (example: 5 or 4).

Marie-Françoise Roy Université de Rennes 1 Elementary recursive complexity results in real algebraic geometry

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 all other cases.
- First explicit counter-example Motzkin '69

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

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

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

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

- 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 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 the field rational functions.
- Sums of squares: proper cone of rational functions, and do not contain P (a cone contains squares, 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.
- 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 $(X_1, \ldots, X_k)$).
- 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.

Definitions
Modern algebra: non constructive proofs
Proof theory: primitive recursive degree bounds
Computer algebra: elementary recursive degree bounds
Discussion

Definition (Hermite's Matrix)

Let $P, Q \in \mathrm{R}[X]$ with $\deg P = p \geq 1$. The Hermite's matrix $\mathrm{Her}(P;Q) \in \mathrm{R}^{p\times p}$ is the matrix defined for $1 \leq j_1, j_2 \leq p$ by

$$\mathrm{Her}(P;Q)_{j_1,j_2} = \mathrm{Tra}(Q(X)\cdot X^{j_1+j_2-2})$$

where $\mathrm{Tra}(A(X))$ is the trace of the linear mapping of multiplication by $A(X) \in \mathrm{R}[X]$ in the R-vector space $\mathrm{R}[X]/P(X)$.

Hermite matrix easy to compute, its entries correspond to linear combination of the Newton sums (moments) of P.

Hermite method

Theorem (Hermite's Theory)

Let $P, Q \in \mathrm{R}[X]$ *with* $\deg P = p \geq 1$. *Then*

$$\mathrm{TaQu}(P, Q) = \mathrm{Si}(\mathrm{Her}(P; Q))$$

where

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

$\mathrm{Si}(\mathrm{Her}(P; Q))$ *is the signature of the symmetric matrix* $\mathrm{Her}(P; Q)$. *Moreover* $\mathrm{Si}(\mathrm{Her}(P; Q))$ *is determined by the signs of the principal minors of* $\mathrm{Her}(P; Q)$.

Proof: uses complex conjugate roots.

Definitions
Modern algebra: non constructive proofs
Proof theory: primitive recursive degree bounds
Computer algebra: elementary recursive degree bounds
Discussion

Transfer principle

- 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.

Marie-Françoise Roy Université de Rennes 1 Elementary recursive complexity results in real algebraic geometry

Remaining problems

- Very indirect proof (by contraposition, uses Zorn).
- No hint on denominators: what are the degree bounds ?
- Artin notes effectivity is desirable but difficult.
- Effectivity problems : is there an algorithm checking whether a given polynomial is everywhere nonnegative?
- Can we use this algorithm to provide a representation as a sum of squares?

Positivstellensatz (Krivine '64, Stengle '74)

- 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 C^k
  $\Longleftrightarrow$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- Grete Hermann, a female student from Hilbert has given in her Ph D dissertation an algorithmic proof of the classical Nullstellensatz, with elementary recursive complexity (doubly exponential in the number of variables).
- For real numbers, statement more complicated.

Positivstellensatz

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

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

$$\exists \quad S = \prod_{i \in I_{\neq}} P_i^{2e_i}, \qquad N = \sum_{I \subset I_{\geq}} \Big(\sum_j k_{I,j} Q_{I,j}^2\Big) \prod_{i \in I} P_i \quad (k_{I,j} > 0),$$

$$Z \in \langle P_i \mid i \in I_{=} \rangle \subset \mathbf{K}[x$$

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

Definitions
Modern algebra: non constructive proofs
Proof theory: primitive recursive degree bounds
Computer algebra: elementary recursive degree bounds
Discussion

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 $\mathcal{H}$

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

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

Positivstellensatz implies Hilbert 17th problem

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

$$\iff \left\{ \begin{array}{rcl} P(x) & \neq & 0 \\ -P(x) & \geq & 0 \end{array} \right. \quad \text{no solution}$$

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

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

Definitions
Modern algebra: non constructive proofs
Proof theory: primitive recursive degree bounds
Computer algebra: elementary recursive degree bounds
Discussion

Positivstellensatz: proofs

- Classical proofs of Positivstellensatz based on Modern Algebra.
- Zorn's lemma and Tranfer principle, very similar to Artin's proof for Hilbert 17th problem.
- non-constructive
- no degree bounds

Remaining problems

- Very indirect proof (by contraposition, uses Zorn).
- Effectivity is desirable but difficult.
- What are the degree bounds in the Positivstellensatz Identity ?
- Effectivity problems : is there an algorithm checking whether a given system of polynomial inequalities is empty?
- If the answer is yes, can we use this algorithm to construct a Positivstellensatz equality ?

