An elementary recursive bound for Positivstellensatz and Hilbert 17th 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
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)
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)
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)
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.
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.
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.
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.
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.
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?
Hilbert 17th problem

- Reformulation proposed by Minkowski.
- Question Hilbert ’1900.
- Is a a non-negative polynomial a sum of squares of rational functions?
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.
What is quantifier elimination?

High school mathematics

\[ \exists x \ ax^2 + bx + c = 0, \ a \neq 0 \]

\[ \iff \]

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

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.

Lombardi, Perrucci, Roy

An elementary recursive bound for Positivstellensatz and Hilbert 17th problem
What is quantifier elimination?

High school mathematics

\[ \exists x \ ax^2 + bx + c = 0, \ a \neq 0 \]

\[ \iff \ b^2 - 4ac \geq 0, \ a \neq 0 \]

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.
What is quantifier elimination?

High school mathematics

\[ \exists x \ ax^2 + bx + c = 0, \ a \neq 0 \]

\[ \iff \]

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

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.
What is quantifier elimination?

High school mathematics

\[ \exists x \ ax^2 + bx + c = 0, a \neq 0 \]

\[ \iff b^2 - 4ac \geq 0, a \neq 0 \]

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

\[ N_i = \sum_{x \in \text{Zer}(P,C)} \mu(x)x^i, \]

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

\[
\text{Herm}(P) = \begin{bmatrix}
N_0 & N_1 & \cdots & \cdots & N_{p-1} \\
N_1 & \cdots & \cdots & N_{p-1} & N_p \\
\vdots & \ddots & \ddots & \ddots & \ddots \\
\vdots & \ddots & N_{p-1} & N_p & \ddots \\
N_{p-1} & N_p & \cdots & \cdots & N_{2p-2}
\end{bmatrix}
\]
Proposition

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

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

with the convention \( a_i = N_i = 0 \) for \( i < 0 \).

Proposition

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

Hint: complex conjugate roots contribute for a difference of two squares.
Hermite’s quadratic form (generalized)

\[ N_i(P, Q) = \sum_{x \in \text{Zer}(P, C)} \mu(x) Q(x) x^i, \]

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

\( \text{Herm}(P, Q)_{i,j} = N_{i+j-2}(P, Q) \)

**Proposition**

*The signature of the Hermite quadratic associated to* \( \text{Herm}(P, Q) \) *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?

Lombardi, Perrucci, Roy
An elementary recursive bound for Positivstellensatz and Hilbert 17th
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?
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 $\leadsto$ primitive recursive degree bounds on $k$ and $d = \deg P$.

• Our work ’14: another constructive proof $\leadsto$ elementary recursive degree bound: $2^{2^d 4^k}$.
Kreisel ’57 - Daykin ’61 - Lombardi ’90 - Schmid ’00: Constructive proofs $\leadsto$ primitive recursive degree bounds on $k$ and $d = \deg P$.

Our work ’14: another constructive proof $\leadsto$ elementary recursive degree bound:

$$2^{2^{2q4^k}}.$$
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, \(\mathbb{C}\) an algebraically closed extension of \(K\),

\(P_1, \ldots, P_s \in K[x_1, \ldots, x_k]\)

\(P_1 = \ldots = P_s = 0\) no solution in \(\mathbb{C}^k\)

\(\iff\)

\(\exists (A_1, \ldots, A_s) \in K[x_1, \ldots, x_k]^s\) \hspace{1cm} \(A_1 P_1 + \cdots + A_s P_s = 1\).

For real numbers, statement more complicated.
Find algebraic identities certifying that a system of sign condition is empty.

In the spirit of Nullstellensatz.

\[ K \text{ a field, } C \text{ an algebraically closed extension of } K, \]
\[ P_1, \ldots, P_s \in K[x_1, \ldots, x_k] \]
\[ P_1 = \ldots = P_s = 0 \text{ no solution in } C^k \]
\[ \iff \]
\[ \exists \ (A_1, \ldots, A_s) \in K[x_1, \ldots, x_k]^s \quad A_1 P_1 + \cdots + A_s P_s = 1. \]

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 \( K \),  
\( P_1, \ldots, P_s \in K[x_1, \ldots, x_k] \)  
\( P_1 = \ldots = P_s = 0 \) no solution in \( C^k \)  
\[ \iff \exists (A_1, \ldots, A_s) \in K[x_1, \ldots, x_k]^s \quad A_1 P_1 + \cdots + A_s P_s = 1. \]

