Symbolic-Numeric Computing in Algebraic Geometry

Jan Verschelde

Department of Math, Stat & CS

University of Illinois at Chicago

Chicago, IL 60607-7045, USA

e-mail: **jan@math.uic.edu**

web: **www.math.uic.edu/~jan**

University of Western Ontario, London, Canada

18 July 2003

Outline of the Talk

1. Homotopies and Path Tracking

   the theorem of Bézout, predictor-corrector methods,

   some complexity issues

2. Numerical Algebraic Geometry

   extend solving to positive dimensional solution components

3. Numerical Irreducible Decomposition

   decompose components into irreducible factors

4. Software and Applications

   the software PHCpack, illustrations of application fields

Numerical Homotopy Continuation Methods

If we wish to solve $f(\mathbf{x}) = \mathbf{0}$, then we construct a system $g(\mathbf{x}) = \mathbf{0}$ whose solutions are known. Consider the *homotopy*

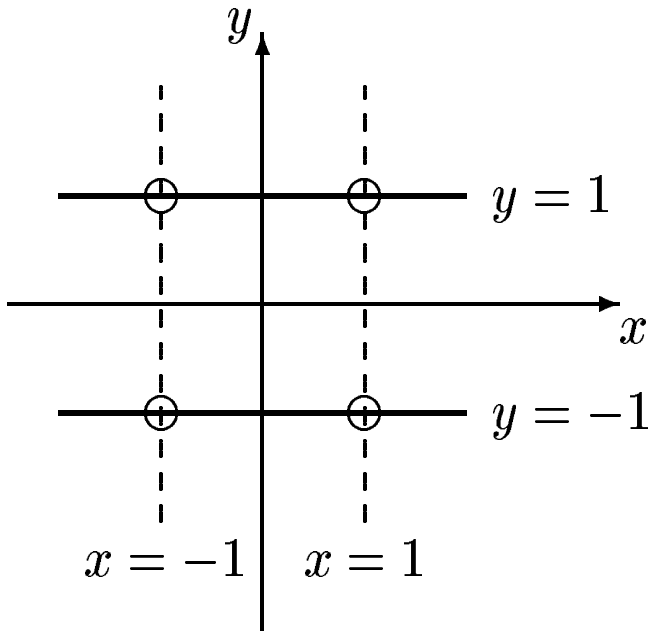
$$H(\mathbf{x}, t) := (1 - t)g(\mathbf{x}) + tf(\mathbf{x}) = \mathbf{0}.$$

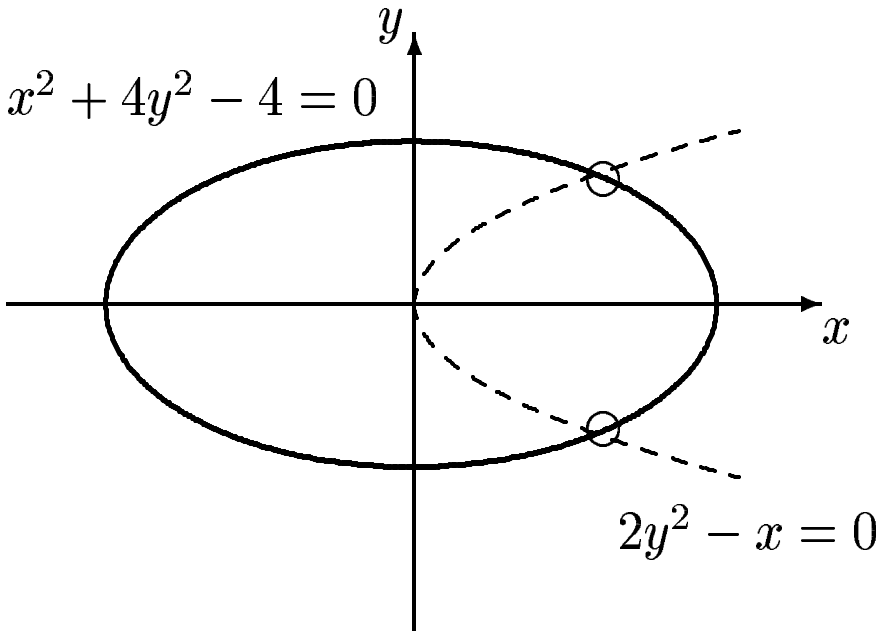
By *continuation*, we trace the paths starting at the known solutions of $g(\mathbf{x}) = \mathbf{0}$ to the desired solutions of $f(\mathbf{x}) = \mathbf{0}$, for t from 0 to 1.

homotopy continuation methods are *symbolic-numeric*:
homotopy methods treat polynomials as algebraic objects,
continuation methods use polynomials as functions.

geometric interpretation: move from general to special,
solve special, and move solutions from special to general.

Product Deformations





$$\gamma \left(\left\{ \begin{array}{r} x^2 - 1 = 0 \\ y^2 - 1 = 0 \end{array} \right) (1-t) \quad + \quad \left(\left\{ \begin{array}{r} x^2 + 4y^2 - 4 = 0 \\ 2y^2 - x = 0 \end{array} \right) t, \quad \gamma \in \mathbb{C}$$

The theorem of Bézout

$f = (f_1, f_2, \ldots, f_n)$

$d_i = \deg(f_i)$

total degree D :

$$D = \prod_{i=1}^{n} d_i$$

$$g(\mathbf{x}) = \begin{cases} \alpha_1 x_1^{d_1} - \beta_1 = 0 & \text{start} \\ \alpha_2 x_2^{d_2} - \beta_2 = 0 & \text{system} \\ \vdots & \alpha_i, \beta_i \in \mathbb{C} \\ \alpha_n x_n^{d_n} - \beta_n = 0 & \text{random} \end{cases}$$

Theorem: $f(\mathbf{x}) = \mathbf{0}$ *has at most* D *isolated solutions in* $\mathbb{C}^n$, *counted with multiplicities.*

Sketch of Proof: $V = \{ \ (f, \mathbf{x}) \in \mathbb{P}(\mathcal{H}_D) \times \mathbb{P}(\mathbb{C}^n) \mid f(\mathbf{x}) = \mathbf{0} \ \}$

$\Sigma' = \{(f, \mathbf{x}) \in V \mid \det(D_{\mathbf{x}} f(\mathbf{x})) = 0\}$, $\Sigma = \pi_1(\Sigma'), \pi_1 : V \to \mathbb{P}(\mathcal{H}_D)$

Elimination theory: Σ is variety $\Rightarrow \mathbb{P}(\mathcal{H}_D) - \Sigma$ is connected.