Definitions
Modern algebra: non constructive proofs
Proof theory: primitive recursive degree bounds
Computer algebra: elementary recursive degree bounds
Discussion

Quantifier elimination

- Classical proofs of Positivstellensatz based on Modern Algebra.
- Constructive proofs use a quantifier elimination algorithm over the reals.
- What is quantifier elimination ?
- High school mathematics

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

$$\Longleftrightarrow$$

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

- Valid for any formula, due to Tarski, using Tarski-queries and induction on the number of variables, algorithm !
- Deciding emptyness of a system of inequalities is algorithmic.

Marie-Françoise Roy Université de Rennes 1 Elementary recursive complexity results in real algebraic geometry

Strategy of Lombardi

- For every system of sign conditions with no solution, find a simple algorithmic proof of the fact there is no solution, based on quantifier elimination
- Use this proof to construct an algebraic incompatibility and control the degrees for the Positivstellensatz.
- Uses notions introduced by Henri Lombardi.
- Key concept : weak inference.

Quantifier elimination methods

- Many existing methods
- The older ones have a primitive recursive complexity : Tarski, Seidenberg, Cohen-Hormander.
- The one chosen by Henri Lombardi for a constructive proof of Positivstellensatz is Cohen-Hormander algorithm as explained in [BCR].

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

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

Definitions
Modern algebra: non constructive proofs
Proof theory: primitive recursive degree bounds
Computer algebra: elementary recursive degree bounds
Discussion

Example:

$$\begin{cases} x & \neq & 0 \\ y - x^2 - 1 & \geq & 0 \\ xy & = & 0 \end{cases} \qquad \text{no solution in } \mathbb{R}^2$$

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

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

The degree of this is incompatibility is 4.

Marie-Françoise Roy Université de Rennes 1 Elementary recursive complexity results in real algebraic geometry

Weak Inference

(in the particular case we need) $\mathcal{F}, \mathcal{G}$ 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.

Weak inferences: case by case reasoning

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

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

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

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

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

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

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

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

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

Weak inferences: case by case reasoning

Starting from two incompatibilities

$\downarrow \mathcal{H},\ \ A < 0 \downarrow \leftarrow$ degree δ_1 $\qquad$ $\downarrow \mathcal{H},\ \ A > 0 \downarrow \leftarrow$ degree δ_2

$$\underbrace{A^{2e_1}S_1}_{>0} + \underbrace{N_1 - N_1'A}_{\geq 0} + \underbrace{Z_1}_{=0} = 0 \qquad \underbrace{A^{2e_2}S_2}_{>0} + \underbrace{N_2 + N_2'A}_{\geq 0} + \underbrace{Z_2}_{=0} = 0$$

we constructed (by making a product) a new incompatibility

$$\underbrace{A^{2e_1+2e_2}S_1S_2}_{>0} + \underbrace{N_1'N_2'A^2 + N_3}_{\geq 0} + \underbrace{Z_3}_{=0} = 0$$

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

Definitions
Modern algebra: non constructive proofs
Proof theory: primitive recursive degree bounds
Computer algebra: elementary recursive degree bounds
Discussion

List of statements needed into weak inferences form

- Many simple weak inferences of that kind are combined to obtain more interesting weak inferences.
- In particular: IVT, the Intermediate Value Theorem, has to be transformed into a weak inference
- Finally Henri Lombardi proved primitive recursive degree bounds for Positivstellensatz, hence of the Hilbert 17 th problem Lombardi '90.
- There are prior or other contributions for the 17 th problem only. • Kreisel '57 - Daykin '61 - - Schmid '00
- All these constructive proofs $\rightsquigarrow$ primitive recursive degree bounds k and $d = \deg P$.

