Polynomial Homotopy Continuation in the Cloud

Jeff Sommars
joint with Nathan Bliss, Jan Verschelde and Xiangcheng Yu

University of Illinois at Chicago
Department of Mathematics, Statistics, and Computer Science

Central Fall Sectional Meeting
2-4 October 2015, Loyola University Chicago, Chicago

Polynomial Homotopy Continuation Methods

$\mathbf{f}(\mathbf{x}) = \mathbf{0}$ is a polynomial system we want to solve,
$\mathbf{g}(\mathbf{x}) = \mathbf{0}$ is a start system ($\mathbf{g}$ is similar to $\mathbf{f}$) with known solutions.

A homotopy $\mathbf{h}(\mathbf{x}, t) = (1 - t)\mathbf{g}(\mathbf{x}) + t\,\mathbf{f}(\mathbf{x}) = \mathbf{0}$, $t \in [0, 1]$,
to solve $\mathbf{f}(\mathbf{x}) = \mathbf{0}$ defines solution paths $\mathbf{x}(t)$: $\mathbf{h}(\mathbf{x}(t), t) \equiv \mathbf{0}$.

Numerical continuation methods track the paths $\mathbf{x}(t)$, from $t = 0$ to 1,
applying predictor-corrector algorithms.

Polynomial homotopy continuation methods are hybrid:

- Symbolic: definition of a homotopy $\mathbf{h}(\mathbf{x}, t) = \mathbf{0}$.
  We exploit the sparse structure of $\mathbf{f}$ when constructing $\mathbf{g}$.
- Numeric: path tracking with predictor-corrector algorithms.
  Verify approximate solutions with special care for diverging paths.

PHCpack

PHCpack is a package for Polynomial Homotopy Continuation.
ACM Transactions on Mathematical Software archived version 1.0
as Algorithm 795, vol. 25, no. 2, pages 251–276, 1999.

blackbox solver:

`phc -b` computes all isolated solutions of a polynomial system.

External software package integrated in PHCpack:

- Fast mixed volume computation by MixedVol of Gao, Li, and Wu, Algorithm 846 of ACM TOMS, vol. 31, pages 555–560, 2005.
- Double double and quad double arithmetic with the QD Library of Hida, Li, and Bailey published in the 15th IEEE Symposium on Computer Arithmetic, pages 155–162. IEEE, 2001.

Interfaces to Macaulay2 (Gross, Petrovic), Maple (Leykin), MATLAB (Guan), Python (Piret), Sage (Hampton, Jokela, Stein).

Interfaces to PHCpack

Three (pure) types of interfaces to the solvers in PHCpack:

1. Command line with interactive menus:

```
phc -b input output
```

2. Python scripting interface with `phcpy`:

```
>>> from phcpy.solver import solve
>>> help(solve)
>>> f = ['x*y + 3*x - 4;', 'x^2 + y^2 - 1;']
>>> s = solve(f)
```

3. A Graphical User Interface (GUI).

   We view a web interface as a GUI that runs in a browser.

Macaulay2 in the Cloud

`PHCpack.m2` is a package distributed with Macaulay2.

Macaulay2 runs in the cloud as well.

An example session with truncated output is below:

```
Macaulay2, version 1.8.1

i1 : loadPackage "PHCpack";

i2 : R = CC[x,y,z];

i3 : S = {x+y+z-1, x^2 + y^2 - 1, x+2*y-3};

i4 : solveSystem(S)

o4 = {{.6+.8*ii, 1.2-.4*ii, -.8-.4*ii},
      {.6-.8*ii, 1.2+.4*ii, -.8+.4*ii}}
```

Motivation for a Cloud Service

In some disciplines, cloud computing has become the norm.

Benefits for the user (but there are risks as well):

- No installation is required, just sign up.

  Installing software can be complicated and a waste of time,
  especially if one want to perform a single experiment.
  The user should not worry about upgrading to newer versions.

- We offer a computing service.

  The web server is hosted by a powerful computer,
  which can be extended with the addition of compute servers.

