

COMPLEXITY ANALYSIS OF POLYNOMIAL ALGORITHMS

FINAL DEGREE PROJECT

Ignacio Iker Prado Rujas



Complutense University of Madrid (UCM)
Double Degree in Mathematics and Computer Science

Tutors:

Juan R. Delgado, José F. Fernando & José M. Gamboa
Department of Algebra, Faculty of Mathematics

July 13th, 2016

Table of contents

1 Introduction to polynomial images of R^n

- The problem
- Examples
- Main results

2 The open quadrant \mathcal{Q} problem

- The first proof: $g := \mathcal{P} \circ Q \circ H$
- The short proof: $f := \mathcal{H} \circ \mathcal{G} \circ \mathcal{F}$
- The topological proof: $\mathcal{F} = f_2 \circ f_1$

3 Complexity analysis

- Some new candidates
- Measurements of the complexity
- Computational analysis

The problem and its origin

- Let R be a real closed field.

Theorem (Tarski-Seidenberg, 1951)

The image of every polynomial map $f : R^m \rightarrow R^n$ is a semialgebraic subset of R^n .

‘Inverse problem’ (Proposed by J.M. Gamboa, 1990)

Characterize the semialgebraic subsets of R^n that are polynomial images of some R^m .

Some introductory examples

- (i) $[0, +\infty)$ is the image of \mathbb{R} under $f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto x^2$.
- (ii) $(0, +\infty)$ **is not** the image of any polynomial map $\mathbb{R} \rightarrow \mathbb{R}$.
- (iii) $(0, +\infty)$ is the image of $f : \mathbb{R}^2 \rightarrow \mathbb{R}, (x, y) \mapsto (xy - 1)^2 + y^2$.
- (iv) $S := \{x^2 + y^2 > 1\} \subset \mathbb{R}^2$ **is not** a polynomial image of \mathbb{R}^2 .
- (v) $\mathcal{H} := \{y > 0\} \subset \mathbb{R}^2$ is the image of the polynomial map
$$\mathbb{R}^2 \rightarrow \mathbb{R}^2, (x, y) \mapsto (y(xy - 1), (xy - 1)^2 + x^2).$$
- (vi) $S_1 := \{xy < 1\} \subset \mathbb{R}^2$ and $S_2 := \{xy > 1, x > 0\} \subset \mathbb{R}^2$ **are not** polynomial images of \mathbb{R}^2 .
- (vii) $S_3 := \mathbb{R}^2 \setminus \{(0, 0)\}$ is the image of the polynomial map
$$\mathbb{R}^2 \rightarrow \mathbb{R}^2, (x, y) \mapsto (xy - 1, (xy - 1)x^2 - y).$$

Statement of the main results

Theorem 1.9

Let $n \geq 2$. For every finite set $F \subset R^n$, the semialgebraic set $R^n \setminus F$ is a polynomial image of R^n .

Theorem 1.10

Let $n \geq 2$. Given independent linear forms h_1, \dots, h_r of R^n , the open semialgebraic set $\{h_1 > 0, \dots, h_r > 0\}$ is a polynomial image of R^n .

Theorem 1.11 (Open quadrant \mathcal{Q} problem)

The open quadrant $\mathcal{Q} := \{x > 0, y > 0\}$ is a polynomial image of R^2 .

Table of contents

1 Introduction to polynomial images of R^n

- The problem
- Examples
- Main results

2 The open quadrant \mathcal{Q} problem

- The first proof: $g := \mathcal{P} \circ Q \circ H$
- The short proof: $f := \mathcal{H} \circ \mathcal{G} \circ \mathcal{F}$
- The topological proof: $\mathcal{F} = f_2 \circ f_1$

3 Complexity analysis

- Some new candidates
- Measurements of the complexity
- Computational analysis

The first proof: $g := \mathcal{P} \circ Q \circ H$

- ★ If $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ verifies that $f(\mathbb{R}^2) = \mathcal{Q}$ then:

The closure of its image must contain the positive half-axes. (♣)

- ★ To verify (♣) we approach the positive half-axes with certain families of curves:

$$\alpha_\lambda(s) := \left(s, \frac{1 + a_\lambda s}{s} \right) \quad \text{and} \quad \beta_\mu(s) := \left(\frac{1 + b_\mu s}{s}, s^3 \right).$$

- ★ The map $\mathcal{P} := (\mathcal{F}, \mathcal{G})$ defined as:

$$\begin{aligned} \mathcal{F}(x, y) &:= (1 - x^3y + y - xy^2)^2 + (x^2y)^2, \\ \mathcal{G}(x, y) &:= (1 - xy + x - x^4y)^2 + (x^2y)^2, \end{aligned}$$

behaves well along those curves, namely:

$$\lim_{s \rightarrow 0} \mathcal{P}(\alpha_\lambda(s)) = (\lambda^2, 0) \quad \text{and} \quad \lim_{s \rightarrow 0} \mathcal{P}(\beta_\mu(s)) = (0, \mu^2).$$

Maps $y^+(\mathbf{x}, v)$ and $y^-(\mathbf{x}, v)$ from the proof for $v \in [0, 5]$

Maps $\gamma_v^+(\mathbf{x})$ and $\gamma_v^-(\mathbf{x})$ from the proof for $v \in [0, 5]$

The first proof: $g := \mathcal{P} \circ Q \circ H$

- ★ The map $H : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ transforms \mathbb{R}^2 in $\mathbb{R}^2 \setminus \{(0,0), (-1,0)\}$:

$$H(x, y) := (xy + 1, x^2(xy + 1)(xy + 2) + y).$$

- ★ The map $Q : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ maps $(0,0) \mapsto (0,-1)$ and $(-1,0) \mapsto (-1,0)$:

$$Q(x, y) = (x, y - x - 1).$$

- ★ The map $\mathcal{P} := (\mathcal{F}, \mathcal{G})$ transforms \mathbb{R}^2 into $\mathcal{Q} \sqcup \{(1,0), (0,1)\}$ and $\mathcal{P}^{-1}(\{(1,0), (0,1)\}) = \{(0,-1), (-1,0)\}$.

