An elementary recursive bound for Positivstellensatz and 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

Association for Turkish Women in Mathematics

27 may, 2016

Positivity and sums of squares

- Is a non-negative polynomial 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)

Positivity and sums of squares

- Is a non-negative polynomial 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)

Positivity and sums of squares

- Is a non-negative polynomial 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)

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.
- A non negative quadratic form 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.
- A non negative quadratic form 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.
- 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.

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.

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

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

is non negative and is not a sum of square of 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.
- No in general.
- First explicit counter-example Motzkin '69

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

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

Motzkin's counter-example

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

- M is non negative. 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 ...

Motzkin's counter-example

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

- M is non negative. 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 ...

Motzkin's counter-example

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

- M is non negative. 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.

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 do 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 do not contain P (a cone contains squares and is closed under addition and multiplication, a proper cone do 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 do 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.
- A real closed field is a totally ordered field where positive elements are squares and a polynomial of odd degree has a root.
- 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.
- A real closed field is a totally ordered field where positive elements are squares and a polynomial of odd degree has a root.
- 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.
- A real closed field is a totally ordered field where positive elements are squares and a polynomial of odd degree has a root.
- 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.
- A real closed field is a totally ordered field where positive elements are squares and a polynomial of odd degree has a root.
- 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 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.

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 "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 $\mathbb{R}$ which is true in a real closed field containing $\mathbb{R}$ is true in $\mathbb{R}$.
- 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 $\mathbb{R}$ if and only if it is true in $\mathbb{R}$
- Special case of quantifier elimination.

Transfer principe

- A statement involving elements of $\mathbb{R}$ which is true in a real closed field containing $\mathbb{R}$ is true in $\mathbb{R}$.
- 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 $\mathbb{R}$ if and only if it is true in $\mathbb{R}$
- Special case of quantifier elimination.

Quantifier elimination

- What is quantifier elimination ?
- High school mathematics

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

$$\iff$$

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

- If true in a real closed field containing $\mathbb{R}$, is true in $\mathbb{R}$!
- Valid for any formula, due to Tarski, use generalizations of Sturm's theorem, or Hermite's quadratic form.

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, use generalizations of Sturm's theorem, or Hermite's quadratic form.

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, use generalizations of Sturm's theorem, or Hermite's quadratic form.

Quantifier elimination

- What is quantifier elimination ?
- High school mathematics

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

$$\iff$$

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

- If true in a real closed field containing $\mathbb{R}$, is true in $\mathbb{R}$!
- Valid for any formula, due to Tarski, use generalizations of Sturm's theorem, or Hermite's quadratic form.

Hermite's quadratic form

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

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

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

Hermite's quadratic form

Proposition

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

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

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.

Hermite's quadratic form (generalized)

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

where $\mu(x)$ is the multiplicity of x.
$\mathrm{Herm}(P, Q)_{i,j} = N_{i+j-2}(P, Q)$

Proposition

The signature of the Hermite quadratic associated to $\mathrm{Herm}(P, Q)$ is the difference between the number of real roots of P where $Q > 0$ and the number of real roots of P where $Q < 0$.

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

Outline of Artin's proof: summary

- 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 "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.

Hilbert's 17th problem: remaining issues

- 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 ?

Hilbert's 17th problem: remaining issues

- 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 ?

Hilbert's 17th problem: remaining issues

- 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 ?

Hilbert's 17th problem: remaining issues

- 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 ?

Hilbert's 17th problem: remaining issues

- 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:

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

• 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:

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

- 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 $\mathbf{C}^k$
  $\Longleftrightarrow$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- For real numbers, statement more complicated.

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 $\mathbf{C}^k$
  $\Longleftrightarrow$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- For real numbers, statement more complicated.

Positivstellensatz (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 $\mathbf{C}^k$
  $\Longleftrightarrow$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- For real numbers, statement more complicated.

- 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 $\mathbf{C}^k$
  $\Longleftrightarrow$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- For real numbers, statement more complicated.

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 $\mathbf{C}^k$
  $\Longleftrightarrow$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- For real numbers, statement more complicated.

Positivstellensatz

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

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

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

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

$k_{I,j}$ positive elements of **K**,

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

Positivstellensatz

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

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

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

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

$k_{I,j}$ positive elements of **K**,

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

Positivstellensatz

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

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

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

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

$k_{I,j}$ positive elements of **K**,

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

Incompatibilities

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

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

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

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

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

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

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:

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

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

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

The degree of this is incompatibility is 4.