- Files and data are stored and managed for the user.

  The input and output files are managed at the server.
  For larger problems, storage space can become an issue.

Current State of Web Interface

A web interface to the blackbox solver of `phc` is running at `https://kepler.math.uic.edu`.

1. The server `kepler` runs Red Hat Linux.
2. Apache is the web server.
3. Our database is MySQL.
4. Python is the scripting language.

All software is free and open source.

The web service was also deployed and tested on a Mac OS X.

In its current state, the setup of the web interface is minimal, but it works!

Motivation to Classify Polynomial Systems

Some interesting questions:

- How hard is a ***new*** system compared to ones already solved?
  The research community works with benchmark systems which are representative of
  - the difficulties of the problems in the field
  - the capabilities of the software

  but are not really meaningful or directly relevant to ***new*** users.
- Has the ***same*** system already been solved?
  If we have a large database of solved systems,
  then how do we store systems and search the database?

The Classification Problem

If we have solved a system with the same structure,
then the solved system is the start system in a homotopy.

For example, the systems

$$\begin{cases} x^2 + xy^2 - 3 = 0 \\ 2x^2y + 5 = 0 \end{cases} \quad \text{and} \quad \begin{cases} 3 + 2ab^2 = 0 \\ b^2 - 5 + 2a^2b = 0 \end{cases}$$

are isomorphic to each other. There support sets are

$$\{\{(2,0),(1,2),(0,0)\},\{(2,1),(0,0)\}\}$$
$$\text{and} \quad \{\{(0,0),(1,2)\},\{(0,2),(0,0),(2,1)\}\}.$$

Definition

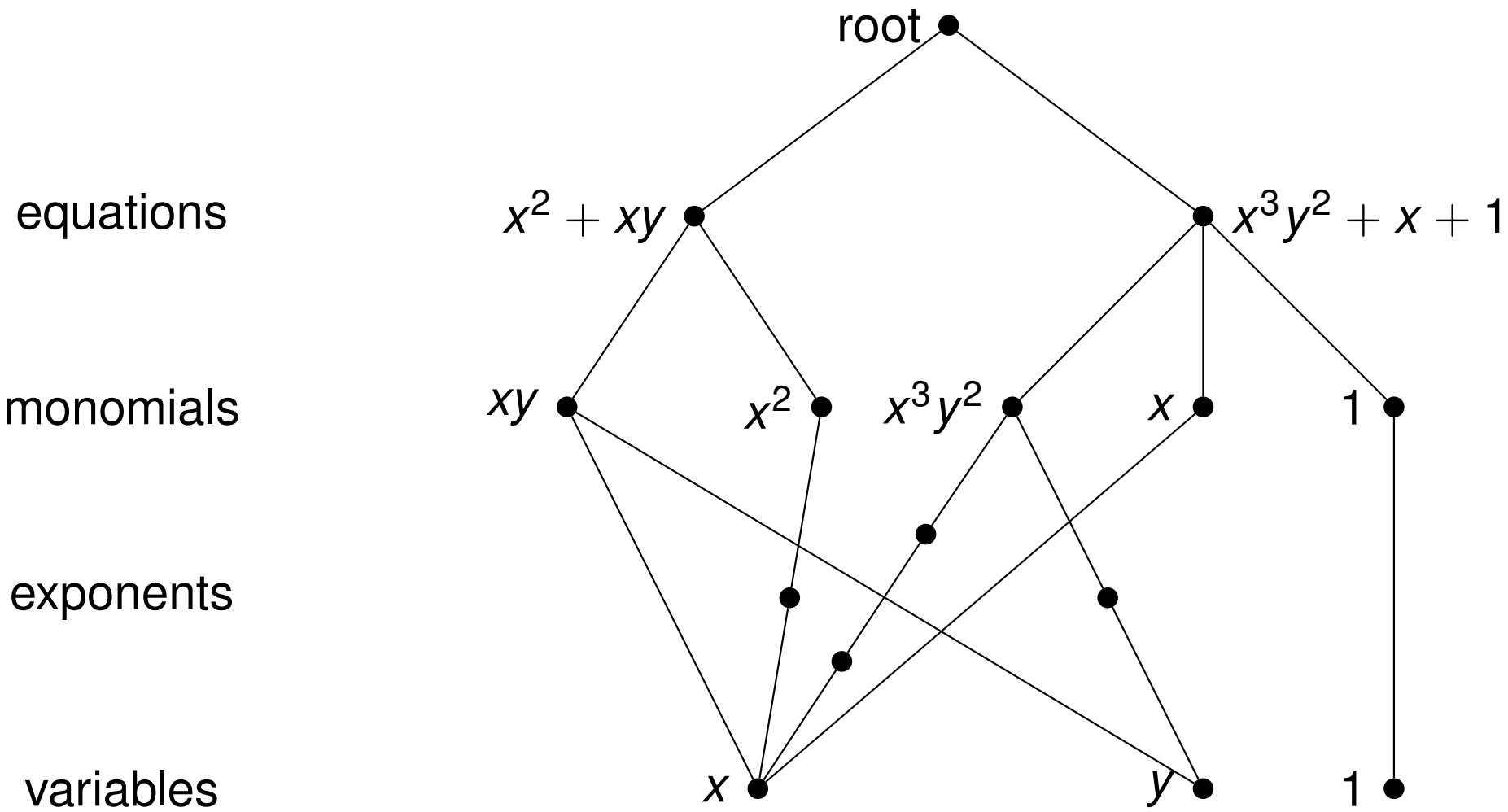
Two sets of support sets are *isomorphic* if there exists a permutation of their equations and variables so that the sets of support sets are identical.

