Polynomial Systems Solving

Burak ŞENER
Mehmet PEKMEZCİ
Mustafa Mert ERGİN
Şefik Temel

Abstract

This work is a survey on the subject Polynomial Systems Solving. First , Polynomial Systems definition is studied , then their solution techniques are studied, finally application areas are discussed.

1 Introduction

1.1 Polynomial

A polynomial is a mathematical expression involving a sum of powers in one or more variables (indeterminates) multiplied by coefficients. A polynomial of order/degree **d** in one variable ($\mathbf{x} \in \mathbf{C}$) (i.e., a univariate polynomial) with constant coefficients ($\mathbf{a_i} \in \mathbf{Q}$) is given by [25]

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d \tag{1}$$

1.1.1 Properties of Polynomials

Properties of polynomials are as follows :

1. A polynomial may not have a term with negative and fractional exponent ($\mathrm{x}^{-\mathrm{n}}$ and $\mathrm{x}^{1/\mathrm{n}}$).
2. $\mathrm{x} \in \mathrm{C}$ and $\mathrm{a_i} \in \mathrm{Q}$
3. Every term ($\mathbf{a_i x^i}$) may be called as monomial (in some books only $\mathbf{x^i}$ is called as monomial).

1.1.2 Solution of Polynomials

Polynomials of orders one to four are solvable using only rational operations and finite root extractions. [25]

1. A first-order equation is trivially solvable.
2. A second-order equation is soluble using the quadratic equation.
3. A third-order equation is solvable using the cubic equation.
4. A fourth-order equation is solvable using the quartic equation.

5. It was proved by Abel and Galois using group theory that general equations of fifth and higher order cannot be solved rationally with finite root extractions (Abel's impossibility theorem).

Solutions of the general quintic equation may be given in terms of **Jacobi theta functions** or **hypergeometric functions** in one variable.[25]

1. Hermite and Kronecker proved that higher order polynomials are not soluble in the same manner.

2. Klein showed that the work of Hermite was implicit in the group properties of the icosahedron. Klein's method of solving the quintic in terms of hypergeometric functions in one variable can be extended to the sextic, but for higher order polynomials, either hypergeometric functions in several variables or "Siegel functions" must be used (Belardinelli 1960, King 1996, Chow 1999).

3. In the 1880s, Poincaré created functions which give the solution to the nth order polynomial equation in finite form. These functions turned out to be "natural" generalizations of the elliptic functions.

1.2 Polynomial System

A system of (multivariate) polynomial equations is a set of simultaneous equations $f_1 = 0$, ..., $f_m = 0$ where the f_i are polynomials in several variables, say x_1, ..., x_n, over some field k (usually $\mathbb{C}$ or $\mathbb{R}$). [24].

In abstract algebra books, a **Polynomial System** is called as **Polynomial Ring** or **Polynomial Algebra**. [25] Abstract algebraic notions are explained in the section 2.

A **Univariate Polynomial System** (coefficients $a_{ij} \in R$ and i,j,n $\in N$) may be given as m equations:

$$\begin{cases} a_{10} + a_{11}x + a_{12}x^2 + a_{13}x^3 + a_{14}x^4 + \ldots + a_{1d}x^d = 0 \\ a_{20} + a_{21}x + a_{22}x^2 + a_{13}x^3 + a_{14}x^4 + \ldots + a_{2d}x^d = 0 \\ a_{30} + a_{31}x + a_{12}x^2 + a_{13}x^3 + a_{14}x^4 + \ldots + a_{3d}x^d = 0 \\ \vdots \\ a_{m0} + a_{m1}x + a_{m2}x^2 + a_{m3}x^3 + a_{m4}x^4 + \ldots + a_{md}x^d = 0 \end{cases} \tag{2}$$

A **Bivariate Polynomial System** (variables $x, y \in R$, coefficients $a_{ij} \in R$ and i,j,n $\in N$) may be given as m equations :

$$\begin{cases} a_{00} + a_{01}xy + a_{02}xy^2 + a_{03}xy^3 + \ldots + a_{0(d\times d)}x^dy^d = 0 \\ a_{10} + a_{11}xy + a_{12}xy^2 + a_{13}xy^3 + \ldots + a_{1(d\times d)}x^dy^d = 0 \\ a_{20} + a_{21}xy + a_{22}xy^2 + a_{23}xy^3 + \ldots + a_{2(d\times d)}x^dy^d = 0 \\ \vdots \\ a_{m00} + a_{m11}xy + a_{m12}xy^2 + a_{m13}xy^3 + \ldots + a_{m(d\times d)}x^dy^d = 0 \end{cases} \tag{3}$$

