Solving Non-linear Equations with Linear Algebra

Daniel Cabarcas

Universidad Nacional de Colombia sede Medellín

CIMPA-ICTP Research in Pairs
2023

UNIVERSIDAD
NACIONAL
DE COLOMBIA

Minicourse Outline

Outline

- Motivation.
- Groebner bases and elimination theory.
- Linear algebra to compute Groebner bases.
- Syzygies and the complexity of Groebner bases computation.

Outline for part I

Motivation

Cryptography

- Algebraic attacks [CP02]

Motivation

Cryptography

- Algebraic attacks [CP02]
- Multivariate public key cryptography [FJ03]

Motivation

Cryptography

- Algebraic attacks [CP02]
- Multivariate public key cryptography [FJ03]
- Rank-metric Code-based cryptography [BBC+20]

Motivation

Cryptography

- Algebraic attacks [CP02]
- Multivariate public key cryptography [FJ03]
- Rank-metric Code-based cryptography [BBC+20]
- Hyperelliptic curves

Motivation

Cryptography

- Algebraic attacks [CP02]
- Multivariate public key cryptography [FJ03]
- Rank-metric Code-based cryptography [BBC$^+$20]
- Hyperelliptic curves

Other applications

- Computer Aided Geometric Design (CAGD).
- Robotics (inverse kinematics).
- Celestial mechanics (central configurations).

Problem Setup

- K a finite field.
- $K[\underline{x}] = k[x_1, \ldots, x_n]$ ring of polynomials.
- K^n n-dimensional affine space over K.

Problem Setup

- K a finite field.
- $K[\underline{x}] = k[x_1, \ldots, x_n]$ ring of polynomials.
- K^n n-dimensional affine space over K.

Problem

Find all solutions in k^n to a system of polynomial equations

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ f_m(x_1, \ldots, x_n) &= 0 \end{aligned}$$

Problem Setup

- K a finite field.
- $K[\underline{x}] = k[x_1, \ldots, x_n]$ ring of polynomials.
- K^n n-dimensional affine space over K.

Problem

Find all solutions in k^n to a system of polynomial equations

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ f_m(x_1, \ldots, x_n) &= 0 \end{aligned}$$

Subproblems:

- Is there a solution?
- Can we list all solutions?
- What is the dimension of the solution space?
- What is the computational cost of solving the system?

Example

Consider the system over GF(7)

$$x^2 + xy + 2x + 5y^2 + 6y + 6 = 0$$
$$x^2 + 3xy + 2x + 6y^2 + y + 2 = 0.$$

Example

Consider the system over GF(7)

$$x^2 + xy + 2x + 5y^2 + 6y + 6 = 0$$
$$x^2 + 3xy + 2x + 6y^2 + y + 2 = 0.$$

It can be rewritten as

$$x + 5y^3 + 6y^2 + 3y + 1 = 0$$
$$y^4 + 4y^3 + 4y^2 + 6 = 0$$

Example

Consider the system over GF(7)

$$x^2 + xy + 2x + 5y^2 + 6y + 6 = 0$$
$$x^2 + 3xy + 2x + 6y^2 + y + 2 = 0.$$

It can be rewritten as

$$x + 5y^3 + 6y^2 + 3y + 1 = 0$$
$$y^4 + 4y^3 + 4y^2 + 6 = 0$$

The second polynomial has 3 roots in GF(7)

$$y = 6, \quad , y = 3, \quad \text{and} \quad y = 2.$$

Example

Consider the system over GF(7)

$$x^2 + xy + 2x + 5y^2 + 6y + 6 = 0$$
$$x^2 + 3xy + 2x + 6y^2 + y + 2 = 0.$$

It can be rewritten as

$$x + 5y^3 + 6y^2 + 3y + 1 = 0$$
$$y^4 + 4y^3 + 4y^2 + 6 = 0$$

The second polynomial has 3 roots in GF(7)

$$y = 6, \quad , y = 3, \quad \text{and} \quad y = 2.$$

Substituting in the first one, we obtain equations in x that can be factored to obtain

$$(1, 6), \quad (4, 3), \quad \text{and} \quad (6, 2).$$

Definitions / Notation

- $\mathbf{V}(f_1, \dots, f_m)$ affine variety.
- $I = \langle f_1, \dots, f_m \rangle$ ideal generated by.
- $\mathbf{V}(I)$ variaty of the ideal I.
- $\mathbf{I}(V)$ the ideal of variety V
- Monomial ordering $<$: total, well-ordering, and preserved under multiplication, e.g. lex, glex.
- Degree, multidegree
- Leading term/coef/monomial

