Certified Numerical Homotopy Continuation

Can a computation using homotopy continuation give a proof?

Anton Leykin

Georgia Tech

Randomization, Relaxation, and Complexity. March 2010.

Polynomial homotopy continuation

- Target system: n equations in n variables,

$$f = (f_1, \ldots, f_n) = \mathbf{0},$$

where $f_i \in R = \mathbb{C}[X_1, ..., X_n]$ for $i = 1, ..., n$.

- Start system: n equations in n variables:

$$g = (g_1, \ldots, g_n) = \mathbf{0},$$

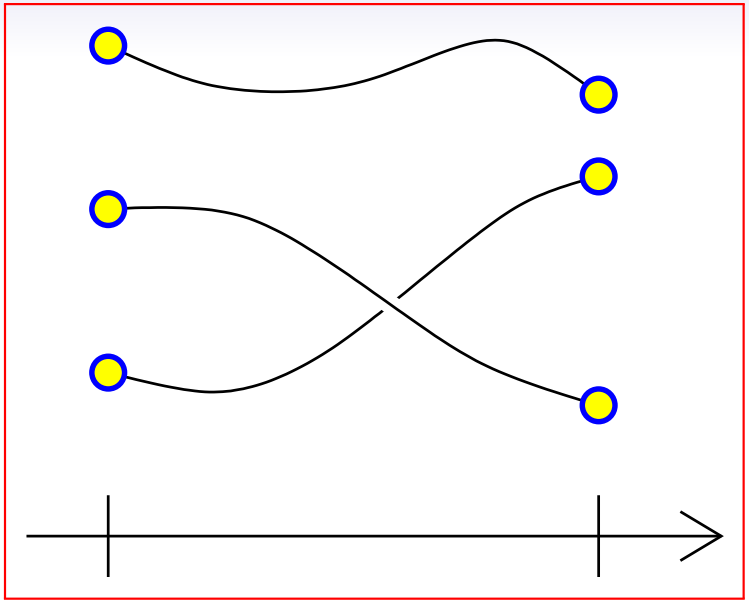
such that it is easy to solve.

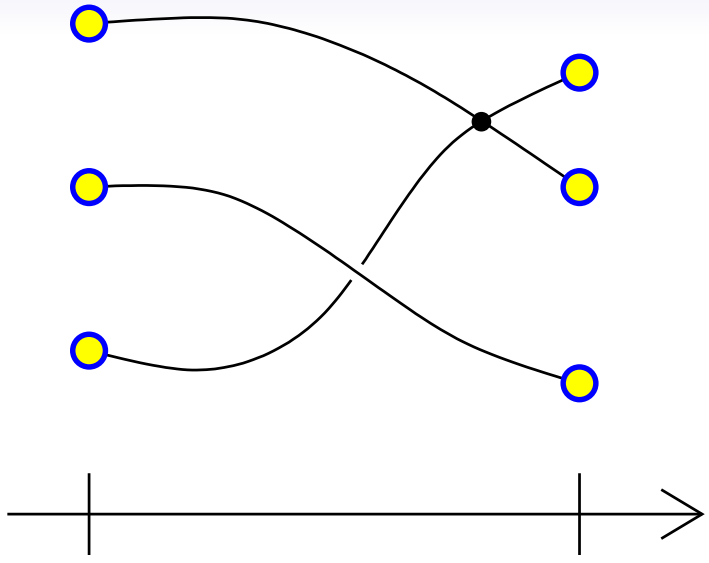
- Homotopy: for $\gamma \in \mathbb{C} \setminus \{0\}$ consider

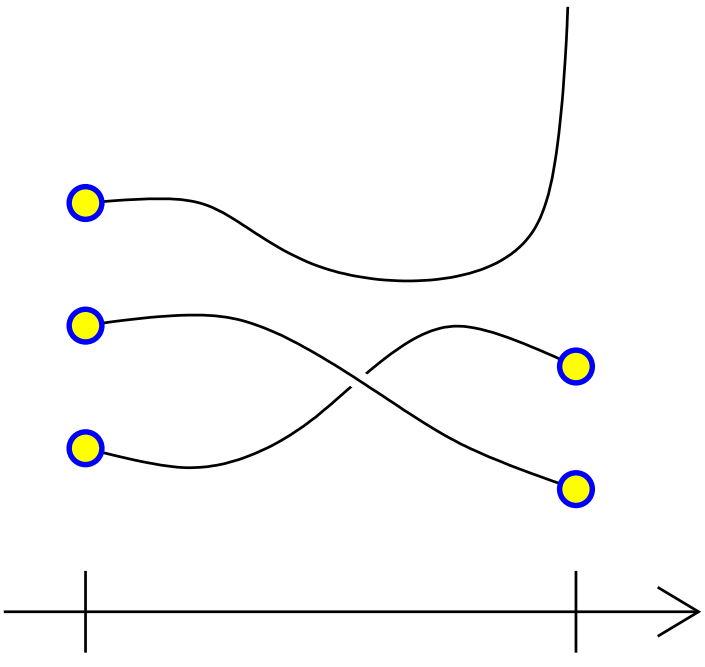
$$h(X, t) = (T - t)g(X) + \gamma t f(X),\ t \in [0, T].$$

