Effective Pourchet's Theorem

Carlos D'Andrea

Jaca, May 13th 2025

UNIVERSITAT DE BARCELONA

Barcelona's CA Seminar

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

“The” Question

“The” Question

Given a polynomial

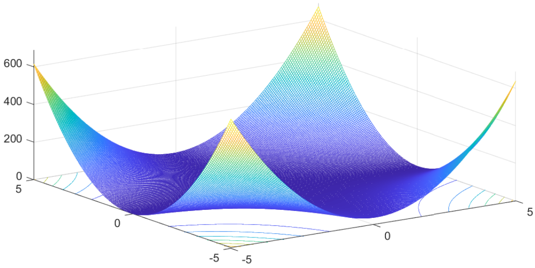
$$f(x_1, \ldots, x_n) \in \mathbb{R}/\mathbb{Q}[x_1, \ldots, x_n]$$

“The” Question

Given a polynomial

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

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



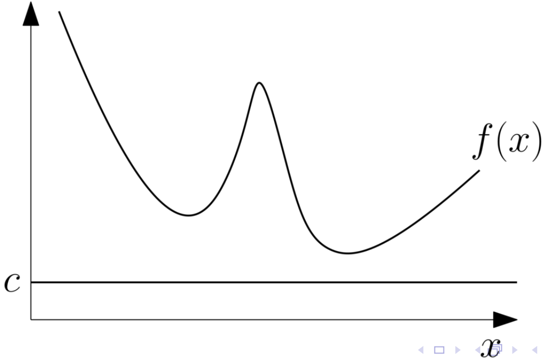
Univariate case

Univariate case

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

Univariate case

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



Univariate rational case?

Univariate rational case?

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

Univariate rational case?

$$f(x) \geq 0 \ \forall x \in \mathbb{R} \iff$$
$$f(x) =$$
$$f_1(x)^2 + f_2(x)^2 + f_3(x)^2 + f_4(x)^2 + f_5(x)^2$$

Pourchet – 1971

Five is sharp

Five is sharp

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

Effective Pourchet

Effective Pourchet

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

Effective Pourchet

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

Pourchet's original proof

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

Pourchet's original proof

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

Pourchet's original proof

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

- Local-global principle

Pourchet's original proof

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

- Local-global principle
- Highly non-algorithmic

Towards an algorithm...

Towards an algorithm...

$$p = \infty$$

Theorem (Easy)

$f(x) \geq 0 \iff f(x) = x_1^2 + x_2^2$ can be solved in $\mathbb{R}[x]$

Towards an algorithm...

$$p = \infty$$

Theorem (Easy)

$f(x) \geq 0 \iff f(x) = x_1^2 + x_2^2$ can be solved in $\mathbb{R}[x]$

Proof:

$$f(x) \geq 0 \iff f(x) = (a^2 + 0^2) \cdot \prod_{i=1}^{N}((x - a_i)^2 + 0^2) \cdot \prod_{j=1}^{M}((x - b_j)^2 + c_j)^2$$

Towards an algorithm...

$$p = \infty$$

Theorem (Easy)

$f(x) \geq 0 \iff f(x) = x_1^2 + x_2^2$ can be solved in $\mathbb{R}[x]$

Proof:

$$f(x) \geq 0 \iff f(x) =$$
$$(a^2 + 0^2) \cdot \prod_{i=1}^{N}((x - a_i)^2 + 0^2) \cdot \prod_{j=1}^{M}((x - b_j)^2 + c_j)^2$$
$$(u^2 + v^2) \cdot (w^2 + z^2) = \alpha^2 + \beta^2$$

Almost all p

Almost all p

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

Almost all p

Any $f(x) \in \mathbb{Q}_p[x]$ is a sum of up to four squares if $p \notin \{2, \infty\}$ five squares suffice if $p = 2$

Up to 4 squares can be computed

Up to 4 squares can be computed

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

Up to 4 squares can be computed

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

Theorem (Pourchet, 71)

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

- $\mathrm{lc}(f)$ is a so4s in K, and

Up to 4 squares can be computed

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

Theorem (Pourchet, 71)

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

- $\mathrm{lc}(f)$ is a so4s in K, and
- for all prime divisor $p(x)$ of $f(x)$ of odd multiplicity, there is a nontrivial solution of $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 0$ in $K[x]/(p(x))$

A criteria

A criteria

Theorem (Pourchet, 71)

Let $f \in \mathbb{Q}[x] \setminus \{0\}$. *TFAE:*

1. f *is a so4s in* $\mathbb{Q}[x]$

A criteria

Theorem (Pourchet, 71)

Let $f \in \mathbb{Q}[x] \setminus \{0\}$. *TFAE:*

1. f *is a so4s in* $\mathbb{Q}[x]$
2. $l(f) > 0$ *and for all irreducible* $p|f$ *of odd mult.* $St(\mathbb{Q}[x]/(p)) \leq 2$

A criteria

Theorem (Pourchet, 71)

Let $f \in \mathbb{Q}[x] \setminus \{0\}$. *TFAE:*

1. f *is a so*4*s in* $\mathbb{Q}[x]$
2. $l(f) > 0$ *and for all irreducible* $p|f$ *of odd mult.* $St(\mathbb{Q}[x]/(p)) \leq 2$
3. $f > 0$ *and in* $\mathbb{Q}_2[x]$ *every prime factor of odd mult.has even degree*

Useful

Useful

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

Useful

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

$\Longrightarrow$ it is not a so4s in $\mathbb{Q}[x]$

Useful

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

$$\Longrightarrow \text{ it is not a so4s in } \mathbb{Q}[x]$$

$$u \in \mathbb{Q}_2 \text{ is a square } \Longleftrightarrow$$

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

Algorithmic approach

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

Sums of 2 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 $a^2 + b^2 = f$.