Thus $h(\mathbf{x}, t) = (1-t)g(\mathbf{x}) + tf(\mathbf{x}) = \mathbf{0}$ avoids $\Sigma, \forall t \in [0, 1)$.

Implicitly defined curves

Consider a homotopy $h_k(x(t), y(t), t) = 0$, $k = 1, 2$.

By $\frac{\partial}{\partial t}$ on homotopy: $\frac{\partial h_k}{\partial x}\frac{\partial x}{\partial t} + \frac{\partial h_k}{\partial y}\frac{\partial y}{\partial t} + \frac{\partial h_k}{\partial t}\frac{\partial t}{\partial t} = 0$, $k = 1, 2$.

Set $\Delta x := \frac{\partial x}{\partial t}$, $\Delta y := \frac{\partial y}{\partial t}$, and $\frac{\partial t}{\partial t} = 1$.

Increment $t := t + \Delta t$

Solve $$\begin{bmatrix} \frac{\partial h_1}{\partial x} & \frac{\partial h_1}{\partial y} \\ \frac{\partial h_2}{\partial x} & \frac{\partial h_2}{\partial y} \end{bmatrix} \begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix} = - \begin{bmatrix} \frac{\partial h_1}{\partial t} \\ \frac{\partial h_2}{\partial t} \end{bmatrix} (Newton)$$

Update $$\begin{cases} x := x + \Delta x \\ y := y + \Delta y \end{cases}$$

Predictor-Corrector Methods

loop

1. predict $\begin{cases} t_{k+1} := t_k + \Delta t \\ \mathbf{x}^{(k+1)} := \mathbf{x}^{(k)} + \Delta \mathbf{x} \end{cases}$

2. correct with Newton

3. if convergence

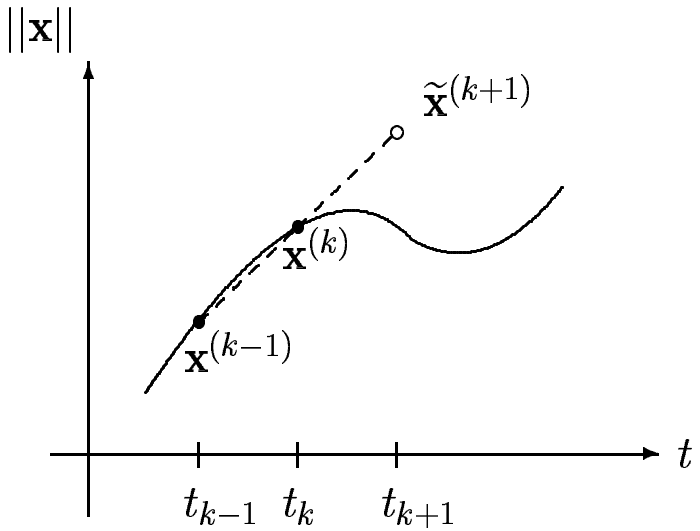
   then enlarge Δt

      continue with $k+1$

   else reduce Δt

      back up and restart at k

until $t = 1$.



$$\widetilde{\mathbf{x}}^{(k+1)} := \mathbf{x}^{(k)} + \lambda\left(\mathbf{x}^{(k)} - \mathbf{x}^{(k-1)}\right)$$

Robustness of Continuation Methods

sure to find **all** *roots at the end of the paths?*

- dealing with curve jumping:
  1. fix #Newton steps to force quadratic convergence;
  2. rerun clustered paths with same discretization of t.
- Robust step control by interval methods, see

R.B. Kearfott and Z. Xing: **An interval step control for continuation methods.** *SIAM J. Numer. Anal.* 31(3): 892–914, 1994.

- Root of multiplicity μ will appear at the end of the paths as a cluster of μ roots.

  Use "endgames", eventually in multi-precision arithmetic.

Complexity Issues

The Problem: a hierarchy of complexity classes

P	:	evaluation of a system at a point
NP	:	find one root of a system
$\#P$	:	find **all** roots of a system (*intractable!*)

Complexity of Homotopies: for bounds on #Newton steps in a linear homotopy, see

L. Blum, F. Cucker, M. Shub, and S. Smale: **Complexity and Real Computation**. Springer 1998.

M. Shub and S. Smale: **Complexity of Bezout's theorem V: Polynomial Time**. *Theoretical Computer Science* 133(1):141–164, 1994.

On average, we can find an approximate zero in polynomial time.

Some Literature

E.L. Allgower and K. Georg: **Numerical Continuation Methods, an Introduction.** Springer 1990. To appear in the SIAM Classics in Applied Mathematics Series.

E.L. Allgower and K. Georg: **Numerical Path Following.** In *Techniques of Scientific Computing (Part 2)*, edited by P.G. Ciarlet and J.L. Lions volume 5 of *Handbook of Numerical Analysis*, pages 3–203. North-Holland, 1997.

A. Morgan: **Solving polynomial systems using continuation for engineering and scientific problems**. Prentice-Hall, 1987.

T.Y. Li: **Solving polynomial systems.** *The Mathematical Intelligencer* 9(3):33–39, 1987.

T.Y. Li: **Numerical solution of multivariate polynomial systems by homotopy continuation methods.** *Acta Numerica* 6:399–436, 1997.

The software PHCpack

J. Verschelde: **Algorithm 795: PHCpack: A general-purpose solver for polynomial systems by homotopy continuation.** *ACM Transactions on Mathematical Software* 25(2): 251-276, 1999.

Available via `http://www.math.uic.edu/~jan/download.html`.