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, \( \mathbb{C} \) an algebraically closed extension of \( K \),
  \( P_1, \ldots, P_s \in K[x_1, \ldots, x_k] \)
  \( P_1 = \ldots = P_s = 0 \) no solution in \( \mathbb{C}^k \)
  \( \iff \)
  \( \exists (A_1, \ldots, A_s) \in K[x_1, \ldots, x_k]^s \quad A_1 P_1 + \cdots + A_s P_s = 1. \)
- 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 $K$,

$P_1, \ldots, P_s \in K[x_1, \ldots, x_k]$

$P_1 = \ldots = P_s = 0$ no solution in $C^k$

$\iff$

$\exists (A_1, \ldots, A_s) \in K[x_1, \ldots, x_k]^s \quad A_1 P_1 + \cdots + A_s P_s = 1.$

For real numbers, statement more complicated.
Positivstellensatz

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

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

$\exists \quad S = \prod_{i \in I_\neq} P_i^{2e_i}, \quad N = \sum_{I_\geq} \left( \sum_{j} k_{l,j} Q_{l,j}^2 \right) \prod_{i \in I} P_i \quad (k_{l,j} > 0 \text{ in } K)$

$Z \in \langle P_i \mid i \in I_= \rangle \subset K[x]$ $k_{l,j}$ positive elements of $K$, such that $S + N + Z = 0$. $> 0 \quad \geq 0 \quad = 0$
• \(K\) an ordered field, \(R\) a real closed extension of \(K\),

• \(P_1, \ldots, P_s \in K[x_1, \ldots, x_k]\),

• \(I \neq, I \geq, I = \subset \{1, \ldots, s\}\),

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

\[ \exists \quad S = \prod_{i \in I \neq} P_i^{2e_i}, \quad N = \sum_{I \subset I \geq} \left( \sum_{j} k_{l,j} Q_{l,j}^2 \right) \prod_{i \in I} P_i \quad (k_{l,j} > 0 \text{ in } K) \]

\[ Z \in \langle P_i \mid i \in I = \rangle \subset K[x] \]

\(k_{l,j}\) positive elements of \(K\),

such that

\[ S > 0 \quad + \quad N \geq 0 \quad + \quad Z = 0. \]
Positivstellensatz

- $K$ an ordered field, $R$ a real closed extension of $K$,

- $P_1, \ldots, P_s \in K[x_1, \ldots, x_k]$,

- $l_\neq, l_\geq, l_= \subset \{1, \ldots, s\}$,

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

\[\exists \quad S = \prod_{i \in l_\neq} P_i^{2e_i}, \quad N = \sum_{l \subset l_\geq} \left( \sum_{j} k_{l,j} Q_{l,j}^2 \right) \prod_{i \in l} P_i \quad (k_{l,j} > 0 \text{ in } K)\]

\[Z \in \langle P_i \mid i \in l_= \rangle \subset K[x]\]

$k_{l,j}$ positive elements of $K$,

such that \[S + N + Z = 0.\]
Incompatibilities

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

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

with

\[ S \in \left\{ \prod_{i \in I \neq} P_{2^e_i} \right\} \quad \leftarrow \text{monoid associated to } \mathcal{H} \]

\[ N \in \left\{ \sum_{I \subset I \geq} \left( \sum_{j} k_{l,j} Q_{l,j}^2 \right) \prod_{i \in I} P_i \right\} \quad \leftarrow \text{cone associated to } \mathcal{H} \]

\[ Z \in \langle P_i \mid i \in I = \rangle \quad \leftarrow \text{ideal associated to } \mathcal{H} \]
Degree of an incompatibility

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

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

\[ S = \prod_{i \in I_\neq} P_i^{2e_i}, \quad N = \sum_{l \subseteq I_\geq} \left( \sum_{j} k_{l,j} Q_{l,j}^2 \right) \prod_{i \in l} P_i, \quad Z = \sum_{i \in I_=} Q_i P_i \]

the degree of \( \mathcal{H} \) is the maximum degree of

\[ S = \prod_{i \in I_\neq} P_i^{2e_i}, \quad Q_{l,j}^2 \prod_{i \in l} P_i \quad (l \subseteq I_\geq, j), \quad Q_i P_i \quad (i \in I_=). \]
Example:

\[
\begin{cases}
    x \neq 0 \\
    y - x^2 - 1 \geq 0 \\
    xy = 0
\end{cases}
\]

no solution in \( \mathbb{R}^2 \)

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

\[
x^2 + x^2(y - x^2 - 1) + x^4 + (-x^2y) = 0.
\]

The degree of this is incompatibility is 4.
Example:

\[
\begin{cases}
  x \neq 0 \\
  y - x^2 - 1 \geq 0 \\
  xy = 0
\end{cases}
\]

no solution in $\mathbb{R}^2$

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

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

The degree of this is incompatibility is 4.
Example:

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

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

\[
\begin{aligned}
  x^2 + x^2(y - x^2 - 1) + x^4 + (-x^2y) &= 0 \\
  > 0 + \underbrace{\geq 0}_{\geq 0} + \underbrace{= 0}_{= 0}
\end{aligned}
\]

The degree of this is incompatibility is 4.
Classical proofs of Positivstellensatz based on Zorn’s lemma and Transfer principle, very similar to Artin’s proof for Hilbert 17th problem.