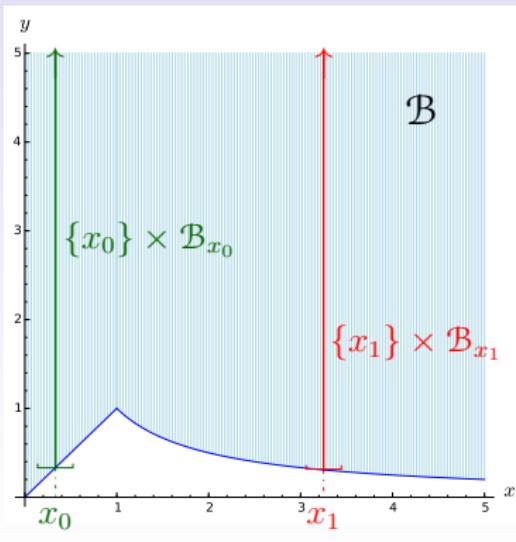
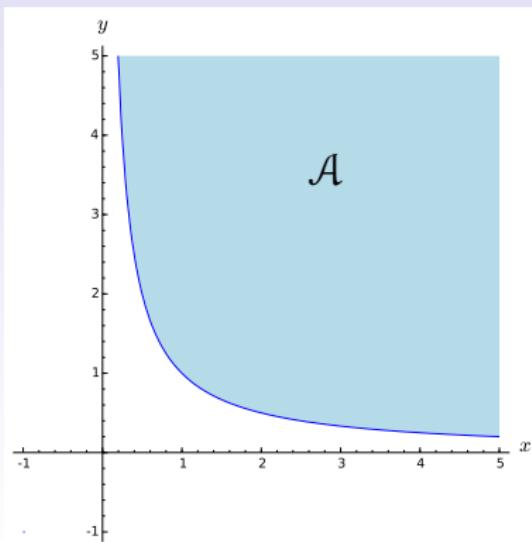
- ★ Then $g(\mathbb{R}^2) = \mathcal{Q}$, where:

$$g := \mathcal{P} \circ Q \circ H : \mathbb{R}^2 \longrightarrow \mathbb{R}^2.$$

The short proof: $f := \mathcal{H} \circ \mathcal{G} \circ \mathcal{F}$

- ★ The map $f := \mathcal{H} \circ \mathcal{G} \circ \mathcal{F} : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ verifies $f(\mathbb{R}^2) = \mathcal{Q}$, where:

$$\boxed{\begin{aligned}\mathcal{F} : \mathbb{R}^2 &\rightarrow \mathbb{R}^2, (x, y) \mapsto ((xy - 1)^2 + x^2, (xy - 1)^2 + y^2), \\ \mathcal{G} : \mathbb{R}^2 &\rightarrow \mathbb{R}^2, (x, y) \mapsto (x, y(xy - 2)^2 + x(xy - 1)^2), \\ \mathcal{H} : \mathbb{R}^2 &\rightarrow \mathbb{R}^2, (x, y) \mapsto (x(xy - 2)^2 + \frac{1}{2}xy^2, y).\end{aligned}}$$



The short proof

Lemma 3.1

The polynomial map \mathcal{F} verifies that $\mathcal{A} \subset \mathcal{F}(\mathbb{R}^2) \subset \mathcal{Q}$.

Lemma 3.2

The polynomial map \mathcal{G} verifies that $\mathcal{B} \subset \mathcal{G}(\mathcal{A}) \subset \mathcal{G}(\mathcal{Q}) \subset \mathcal{Q}$.

Lemma 3.3

The polynomial map \mathcal{H} verifies that $\mathcal{H}(\mathcal{B}) = \mathcal{H}(\mathcal{Q}) = \mathcal{Q}$.

$$\mathcal{Q} \stackrel{3.3}{=} \mathcal{H}(\mathcal{B}) \stackrel{3.2}{\subset} (\mathcal{H} \circ \mathcal{G})(\mathcal{A}) \stackrel{3.1}{\subset} (\mathcal{H} \circ \mathcal{G} \circ \mathcal{F})(\mathbb{R}^2) \stackrel{3.1}{\subset} (\mathcal{H} \circ \mathcal{G})(\mathcal{Q}) \stackrel{3.2}{\subset} \mathcal{H}(\mathcal{Q}) \stackrel{3.3}{=} \mathcal{Q}.$$

