New conditions for the intersection of algebraic curves with polydisk

Yacine Bouzidi⋆

⋆ INRIA Lille - Nord Europe,

⋆ yacine.bouzidi@inria.fr

Luminy, Marseille, February 4th, 2019

Journées Nationales de Calcul Formel

Intersection with polydisk: a historical problem

Consider the closed unit polydisk of $\mathbb{C}^n$

$$\mathbb{U}^n := \{z = (z_1, \ldots, z_n) \in \mathbb{C}^n \mid |z_i| \leq 1, i = 1, \ldots, n\}$$

Let $\mathcal{V} \subset \mathbb{C}^n$ be an algebraic variety

$$\mathcal{V} := \{z = (z_1, \ldots, z_n) \in \mathbb{C}^n \mid f_1(z) = \cdots = f_m(z) = 0\},$$

where $f_1, \ldots, f_m \in \mathbb{Q}[z_1, \ldots, z_n]$

Problem: Decide whether or not

$$\mathcal{V} \cap \mathbb{U}^n = \emptyset$$

Application:

$m = 1$: stability condition for n-dimensional systems

$m > 1$: stabilization condition for n-dimensional systems

From a complex to a real problem

For a polynomial system $\{f_1, \ldots, f_m\} \subset \mathbb{Q}[z_1, \ldots, z_n]$

If $z_k = a_k + i\, b_k$, $a_k, b_k \in \mathbb{R}$ the problem is equivalent to:

$$\begin{cases} \mathcal{R}(f_j(a_1 + i\, b_1, \ldots, a_n + i\, b_n)) = 0 & \multirow{2}{*}{$j = 1, \ldots, m$} \\ \mathcal{C}(f_j(a_1 + i\, b_1, \ldots, a_n + i\, b_n)) = 0 & \\ a_k^2 + b_k^2 - 1 \leq 0 & k = 1, \ldots, n \end{cases}$$

Problem reduced to testing the emptiness of a semi-algebraic set in $\mathbb{R}^{2n}$

Generically of dimension $2(n - m)$

Drawback: the number of variables is doubled !

The Strintzis-Decarlo conditions

For the case $m = 1$, simpler conditions have been derived

Theorem (Strintzis, Decarlo et. al. 77)

Let $f(z_1, \ldots, z_n) \in \mathbb{R}[z_1, \ldots, z_n]$, the following two conditions are equivalent:

$$f(z_1, \ldots, z_n) \neq 0 \;\; \textit{when} \;\; |z_1| \leq 1, \ldots, |z_n| \leq 1.$$

$$\begin{cases} f(z_1, 1, \ldots, 1) & \neq 0, \quad \textit{when} \quad |z_1| \leq 1, \\ f(1, z_2, 1, \ldots, 1) & \neq 0, \quad \textit{when} \quad |z_2| \leq 1, \\ \vdots & \qquad\qquad\qquad\qquad \vdots \\ f(1, \ldots, 1, z_n) & \neq 0, \quad \textit{when} \quad |z_n| \leq 1, \\ f(z_1, \ldots, z_n) & \neq 0, \quad \textit{when} \quad |z_1| = \ldots = |z_n| = 1. \end{cases}$$

The problem reduces to an intersection with

$$\mathbb{T}^n := \{z = (z_1, \ldots, z_n) \in \mathbb{C}^n \mid |z_k| = 1, k = 1, \ldots, n\}$$

Setting $z_i = \frac{x+i}{x-i}$ in the last condition $\rightsquigarrow$ checking the emptiness of an algebraic set in $\mathbb{R}^n$. [B. Quadrat, Rouillier 2016]

Idea of the original proof

Consider w.lo.g the case $n = 2$

$$f(z_1, z_2) \neq 0 \text{ when } |z_1| \leq 1, |z_2| \leq 1 \iff \begin{cases} f(1, z_2) \neq 0, & \text{when } |z_2| \leq 1 \\ f(z_1, 1) \neq 0, & \text{when } |z_1| \leq 1 \\ f(z_1, z_2) \neq 0, & \text{when } |z_1| = |z_2| = 1 \end{cases}$$

Proof based on the continuity of the following function in $\mathbb{U}$

$$N(z_1) = \frac{1}{2\pi j} \oint_{|z_2|=1} \frac{\partial f(z_1, z_2)}{\partial z_2} [f(z_1, z_2)]^{-1} d\, z_2$$

$N(z_1)$ is the number of zeros in z_2 of $f(z_1, z_2)$ lying in $|z_2| \leq 1$

$N(z_1)$ is integer-valued $\rightsquigarrow$ constant $\rightsquigarrow$ 0

It does not generalize to arbitrary algebraic varieties ! at least straighforwardly.

