Certificates in Numerical Algebraic Geometry

Jan Verschelde

University of Illinois at Chicago
Department of Mathematics, Statistics, and Computer Science
http://www.math.uic.edu/~jan
jan@math.uic.edu

FoCM'08 Real Number Complexity Workshop
City University of Hong Kong, June 16-18, 2008

Outline

Problem Statement

about numerically solving polynomial systems

Given a polynomial system:

$$f(\mathbf{x}) = \mathbf{0} \qquad \begin{aligned} f &= (f_1, f_2, \ldots, f_N) \\ \mathbf{x} &= (x_1, x_2, \ldots, x_n) \end{aligned}$$

and numerical representations of solutions,
as output of some software,
then we ask

1. how can a user verify the computed solutions?
2. how should a program certify the computed solutions?

Some Samples of Questions
users of PHCpack

A program works when the author is using it.
$\leftrightarrow$ Software gives meaningful answers to general users,
with backgrounds often vastly different than programmers.

PHCpack is software which returns numerical solutions.

- Dhagash Mehta (U. of Adelaide): particle physics
  $\rightarrow$ confirm results after tracking 772,063 solution paths?
- Christian Stump (U. of Vienna): equiareal triangulations
  $\rightarrow$ algebraic expressions for all real solutions?
- Sergei Stepanchuk (U. of Pennsylvania): equilibria in markets
  $\rightarrow$ there seems to be a solution curve of multiplicity two?

Of a benchmark system we know the solution, but we
do not know the answers for systems arising in applications.

Global and Local Questions
and some partial answers

Global questions:

- what are the dimensions of the solutions?
- for each dimension what are the degrees?

Local questions:

- is the solution isolated or not?
- what is the multiplicity structure?

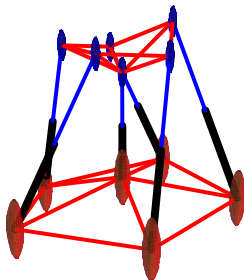Some partial answers:

1. root counts (Bézout, Bernshteĭn-Kushnirenko-Khovanskiĭ)
2. multiprecision arithmetic; apply alpha theory

For applications we often need *apriori* certificates
before committing to lengthy calculations and investigations.

Example I: the Stewart-Gough platform

forty isolated solutions

end plate, the platform

is connected by legs to

a stationary base

Forward Displacement Problem:
>   Given: position of base and leg lengths.
>   Wanted: position of end plate.

Input: 8 quadratic equations in 8 unknowns.

Solving the Forward Displacement Problem
using an optimal multihomogeneous homotopy

C.W. Wampler. **Forward displacement analysis of general six-in-parallel SPS (Stewart) platform manipulators using soma coordinates.** *Mech. Mach. Theory* 31(3), 331–337, 1996.

The setup leads to a multihomogeneous homotopy with 80 paths.
Sign symmetry: 40 generating solutions.

The multihomogeneous Bézout bound shows #isolated roots ≤ 40.

A generic Stewart-Gough platform has 40 isolated complex solutions.
Numerical justification:

1. choose generic values for the parameters of the platform,
2. solve the system using a multihomogeneous homotopy,
3. show that all solutions are approximate roots.

Certifying Isolated Solutions

Mina Khan Master Thesis 2007

Following α-theory of Shub & Smale:

$$\gamma(f,\zeta) = ||\zeta|| \max_{k>1} \left\| Df(\zeta)^{-1} \frac{D^k f(\zeta)}{k!} \right\|^{1/(k-1)},$$

for ζ a solution of f. Then

$$r = \frac{3 - \sqrt{7}}{2\gamma(f,\zeta)} \text{ is radius of convergence.}$$

Evaluate r for forward displacement platform: r is 10^{-4}.
Some comments on the computations:

- use of Maple's multiprecision arithmetic
- for quadratics: stop at $k = 2$ in $\gamma(f,\zeta)$
- choice of compactification influences $|| \cdot ||$

Example II: the Griffis-Duffy platform
architecturally singular platforms move

M. Griffis and J. Duffy: *Method and apparatus for controlling geometrically simple parallel mechanisms with distinctive connections.* US Patent 5,179,525, 1993.
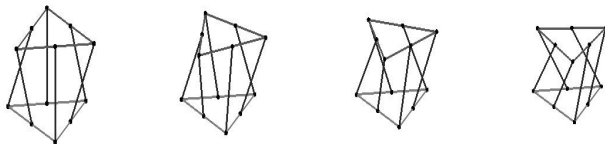
Input: 7 quadrics and one linear equation in 8 unknowns.