A **Multivariate Polynomial System** (N variables $x_1 \ldots x_N \in R$, coefficients $a_{ij} \in R$ and i,j,n $\in N$) may be given as m equations :

$$\begin{cases} a_{00} + \sum_{i_1,\dots,i_n}^{d} a_{0i}{x_1}^{i_1}{x_2}^{i_2}\dots {x_n}^{i_n} = 0 \\ a_{10} + \sum_{i_1,\dots,i_n}^{d} a_{1i}{x_1}^{i_1}{x_2}^{i_2}\dots {x_n}^{i_n} = 0 \\ \vdots \\ a_{m0} + \sum_{i_1,\dots,i_n}^{d} a_{mi}{x_1}^{i_1}{x_2}^{i_2}\dots {x_n}^{i_n} = 0 \end{cases} \tag{4}$$

2 Abstract Algeraic Notions

[22]

3 Geometrical Meaning

An affine variety $\mathrm{V}(\mathrm{f}_1 \dots \mathrm{f}_\mathrm{s}) \subset \mathrm{k}^\mathrm{n}$ is the set of all solutions of the system of equations $\mathrm{f}_1(\mathrm{x}_1 \dots \mathrm{x}_\mathrm{n}) = \dots = \mathrm{f}_\mathrm{s}(\mathrm{x}_1 \dots \mathrm{x}_\mathrm{n}) = 0$. We will use the letters V,W,etc. to denote affine varieties. [28]

The conic sections studied in analytic geometry (circles, ellipses, parabolas) are affine varieties. Likewise, graphs of polynomial functions are affine varieties [the graph of $\mathbf{y} = \mathbf{f}(\mathbf{x})$ is $\mathbf{V}(\mathbf{y} - \mathbf{f}(\mathbf{x}))$]. Although not as obvious, graphs of rational functions are also affine varieties. For example, consider the graph of $\mathbf{y} = \frac{\mathbf{x^3-1}}{\mathbf{x}}$:

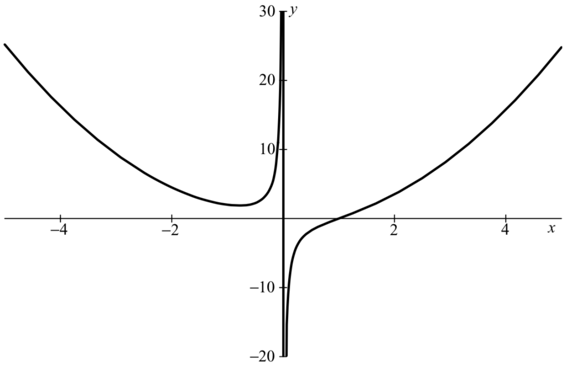

Figure 1

3-dimensional space example. A nice affine variety is given by paraboloid of revolution $\mathbf{V}(\mathbf{z} - \mathbf{x^2} - \mathbf{y})$, which is obtained by rotating the parabola $\mathbf{z} = \mathbf{x^2}$ about the z-axis. This gives us the picture:

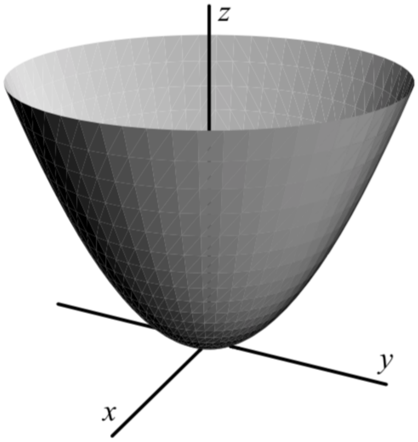

Figure 2

A much more complicated surface is given by $\mathbf{V(x^2 - y^2z^2 + z^3)}$:

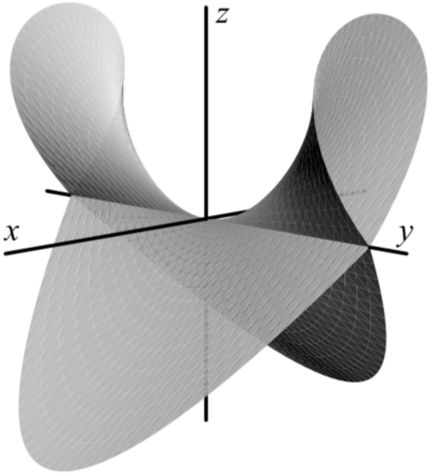

Figure 3

4 Polynomial Systems Solution Methods

5 Solver Software

There are many kind of solving softwares available for polynomial systems. We can separate them to two groups as native libraries and services. Native libraries In this section three libraries will be explained.

5.1 Libraries

Michael Thomas Flanagan's Java Scientific Library Flanagan library has many kind of operational functions, graph plotting, regression, polynomial operations, data smoothing etc. This library has many useful advantages but use for commercial purposes isn't permitted.

M4GB [27] is an efficient algorithm for computing Grobner-Bases. It's an extension of Buchberger's algorithm. It stores already computed (tail-)reduced multiples of basis polynomials to prevent redundant work in reduction step. And it exploits efficient linear algebra for the reduction step. They run a benchmark test with four libraries, OpenF4, FGb, Magma and M4GB. Others are different libraries to compute Grobner-Bases.

