Effective Pourchet's Theorem

Carlos D'Andrea

Nice 24/06/26

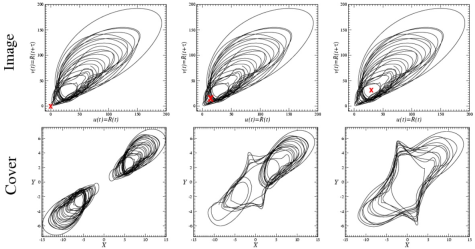
Happy Birthday André!

Happy Birthday André!

Happy Birthday André!

El roce hace el cariño

El roce hace el cariño



(a) $u_0 = 0$ (b) $u_0 = 15$ (c) $u_0 = 30$

Singularities of families of algebraic plane curves with “controlled” coefficients tend to the equidistribution
[Diaconis-Galligó]

JOURNAL ARTICLE

QUANTITATIVE EQUIDISTRIBUTION FOR THE SOLUTIONS OF SYSTEMS OF SPARSE POLYNOMIAL EQUATIONS

Carlos D'Andrea, André Galligo and Martín Sombra

American Journal of Mathematics
Vol. 136, No. 6 (December 2014), pp. 1543-1579 (37 pages)
Published By: The Johns Hopkins University

JOURNAL ARTICLE

QUANTITATIVE EQUIDISTRIBUTION FOR THE SOLUTIONS OF SYSTEMS OF SPARSE POLYNOMIAL EQUATIONS

Carlos D'Andrea, André Galligo and Martín Sombra

American Journal of Mathematics
Vol. 136, No. 6 (December 2014), pp. 1543-1579 (37 pages)
Published By: The Johns Hopkins University

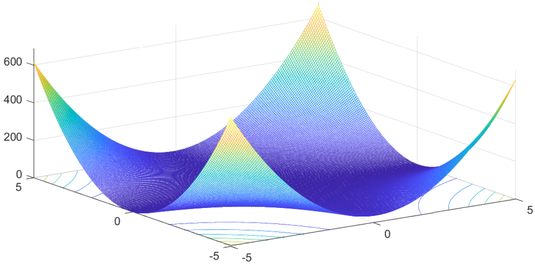
msp
ALGEBRA AND NUMBER THEORY 11:7 (2017)
dx.doi.org/10.2140/ant.2017.11.1627

Quantitative equidistribution of Galois orbits of small points in the N-dimensional torus

Carlos D'Andrea, Marta Narváez-Clauss and Martín Sombra

We present a quantitative version of Bilu's theorem on the limit distribution of Galois orbits of sequences of points of small height in the N-dimensional algebraic torus. Our result gives, for a given point, an explicit bound for the discrepancy between its Galois orbit and the uniform distribution on the compact subtorus, in terms of the height and the generalized degree of the point.

Today we have...



Yet another story involving polynomials

Joint work with

- Ana Belén de Felipe – UPC
- Eulàlia Montoro – UB
- Joel Hurtado – UPC
- Teresa Cortadellas Benítez – URL

`arXiv:2511.11783`

“The” general question

“The” general question

Given a polynomial

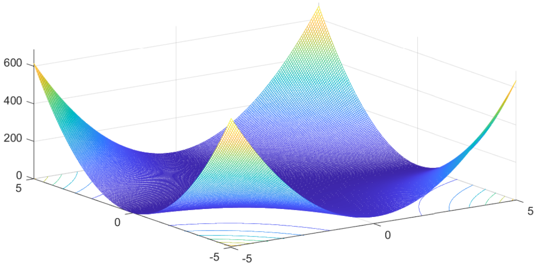
$$f(x_1, \ldots, x_n) \in \mathbb{R}/\mathbb{Q}[x_1, \ldots, x_n]$$

"The" general question

Given a polynomial

$$f(x_1,\ldots,x_n)\in\mathbb{R}/\mathbb{Q}[x_1,\ldots,x_n]$$

How can we certify if $f\geq 0$?



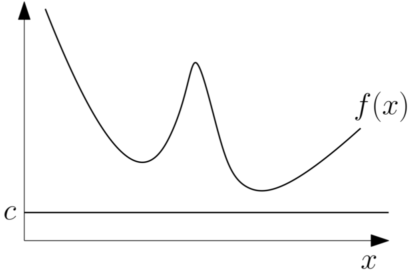
In one variable...