Roadmap

- Problem: How to find $\mathbf{V}(f_1, \ldots, f_m)$?
- If we had an "echelonized" basis,
- then we can solve for the last variable.
- Next, for each $x_n = a_n$ we substitute in the other equations to find partial candidate solutions
- Continue this way until first variable.

Roadmap

- Problem: How to find $\mathbf{V}(f_1, \ldots, f_m)$?
- If we had an "echelonized" basis,
- then we can solve for the last variable.
- Next, for each $x_n = a_n$ we substitute in the other equations to find partial candidate solutions
- Continue this way until first variable.

Questions:

- How to find such a basis? $\rightarrow$ Groebner basis lex order.

Roadmap

- Problem: How to find $\mathbf{V}(f_1, \ldots, f_m)$?
- If we had an "echelonized" basis,
- then we can solve for the last variable.
- Next, for each $x_n = a_n$ we substitute in the other equations to find partial candidate solutions
- Continue this way until first variable.

Questions:

- How to find such a basis? $\rightarrow$ Groebner basis lex order.
- What guarantees that we can continue this process? $\rightarrow$ Elimination theorem.

A Division Algorithm in $K[\underline{x}]$

Theorem

Given $<$, $F = (f_1, \ldots, f_m)$, every $f \in K[\underline{x}]$ can be written as

$$f = a_1 f_1 + \cdots + a_m f_m + r,$$

where $a_i, r \in K[\underline{x}]$, so that no monomial in r is divisible by any leading term of f_i's.

A Division Algorithm in $K[\underline{x}]$

Theorem

Given $<$, $F = (f_1, \ldots, f_m)$, every $f \in K[\underline{x}]$ can be written as

$$f = a_1 f_1 + \cdots + a_m f_m + r,$$

where $a_i, r \in K[\underline{x}]$, so that no monomial in r is divisible by any leading term of f_i's.

- No unique reminders.
- It does not solve ideal membership.

A Division Algorithm in $K[\underline{x}]$

$\texttt{normal\_form}(g, F)$

Require: F finite tuple in $K[\underline{x}]$

Require: $g \in K[\underline{x}]$

1: $h := g$

2: **while** $\exists f \in F,\ t \in \text{terms}(h)$ s.t $\text{LT}(f) \mid t$ **do**

3: let $f \in F,\ t \in \text{terms}(h)$ s.t $\text{LT}(f) \mid t$

4: $h := h - \frac{t}{\text{LT}(f)} \cdot f$

5: **return** h

Groebner Basis - Definition

Monomial Ideals

- I is a monomial ideal if $\exists A \subseteq \mathbb{Z}^n_{\geq 0}$, s.t $I = \langle x^\alpha : \alpha \in A \rangle$.

Groebner Basis - Definition

Monomial Ideals

- I is a monomial ideal if $\exists A \subseteq \mathbb{Z}^n_{\geq 0}$, s.t $I = \langle x^\alpha : \alpha \in A \rangle$.
- Dickson's Lemma: Any monomial ideal $I = \langle x^\alpha : \alpha \in A \rangle$ is generated by a finite subset of $\{x^\alpha : \alpha \in A\}$.

Groebner Basis - Definition

Monomial Ideals

- I is a monomial ideal if $\exists A \subseteq \mathbb{Z}^n_{\geq 0}$, s.t $I = \langle x^\alpha : \alpha \in A \rangle$.
- Dickson's Lemma: Any monomial ideal $I = \langle x^\alpha : \alpha \in A \rangle$ is generated by a finite subset of $\{x^\alpha : \alpha \in A\}$.

- Hilbert Basis Theorem: Every ideal in $K[\underline{x}]$ has a finite generating set.