The topological proof: $\mathcal{F} = f_2 \circ f_1$

- ★ The map $\mathcal{F} := (\mathcal{F}_1, \mathcal{F}_2) : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ defined as:

$$\boxed{\begin{aligned}\mathcal{F}_1(x, y) &:= (x^2y^4 + x^4y^2 - y^2 - 1)^2 + x^6y^4, \\ \mathcal{F}_2(x, y) &:= (x^6y^2 + x^2y^2 - x^2 - 1)^2 + x^6y^4,\end{aligned}}$$

can be expressed as $\mathcal{F} = f_2 \circ f_1$, with:

$$f_1(x, y) := (x^2, y^2),$$

$$f_2(x, y) := ((xy^2 + x^2y - y - 1)^2 + x^3y^2, (x^3y + xy - x - 1)^2 + x^3y^2).$$

- ★ The map $f_1(x, y)$ verifies $f_1(\mathbb{R}^2) = \overline{\mathcal{Q}} := \{x \geq 0, y \geq 0\}$, so given $a, b > 0$, we must provide $x, y \geq 0$ such that $f_2(x, y) = (a, b)$, namely:

$$\begin{cases} f_{2,1}(x, y) = a, \\ f_{2,2}(x, y) = b. \end{cases}$$

The topological proof: The key step

The boundary map
 $\partial\tilde{\phi}_M : \partial\tilde{\mathcal{R}}_M \rightarrow \mathbb{R}^3$ meets
transversally once \mathcal{D}_1 .

The boundary map
 $\partial\tilde{\phi}_M : \partial\tilde{\mathcal{R}}_M \rightarrow \mathbb{R}^3$ meets
transversally once \mathcal{D}_2 .

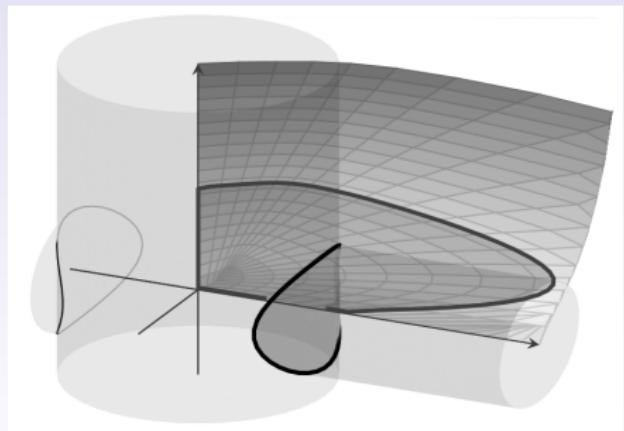
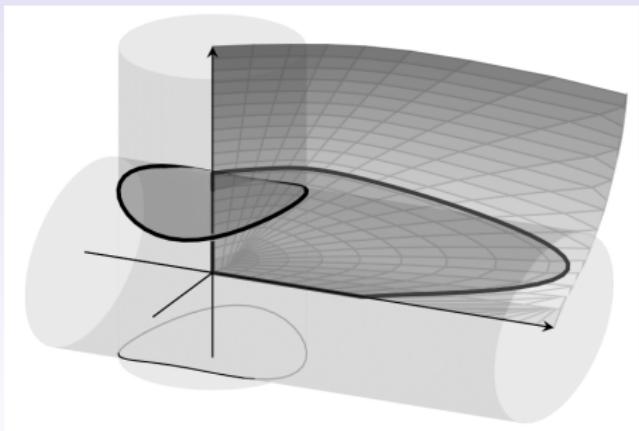


Table of contents

1 Introduction to polynomial images of R^n

- The problem
- Examples
- Main results

2 The open quadrant \mathcal{Q} problem

- The first proof: $g := \mathcal{P} \circ Q \circ H$
- The short proof: $f := \mathcal{H} \circ \mathcal{G} \circ \mathcal{F}$
- The topological proof: $\mathcal{F} = f_2 \circ f_1$

3 Complexity analysis

- Some new candidates
- Measurements of the complexity
- Computational analysis

Some new candidates

- ★ New polynomial maps $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ whose images “should be” \mathcal{Q} :

$$\cdot \mathcal{N}_1(x, y) := (x^4y^4 + (x^2y + xy^2 - 1)^2(y^2 + 1), \\ x^4y^4 + (x^2y + xy^2 - 1)^2(x^2 + 1)).$$

$$\cdot \mathcal{N}_2(x, y) := (x^2y^2 + (x^2y + xy^2 - 1)^2(y^2 + 1), \\ x^2y^2 + (x^2y + xy^2 - 1)^2(x^2 + 1)).$$

$$\cdot \mathcal{N}_3(x, y) := (x^6y^4 + (x^2y + xy^2 - 1)^2(y^2 + 1), \\ x^4y^6 + (x^2y + xy^2 - 1)^2(x^2 + 1)).$$

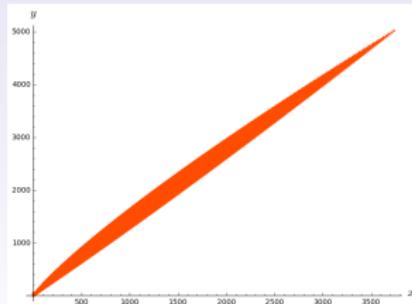
Measurements of the complexity

- ★ **Optimal algebraic structure:** Minimum total degree and sparseness (minimum number of monomials).
- ★ **Optimal multiplicative complexity:** Minimum number of non-scalar products.