In one variable...

$$f(t) \geq 0 \ \forall t \in \mathbb{R} \iff$$

In one variable...

$$f(t) \geq 0 \; \forall t \in \mathbb{R} \iff$$
$$f(x) = f_1(x)^2 + f_2(x)^2$$
$$f_1(x),\ f_2(x) \in \mathbb{R}[x]$$



Rational coefficients?

Rational coefficients?

$$f(t) \geq 0 \ \forall t \in \mathbb{R} \iff$$

Rational coefficients?

$$f(t) \geq 0 \ \forall t \in \mathbb{R} \iff$$

$$f(x) =$$

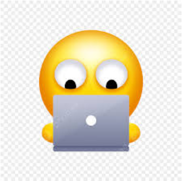
$$f_1(x)^2 + f_2(x)^2 + f_3(x)^2 + f_4(x)^2 + f_5(x)^2$$

Pourchet – 1971

Is 5 optimal?

Is 5 optimal?

$$x^2 + 7 = x^2 + 2^2 + 1^2 + 1^2 + 1^2$$



Yves Pourchet

Yves Pourchet

AMERICAN MATHEMATICAL SOCIETY
MATHSCINET
MATHEMATICAL REVIEWS

Matches: 4

Batch Download: Reviews (HTML) | Retrieve Marked | Retrieve First 50 | Mark All | Unmark All

Publications results for "Author=(pourchet)"

Sort by: Newest

Search within results

Item Type
- Reviewed (4)

Authors
- Pourchet, Yves (3)
- Pourchet, Y. (1)

Primary Classification
- Field theory and polynomials (3)
- Number Theory (1)

MR0541979 Reviewed Pourchet, Yves Solution du problème arithmétique du quotient de Hadamard de deux fractions rationnelles. (French) *C. R. Acad. Sci. Paris Sér. A-B* 288 (1979), no. 23, A1055–A1057. 12A10
Review PDF | Clipboard | Journal | Article | 7 Citations

MR0424774 Reviewed Pourchet, Yves Sur l'homogénéité différentielle et la dénomination. (French) *C. R. Acad. Sci. Paris Sér. A-B* 280 (1975), Ai, A697–A700. 12H05
Review PDF | Clipboard | Journal | Article

MR0371871 Reviewed Pourchet, Yves Polynomes différentiels homogènes et dénomination d'un polynome différentiel. (French) *C. R. Acad. Sci. Paris Sér. A* 279 (1974), 209–212. (Reviewer: Jerald Kovacic) 12H05
Review PDF | Clipboard | Journal | Article

MR0289442 Reviewed Pourchet, Y. Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques. (French) *Acta Arith.* 19 (1971), 89–104. (Reviewer: O. H. Körner) 10.46 (12.00)
Review PDF | Clipboard | Journal | Article | 28 Citations

Yves Pourchet

American Mathematical Society
MathSciNet
Mathematical Reviews

Matches: 4

Batch Download: Reviews (HTML) | Retrieve Marked | Retrieve First 50 | Mark All | Unmark All

Publications results for "Author=(pourchet)"

Sort by: Newest

Search within results

Item Type
- Reviewed (4)

Authors
- Pourchet, Yves (3)
- Pourchet, Y. (1)

Primary Classification
- Field theory and polynomials (3)
- Number Theory (1)

MR0541979 Reviewed Pourchet, Yves Solution du problème arithmétique du quotient de Hadamard de deux fractions rationnelles. (French) *C. R. Acad. Sci. Paris Sér. A-B* 288 (1979), no. 23, A1055–A1057. 12A10
Review PDF | Clipboard | Journal | Article | 7 Citations

MR0424774 Reviewed Pourchet, Yves Sur l'homogénéité différentielle et la dénomination. (French) *C. R. Acad. Sci. Paris Sér. A-B* 280 (1975), Ai, A697–A700. 12H05
Review PDF | Clipboard | Journal | Article

MR0371871 Reviewed Pourchet, Yves Polynomes différentiels homogènes et dénomination d'un polynome différentiel. (French) *C. R. Acad. Sci. Paris Sér. A* 279 (1974), 209–212. (Reviewer: Jerald Kovacic) 12H05
Review PDF | Clipboard | Journal | Article