Modes of operation:

1. As a blackbox: `phc -b input output`.
2. In toolbox mode (call `phc` with other options).
3. The library PHCpack, in Ada with C interface, used with MPI.

Papers documenting the usefulness of PHCpack

R.S. Datta: **Using Computer Algebra To Compute Nash Equilibria**. To be presented at ISSAC 2003.

C. Durand and C.M. Hoffmann: **Variational Constraints in 3D**. In Proceedings of the International Conference on Shape Modeling and Applications, Aizu-Wakamatsu, Japan, pages 90-98, IEEE Computer Society, 1999.

C. Durand and C.M. Hoffmann: **A systematic framework for solving geometric constraints analytically**. *J. Symbolic Computation* 30(5):493-520, 2000.

B. Haas: **A Simple Counterexample to Kouchnirenko's Conjecture**. *Beitraege zur Algebra und Geometrie/Contributions to Algebra and Geometry* 43(1):1-8, 2002.

E. Lee and C. Mavroidis: **Solving the Geometric Design Problem of Spatial 3R Robot Manipulators Using Polynomial Continuation.** *Journal of Mechanical Design, Transactions of the ASME* 124(4):652-661, 2002.

E. Lee, C. Mavroidis, and J. Morman: **Geometric Design of Spatial 3R Manipulators**. *Proceedings of the 2002 NSF Design, Service, and Manufacturing Grantees and Research Conference*, San Juan, Puerto Rico, January 7-10, 2002.

More papers documenting the usefulness of PHCpack

M. Oskarsson, A. Zisserman and K. Astrom: **Minimal Projective Reconstruction for combinations of Points and Lines in Three Views**. *Electronic Proceedings of BMVC2002 - The 13th British Machine Vision Conference 2002*, pages 63 - 72.

P.A. Parillo and B. Sturmfels: **Minimizing Polynomial Functions**. presented at the *Workshop on Algorithmic and Quantitative Aspects of Real Algebraic Geometry in Mathematics and Computer Science,* held at DIMACS, Rutgers University, March 12-16, 2001.

H. Schreiber, K. Meer, and B.J. Schmitt: **Dimensional synthesis of planar Stephenson mechanisms for motion generation using circlepoint search and homotopy methods.** *Mechanism and Machine Theory* 37(7):717-737, 2002.

F. Sottile: **Real Schubert Calculus: Polynomial systems and a conjecture of Shapiro and Shapiro**. *Experimental Mathematics* 9(2): 161-182, 2000.

C.W. Wampler: **Isotropic coordinates, circularity and Bezout numbers: planar kinematics from a new perspective**. *Proceedings of the 1996 ASME Design Engineering Technical Conference.* Irvine, CA, Aug 18–22, 1996. (CD-ROM).

F. Xie, G. Reid, and S. Valluri: **A numerical method for the one dimensional action functional for FBG structures**. *Can J. Phys.* 76: 1-21, 2002.

Solution sets to polynomial systems

Polynomial in One Variable	**System of Polynomials**
one equation, one variable	n equations, N variables
solutions are points	points, lines, surfaces, ...
multiple roots	sets with multiplicity
Factorization: $\prod_i (x - a_i)^{\mu_i}$	**Irreducible Decomposition**
Numerical Representation	
set of points	set of witness sets

Joint Work with A.J. Sommese and C.W. Wampler

A.J. Sommese and JV: **Numerical homotopies to compute generic points on positive dimensional algebraic sets.** *Journal of Complexity* 16(3):572–602, 2000.

A.J. Sommese, JV and C.W. Wampler: **Numerical decomposition of the solution sets of polynomial systems into irreducible components.** *SIAM J. Numer. Anal.* 38(6):2022–2046, 2001.

A.J. Sommese, JV and C.W. Wampler: **Using monodromy to decompose solution sets of polynomial systems into irreducible components.** In *Application of Algebraic Geometry to Coding Theory, Physics and Computation*, ed. by C. Ciliberto et al., pages 297–315, Kluwer AP.

A.J. Sommese, JV and C.W. Wampler: **Symmetric functions applied to decomposing solution sets of polynomial systems.** *SIAM J. Numer. Anal.* 40(6):2026–2046, 2002.

A.J. Sommese, JV and C.W. Wampler: **Advances in polynomial continuation for solving problems in kinematics.** Paper DETC2002/MECH-34254, *Proc. ASME Design Engineering Technical Conf.* (CDROM), Montreal, Quebec, Sept. 29-Oct. 2, 2002.

A.J. Sommese, JV and C.W. Wampler: **Numerical irreducible decomposition using PHCpack.** In *Algebra, Geometry, and Software Systems*, edited by M. Joswig and N. Takayama, pages 109–130, Springer-Verlag, 2003.

An Illustrative Example

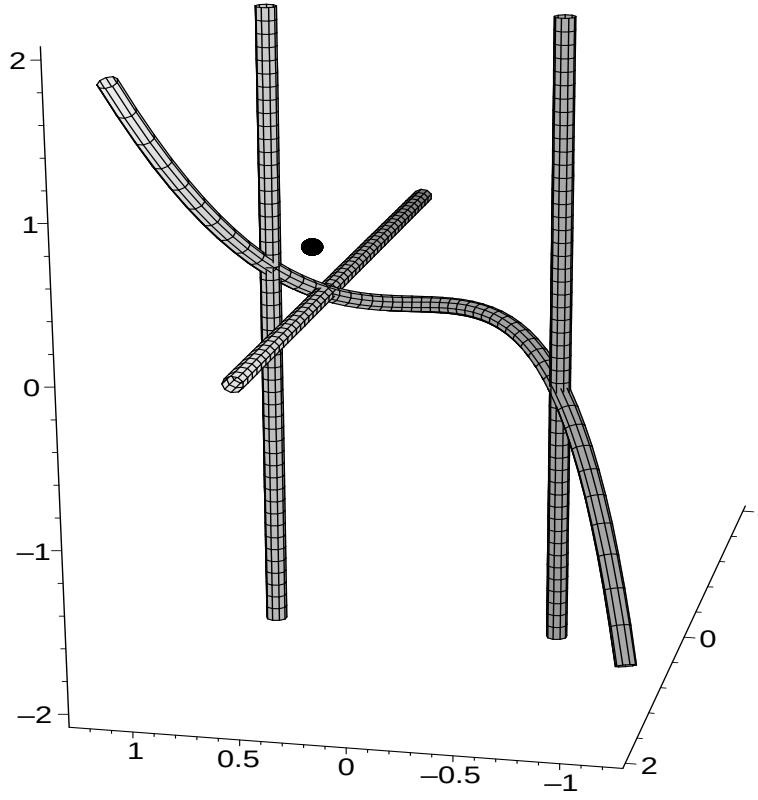
$$f(x,y,z) = \begin{cases} (y-x^2)(x^2+y^2+z^2-1)(x-0.5) = 0 \\ (z-x^3)(x^2+y^2+z^2-1)(y-0.5) = 0 \\ (y-x^2)(z-x^3)(x^2+y^2+z^2-1)(z-0.5) = 0 \end{cases}$$