The Isomorphism Problem of Polynomials

Related work occurs in multivariate cryptography.

- J. Patarin. **Hidden fields equations (HFE) and isomorphism of polynomials (IP): Two new families of asymmetric algorithms.** In U. Maurer, editor, *Advances in Cryptology - EUROCRYPT'96*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Springer-Verlag, 1996.
- J.-C. Faugère and L. Perret. **Polynomial equivalence problems: Algorithmic and theoretical aspects.** In S. Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 30–47. Springer-Verlag, 2006.
- C. Bouillaguet, P.-A. Fouque, and A. Véber. **Graph-theoretic algorithms for the "Isomorphism of Polynomials" problem.** In T. Johansson and P. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 211–227. Springer-Verlag, 2013.

Representing a System as a Graph



The Graph Isomorphism Problem

Definition

The *graph isomorphism problem* asks whether for two undirected graphs F, G there is a bijection ϕ between their vertices that preserves incidence;
i.e.: if a and b are vertices connected by an edge in F (respectively G), then $\phi(a)$ and $\phi(b)$ are connected by an edge in G (respectively F).

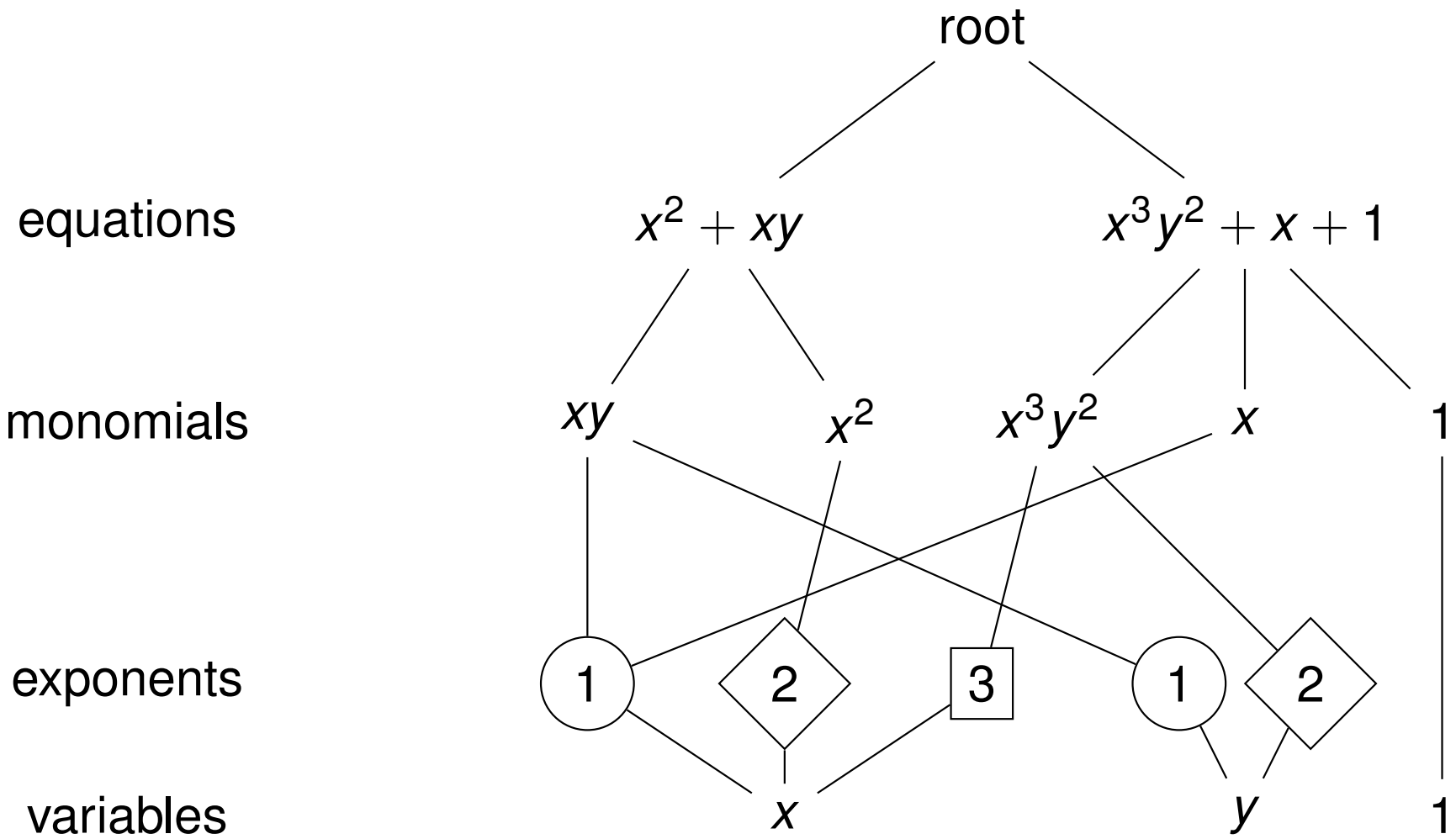
Proposition

The problem of determining whether two sets of support sets are isomorphic is equivalent to the graph isomorphism problem.

