

# 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 Monomials

A monomial in  $x_1, x_2, \dots, x_n$  is a product of the form

$$x_1^{\alpha_1} \times x_2^{\alpha_2} \dots \times x_n^{\alpha_n} \quad (1)$$

where all of the exponents  $\alpha_1, \dots, \alpha_n$  are nonnegative integers. The total degree of this monomial is the sum  $\alpha_1 + \dots + \alpha_n$ .

### 1.2 Polynomials

A polynomial  $f$  in  $x_1, x_2, \dots, x_n$  with coefficients in a field  $k$  is a finite linear combination (with coefficients in  $k$ ) of monomials. We will write a polynomial  $f$  in the form :[29]

$$f = \sum_{\alpha} a_{\alpha} x^{\alpha}, a^{\alpha} \in k, \alpha \in Z, x^{\alpha} \in C \quad (2)$$

where the sum is over a finite number of  $n$ -tuples  $\alpha = (\alpha_1, \dots, \alpha_n)$ . The set of all polynomials in  $x_1, x_2, \dots, x_n$  with coefficients in  $k$  is denoted  $k[x_1, x_2, \dots, x_n]$ .

A polynomial of order/degree  $\mathbf{d}$  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]

$$P(x) = a_0 + a_1x + a_2x^2 + \dots + a_dx^d \quad (3)$$

#### 1.2.1 Properties of Polynomials

Properties of polynomials are as follows :

1. A polynomial may not have a term with negative and fractional exponent ( $x^{-n}$  and  $x^{1/n}$ ).
2.  $x \in C$  and  $a_i$  may be either  $\in Q$  or  $\in R$  or  $\in C$ , that we call field  $k$ .
3. Every term ( $\mathbf{a}_i \mathbf{x}^{\mathbf{i}}$ ) is composed of a coefficient ( $\mathbf{a}_i$ ) and a monomial ( $\mathbf{x}^{\mathbf{i}}$ ).

### 1.2.2 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.

### 1.3 Polynomial System

A system of (multivariate) polynomial equations is a set of simultaneous equations  $f_1 = 0, \dots, f_m = 0$  where the  $f_i$  are polynomials in several variables, say  $x_1, \dots, x_n$ , 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  $a_{ij} \in \mathbb{R}$  and  $i, j, n \in \mathbb{N}$ ) may be given as  $m$  equations:

$$\begin{cases} a_{10} + a_{11}x + a_{12}x^2 + a_{13}x^3 + a_{14}x^4 + \dots + a_{1d}x^d = 0 \\ a_{20} + a_{21}x + a_{22}x^2 + a_{23}x^3 + a_{24}x^4 + \dots + a_{2d}x^d = 0 \\ a_{30} + a_{31}x + a_{32}x^2 + a_{33}x^3 + a_{34}x^4 + \dots + a_{3d}x^d = 0 \\ \vdots \\ a_{m0} + a_{m1}x + a_{m2}x^2 + a_{m3}x^3 + a_{m4}x^4 + \dots + a_{md}x^d = 0 \end{cases} \quad (4)$$

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

$$\begin{cases} a_{00} + a_{01}xy + a_{02}xy^2 + a_{03}xy^3 + \dots + a_{0(d \times d)}x^d y^d = 0 \\ a_{10} + a_{11}xy + a_{12}xy^2 + a_{13}xy^3 + \dots + a_{1(d \times d)}x^d y^d = 0 \\ a_{20} + a_{21}xy + a_{22}xy^2 + a_{23}xy^3 + \dots + a_{2(d \times d)}x^d y^d = 0 \\ \vdots \\ a_{m00} + a_{m11}xy + a_{m12}xy^2 + a_{m13}xy^3 + \dots + a_{m(d \times d)}x^d y^d = 0 \end{cases} \quad (5)$$

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

$$\begin{cases} a_{00} + \sum_{i_1, \dots, i_n}^d a_{0i} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} = 0 \\ a_{10} + \sum_{i_1, \dots, i_n}^d a_{1i} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} = 0 \\ \vdots \\ a_{m0} + \sum_{i_1, \dots, i_n}^d a_{mi} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} = 0 \end{cases} \quad (6)$$

## 2 Abstract Algebraic Notions

The following abstract algebraic notions are explained briefly in order to understand better the polynomials and their relation to the geometry. **At the heart of the group theory, symmetry lies.** All the contents in this section is taken either from [22] or [29] if not cited explicitly.