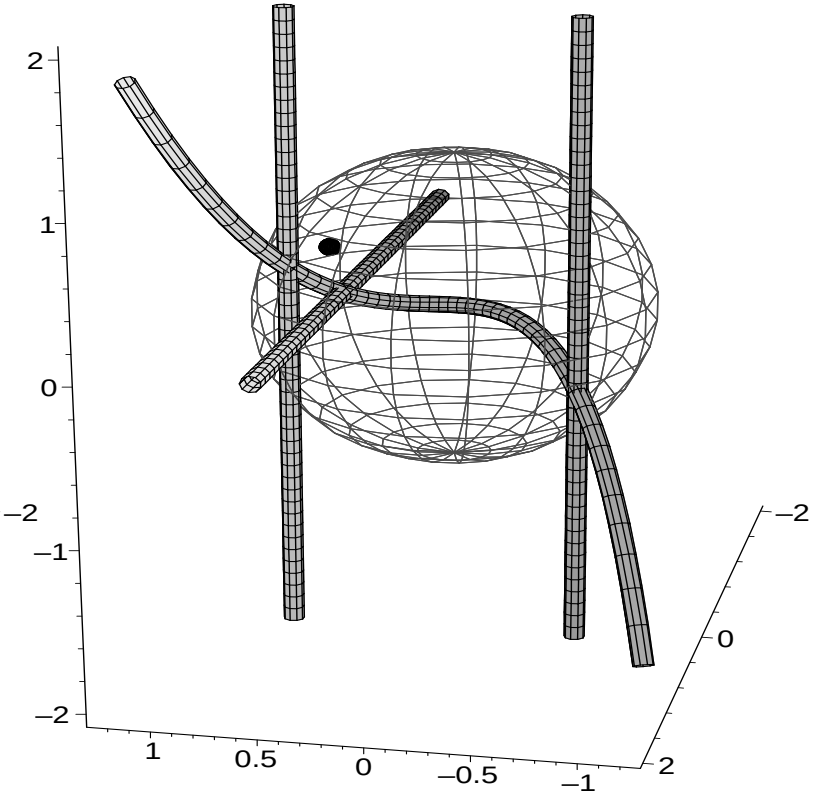
Irreducible decomposition of $Z = f^{-1}(\mathbf{0})$ is

$$Z = Z_2 \cup Z_1 \cup Z_0 = \{Z_{21}\} \cup \{Z_{11} \cup Z_{12} \cup Z_{13} \cup Z_{14}\} \cup \{Z_{01}\}$$

with
1. Z_{21} is the sphere $x^2+y^2+z^2-1=0$,
2. Z_{11} is the line $(x = 0.5, z = 0.5^3)$,
3. Z_{12} is the line $(x = \sqrt{0.5}, y = 0.5)$,
4. Z_{13} is the line $(x = -\sqrt{0.5}, y = 0.5)$,
5. Z_{14} is the twisted cubic $(y - x^2 = 0, z - x^3 = 0)$,
6. Z_{01} is the point $(x = 0.5, y = 0.5, z = 0.5)$.

An Illustrative Example - the plots





Witness Sets

A witness point is a solution of a polynomial system which lies on a set of generic hyperplanes.

- The number of generic hyperplanes used to isolate a point from a solution component

  equals the **dimension** of the solution component.

- The number of witness points on one component cut out by the same set of generic hyperplanes

  equals the **degree** of the solution component.

A witness set for a k-dimensional solution component consists of k random hyperplanes and a set of isolated solutions of the system cut with those hyperplanes.

Membership Test

Does the point $\mathbf{z}$ *belong to a component?*

Given: a point in space $\mathbf{z} \in \mathbb{C}^N$; a system $f(\mathbf{x}) = \mathbf{0}$;

and a witness set W, $W = (Z, L)$:

for all $\mathbf{w} \in Z : f(\mathbf{w}) = \mathbf{0}$ and $L(\mathbf{w}) = \mathbf{0}$.