Groebner Basis - Definition

Monomial Ideals

- I is a monomial ideal if $\exists A \subseteq \mathbb{Z}^n_{\geq 0}$, s.t $I = \langle x^\alpha : \alpha \in A \rangle$.
- Dickson's Lemma: Any monomial ideal $I = \langle x^\alpha : \alpha \in A \rangle$ is generated by a finite subset of $\{x^\alpha : \alpha \in A\}$.

- Hilbert Basis Theorem: Every ideal in $K[\underline{x}]$ has a finite generating set.
- A finite subset G of an ideal I is called Groebner basis if

$$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle .$$

Groebner Basis - Definition

Monomial Ideals

- I is a monomial ideal if $\exists A \subseteq \mathbb{Z}^n_{\geq 0}$, s.t $I = \langle x^\alpha : \alpha \in A \rangle$.
- Dickson's Lemma: Any monomial ideal $I = \langle x^\alpha : \alpha \in A \rangle$ is generated by a finite subset of $\{x^\alpha : \alpha \in A\}$.

- Hilbert Basis Theorem: Every ideal in $K[\underline{x}]$ has a finite generating set.
- A finite subset G of an ideal I is called Groebner basis if

$$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle .$$

- Every ideal $\neq 0$ has a Groebner basis and it generates the ideal.

Groebner Basis - Definition

Monomial Ideals

- I is a monomial ideal if $\exists A \subseteq \mathbb{Z}^n_{\geq 0}$, s.t $I = \langle x^\alpha : \alpha \in A \rangle$.
- Dickson's Lemma: Any monomial ideal $I = \langle x^\alpha : \alpha \in A \rangle$ is generated by a finite subset of $\{x^\alpha : \alpha \in A\}$.

- Hilbert Basis Theorem: Every ideal in $K[\underline{x}]$ has a finite generating set.
- A finite subset G of an ideal I is called Groebner basis if

$$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle .$$

- Every ideal $\neq 0$ has a Groebner basis and it generates the ideal.
- Every ascending chain of ideals eventually stabilizes.

Groebner Basis - Definition

Monomial Ideals

- I is a monomial ideal if $\exists A \subseteq \mathbb{Z}^n_{\geq 0}$, s.t $I = \langle x^\alpha : \alpha \in A \rangle$.
- Dickson's Lemma: Any monomial ideal $I = \langle x^\alpha : \alpha \in A \rangle$ is generated by a finite subset of $\{x^\alpha : \alpha \in A\}$.

- Hilbert Basis Theorem: Every ideal in $K[\underline{x}]$ has a finite generating set.
- A finite subset G of an ideal I is called Groebner basis if

$$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle .$$

- Every ideal $\neq 0$ has a Groebner basis and it generates the ideal.
- Every ascending chain of ideals eventually stabilizes.
- If $I = \langle f_1, \ldots, f_m \rangle$, then $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_m)$.

Groebner Basis - Properties

Proposition

Let G be a GB for an ideal I, and $f \in K[\underline{x}]$. Then there exists a unique $r \in K[\underline{x}]$ s.t $f = g + r$ for some $g \in I$ and no term of r is divisible by any LT of G.

Groebner Basis - Properties

Proposition

Let G be a GB for an ideal I, and $f \in K[\underline{x}]$. Then there exists a unique $r \in K[\underline{x}]$ s.t $f = g + r$ for some $g \in I$ and no term of r is divisible by any LT of G.

- r is obtained by the division algorithm.
- $f \in G$ iff $r = 0$.

Groebner Basis - Computation

Definition

Let $f, g \in K[\underline{x}]$ be non-zero. The S-polynomial of f and g is

$$S(f,g) = \frac{\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(f)} f - \frac{\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(g)} g.$$

Groebner Basis - Computation

Definition

Let $f, g \in K[\underline{x}]$ be non-zero. The S-polynomial of f and g is

$$S(f,g) = \frac{\operatorname{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(f)} f - \frac{\operatorname{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(g)} g.$$

Theorem (Buchberger's Criterion)

Let $I = \langle g_1, \ldots, g_t \rangle$ be an ideal in $K[\underline{x}]$. G is a GB iff, for all $i \neq j$, the reminder on division of $S(g_i, g_j)$ by G is zero.