Example:

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

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

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

The degree of this is incompatibility is 4.

Example:

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

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

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

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.
- Constructive proofs use quantifier elimination over the reals.
  Various methods for quantifier elimination.

Positivstellensatz: proofs

- Classical proofs of Positivstellensatz based on Zorn's lemma and Tranfer principle, very similar to Artin's proof for Hilbert 17th problem.
- Constructive proofs use quantifier elimination over the reals.
  Various methods for quantifier elimination.

Positivstellensatz: proofs

- Classical proofs of Positivstellensatz based on Zorn's lemma and Tranfer principle, very similar to Artin's proof for Hilbert 17th problem.
- Constructive proofs use quantifier elimination over the reals.
  Various methods for quantifier elimination.

Quantifier elimination

- Various techniques (more or less sophisticated and more or less efficient).
- Cohen-Hormander method very simple conceptually but primitive recursive (not elementary recursive)
- Cylindrical decomposition elementary recursive
- realizable sign conditions for $\mathcal{P} \subset \mathbf{K}[x_1, \ldots, x_k]$ are fixed by list of non empty sign conditions for $\mathrm{Proj}(\mathcal{P}) \subset \mathbf{K}[x_1, \ldots, x_{k-1}]$ (determinants extracted from Hermite matrices)
- classical cylindrical decomposition uses the notion of connected component

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.
- Method :transform a proof that a system of sign conditions is empty, based on a quantifier elimination method, into an incompatibility.

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.
- Method :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 :

  - 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.
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: 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
:

- 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.
  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: 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
:

- 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.
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: 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 :

- 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.
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

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

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

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

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

Positivstellensatz implies Hilbert 17th problem

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

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

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

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

Positivstellensatz implies Hilbert 17th problem

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

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

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

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

Positivstellensatz implies Hilbert 17th problem

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

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

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

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

Positivstellensatz implies Hilbert 17th problem

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

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

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

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

Our strategy

- For every system of sign conditions with no solution, construct an algebraic incompatibility and control the degrees for the Positivstellensatz.
- Recover Hilbert's 17 th problem as a special case
- Uses notions introduced in Lombardi '90
- Key concept : weak inference.

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.

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

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

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

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

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

From right to left.

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.

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

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

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

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

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

From right to left.

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.

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

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

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

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

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

From right to left.

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.

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

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

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

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

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

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

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

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

$\searrow \qquad \swarrow$

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

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

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

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

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

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

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

$\searrow \quad \swarrow$

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

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

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

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

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

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

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

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

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

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

$\searrow \quad \swarrow$

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

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

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

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

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

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

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

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

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

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

$\searrow \qquad \swarrow$

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

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

$\downarrow \mathcal{H},\ A \neq 0 \downarrow \leftarrow$ 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)

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)

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)

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
- Sylvester's inertia law: the signature of a quadratic form is well defined

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
- 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 and sign determination)
- finally : realizable sign conditions for $\mathcal{P} \subset \mathbf{K}[x_1, \ldots, x_k]$ fixed by list of non empty sign conditions for $\mathrm{Proj}(\mathcal{P}) \subset \mathbf{K}[x_1, \ldots, x_{k-1}]$: variant of cylindrical decomposition (which does not use the notion of connected component)

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 and sign determination)
- finally : realizable sign conditions for $\mathcal{P} \subset \mathbf{K}[x_1, \ldots, x_k]$ fixed by list of non empty sign conditions for $\mathrm{Proj}(\mathcal{P}) \subset \mathbf{K}[x_1, \ldots, x_{k-1}]$: variant of cylindrical decomposition (which does not use the notion of connected component)

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 incompatibility 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

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

This 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 !

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

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

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 weak inference 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 weak inference corresponding to the fundamental theorem of algebra
- our variant of cylindrical decomposition then gives univariate polynomials of doubly exponential degrees
- finally : a tower of 5 exponentials
- we are lucky enough that all the other steps do not spoil this bound
- long paper (85 pages) ... maybe a monograph ?

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 weak inference 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 weak inference corresponding to the fundamental theorem of algebra
- our variant of cylindrical decomposition then gives univariate polynomials of doubly exponential degrees
- finally : a tower of 5 exponentials
- we are lucky enough that all the other steps do not spoil this bound
- long paper (85 pages) ... maybe a monograph ?