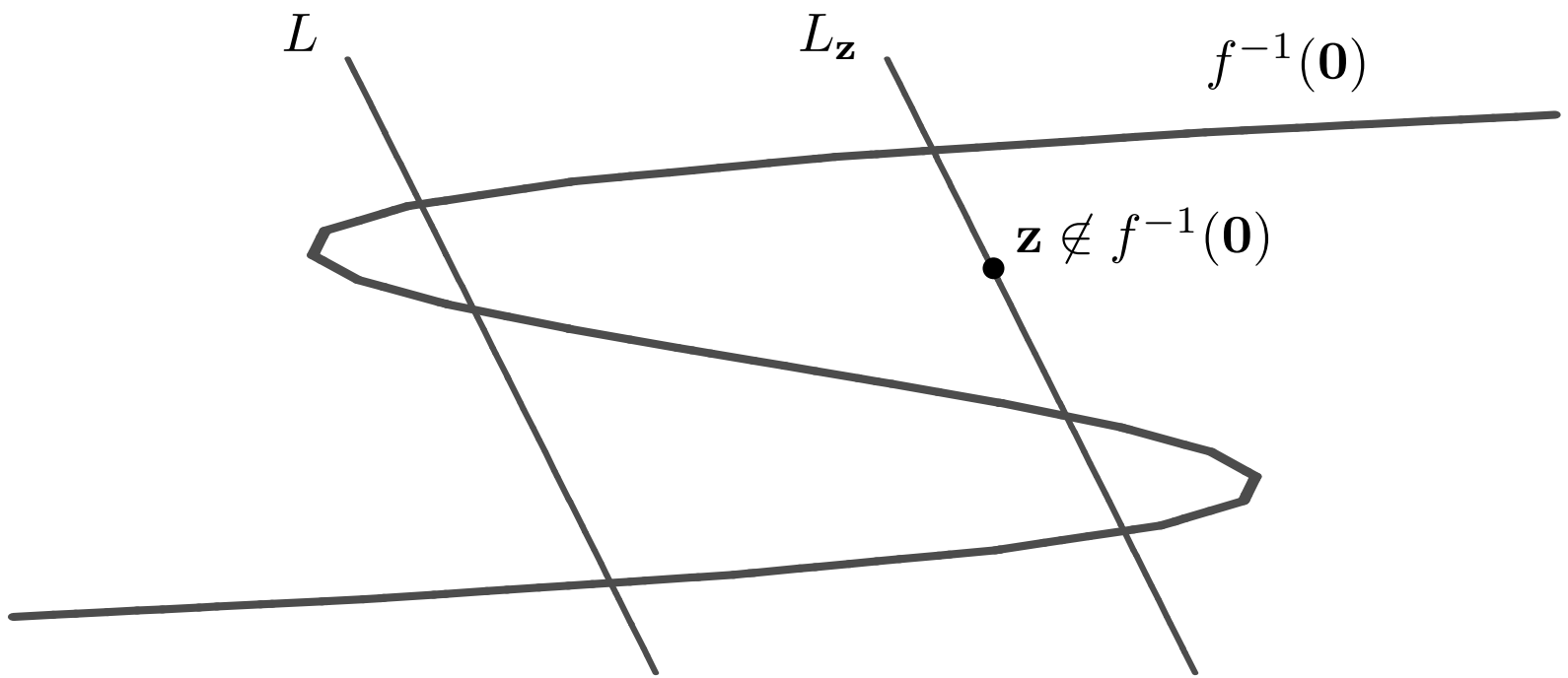
1. Let $L_{\mathbf{z}}$ be a set of hyperplanes through $\mathbf{z}$, and define

$$h(\mathbf{x}, t) = \begin{cases} f(\mathbf{x}) = \mathbf{0} \\ L_{\mathbf{z}}(\mathbf{x})t + L(\mathbf{x})(1-t) = \mathbf{0} \end{cases}$$

