Effective polydisk nullstellensatz : the zero-dimensional case

Yacine Bouzidi⋆

⋆ INRIA Lille - Nord Europe, NON-A project

⋆ yacine.bouzidi@inria.fr

supported by the ANR MSDOS

January 20, 2017

Joint work with T. Cluzeau, G. Moroz and A. Quadrat

Nullstellensatz theorem

- David Hilbert 1890
- $I = \langle p_1, \ldots, p_m \rangle$ is a polynomial ideal in $\mathbb{Q}[z_1, \ldots, z_n]$ and its variety

$$V(I) = \{z \in \mathbb{C}^n \mid p_1(z) = \cdots = p_m(z) = 0\}$$

- Nullstellensatz theorem (weak): (i) and (ii) are equivalent

1. $V_{\mathbb{C}}(I) = \emptyset$
2. $\exists u_1, \ldots, u_m \in \mathbb{Q}[z_1, \ldots, z_n]$ such that

$$\sum_{i=1}^{m} u_i \, p_i = 1$$

Polydisk nullstellensatz theorem

- The closed unit polydisk

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

- Polydisk nullstellensatz theorem : (i) and (ii) are equivalent

1. $V_{\mathbb{C}}(I) \cap \overline{\mathbb{U}}^n = \emptyset$
2. $\exists s, u_1, \ldots, u_m \in \mathbb{Q}[z_1, \ldots, z_n]$ such that $s = \sum_{i=1}^m u_i\, p_i$ and

$$V_{\mathbb{C}}(s) \cap \overline{\mathbb{U}}^n = \emptyset$$

Effective polydisk nullstellensatz

• Given an ideal $I \subset \mathbb{Q}[z_1, \ldots, z_n]$, two problems stem from the previous theorem:

1. Check whether $V_{\mathbb{C}}(I) \cap \overline{\mathbb{U}}^n = \emptyset$
2. Compute $s \in I$ and $u_1, \ldots, u_m$ such that

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

Motivation : stabilisation of n-D systems

- $A := \mathbb{Q}[z_1, \ldots, z_n]$ the polynomial ring
- Every n-D system P can be represented by a matrix

$$R \in A^{q \times (q+r)}$$

- Theorem: P is internally stabilizable if the ideal I generated by the reduced $q \times q$ minors of R is devoid from zeros in $\overline{\mathbb{U}}^n$.

- A stabilizing control can be constructed by computing $s \in I$:

$$V_{\mathbb{C}}(s) \cap \overline{\mathbb{U}}^n = \emptyset$$

Existing work

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

- $z_k = x_k + i\, y_k$ and $x_k^2 - y_k^2 - 1 \leq 0 \rightsquigarrow$ emptiness of semi-algebraic sets : effective but not efficient
- The case $I = \langle p \rangle$: [B. Quadrat and Rouillier, 15]

2. Computation of the polynomial $s \in I$ with $V_{\mathbb{C}}(s) \cap \overline{\mathbb{U}}^n = \emptyset$

- [Berenstein and Struppa 86] : rational functions
- [Bridges et al. 03] : constructive proof but not effective
- [Xu et. al 94] : Zero-dimensional ideal, also not effective

The radical zero dimensional case

- We restrict the study to zero-dimensional ideal:

$$\sharp V_{\mathbb{C}}(I) < \infty$$

- We also suppose without loss of generality that I is a radical ideal:

$$I = \sqrt{I}$$

Intersection with the polydisk

- Goal: For a given zero-dimensional ideal I, check that

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

- Tool: Univariate representation of the complex zeros of I

$\rightsquigarrow$ A one-to-one mapping between the zeros of I and the roots of a univariate polynomial

$$\begin{array}{rcl} V(I) & \longrightarrow & V(f) = \{t \in \mathbb{C} \mid f(t) = 0\} \\ z = (z_1, \dots, z_n) & \longmapsto & t = a_1\, z_1 + \cdots + a_n\, z_n, \end{array}$$

and

$$\begin{array}{rcl} V(f) & \longrightarrow & V(I) \\ t & \longmapsto & (g_{z_1}(t), \dots, g_{z_n}(t)), \end{array}$$

Intersection with the polydisk: the algorithm

- Compute a Univariate Representation of $\langle p_1, \ldots, p_m \rangle$

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

- 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 $f(t)$ and $z_i - g_{z_i}(t)$ with respect to t $\rightsquigarrow$ **e.g:** via Möbius transform.