Representing Solution Curves

Given a polynomial system:

$$f(\mathbf{x}) = \mathbf{0} \qquad \begin{aligned} f &= (f_1, f_2, \ldots, f_n) \\ \mathbf{x} &= (x_1, x_2, \ldots, x_n) \end{aligned}$$

Let z be a slack variable. Choose

1. n random multiplier variables $\gamma \in \mathbb{C}^{n \times 1}$; and
2. $n + 1$ coefficients of a general hyperplane.

Then the embedding $\mathcal{E}(f)$ of f is

$$\mathcal{E}(f) = \left\{ \begin{aligned} f(\mathbf{x}) + \gamma z &= \mathbf{0} \\ c_0 + c_1 x_1 + \cdots + c_n x_n + z &= 0 \end{aligned} \right.$$

Solve $\mathcal{E}(f) = \mathbf{0}$: we find 40 isolated solutions.
Move general hyperplane to sample the solution curve.

Positive Dimensional Solution Sets
represented numerically by witness sets

Given a system $f(\mathbf{x}) = \mathbf{0}$, we represent
a component of $f^{-1}(\mathbf{0})$ of dimension k and degree d by

- k general hyperplanes L to cut the dimension; and
- d generic points in $f^{-1}(\mathbf{0}) \cap L$.

Witness set representations reduce to isolated solutions,
for which the same α-theory applies.

Using a flag of linear spaces, defined by an decreasing sequence of
subsets of the k general hyperplanes,

$$L = L_k \supset L_{k-1} \supset \cdots \supset L_1 \supset L_0 = \emptyset,$$

we move solutions with nonzero slack values to generic points on
lower dimensional components, using a cascade of homotopies.

Problem Statement
some wishful thinking...

Computing witness sets is more expensive than isolated solutions.

A solver cannot assume the user cares only about isolated solutions.

To justify longer execution times and more elaborate homotopies, how do we show *quickly* there are positive dimensional solution sets?

The certificate should be *compact* and have a short representation. The user should be able to manipulate the certificate in any computer algebra or scientific software system.

A Tropical View
joint with Danko Adrovic

Three observations:

1. If there is a positive dimensional solution set,
   then it stretches out to infinity.
   We tropicalize the polynomials in the system.

2. Bernshteĭn 2nd theorem: solutions at infinity are solutions of
   systems supported on faces of the Newton polytopes.
   Tropisms identify those faces.

3. Solutions at infinity give the leading coefficients of Puiseux series.
   The next term in a Puiseux series gives a certificate.

Tropisms and the first terms of a Puiseux series expansion
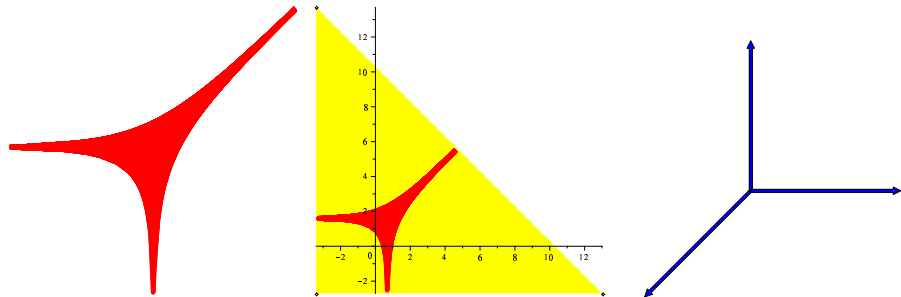give apriori certificates for a solution component.

Tropicalizations of Polynomials

an asymptotic view on algebraic varieties (G.M. Bergman 1971)

Definition (Gel'fand, Kapranov, and Zelevinsky 1994)

The ***amoeba*** of a variety is its image under the map log:
$(\mathbb{C}^*)^n \to \mathbb{R}^n : \mathbf{x} \mapsto \log(|\mathbf{x}|), \log(|\mathbf{x}|) = (\log(|x_1|), \log(|x_2|), \ldots, \log(|x_n|))$.