MR0289442 Reviewed Pourchet, Y. Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques. (French) *Acta Arith.* 19 (1971), 89–104. (Reviewer: O. H. Körner) 10.46 (12.00)
Review PDF | Clipboard | Journal | Article | 28 Citations

ACTA ARITHMETICA
XIX (1971)

Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques

par

Y. Pourchet (Paris)

Dans [7] Landau démontre que tout polynôme défini positif à une indéterminée sur le corps des nombres rationnels est somme des carrés de huit polynômes sur ce corps. Je montre dans ce travail que ce nombre peut être ramené à cinq (corollaire 4 du théorème 2), sans d'ailleurs pouvoir être abaissé davantage (proposition 10).

This talk – Effective Pourchet

This talk – Effective Pourchet

- **Input:**
  $f(x) \in \mathbb{Q}[x],\ f(t) \geq 0 \forall t \in \mathbb{R}$

This talk – Effective Pourchet

- **Input:**
  $f(x) \in \mathbb{Q}[x], \; f(t) \geq 0 \forall t \in \mathbb{R}$
- **Output:** $f_1(x), \ldots, f_5(x) \in \mathbb{Q}[x]$,
  $f(x) = f_1(x)^2 + \ldots + f_5(x)^2$

Pourchet's original approach

Pourchet's original approach

$$f(x) = f_1(x)^2 + \ldots + f_5(x)^2 \iff$$

Pourchet's original approach

$$f(x) = f_1(x)^2 + \ldots + f_5(x)^2 \iff$$
$$f(x) = f_{1p}(x)^2 + \ldots + f_{5p}(x)^2$$
$$\forall p \in \{2, 3, 5, \ldots,\} \cup \{\infty\}$$

Pourchet's original approach

$$f(x) = f_1(x)^2 + \ldots + f_5(x)^2 \iff f(x) = f_{1p}(x)^2 + \ldots + f_{5p}(x)^2 \quad \forall p \in \{2, 3, 5, \ldots, \} \cup \{\infty\}$$

- Local-Global Principle (Hasse-Minkowski)

Pourchet's original approach

$$f(x) = f_1(x)^2 + \ldots + f_5(x)^2 \iff$$
$$f(x) = f_{1p}(x)^2 + \ldots + f_{5p}(x)^2$$
$$\forall p \in \{2, 3, 5, \ldots, \} \cup \{\infty\}$$

- Local-Global Principle (Hasse-Minkowski)
- Non algorithmic

An algorithm?

An algorithm?

$$p = \infty$$

Easy on $\mathbb{R}$

$f(t) \geq 0 \iff y_1^2 + y_2^2 = f(x)$ has a solution in $\mathbb{R}[x]$

An algorithm?

$$p = \infty$$

Easy on $\mathbb{R}$

$f(t) \geq 0 \iff y_1^2 + y_2^2 = f(x)$ has a solution in $\mathbb{R}[x]$

Proof:

$x^2 + ax + b = (x - c)^2 + d^2$ if $a^2 - 4b < 0$

An algorithm?

$$p = \infty$$

Easy on $\mathbb{R}$

$f(t) \geq 0 \iff y_1^2 + y_2^2 = f(x)$ has a solution in $\mathbb{R}[x]$

Proof:

$x^2 + ax + b = (x - c)^2 + d^2$ if $a^2 - 4b < 0$

$$(x - a)^{2k} = ((x - a)^k)^2 + 0^2$$

An algorithm?

$$p = \infty$$

Easy on $\mathbb{R}$

$f(t) \geq 0 \iff y_1^2 + y_2^2 = f(x)$ has a solution in $\mathbb{R}[x]$

Proof:

$$x^2 + ax + b = (x - c)^2 + d^2 \text{ if } a^2 - 4b < 0$$

$$(x - a)^{2k} = ((x - a)^k)^2 + 0^2$$

$$\boxed{(u^2 + v^2) \cdot (w^2 + z^2) = \alpha^2 + \beta^2}$$

Almost all p

Almost all p

Any $f(x) \in \mathbb{Q}_p[x]$ is a sum of **at most four** squares if $p \notin \{2, \infty\}$