Polydisk nullstellensatz theorem

- Goal: A constructive proof for the following theorem

Theorem

Let $I := \langle p_1, \ldots, p_m \rangle$ *be a zero-dimensional ideal such that*

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

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

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

The existing approach: [Xu et al. 94]

- For each z_i, compute the elimination polynomial

$$\langle R_{z_i} \rangle = I \cap \mathbb{Q}[z_i]$$

- Factorize each $R_{z_i} = R_{s,z_i} \times R_{u,z_i}$ such that

$$R_{s,z_i}(\alpha) = 0 \implies |\alpha| > 1 \quad \text{and} \quad R_{u,z_i}(\beta) = 0 \implies |\beta| \leq 1$$

- Construct the polynomial $s = \prod_{i=1}^{n} R_{s,z_i}$
- s vanishes at all the zeros of $I \Rightarrow$ one can compute polynomials $u_1, \ldots, u_m \in \mathbb{Q}[z_1, \ldots, z_n]$ s.t.

$$s = \sum_{i=1}^{m} u_i\, p_i$$

- Problem: **Not effective**

$R(z_i)$ can be irreducible $\rightsquigarrow$ factorization in $\mathbb{C}[z_i]$!

Our approach

- Idea: Apply the previous approach on a system whose solutions are rational approximations of the solutions of I

1. Compute rational approximations of the solutions of I
2. Compute the corresponding polynomials R_{s,z_i} in $\mathbb{Q}[z_i]$
3. Compute the cofactors u_i in the nullstellensatz relation
4. Use these cofactors to deduce the polynomial s

- Start with a Univariate Representation of $I = \langle p_1, \ldots, p_m \rangle$
- Let $I_r := \langle f, z_1 - g_{z_1}, \ldots, z_n - g_{z_n} \rangle \subset \mathbb{Q}[t, z_1, \ldots, z_n]$

Our approach

- Compute $\widetilde{f}(t) = \prod_{k=1}^{n} (t - \widetilde{\gamma}_k)$ where $\widetilde{\gamma}_k$ are rational approximations of the roots of f
- For each z_i compute $\widetilde{R}_{s,z_i} = \prod (z_i - g_{z_i}(\widetilde{\gamma}_k))$ such that $|g_{z_i}(\widetilde{\gamma}_k)| > 1$
- All the $\widetilde{R}_{s,z_i}$ are now in $\mathbb{Q}[z_i]$
- Compute the product of $\widetilde{R}_{s,z_i}$, $\widetilde{s} = \prod_{i=1}^{n} \widetilde{R}_{s,z_i}$

$\implies \widetilde{s} \in \langle \widetilde{f}, z_1 - g_{z_1}, \ldots, z_n - g_{z_n} \rangle$,

$\implies \exists\ \widetilde{u}_0, \widetilde{u}_1, \ldots, \widetilde{u}_n \in \mathbb{Q}[t, z_1, \ldots, z_n]$ such that

$$\widetilde{s} = \widetilde{u_0}\,\widetilde{f} + \sum_{i=1}^{n} \widetilde{u}_i (z_i - g_{z_i})$$

Main result

- Let $\epsilon > 0$ be such that $\max_{k\in\{1,\dots,n\}}(|\gamma_k - \widetilde{\gamma}_k|) < \epsilon$
- $\widetilde{u}_{i,\epsilon}, \widetilde{f}_\epsilon$ and $\widetilde{s}_\epsilon$ are the previous approximated polynomials *wrt* ϵ

Theorem

1. *The polynomial* $s = \widetilde{s}_\epsilon - \widetilde{u}_{0,\epsilon}\,(\widetilde{f}_\epsilon - f)$ *belongs to the ideal* I_r.
2. *There exists* $\epsilon > 0$ *such that* $s(\sum_{i=1}^{n} a_i\, z_i, z_1, \dots, z_n)$ *has no zeros in the* $\overline{\mathbb{U}}^n$.

Algorithm: For successive small ϵ

- Compute the polynomial s
- Check that $V_{\mathbb{C}}(s) \cap \overline{\mathbb{U}}^n = \emptyset$ [B. et al. 15]

Sketch of proof

1. $s = \tilde{s}_\epsilon - \tilde{u}_{0,\epsilon}\,(\tilde{f}_\epsilon - f) = \sum_{i=1}^{n} \tilde{u}_{i,\epsilon}\,(z_i - g_{z_i}) + \tilde{u}_{0,\epsilon}\, f$, so that s vanishes on $V(I_r)$, which implies $s \in I_r$
2. We prove that $\forall \lambda \in \overline{\mathbb{U}}^n$, $|s(\lambda)| > 0$

   On the one hand,

   $$\forall \lambda \in \overline{\mathbb{U}}^n, |\tilde{u}_{0,\epsilon}(\lambda)(\tilde{f}_\epsilon(\lambda) - f(\lambda))| \leq \epsilon\,\rho\,\delta$$

   where ρ (resp., δ) does not depend on ϵ.