### 2.1 Group

A group is a pair  $(G, \mu)$  with a non-empty set  $G$  and a “binary operation”  $(\mu)$  that satisfies :

1. **Closure** :  $a, b \in G \implies \mu(a, b) \in G$
2. **Associativity** :  $a, b, c \in G, \mu(\mu(a, b), c) = \mu(a, \mu(b, c))$
3. **Neutral Element** :  $\exists e \in G, \forall a \in G, \mu(a, e) = \mu(e, a) = a$
4. **Inverse Element** :  $\forall a \in G, \exists a^{-1} \in G, \mu(a, a^{-1}) = \mu(a^{-1}, a) = e$

**For Example** :  $(\mathbb{N}, +), (\mathbb{R} \setminus \{0\}, \cdot)$ .

#### 2.1.1 Commutative (Abelian) Group

if a group has the commutativity property, it is called commutative (Abelian) group.

1. **Commutativity** :  $\forall a, b \in G, \mu(a, b) = \mu(b, a)$

### 2.1.2 Homomorphism

A map(function) between two groups  $(\phi : G \rightarrow H)$ , is called Homomorphism iff

$$\phi(a + b) = \phi(a) * \phi(b) \quad (7)$$

$(a, b \in G, (G, +), (H, *))$

For example exponential function (or map) is a Homomorphism because  $e^{(a+b)} = e^a \cdot e^b$ ,

1. **Isomorphism** : if  $\phi$  is bijective
2. **Automorphism** : Isomorphism with  $G=H$

## 2.2 Ring

Every ring is a group with one additional operation. (i.e.  $(G, +, \cdot)$ ). More formally, a ring is a triple  $(R, \alpha, \mu)$ , with a set  $R$  together with two maps(or functions, or operations) :

$$\alpha : R \times R \rightarrow R, (a, b) \rightarrow a + b := \alpha(a, b), \text{addition} \quad (8)$$

and

$$\mu : R \times R \rightarrow R, (a, b) \rightarrow a \cdot b := \mu(a, b), \text{multiplication} \quad (9)$$

such that :

1. The pair  $(R, \alpha)$  is an (additively written) commutative (abelian) group.
2. The multiplication  $\mu$  is associative :  $(ab)c = a(bc)$ ,  $a, b, c \in R$
3. The multiplication is “distributive” over the addition :  $a(b + c) = ab + ac$ ,  $(a + b)c = ac + bc$ ,  $\forall a, b, c \in R$ .

For example,  $(\mathbb{Z}, +, \cdot)$  forms a ring.

### 2.2.1 Commutative (Abelian) Ring with Unity

A ring is commutative with unity if :

1. There is an element  $1 \in R \setminus \{0\}$ , such that  $1a = a = a1, \forall a \in R$
2. The multiplication is commutative :  $ab = ba, \forall a, b \in R$ .

### 2.2.2 Polynomial Ring

The sum and product of two polynomials is again a polynomial. We say that a polynomial  $f$  divides a polynomial  $g$  provided that  $g = f \cdot h$  for some polynomial  $h \in k[x_1, x_2, \dots, x_n]$ .

One can show that, under addition and multiplication,  $k[x_1, x_2, \dots, x_n]$  satisfies all of the field axioms except for the existence of multiplicative inverses (because, for example,  $1/x$  is not a polynomial).

Such a mathematical structure is called a commutative ring and for this reason we will refer to  $k[x_1, x_2, \dots, x_n]$  as a **polynomial ring**. The coefficients of the polynomials are the elements of a Polynomial Ring. (We put the  $a_i$  instead of  $x_i$ )

## 2.3 Field

A field is a commutative ring with identity (1), in which every non-zero element has a multiplicative inverse.<sup>1</sup>

For example : the rings  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  are actually fields.

