Effectivity and Complexity Results in Hilbert's 17th problem

Marie-Françoise Roy
Université de Rennes 1, France
based on joint work with
Henri Lombardi
Université de Franche-Comté, France
and
Daniel Perrucci
Universidad de Buenos Aires, Argentina

Big Proof, Cambridge
28 june, 2017

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

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

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

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

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.

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.

Motzkin's counter-example

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

- 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

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

- 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

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

- 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 does 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 does 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 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.

Outline of Artin's proof

- Suppose P is not a sum of squares of rational functions.
- Sums of squares form a proper cone of the field of rational functions, and does not contain P .
- Using Zorn, get a total order on the field of rational functions which does not contain P.
- Taking the real closure of the field of rational functions for this order, get a real closed field in which P takes negative values (when evaluated at the "generic point" = the point $(X_1, \ldots, X_k)$).
- Then P takes negative values over the reals. First instance of a transfer principle in real algebraic geometry. Based on Sturm's theorem, or Hermite quadratic form.

Transfer principe

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

$$\forall x_1 \ \ldots \ \forall x_k \ P(x_1, \ldots, x_k) \geq 0$$

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 $\mathbb{R}$ (such as the real closure of the field of rational functions for a chosen total order) is true in $\mathbb{R}$.
- Not any statement, only "first order logic statement".
- Example of such statement

$$\forall x_1 \ \ldots \ \forall x_k \ P(x_1, \ldots, x_k) \geq 0$$

  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

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

$$\Longleftrightarrow$$

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

- 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

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

$$\Longleftrightarrow$$

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

- 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.

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

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

Hermite's quadratic form

$$a \neq 0, P(x) = ax^2 + bx + c = a(x - x_1)(x - x_2)$$

$$N_0 = x_1^0 + x_2^0 = 2$$

$$N_1 = x_1 + x_2 = -\frac{b}{a}$$

$$N_2 = x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1x_2 = \frac{b^2}{a^2} - 2\frac{c}{a} = \frac{b^2 - 2ac}{a^2}$$

$$\mathrm{Herm}(P) = \begin{bmatrix} N_0 & N_1 \\ N_1 & N_2 \end{bmatrix} = \begin{bmatrix} 2 & -\frac{b}{a} \\ -\frac{b}{a} & \frac{b^2-2ac}{a^2} \end{bmatrix}$$

$$\det(\mathrm{Herm}(P)) = \frac{b^2 - 4ac}{a^2} = \frac{\Delta}{a^2}$$

The signature of $\mathrm{Herm}(P)$ is

- 2 if $\Delta > 0$ (2 real roots)
- 1 if $\Delta = 0$ (1 real root)
- 0 if $\Delta < 0$ (no real root)

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

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

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

Proposition

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

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

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 Tarski query of P and Q :*

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

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

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?
- Quantifier elimination decides whether the polynomial is everywhere non negative, but how to construct the representation ?
- 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?
- Quantifier elimination decides whether the polynomial is everywhere non negative, but how to construct the representation ?
- 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?
- Quantifier elimination decides whether the polynomial is everywhere non negative, but how to construct the representation ?
- 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?
- Quantifier elimination decides whether the polynomial is everywhere non negative, but how to construct the representation ?
- 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?
- Quantifier elimination decides whether the polynomial is everywhere non negative, but how to construct the representation ?
- 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?
- Quantifier elimination decides whether the polynomial is everywhere non negative, but how to construct the representation ?
- Complexity problems : what are the best possible bounds on the degrees of the polynomials in this representation ?

Complexity estimates for Hilbert 17th problem

- 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:

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

Complexity estimates for Hilbert 17th problem

- 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:

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

Positivstellensatz (Krivine '64, Stengle '74)

- 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 (Krivine '64, Stengle '74)

- 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 (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.

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.