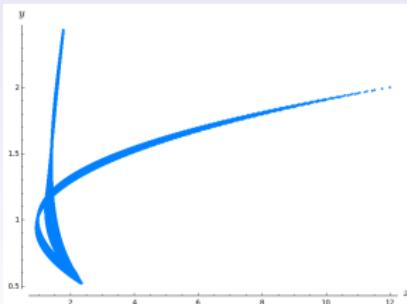
	Total degree	Total number of monomials	Non-escalar complexity
$g = \mathcal{P} \circ Q \circ H$	56	167	13
$f = \mathcal{H} \circ \mathcal{G} \circ \mathcal{F}$	72	350	11
$\mathcal{F} = f_2 \circ f_1$	28	22	11
\mathcal{N}_1	16	24	10
\mathcal{N}_2	16	26	8
\mathcal{N}_3	20	26	13

Uniformly distributed points contained in a square

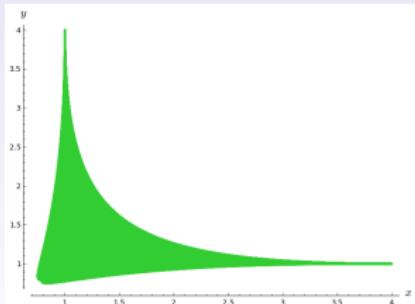
	$g = \mathcal{P} \circ Q \circ H$	$f = \mathcal{H} \circ \mathcal{G} \circ \mathcal{F}$	\mathcal{F}
$\mathcal{P}_1 \rightsquigarrow [-10, 10]^2$	0.19 s	0.17 s	0.07 s
$\mathcal{P}_2 \rightsquigarrow [-100, 100]^2$	17.38 s	16.23 s	6.88 s
$\mathcal{P}_3 \rightsquigarrow [0, 1]^2$	410.73 s	389.74 s	155.09 s
$\mathcal{P}_4 \rightsquigarrow [-1, 1]^2$	408.88 s	392.34 s	155.29 s
$\mathcal{P}_5 \rightsquigarrow [-10, 10]^2$	17.10 s	15.45 s	7.00 s
$\mathcal{P}_6 \rightsquigarrow [-10, 10]^2$	1633.50 s	1640.01 s	625.11 s



(a) $g(\mathcal{P}_3)$.

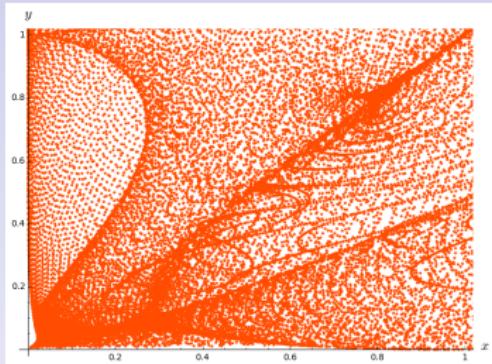


(b) $f(\mathcal{P}_3)$.

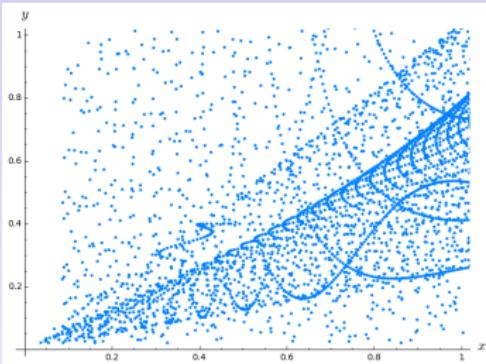


(c) $\mathcal{F}(\mathcal{P}_3)$.

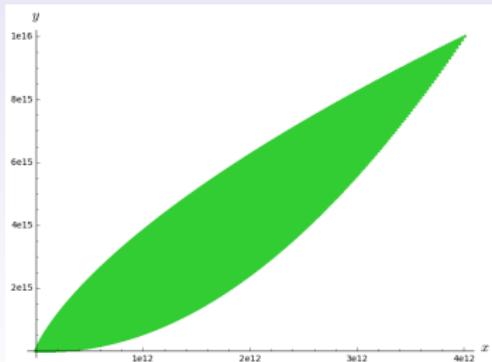
Grid of $4 \cdot 10^6$ points in $[-10, 10] \times [-10, 10]$: g, f, \mathcal{F}



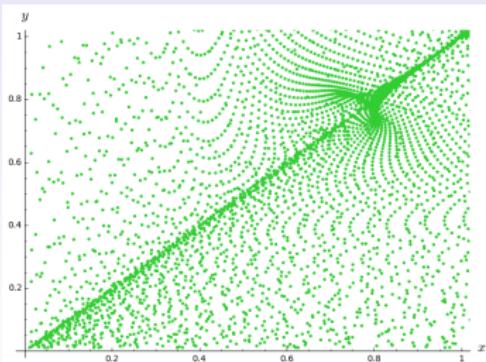
(a) $g(\mathcal{P}_6) \rightsquigarrow 1633.50$ s.



(b) $f(\mathcal{P}_6) \rightsquigarrow 1640.01$ s.

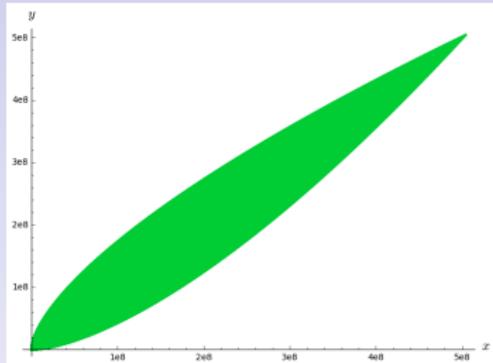


(c) $\mathcal{F}(\mathcal{P}_6) \rightsquigarrow 625.11$ s.