Buchberger's Algorithm

Require: F is a finite subset of $K[\underline{x}]$

$G := F$

$B := \{\{g_1, g_2\} \mid g_1, g_2 \in G, g_1 \neq g_2\}$

while $B \neq \emptyset$ **do**

  let $\{g_1, g_2\}$ be an element of B

  $B := B \setminus \{\{g_1, g_2\}\}$

  $h := \mathrm{S}(g_1, g_2)$

  $r :=$ `normal_form`(h, G)

  if $r \neq 0$ **then**

    $B := B \cup \{\{g, r\} \mid g \in G\}$

    $G := G \cup \{r\}$

return G

Improvements Until the 90's

1. Pair order selection. Normal strategy: choose min lcm pair.

Improvements Until the 90's

1. Pair order selection. Normal strategy: choose min lcm pair.
2. When a new basis element is produced, reduce all elements with respect to it.

Improvements Until the 90's

1. Pair order selection. Normal strategy: choose min lcm pair.
2. When a new basis element is produced, reduce all elements with respect to it.
3. Criteria to discard a-priori pairs which are known to reduce to zero.

Elimination Ideals

Definition

Given $I = \langle f_1, \ldots, f_m \rangle \subset K[\underline{x}]$, the ℓ-th elimination ideal is the ideal of $K[x_{\ell+1}, \ldots, x_n]$ defined by

$$I_\ell = I \cap K[x_{\ell+1}, \ldots, x_n].$$

Elimination Ideals

Definition

Given $I = \langle f_1, \ldots, f_m \rangle \subset K[\underline{x}]$, the ℓ-th elimination ideal is the ideal of $K[x_{\ell+1}, \ldots, x_n]$ defined by

$$I_\ell = I \cap K[x_{\ell+1}, \ldots, x_n].$$

Theorem

Let I be an ideal of $K[\underline{x}]$ and G a GB of I w.r.t lex order $x_1 > x_2 > \cdots > x_n$. Then for every $0 \leq \ell \leq n$, the set

$$G_\ell = G \cap K[x_{\ell+1}, \ldots, x_n]$$

is a GB of I_ℓ.

Other Relevant Results

- **Extension Theorem:** Gives a condition for when a partial solution can be extended (for algebraically closed field).

Other Relevant Results

- **Extension Theorem:** Gives a condition for when a partial solution can be extended (for algebraically closed field).
- **Clousure Theorem:** $\mathbf{V}(I_\ell)$ is the smallest affine variety containing $\pi_\ell(V)$ (for algebraically closed field).

Other Relevant Results

- **Extension Theorem:** Gives a condition for when a partial solution can be extended (for algebraically closed field).
- **Clousure Theorem:** $\mathbf{V}(I_\ell)$ is the smallest affine variety containing $\pi_\ell(V)$ (for algebraically closed field).
- **Nullstellensatz:** precisely determines $\mathbf{I}(\mathbf{V}(I))$ (for algebraically closed field).

Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel.
Improvements of algebraic attacks for solving the rank decoding and minrank problems.
In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 507–536, Cham, 2020. Springer International Publishing.

Nicolas T. Courtois and Josef Pieprzyk.
Cryptanalysis of block ciphers with overdefined systems of equations.
In Yuliang Zheng, editor, *Advances in Cryptology — ASIACRYPT 2002*, pages 267–287, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg.

Jean-Charles Faugère and Antoine Joux.
Algebraic cryptanalysis of hidden field equation (hfe) cryptosystems using gröbner bases.
In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003*, pages 44–60, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

Thanks

Daniel Cabarcas – dcabarc@unal.edu.co

UNIVERSIDAD
NACIONAL
DE COLOMBIA

Solving Non-linear Equations with Linear Algebra

Part II - Linear Algebra Enters the Picture

Daniel Cabarcas

Universidad Nacional de Colombia sede Medellín

CIMPA-ICTP Research in Pairs
2023

Minicourse Outline

- Motivation.
- Groebner bases and elimination theory.
- Linear algebra to compute Groebner bases.
- Syzygies and the complexity of Groebner bases computation.