Quantitative 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 $\mathbf{C}^k$
  $\Longleftrightarrow$
  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- What are the degree of the A_i ?
- using resultants (Grete Hermann 1925):double exponential degrees in k
- more recently (Brownawell 1987 (analytic methods),..., Kollar (algebraic methods), ..., further improved by Sombra) single exponential degrees, cannot be improved

Quantitative 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 $\mathbf{C}^k$

  $\Longleftrightarrow$

  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- What are the degree of the A_i ?
- using resultants (Grete Hermann 1925):double exponential degrees in k
- more recently (Brownawell 1987 (analytic methods),..., Kollar (algebraic methods), ..., further improved by Sombra) single exponential degrees, cannot be improved

Quantitative 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 $\mathbf{C}^k$

  $\Longleftrightarrow$

  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- What are the degree of the A_i ?
- using resultants (Grete Hermann 1925):double exponential degrees in k
- more recently (Brownawell 1987 (analytic methods),..., Kollar (algebraic methods), ..., further improved by Sombra) single exponential degrees, cannot be improved

Quantitative 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 $\mathbf{C}^k$

  $\Longleftrightarrow$

  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- What are the degree of the A_i ?
- using resultants (Grete Hermann 1925):double exponential degrees in k
- more recently (Brownawell 1987 (analytic methods),..., Kollar (algebraic methods), ..., further improved by Sombra) single exponential degrees, cannot be improved

Quantitative 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 $\mathbf{C}^k$

  $\Longleftrightarrow$

  $\exists \quad (A_1, \ldots, A_s) \in \mathbf{K}[x_1, \ldots, x_k]^s \qquad A_1 P_1 + \cdots + A_s P_s = 1.$
- What are the degree of the A_i ?
- using resultants (Grete Hermann 1925):double exponential degrees in k
- more recently (Brownawell 1987 (analytic methods),..., Kollar (algebraic methods), ..., further improved by Sombra) single exponential degrees, cannot be improved

Positivstellensatz

- **K** an ordered field (where positive elements have square roots (avoid technicalities)), **R** a real closed extension of **K**,

- $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$,
- $I_{\neq}, I_{\geq}, I_{=} \subset \{1, \ldots, s\}$,

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

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

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

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

Positivstellensatz

- **K** an ordered field (where positive elements have square roots (avoid technicalities)), **R** a real closed extension of **K**,
- $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$,
- $I_{\neq}, I_{\geq}, I_{=} \subset \{1, \ldots, s\}$,

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

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

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

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

Positivstellensatz

- **K** an ordered field (where positive elements have square roots (avoid technicalities)), **R** a real closed extension of **K**,
- $P_1, \ldots, P_s \in \mathbf{K}[x_1, \ldots, x_k]$,
- $I_{\neq}, I_{\geq}, I_{=} \subset \{1, \ldots, s\}$,

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

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

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

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

Incompatibilities

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

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

with

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

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

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

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

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

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 of incompatibility

$$P < 0, P \geq 0 \text{ has no solution in } \mathbb{R}^k$$

$$\downarrow\ P \neq 0, -P \geq 0, P \geq 0\ \downarrow$$

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

The degree of this incompatibily is $2\deg(P)$.

Example of incompatibility

$$P < 0, P \geq 0 \text{ has no solution in } \mathbb{R}^k$$

$$\downarrow \; P \neq 0, -P \geq 0, P \geq 0 \; \downarrow$$

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

The degree of this incompatibily is $2\deg(P)$.

Example of incompatibility

With $\Delta = b^2 - 4ac$,

$$\begin{cases} ax^2 + bx + c & = & 0 \\ \Delta & < & 0 \end{cases} \quad \text{has no solution in } \mathbb{R}^2$$

(the roots are complex when $\Delta < 0$)

$$\downarrow \ \Delta \neq 0, -\Delta \geq 0, ax^2 + bx + c = 0, \ \downarrow$$

$$\underbrace{\Delta^2}_{>0} + \underbrace{(-\Delta)(2ax+b)^2}_{\geq 0} + \underbrace{4a\Delta(ax^2+bx+c)}_{=0} = 0.$$

The degree of this incompatibility is 4 (if a, b, c, x are variables).

Example of incompatibility

With $\Delta = b^2 - 4ac$,

$$\begin{cases} ax^2 + bx + c & = & 0 \\ \Delta & < & 0 \end{cases} \quad \text{has no solution in } \mathbb{R}^2$$

(the roots are complex when $\Delta < 0$)

$$\downarrow \ \Delta \neq 0, -\Delta \geq 0, ax^2 + bx + c = 0, \ \downarrow$$

$$\underbrace{\Delta^2}_{>0} + \underbrace{(-\Delta)(2ax+b)^2}_{\geq 0} + \underbrace{4a\Delta(ax^2+bx+c)}_{=0} = 0.$$

The degree of this incompatibility is 4 (if a, b, c, x are variables).

