Elementary recursive degree bounds for Hilbert's 17th problem and Positivstellensatz.

Marie-Françoise Roy
Université de Rennes

Dortmund, October 27, 2023
Quadratic Forms and Real Algebra,
Conference on the occasion of Eberhard Becker's 80th birthday

Before starting

Positive polynomials, Oberwolfach, 2002

Before starting

Small meeting, organized by Eberhard Becker (Dortmund), Christian Berg (Kobenhavn) and Alexander Prestel (Konstanz).
First talk by Eberhard Becker "The concept of the meeting".
The summary of his talk starts with: "The meeting brings together researchers from various areas ...."

Before starting

Small meeting, organized by Eberhard Becker (Dortmund), Christian Berg (Kobenhavn) and Alexander Prestel (Konstanz).
First talk by Eberhard Becker "The concept of the meeting".
The summary of his talk starts with: "The meeting brings together researchers from various areas ...."
Meeting for the first time people outside our group of real algebraic geometers, such as Jean-Bernard Lasserre, Yuri Nesterov, Mihai Putinar, Konrad Schmudgen ...

More embarrassing

The topic of my talk was "Degree bounds for Positivstellensatz" and I was describing a sketch of a proof with degree bounds given by a tower of 3 exponents.

More embarrassing

The topic of my talk was "Degree bounds for Positivstellensatz" and I was describing a sketch of a proof with degree bounds given by a tower of 3 exponents.
Twenty years later I am able to present a full proof with a tower of 5 exponents ...
Joint work with Henri Lombardi and Daniel Perrucci.

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 choice of 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: 3 or 5).

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.

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 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.

Definition (Hermite's Matrix)

Let $P, Q \in \mathbf{K}[X]$ with $\deg P = p \geq 1$, $\mathbf{K}$ a field. The Hermite's matrix $\mathrm{Her}(P; Q) \in \mathbf{K}^{p \times p}$ 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 $A(X) \in \mathbf{K}[X]$ in the $\mathbf{R}$-vector space $\mathbf{K}[X]/P(X)$.

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

Hermite method

K an ordered field, **R** a real closed extension of **K**

Theorem (Hermite's Theory)

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

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

where

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

$\mathrm{Si}(\mathrm{Her}(P; Q))$ *is the signature of the symmetric matrix* $\mathrm{Her}(P; Q)$.

Proof: uses complex conjugate roots.
Moreover $\mathrm{Si}(\mathrm{Her}(P; Q))$ is determined by the signs of the principal minors of $\mathrm{Her}(P; Q)$, which belong to **K**.

Transfer principe

K an ordered field, **R** a real closed extension of **K**

- A statement involving elements of **K** 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

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

with $P \in \mathbf{K}[x_1, \ldots, x_k]$ is true in a real closed field containing **R** if and only if it is true in **R**

- Special case of quantifier elimination. Algorithmic from start (Tarski), complexity issues.

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.
- There are algorithms checking whether a given polynomial is everywhere nonnegative.
- Can we use these algorithms to provides a representation as a sum of squares?
- What are the bounds we get ?

Positivstellensatz (Krivine '64, Stengle '74)

More generally

- Find algebraic identities certifying that a system of sign condition is empty.
- In the spirit of Nullstellensatz.
  $\mathbf{K}$ a field, $\mathbf{C}$ an algebraically closed extension of $\mathbf{K}$,
  $P_1, \ldots, P_s \in \mathbf{K}[X_1, \ldots, X_k]$
  $P_1 = \ldots = P_s = 0$ no solution in $\mathbf{C}^k$

  $\Longleftrightarrow$

  $$\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[X_1, \ldots, X_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$$
- For real numbers, statement more complicated.

Positivstellensatz

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

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

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

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

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

Incompatibilities

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

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

with

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

$N \in \left\{ \sum_{I \subset I_{\geq}} \left(\sum_j k_{I,j} Q_{I,j}^2 \right) \prod_{i \in I} P_i \right\} (k_{I,j} > 0)$ cone of $\mathcal{H}$

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

Positivstellensatz implies Hilbert 17th problem

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

$$\iff \begin{cases} P(x) \neq 0 \\ -P(x) \geq 0 \end{cases} \text{ no solution in } \mathbf{R}^k$$

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

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

Positivstellensatz: 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

- Want to prove Hilbert 17 th problem using Positivstellensatz.
- But again very indirect proof (by contraposition, uses Zorn).
- Effectivity result difficult.
- What are the degree bounds in the Positivstellensatz Identity ?
- There are algorithms checking whether a given system of polynomial inequalities is empty.
- Can we use thes algorithms to construct a Positivstellensatz equality ? With which degree bounds ?

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.

Degree of an incompatibility

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

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

$$S = \prod_{i \in I_{\neq}} P_i^{2e_i}, N = \sum_{I \subset I_{\geq}} \left(\sum_j k_{I,j}, Q_{I,j}^2\right) \prod_{i \in I} P_i, k_{I,j} > 0, Z = \sum_{i \in I_{=}} Q_i P_i$$

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

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

Example:

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

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

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

The degree of this incompatibility is 4.