A practical solution: the software package **nauty**.

B.D. McKay and A. Piperno. **Practical graph isomorphism, II.** *Journal of Symbolic Computation*, 60:94–112, 2014.

Canonical Graph Labelings with Nauty



Benchmarking Nauty on Cyclic n-roots

$$\text{cyclic 3-roots:} \begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1x_2 + x_2x_3 + x_3x_1 = 0 \\ x_1x_2x_3 - 1 = 0. \end{cases}$$

Times in milliseconds for small values of n,
to compute the canonical form with `nauty`:

n	time	#nodes	#characters
4	0.006	29	526
6	0.006	53	1,256
8	0.006	85	2,545
10	0.007	125	5,121
12	0.007	173	8,761

Note: computing the root counts by `phc -b`
for the cyclic 10-roots problems takes 48.8 seconds.

Cyclic *n*-roots, for large *n*

For larger values of the dimension of the cyclic *n*-root problem, times and sizes of the data start to grow exponentially.

n	time	#nodes	#characters
16	0.010	293	20,029
32	0.045	1,093	168,622
48	0.265	2,405	601,702
64	1.200	4,229	1,427,890
80	4.316	6,565	2,778,546
96	15.274	9,413	4,784,390
112	38.747	12,773	8,595,408
128	80.700	16,645	13,094,752

Note: computing all isolated solutions is no longer possible.
With GPU acceleration, tracking a limited number of paths is possible.

