Bases de Gröbner et systèmes structurés

Thibaut Verron,
sous la direction de Jean-Charles Faugère et Mohab Safey El Din

UPMC Sorbonne Universités, Paris, France
INRIA Paris-Rocquencourt, Équipe PolSys
Laboratoire d'Informatique de Paris 6, UMR CNRS 7606

Rencontres Doctorales Lebesgue, 13 octobre 2014

Problem statement

Polynomial System Solving (PoSSo)

- Input: polynomial system $f_1, \ldots, f_m \in \mathbb{K}[X_1, \ldots, X_n]$
- Output: exact "solution" of the system:
  - list of the solutions if finite
  - parametrization of the set of solutions
  - list of one point per connected component…

Many applications

- Good model for many problems

  Examples: cryptography attacks, mechanical systems, physics, optimization…
- Also useful for theoretical problems

  Examples: algorithmic geometry, real algebraic geometry…

Several tools

- Multivariate resultants
- Triangular sets
- Gröbner bases

Gröbner bases

Goal

Solving the Membership Problem:

- Input: $f_1, \ldots, f_m, f \in \mathbb{K}[X_1, \ldots, X_n]$
- Output: "True" iff $f \in I := \langle f_1, \ldots, f_m \rangle$

Equivalently, build a Normal Form for I:
a computable function NF_I such that

$$\mathrm{NF}_I(f) = 0 \iff f \in I$$

Gröbner bases

Goal

Solving the Membership Problem:

- Input: $f_1, \ldots, f_m, f \in \mathbb{K}[X_1, \ldots, X_n]$
- Output: "True" iff $f \in I := \langle f_1, \ldots, f_m \rangle$

Equivalently, build a Normal Form for I:
a computable function NF_I such that

$$\mathrm{NF}_I(f) = 0 \iff f \in I$$

Two easy cases

	Univariate case	
Basis	Unique generator (gcd)	
Reduction	Modular reduction	
Algorithm	Euclid algorithm	

Gröbner bases

Goal

Solving the Membership Problem:

- Input: $f_1, \dots, f_m, f \in \mathbb{K}[X_1, \dots, X_n]$
- Output: "True" iff $f \in I := \langle f_1, \dots, f_m \rangle$

Equivalently, build a Normal Form for I:
a computable function NF_I such that

$$\mathrm{NF}_I(f) = 0 \iff f \in I$$

Two easy cases

	Univariate case	Degree 1
Basis	Unique generator (gcd)	Linear basis
Reduction	Modular reduction	Gauss reduction
Algorithm	Euclid algorithm	Gauss reduction

Gröbner bases

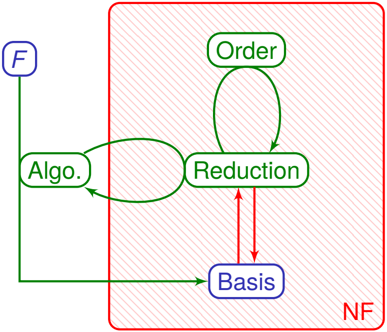
Goal

Solving the Membership Problem:

- Input: $f_1, \ldots, f_m, f \in \mathbb{K}[X_1, \ldots, X_n]$
- Output: "True" iff $f \in I := \langle f_1, \ldots, f_m \rangle$

Equivalently, build a Normal Form for I:
a computable function NF_I such that

$$\mathrm{NF}_I(f) = 0 \iff f \in I$$



Two easy cases

	Univariate case	Degree 1
Basis	Unique generator (gcd)	Linear basis
Reduction	Modular reduction	Gauss reduction
Algorithm	Euclid algorithm	Gauss reduction
Implicit order	Degree	Columns of the matrix

Gröbner bases

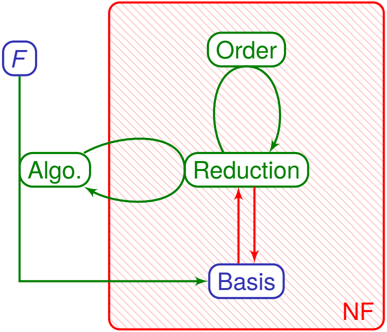
Goal

Solving the Membership Problem:

- Input: $f_1, \ldots, f_m, f \in \mathbb{K}[X_1, \ldots, X_n]$
- Output: "True" iff $f \in I := \langle f_1, \ldots, f_m \rangle$

Equivalently, build a Normal Form for I:
a computable function NF_I such that

$$\mathrm{NF}_I(f) = 0 \iff f \in I$$



General case

	General case
Basis	Gröbner basis
Reduction	$\mathrm{LT}(f) = m \cdot \mathrm{LT}(g) \implies f - mg = \ldots$
Algorithm	Buchberger, Lazard, F_4, F_5...
Explicit order	Monomial order

$\mathrm{LT}(f) =$ "leading term" of f (largest monomial in the support)

Polynomial system

$$\begin{cases} f: X^2 + 2XY + Y^2 + X = 0 \\ g: X^2 - XY + Y^2 + Y - 1 = 0 \end{cases}$$

Pair-wise reductions:

$g_1 = f - g = 0X^2 + 3XY + \dots$

$g_2 = Yf - Xg_1 = 0X^2Y + Y^3 + \dots$

$\dots$

Gröbner basis

$$\begin{cases} Y^3 + Y^2 - \frac{4}{9}X - \frac{2}{9}Y - \frac{4}{9} \\ X^2 + Y^2 + \frac{1}{3}X + \frac{2}{3}Y - \frac{2}{3} \\ XY + \frac{1}{3}X - \frac{1}{3}Y + \frac{1}{3} \end{cases}$$

Algorithms

Polynomial system

$$\begin{cases} f: X^2 + 2XY + Y^2 + X = 0 \\ g: X^2 - XY + Y^2 + Y - 1 = 0 \end{cases}$$

Macaulay matrix

$$\begin{array}{r} Xf \\ Yf \\ f \\ Xg \\ Yg \\ g \end{array} \begin{bmatrix} 1 & 2 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 1 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 & 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & -1 & 1 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 1 & -1 \end{bmatrix}$$

Pair-wise reductions:

$g_1 = f - g = 0X^2 + 3XY + \ldots$

$g_2 = Yf - Xg_1 = 0X^2Y + Y^3 + \ldots$

$\ldots$

Row-echelon form

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{8}{9} & -\frac{4}{9} & \frac{1}{9} \\ 0 & 1 & 0 & 0 & 0 & 0 & -\frac{1}{3} & \frac{1}{3} & -\frac{1}{3} & \frac{1}{3} \\ 0 & 0 & 1 & 0 & 0 & 0 & -\frac{1}{3} & -\frac{1}{9} & \frac{4}{9} & -\frac{1}{9} \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & -\frac{4}{9} & -\frac{2}{9} & -\frac{4}{9} \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & \frac{1}{3} & \frac{2}{3} & -\frac{2}{3} \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & \frac{1}{3} & -\frac{1}{3} & \frac{1}{3} \end{bmatrix}$$

Gröbner basis

$$\begin{cases} Y^3 + Y^2 - \frac{4}{9}X - \frac{2}{9}Y - \frac{4}{9} \\ X^2 + Y^2 + \frac{1}{3}X + \frac{2}{3}Y - \frac{2}{3} \\ XY + \frac{1}{3}X - \frac{1}{3}Y + \frac{1}{3} \end{cases}$$

Algorithms

Polynomial system

$$\begin{cases} f: X^2 + 2XY + Y^2 + X = 0 \\ g: X^2 - XY + Y^2 + Y - 1 = 0 \end{cases}$$

Macaulay matrix

$$\begin{array}{r} Xf \\ Yf \\ f \\ Xg \\ Yg \\ g \end{array} \begin{bmatrix} 1 & 2 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 1 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 & 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & -1 & 1 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 1 & -1 \end{bmatrix}$$

Pair-wise reductions:

$g_1 = f - g = 0X^2 + 3XY + \dots$

$g_2 = Yf - Xg_1 = 0X^2Y + Y^3 + \dots$

$\dots$

(Buchberger)

(Lazard, F_4 , F_5 ...)