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

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

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

List of statements needed into weak inferences form

- Many simple weak inferences of that kind are combined to obtain more interesting weak inferences.
- In particular: IVT : Intermediate Value Theorem.
- Finally Henri Lombardi proved primitive recursive degree bounds for Positivstellensatz, hence of the Hilbert 17 th problem and Real Nullstellensatz Lombardi '90. Based in Cohen-Hörmander algorithm for quantifier elimination.
- There are prior or other contributions for the 17 th problem only. Kreisel '57 - Daykin '61 - - Schmid '00. Constructive proofs giving primitive recursive degree bounds k and $d = \deg P$.

Sign determination

- $\mathbf{K}$ an ordered field, $\mathbf{R}$ a real closed extension of $\mathbf{K}$
- a univariate non zero polynomial P and a list of other univariate polynomials $Q_1, \ldots, Q_s$ all in $\mathbf{K}[X]$
- 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 $\mathbf{R}$)
- variant: compute also the corresponding cardinalities

Special case : Tarski query

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

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

Special case : Tarski query

$c(P = 0, Q = 0)$ is the number of roots of P in $\mathbf{R}$ 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. Computations taking place n $\mathbf{K}$, real roots in $\mathbf{R}$.

Hermite method

Notation

Let $P, Q \in \mathbf{K}[X]$ *with* $\deg P = p \geq 1$. *For* $0 \leq j \leq p-1$, *we denote by* $\mathrm{HMi}_j(P;Q)$ *the* $(p-j)$*-th principal minor of* $\mathrm{Her}(P;Q)$, *with* $\mathrm{HMi}_p(P;Q) = 1$. *We denote by* $\mathrm{HMi}(P;Q)$ *the list*

$$[\mathrm{HMi}_0(P;Q), \ldots, \mathrm{HMi}_p(P;Q)] \subset \mathbf{K}.$$

The signs of the elements of $\mathrm{HMi}(P;Q)$ determines the Tarski Query.

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

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**.
  John Canny ... joint work with Aviva Szpirglas

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.

Fourier ... Thom ... joint work with Michel Coste

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 with connected components of sign conditions is crucial

Joint work with Daniel Perrucci and Henri Lombardi

Construct specific algebraic identities

- a real polynomial of odd degree has a real root
- a real polynomial has a complex root (by Laplace's algebraic proof of FTA)
- Tarski queries are computed by Hermite quadratic forms
- Sylvester's inertia law for quadratic forms holds
- realizable sign conditions for a family of univariate polynomials at the roots of a polynomial, are 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.

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:

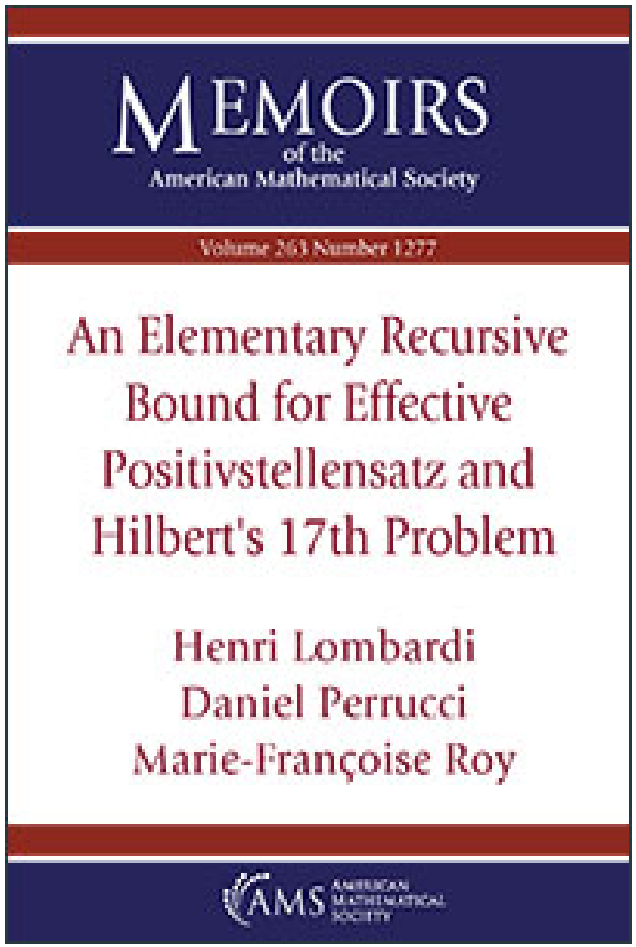
$$2^{2^{2^{d^{4^k}}}}.$$

and similar results for Positivstellensatz.
Joint work with Henri Lombardi and Daniel Perrucci.

Discussion

- Why a tower of 5 exponentials rather than ... 3 ...?
- 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 starting from a polynomial of degree d produces a polynomial of odd degree d^d : three levels of exponentials 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 determinants of Hermite matrices)
- finally : a tower of 5 exponentials
- long paper, appeared in Memoirs of the AMS ...

Finally !



Memoirs of the AMS, Vol 263, Number 1277, January 2020.
Complete version already on arxiv 2014 ...