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

Solve the norm equation

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

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

Factor f into a product of monic irreducible polynomials

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

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

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

  Set

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

  Update a and b setting:

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

Update a and b setting:

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

return a, b.

Sums of 3 or 4 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 $g_1, \ldots, g_4$ 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 do you tackle 5 polynomials?

How do you tackle 5 polynomials?

$$f(x) > 0$$

How do you tackle 5 polynomials?

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

for $\ell \gg 0$

How do you tackle 5 polynomials?

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

for $\ell \gg 0$

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

Algorithm 6

Algorithm 6

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

Input: A positive square-free polynomial $f = c_0 + c_1 x + \cdots + c_d x^d \in \mathbb{Q}[x]$. The 2-adic valuations of the coefficients of f are $k_j := \operatorname{ord}_2 c_j$ for $0 \le j \le d$. 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.
```

Conjectural Algorithm

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.
```

Our contributions

(C**D**DHM)

Our contributions

(C**D**DHM)

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

Our contributions

(C**D**DHM)

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

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

$k = 0, 1, \ldots,$ $N \in \mathbb{N}$ odd, $N > 64$

An extension

(C**D**DHM)

An extension

(C**D**DHM)

Theorem

If $f(x) = c_0 + \ldots + c_d x^d$ with $d = 2(2k+1)$, $k \in \mathbb{N}$, $\ell \in \mathbb{N}$ such that $f(t) - \frac{1}{2^{2\ell}}(t^2+t+1)^{2k} t^2 > 0 \forall t$,

An extension

(C**D**DHM)

Theorem

If $f(x) = c_0 + \ldots + c_d x^d$ with $d = 2(2k+1),\ k \in \mathbb{N},\ \ell \in \mathbb{N}$ such that $f(t) - \frac{1}{2^{2\ell}}(t^2+t+1)^{2k}t^2 > 0 \forall t$, then $f(x) - \frac{1}{2^{2\ell}}(x^2+x+1)^{2k}x^2$ is a so4s if c_0 is not a square in $\mathbb{Q}_2$.

Work in Progress

Work in Progress

What to do if c_0 and c_d are squares in $\mathbb{Q}_2$

Main idea

Main idea

Use $f(x) - h(x)^2 > 0$ *and in* $\mathbb{Q}_2[x]$ *every prime factor of odd multiplicity has even degree*

Main idea

Use $f(x) - h(x)^2 > 0$ *and in* $\mathbb{Q}_2[x]$ *every prime factor of odd multiplicity has even degree*

- Irreducibility in $\mathbb{Q}_2[x]$ via 2-adic Newton polygons

Main idea

Use $f(x) - h(x)^2 > 0$ *and in* $\mathbb{Q}_2[x]$ *every prime factor of odd multiplicity has even degree*

- Irreducibility in $\mathbb{Q}_2[x]$ via 2-adic Newton polygons
- p-adic topology in $\mathbb{Q}_2$

Main idea

Use $f(x) - h(x)^2 > 0$ *and in* $\mathbb{Q}_2[x]$

every prime factor of odd multiplicity has even degree

- Irreducibility in $\mathbb{Q}_2[x]$ via 2-adic Newton polygons
- p-adic topology in $\mathbb{Q}_2$
- Hensel Lemma

In general...

In general...

You do not need 5 or 6 polynomials to test positivity:

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

In general...

You do not need 5 or 6 polynomials to test positivity:

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

- semidefinitive optimization (over the reals)

In general...

You do not need 5 or 6 polynomials to test positivity:

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

- semidefinitive optimization (over the reals)
- over the rationals
  Baldo-Krick-Mourrain 2024

Multivariate case is trickier

Multivariate case is trickier

Not true anymore:

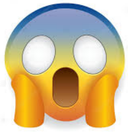
$$f(x_1, x_2) = 1 + x_1^2 x_2^2 (x_1^2 + x_2^2 - 3) \geq 0$$

Multivariate case is trickier

Not true anymore:

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

but not a sum of finite squares

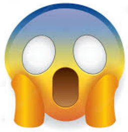


Multivariate case is trickier

Not true anymore:

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

but not a sum of finite squares



Negative solution to Hilbert's 17th Problem

Reals versus racionals

Reals versus racionals

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

Reals versus racionals

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

but cannot written as a sos with polynomials in $\mathbb{Q}[x_0, x_1, x_2, x_3]$

References

References

- Magron, Victor; Koprowski, Przemyslaw; Vaccon, Tristan. **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)
- Rajwade, A. R. **Squares.** Cambridge University Press, Cambridge, 1993

Thanks!

UNIVERSITAT DE BARCELONA