   On the other hand,

   $$\forall\ \lambda \in \overline{\mathbb{U}}^n,\ |\tilde{s}_\epsilon(\lambda)| \geq (m - \epsilon)^d.$$

   $\Rightarrow$ for sufficiently small ϵ,

   $$\begin{aligned} \forall \lambda \in \overline{\mathbb{U}}^n,\ |s(\lambda)| &\geq |\tilde{s}_\epsilon(\lambda)| - |\tilde{u}_{0,\epsilon}(\lambda)(\tilde{f}_\epsilon(\lambda) - f(\lambda))| \\ &\geq (m - \epsilon)^d - \epsilon\,\rho\,\delta \\ &> 0. \end{aligned}$$

Example

- $I = \langle p_1, p_2 \rangle$ where $p_1 = z_1^2 - 2\,z_1 - 2$ and $p_2 = z_1 + z_2 - 2$
- Both p_1 and p_2 have zeros inside $\overline{\mathbb{U}}^2$
- $V(I) : \{(1-\sqrt{3}, 1+\sqrt{3}), (1+\sqrt{3}, 1-\sqrt{3})\} \rightsquigarrow V(I) \cap \overline{\mathbb{U}}^2 = \emptyset$
- The elimination polynomials $z_i^2 - 2\,z_i - 2$ are irreducible in $\mathbb{Q}[z_i]$
- A univariate representation of I is given by

$$f(t) := t^2 - 2\,t - 2 = 0, \quad z_1 = t, \quad z_2 = 2 - t.$$

The roots of $f(t)$ are $\gamma_1 \approx -0.73$ and $\gamma_2 \approx 2.73$

Set $\epsilon = \frac{1}{2}$, we get the approximate roots (in $\mathbb{Q}$) $\widetilde{\gamma}_1 = -\frac{1}{2}$ and $\widetilde{\gamma}_2 = 3$

which yields the approximated polynomials

$$\widetilde{f}(t) = \left(t + \frac{1}{2}\right)(t-3), \quad \widetilde{s}(z_1, z_2) = (z_1 - 3)\left(z_2 - \frac{5}{2}\right)$$

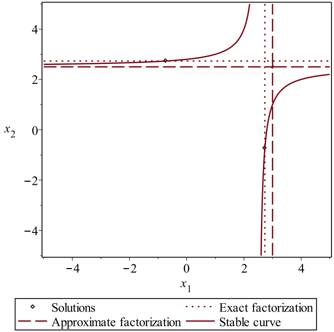
Example (next)

From the previous polynomials, we obtain

$$u_0(t) = -1, \quad (\widetilde{f} - f)(t) = -\frac{1}{2}\,t + \frac{1}{2}.$$

Finally, after substituting $t = z_1$ in $\widetilde{f} - f$, we get:

$$s(z_1, z_2) = z_1\,z_2 - 3\,z_1 - 3\,z_2 + 8.$$



Conclusion and futur work

- Complete Maple implementation
- Investigate the size of the output wrt the distance of the solutions from the polydisk
- Tackle the general polydisk nullstellensatz problem $\rightsquigarrow$ Ideals with arbitrary dimension.
- Small part of a larger module theory over the ring of rational fractions with no poles in the unit polydisk

$$A := \{\frac{r}{s} \mid 0 \neq s, r \in \mathbb{R}[z_1, \ldots, z_n], V_{\mathbb{C}}(s) \cap \overline{\mathbb{U}}^n = \emptyset\}$$

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

[Deligne thm]: Projectivity $\implies$ freeness (no constructive proof)

Conclusion and futur work

- Complete Maple implementation

- Investigate the size of the output wrt the distance of the solutions from the polydisk

- Tackle the general polydisk nullstellensatz problem $\rightsquigarrow$ Ideals with arbitrary dimension.

- Small part of a larger module theory over the ring of rational fractions with no poles in the unit polydisk

$$A := \{\frac{r}{s} \mid 0 \neq s, r \in \mathbb{R}[z_1, \dots, z_n], V_{\mathbb{C}}(s) \cap \overline{\mathbb{U}}^n = \emptyset\}$$

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

[Deligne thm]: Projectivity $\implies$ freeness (no constructive proof)

Thank you

Extension to systems with arbitrary dimension