2. Trace all paths starting at $\mathbf{w} \in Z$, for t from 0 to 1.

3. The test $(\mathbf{z}, 1) \in h^{-1}(\mathbf{0})$? answers the question above.

Membership Test – an example

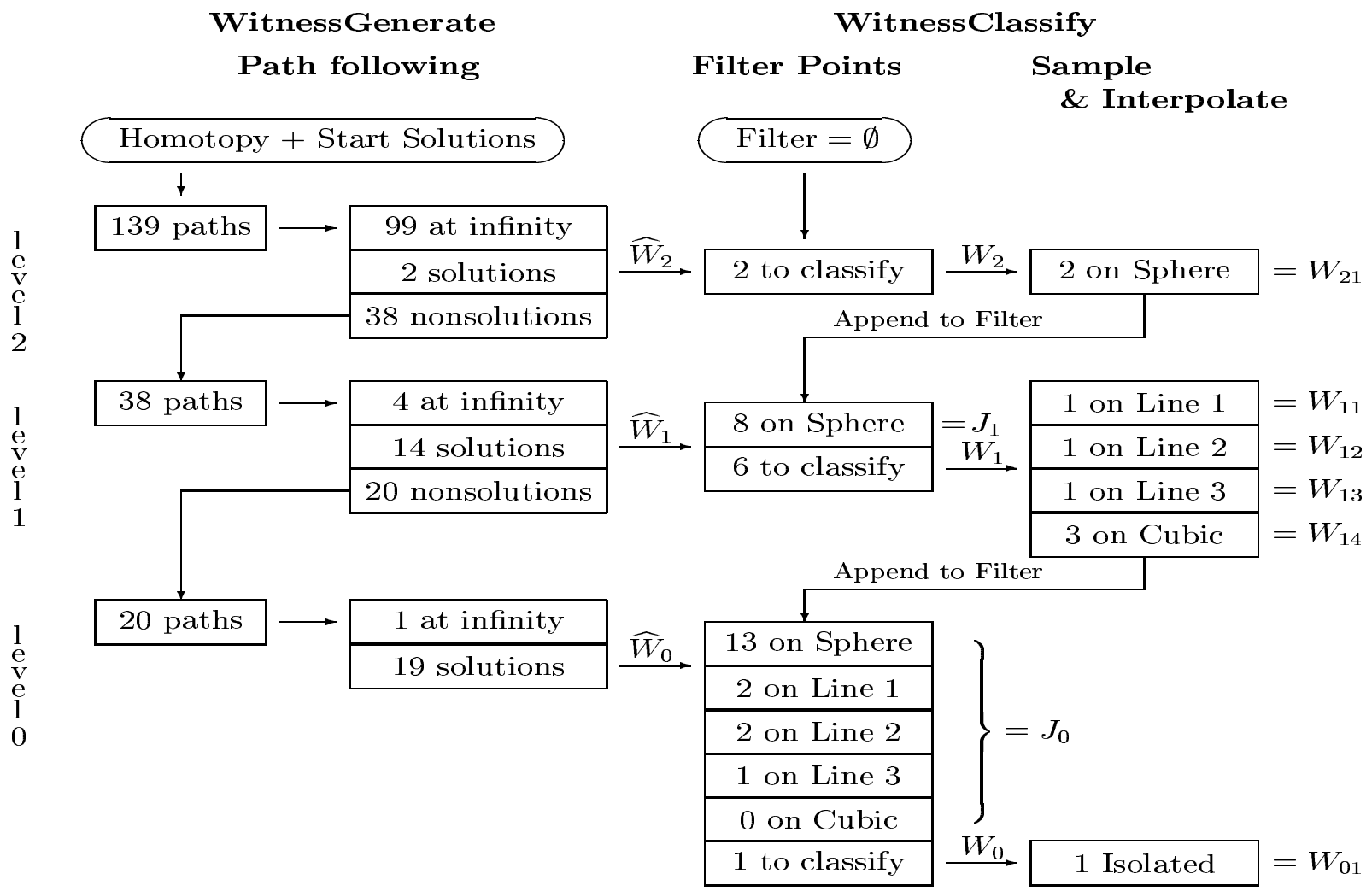


$$h(\mathbf{x}, t) = \begin{cases} f(\mathbf{x}) = \mathbf{0} \\ L_{\mathbf{z}}(\mathbf{x})t + L(\mathbf{x})(1-t) = \mathbf{0} \end{cases}$$

Numerical Algebraic Geometry Dictionary

Algebraic Geometry	example in 3-space	Numerical Analysis
variety	collection of points, algebraic curves, and algebraic surfaces	polynomial system + union of witness sets, see below for the definition of a witness set
irreducible variety	a single point, or a single curve, or a single surface	polynomial system + witness set + probability-one membership test
generic point on an irreducible variety	random point on an algebraic curve or surface	point in witness set; a witness point is a solution of polynomial system on the variety and on a random slice whose codimension is the dimension of the variety
pure dimensional variety	one or more points, or one or more curves, or one or more surfaces	polynomial system + set of witness sets of same dimension + probability-one membership tests
irreducible decomposition of a variety	several pieces of different dimensions	polynomial system + array of sets of witness sets and probability-one membership tests

A Numerical Irreducible Decomposition of the Illustrative Example



Factoring Solution Components

Input: $f(\mathbf{x}) = \mathbf{0}$ polynomial system with a positive dimensional solution component, represented by witness set.

coefficients of f known approximately, work with limited precision

Wanted: decompose the component into irreducible factors, for each factor, give its degree and multiplicity.

Symbolic-Numeric issue: essential numerical information (such as degree and multiplicity of each factor), is obtained much faster than the full symbolic representation.

E. Kaltofen: **Challenges of symbolic computation: my favorite open problems**. *J. Symbolic Computation* 29(6): 891–919, 2000.

Related Work

Y. Huang, W. Wu, H.J. Stetter, and L. Zhi: **Pseudofactors of multivariate polynomials.** In *Proceedings of ISSAC 2000*, ed. by C. Traverso, pages 161–168, ACM 2000.

R.M. Corless, M.W. Giesbrecht, M. van Hoeij, I.S. Kotsireas and S.M. Watt: **Towards factoring bivariate approximate polynomials.** In *Proceedings of ISSAC 2001*, ed. by B. Mourrain, pages 85–92, ACM 2001.

A. Galligo and D. Rupprecht: **Semi-numerical determination of irreducible branches of a reduced space curve.** In *Proceedings of ISSAC 2001*, ed. by B. Mourrain, pages 137–142, ACM 2001.

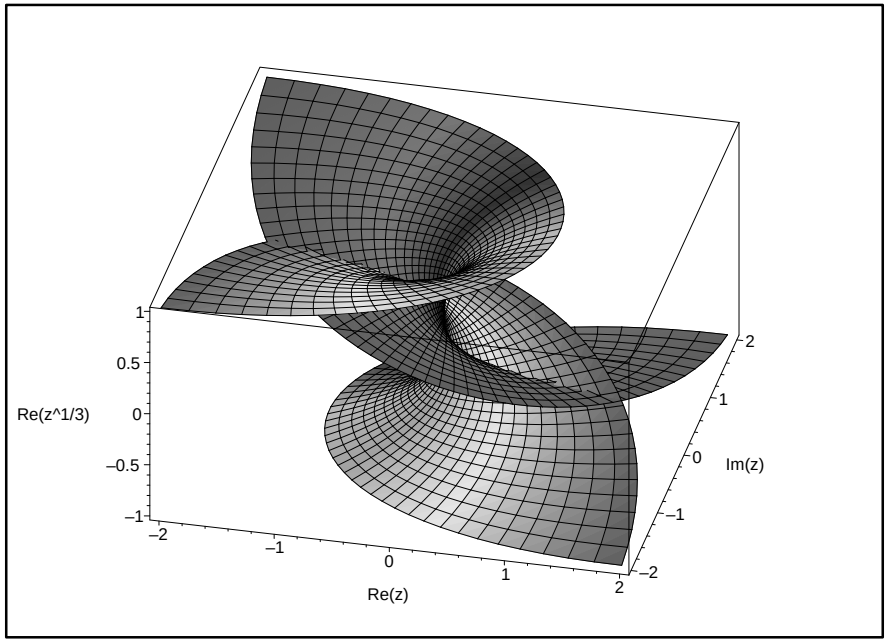
A. Galligo and D. Rupprecht: **Irreducible decomposition of curves.** *J. Symbolic Computation* 33(5):661–677, 2002.

T. Sasaki: **Approximate multivariate polynomial factorization based on zero-sum relations.** In *Proceedings of ISSAC 2001*, ed. by B. Mourrain, pages 284–291, ACM 2001.

R.M. Corless, A. Galligo, I.S. Kotsireas, and S.M. Watt: **A geometric-numeric algorithm for absolute factorization of multivariate polynomials.** In *Proceedings of ISSAC 2002*, ed. by T. Mora, pages 37–45, ACM 2002.

E. Kaltofen and J. May: **On approximate irreducibility of polynomials in several variables.** To appear in *Proceedings of ISSAC 2003*.

The Riemann Surface of $z^3 - w = 0$:



R.M. Corless and D.J. Jeffrey: **Graphing elementary Riemann surfaces.** *SIGSAM Bulletin* 32(1):11–17, 1998.