The tentacles of the amoeba are encoded in the inner normals,
i.e.: vectors perpendicular to the edges of the Newton polytope.

Inner Normals represent Tentacles

$$f := x^3y + x^2y^3 + x^5y^3 + x^4y^5 + x^2y^7 + x^3y^7$$
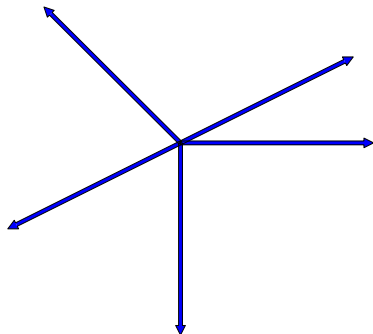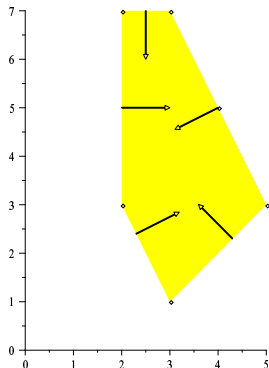
The collection of inner normals to the edges of the Newton polygon forms **a tropicalization** of f.

Normal Fan
a tropicalization of a polynomial

> **Definition**
>
> Let P be the Newton polytope of f.
> The ***normal cone to a vertex p of P*** is
>
> $$\{\, v \neq 0 \mid \langle p, v \rangle = \min_{q \in P} \langle q, v \rangle \,\}.$$
>
> The ***normal cone to an edge spanned by p_1 and p_2*** is
>
> $$\{\, v \neq 0 \mid \langle p_1, v \rangle = \langle p_2, v \rangle = \min_{q \in P} \langle q, v \rangle \,\}.$$
>
> The ***normal fan*** of P is the collection of all normal cones to vertices and edges of P.
> All normal cones to the edges of P define ***a tropicalization of f***.

Tropisms
for Puiseux expansions (J. Maurer 1980)

screensaver dictionary definition:
the turning of all or part of an organism in a particular direction in response to an external stimulus

Definition

Consider the system $f(\mathbf{x}) = \mathbf{0}$ with $f = (f_1, f_2, \ldots, f_N)$ and $\mathbf{x} = (x_1, x_2, \ldots, x_n)$. Let $(P_1, P_2, \ldots, P_N)$ be the tuple of Newton polytopes of f. A ***tropism*** is a vector perpendicular to one edge of each P_i, for $i = 1, 2, \ldots, N$.

This definition is adapted from Joseph Maurer: *Puiseux expansion for space curves.* Manuscripta Math. 32:91-100, 1980.

Monique Lejeune-Jalabert and Bernard Tessier: *Clôture intégrale des idéaux et équisingularité.* arXiv:0803.2369v1 16 Mar 2008.
First part are notes of a 1973-74 seminar.

Initial Forms

Why are tropisms so important?

Selecting those monomials which span the edges picked out by the tropism defines a polynomial system which admit a solution in $(\mathbb{C}^*)^n$.

Definition

Let $\mathbf{v}$ be a direction vector. Consider $f = \displaystyle\sum_{\mathbf{a} \in A} c_\mathbf{a} \mathbf{x}^\mathbf{a}$.

The ***initial form of f in the direction $\mathbf{v}$*** is

$$\text{in}_\mathbf{v}(f) = \sum_{\substack{\mathbf{a} \,\in\, A \\ \langle \mathbf{a}, \mathbf{v} \rangle = m}} c_\mathbf{a} \mathbf{x}^\mathbf{a},$$

where $m = \min\{\ \langle \mathbf{a}, \mathbf{v} \rangle \mid \mathbf{a} \in A\ \}$.

Bernshteĭn's Second Theorem 1975

rephrased in the tropical language

Theorem (Bernshteĭn Theorem B 1975)

Consider $f(\mathbf{x}) = \mathbf{0}$, $f = (f_1, f_2, \ldots, f_n)$, $\mathbf{x} = (x_1, x_2, \ldots, x_n)$.
Denote by $\mathcal{P}$ the tuple of Newton polytopes of f.
If for all tropisms $\mathbf{v}$: $\mathrm{in}_\mathbf{v}(f)(\mathbf{x}) = \mathbf{0}$ has no solutions in $(\mathbb{C}^*)^n$,
then $f(\mathbf{x}) = \mathbf{0}$ has exactly as many isolated solutions in $(\mathbb{C}^*)^n$
as the mixed volume of $\mathcal{P}$.