Algebraic Statistics

Algebraic statistics can require solving polynomial systems.

1. Maximum likelihood
2. Parameter identifiability
3. More..?

Gaussian cycle conjecture

A Gaussian cycle conjecture from algebraic statistics leads to a family of square systems.

- M. Drton, B. Sturmfels, and S. Sullivant. **Lectures on algebraic statistics.** Volume 39 of *Oberwolfach Seminars*. Birkhäuser, 2009.
- E. Gross, S. Petrovic, and J. Verschelde. **Interfacing with PHCpack.** Volume 5 of *The Journal of Software for Algebra and Geometry*, pages 20-25. Mathematical Sciences Publishers, 2013.

$$x_{45}y_{24} + x_{55}y_{25} + x_{56}y_{26} = 0, x_{34}y_{13} + x_{44}y_{14} + x_{45}y_{15} = 0$$

$$x_{11} + 2x_{12} + \frac{2}{3}x_{16} - 1 = 0, x_{23}y_{13} + \frac{5}{2}x_{12} + \frac{11}{2}x_{22} = 0$$

$$x_{33}y_{13} + x_{34}y_{14} + \frac{11}{2}x_{23} = 0, x_{44}y_{24} + x_{45}y_{25} + \frac{12}{5}x_{34} = 0$$

$$x_{45}y_{14} + x_{55}y_{15} + \frac{45}{2}x_{56} = 0, x_{56}y_{15} + \frac{22}{3}x_{16} + \frac{45}{2}x_{66} = 0$$

$$\frac{82}{7}x_{12} + \frac{17}{2}x_{22} + \frac{12}{5}x_{23} - 1 = 0, x_{34}y_{24} + \frac{14}{11}x_{23} + \frac{12}{5}x_{33} = 0$$

$$x_{56}y_{25} + x_{66}y_{26} + \frac{82}{7}x_{16} = 0, \frac{12}{5}x_{23} + \frac{282}{5}x_{33} + \frac{102}{14}x_{34} - 1 = 0$$

$$x_{45}y_{35} + \frac{282}{5}x_{34} + \frac{102}{14}x_{44} = 0, x_{55}y_{35} + x_{56}y_{36} + \frac{102}{14}x_{45} = 0$$

$$x_{16}y_{13} + x_{56}y_{35} + x_{66}y_{36} = 0, 10x_{34} + \frac{205}{16}x_{44} + \frac{30}{2}x_{45} - 1 = 0$$

$$x_{56}y_{46} + \frac{205}{16}x_{45} + \frac{30}{2}x_{55} = 0, x_{16}y_{14} + x_{66}y_{46} + \frac{305}{25}x_{56} = 0$$

$$\frac{305}{25}x_{45} + \frac{517}{7}x_{55} + \frac{89}{3}x_{56} - 1 = 0, x_{16}y_{15} + \frac{517}{78}x_{56} + \frac{89}{3}x_{66} = 0$$

$$\frac{450}{21}x_{16} + \frac{89}{3}x_{56} + \frac{293}{19}x_{66} - 1 = 0$$

Gaussian cycle conjecture

Computing isolated solutions with PHCpack:

1. 6 variable case was instantaneous to find 1 solution
2. 21 variable case 8 minutes to find 67 solutions
3. 118 variable case didn't terminate

n	time	#nodes	#characters
6	0.024	53	1,028
21	0.026	194	4,724
118	0.093	1,153	33,472

Conclusions

1. We have a web interface to PHCpack which you should try out! `https://kepler.math.uic.edu`
2. Classifying support sets with nauty is much faster than computing all isolated solutions of a system.

- N. Bliss, J. Sommars, J. Verschelde, X. Yu. **Solving polynomial systems in the cloud with polynomial homotopy continuation.** Volume 9301 of *Lecture Notes in Computer Science*, pages 87-100. Springer-Verlag, 2015.