Marie-Françoise Roy Université de Rennes 1 Elementary recursive complexity results in real algebraic geometry

Sign determination

- R a real closed field (such as $\mathbb{R}$, $\mathbb{R}_{\mathrm{alg}}$, $\mathbb{R}\langle\epsilon\rangle$)
- a univariate non zero polynomial P and a list of other univariate polynomials $Q_1, \ldots, Q_s$ all in $\mathrm{R}[X]$
- find the list of non-empty sign conditions (i.e. elements of $\{0, 1, -1\}^s$) realized by $Q_1, \ldots, Q_s$ at the real roots of P (i.e. roots in R)
- variant: compute also the corresponding cardinalities

Special case 1: real root counting

- a univariate non zero polynomial $P \in \mathrm{R}[X]$
- decide whether P has a real root (i.e. a root in R) or not
- variant: compute also the number of roots of P in R
- using Hermite's method

Special case 2: Tarski query

- a univariate non zero polynomial $P \in \mathrm{R}[X]$ and another polynomial $Q \in \mathrm{R}[X]$
- decide the signs of Q at the roots of P in R (variant: count the cardinalities)
- tool : Tarski-query

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

- using Hermite's method

Definitions
Modern algebra: non constructive proofs
Proof theory: primitive recursive degree bounds
Computer algebra: elementary recursive degree bounds
Discussion

Special case 2: Tarski query

$c(P = 0, Q = 0)$ is the number of roots of P in R where $Q = 0$ etc

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} c(P=0, Q=0) \\ c(P=0, Q>0) \\ c(P=0, Q<0) \end{bmatrix} = \begin{bmatrix} \mathrm{TaQu}(P, 1) \\ \mathrm{TaQu}(P, Q) \\ \mathrm{TaQu}(P, Q^2) \end{bmatrix}$$

Compute three Tarski-queries, then compute three cardinals and decide which are the non-empty sign conditions.
Using Hermite's method.

General case

- Tarski-queries are considered as black-boxes
- compute Tarski-queries of P and products of the Q_i or their squares (using Hermite's method for example)
- solve a linear system,
- compute the cardinals of sign conditions at the roots of P,
- gives sign determination

Naive algorithm

Order the elements of $\{0, 1, -1\}^s$ lexicographically and consider the elements of $\{0, 1, 2\}^s$ as coding all natural numbers smaller than $3^s - 1$.

- Perform the 3^s products of the Q_i and Q_i^2
- Compute the 3^s corresponding Tarski-queries, which defined a vector t
- Define the $3^s \times 3^s$ matrix of signs M whose columns are indexed by $\{0, 1, -1\}^s$ and rows are indexed by $\{0, 1, 2\}^s$, the σ, α entry being the sign taken by $Q_1^{\alpha_1} \ldots, Q_s^{\alpha_s}$ at σ.
- solve the linear system $M \cdot c = t$ where c is the unknown
- keep the non-zero elements of c which are the cardinals of the non-empty sign conditions

Naive algorithm

Example for $s = 2$, the matrix of signs is

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & -1 & -1 & -1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 1 & -1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

and is invertible.

Definitions
Modern algebra: non constructive proofs
Proof theory: primitive recursive degree bounds
Computer algebra: elementary recursive degree bounds
Discussion

Naive algorithm

Rows are numbered from 0 to 8. The row of number 4 (fifth row) is the sign of the polynomial $Q_1 Q_2$ on the list of signs (since 4 is written 1+3 in basis 3)

$$\begin{array}{rccccccccc} \mathrm{sign}(Q_1) & 0 & 0 & 0 & 1 & 1 & 1 & -1 & -1 & -1 \\ \mathrm{sign}(Q_2) & 0 & 1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 \\ \mathrm{sign}(Q_1 Q_2) & 0 & 0 & 0 & 0 & 1 & -1 & 0 & -1 & 1 \end{array}$$

The correctness is proved by induction on s.
The number of calls to the Tarski-query black box is exponential in s.

Improved algorithm

- Notice that the number of non-empty sign conditions is at most the number $r \leq d$ of real roots
- Remove non-empty sign conditions at each induction step
- Use the special structure of the matrix to solve the linear system in quadratic time
- **Prove that the $Q_1^{\alpha_1}\ldots,Q_s^{\alpha_s}$ whose Tarski-query is computed in the algorithm have at most $\log_2 d$ non zero entries**.

Definitions
Modern algebra: non constructive proofs
Proof theory: primitive recursive degree bounds
Computer algebra: elementary recursive degree bounds
Discussion

Complexity

- The total number of calls to the Tarski-query blackbox is $3sd$
- The Tarski-query blackbox is called for P and polynomials of degree at most $2d\log_2 d$

Marie-Françoise Roy Université de Rennes 1 Elementary recursive complexity results in real algebraic geometry

Real algebraic numbers

- Real algebraic numbers can be characterized by the signs they give to their derivatives (Thom encodings) : easy by induction on the degree
- Thom encodings can be computed by sign determination
- No numerical approach needed, valid on any real closed field
- Once we know the Thom encodings, sign determination gets simplified, only products of (a few) derivatives and one of the other polynomial (or its square) are used.