- No tropisms $\mathbf{v}$: $\mathrm{in}_\mathbf{v}(f)(\mathbf{x}) = \mathbf{0}$ has roots in $(\mathbb{C}^*)^n$
  $\Rightarrow$ no solutions at infinity.

Solutions at infinity are roots of $\mathrm{in}_\mathbf{v}(f)(\mathbf{x}) = \mathbf{0}$.

— —

Complexity of Bernshteĭn's first theorem:
  G. Jeronimo, G. Matera, P. Solernó, and A. Waissbein: **Deformation
    Techniques for Sparse Systems.** To appear in *Found. Comput. Math.*

Tropical Algebraic Geometry
a new language describing asymptotics of varieties

Polyhedral methods in a tropical world:

1. tropicalizations of polynomials and polytopes

   ▶ amoebas are images of varieties under the log map
   ▶ a Newton polytope P is a compactification of an amoeba

   $\rightarrow$ a tropicalization is an inner normal fan of P

2. tropisms

   ▶ are in the intersection of normal cones
     to the edges of the lifted polytopes
   ▶ give the leading powers to the Puiseux expansions
     for the start of the solution curves

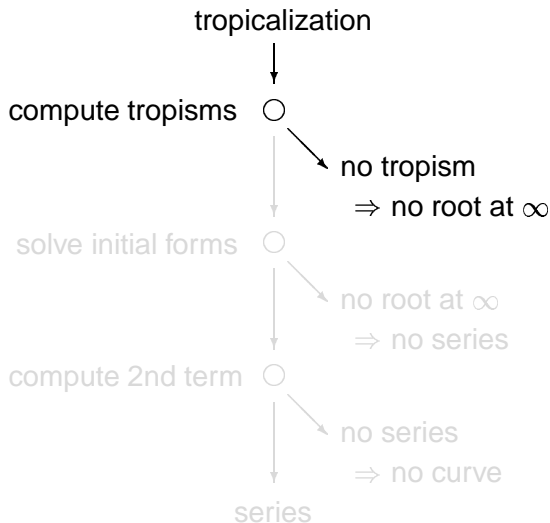**J. Maurer:** Puiseux expansion for space curves.
Manuscripta Math. 32: 91–100, 1980.

towards a polyhedral method for curves . . .

Computing a Series Expansion

a staggered approach to find a certificate for a solution curve

tropicalization

compute tropisms ◯

no tropism
⇒ no root at ∞

solve initial forms ◯

no root at ∞
⇒ no series

compute 2nd term ◯

no series
⇒ no curve

series

Computing a Series Expansion

a staggered approach to find a certificate for a solution curve

tropicalization

compute tropisms $\bigcirc$

> no tropism
> $\Rightarrow$ no root at ∞

solve initial forms $\bigcirc$

> no root at ∞
> $\Rightarrow$ no series

compute 2nd term $\bigcirc$

> no series
> $\Rightarrow$ no curve

series

Computing a Series Expansion

a staggered approach to find a certificate for a solution curve

tropicalization

compute tropisms ○

no tropism
$\Rightarrow$ no root at ∞

solve initial forms ○

no root at ∞
$\Rightarrow$ no series

compute 2nd term ○
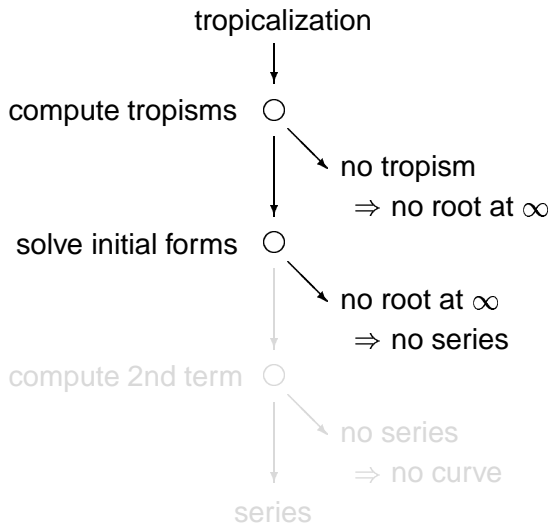
no series
$\Rightarrow$ no curve