Our contributions

1. New conditions for the case of complete intersection algebraic curves

⇝ **The main ingredient**: a new Strintzis-like theorem based on continuity arguments

2. A new algorithm for testing the intersection between algebraic curves and polydisk

⇝ The problem is reduced to zero-dimensional systems solving

For simplicity, we focus in this talk on the case of algebraic curves in $\mathbb{C}^3$

The simplest case : algebraic curves in $\mathbb{C}^2$

Let $\mathcal{C}$ be an algebraic curve in $\mathbb{C}^2$

$$\mathcal{C} := \{(z_1, z_2) \in \mathbb{C}^2 \mid f(z_1, z_2) = 0\},$$

where $f(z_1, z_2) \in \mathbb{Q}[z_1, z_2]$

Theorem (Strintzis, Decarlo et. al. 77)

The following two conditions are equivalent

$$f(z_1, z_z) \neq 0 \;\; \textit{when} \;\; |z_1| \leq 1, |z_2| \leq 1.$$

$$\begin{cases} f(1, z_2) \neq 0, & \textit{when} \quad |z_2| \leq 1 \\ f(z_1, 1) \neq 0, & \textit{when} \quad |z_1| \leq 1 \\ f(z_1, z_2) \neq 0, & \textit{when} \quad |z_1| = |z_2| = 1 \end{cases}$$

Sketch of the proof [B. and Moroz]

We proceed by contraposition.

Let $(\alpha, \beta) \in \mathbb{U}^2 \mid f(\alpha, \beta) = 0$.

Consider the continuous path inside the complex unit disk:

$$\alpha(t) : \begin{array}{ccc} [0,1] & \longrightarrow & \mathbb{U} \\ t & \longmapsto & (1-t)\alpha + t \end{array}$$

and consider the polynomial

$$f(\alpha(t), z_2) = a_n(t)\, z_2^n + a_{n-1}(t)\, z_2^{n-1} + \cdots + a_0(t)$$

Sketch of the proof [B. and Moroz]

We proceed by contraposition.

Let $(\alpha, \beta) \in \mathbb{U}^2 \mid f(\alpha, \beta) = 0$.

Consider the continuous path inside the complex unit disk:

$$\alpha(t) : \begin{array}{ccc} [0,1] & \longrightarrow & \mathbb{U} \\ t & \longmapsto & (1-t)\alpha + t \end{array}$$

and consider the polynomial

$$f(\alpha(t), z_2) = a_n(t)\, z_2^n + a_{n-1}(t)\, z_2^{n-1} + \cdots + a_0(t)$$

Two cases:

$\forall t \in [0,1], a_n(t) \neq 0$: the roots of $f(\alpha(t), z_2)$ vary continuously when t goes from 0 to 1

$\implies \exists \beta_1$ and $\beta(t) : [0,1] \to \mathbb{C}$ such that $f(1, \beta_1) = 0$ and $\beta(0) = \beta, \beta(1) = \beta_1$.

Two cases:

$|\beta_1| \leq 1 \implies \exists \beta \in \mathbb{U} \mid f(1, \beta) = 0$ (first condition of the theorem)

$|\beta_1| > 1$, by the continuity of the norm $\implies \exists (\alpha, \beta) \in \mathbb{U} \times \mathbb{T} \mid f(\alpha, \beta) = 0$

Sketch of the proof (end)

$\exists t_0 \in [0,1], a_n(t_0) = a_{n-1}(t_0) = \cdots = a_{m+1}(t_0) = 0, a_m(t_0) \neq 0$: $n - m$ roots of f go continuously to infinity while t tends to t_0.

Two cases:

β is not among these roots $\implies$ back to the first case

β is among these roots, by the continuity of the norm $\implies \exists t_1 \leq t_0$ and $(\alpha_1 = \alpha(t_1), \beta_1 = \beta(t_1)) \in \mathbb{U} \times \mathbb{T}$ such that $f(\alpha_1, \beta_1) = 0$

Sketch of the proof (end)

$\exists t_0 \in [0,1], a_n(t_0) = a_{n-1}(t_0) = \cdots = a_{m+1}(t_0) = 0, a_m(t_0) \neq 0$: $n-m$ roots of f go continuously to infinity while t tends to t_0.