Almost all p

Any $f(x) \in \mathbb{Q}_p[x]$ is a sum of **at most four** squares if $p \notin \{2, \infty\}$

Five squares are enough if $p = 2$

Sums of 4 squares are computable

Sums of 4 squares are computable

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)$$
$$= (z_1^2 + z_2^2 + z_3^2 + z_4^2)$$

Sums of 4 squares are computable

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = (z_1^2+z_2^2+z_3^2+z_4^2)$$

Theorem (Pourchet, 71)

$f(x) = f_1^2+f_2^2+f_3^2+f_4^2$ in $K[x] \iff$

- $\operatorname{lc}(f) = a_1^2+a_2^2+a_3^2+a_4^2$ in K, and

Sums of 4 squares are computable

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = (z_1^2+z_2^2+z_3^2+z_4^2)$$

Theorem (Pourchet, 71)

$f(x)=f_1^2+f_2^2+f_3^2+f_4^2$ in $K[x]$ $\iff$

- $\mathrm{lc}(f)=a_1^2+a_2^2+a_3^2+a_4^2$ in K, and
- $\forall p(x)$ prime divisor of $f(x)$ with $v_p(f)$ odd, there is a non trivial solution of $x_1^2+x_2^2+x_3^2+x_4^2=0$ in $K[x]/(p(x))$

Useful criteria

Useful criteria

$$x^2 + 7 = (x - \alpha) \cdot (x + \alpha) \text{ en } \mathbb{Q}_2[x]$$

Useful criteria

$$x^2 + 7 = (x - \alpha) \cdot (x + \alpha) \text{ en } \mathbb{Q}_2[x]$$
$$\Longrightarrow \notin \sum\nolimits_4 \mathbb{Q}[x]^2$$

Useful criteria

$$x^2 + 7 = (x - \alpha) \cdot (x + \alpha) \text{ en } \mathbb{Q}_2[x]$$
$$\Longrightarrow \notin \sum_4 \mathbb{Q}[x]^2$$

$$u \in \mathbb{Q}_2^2 \iff$$
$$u = 2^{2a}(8b + 1),\ a \in \mathbb{Z},\ b \in \mathbb{Z}_2$$

Algorithm

Pourchet's theorem in action: decomposing univariate nonnegative polynomials as sums of five squares

Victor Magron
CNRS LAAS & Institut de Mathématiques de Toulouse
Toulouse, France
victor.magron@laas.fr

Przemysław Koprowski
University of Silesia in Katowice, Institute of Mathematics
Katowice, Poland
przemyslaw.koprowski@us.edu.pl

Tristan Vaccon
Université de Limoges; CNRS, XLIM UMR 7252
Limoges, France
tristan.vaccon@unilim.fr

ISSAC 2023

Sum of two squares

Algorithm 1 Computing a decomposition of a polynomial as a sum of two squares

Input: A polynomial $f \in \mathbb{Q}[x]$, which is a priori known to be a sum of two squares in $\mathbb{Q}[x]$.

Output: Polynomials $a, b \in \mathbb{Q}[x]$ such that $a^2 + b^2 = f$.

1: Construct the quadratic field extension $\mathbb{Q}(i)/\mathbb{Q}$.

2: Solve the norm equation

$$\mathrm{lc}(f) = N_{\mathbb{Q}(i)/\mathbb{Q}}(x)$$

and denote a solution by $a + bi \in \mathbb{Q}(i)$.

3: Factor f into a product of monic irreducible polynomials

$$f = \mathrm{lc}(f) \cdot p_1^{e_1} \cdots p_k^{e_k}.$$

4: **for** every factor p_j, such that the corresponding exponent e_j is odd **do**

5: Factor p_j over $\mathbb{Q}(i)$ into a product $p_j = g_j \cdot h_j$ with $g_j, h_j \in \mathbb{Q}(i)[x]$.

6: Set

$$a_j := \frac{1}{2} \cdot (g_j + h_j), \qquad b_j := \frac{1}{2i} \cdot (g_j - h_j).$$

7: Update a and b setting:

$$a := aa_j + bb_j \qquad \text{and} \qquad b := ab_j - ba_j.$$

8: Update a and b setting:

$$a := a \cdot \prod_{j \le k} p_j^{2\lfloor e_j/2 \rfloor} \qquad \text{and} \qquad b := b \cdot \prod_{j \le k} p_j^{2\lfloor e_j/2 \rfloor}.$$

9: **return** a, b.