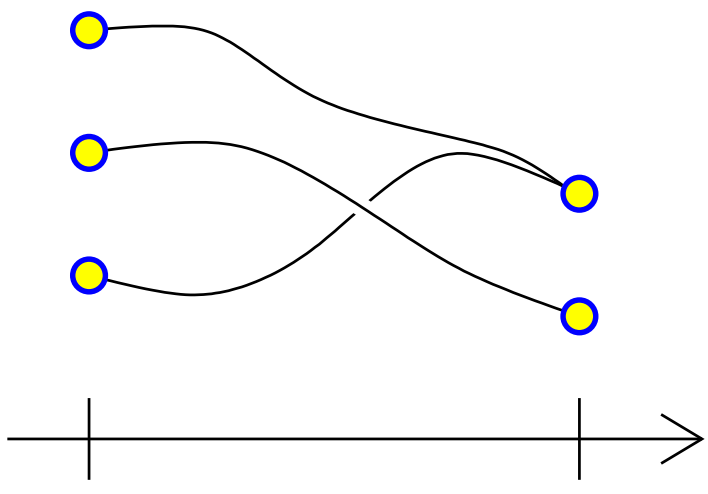
Example (Total-degree homotopy)

		target				start
f_1	$=$	$x_1^4 x_2 + 5x_1^2 x_2^3 + x_1^3 - 4$		g_1	$=$	$x_1^5 - 1$
f_2	$=$	$x_1^2 - x_1 x_2 + x_2 - 8$		g_2	$=$	$x_2^2 - 1$









Numerical algebraic geometry software

- PHCpack (Verschelde);
- Bertini (group of Sommese);
- HOM4PS (group of T.Y.Li).
- NAG4M2, Numerical Algebraic Geometry for Macaulay2 (L.).

Motivation

Certify homotopies in monodromy computations:

- Monodromy breakup in numerical irreducible decomposition.
- Pure math applications, e.g.:
  - Di Rocco, Eklund, Peterson, Sommese “Chern numbers of smooth varieties via homotopy continuation and intersection theory” (2009)
  - L., Sottile “Galois groups of Schubert problems via homotopy computation” (2009)

Create a tool for experiments useful for...

- Complexity analysis: Smale’s 17th problem.
- Better understanding of reliability of heuristic methods.

Affine:

- Polynomials of degree at most l: $\mathcal{P}_l = \mathbb{C}_l[X_1, \ldots, X_n]$.
- Square systems of polynomials: $\mathcal{P}_{(d)} = \mathcal{P}_{d_1} \times \cdots \times \mathcal{P}_{d_n}$, where $(d) = (d_1, \ldots, d_n)$.
- **Problem 1**: Assuming $f \in \mathcal{P}_{(d)}$ has finitely many zeros, find approximately one, several, or all zeros of f in $\mathbb{C}^n$.

Projective:

- Homogeneous systems: $\mathcal{H}_{(d)} = \mathcal{H}_{d_1} \times \cdots \times \mathcal{H}_{d_n}$, where $\mathcal{H}_{d_i}$ is homogeneous polynomials in $\mathbb{C}[X_0, X_1, \ldots, X_n]$ of degree d_i.
- **Problem 2**: Assuming $h \in \mathcal{H}_{(d)}$ has finitely many zeros, find approximately one, several or all zeros of h in $\mathbb{P}(\mathbb{C}^{n+1})$.

α-theory basics

For $f \in \mathcal{P}_{(d)}$ and $x \in \mathbb{C}^n$, let

$$N(f)(x) = x - Df(x)^{-1} f(x),$$

Definition

$x \in \mathbb{C}^n$ is an approximate zero with associated zero $\eta \in \mathbb{C}^n$ if

$$\|N(f)^l(x) - \eta\| \leq \frac{\|x - \eta\|}{2^{2^l - 1}}, \quad l \geq 0.$$

For $h \in \mathcal{H}_{(d)}$ and $z \in \mathbb{P}(\mathbb{C}^{n+1})$, let

$$\begin{aligned} N_{\mathbb{P}}(h)(z) &= z - (Dh(z)\,|_{z^\perp})^{-1}\, h(z) \\ &= z - \begin{pmatrix} Dh(z) \\ z^* \end{pmatrix}^{-1} \begin{pmatrix} h(z) \\ 0 \end{pmatrix}. \end{aligned}$$

Definition

$z \in \mathbb{P}(\mathbb{C}^{n+1})$ is an approximate zero with associated zero $\zeta \in \mathbb{P}(\mathbb{C}^{n+1})$ if

$$d_R(N_{\mathbb{P}}(h)^l(z), \zeta) \leq \frac{d_R(z, \zeta)}{2^{2^l - 1}}, \quad l \geq 0,$$

Riemann distance in $\mathbb{P}(\mathbb{C}^{n+1})$:

$d_R(z, z') = \arccos \frac{|\langle z, z' \rangle|}{\|z\|\,\|z'\|} \in [0, \pi/2]$.