Two cases:

β is not among these roots $\Longrightarrow$ back to the first case

β is among these roots, by the continuity of the norm $\Longrightarrow \exists t_1 \leq t_0$ and $(\alpha_1 = \alpha(t_1), \beta_1 = \beta(t_1)) \in \mathbb{U} \times \mathbb{T}$ such that $f(\alpha_1, \beta_1) = 0$

One condition left,

$$\exists(\alpha, \beta) \in \mathbb{U} \times \mathbb{T} \mid f(\alpha, \beta) = 0$$

We proceed in the same way considering this time the following continuous path in $\mathbb{T}$

$$\beta(t) : \begin{array}{ccc} [0,1] & \longrightarrow & \mathbb{T} \\ t & \longmapsto & e^{i(1-t)\theta} \end{array}$$

where $\beta = e^{i\theta}$

Algebraic curves in $\mathbb{C}^3$

Let $\mathcal{C}$ be an algebraic curve in $\mathbb{C}^3$

$$\mathcal{C} := \{(z_1, z_2, z_3) \in \mathbb{C}^3 \mid f(z_1, z_2, z_3) = g(z_1, z_2, z_3) = 0\},$$

where $f, g \in \mathbb{Q}[z_1, z_2, z_3]$ are in complete intersection.

We make the following **assumptions**

- The ideal $\langle f, g \rangle$ is radical
- For any fixed value of z_i, $\sharp V_{\mathbb{C}}(\langle f(., z_i, .), g(., z_i, .)\rangle) < \infty$.

  $\rightsquigarrow$ The curve $\mathcal{C}$ does not admit a whole component lying in the plan orthogonal to any direction z_i.

Algebraic curves in $\mathbb{C}^3$

For a given z_i, consider the following canonical projection map

$$\Pi_i : \begin{array}{ccc} \mathbb{C}^3 & \longrightarrow & \mathbb{C} \\ (z_1, z_2, z_3) & \longmapsto & z_i \end{array}$$

As well as the following sets

- $\mathcal{V}_s \subset \mathbb{C}^2$ is the set of singular points of $\mathcal{C} = V(\langle f, g \rangle)$.
- $\mathcal{V}_c^i \subset \mathbb{C}^2$ is the set of critical points of Π_i restricted to $\mathcal{C}$ and $\Pi_i(\mathcal{V}_c^i)$ its projection on the z_i-axis.
- $\mathcal{V}_\infty^i \subset \mathbb{C}$ is the set of non-properness points of Π_i, i.e.,: $z_i \in \mathbb{C}$ such that $\Pi_i^{-1}(\mathcal{V}) \cap \mathcal{C}$ is not compact for any compact neighborhood $\mathcal{V}$ of z_i.

Algebraic curves in $\mathbb{C}^3$

Theorem

Under our assumptions, $\mathcal{V}_c^i \cup \mathcal{V}_s$ and $\mathcal{V}_\infty^i$ are $\mathbb{Q}$-Zariski closed sets of dimension zero.

Proof

• $\mathbb{Q}$-Zariski closedness

$\mathcal{V}_c^i \cup \mathcal{V}_s = V(\langle f, g, Jac_{z_i}(f,g)\rangle)$ where $Jac_{z_i}(f,g) = \langle \frac{\partial f}{\partial z_j}\frac{\partial g}{\partial z_k} - \frac{\partial f}{\partial z_k}\frac{\partial g}{\partial z_j}\rangle$ with $j, k \neq i$

$\mathcal{V}_\infty^i = \pi(\mathcal{C}_p \cap \mathcal{H}_\infty)$ where $\mathcal{C}_p$ is the projective closure of $\mathcal{C}$ in $\mathbb{C} \times \mathbb{P}^2$, $\mathcal{H}_\infty$ is the plan at infinity in $\mathbb{C} \times \mathbb{P}^2$ and $\pi : \mathbb{C} \times \mathbb{P}^2 \to \mathbb{C}$ the projection.