Sum of three or four squares

Algorithm 3 Initial solution: modular sum of squares

Input: An irreducible polynomial $f \in \mathbb{Q}[x]$, which is a priori known to be a sum of 3 or 4 squares.

Output: Polynomials h and $g_1, \dots, g_4$ in $\mathbb{Q}[x]$, such that $\deg h \leq \deg f - 2$ and $fh = g_1^2 + \cdots + g_4^2$.

1: Construct the number fields:

$$K := \mathbb{Q}[x]/(f) \qquad \text{and} \qquad L := K(i).$$

2: Solve the norm equation

$$-1 = N_{L/K}(x)$$

and denote the solution by $\xi = \overline{g}_1 + \overline{g}_2 i$, where $g_1, g_2 \in \mathbb{Q}[x]$ are polynomials of degree strictly less than $\deg f$ and $\overline{g}_j$ denotes the image of g_j under the canonical epimorphism $\mathbb{Q}[x] \twoheadrightarrow K$.

3: Set $g_3 := 1$, $g_4 := 0$ and let $h := {(g_1^2 + \cdots + g_4^2)}/{f}$.

4: **return** h, g_1, g_2, g_3, g_4.

How to use this for 5 polynomials?

How to use this for 5 polynomials?

$$f(t) > 0$$

How to use this for 5 polynomials?

$$f(t) > 0 \ldots f(t) - \left(\frac{1}{2^\ell}\right)^2 > 0$$

if $\ell \gg 0$

How to use this for 5 polynomials?

$$f(t) > 0 \ldots f(t) - \left(\frac{1}{2^\ell}\right)^2 > 0$$

if $\ell \gg 0$

$$f(x) - \left(\frac{1}{2^\ell}\right)^2 = f_1^2 + f_2^2 + f_3^2 + f_4^2??$$

Algorithm 6

Algorithm 6

Algorithm 6 Reduction to a sum of 4 squares: odd valuation case

Input: A positive square-free polynomial $f = c_0 + c_1x + \cdots + c_dx^d \in \mathbb{Q}[x]$. The 2-adic valuations of the coefficients of f are $k_j := \operatorname{ord}_2 c_j$ for $0 \leq j \leq d$. Ensure k_d is odd. It is assumed that f is not a sum of 4 squares.

Output: A polynomial $h \in \mathbb{Q}[x]$ such that $f - h^2$ is a sum of 4 (or fewer) squares.

1: Find a positive number ε such that

$$\varepsilon < \inf\{f(x) \mid x \in \mathbb{R}\}.$$

2: Set $l_1 := \lceil -1/2 \cdot \lg \varepsilon \rceil$.

3: Set $l_2 := \lceil -k_0/2 \rceil + 1$.

4: Set

$$l_3 := \left\lceil \max\left\{ \frac{jk_d - dk_j}{2d - 2j} \mid 0 < j < d \right\} \right\rceil.$$

5: Initialize $l := \max\{l_1, l_2, l_3\}$.

6: **while** $\gcd(d, 2l + k_d) \neq 1$ **do**

7: $\quad l := l + 1$.

8: **return** $h := 2^{-l}$.

Sum of 6 squares

Algorithm 8 Decomposition of a nonnegative univariate rational polynomial into a sum of 6 squares

Input: A nonnegative polynomial $f \in \mathbb{Q}[x]$.
Output: Polynomials $f_1, \ldots, f_6 \in \mathbb{Q}[x]$ such that $f_1^2 + \cdots + f_6^2 = f$.

```
if f is a square then
    return f_1 := √f, f_2 := ··· f_6 := 0.
if f is a sum of 2 squares {Use Observation 8 to check it} then
    Execute Algorithm 1 to obtain f_1, f_2 ∈ Q[x] such that f_1^2 + f_2^2 = f.
    return f_1, f_2 and f_3 := ··· f_6 := 0.
if f is a sum of 4 squares {Use [36, Theorem 17.2] to check it} then
    Execute Algorithm 5, to obtain f_1, ..., f_4 ∈ Q[x] such that f_1^2 + ··· + f_4^2 = f.
    return f_1, ..., f_4 and f_5 := f_6 := 0
Compute the square-free decomposition of f = g · h^2, where g, h ∈ Q[x] and g is square-free.
Execute Algorithm 7 with g as an input to obtain g_1, g_2 ∈ Q[x] such that g − g_1^2 − g_2^2 is a sum of 4 squares in Q[x].
Execute Algorithm 5 to decompose g − g_1^2 − g_2^2 into a sum of 4 squares in Q[x]. Denote the output by g_3, ..., g_6.
return f_1 := g_1 h, ..., f_6 := g_6 h.
```

