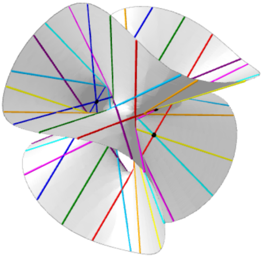
Numerical Algebraic Geometry and Certification

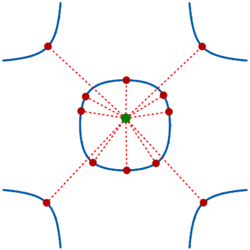
Oskar Henriksson
University of Copenhagen

December 18, 2022

Plan for the week

- Introduction to numerical algebraic geometry, with emphasis on computational tools in Julia, and the basic underlying ideas.
- This lecture: Background and **certification**.
- Tuesday session: **Homotopy continuation** and exercises.





Images from: `https://analyticphysics.com/`

P. Breiding, F. Sottile, J. Woodcock. Euclidean distance degree and mixed volume. *Found. Comput. Math.* (2022).

What is Numerical Algebraic Geometry?

Our goal is to solve polynomial systems over the complex numbers:

$$\begin{cases} f_1(x_1,\dots,x_n) = 0 \\ \vdots \\ f_m(x_1,\dots,x_n) = 0 \end{cases} \qquad F = (f_1,\dots,f_m) \in (\mathbb{C}[x_1,\dots,x_n])^m\,.$$

We want an explicit description of $\mathbb{V}(f_1,\dots,f_m) \subseteq \mathbb{C}^n$:

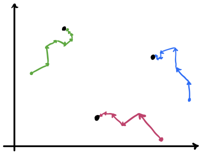
- How many solutions are there?
- If **finitely many**, find rational approximations of all solutions.
- If **infinitely many**, find sample points and describe the geometry (dimension, irreducible components, etc.).

Numerical algebraic geometry does this by combining *algebra* and *numerics*!

Methods for approximating solutions

Newton's method:

$$x^{(n+1)} = x^{(n)} - \left(\frac{\partial F}{\partial x}\right)^{-1} F(x^{(n)})$$



Elimination (Week 3):

$$\begin{cases} x^2 + y^2 + z^2 - 4 = 0 \\ x^2 + 2y^2 - 5 = 0 \\ xz - 1 = 0 \end{cases} \rightsquigarrow \begin{cases} x - 3z + 2z^3 = 0 \\ y^2 - z^2 - 1 = 0 \\ 2z^4 - 3z^2 + 1 = 0 \end{cases}$$

Eigenvalues of multiplication matrices (Week 4):

$$\begin{cases} 1 + x - y - xy = 0 \\ 1 - x + 2y = 0 \end{cases} \rightsquigarrow m_x = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad m_y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Homotopy continuation (Tuesday).

The certification problem

Suppose that we have approximate solutions $\xi^{(1)}, \ldots, \xi^{(k)} \in \mathbb{C}^n$ of a system

$$F = (f_1, \ldots, f_m) \in (\mathbb{C}[x_1, \ldots, x_n])^m .$$

What can we say about the true solutions that $\xi^{(1)}, \ldots, \xi^{(k)}$ approximate?

- How big is the **approximation error**?
- Do they approximate **distinct** true solutions?
- Are any of the true solutions **real**?
- Are any of the true solutions **positive**?

Example: The univariate $f(x) = x^3 - 4x - 5$ with approximations

$\xi^{(1)} =$ `-1.228339171522055 + 0.7255696802419939im`

$\xi^{(2)} =$ `-1.228339171522054 - 0.725569680241994im`

$\xi^{(3)} =$ `2.456678343044111 - 3.851859888774472e-18im`.

The `certify` feature in `HomotopyContinuation.jl` can answer these questions, **with rigorous proofs**!

The certification problem

Suppose that we have approximate solutions $\xi^{(1)}, \ldots, \xi^{(k)} \in \mathbb{C}^n$ of a system

$$F = (f_1, \ldots, f_m) \in (\mathbb{C}[x_1, \ldots, x_n])^m .$$

What can we say about the true solutions that $\xi^{(1)}, \ldots, \xi^{(k)}$ approximate?

- How big is the **approximation error**?
- Do they approximate **distinct** true solutions?
- Are any of the true solutions **real**?
- Are any of the true solutions **positive**?

```
using HomotopyContinuation
@var x
F = System([x^3-4*x-5])
approximations = [[-1.2283391715220555 + 0.7255696802419939im],[-1.2283391715220554 - 0.72556968024199
cert = certify(F,approximations)
```

```
CertificationResult
===================
• 3 solution candidates given
• 3 certified solution intervals (1 real, 2 complex)
• 3 distinct certified solution intervals (1 real, 2 complex)
```

How does `certify` do this (roughly speaking)?

Input:

- A square polynomial system $F = (f_1, \ldots, f_n) \in (\mathbb{C}[x_1, \ldots, x_n])^n$.
- A list of approximations of solutions $\xi^{(1)}, \ldots, \xi^{(k)} \in \mathbb{C}^n$.

Step 1: Refine each $\xi^{(i)}$ with Newton's method to better approximation $\tilde{\xi}^{(i)}$.