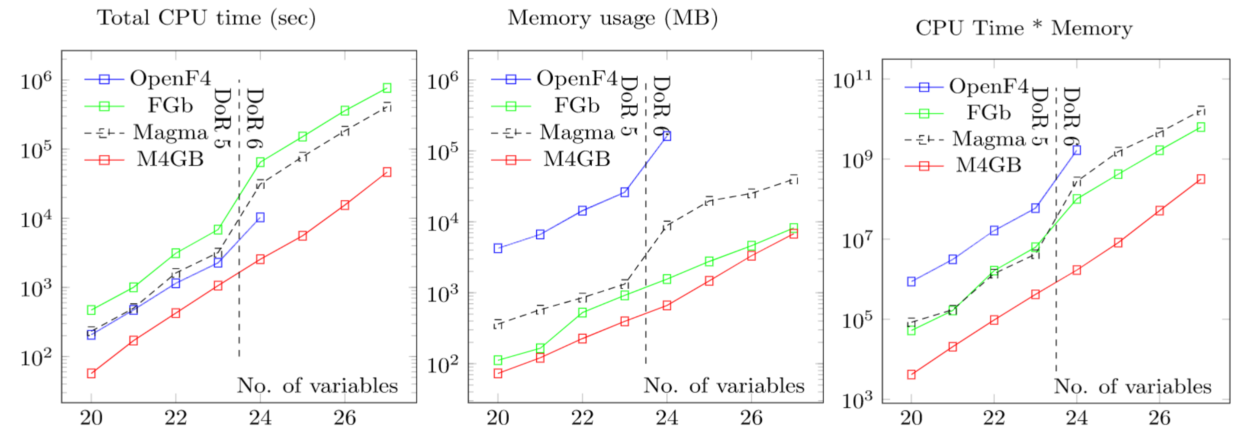

Figure 4: equations = variables * 2

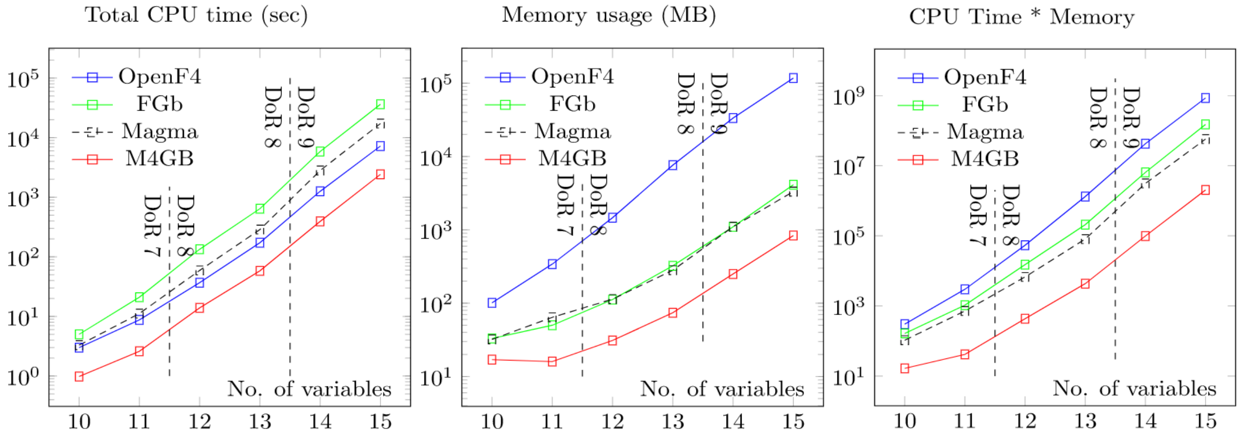

Figure 5: results for equations = variables + 1

6 Applications

Systems of polynomial equations show up in many applications areas such as robotics (kinematics,motion planning, collision detection, etc.), computer vision (object modeling, surface fitting,recognition, etc.), graphics, geometric modeling (curve and surface intersections), computer-aided design, mechanical design, and chemical equilibrium systems. [26]

6.1 Robotics

System of polynomial equations may use to model a robot arm. If $(\mathbf{x_i}, \mathbf{y_i})$ is the coordinates of some joint, $(\mathbf{x_i+1}, \mathbf{y_i+1})$ is the coordinates of the next joint (or the hand) and the segment has length Li then we get the equation [23]

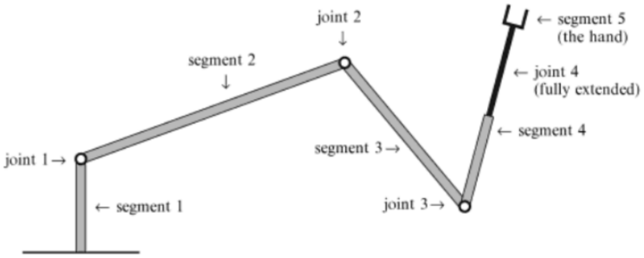

Figure 6: Robot Arm

$$(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2 = L_i^2 \tag{5}$$

Note that the angle at the i-th joint can be computed from the equations

$$x_{i+1} - x_i = L_i \cos(\theta_i) \tag{6}$$

$$y_{i+1} - y_i = L_i \sin(\theta_i) \tag{7}$$

6.2 Geometry

Many statements in Euclidean geometry can be formulated as result about systems of polynomial equations.[23]

Example: Euclidean geometry says that *the bisectors of the three sides of a triangle meet in one point.*

One vertex, A, of the triangle can be assumed to be the origin and another, B, to have coordinates (c, 0), without loss of generality. The third vertex, C, has coordinates (a,b). The bisectors of AB and BC meet in some point, with coordinates (x1, y1). We get the following equations

$$x_1 - \frac{c}{2} = 0 \tag{8}$$

$$\frac{c-a}{b} \cdot x_1 - y_1 + \frac{a^2 + b^2 - c^2}{2b} = 0 \tag{9}$$

Similarly, if (x2,y2) are the coordinates of the intersection of the bisectors of AB and AC we have

$$x_2 - \frac{c}{2} = 0 \tag{10}$$

$$\frac{a}{b} \cdot x_2 + y_2 - \frac{b^2 + a^2}{2b} = 0 \tag{11}$$

7 Conclusion

References

[1] Strumfels Bernd, *Solving Systems of Polynomial Equations*, American Mathematical Society , Conference Board of Mathematical Sciences, Berkeley,CA, 2002.

[2] Manocha Dinesh, *Solving Systems of Polynomial Equations*, IEEE Computer Graphics and Applications University of North Carolina, 1994.

[3] L.H. Zhi and Y. Notake and H. Kai and M.-T. Noda and K.I. Shiraishi, *Hybrid Method for Solving Polynomial Equations*, Proceedings of the Asian Technology Conference in Mathematics, pp.492-501, Guangzhou, China, 1999.

[4] Bard Gregory, *Algorithms for Solving Linear and Polynomial Systems of Equations Over Finite Fields With Applications to Cryptanalysis*, University of Maryland PHD Thesis, 2007.