Example of incompatibility

With $\Delta = b^2 - 4ac$,

$$\begin{cases} ax^2 + bx + c & = & 0 \\ \Delta & < & 0 \end{cases} \quad \text{has no solution in } \mathbb{R}^2$$

(the roots are complex when $\Delta < 0$)

$$\downarrow \ \Delta \neq 0, -\Delta \geq 0, ax^2 + bx + c = 0, \ \downarrow$$

$$\underbrace{\Delta^2}_{>0} + \underbrace{(-\Delta)(2ax+b)^2}_{\geq 0} + \underbrace{4a\Delta(ax^2+bx+c)}_{=0} = 0.$$

The degree of this incompatibility is 4 (if a, b, c, x are variables).

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 techniques 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 techniques 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 techniques for quantifier elimination.

Quantifier elimination

- Most methods eliminate variables one after the other : projection method
- list of realizable sign conditions for $\mathcal{P} \subset \mathbf{K}[x_1, \ldots, x_k]$ are fixed by list of realizable sign conditions for $\mathrm{Proj}(\mathcal{P}) \subset \mathbf{K}[x_1, \ldots, x_{k-1}]$
- Cohen-Hormander method very simple conceptually but primitive recursive (not elementary recursive) (same situation with Tarski and Seidenberg),
- projection method can be made efficient = elementary recursive
- classical cylindrical decomposition is elementary recursive BUT its proof of correctness uses the geometric notion of connected component
- new projection method with proof of correctness based only on algebra (using Thom's encoding of real roots by sign of derivatives and sign determination)

Tools for elementary recursive quantifier elimination based only on algebra

- Thom encoding: a real root x of a univariate polynomial P is identified by the signs at x of the derivatives of P
- sign determination : compute at the roots of P the signs of a list of polynomials $Q_1, \ldots, Q_s$ efficient algorithm using Tarski queries of a few products of the Q_i
- sign determination is used to compute Thom encodings

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
- Constructive proofs use quantifier elimination over the reals.
- Method :transform a purely algebraic 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
- Constructive proofs use quantifier elimination over the reals.
- Method :transform a purely algebraic 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 our efficient projection method (with correctness proof based only on algebra, using Thom's encoding of real roots by sign of derivatives and sign determination) .

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 our efficient projection method (with correctness proof based only on algebra, using Thom's encoding of real roots by sign of derivatives and sign determination) .

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 our efficient projection method (with correctness proof based only on algebra, using Thom's encoding of real roots by sign of derivatives and sign determination) .

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 our efficient projection method (with correctness proof based only on algebra, using Thom's encoding of real roots by sign of derivatives and sign determination) .

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

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

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

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

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

Positivstellensatz implies Hilbert 17th problem

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

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

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

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

Positivstellensatz implies Hilbert 17th problem

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

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

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

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

Positivstellensatz implies Hilbert 17th problem

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

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

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

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

Positivstellensatz implies Hilbert 17th problem

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

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

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

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

Our strategy

- Transform a purely algebraic proof that the realizable sign conditions cover $\mathbf{R}^k$ into a method of construction of incompatibilities for non realizable sign conditions, controling the degrees.
- Constructive Positivstellensatz.
- Recover Hilbert's 17 th problem as a special case
- Uses notions introduced in Lombardi '90
- Key concept : weak inference.

Weak inference

(in the particular case we need)

Definition (weak inference)

$\mathcal{F}, \mathcal{G}$ systems of sing conditions in $\mathbf{K}[u]$ 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 conditions (context) $\mathcal{C}$ in $\mathbf{K}[v]$ with $v \supset u$ not containing t and every incompatibility

$$\downarrow \mathcal{G}(u, t),\ \mathcal{C}(v) \downarrow_{\mathbf{K}[v,t]}$$

produces an incompatibility

$$\downarrow \mathcal{F}(u),\ \mathcal{C}(v) \downarrow_{\mathbf{K}[v]} .$$

From right to left.

Construction ? an example !

Weak inference

(in the particular case we need)

Definition (weak inference)

$\mathcal{F}, \mathcal{G}$ systems of sing conditions in $\mathbf{K}[u]$ 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 conditions (context) $\mathcal{C}$ in $\mathbf{K}[v]$ with $v \supset u$ not containing t and every incompatibility

$$\downarrow \mathcal{G}(u,t),\ \mathcal{C}(v) \downarrow_{\mathbf{K}[v,t]}$$

produces an incompatibility

$$\downarrow \mathcal{F}(u),\ \mathcal{C}(v) \downarrow_{\mathbf{K}[v]}\ .$$

From right to left.