## 2.4 Affine Space

Given a field  $k$  and a positive integer  $n$ , we define the  $n$ -dimensional affine space over  $k$  to be the set

$$k^n = \{(a_1, \dots, a_n) | a_1, \dots, a_n \in k\} \quad (10)$$

For an example of affine space, consider the case  $k = \mathbb{R}$ . Here we get the familiar space  $\mathbb{R}^n$  from calculus and linear algebra. In general, we call  $k^1 = k$  affine line, and  $k^2$  affine plane.

### 2.4.1 Affine vs Vector Space

<sup>2</sup>An affine space is basically a vector space that doesn't necessarily have an identity vector. Vector spaces and Affine spaces are abstractions of different properties of Euclidean space. Like many abstractions, once abstracted they become more general.

A Vector space abstracts linearity/linear combinations. This involves the concept of a zero, scaling things up and down, and adding them to each other.

An Affine space abstracts the affine combinations. You can think of an affine combination as a weighted average, or a convex hull (if you limit the coefficients to be between 0 and 1). As it turns out, you do not need a zero, nor do you need the concept of "scaling", nor do you need full on addition, in order to have a concept of weighted average and convex hull within a space.

If you look at the Earth, the lines of longitude have a zero point, but that zero point is arbitrary – it has no meaning. The lines of longitude are an affine space. We measure them in degrees (or radians), and we have picked a zero, but other than it being useful to agree where the zero is, it isn't a special line.

The space of rotations around a circle, on the other hand, have a zero that is meaningful – zero means you don't rotate. We measure them as a vector space.

The lines of longitude are measured as rotations away from our arbitrary point we assigned zero. But what matters about them is the ability to say how far apart two longitude are from each other, not any one line's absolute value.

If we were doing some math and it would be useful to move the zero of longitude, we are free to do so. But if we want to move the zero in the space of rotation (to say bending things 90 degrees) we are not nearly as free.

In general, your location is an affine space, as there is no special place, and scaling your location by a factor of 3 makes no sense, and adding two locations makes no sense – but taking the average of two locations makes sense.

The (directed) distance between locations is a vector space. Saying something is twice as far as another distance makes sense, the "same place" (distance zero) makes sense, and adding two directed distances together makes sense.

<sup>1</sup><http://www-history.mcs.st-and.ac.uk/~john/MT4517/Lectures/L4.html>

<sup>2</sup><https://math.stackexchange.com/questions/884666/what-are-differences-between-affine-space-and-vector-space>

And you can pick a spot and describe locations as the directed distance from that particular spot, but the spot picked was arbitrary, and if it would be useful to pick a different spot, you are free to.

## 2.4.2 How Polynomials Relate to Affine Space

[29] The key idea is that a polynomial

$$f = \sum_{\alpha} a_{\alpha} x^{\alpha}, f \in k, a_{\alpha} \in k, \alpha \in Z, x^{\alpha} \in C \quad (11)$$

gives the function

$$f = k^n \rightarrow k \quad (12)$$

defined as follows: given  $(\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n) \in \mathbf{k}^n$ , replace every  $x_i$  by  $a_i$  in the expression for  $f$ . Since all of the coefficients also lie in  $k$ , this operation gives an element  $\mathbf{f}(\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n) \in \mathbf{k}$ . The ability to regard a polynomial as a function is what makes it possible to link algebra and geometry.

## 2.5 Affine Varieties

[29] Affine Variety is a geometric object defined as follows :

Let  $k$  be a field, and let  $f_1, f_2, \dots, f_n$  be polynomials  $\in k[x_1, \dots, x_n]$ . Then we set

$$V(f_1, \dots, f_s) = \{(a_1, \dots, a_n) \in k^n \mid f_i(a_1, \dots, a_n) = 0, \forall i, 1 \leq i \leq s\} \quad (13)$$

We call affine variety  $V(f_1, \dots, f_s)$  defined by  $f_1, \dots, f_s$ .

Thus, an affine variety  $V(f_1, \dots, f_s) \subseteq k^n$  is the set of all solutions of the system of equations  $f_1(x_1, \dots, x_n) = \dots = f_s(x_1, \dots, x_n) = 0$ . We will use the letters  $V, W$ , etc. to denote affine varieties.