• Zero-dimensionality

Sard theorem + assumptions $\rightsquigarrow$ $\mathcal{V}_c^i \cup \mathcal{V}_s$ is zero-dimensional

Non-properness locus is of co-dimension 1 $\rightsquigarrow$ $\mathcal{V}_\infty^i$ is zero-dimensional

Algebraic curves in $\mathbb{C}^3$

Theorem (Lazard, Rouillier 07)

For any open disk $\mathcal{D} \in \mathbb{C} / \{\Pi_i(\mathcal{V}_c^i) \cup \Pi_i(\mathcal{V}_s) \cup \mathcal{V}_\infty^i\}$, the canonical projection

$$\Pi_i : \Pi_i^{-1}(\mathcal{D}) \cap \mathcal{C} \longrightarrow \mathcal{D}$$

is an analytic covering of $\mathcal{D}$.

In broad terms, it is said that over any open disk $\mathcal{D}$ in $\mathbb{C} / \{\Pi_i(\mathcal{V}_c^i) \cup \Pi_i(\mathcal{V}_s) \cup \mathcal{V}_\infty^i\}$, the solutions of the system $\{f, g\}$ in $z_{j \neq i}$ are continuous functions of the variable z_i.

The main theorem

Let $\mathcal{C}$ be a curve defined as

$$\mathcal{C} := \{(z_1, z_2, z_3) \in \mathbb{C}^3 \mid f(z_1, z_2, z_3) = g(z_1, z_2, z_3) = 0\},$$

that fulfills the assumptions.

Define the set of ramification points $\mathcal{W}$ as

$$\mathcal{W} := \mathcal{V}_s \cup \mathcal{V}_c^1 \cup \mathcal{V}_c^2 \cup \mathcal{V}_c^3$$

Notation

$f_{z_i=1}$ is the polynomial resulting from f after the substitution $z_i = 1$

$\mathbb{E}_i = \{(z_1, z_2, z_3) \in \mathbb{C}^3 \mid \ |z_i| \leq 1 \text{ and } |z_{j\neq i}| = 1\}$

Theorem

If $\mathcal{W} \cap \mathbb{U}^3 = \emptyset$ then the two following conditions are equivalent

1. $\mathcal{C} \cap \mathbb{U}^3 = \emptyset$
2. $\forall i \in \{1, 2, 3\}, V(\langle f_{z_i=1}, g_{z_i=1}\rangle) \cap \mathbb{U}^2 = \emptyset$ *and* $V(\langle f, g\rangle) \cap \mathbb{E}_i = \emptyset$

Sketch of the proof

Similarly as in the proof of Theorem 2, we proceed by the contrapose.

Let $(\alpha, \beta, \gamma) \in \mathbb{U}^3 \mid \{f(\alpha, \beta, \gamma) = g(\alpha, \beta, \gamma) = 0\}$.

Consider the continuous path inside the complex unit disk:

$$\alpha(t) : \begin{array}{ccc} [0,1] & \longrightarrow & \mathbb{U} \\ t & \longmapsto & (1-t)\alpha + t \end{array}$$

and the following polynomial system

$$S := \{f(\alpha(t), z_2, z_3) = g(\alpha(t), z_2, z_3) = 0\}$$

If $V(\alpha([0,1])) \cap \mathcal{V}^1_\infty = \emptyset$: the roots of S vary continuously in $\mathbb{U}^2$ when $t = 0 \rightsquigarrow 1$. Then

$\exists\, (\beta_1, \gamma_1) \in \mathbb{U}^2$ such that $f(1, \beta_1, \gamma_1) = g(1, \beta_1, \gamma_1) = 0$

Or

$\exists\, (\alpha_1, \beta_1, \gamma_1) \in \mathbb{U}^2 \times \mathbb{T}$ such that $f(\alpha_1, \beta_1, \gamma_1) = g(\alpha_1, \beta_1, \gamma_1) = 0$

Or

$\exists\, (\alpha_1, \beta_1, \gamma_1) \in \mathbb{U} \times \mathbb{T} \times \mathbb{U}$ such that $f(\alpha_1, \beta_1, \gamma_1) = g(\alpha_1, \beta_1, \gamma_1) = 0$

Sketch of the proof (end)

If $\exists t_0 \in [0,1] \mid \alpha(t_0) \in \mathcal{V}^1_\infty$: some roots of S go to infinity in z_2 or z_3 while t tends to t_0.

Two cases:

(β, γ) is not among these roots $\Longrightarrow$ back to the first case.