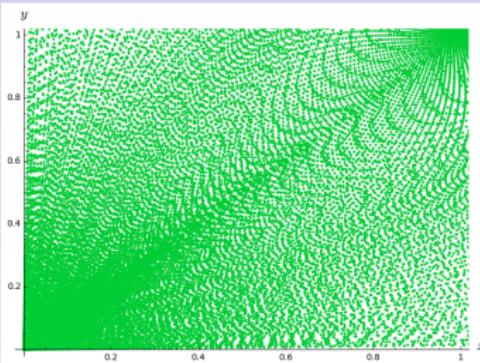


(d) $\mathcal{F}(\mathcal{P}_6) \rightsquigarrow 625.11$ s.

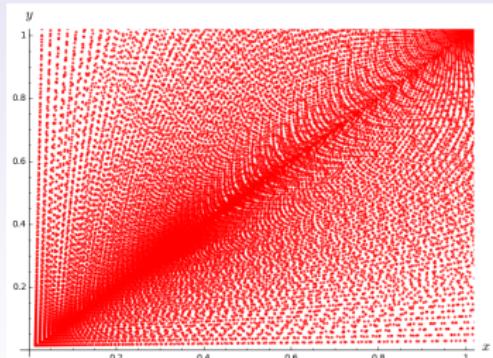
Grid of $4 \cdot 10^6$ points in $[-10, 10] \times [-10, 10]$: $\mathcal{N}_1, \mathcal{N}_2, \mathcal{N}_3$



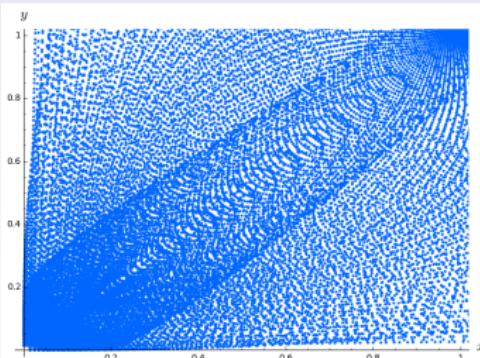
(a) $\mathcal{N}_1(\mathcal{P}_6) \rightsquigarrow 610.06$ s.



(b) $\mathcal{N}_1(\mathcal{P}_6) \rightsquigarrow 610.06$ s.



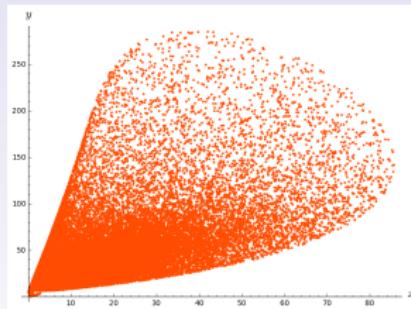
(c) $\mathcal{N}_2(\mathcal{P}_6) \rightsquigarrow 624.18$ s.



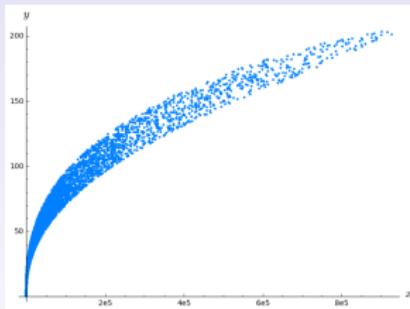
(d) $\mathcal{N}_3(\mathcal{P}_6) \rightsquigarrow 615.09$ s.

Randomly distributed points contained in a disc

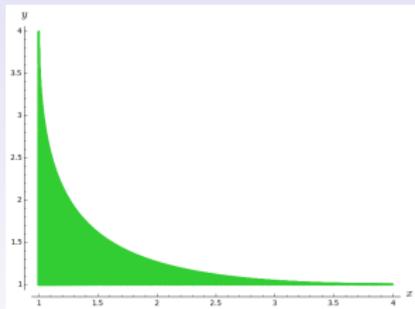
	$g = \mathcal{P} \circ Q \circ H$	$f = \mathcal{H} \circ \mathcal{G} \circ \mathcal{F}$	\mathcal{F}	\mathcal{N}_1	\mathcal{N}_2	\mathcal{N}_3
\mathbb{D}_1	131.97 s	99.56 s	32.02 s	39.61 s	39.31 s	39.13 s
\mathbb{D}_{100}	131.62 s	100.84 s	32.36 s	39.80 s	38.61 s	39.78 s



(a) $g(\mathbb{D}_1)$.

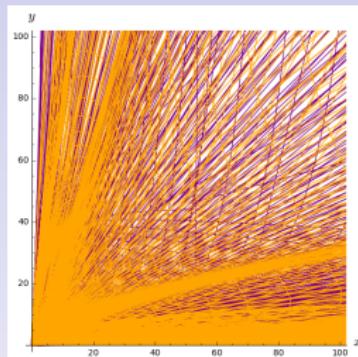


(b) $f(\mathbb{D}_1)$.