### 2.5.1 Example 1

The variety  $V(x^2 + y^2 - 1) \subseteq \mathbb{R}^2$  is the circle of radius 1 centered at the origin :

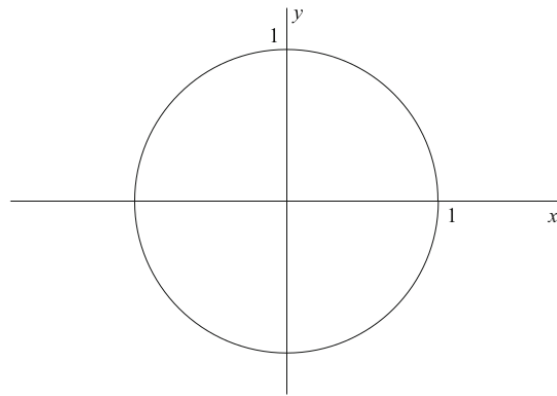


Figure 1

### 2.5.2 Example 2

The variety  $V((x^2 + y^2 - 1)(3x + 6y - 4)) \subseteq \mathbb{R}^2$  defines all the points satisfying the circle of radius 1 centered at the origin and the line defined by the equation  $(3x+6y-4)$ :

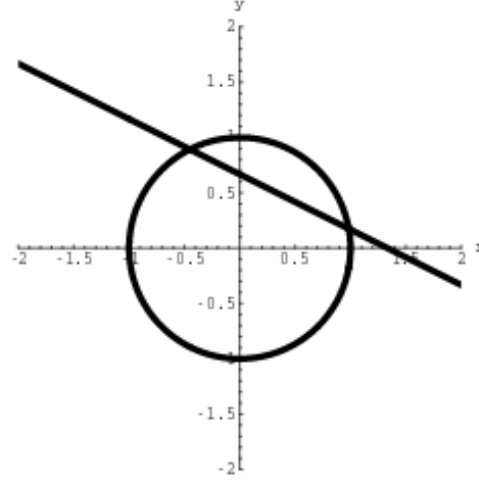


Figure 2  
3

## 2.6 Ideal

Ideal is an algebraic object. The real importance of ideals is that they will give us a language for computing with affine varieties. In the next section we will define relation between polynomials, varieties (geometric object) and ideals (algebraic objects).

### Definition 1 :

$R$  is a commutative ring, a subset  $I \subseteq k[x_1, \dots, x_n]$  ( $I \subseteq R$ ) is an **Ideal** if it satisfies :

1.  $0 \in I$
2.  $f, g \in I \implies f + g \in I$
3.  $f \in I, h \in R, \implies h \cdot f \in I$

### Example 1 :

$(\mathbb{Z}, +, \cdot)$  is a commutative ring, Even numbers  $(2\mathbb{Z}, +, \cdot)$  is an ideal.

### Definition 2 :

Let  $f_1, \dots, f_s$  be a polynomial ring, in other words, be polynomials in  $k[x_1, \dots, x_n]$  then we set

$$\langle f_1, \dots, f_s \rangle = \left\{ \sum_{i=1}^s h_i \cdot f_i \mid h_1, \dots, h_s \in k[x_1, \dots, x_n] \right\} \quad (14)$$

$\langle f_1, \dots, f_s \rangle$  is an ideal **generated by**  $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ .

## 2.7 Relation Between Algebra and Geometry

### Proposition 1 :

if  $f_1, \dots, f_s$  and  $g_1, \dots, g_t$  are bases of the same ideal in the ring  $k[x_1, \dots, x_n]$  so that  $\langle f_1, \dots, f_s \rangle = \langle g_1, \dots, g_t \rangle$ , then we have  $V(f_1, \dots, f_s) = V(g_1, \dots, g_t)$

### Example 1 :

As an example, consider the variety  $V(2x^2 + 3y^2 - 11, x^2 - y^2 - 3)$ .

It is easy to show that  $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \rangle = \langle x^2 - 4, y^2 - 1 \rangle$  so that

$$V(2x^2 + 3y^2 - 11, x^2 - y^2 - 3) = V(x^2 - 4, y^2 - 1) = \{(+/-2, +/-1)\}$$

by the above proposition. Thus, by changing the basis of the ideal, we made it easier to determine the variety.