Bombieri-Weyl norm

- For $v, w \in \mathcal{H}_l$,

$$v = \sum_{|\alpha|=l} a_\alpha X^\alpha, \quad w = \sum_{|\alpha|=l} b_\alpha X^\alpha, \quad \alpha = (\alpha_0, \ldots, \alpha_n), \ |\alpha| = \sum_{i=0}^{n} \alpha_i,$$

define Bombieri-Weyl Hermitian product

$$\langle v, w \rangle = \sum_{|\alpha|=l} \binom{l}{\alpha}^{-1} a_\alpha \overline{b_\alpha}, \text{ where } \binom{l}{\alpha} = \frac{l!}{\alpha_0! \cdots \alpha_n!}$$

- For $h = (h_1, \ldots, h_n)$ and $h' = (h'_1, \ldots, h'_n)$ in $\mathcal{H}_{(d)}$,

$$\langle h, h' \rangle = \langle h_1, h'_1 \rangle + \cdots + \langle h_n, h'_n \rangle, \quad \|h\| = \langle h, h \rangle^{1/2}.$$

- Invariant under unitary transformations.

Linear homotopy on a sphere

Given a pair (start and target) of systems $g, f \in \mathcal{H}_{(d)}$,

- normalize to the sphere $\mathbb{S} = \{f \in \mathcal{H}_{(d)} : \|f\| = 1\}$
- linear homotopy in $\mathbb{S}$ with arc-length parametrization:

$$t \to h_t = g\cos(t) + \frac{f - Re(\langle f, g\rangle)g}{\sqrt{1 - Re(\langle f, g\rangle)^2}}\sin(t), \quad t \in [0, T],$$

  where $T = \arcsin\sqrt{1 - Re\langle f, g\rangle^2} =$ distance(f, g).
- predictor: "order 0" (copy approximation from previous step)
- corrector: one step of projective Newton's iterator.

Certified step control

- given: linear homotopy $t \to h_t$, a root of z_0 of h_0;
- want: sequences $0 = t_0 < t_1 < \ldots < t_k = T$ and $z_0, \ldots, z_k \in \mathbb{P}(\mathbb{C}^{n+1})$, such that z_i is an approximate root of h_{t_i} lying of the same (regular) homotopy path as z_0.

Theorem: Let $\Delta t_i = \min\{\frac{0.04804448}{d^{3/2}\varphi_i}, T - t_i\}$ where $\varphi_i = \chi_{i,1}\chi_{i,2}$ where

$$\chi_{i,1} = \left\| \begin{pmatrix} Dg_i(z_i) \\ z_i^* \end{pmatrix}^{-1} \begin{pmatrix} \sqrt{d_1} & & \\ & \ddots & \\ & & \sqrt{d_n} \\ & & & 1 \end{pmatrix} \right\|$$

$$\chi_{i,2} = \left(\|\dot{g}_i\|^2 + \left\| \begin{pmatrix} Dg_i(z_i) \\ z_i^* \end{pmatrix}^{-1} \begin{pmatrix} \dot{g}_i(z_i) \\ 0 \end{pmatrix} \right\|^2 \right)^{1/2}$$

where $d = \max\{d_1, \ldots, d_n\}$ and $g_i = h_{t_i}$.
Then $t_{i+1} = t_i + \Delta t_i$ determines a solution to the problem.

Experiments

- Random$_{(d_1,\ldots,d_n)}$: a random system in $\mathbb{S} \subset \mathcal{H}_{(d)}$ with uniform distribution;

system	#sol.	#steps/path (C)	#steps/path (H)
Random$_{(2,2)}$	4	198	11
Random$_{(2,2,2)}$	8	370	11
Random$_{(2,2,2,2)}$	16	813	16
Random$_{(2,2,2,2,2)}$	32	1542	16
Random$_{(2,2,2,2,2,2)}$	64	2211	18
Katsura$_3$	4	569	12
Katsura$_4$	8	1149	15
Katsura$_5$	16	1498	13
Katsura$_6$	32	2361	18

Average #steps/path: (C) = certified, (H) = heuristic.