series
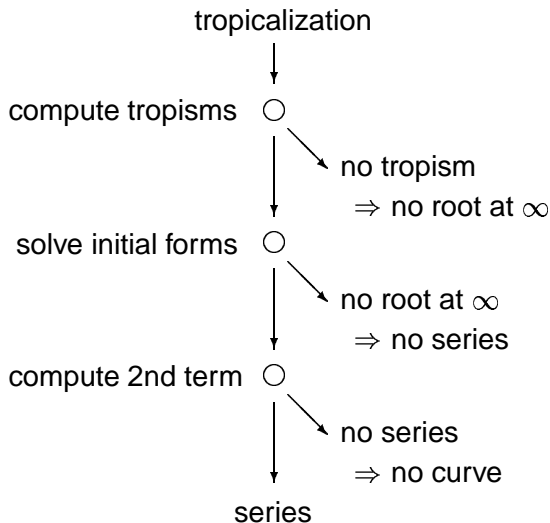
the cyclic 8-roots system
a well known benchmark problem

a system of 8 equations in 8 unknowns:

$$
f(\mathbf{z}) = \begin{cases}
z_0 + z_1 + z_2 + z_3 + z_4 + z_5 + z_6 + z_7 = 0 \\
z_0 z_1 + z_1 z_2 + z_2 z_3 + z_3 z_4 + z_4 z_5 + z_5 z_6 + z_6 z_7 + z_7 z_0 = 0 \\
i = 3, 4, \ldots, 7 : \sum_{j=0}^{7} \prod_{k=j}^{i} z_{k \bmod 8} = 0 \\
z_0 z_1 z_2 z_3 z_4 z_5 z_6 z_7 - 1 = 0
\end{cases}
$$

J. Backelin: "Square multiples n give infinitely many cyclic n-roots".
Reports, Matematiska Institutionen, Stockholms Universitet, 1989.
$n = 8$ has 4 as divisor, $4 = 2^2$, so infinitely many roots

how to verify numerically?

Tropisms coming from Endgames

Directions of diverging paths for cyclic 8-roots:

tropisms	m	accuracy	#paths
$\pm(-1, 1, -1, 1, -1, 1, -1, 1)$	1	10^{-3}	32
$\pm(-1, 0, 0, 1, 0, -1, 1, 0)$	1	10^{-7}	8
$\pm(0, -1, 0, 0, 1, 0, -1, 1)$	1	10^{-6}	8
$\pm(1, 0, -1, 0, 0, 1, 0, -1)$	1	10^{-7}	8
$\pm(-1, 1, 0, -1, 0, 0, 1, 0)$	1	10^{-6}	8
$\pm(0, -1, 1, 0, -1, 0, 0, 1)$	1	10^{-6}	8
$\pm(1, 0, -1, 1, 0, -1, 0, 0)$	1	10^{-7}	8
$\pm(0, 1, 0, -1, 1, 0, -1, 0)$	1	10^{-6}	8
$\pm(0, 0, 1, 0, -1, 1, 0, -1)$	1	10^{-6}	8

Every tropism **v** defines an initial form $\text{in}_{\mathbf{v}}(f)$.
Every equation in $\text{in}_{\mathbf{v}}(f)$ has at least two monomials
$\Rightarrow$ admits a solution with all components nonzero.

An Initial Form of the cyclic 8-roots system

For the tropism $\mathbf{v} = (-1, 0, 0, +1, 0, -1, +1, 0)$:

$$
\text{in}_{\mathbf{v}}(f)(\mathbf{z}) = \begin{cases}
z_0 + z_5 = 0 \\
z_0 z_1 + z_4 z_5 + z_7 z_0 = 0 \\
z_0 z_1 z_2 + z_7 z_0 z_1 = 0 \\
z_5 z_6 z_7 z_0 + z_7 z_0 z_1 z_2 = 0 \\
z_4 z_5 z_6 z_7 z_0 + z_5 z_6 z_7 z_0 z_1 = 0 \\
z_0 z_1 z_2 z_3 z_4 z_5 + z_4 z_5 z_6 z_7 z_0 z_1 + z_5 z_6 z_7 z_0 z_1 z_2 = 0 \\
z_4 z_5 z_6 z_7 z_0 z_1 z_2 + z_7 z_0 z_1 z_2 z_3 z_4 z_5 = 0 \\
z_0 z_1 z_2 z_3 z_4 z_5 z_6 z_7 - 1 = 0
\end{cases}
$$

Observe: for all $\mathbf{z}^{\mathbf{a}}$: $\langle \mathbf{a}, \mathbf{v} \rangle = -1$,
except for the last equation: $\langle \mathbf{a}, \mathbf{v} \rangle = 0$.