Constructive proofs use quantifier elimination over the reals.
Various methods for quantifier elimination.
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.
Classical proofs of Positivstellensatz based on Zorn’s lemma and Transfer 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 $\mathcal{P} \subset \mathbb{K}[x_1, \ldots, x_k]$ are fixed by list of non empty sign conditions for $\text{Proj}(\mathcal{P}) \subset \mathbb{K}[x_1, \ldots, x_{k-1}]$ (determinants extracted from Hermite matrices)
- Classical cylindrical decomposition uses the notion of connected component
Classical proofs of Positivstellensatz based on Zorn’s lemma and Transfer principle, very similar to Artin’s proof for Hilbert’s 17th 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.
Classical proofs of Positivstellensatz based on Zorn’s lemma and Transfer principle, very similar to Artin’s proof for Hilbert’s 17th 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.
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 $s$:

$$2^{2^{\max\{2,d\}4^k}} + s^2^k \max\{2,d\}16^k \text{bit}(d).$$
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 $s$:
$$2^{2^{2\max\{2,d\}4^k + s^2k \max\{2,d\}16^k \text{bit}(d)}}.$$
• **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 $s$:

$$2^{2^\max\{2,d\}4^k} + s^k \max\{2,d\}16^k \text{bit}(d).$$
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 \( s \):

\[
2^{2^\max\{2, d\}^4 k} + s^k \quad \max\{2, d\}^{16^k \text{bit}(d)}.
\]
$P \geq 0$ in $\mathbb{R}^k \iff P(x) < 0$ no solution

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

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

$\quad > 0 \quad \geq 0$

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

Lombardi, Perrucci, Roy

An elementary recursive bound for Positivstellensatz and Hilbert 17th problem
Positivstellensatz implies Hilbert 17th problem

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

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

\[ P^{2e} + \sum_i Q_i^2 - (\sum_j R_j^2)P = 0 \]

\[ > 0 \iff \geq 0 \]

\[ \Rightarrow P = \frac{P^{2e} + \sum_i Q_i^2}{\sum_j R_j^2} = \frac{(P^{2e} + \sum_i Q_i^2)(\sum_j R_j^2)}{(\sum_j R_j^2)^2}. \]
Positivstellensatz implies Hilbert 17th problem

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

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

\[ P^{2e} + \sum_i Q_i^2 - (\sum_j R_j^2)P = 0 \]

\[ \iff P = \frac{P^{2e} + \sum_i Q_i^2}{\sum_j R_j^2} = \frac{(P^{2e} + \sum_i Q_i^2)(\sum_j R_j^2)}{(\sum_j R_j^2)^2}. \]
Positivstellensatz implies Hilbert 17th problem

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

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

\[ P^{2e} + \sum_i Q_i^2 - (\sum_j R_j^2)P = 0 \]

\[ \iff \frac{P^{2e} + \sum_i Q_i^2}{\sum_j R_j^2} = \frac{(P^{2e} + \sum_i Q_i^2)(\sum_j R_j^2)}{(\sum_j R_j^2)^2}. \]
Positivstellensatz implies Hilbert 17th problem

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

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

\[ P^{2e} + \sum_i Q_i^2 - (\sum_j R_j^2)P = 0 \]

\[ \iff \begin{cases} > 0 \\ \geq 0 \end{cases} \]

\[ \implies P = \frac{P^{2e} + \sum_i Q_i^2}{\sum_j R_j^2} = \frac{(P^{2e} + \sum_i Q_i^2)(\sum_j R_j^2)}{(\sum_j R_j^2)^2}. \]
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 17th problem as a special case.
- Uses notions introduced in Lombardi ’90.
- Key concept: weak inference.
Weak inferences: case by case reasoning

\[ A \neq 0 \implies A < 0 \lor A > 0 \]

Let \( \mathcal{H} \) be any system of sign conditions.