Row-echelon form

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{8}{9} & -\frac{4}{9} & \frac{1}{9} \\ 0 & 1 & 0 & 0 & 0 & 0 & -\frac{1}{3} & \frac{1}{3} & -\frac{1}{3} & \frac{1}{3} \\ 0 & 0 & 1 & 0 & 0 & 0 & -\frac{1}{3} & -\frac{1}{9} & \frac{4}{9} & -\frac{1}{9} \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & -\frac{4}{9} & -\frac{2}{9} & -\frac{4}{9} \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & \frac{1}{3} & \frac{2}{3} & -\frac{2}{3} \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & \frac{1}{3} & -\frac{1}{3} & \frac{1}{3} \end{bmatrix}$$

Gröbner basis

$$\begin{cases} Y^3 + Y^2 - \frac{4}{9}X - \frac{2}{9}Y - \frac{4}{9} \\ X^2 + Y^2 + \frac{1}{3}X + \frac{2}{3}Y - \frac{2}{3} \\ XY + \frac{1}{3}X - \frac{1}{3}Y + \frac{1}{3} \end{cases}$$

Computing Gröbner bases in practice

Importance of structure

- Even modern algorithms can be slow in full generality
- For a given system (from an application), full generality is not necessary
- Good structures:
  - Example: homogeneous systems
  - Natural or easy to test
  - Dedicated algorithms or strategies
- Good algebraic properties:
  - Example: finite number of solutions
  - Hard to test but generic
  - Complexity improvements to all algorithms

Example of structure: homogeneous polynomials

Definitions, basic property

- Homogeneous polynomial = only monomials of the same degree
- Homogeneous ideal = generated by homogeneous polynomials
- I homogeneous, $f = f_d + \cdots + f_0$ homogeneous components

$$f \in I \iff \forall i, f_i \in I$$

Algorithmic advantages

- Only need to consider homogeneous polynomials
- Reduce several smaller matrices
- Algorithms more predictible:

$$f \text{ “reduces to” } g \neq 0 \implies \deg(g) \geq \deg(f)$$

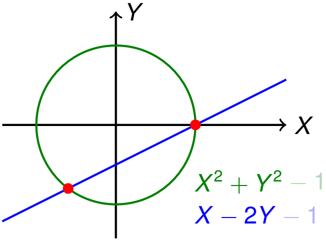
Example of property: regular sequences

Definition

$F = (f_1, \ldots, f_m)$ homo. $\in \mathbb{K}[\mathbf{X}]$ is regular iff

$$\begin{cases} \langle F \rangle \subsetneq \mathbb{K}[\mathbf{X}] \\ \forall i,\ f_i \text{ is no zero-divisor in } \mathbb{K}[\mathbf{X}]/\langle f_1, \ldots, f_{i-1} \rangle \end{cases}$$

$\iff$ "complete intersection"



Properties

- Algorithmic: no reductions to zero in F_5 $\rightsquigarrow$ faster computations
- Algebraic: Hilbert Series $\rightsquigarrow$ complexity bounds
- Geometric: generic property

Our work: weighted homogeneous systems

Definitions

- System of weights: $(w_1, \dots, w_n) \in \mathbb{N}^{*n}$
- W-degree: $\deg_W(X_1^{\alpha_1} \cdots X_n^{\alpha_n}) = \sum_{i=1}^{n} w_i \alpha_i$
- W-homogeneous polynomial

Some results...

- Algorithmic strategy:
  - How to compute a GB?

    $F(X_1, \dots, X_n)$ W-homogeneous $\iff$ $F(X_1^{w_1}, \dots, X_n^{w_n})$ homogeneous
- Additional properties:
  - What properties to use? Are they generic?
    Do they have an easy characterization?
- Complexity bounds:
  - Structure: size of the matrices divided by $\prod w_i$
  - Generic properties: complexity overall divided by $(\prod w_i)^3$

Our work: weighted homogeneous systems

Definitions

- System of weights: $(w_1, \ldots, w_n) \in \mathbb{N}^{*n}$
- W-degree: $\deg_W(X_1^{\alpha_1} \cdots X_n^{\alpha_n}) = \sum_{i=1}^n w_i \alpha_i$
- W-homogeneous polynomial

Some results...

- Algorithmic strategy
- Additional properties
- Complexity bounds

... and more questions

- Additional structures:
  - Several systems of weights?
  - Non-positive weights?
- Strategy for affine systems:
  - How to choose the weights for a given system?

Thank you for your attention!