Transforming Coordinates
to eliminate one variable

The tropism $\mathbf{v} = (-1, 0, 0, +1, 0, -1, +1, 0)$ defines a change of coordinates:

$$\begin{cases} z_0 = x_0^{-1} \\ z_1 = x_0^0 x_1 \\ z_2 = x_0^0 x_2 \\ z_3 = x_0^{+1} x_3 \\ z_4 = x_0^0 x_4 \\ z_5 = x_0^{-1} x_5 \\ z_6 = x_0^{+1} x_6 \\ z_7 = x_0^0 x_7 \end{cases} \quad \text{in}_{\mathbf{v}}(f)(\mathbf{x}) = \begin{cases} 1 + x_5 = 0 \\ x_1 + x_4 x_5 + x_7 = 0 \\ x_1 x_2 + x_7 x_1 = 0 \\ x_5 x_6 x_7 + x_7 x_1 x_2 = 0 \\ x_4 x_5 x_6 x_7 + x_5 x_6 x_7 x_1 = 0 \\ x_1 x_2 x_3 x_4 x_5 + x_4 x_5 x_6 x_7 x_1 \\ \quad + x_5 x_6 x_7 x_1 x_2 = 0 \\ x_4 x_5 x_6 x_7 x_1 x_2 + x_7 x_1 x_2 x_3 x_4 x_5 = 0 \\ x_1 x_2 x_3 x_4 x_5 x_6 x_7 - 1 = 0 \end{cases}$$

After clearing x_0, $\text{in}_{\mathbf{v}}(f)$ consists of 8 equations in 7 unknowns.

Solving an overconstrained Initial Form

Choose eight random numbers $\gamma_k \in \mathbb{C}$, $k = 1, 2, \ldots, 8$,
to introduce a slack variable s:

$$
\text{in}_{\mathbf{v}}(f)(\mathbf{x}, s) = \begin{cases}
1 + x_5 + \gamma_1 s = 0 \\
x_1 + x_4 x_5 + x_7 + \gamma_2 s = 0 \\
x_1 x_2 + x_7 x_1 + \gamma_3 s = 0 \\
x_5 x_6 x_7 + x_7 x_1 x_2 + \gamma_4 s = 0 \\
x_4 x_5 x_6 x_7 + x_5 x_6 x_7 x_1 + \gamma_5 s = 0 \\
x_1 x_2 x_3 x_4 x_5 + x_4 x_5 x_6 x_7 x_1 + x_5 x_6 x_7 x_1 x_2 + \gamma_6 s = 0 \\
x_4 x_5 x_6 x_7 x_1 x_2 + x_7 x_1 x_2 x_3 x_4 x_5 + \gamma_7 s = 0 \\
x_1 x_2 x_3 x_4 x_5 x_6 x_7 - 1 + \gamma_8 s = 0
\end{cases}
$$

The mixed volume of this system is 25 and is exact.
Among the 25 solutions, there are 8 with $s = 0$.

The first Term of a Puiseux Expansion

For $f(\mathbf{x}) = \text{in}_{\mathbf{e}} f(x) + O(x_0)$, $\mathbf{e} = (1, 0, 0, 0, 0, 0, 0, 0)$,
we use a solution as the leading term of a Puiseux expansion:

$$
\begin{cases}
x_0 = t^1 \\
x_1 = (\ 0.5 + 0.5i\ )\ t^0 & +y_1\ t \\
x_2 = (\ 1 + i\ )\ t^0 & +y_2\ t \\
x_3 = (\ -i\ )\ t^0 & +y_3\ t \\
x_4 = (\ -0.5 - 0.5i\ )\ t^0 & +y_4\ t \\
x_5 = (\ -1\ )\ t^0 & +y_5\ t \\
x_6 = (\ i\ )\ t^0 & +y_6\ t \\
x_7 = (\ -1 - i\ )\ t^0 & +y_7\ t
\end{cases}
\qquad i = \sqrt{-1}.
$$

Decide whether solution is isolated: substitute series in $f(\mathbf{x}) = \mathbf{0}$
and solve for y_k, $k = 1, 2, \ldots, 7$ in lowest order terms of t.
$\rightarrow$ solve an overdetermined linear system in the coefficients
of the 2nd term of the Puiseux expansion.