Definitions
Modern algebra: non constructive proofs
Proof theory: primitive recursive degree bounds
Computer algebra: elementary recursive degree bounds
Discussion

Sign determination and quantifier elimination

- Eliminating one variable corresponds (basically) to parametric sign determination
- $P, Q_1, \ldots, Q_s$ are polynomials in parameters u and main variable X
- compute polynomials in the parameters u whose signs fix the list of non-empty sign conditions realized by $Q_1[u][X], \ldots, Q_s[u][X]$, at the real roots of $P[u][X]$

Marie-Françoise Roy Université de Rennes 1 Elementary recursive complexity results in real algebraic geometry

Sign determination and quantifier elimination

- Tarski's proof of quantifier elimination is basically naive sign determination
- Complexity primitive recursive

There are much better quantifier elimination methods

- Cynlindrical algebraic decomposition is doubly exponential
- Polynomial when the number of variables is fixed
- Uses the notion of connected component of a sign condition

More recent methods doubly exponential in the number of blocks of quantifiers and polynomial when this number if fixed. Use even more geometry (critical points ...).

Sign determination and quantifier elimination

- New purely algebraic quantifier elimination method using sign determination and Thom encodings
- Complexity elementary recursive
- Polynomial in the number of polynomials when the number of variables is fixed but **NOT** in the degree of the polynomials
- Does not need the notion of a connected component of a sign condition

Elementary recursive degree bounds for Positivstellensatz

- strategy: transform a simple proof that a system of inequalities has no solution into the construction of an algebraic identity
- turn the preceding ingredients : computation of signature of Hermite quadratic form, Thom encodings, sign determination into construction of algebraic identities
- control the degree of these identities
- not having to deal sign connected components of sign conditions is crucial

(Joint work with Daniel Perrucci and Henri Lombardi)

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 algebraic proofof the Fudamental Theorem of Algebra)
- 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 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) !

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 $\mathcal{H}$ itself

Going right to left.

Definitions
Modern algebra: non constructive proofs
Proof theory: primitive recursive degree bounds
Computer algebra: elementary recursive degree bounds
Discussion

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

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

is an initial incompatibility of $P \geq 0, P \neq 0, -P \geq 0$!
Hence, taking $\mathcal{H} = [P \neq 0, -P \geq 0]$ we know how to construct an incompatibility of $\mathcal{H}$ itself !

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

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

Elementary recursive Hilbert 17 th problem

A non negative polynomials of degree d in k variables can be represented as a sum of squares of rational functions with elementary recursive degree bound:

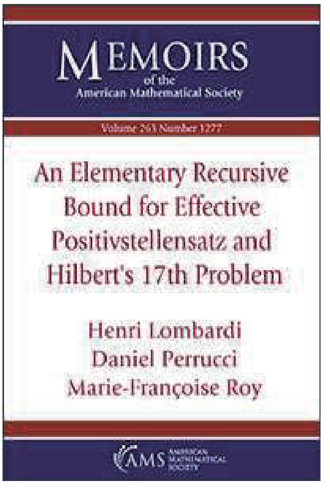
$$2^{2^{2^{d^{4^k}}}}.$$

[LPR]
and similar results for Positivstellensatz and Real Nullestellensatz

Discussion

- Why a tower of five exponentials ?
- outcome of our method ... no other reason ...
- the existence of a real root for an univariate polynomials of degree d already gives a construction of algebraic identities with two level of exponentials
- the proof of Laplace starts from a polynomial of degree d and produces a polynomial of degree d^d : triple exponential for the construction of algebraic identities corresponding to the fundamental theorem of algebra
- our projection method based only on algebra then gives univariate polynomials of doubly exponential degrees (eliminating variables one after the other using Hermite's method)
- finally : a tower of 5 exponentials
- long paper, appeared in Memoirs of the AMS ...

If you want to read more



Definitions
Modern algebra: non constructive proofs
Proof theory: primitive recursive degree bounds
Computer algebra: elementary recursive degree bounds
Discussion

References

[BGP] Blekherman G., Gouveia J. and Pfeiffer J. Sums of Squares on the Hypercube Manuscript. arXiv:1402.4199. [BCR] J. Bochnak , M. Coste , M.-F. Roy. Real algebraic geometry. Second edition in english.Ergebnisse der Mat., vol. 36. Berlin Heidelberg New York: Springer (1998)

[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.

[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) .

[LPR] 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 many other references there)