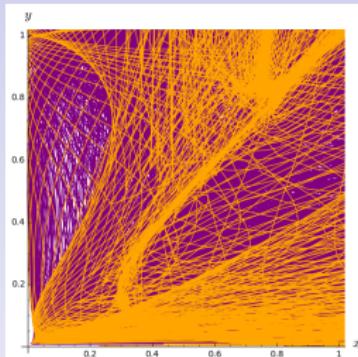


(c) $\mathcal{F}(\mathbb{D}_1)$.

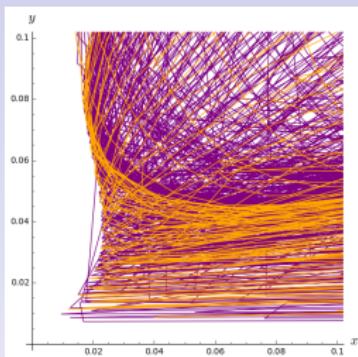
Using families of curves for g and f_2



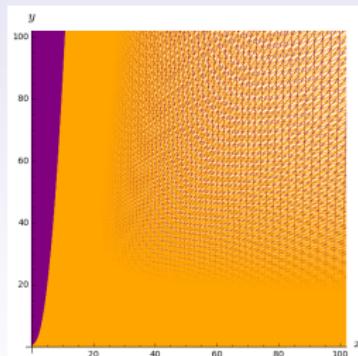
(a) g in $[0, 100]^2$.



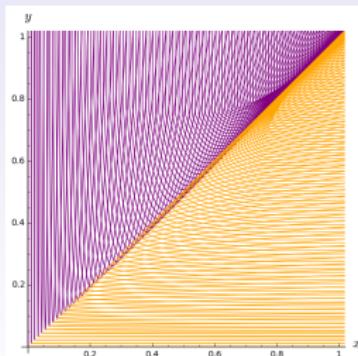
(b) g in $[0, 1]^2$.



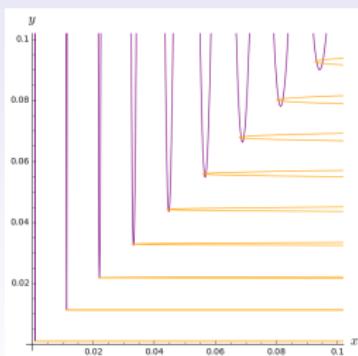
(c) g in $[0, 0.1]^2$.



(d) f_2 in $[0, 100]^2$.

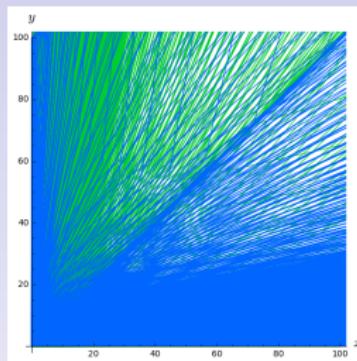


(e) f_2 in $[0, 1]^2$.

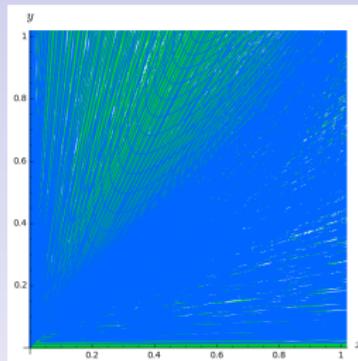


(f) f_2 in $[0, 0.1]^2$.

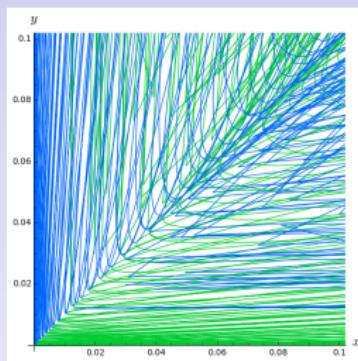
Using families of curves for \mathcal{N}_1 and \mathcal{N}_2



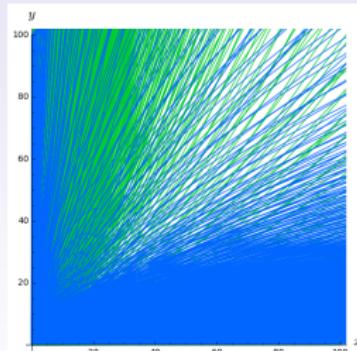
(a) \mathcal{N}_1 in $[0, 100]^2$.



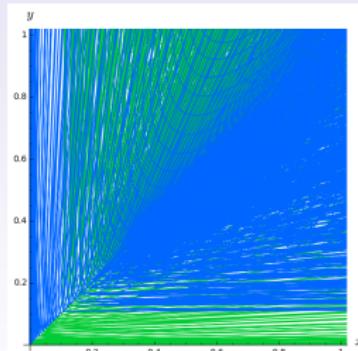
(b) \mathcal{N}_1 in $[0, 1]^2$.



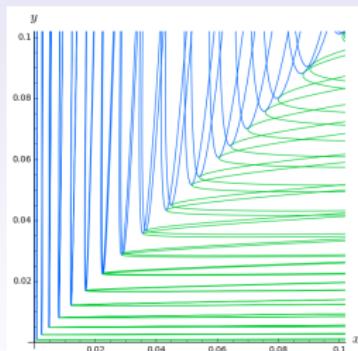
(c) \mathcal{N}_1 in $[0, 0.1]^2$.



(d) \mathcal{N}_2 in $[0, 100]^2$.