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 weak inference 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 weak inference corresponding to the fundamental theorem of algebra
- our variant of cylindrical decomposition then gives univariate polynomials of doubly exponential degrees
- finally : a tower of 5 exponentials
- we are lucky enough that all the other steps do not spoil this bound
- long paper (85 pages) ... maybe a monograph ?

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 weak inference 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 weak inference corresponding to the fundamental theorem of algebra
- our variant of cylindrical decomposition then gives univariate polynomials of doubly exponential degrees
- finally : a tower of 5 exponentials
- we are lucky enough that all the other steps do not spoil this bound
- long paper (85 pages) ... maybe a monograph ?

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 weak inference 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 weak inference corresponding to the fundamental theorem of algebra
- our variant of cylindrical decomposition then gives univariate polynomials of doubly exponential degrees
- finally : a tower of 5 exponentials
- we are lucky enough that all the other steps do not spoil this bound
- long paper (85 pages) ... maybe a monograph ?

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 weak inference 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 weak inference corresponding to the fundamental theorem of algebra
- our variant of cylindrical decomposition then gives univariate polynomials of doubly exponential degrees
- finally : a tower of 5 exponentials
- we are lucky enough that all the other steps do not spoil this bound
- long paper (85 pages) ... maybe a monograph ?

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 weak inference 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 weak inference corresponding to the fundamental theorem of algebra
- our variant of cylindrical decomposition then gives univariate polynomials of doubly exponential degrees
- finally : a tower of 5 exponentials
- we are lucky enough that all the other steps do not spoil this bound
- long paper (85 pages) ... maybe a monograph ?

Discussion

- What can be hoped for ?
- Positivstellensatz: single exponential lower bounds [GV2].
- Best lower bound for Hilbert 17th problem : degree linear in k (recent result by [BGP]) !
- Upper bounds
- Nullstellensatz : single exponential (..., Kollar, Jelonek, ...).
- Deciding emptyness for the reals (more sophisticated than cylindrical decomposition) : single exponential: Grigori'ev-Vorobjov results [GV1].

Discussion

- What can be hoped for ?
- Positivstellensatz: single exponential lower bounds [GV2].
- Best lower bound for Hilbert 17th problem : degree linear in k (recent result by [BGP]) !
- Upper bounds
- Nullstellensatz : single exponential (..., Kollar, Jelonek, ...).
- Deciding emptyness for the reals (more sophisticated than cylindrical decomposition) : single exponential: Grigori'ev-Vorobjov results [GV1].

Discussion

- What can be hoped for ?
- Positivstellensatz: single exponential lower bounds [GV2].
- Best lower bound for Hilbert 17th problem : degree linear in k (recent result by [BGP]) !
- Upper bounds
- Nullstellensatz : single exponential (..., Kollar, Jelonek, ...).
- Deciding emptyness for the reals (more sophisticated than cylindrical decomposition) : single exponential: Grigori'ev-Vorobjov results [GV1].

Discussion

- What can be hoped for ?
- Positivstellensatz: single exponential lower bounds [GV2].
- Best lower bound for Hilbert 17th problem : degree linear in k (recent result by [BGP]) !
- Upper bounds
- Nullstellensatz : single exponential (..., Kollar, Jelonek, ...).
- Deciding emptyness for the reals (more sophisticated than cylindrical decomposition) : single exponential: Grigori'ev-Vorobjov results [GV1].

Discussion

- What can be hoped for ?
- Positivstellensatz: single exponential lower bounds [GV2].
- Best lower bound for Hilbert 17th problem : degree linear in k (recent result by [BGP]) !
- Upper bounds
- Nullstellensatz : single exponential (..., Kollar, Jelonek, ...).
- Deciding emptyness for the reals (more sophisticated than cylindrical decomposition) : single exponential: Grigori'ev-Vorobjov results [GV1].

Related work

- Variant of cylindrical algebraic decomposition, what for ?
- Gives an algebraic elementary recursive proof of quantifier elimination based on Thom encodings and sign determination, not using the notion of connected component.
- Slightly worse complexity than CAD (number of polynomials is not polynomial in d when k is fixed). Joint work with D. Perrucci.
- Constructive real algebraic geometry (certified in Coq). Work of Cyril Cohen, Assia Mahboubi.

References

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

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

[GV2] D. 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)