Monodromy to Decompose Solution Components

Given: a system $f(\mathbf{x}) = \mathbf{0}$; and $W = (Z, L)$:

for all $\mathbf{w} \in Z : f(\mathbf{w}) = \mathbf{0}$ and $L(\mathbf{w}) = \mathbf{0}$.

Wanted: partition of Z so that all points in a subset of Z lie on the same irreducible factor.

Example: does $f(x, y) = xy - 1 = 0$ factor?

Consider $H(x, y, \theta) = \begin{cases} xy - 1 = 0 \\ x + y = 4e^{i\theta} \end{cases}$ for $\theta \in [0, 2\pi]$.

For $\theta = 0$, we start with two real solutions. When $\theta > 0$, the solutions turn complex, real again at $\theta = \pi$, then complex until at $\theta = 2\pi$. Back at $\theta = 2\pi$, we have again two real solutions, but their order is permuted $\Rightarrow$ irreducible.

Connecting Witness Points

1. For two sets of hyperplanes K and L, and a random $\gamma \in \mathbb{C}$

$$H(\mathbf{x}, t, K, L, \gamma) = \begin{cases} f(\mathbf{x}) = \mathbf{0} \\ \gamma K(\mathbf{x})(1-t) + L(\mathbf{x})t = \mathbf{0} \end{cases}$$

   We start paths at $t = 0$ and end at $t = 1$.

2. For $\alpha \in \mathbb{C}$, trace the paths defined by $H(\mathbf{x}, t, K, L, \alpha) = \mathbf{0}$.

   For $\beta \in \mathbb{C}$, trace the paths defined by $H(\mathbf{x}, t, L, K, \beta) = \mathbf{0}$.

   Compare start points of first path tracking with end points of second path tracking. Points which are permuted belong to the same irreducible factor.

3. Repeat the loop with other hyperplanes.

Linear Traces – an example

$$\begin{array}{rrcl} \text{Consider} & f(x, y(x)) & = & (y - y_1(x))(y - y_2(x))(y - y_3(x)) \\ & & = & y^3 - t_1(x)y^2 + t_2(x)y - t_3(x) \end{array}$$

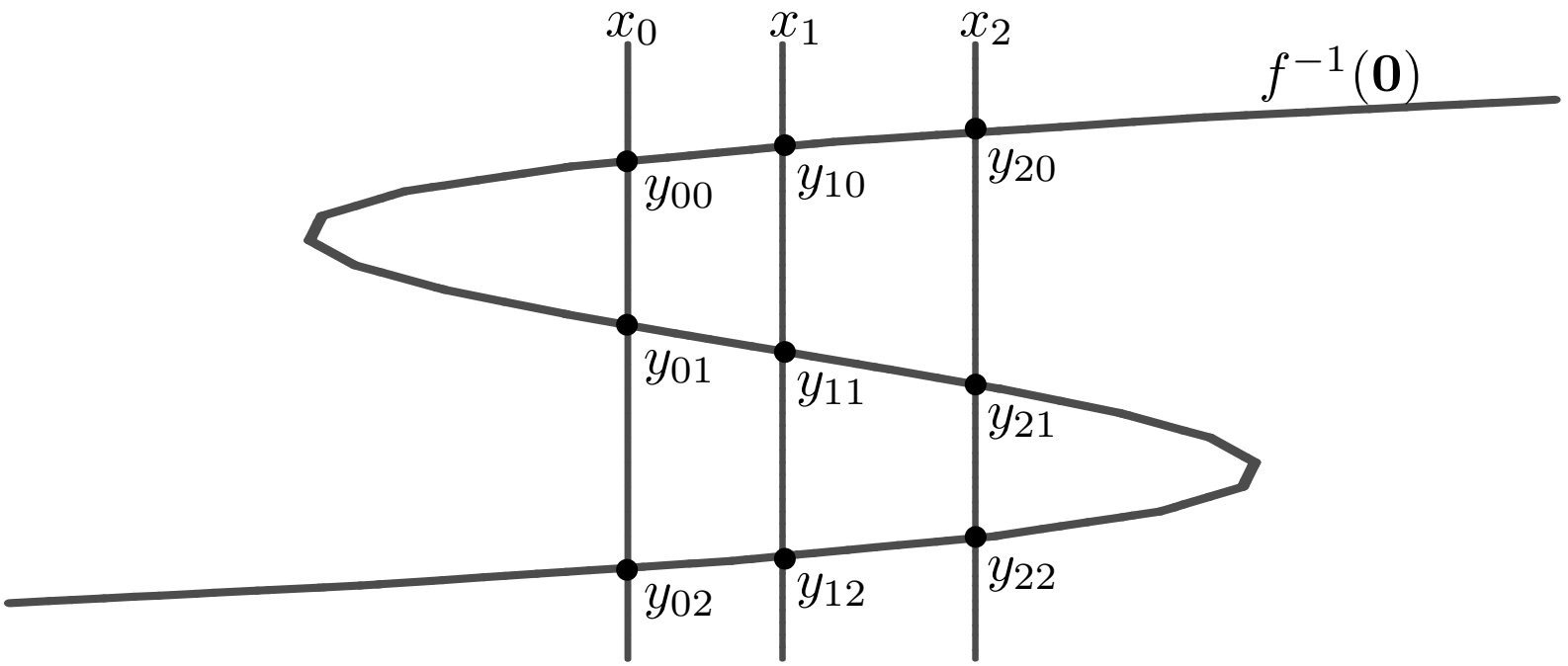
We are interested in the linear trace: $t_1(x) = c_1 x + c_0$.

Sample the cubic at $x = x_0$ and $x = x_1$. The samples are $\{(x_0, y_{00}), (x_0, y_{01}), (x_0, y_{02})\}$ and $\{(x_1, y_{10}), (x_1, y_{11}), (x_1, y_{12})\}$.

$$\text{Solve} \quad \begin{cases} y_{00} + y_{01} + y_{02} = c_1 x_0 + c_0 \\ y_{10} + y_{11} + y_{12} = c_1 x_1 + c_0 \end{cases} \quad \text{to find} \quad c_0, c_1.$$

With t_1 we can predict the sum of the y's for a fixed choice of x. For example, samples at $x = x_2$ are $\{(x_2, y_{20}), (x_2, y_{21}), (x_2, y_{22})\}$. Then, $t_1(x_2) = c_1 x_2 + c_0 = y_{20} + y_{21} + y_{22}$.