\[
\begin{align*}
\downarrow \mathcal{H}, \quad A < 0 \downarrow & \quad \implies \begin{cases} 
\mathcal{H}(x) \\
A(x) < 0
\end{cases} \quad \text{no solution} \\
\downarrow \mathcal{H}, \quad A > 0 \downarrow & \quad \implies \begin{cases} 
\mathcal{H}(x) \\
A(x) > 0
\end{cases} \quad \text{no solution} \\
\downarrow \downarrow & \quad \implies \begin{cases} 
\mathcal{H}(x) \\
A(x) \neq 0
\end{cases} \quad \text{no solution}
\end{align*}
\]

\[ A \neq 0 \vdash A < 0 \lor A > 0 \]

From right to left.
Weak inferences: case by case reasoning

\[ A \neq 0 \quad \implies \quad A < 0 \quad \lor \quad A > 0 \]

Let \( \mathcal{H} \) be any system of sign conditions.

\[ \downarrow \mathcal{H}, \quad A < 0 \quad \downarrow \quad \implies \quad \left\{ \begin{array}{c} \mathcal{H}(x) \\ A(x) < 0 \end{array} \right\} \quad \text{no solution} \]

\[ \downarrow \mathcal{H}, \quad A > 0 \quad \downarrow \quad \implies \quad \left\{ \begin{array}{c} \mathcal{H}(x) \\ A(x) > 0 \end{array} \right\} \quad \text{no solution} \]

\[ \downarrow \mathcal{H}, \quad A \neq 0 \quad \downarrow \quad \implies \quad \left\{ \begin{array}{c} \mathcal{H}(x) \\ A(x) \neq 0 \end{array} \right\} \quad \text{no solution} \]

\[ A \neq 0 \quad \vdash \quad A < 0 \quad \lor \quad A > 0 \]

From right to left.

Lombardi, Perrucci, Roy  
An elementary recursive bound for Positivstellensatz and Hilbert 17th problem
Weak inferences: case by case reasoning

\[ A \neq 0 \implies A < 0 \lor A > 0 \]

Let \( \mathcal{H} \) be any system of sign conditions.

\[
\begin{align*}
\downarrow \mathcal{H}, \quad A < 0 & \quad \implies \quad \begin{cases} \mathcal{H}(x) \\ A(x) < 0 \end{cases} \quad \text{no solution} \\
\downarrow \mathcal{H}, \quad A > 0 & \quad \implies \quad \begin{cases} \mathcal{H}(x) \\ A(x) > 0 \end{cases} \quad \text{no solution} \\
\downarrow \mathcal{H}, \quad A \neq 0 & \quad \implies \quad \begin{cases} \mathcal{H}(x) \\ A(x) \neq 0 \end{cases} \quad \text{no solution}
\end{align*}
\]

\[ A \neq 0 \quad \vdash \quad A < 0 \lor A > 0 \]

From right to left.
Weak inferences: case by case reasoning

\[ A \neq 0 \quad \implies \quad A < 0 \lor A > 0 \]

Let \( \mathcal{H} \) be any system of sign conditions.

\[
\begin{align*}
\downarrow \mathcal{H}, \quad A < 0 & \quad \implies \quad \left\{ \begin{array}{l}
\mathcal{H}(x) \\
A(x)
\end{array} \right\} < 0 \quad \text{no solution}
\
\downarrow \mathcal{H}, \quad A > 0 & \quad \implies \quad \left\{ \begin{array}{l}
\mathcal{H}(x) \\
A(x)
\end{array} \right\} > 0 \quad \text{no solution}
\
\downarrow \mathcal{H}, \quad A \neq 0 & \quad \leftrightarrow \quad \left\{ \begin{array}{l}
\mathcal{H}(x) \\
A(x)
\end{array} \right\} \neq 0 \quad \text{no solution}
\end{align*}
\]

\[ A \neq 0 \quad \vdash \quad A < 0 \lor A > 0 \]

From right to left.

Lombardi, Perrucci, Roy

An elementary recursive bound for Positivstellensatz and Hilbert 17th problem
\( A \not= 0 \vdash A < 0 \lor A > 0 \)

\[
\begin{align*}
\downarrow \mathcal{H}, \ A < 0 \downarrow & \quad \leftarrow \text{degree } \delta_1 \\
A^{2e_1} S_1 + N_1 - N'_1 A + Z_1 &= 0 \\
A^{2e_1} S_1 + N_1 + Z_1 &= N'_1 A \\
\downarrow \mathcal{H}, \ A > 0 \downarrow & \quad \leftarrow \text{degree } \delta_2 \\
A^{2e_2} S_2 + N_2 + N'_2 A + Z_2 &= 0 \\
A^{2e_2} S_2 + N_2 + Z_2 &= -N'_2 A \\
\downarrow \mathcal{H}, \ A \not= 0 \downarrow & \quad \leftarrow \text{degree } \delta_1 + \delta_2 \\
A^{2e_1+2e_2} S_1 S_2 + N_3 + Z_3 &= -N'_1 N'_2 A^2 \\
A^{2e_1+2e_2} S_1 S_2 + N_1' N_2' A^2 + N_3 + Z_3 &= 0 \\
\end{align*}
\]
\( A \neq 0 \quad \vdash \quad A < 0 \quad \lor \quad A > 0 \)