<b>ALGEBRA</b>		<b>GEOMETRY</b>
radical ideals		varieties
$I$	$\longrightarrow$	$\mathbf{V}(I)$
$\mathbf{I}(V)$	$\longleftarrow$	$V$
addition of ideals		intersection of varieties
$I + J$	$\longrightarrow$	$\mathbf{V}(I) \cap \mathbf{V}(J)$
$\sqrt{\mathbf{I}(V) + \mathbf{I}(W)}$	$\longleftarrow$	$V \cap W$
product of ideals		union of varieties
$IJ$	$\longrightarrow$	$\mathbf{V}(I) \cup \mathbf{V}(J)$
$\sqrt{\mathbf{I}(V)\mathbf{I}(W)}$	$\longleftarrow$	$V \cup W$
intersection of ideals		union of varieties
$I \cap J$	$\longrightarrow$	$\mathbf{V}(I) \cup \mathbf{V}(J)$
$\mathbf{I}(V) \cap \mathbf{I}(W)$	$\longleftarrow$	$V \cup W$
ideal quotients		difference of varieties
$I : J$	$\longrightarrow$	$\overline{\mathbf{V}(I) \setminus \mathbf{V}(J)}$
$\mathbf{I}(V) : \mathbf{I}(W)$	$\longleftarrow$	$V \setminus W$
elimination of variables		projection of varieties
$I \cap k[x_{l+1}, \dots, x_n]$	$\longleftrightarrow$	$\overline{\pi_I(\mathbf{V}(I))}$
prime ideal	$\longleftrightarrow$	irreducible variety
minimal decomposition		minimal decomposition
$I = P_1 \cap \dots \cap P_m$	$\longrightarrow$	$\mathbf{V}(I) = \mathbf{V}(P_1) \cup \dots \cup \mathbf{V}(P_m)$
$\mathbf{I}(V) = \mathbf{I}(V_1) \cap \dots \cap \mathbf{I}(V_m)$	$\longleftarrow$	$V = V_1 \cup \dots \cup V_m$
maximal ideal	$\longleftrightarrow$	point of affine space
ascending chain condition	$\longleftrightarrow$	descending chain condition

Figure 3

### 3 Geometrical Meaning

An affine variety  $\mathbf{V}(f_1 \dots f_s) \subset \mathbb{A}^n$  is the set of all solutions of the system of equations  $f_1(x_1 \dots x_n) = \dots = f_s(x_1 \dots x_n) = 0$ . We will use the letters  $V, W$ , etc. to denote affine varieties. [29]

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  $y = \frac{x^3-1}{x}$  :