[5] Luk Bettale 1 , Jean-Charles Faugère, Ludovic Perret, *Solving multivariate polynomial systems over finite fields : Hybrid approach*, Journées Nationales du Calcul Formel, UPMC, CNRS, INRIA Paris-Rocquencourt, 2002.

[6] M. MORHAC, *One-Modulus Residue Arithmetic Algorithm to Solve Linear Equations Exactly*, Institute of Physics, Slovak Academy of Sciences Bratislava, Slovakia, 1994.

[7] I.Z. Emiris, A. Mantzaflaris, E. Tsigaridas, *On the Bit Complexity of Solving Bilinear Polynomial Systems*, Johan Radon Institute for Computational Mathematics, Austrian Academy Of Sciences, 2016.

[8] Jan Verschelde, *Homotopy Methods for Solving Polynomial Systems*, ISSAC'05 Beijing, China, 2005.

[9] Nicolas Courtois , Alexander Klimov , Jacques Patarin , Adi Shamir *Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations*, International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT-2000, 2000.

[10] Daniel Lazard, *Thirty years of Polynomial System Solving, and now?*, Journal of Symbolic Computation , UPMC Univ. Paris, France, 2008.

[11] Changbo Chen, *Solving Polynomial Systems via Triangular Decomposition*, PHD Thesis The University of Western Ontario, 2011.

[12] Jean-Charles Faugère, Pierrick Gaudry, Louise Huot, Guénaël Renault, *Polynomial Systems Solving by Fast Linear Algebra*, HAL ¡hal-00816724v1¿, 2013.

[13] Didier Bondyfalat, Bernard Mourrain ,Victor Y. Pan *Controlled iterative methods for solving polynomial systems*, ISSAC 98 , 1998.

[14] M. G. MARINARI, H. M. MÖLLER, AND T. MORA *ON MULTIPLICITIES IN POLYNOMIAL SYSTEM SOLVING*, TRANSACTIONS OF THE AMERICAN MATHEMATICAL SOCIETY, 1996.

[15] Changbo Chen, Marc Moreno Maza, *Algorithms for computing triangular decomposition of polynomial systems*, Journal of Symbolic Computation, 2012.

[16] Tien-Yien Li, *SOLVING POLYNOMIAL SYSTEMS BY POLYHEDRAL HOMOTOPIES*, TAIWANESE JOURNAL OF MATHEMATICS, 1999.

[17] Timothy Duff, Cvetelina Hill , Anders Jensen, Kisun Lee, Anton Leykin, Jeff Sommars, *Solving polynomial systems via homotopy continuation and monodromy*, CoRR, 2017.

[18] Andrew J. Sommese , Jan Verschelde , Charles W. Wampler , *Solving Polynomial Systems Equation by Equation*, Dickenstein A., Schreyer FO., Sommese A.J. (eds) Algorithms in Algebraic Geometry, 2006.

[19] Dan Bates, *Course Notes for Math 676: Computational Algebraic Geometry Spring 2009*, Colorado State University, 2009.

[20] Chenqi Mou, *Solving Polynomial Systems over Finite Fields:Algorithms, Implementation and Applications*, HAL, Université Pierre et Marie Curie, 2013.

[21] Caminata Alessio , Gorla Elisa. *Solving Multivariate Polynomial Systems and an Invariant from Commutative Algebra.* , 2017.

[22] Karl-Heinz Fieseler, *Groups, Rings and Fields* , Upsalla 2010.

[23] Johan Richter, *Systems of polynomial equations*, 2013.

[24] *https://en.wikipedia.org/wiki/System_of_polynomial_equations*, Wikipedia,2018.

[25] *http://mathworld.wolfram.com/Polynomial.html*, Wolfram,2018.

[26] *https://pdfs.semanticscholar.org/295c/9b5d5e1120fdb3d5cf2386d8f6a92884d9f5.pdf*, Yan-Bin Jia,2017.

[27] Rusydi Makarim, Marc Stevens *M4GB: An Efficient Gröbner-Basis Algorithm*, ISSAC 2017.

[28] Cox, Little, O'Shea, *Ideals, Varieties, and Algorithms Book*,