Linear Traces – example continued



Use $\{(x_0, y_{00}), (x_0, y_{01}), (x_0, y_{02})\}$ and $\{(x_1, y_{10}), (x_1, y_{11}), (x_1, y_{12})\}$ to find the linear trace $t_1(x) = c_0 + c_1 x$.

At $\{(x_2, y_{20}), (x_2, y_{21}), (x_2, y_{22})\}$: $c_0 + c_1 x_2 = y_{20} + y_{21} + y_{22}$?

Validation of Breakup with Linear Trace

Do we have enough witness points on a factor?

- We may not have enough monodromy loops to connect all witness points on the same irreducible component.
- For a k-dimensional solution component, it suffices to consider a curve on the component cut out by $k-1$ random hyperplanes. The factorization of the curve tells the decomposition of the solution component.
- We have enough witness points on the curve if the value at the linear trace can predict the sum of one coordinate of all points in the set.

Application: Architecturally Singular Platforms

Special Griffis-Duffy type

- Base and endplate are equilateral triangles.
- Legs connect vertices to midpoints.

Results of Husty and Karger

Self-motions of Griffis-Duffy type parallel manipulators. In *Proc. 2000 IEEE Int. Conf. Robotics and Automation* (CDROM), 2000.

The special Griffis-Duffy platforms *move*:

- Case 1: Plates not equal, legs not equal.
  - Curve is degree 20 in Euler parameters.
  - Curve is degree 40 in position.
- Case 2: Plates congruent, legs all equal.
  - Factors are degrees $(4+4)+6+2=16$ in Euler parameters.
  - Factors are degrees $(8+8)+12+4=32$ in position.

Question: *Can we confirm these results numerically?*

Components of Griffis-Duffy Platforms

Solution components by degree

Husty & Karger		SVW	
Euler	Position	Study	Position
General Case			
20	40	28	40
Legs equal, Plates equal			
		6	8
4	8	6	8
4	8	6	8
6	12	6	12
2	4	4	4
16	32	28	40

Griffis-Duffy Platforms: Factorization

Case A: One irreducible component of degree 28 (general case).

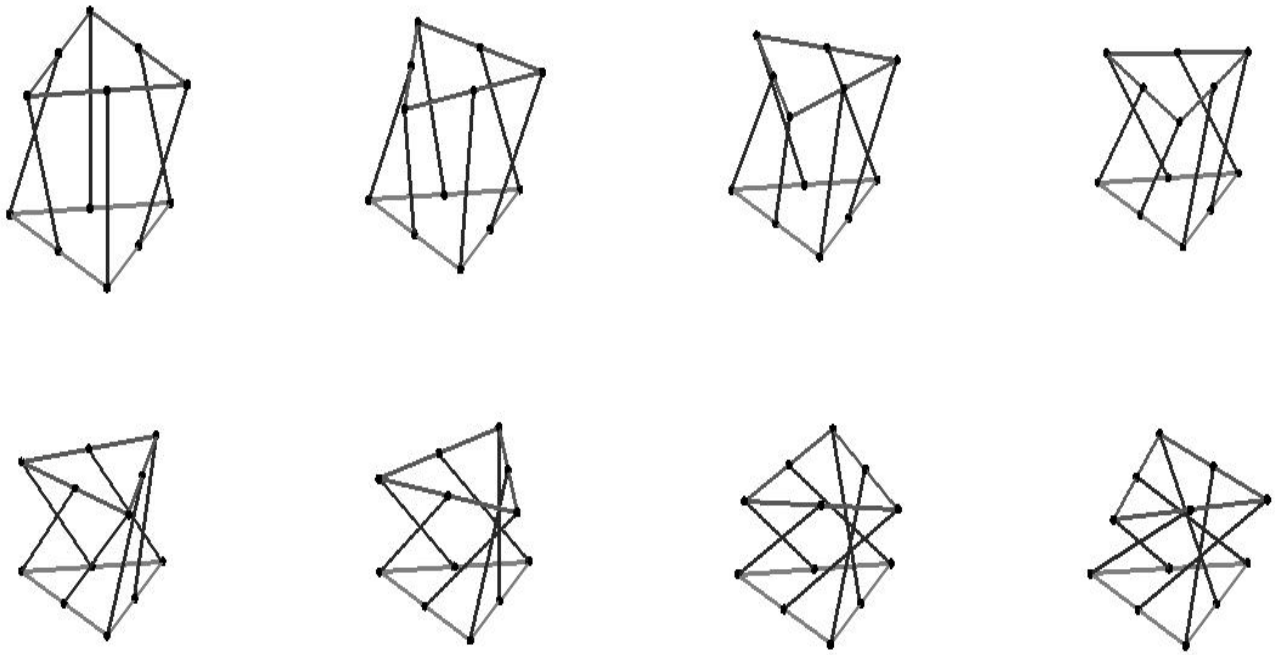
Case B: Five irreducible components of degrees 6, 6, 6, 6, and 4.

user cpu on 800Mhz	Case A	Case B
witness points	1m 12s 480ms	
monodromy breakup	33s 430ms	27s 630ms
Newton interpolation	1h 19m 13s 110ms	2m 34s 50ms
32 decimal places used to interpolate polynomial of degree 28		
linear trace	4s 750ms	4s 320ms

Linear traces replace Newton interpolation:

$\Rightarrow$ **time to factor independent of geometry!**

Griffis-Duffy Platforms: an Animation



Future Directions

- development of methods

  $\rightarrow$ systems with parameters

  $\rightarrow$ irreducible decomposition over the real numbers

- a software platform

  $\rightarrow$ analogue to LAPACK for polynomial systems

- specialize to applications

  $\rightarrow$ impact on science and engineering