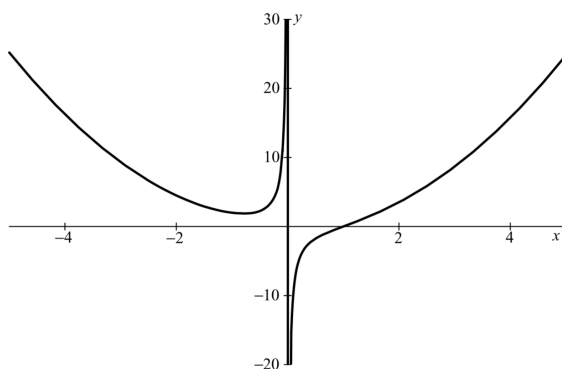


Figure 4

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

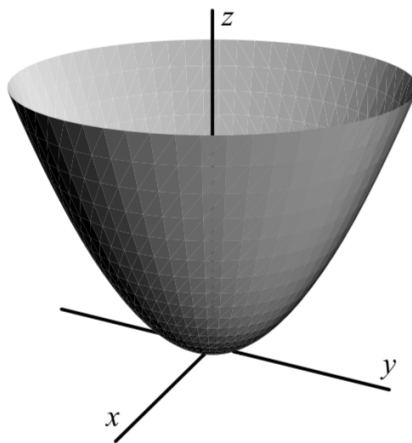


Figure 5

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

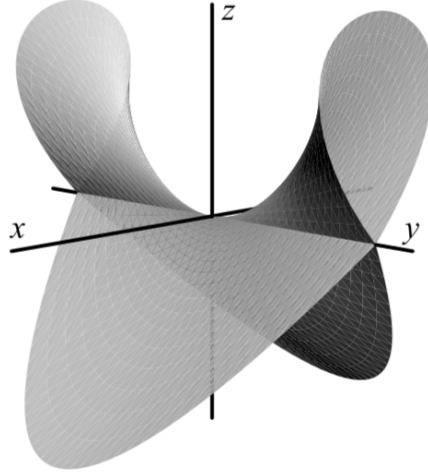


Figure 6

## 4 Polynomial Systems Solution Methods

## 5 Solver Software

There are many solving softwares available for computing polynomial systems.

**M4GB** [27] is an efficient algorithm for computing Grobner-Bases written in C. It's an extension of Buchberger's algorithm. It stores already computed (tail-)reduced multiplies 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.