Construction ? an example !

Example of a weak inference: the positive elements are squares

$$A(u) \geq 0 \quad \Longrightarrow \exists t\ A(u) = t^2$$

$A(u)$ any multivariate polynomial, $\mathcal{C}(v)$ any system of sign condition (context)

$$\downarrow \mathcal{C}(v), A(u) = t^2 \downarrow \quad \longrightarrow \quad \left\{ \begin{array}{c} \mathcal{C}(v) \\ A(u) = t^2 \end{array} \right. \text{ has no solution}$$

$$\downarrow$$

$$\downarrow \mathcal{C}(v),\ A(u) \geq 0 \downarrow \quad \longrightarrow \quad \left\{ \begin{array}{c} \mathcal{C}(v) \\ A(u) \geq 0 \end{array} \right. \text{ has no solution}$$

$$A(u) \geq 0 \quad \vdash \quad \exists\, t\ A(u) = t^2$$

From right to left.

Example of a weak inference: the positive elements are squares

$$A(u) \geq 0 \implies \exists t\ A(u) = t^2$$

$A(u)$ any multivariate polynomial, $\mathcal{C}(v)$ any system of sign condition (context)

$$\downarrow\ \mathcal{C}(v), A(u) = t^2\ \downarrow \longrightarrow \left\{ \begin{array}{c} \mathcal{C}(v) \\ A(u) = t^2 \end{array} \right. \text{ has no solution}$$

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

$$\downarrow\ \mathcal{C}(v),\ \ A(u) \geq 0\ \downarrow \longrightarrow \left\{ \begin{array}{c} \mathcal{C}(v) \\ A(u) \geq 0 \end{array} \right. \text{ has no solution}$$

$$A(u) \geq 0 \vdash \exists\ t\ A(u) = t^2$$

From right to left.

Example of a weak inference: the positive elements are squares

$$A(u) \geq 0 \implies \exists t\ A(u) = t^2$$

$A(u)$ any multivariate polynomial, $\mathcal{C}(v)$ any system of sign condition (context)

$$\downarrow\ \mathcal{C}(v), A(u) = t^2\ \downarrow \longrightarrow \left\{ \begin{array}{c} \mathcal{C}(v) \\ A(u) = t^2 \end{array} \right. \text{ has no solution}$$

$$\downarrow\ \mathcal{C}(v),\ \ A(u) \geq 0\ \downarrow \longrightarrow \left\{ \begin{array}{c} \mathcal{C}(v) \\ A(u) \geq 0 \end{array} \right. \text{ has no solution}$$

$$A(u) \geq 0 \vdash \exists\ t\ A(u) = t^2$$

From right to left.

Example of a weak inference: the positive elements are squares

$$A(u) \geq 0 \implies \exists t\ A(u) = t^2$$

$A(u)$ any multivariate polynomial, $\mathcal{C}(v)$ any system of sign condition (context)

$$\downarrow\ \mathcal{C}(v), A(u) = t^2\ \downarrow \longrightarrow \left\{ \begin{array}{c} \mathcal{C}(v) \\ A(u) = t^2 \end{array} \right. \text{ has no solution}$$

$$\downarrow\ \mathcal{C}(v),\ \ A(u) \geq 0\ \downarrow \longrightarrow \left\{ \begin{array}{c} \mathcal{C}(v) \\ A(u) \geq 0 \end{array} \right. \text{ has no solution}$$

$$A(u) \geq 0 \vdash \exists\ t\ A(u) = t^2$$

From right to left.

The construction

We are given an incompatibility

$$S + \sum_i V_i^2(t) \cdot N_i + \sum_j W_j(t) \cdot Z_j + W(t) \cdot (t^2 - A) = 0 \qquad (2)$$

$V_{i1} \cdot t + V_{i0}$ the remainder of $V_i(t)$ in the division by $t^2 - A$
$W_{j1} \cdot t + W_{j0}$ the remainder of $W_j(t)$ in the division by $t^2 - A$
there exists $W'(t) \in \mathbf{K}[v][t]$ such that

$$S + \sum_i (V_{i1} \cdot t + V_{i0})^2 \cdot N_i + \sum_j (W_{j1} \cdot t + W_{j0}) \cdot Z_j + W'(t) \cdot (t^2 - A) = 0.$$

which is rewritten in

$$S + \sum_i (V_{i1}^2 \cdot A + V_{i0}^2) \cdot N_i + \sum_j W_{j0} \cdot Z_j + W''' \cdot t + W''(t) \cdot (t^2 - A) = 0.$$

with $W''' \in \mathbf{K}[v]$ and $W''(t) \in \mathbf{K}[v][t]$.