\[ \downarrow \mathcal{H}, \ A < 0 \quad \downarrow \quad \leftarrow \text{degree } \delta_1 \]

\[
A^{2e_1} S_1 + N_1 - N'_1 A + Z_1 = 0
\]

\[
A^{2e_1} S_1 + N_1 + Z_1 = N'_1 A
\]

\[ \downarrow \mathcal{H}, \ A > 0 \quad \downarrow \quad \leftarrow \text{degree } \delta_2 \]

\[
A^{2e_2} S_2 + N_2 + N'_2 A + Z_2 = 0
\]

\[
A^{2e_2} S_2 + N_2 + Z_2 = -N'_2 A
\]

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

\[
A^{2e_1+2e_2} S_1 S_2 + N_3 + Z_3 = -N'_1 N'_2 A^2
\]

\[
A^{2e_1+2e_2} S_1 S_2 + N'_1 N'_2 A^2 + N_3 + Z_3 = 0
\]
$A \neq 0 \quad \vdash \quad A < 0 \quad \lor \quad A > 0$

$\downarrow \mathcal{H}, \quad A < 0 \quad \downarrow \quad \leftarrow \text{degree } \delta_1$

\[
A^{2e_1} S_1 + N_1 - N'_1 A + Z_1 = 0
\]

$\downarrow \mathcal{H}, \quad A > 0 \quad \downarrow \quad \leftarrow \text{degree } \delta_2$

\[
A^{2e_2} S_2 + N_2 + N'_2 A + Z_2 = 0
\]

$A^{2e_1} S_1 + N_1 + Z_1 = N'_1 A$

\[
A^{2e_2} S_2 + N_2 + Z_2 = -N'_2 A
\]

\[
A^{2e_1+2e_2} S_1 S_2 + N_3 + Z_3 = -N'_1 N'_2 A^2
\]

$A^{2e_1+2e_2} S_1 S_2 + N'_1 N'_2 A^2 + N_3 + Z_3 = 0$

$\downarrow \mathcal{H}, \quad A \neq 0 \quad \downarrow \quad \leftarrow \text{degree } \delta_1 + \delta_2$
\[ A \neq 0 \quad \vdash \quad A < 0 \quad \lor \quad A > 0 \]

\[
\downarrow \mathcal{H}, \quad A < 0 \quad \downarrow \quad \leftarrow \text{degree } \delta_1
\]

\[
A^{2e_1} S_1 + N_1 - N'_1 A + Z_1 = 0
\]

\[
A^{2e_1} S_1 + N_1 + Z_1 = N'_1 A
\]

\[
\downarrow \quad \Downarrow
\]

\[
A^{2e_1 + 2e_2} S_1 S_2 + N_3 + Z_3 = -N'_1 N'_2 A^2
\]

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

\[
A^{2e_2} S_2 + N_2 + N'_2 A + Z_2 = 0
\]

\[
A^{2e_2} S_2 + N_2 + Z_2 = -N'_2 A
\]
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)
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)
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 $\mathcal{P} \subset K[x_1, \ldots, x_k]$ fixed by list of non empty sign conditions for $\text{Proj}(\mathcal{P}) \subset K[x_1, \ldots, x_{k-1}]$: 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 $\text{Proj}(\mathcal{P}) \subset \mathbf{K}[x_1, \ldots, x_{k-1}]$: variant of cylindrical decomposition (which does not use the notion of connected component)
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

$$\vdash P \geq 0.$$  

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 $\mathcal{H}$ 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 initial incompatibility of $P \geq 0, P \neq 0, -P \geq 0$!

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

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

which is the final incompatibility we are looking for!!

We expressed $P$ as a sum of squares of rational functions!!

Lombardi, Perrucci, Roy

An elementary recursive bound for Positivstellensatz and Hilbert 17th problem
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?
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?
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 emptiness 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 emptiness 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 emptiness for the reals (more sophisticated than cylindrical decomposition): single exponential: Grigori’ev-Vorobjov results [GV1].
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 emptiness 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 emptiness for the reals (more sophisticated than cylindrical decomposition): single exponential: Grigori’ev-Vorobjov results [GV1].
• 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


(and all other references there)