Outline for Part II

Recall the Buchberger Algorithm

Require: F is a finite subset of $K[\underline{x}]$

$G := F$

$B := \{\{g_1, g_2\} \mid g_1, g_2 \in G, g_1 \neq g_2\}$

while $B \neq \emptyset$ **do**

  let $\{g_1, g_2\}$ be an element of B

  $B := B \setminus \{\{g_1, g_2\}\}$

  $h := \mathrm{S}(g_1, g_2)$

  $r := \texttt{normal\_form}(h, G)$

  if $r \neq 0$ **then**

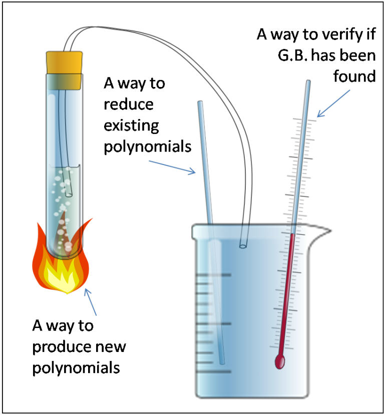
    $B := B \cup \{\{g, r\} \mid g \in G\}$

    $G := G \cup \{r\}$

return G

General Framework

$$\mathrm{LM}(\langle p_1, \ldots, p_m \rangle) = \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_r) \rangle$$



XL(Extended Linearization) [CKPA00]

$$1x^2 + 2xy + 3y^2 + 4x + 5y - 6 = 0$$
$$7x^2 + 8xy + 9y^2 + 0x + 1y - 2 = 0$$
$$3x^2 + 4xy + 5y^2 + 6x + 7y - 8 = 0$$

$$\Big\downarrow \text{Linearize}$$

$$\begin{array}{c} \begin{array}{cccccc} x^2 & xy & y^2 & x & y & 1 \end{array} \\ \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & -6 \\ 7 & 8 & 9 & 0 & 1 & -2 \\ 3 & 4 & 5 & 6 & 7 & -8 \end{bmatrix} \end{array} \xrightarrow{\text{Gauss}} \begin{array}{c} \begin{array}{cccccc} x^2 & xy & y^2 & x & y & 1 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & * & * & * \\ 0 & 1 & 0 & * & * & * \\ 0 & 0 & 1 & * & * & * \end{bmatrix} \end{array}$$

XL(Extended Linearization) [CKPA00]

$$1x^3 + 2x^2y + 3xy^2 + 4x^2 + 5xy - 6x = 0$$

Enlarge

$*x$

$$\begin{aligned} 1x^2 + 2xy + 3y^2 + 4x + 5y - 6 &= 0 \\ 7x^2 + 8xy + 9y^2 + 0x + 1y - 2 &= 0 \\ 3x^2 + 4xy + 5y^2 + 6x + 7y - 8 &= 0 \end{aligned}$$

Linearize

$$\begin{array}{c} \begin{array}{cccccc} x^2 & xy & y^2 & x & y & 1 \end{array} \\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & -6 \\ 7 & 8 & 9 & 0 & 1 & -2 \\ 3 & 4 & 5 & 6 & 7 & -8 \end{pmatrix} \end{array} \xrightarrow{\text{Gauss}} \begin{array}{c} \begin{array}{cccccc} x^2 & xy & y^2 & x & y & 1 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & * & * & * \\ 0 & 1 & 0 & * & * & * \\ 0 & 0 & 1 & * & * & * \end{pmatrix} \end{array}$$

XL(Extended Linearization) [CKPA00]

$$
\begin{array}{c}
\begin{array}{cccccccccc}
x^3 & x^2y & xy^2 & y^3 & x^2 & xy & y^2 & x & y & 1
\end{array} \\
\begin{pmatrix}
1 & 2 & 3 & 0 & 4 & 5 & 0 & -6 & 0 & 0 \\
7 & 8 & 9 & 0 & 0 & 1 & 0 & -2 & 0 & 0 \\
3 & 4 & 5 & 0 & 6 & 7 & 0 & -8 & 0 & 0 \\
0 & 1 & 2 & 3 & 0 & 4 & 5 & 0 & -6 & 0 \\
0 & 7 & 8 & 9 & 0 & 0 & 1 & 0 & -2 & 0 \\
0 & 3 & 4 & 5 & 0 & 6 & 7 & 0 & -8 & 0 \\
 & & & & 1 & 2 & 3 & 4 & 5 & -6 \\
 & & & & 7 & 8 & 9 & 0 & 1 & -2 \\
 & & & & 3 & 4 & 5 & 6 & 7 & -8
\end{pmatrix}
\end{array}
$$