Conjecture

Algorithm 9 Reduction to a sum of 4 squares

Input: A positive square-free polynomial $f = c_0 + c_1 x + \cdots + c_d x^d \in \mathbb{Q}[x]$.

Output: A polynomial $h \in \mathbb{Q}[x]$ such that $f - h^2$ is a sum of 4 (or fewer) squares.

if f is a sum of 4 squares **then**
  return $h := 0$.
Set $f_* := c_d + c_{d-1}x + \cdots + c_0 x^d$.
Find a positive number ε such that

$$\varepsilon < \inf\{f(x) \mid x \in \mathbb{R}\} \quad \text{and} \quad \varepsilon < \inf\{f_*(x) \mid x \in \mathbb{R}\}.$$

Initialize $l := \lceil -{}^1/_2 \cdot \lg \varepsilon \rceil$.
while True **do**
  if $f - 2^{-2l}$ is irreducible in $\mathbb{Q}_2[x]$ **then**
    return $h := 2^{-l}$.
  if $f - 2^{-2l}x^d$ is irreducible in $\mathbb{Q}_2[x]$ **then**
    return $h := 2^{-l}x^{d/2}$.
  $l := l + 1$.

Our results

(C**D**DHM)

Our results

(C**D**DHM)

- The conjecture works if $\deg(f(x)) = 4k$

Our results

(C**D**DHM)

- The conjecture works if $\deg(f(x)) = 4k$
- It does not work for this family:

$$\boxed{f_{k,N}(x) = \frac{4x^{2(2k+1)} + x^{2k+1} + 4}{N^2}}$$

$k = 0, \ldots,$ $N \in \mathbb{N}$ odd, $N > 64$

Extension of the method

(C**D**DHM)

Extension of the method

(C**D**DHM)

Theorem

If $f(x) \in \mathbb{Q}[x]$ of degree $d = 2(2k+1),\ k \in \mathbb{N},\ \ell \in \mathbb{N}$ such that $f(t) - \frac{1}{2^{2\ell}}(t^2+t+1)^{2k}t^2 > 0\ \forall t \in \mathbb{R}$

Extension of the method

(C**D**DHM)

Theorem

If $f(x) \in \mathbb{Q}[x]$ of degree $d = 2(2k+1)$, $k \in \mathbb{N}$, $\ell \in \mathbb{N}$ such that $f(t) - \frac{1}{2^{2\ell}}(t^2+t+1)^{2k}t^2 > 0 \ \forall t \in \mathbb{R}$ then $f(x) - \frac{1}{2^{2\ell}}(x^2+x+1)^{2k}x^2 \in \sum_4 \mathbb{Q}[x]^2$ if $f(0) \notin \mathbb{Q}_2^2$

Missing case

Missing case

What if $f(0) \in \mathbb{Q}_2^2$?

Missing case

What if $f(0) \in \mathbb{Q}_2^2$?

$f(\alpha) \in \mathbb{Q}_2^2 \; \forall \alpha \in \mathbb{Q}_2 => f \in \mathbb{Q}[x]^2$?

Missing case

What if $f(0) \in \mathbb{Q}_2^2$?

$$f(\alpha) \in \mathbb{Q}_2^2 \ \forall \alpha \in \mathbb{Q}_2 => f \in \mathbb{Q}[x]^2?$$

$$\boxed{4x^6 + 4x^3 + 9 = (1 + 2x^3)^2 + 8}$$

Missing case

What if $f(0) \in \mathbb{Q}_2^2$?

$$f(\alpha) \in \mathbb{Q}_2^2 \ \forall \alpha \in \mathbb{Q}_2 \implies f \in \mathbb{Q}[x]^2?$$

$$\boxed{4x^6 + 4x^3 + 9 = (1 + 2x^3)^2 + 8}$$

Conjecture

If $f(x) \in \mathbb{Q}_2[x]$ is square-free and $f(\mathbb{Q}_2^2) \subset \mathbb{Q}_2^2$ then it is a product of irreducibles of even degree in $\mathbb{Q}_2[x]$

In general...