(e) \mathcal{N}_2 in $[0, 1]^2$.



(f) \mathcal{N}_2 in $[0, 0.1]^2$.

Some bibliography

-  J. Bochnak, M. Coste, M.-F. Roy: Géométrie algébrique réelle. *Ergeb. Math.* **12**, Springer-Verlag, Berlin, Heidelberg, New York (1987).
-  J.F. Fernando, J.M. Gamboa: Polynomial images of \mathbb{R}^n . *J. Pure Appl. Algebra*, **179** (2003), 241–254.
-  J.F. Fernando, J.M. Gamboa, C. Ueno: The open quadrant problem: A topological proof. A mathematical tribute to Professor José María Montesinos. Departamento de Geometría y Topología. Facultad de CC. Matemáticas UCM, (2016), 337–350.
-  J.F. Fernando, C. Ueno: On the open quadrant as a polynomial image of \mathbb{R}^2 (revisited).
-  C. Ueno: Imágenes polinómicas y regulares de espacios euclídeos. Ph.D. Thesis UCM, (2012).

The first proof: $g := \mathcal{P} \circ Q \circ H$

- $\star \mathcal{Q} \subset \mathcal{P}(\mathbb{R}^2) \rightsquigarrow$ Fix $v > 0$ and proof that $\mathcal{F}(\{\mathcal{G} = v\}) \supset (0, +\infty)$:
- **Step 1:** Parametrization of the curve $\{\mathcal{G} - v = 0\}$. Define $\gamma_v^+(\mathbf{x}, v) := \mathcal{F}(\mathbf{x}, y^+(\mathbf{x}, v))$ and $\gamma_v^-(\mathbf{x}, v) := \mathcal{F}(\mathbf{x}, y^-(\mathbf{x}, v)) \rightsquigarrow$
$$(0, +\infty) \overset{?}{\subset} \text{im}(\gamma_v^+) \cup \text{im}(\gamma_v^-).$$
- **Step 2:** Main properties of γ_v^+ and γ_v^- . Except for $\gamma_1^-(x)$, we have:
$$\lim_{x \rightarrow \pm\infty} \gamma_v^+(x) = \lim_{x \rightarrow \pm\infty} \gamma_v^-(x) = 0, \quad \lim_{x \rightarrow 0} \gamma_v^+(x) = \lim_{x \rightarrow 0} \gamma_v^-(x) = +\infty.$$
- **Step 3:** When $v \geq 0.28^2$ we have $(0, +\infty) \subset \text{im}(\gamma_v^+)$.
- **Step 4:** When $0 < v < 0.28^2$ we have $(0, +\infty) \subset \text{im}(\gamma_v^-)$.

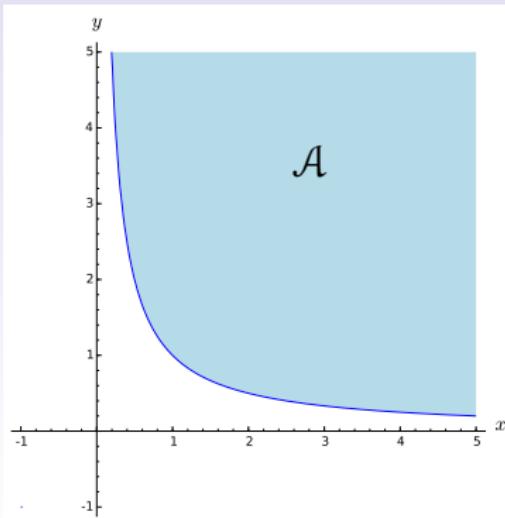
The short proof: The first lemma

Lemma 3.1

Let $\mathcal{A} := \{xy \geq 1\} \cap \mathcal{Q}$. Then the image of the map

$$\mathcal{F} := (\mathcal{F}_1, \mathcal{F}_2) : \mathbb{R}^2 \rightarrow \mathbb{R}^2, (x, y) \mapsto ((xy - 1)^2 + x^2, (xy - 1)^2 + y^2)$$

satisfies that $\mathcal{A} \subset \mathcal{F}(\mathbb{R}^2) \subset \mathcal{Q}$.



The short proof: The second lemma

Lemma 3.2

Let $\mathcal{B} := \mathcal{A} \cup \{y \geq x > 0\}$. Then, the map

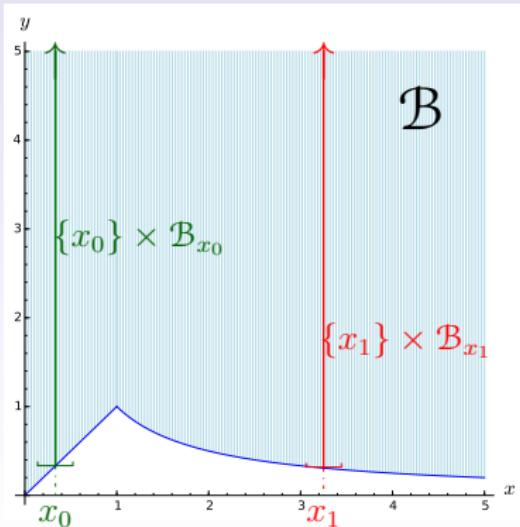
$$\mathcal{G} := (\mathcal{G}_1, \mathcal{G}_2) : \mathbb{R}^2 \rightarrow \mathbb{R}^2, (x, y) \mapsto (x, y(xy - 2)^2 + x(xy - 1)^2)$$

satisfies that $\mathcal{B} \subset \mathcal{G}(\mathcal{A}) \subset \mathcal{G}(\mathcal{Q}) \subset \mathcal{Q}$.