(β, γ) is among these roots, then

$\exists\ (\alpha_1, \beta_1, \gamma_1) \in \mathbb{U}^2 \times \mathbb{T}$ such that $f(\alpha_1, \beta_1, \gamma_1) = g(\alpha_1, \beta_1, \gamma_1) = 0$

Or

$\exists\ (\alpha_1, \beta_1, \gamma_1) \in \mathbb{U} \times \mathbb{T} \times \mathbb{U}$ such that $f(\alpha_1, \beta_1, \gamma_1) = g(\alpha_1, \beta_1, \gamma_1) = 0$

Starting from one of the two last condition, we proceed in the same way considering this time a continuous path on the circle $\mathbb{T}$ for one of the other variable. say β

$$\beta(t) : \begin{array}{ccc} [0,1] & \longrightarrow & \mathbb{T} \\ t & \longmapsto & e^{i(1-t)\theta} \end{array}$$

where $\beta = e^{i\theta}$

An intersection algorithm

The algorithm consists of the following steps

1. If $(\mathcal{W} \cap \mathbb{U}^3 \neq \emptyset)$, then return true
2. For i from 1 to 3 do

   $\rightsquigarrow$ If $(V(\langle f_{z_i=1}, g_{z_i=1} \rangle) \cap \mathbb{U}^2 \neq \emptyset$ or $V(\langle f, g \rangle) \cap \mathbb{E}_i \neq \emptyset)$, then return true
3. return false

Checking the conditions

All the conditions involve only zero-dimensional systems

- $\mathcal{W}$ is zero-dimensional in $\mathbb{C}^3$.
- $V(f_{z_i=1}, g_{z_i=1})$ is zero-dimensional in $\mathbb{C}^2$.
- $V(f,g) \cap \mathbb{E}_i$ by the change of variables $\begin{cases} z_i = a + i\,b \\ z_{j \neq i} = \frac{(x_j - i)}{(x_j + i)} \end{cases}$ is zero dimensional in $\mathbb{R}^4$

The problem is thus reduced to the computation of a sign of polynomials at the real solutions of zero-dimensional algebraic systems

Convinient tool: univariate representation of the solution

$$\{\mathcal{X}(t) = 0, z_1 = g_{z_1}(t), \ldots, z_n = g_{z_n}(t)\}$$

$\rightsquigarrow$ reduces the problem to the computation of the sign of a univariate polynomial at a real algebraic number.

Sign computation

Compute a Univariate Representation of $\langle f_1, \ldots, f_m \rangle$

$$\{\mathcal{X}(t) = 0, z_1 = g_{z_1}(t), \ldots, z_n = g_{z_n}(t)\}$$

Isolation into pair of intervals: $z_k = [a_{k,1}, a_{k,2}] + i\,[b_{k,1}, b_{k,2}]$

Compute the sign of $[a_{k,1}, a_{k,2}]^2 + [b_{k,1}, b_{k,2}]^2 - 1$

What if some coordinates are on the unit circle ? $\rightsquigarrow$ Cannot conclude

Need to identify these coordinates or at least to count them

For each z_i, this can be read on the resultant of $\mathcal{X}(t)$ and $z_i - g_{z_i}(t)$ with respect to t
$\rightsquigarrow$ **e.g:** via Möbius transform.

Conclusion

Contributions

- New conditions for the intersection of algebraic curves with polydisks
- Effective algorithm for testing the stabilization of a class of *n*-D systems

  [B et. al 2016] : dimension zero, [B. 2019]: dimension one

  $\rightsquigarrow$ Complete analysis of the stabilization of 3-D systems

Conclusion

Contributions

- New conditions for the intersection of algebraic curves with polydisks
- Effective algorithm for testing the stabilization of a class of n-D systems

  [B et. al 2016] : dimension zero, [B. 2019]: dimension one

  $\rightsquigarrow$ Complete analysis of the stabilization of 3-D systems

Perspectives

- Conditions for arbitrary algebraic varieties
- Constructive and effective **polydisk Nullstelensatz**

  Let $I := \langle f_1, \ldots, f_m \rangle \subset \mathbb{Q}[z_1, \ldots, z_n]$ such that

$$V_{\mathbb{C}}(I) \cap \mathbb{U}^n = \emptyset.$$

  Then, there exists a polynomial s as well as $u_1, \ldots, u_m \in \mathbb{Q}[z_1, \ldots, z_n]$ such that

$$s = \sum_{i=1}^{m} u_i\, f_i \quad \text{and} \quad V_{\mathbb{C}}(s) \cap \mathbb{U}^n = \emptyset$$

Thank you for your attention