In general...

You do not need 2 or 5 polinomials to certify nonegativity:

$$f \geq 0 \iff f = \sum_{i=1}^{N} f_i^2$$

In general...

You do not need 2 or 5 polinomials to certify nonegativity:

$$f \geq 0 \iff f = \sum_{i=1}^{N} f_i^2$$

- Semidefinite optimization ($\mathbb{R}[x]$)

In general...

You do not need 2 or 5 polinomials to certify nonegativity:

$$f \geq 0 \iff f = \sum_{i=1}^{N} f_i^2$$

- Semidefinite optimization ($\mathbb{R}[x]$)
- Over $\mathbb{Q}[x]$
  (Baldo-Krick-Mourrain 2025)

It is harder in more variables

It is harder in more variables

Positivity vs sums of squares

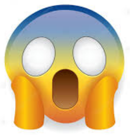
$$f(x_1, x_2) = 1 + x_1^2 x_2^2 (x_1^2 + x_2^2 - 3) \geq 0$$

It is harder in more variables

Positivity vs sums of squares

$$f(x_1, x_2) = 1 + x_1^2 x_2^2 (x_1^2 + x_2^2 - 3) \geq 0$$

but this polynomial is not a sum of any number of squares

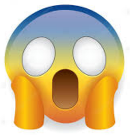


It is harder in more variables

Positivity vs sums of squares

$$f(x_1, x_2) = 1 + x_1^2 x_2^2 (x_1^2 + x_2^2 - 3) \geq 0$$

but this polynomial is not a sum of any number of squares



Hilbert's 17 Problem

$\mathbb{R}$ vs $\mathbb{Q}$

$\mathbb{R}$ vs $\mathbb{Q}$

$$40x_0^4 + 8x_0^2x_1^2 + 32x_0^2x_1x_2 + 64x_0^2x_1x_3$$
$$+16x_0^2x_2^2 + 16x_0^2x_2x_3 + 32x_0^2x_3^2 + 2x_1^4$$
$$+8x_1^2x_2^2 + 8x_1^2x_2x_3 + 16x_1x_2x_3^2$$
$$+8x_2^2x_3^2 + 8x_3^4 = f_1^2 + f_2^2 + f_3^2 + f_4^2$$

$\mathbb{R}$ vs $\mathbb{Q}$

$$40x_0^4 + 8x_0^2x_1^2 + 32x_0^2x_1x_2 + 64x_0^2x_1x_3$$
$$+16x_0^2x_2^2 + 16x_0^2x_2x_3 + 32x_0^2x_3^2 + 2x_1^4$$
$$+8x_1^2x_2^2 + 8x_1^2x_2x_3 + 16x_1x_2x_3^2$$
$$+8x_2^2x_3^2 + 8x_3^4 = f_1^2 + f_2^2 + f_3^2 + f_4^2$$

over $\mathbb{R}$

$\mathbb{R}$ vs $\mathbb{Q}$

$$40x_0^4 + 8x_0^2x_1^2 + 32x_0^2x_1x_2 + 64x_0^2x_1x_3 + 16x_0^2x_2^2 + 16x_0^2x_2x_3 + 32x_0^2x_3^2 + 2x_1^4 + 8x_1^2x_2^2 + 8x_1^2x_2x_3 + 16x_1x_2x_3^2 + 8x_2^2x_3^2 + 8x_3^4 = f_1^2 + f_2^2 + f_3^2 + f_4^2$$

over $\mathbb{R}$ but cannot be written as any sum of squares over $\mathbb{Q}$

References

References

- Koprowski, P.; Magron, V.; Vaccon, T. **Pourchet's theorem in action: decomposing univariate nonnegative polynomials as sums of five squares.** Proceedings of ISSAC 2023
- Pourchet, Y. **Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques.** Acta Arith. 19 (1971)

Thanks!

arXiv:2511.11783