$$y_x := \min\{x, 1/x\},$$

$$\mathcal{B}_x := [y_x, +\infty),$$

$$\mathcal{B} = \bigsqcup_{x>0} (\{x\} \times \mathcal{B}_x).$$



The short proof: The third lemma

Lemma 3.3

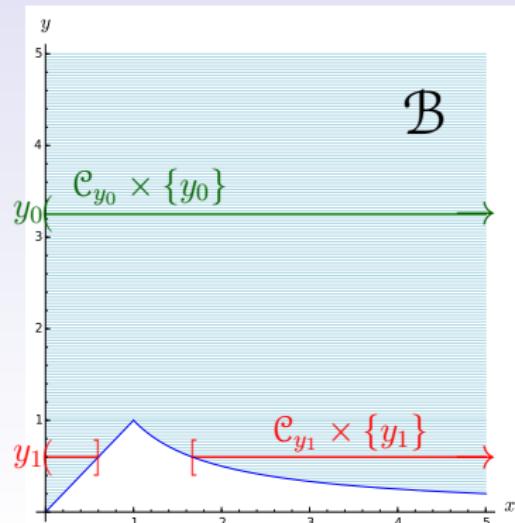
The polynomial map

$$\mathcal{H} := (\mathcal{H}_1, \mathcal{H}_2) : \mathbb{R}^2 \rightarrow \mathbb{R}^2, (x, y) \mapsto (x(xy - 2)^2 + \frac{1}{2}xy^2, y)$$

satisfies $\mathcal{H}(\mathcal{B}) = \mathcal{H}(\mathcal{Q}) = \mathcal{Q}$.

$$\mathcal{C}_y := \begin{cases} (0, +\infty) & \text{if } y \geq 1, \\ (0, y] \cup [1/y, +\infty) & \text{if } 0 < y < 1. \end{cases}$$

$$\mathcal{B} = \bigsqcup_{y>0} (\mathcal{C}_y \times \{y\}).$$



The short proof

Lemma 3.1

The polynomial map \mathcal{F} verifies that $\mathcal{A} \subset \mathcal{F}(\mathbb{R}^2) \subset \mathcal{Q}$.

Lemma 3.2

The polynomial map \mathcal{G} verifies that $\mathcal{B} \subset \mathcal{G}(\mathcal{A}) \subset \mathcal{G}(\mathcal{Q}) \subset \mathcal{Q}$.

Lemma 3.3

The polynomial map \mathcal{H} verifies that $\mathcal{H}(\mathcal{B}) = \mathcal{H}(\mathcal{Q}) = \mathcal{Q}$.

$$\mathcal{Q} \stackrel{3.3}{=} \mathcal{H}(\mathcal{B}) \stackrel{3.2}{\subset} (\mathcal{H} \circ \mathcal{G})(\mathcal{A}) \stackrel{3.1}{\subset} (\mathcal{H} \circ \mathcal{G} \circ \mathcal{F})(\mathbb{R}^2) \stackrel{3.1}{\subset} (\mathcal{H} \circ \mathcal{G})(\mathcal{Q}) \stackrel{3.2}{\subset} \mathcal{H}(\mathcal{Q}) \stackrel{3.3}{=} \mathcal{Q}.$$

The topological proof: $\mathcal{F} = f_2 \circ f_1$

· **Step 1:** Factor $\mathcal{F} = f_2 \circ f_1$, with:

$$f_1(x, y) := (x^2, y^2) \rightsquigarrow f_1(\mathbb{R}^2) = \overline{\mathcal{Q}} := \{x \geq 0, y \geq 0\},$$

$$f_2(x, y) := ((xy^2 + x^2y - y - 1)^2 + x^3y^2, (x^3y + xy - x - 1)^2 + x^3y^2).$$

· **Step 2:** Factor $f_2 = h \circ g$, where $g : \overline{\mathcal{Q}} \rightarrow \mathbb{R}^3$, $h : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ and:

$$g(x, y) := (xy^2 + x^2y - y - 1, x^{3/2}y, x^3y + xy - x - 1),$$

$$h(x, y, z) := (x^2 + y^2, y^2 + z^2).$$

· **Step 3:** Let $\mathcal{S} := g(\overline{\mathcal{Q}})$. Then:

$$\forall (A^2, B^2) \in \mathcal{Q} : h^{-1}(\{(A^2, B^2)\}) \cap \mathcal{S} \neq \emptyset.$$

· **Step 4:** For fixed values $B \geq A > 0$: $\partial\mathcal{D}_1 \cap \mathcal{S} \neq \emptyset \neq \partial\mathcal{D}_2 \cap \mathcal{S}$.

The topological proof: Step 4

The boundary map
 $\partial\tilde{\phi}_M : \partial\tilde{\mathcal{R}}_M \rightarrow \mathbb{R}^3$ meets
transversally once \mathcal{D}_1 .

The boundary map
 $\partial\tilde{\phi}_M : \partial\tilde{\mathcal{R}}_M \rightarrow \mathbb{R}^3$ meets
transversally once \mathcal{D}_2 .