Step 2: For each $\tilde{\xi}^{(i)}$, construct a well-chosen small box

$$I^{(i)} = \left(\tilde{\xi}_1^{(i)} \pm \varepsilon_1^{(i)}\right) \times \left(\tilde{\xi}_2^{(i)} \pm \varepsilon_2^{(i)}\right) \times \cdots \times \left(\tilde{\xi}_n^{(i)} \pm \varepsilon_n^{(i)}\right) \subseteq \mathbb{C}^n$$

and prove (using *interval arithmetic*) the following properties:

- Each $I^{(i)}$ contains **precisely one** true solution of the system.
- Newton's method **converges** to the true solution from any point in $I^{(i)}$.

Output: The boxes $I^{(1)}, \ldots, I^{(k)}$, plus some extra info (for instance data that makes it possible to verify that each box contains preicely one solution).

Drawing conclusions from the boxes

Running example: The univariate $f(x) = x^3 - 4x - 5$ with approximations

$$\xi^{(1)} = \texttt{-1.228339171522055 + 0.7255696802419939im}$$

$$\xi^{(2)} = \texttt{-1.228339171522054 - 0.725569680241994im}$$

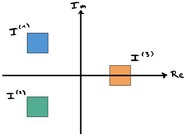
$$\xi^{(3)} = \texttt{2.456678343044111 - 3.851859888774472e-18im}.$$

```
cert = certify(F,approximations)
for c in certificates(cert)
    display( certified_solution_interval(c) )
end
```

```
1×1 Arblib.AcbMatrix:
 [-1.228339171522 +/- 5.14e-13] + [0.725569680242 +/- 4.64e-13]im

1×1 Arblib.AcbMatrix:
 [-1.228339171522 +/- 5.14e-13] + [-0.725569680242 +/- 4.64e-13]im

1×1 Arblib.AcbMatrix:
 [2.456678343044 +/- 5.95e-13] + [+/- 4.84e-13]im
```



Proposition

- If $I^{(i)} \cap I^{(j)} = \varnothing$, then $\xi^{(i)}$ and $\xi^{(j)}$ approximate **distinct** true solutions.
- If $I^{(i)} \cap \mathbb{R}^n = \varnothing$, then $\xi^{(i)}$ approximates a **nonreal** solution.

Left to answer: How can we prove that a $\xi^{(i)}$ approximates a real solution?

Strategy for certifying reality (sketch)

Let $F = (f_1, \dots, f_n) \in (\mathbb{R}[x_1, \dots, x_n])^n$, let $\xi \in \mathbb{C}^n$ be an approximation of a root.
Let $I \subseteq \mathbb{C}^n$ be a box with $\xi \in I$, where we have verified that there is a unique root.

Let's call this unique root s. We want to show that $s \in \mathbb{R}^n$.

Key observation: Since the system has **real coefficients**, $\bar{s}$ is also a root.

The way `certify` tries to do this is as follows:

- Use Newton's method to shrink I to a smaller set $J \subseteq I$ with $s \in J$.
- Let $\bar{J}$ be the elementwise conjugate.
- Check if $\bar{J} \subseteq I$.
- If yes, then $\bar{s} \in I$ (since $\bar{s} \in \bar{J}$).
- But s was by assumption the unique root in I.
- Hence $\bar{s} = s$, which shows that $s \in \mathbb{R}^n$.

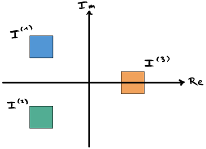
Certifying reality in practice

```
cert = certify(F,approximations)
for c in certificates(cert)
    display( is_real(c) )
end
```

```
false

false

true
```



- The command `is_real` returns **true** on the ith element of `certificates(cert)` if we were able to verify that $\xi^{(i)}$ approximates a real true solution.

  In this case, we have a *proof* that $\xi^{(i)}$ approximates a real true solution.
- It returns **false** if the program failed to certify reality.

  This does *not* necessarily mean that $\xi^{(i)}$ approximates a nonreal solution. To prove this, we should instead try to show $I^{(i)} \cap \mathbb{R}^n = \varnothing$.

Proposition

Suppose $\xi^{(i)}$ approximates a real true solution. Then that solution is contained in the real part $\mathrm{Re}(I^{(i)}) \subseteq \mathbb{R}^n$. In particular, if $\mathrm{Re}(I^{(i)}) \subseteq \mathbb{R}^n_{>0}$, then the true solution must be positive.

Summary

Given a system $F = (f_1, \ldots, f_n) \in (\mathbb{C}[x_1, \ldots, x_n])^n$ with finitely many solutions, numerical algebraic geometry attempts to describe $\mathbb{V}(f_1, \ldots, f_n) \subseteq \mathbb{C}^n$ with the help of rational approximations.

Common approximation methods: Newton's method, elimination, eigenvalues of multiplication matrices, homotopy continuation...

The `certify` command in `HomotopyContinuation.jl` provides **provable** information about the *true solutions* that our approximations approximate, concerning distinctness, reality and positivity.

- The `certify` commands can be used for **any** list of approximate solutions. They don't necessarily have to come from homotopy continuation.
- Certification won't tell us whether we have found **all** solutions to our system. To say something about this we need an **upper bound** on $\#\mathbb{V}(f_1, \ldots, f_n)$, e.g.

$$\#\mathbb{V}(f_1, \ldots, f_n) \leqslant \dim_{\mathbb{C}}\left(\frac{\mathbb{C}[x_1,\ldots,x_n]}{\langle f_1,\ldots,f_n\rangle}\right) ,$$

  or the Bézout bound (Tuesday), or the mixed volume (Week 7).