Polynomial Systems Solving

Burak Şener
Mehmet Pekmezci
Mustafa Mert Ergin
Şefik Temel

History of Poly-Nomial

Poly = Multi (Greek)
Nomial = Nomos (“Law” in Greek)
Nomial = Nomen (“Name” in Latin)

Diophantus - Egypt (~ 250)
Al-Khwarizmi - Persia (~ 850)
François Viète - France (1540 – 1603)
René Descartes – France - La Géométrie - 1637

Al-Khwarizmi – Algorithm - Algebra

Definitions

Bivariate Polynomial Systems

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

Multivariate Polynomial Systems

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

GOAL : Find the Roots (Points cutting the x axis)

Abstract Algebra

- Group (G,+) (closure, associativity, neutral, inverse, commutativity)
  - Homomorphism (isomorphism, automorphism)

- Ring (R, + , *) = (G,+) , (* is distributive over +, and associative)

- Ideal = Polynomial Ring = Commutative Ring

1. $0 \in \mathrm{I}$
2. $\mathrm{f}, \mathrm{g} \in \mathrm{I} \implies \mathrm{f} + \mathrm{g} \in \mathrm{I}$
3. $\mathrm{f} \in \mathrm{I}, \mathrm{h} \in \mathrm{G}, \implies \mathrm{h.f} \in \mathrm{I}$

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

$$(x-2)(x-1)=x^2-3x+2$$

$$\langle f_1, .., f_s \rangle = \left\{ \sum_{i=1}^{s} h_i . f_i | h_1, ..., h_s \in k[x_1, ..., x_n] \right\}$$

$\langle \mathrm{f}_1, .., \mathrm{f}_\mathrm{s} \rangle$ is an ideal **generated by** $\mathrm{f}_1, .., \mathrm{f}_\mathrm{s} \in \mathrm{k}[\mathrm{x}_1, ..., \mathrm{x}_\mathrm{n}]$.

$\langle 2\mathrm{x}^2 + 3\mathrm{y}^2 - 11, \mathrm{x}^2 - \mathrm{y}^2 - 3 \rangle = \langle \mathrm{x}^2 - 4, \mathrm{y}^2 - 1 \rangle$ Greatest Common Divisor (Basis)

Algebra - Geometry

- Affine Space : $k^n = \{(a_1, .., a_n) | a_1, .., a_n \in k\}$

- Affine Variety :

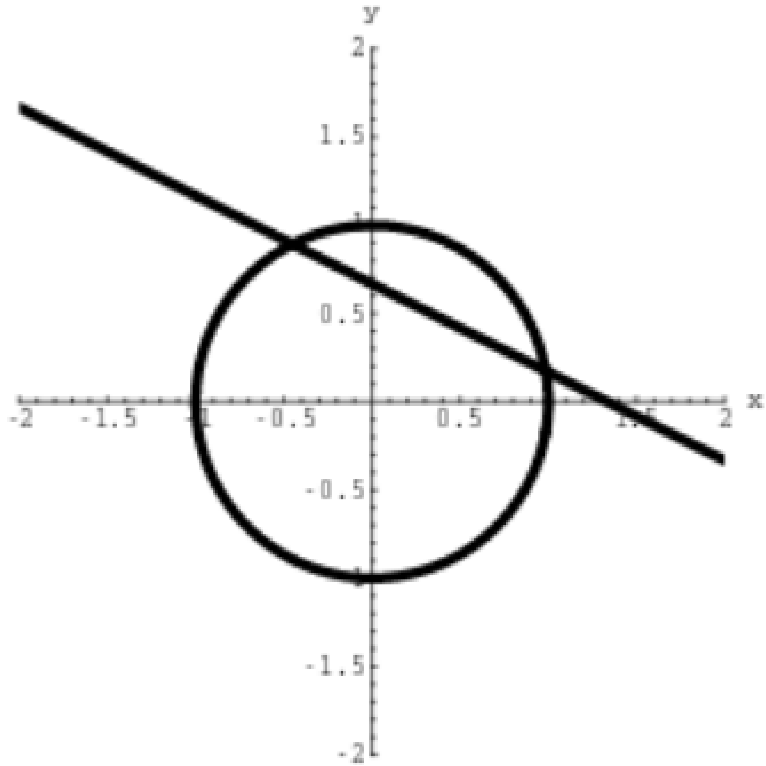
Let k be a field, and let $\mathrm{f_1, f_2, ..., f_n}$ be polynomials $\in \mathrm{k[x_1, ..., x_n]}$. Then we set

$$V(f_1, .., f_s) = \{(a_1, ..a_n) \in k^n | f_i(a_1, ...1_n) = 0, \forall i, 1 \leq i \leq s\} \tag{13}$$

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

Algebra - Geometry

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



Relation Between Ideal and Variety

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

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
$V(2x^2 + 3y^2 - 11, x^2 - y^2 - 3) = V(x^2 - 4, y^2 - 1) = \{(\pm 2, \pm 1)\}$
Thus, by changing the basis of the ideal, we made it easier to determine the variety.

$$\begin{array}{lclcl} \textbf{polynomials} & & \textbf{variety} & & \textbf{ideal} \\ f_1, \ldots, f_s & \longrightarrow & V(f_1, \ldots, f_s) & \longrightarrow & I(V(f_1, \ldots, f_s)) \end{array}$$