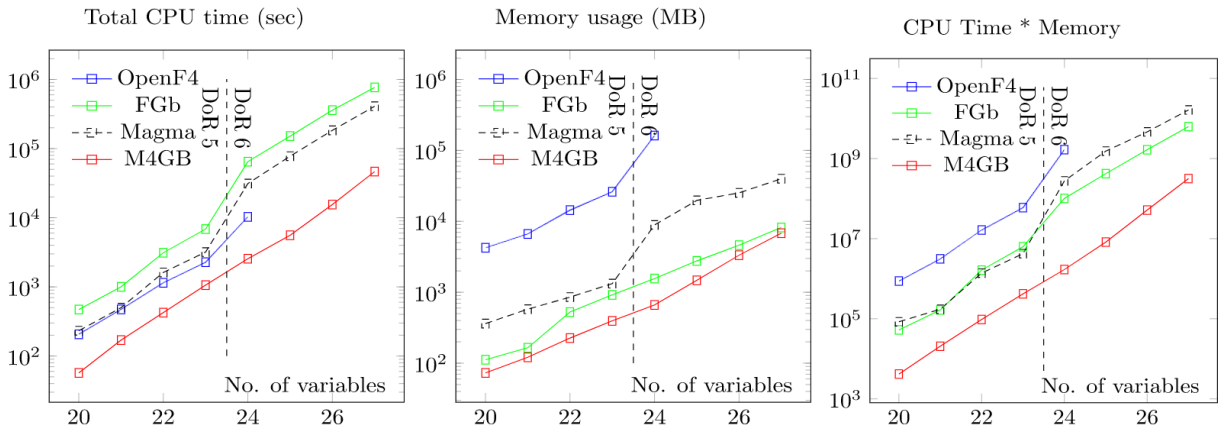


Figure 7: results for equations = variables \* 2

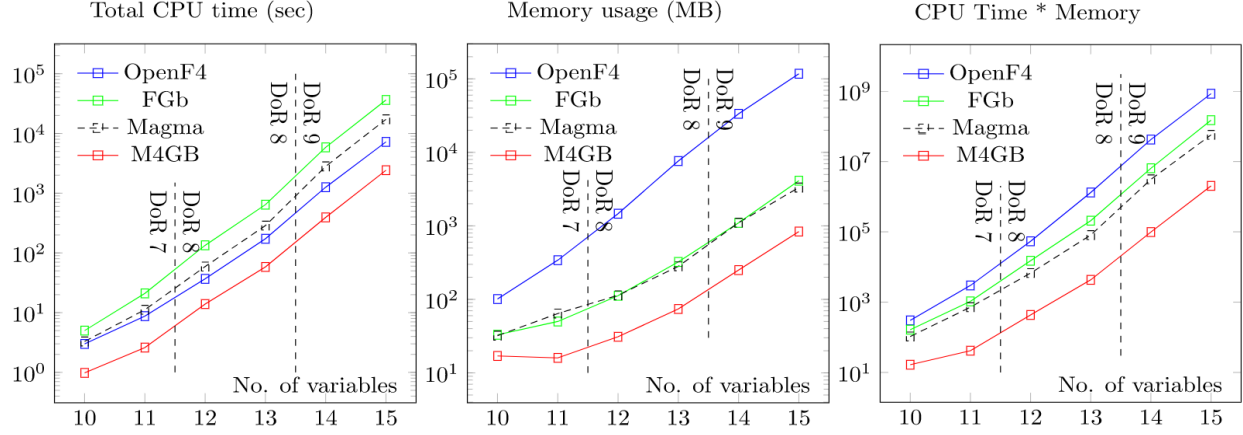


Figure 8: results for equations = variables + 1

**SymPy** [28] is a Python open-source library for symbolic mathematics. For groebnar-bases calculation it has `sympy.polys.polytools.groebner(F, *gens, **args)` method. it uses `order` argument to set the monomial ordering that will be used to compute the basis. Order argument can be "lex", "grlex" and "grevlex". Default order is "lex" example usages are below.

```
>>> groebner([x*y - 2*y, 2*y**2 - x**2], x, y, order='lex')
GroebnerBasis([x**2 - 2*y**2, x*y - 2*y, y**3 - 2*y], x, y, domain='ZZ', order='lex')

>>> groebner([x*y - 2*y, 2*y**2 - x**2], x, y, order='grlex')
GroebnerBasis([y**3 - 2*y, x**2 - 2*y**2, x*y - 2*y], x, y, domain='ZZ', order='grlex')

>>> groebner([x*y - 2*y, 2*y**2 - x**2], x, y, order='grevlex')
GroebnerBasis([y**3 - 2*y, x**2 - 2*y**2, x*y - 2*y], x, y, domain='ZZ', order='grevlex')
```

## 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,  $(\mathbf{x}_i + \mathbf{1}, \mathbf{y}_i + \mathbf{1})$  is the coordinates of the next joint (or the hand) and the segment has length  $L_i$  then we get the equation [23]

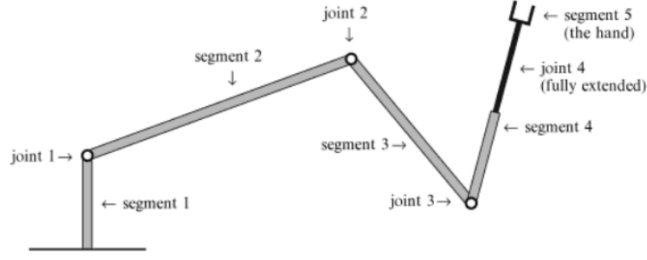


Figure 9: Robot Arm

$$(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2 = L_i^2 \quad (15)$$

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

$$x_{i+1} - x_i = L_i \cos(\theta_i) \quad (16)$$

$$y_{i+1} - y_i = L_i \sin(\theta_i) \quad (17)$$

## 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  $(x_1, y_1)$ . We get the following equations

$$x_1 - \frac{c}{2} = 0 \quad (18)$$

$$\frac{c-a}{b} \cdot x_1 - y_1 + \frac{a^2 + b^2 - c^2}{2b} = 0 \quad (19)$$

Similarly, if  $(x_2, y_2)$  are the coordinates of the intersection of the bisectors of AB and AC we have

$$x_2 - \frac{c}{2} = 0 \quad (20)$$

$$\frac{a}{b} \cdot x_2 + y_2 - \frac{b^2 + a^2}{2b} = 0 \quad (21)$$

## 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, Guénaél Renault, *Polynomial Systems Solving by Fast Linear Algebra*, HAL jhal-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](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] Meurer, Aaron P. Smith, Christopher Paprocki, Mateusz Čertík, Ondřej B. Kirpichev, Sergey Rocklin, Matthew Kumar, AMiT Ivanov, Sergiu Moore, Jason Singh, Sartaj Rathnayake, Thilina Vig, Sean E. Granger, Brian P. Muller, Richard Bonazzi, Francesco Gupta, Harsh Vats, Shivam Johansson, Fredrik Pedregosa, Fabian Scopatz, Anthony, *SymPy: Symbolic computing in Python*, PeerJ Computer Science. 3. e103. 10.7717/peerj-cs.103 2017.
- [29] Cox, Little, O'Shea, *Ideals, Varieties, and Algorithms Book*,