The construction (end)

We had

$$S+\sum_i (V_{i1}^2 \cdot A + V_{i0}^2)\cdot N_i + \sum_j W_{j0}\cdot Z_j + W'''\cdot t + W''(t)\cdot(t^2 - A) = 0.$$

Examining the degrees in t, we find $W''(t) = 0$, then $W''' = 0$
This ends the proof since

$$S + \sum_i (V_{i1}^2 \cdot A + V_{i0}^2)\cdot N_i + \sum_j W_{j0}\cdot Z_j = 0.$$

is the incompatibility we are looking for. And it is possible to keep track of the degree with respect to the variables.

Construction ?

- Recipee producing a new incompatibility starting from a given incompatibility.
- In our example what are the ingredients of the recipee ?
- Make an euclidean division.
- Group terms differenty.
- Deduce that some expressions are zero identifying the degrees.
- Keep track of the degrees with respect to the various variables.

List of statements needed into weak inferences form : axioms

- axioms of ordered fields
- a positive element has a square root (our example)
- a real polynomial of odd degree has a real root
- controling the degrees

List of statements needed into weak inferences form : axioms

- axioms of ordered fields
- a positive element has a square root (our example)
- a real polynomial of odd degree has a real root
- controling the degrees

List of statements needed into weak inferences form: classical algebra

- a real polynomial has a complex root (using an algebraic proof due to Laplace)
- signature of Hermite's quadratic form gives the number of real roots of a polynomial, and the Tarski queries and also by sign conditions on principal minors
- signature of Hermite's quadratic form determined 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: classical algebra

- a real polynomial has a complex root (using an algebraic proof due to Laplace)
- signature of Hermite's quadratic form gives the number of real roots of a polynomial, and the Tarski queries and also by sign conditions on principal minors
- signature of Hermite's quadratic form determined 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: modern computer algebra

- realizable sign conditions for a family of univariate polynomials at the roots of a polynomial fixed by sign of minors of several Hermite quadratic form (using Thom's encoding of real roots and sign determination)
- list of realizable sign conditions for $\mathcal{P} \subset \mathbf{K}[x_1, \ldots, x_k]$ fixed by realizable sign conditions for $\mathrm{Proj}(\mathcal{P}) \subset \mathbf{K}[x_1, \ldots, x_{k-1}]$: efficient projection method using only algebra
- list of realizable sign conditions for $\mathcal{P} \subset \mathbf{K}[x_1, \ldots, x_k]$ cover $\mathbf{R}^k$ by induction (eliminating variables one by one).

List of statements into weak inferences form: modern computer algebra

- realizable sign conditions for a family of univariate polynomials at the roots of a polynomial fixed by sign of minors of several Hermite quadratic form (using Thom's encoding of real roots and sign determination)
- list of realizable sign conditions for $\mathcal{P} \subset \mathbf{K}[x_1, \ldots, x_k]$ fixed by realizable sign conditions for $\mathrm{Proj}(\mathcal{P}) \subset \mathbf{K}[x_1, \ldots, x_{k-1}]$: efficient projection method using only algebra
- list of realizable sign conditions for $\mathcal{P} \subset \mathbf{K}[x_1, \ldots, x_k]$ cover $\mathbf{R}^k$ by induction (eliminating variables one by one).

How is produced the sum of squares ?

Suppose that P takes always non negative values. The proof that

$$P \geq 0$$

(no other realizable sign condition) is transformed, step by step, in a proof of the weak inference

$$\vdash \quad P \geq 0,$$

using $\mathrm{Proj}(\{P\})$, $\mathrm{Proj}(\mathrm{Proj}(\{P\}))$ etc...
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

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

This is an 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 !!!

Discussion: relevant for Big Proof ?

- many possible meanings for BIG
- Artin's proof is great
- constructive proofs took a long time to appear
- our work took 25 years (and ended thanks to Daniel Perrucci)
- our paper is long
- our bound in unusually high for a construction in algebra
- some technical lemmas on degree estimates are totally elementary and very hard to check (any volunteers ?)