Complexity

- The condition number at $(h, z) \in \mathcal{H}_{(d)} \times \mathbb{P}(\mathbb{C}^{n+1})$:

$$\mu(h, z) = \|h\| \, \|(Dh(z) \mid_{z^\perp})^{-1} \mathrm{Diag}(\|z\|^{d_i - 1} d_i^{1/2})\|,$$

  or $\mu(h, z) = \infty$ if $Dh(\zeta) \mid_{z^\perp}$ is not invertible.

- If $\mathcal{C}_0 = \int_0^T \mu(h_t, \zeta_t) \|\dot{h}_t, \dot{\zeta}_t\| \, dt < \infty$,

$$\#\text{steps} \leq \lceil 71 d^{3/2} \mathcal{C}_0 \rceil.$$

- Consider the uniform probability measure on $\mathbb{S} = \{h \in \mathcal{H}_{(d)} : \|h\| = 1\}$.
- Smale: can one solution of $h \in \mathbb{S}$ be computed in polynomial time on average?

Almost polynomial...

- "Good" initial pair:

$$g(z) = \begin{cases} d_1^{1/2} X_0^{d_1-1} X_1 \\ \vdots \\ d_n^{1/2} X_0^{d_n-1} X_n \end{cases}, \quad e_0 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

- **Conjecture** [Shub and Smale (1994)]: For the initial pair (g, e_0) the average length $\mathrm{E}(\mathcal{C}_0(f, g, e_0))$ of the homotopy path in the condition metric is "small quantity polynomial in N", where

$$N + 1 = \dim \mathcal{H}_{(d)}.$$

- Bürguisser and Cucker (2010): $\mathrm{E}(\mathcal{C}_0(f, g, e_0)) = O(N^{\log(\log(N))})$.

Random initial pair (g, ζ_0)

1. Given $\zeta \in \mathbb{P}(\mathbb{C}^{n+1})$, let $R_\zeta = \{\tilde{h} \in \mathcal{H}_{(d)} : \tilde{h}(\zeta) = 0, D\tilde{h}(\zeta) = 0\}$.
   E.g., $R_{e_0} = \{X_0^{d_i-2} p_2(X_1, \ldots, X_n) + X_0^{d_i-3} p_3(X_1, \ldots, X_n) + \cdots\}$, where $p_k \in \mathbb{C}[X_1, \ldots, X_n]$ homogeneous of degree k.
2. Choose $(M, l) \in \mathbb{C}^{n^2+n} \times \mathbb{C}^{N+1-n^2-n} = \mathbb{C}^{N+1}$ randomly in $B(\mathbb{C}^{N+1}) = \{r \in \mathbb{C}^{N+1} : \|r\|_2 \leq 1\}$.
3. Let $\zeta_0 \in Ker(M)$ be a random unit vector in $Ker(M)$.
4. Pick $h \in B(R_{\zeta_0})$.
5. Let $\hat{g} \in \mathcal{H}_{(d)}$ be the polynomial system defined by

$$\hat{g}(z) = \sqrt{1 - \|M\|_F^2}\, h(z) + \begin{pmatrix} \langle z, \zeta_0 \rangle^{d_1 - 1} \sqrt{d_1} & & \\ & \ddots & \\ & & \langle z, \zeta_0 \rangle^{d_n - 1} \sqrt{d_n} \end{pmatrix} Mz$$

6. Let $g = \frac{\hat{g}}{\|\hat{g}\|}$.

Theorem

- Beltran and Pardo [2009]:
  1. Roots of f are obtained by the random linear homotopy with equal probability.
  2. $\mathrm{E}(\mathcal{C}_0(f, g, \zeta)) = O(d^{3/2} n N)$.
- **Conjecture**: The "good" initial pair (g, e_0) composed with a random unitary coordinate transformation results in equiprobability of the roots.

Comparison: random, total-degree, and "good"

- Experiment: find a solution of a random system system of n quadrics with each method 1000 times.

n	4	5	6	7	8	9
E_{good}	634.674	1001.25	1452.57	2007.84	2622.45	3436.89
Var_{good}	131068	298812	533223	926359	1508480	2699130
$\#fail_{good}$	3	3	12	10	22	29
E_{total}	825.927	1373.76	2028.24	2832.46	3966.77	5073.65
Var_{total}	183124	464962	930163	1545670	3297580	4580160
$\#fail_{total}$	1	3	5	13	16	19
E_{rand}	1075.58	1777.03	2603.78	3714.34	5013.25	6662.46
Var_{rand}	320481	647500	1217820	2546390	4075190	7423540
$\#fail_{rand}$	2	1	7	16	26	37
$B(n,d,N)$	856524	1873646	3597401	6295451	10278286	15899224

- Random homotopies have the best theoretical bound: $B(n,d,N) = 284\sqrt{2}\pi nNd^{3/2}$.
- Observation 1: $E_{good} < E_{total} < E_{rand}$.
- Observation 2: #steps $\sim \frac{N}{\sqrt{n}}$ for all three cases.