The second Term of a Puiseux Expansion

Because we find a nonzero solution for the y_k coefficients,
we use it as the second term of a Puiseux expansion:

$$
\begin{cases}
x_0 = t^1 \\
x_1 = (\, 0.5 + 0.5i \,)\, t^0 & + (\, -0.5i \,)\, t \\
x_2 = (\, 1 + i \,)\, t^0 & + (\, -i \,)\, t \\
x_3 = (\, -i \,)\, t^0 & + (\, 1 - i \,)\, t \\
x_4 = (\, -0.5 - 0.5i \,)\, t^0 & + (\, 0.5i \,)\, t \\
x_5 = (\, -1 \,)\, t^0 & + (\, 0 \,)\, t \\
x_6 = (\, i \,)\, t^0 & + (\, -1 + i \,)\, t \\
x_7 = (\, -1 - i \,)\, t^0 & + (\, i \,)\, t
\end{cases}
\qquad i = \sqrt{-1}.
$$

Substitute series in $f(\mathbf{x})$: result is $O(t^2)$.

the cyclic 12-roots problem

According to J. Backelin, also here infinitely many solutions.

Mixed volume is 500,352 and increases to 983,952
by adding one random hyperplane and slack variable.

Like for cyclic 8, $\mathbf{v} = (-1, +1, -1, +1, -1, +1, -1, +1, -1, +1, -1, +1)$
is a tropism. Mixed volume of $\text{in}_{\mathbf{v}}(f)(\mathbf{x}, s) = \mathbf{0}$ is 49,816.
One of the solutions is

$x_0 = t$	$x_1 = 0.5 - 0.866025403784439i$
$x_2 = -1.0$	$x_3 = -0.5 - 0.866025403784439i$
$x_4 = -0.5 + 0.866025403784439i$	$x_5 = 0.5 + 0.866025403784439i$
$x_6 = -1.0$	$x_7 = -0.5 + 0.866025403784438i$
$x_8 = 1.0$	$x_9 = 0.5 + 0.866025403784438i$
$x_{10} = 0.5 - 0.866025403784439i$	$x_{11} = -0.5 - 0.866025403784439i$

It satisfies not only $\text{in}_{\mathbf{v}}(f)$, but also f itself.

An Exact Solution for cyclic 12-roots

For the tropism $\mathbf{v} = (-1, +1, -1, +1, -1, +1, -1, +1, -1, +1, -1, +1)$:

$$z_0 = t^{-1} \qquad\qquad z_1 = t\left(\tfrac{1}{2} - \tfrac{1}{2}i\sqrt{3}\right)$$

$$z_2 = -t^{-1} \qquad\qquad z_3 = t\left(-\tfrac{1}{2} - \tfrac{1}{2}i\sqrt{3}\right)$$

$$z_4 = t^{-1}\left(-\tfrac{1}{2} + \tfrac{1}{2}i\sqrt{3}\right) \quad z_5 = t\left(\tfrac{1}{2} + \tfrac{1}{2}i\sqrt{3}\right)$$

$$z_6 = -t^{-1} \qquad\qquad z_7 = t\left(-\tfrac{1}{2} + \tfrac{1}{2}i\sqrt{3}\right)$$

$$z_8 = t^{-1} \qquad\qquad z_9 = t\left(\tfrac{1}{2} + \tfrac{1}{2}i\sqrt{3}\right)$$

$$z_{10} = t^{-1}\left(\tfrac{1}{2} - \tfrac{1}{2}i\sqrt{3}\right) \quad z_{11} = t\left(-\tfrac{1}{2} - \tfrac{1}{2}i\sqrt{3}\right)$$

makes the system entirely and exactly equal to zero.

Conclusion

An apriori certificate for a solution component consists of

1. a tropism: leading powers of a Puiseux series,
2. a root at infinity: leading coefficients of the Puiseux series,
3. the next term in the Puiseux series.

The certificate is compact and easy to verify with substitution.

Preprocessing for more costly representations:

- either lifting fibers for a geometric resolution,
- or witness sets in a numerical irreducible decomposition.