Discussion: relevant for Big Proof ?

- many possible meanings for BIG
- Artin's proof is great
- constructive proofs took a long time to appear
- our work took 25 years (and ended thanks to Daniel Perrucci)
- our paper is long
- our bound in unusually high for a construction in algebra
- some technical lemmas on degree estimates are totally elementary and very hard to check (any volunteers ?)

Discussion: relevant for Big Proof ?

- many possible meanings for BIG
- Artin's proof is great
- constructive proofs took a long time to appear
- our work took 25 years (and ended thanks to Daniel Perrucci)
- our paper is long
- our bound in unusually high for a construction in algebra
- some technical lemmas on degree estimates are totally elementary and very hard to check (any volunteers ?)

Discussion: relevant for Big Proof ?

- many possible meanings for BIG
- Artin's proof is great
- constructive proofs took a long time to appear
- our work took 25 years (and ended thanks to Daniel Perrucci)
- our paper is long
- our bound in unusually high for a construction in algebra
- some technical lemmas on degree estimates are totally elementary and very hard to check (any volunteers ?)

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 projection method (with correctness proof based only on algebra) 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 (to appear in Memoirs of the AMS) ...

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 projection method (with correctness proof based only on algebra) 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 (to appear in Memoirs of the AMS) ...

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 projection method (with correctness proof based only on algebra) 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 (to appear in Memoirs of the AMS) ...

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 projection method (with correctness proof based only on algebra) 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 (to appear in Memoirs of the AMS) ...

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 projection method (with correctness proof based only on algebra) 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 (to appear in Memoirs of the AMS) ...

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 projection method (with correctness proof based only on algebra) 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 (to appear in Memoirs of the AMS) ...

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 projection method (with correctness proof based only on algebra) 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 (to appear in Memoirs of the AMS) ...

Discussion

- What can be hoped for ?
- Positivstellensatz: single exponential lower bounds (Grigorev Vorobjov)
- Best lower bound for Hilbert 17th problem : degree linear in k (recent result by Bleckerman and co) !
- Upper bounds
- Nullstellensatz : single exponential (..., Kollar, ...).
- Deciding emptyness for the reals (more sophisticated than projecting variable one by one) : single exponential: Grigori'ev-Vorobjov results, can this be used ?

Discussion

- What can be hoped for ?
- Positivstellensatz: single exponential lower bounds (Grigorev Vorobjov)
- Best lower bound for Hilbert 17th problem : degree linear in k (recent result by Bleckerman and co) !
- Upper bounds
- Nullstellensatz : single exponential (..., Kollar, ...).
- Deciding emptyness for the reals (more sophisticated than projecting variable one by one) : single exponential: Grigori'ev-Vorobjov results, can this be used ?

Discussion

- What can be hoped for ?
- Positivstellensatz: single exponential lower bounds (Grigorev Vorobjov)
- Best lower bound for Hilbert 17th problem : degree linear in k (recent result by Bleckerman and co) !
- Upper bounds
- Nullstellensatz : single exponential (..., Kollar, ...).
- Deciding emptyness for the reals (more sophisticated than projecting variable one by one) : single exponential: Grigori'ev-Vorobjov results, can this be used ?

Discussion

- What can be hoped for ?
- Positivstellensatz: single exponential lower bounds (Grigorev Vorobjov)
- Best lower bound for Hilbert 17th problem : degree linear in k (recent result by Bleckerman and co) !
- Upper bounds
- Nullstellensatz : single exponential (..., Kollar, ...).
- Deciding emptyness for the reals (more sophisticated than projecting variable one by one) : single exponential: Grigori'ev-Vorobjov results, can this be used ?

Discussion

- What can be hoped for ?
- Positivstellensatz: single exponential lower bounds (Grigorev Vorobjov)
- Best lower bound for Hilbert 17th problem : degree linear in k (recent result by Bleckerman and co) !
- Upper bounds
- Nullstellensatz : single exponential (..., Kollar, ...).
- Deciding emptyness for the reals (more sophisticated than projecting variable one by one) : single exponential: Grigori'ev-Vorobjov results, can this be used ?

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.

[PR] D. Perrucci, M.-F. Roy, *Elementary recursive quantifier elimination based on Thom encoding and sign determination*, Final version, to appear in Annals of Pure and Applied Logic https://arxiv.org/abs/1609.02879

[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 all other references there)