XL(Extended Linearization) [CKPA00]

x^3	x^2y	xy^2	y^3	x^2	xy	y^2	x	y	1	d
3				2			1		0	
1	2	3	0	4	5	0	-6	0	0	
7	8	9	0	0	1	0	-2	0	0	
3	4	5	0	6	7	0	-8	0	0	
0	1	2	3	0	4	5	0	-6	0	3
0	7	8	9	0	0	1	0	-2	0	
0	3	4	5	0	6	7	0	-8	0	
				1	2	3	4	5	-6	
				7	8	9	0	1	-2	2
				3	4	5	6	7	-8	

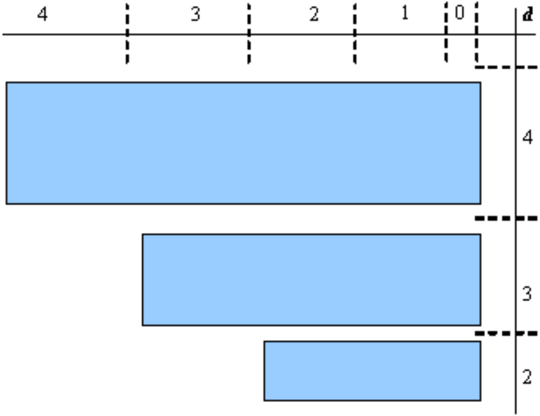
XL(Extended Linearization) [CKPA00]

x^3	x^2y	xy^2	y^3	x^2	xy	y^2	x	y	1	
	3				2		1		0	d
1	0	0	0	0	0	0	0	0	*	3
0	1	0	0	0	0	0	0	0	*	
0	0	1	0	0	0	0	0	0	*	
0	0	0	1	0	0	0	0	0	*	
0	0	0	0	1	0	0	0	0	*	
0	0	0	0	0	1	0	0	0	*	
				0	0	1	0	0	*	2
				0	0	0	1	0	*	
				0	0	0	0	1	*	

XL(Extended Linearization) [CKPA00]

x^3	x^2y	xy^2	y^3	x^2	xy	y^2	x	y	1	
	3				2		1		0	d
1	0	0	0	0	0	0	0	0	*	
0	1	0	0	0	0	0	0	0	*	3
0	0	1	0	0	0	0	0	0	*	
0	0	0	1	0	0	0	0	0	*	
0	0	0	0	1	0	0	0	0	*	
0	0	0	0	0	1	0	0	0	*	2
				0	0	1	0	0	*	
				0	0	0	1	0	*	1
				0	0	0	0	1	*	

XL(Extended Linearization) [CKPA00]



Staggered Linear Basis

- The idea of using linear algebra to compute Groebner bases dates back to [Laz83].

Staggered Linear Basis

- The idea of using linear algebra to compute Groebner bases dates back to [Laz83].
- **Key observation:** an homogeneous ideal $I \subset K[\underline{x}]$ is a K-vector space, and its degree d component I_d is a finite dimensional subspace ($I_{\leq d}$ in the affine case).

Staggered Linear Basis

- The idea of using linear algebra to compute Groebner bases dates back to [Laz83].
- **Key observation:** an homogeneous ideal $I \subset K[\underline{x}]$ is a K-vector space, and its degree d component I_d is a finite dimensional subspace ($I_{\leq d}$ in the affine case).

Definition

Let V be a k-subspace of $K[\underline{x}]$. A subset B of $V \setminus \{0\}$ is called a **staggered linear basis** of V, if B generates V and B is staggered, that is, for all $f \neq g \in B$, $\mathrm{LM}(f) \neq \mathrm{LM}(g)$.

Staggered Linear Basis

- The idea of using linear algebra to compute Groebner bases dates back to [Laz83].
- **Key observation:** an homogeneous ideal $I \subset K[\underline{x}]$ is a K-vector space, and its degree d component I_d is a finite dimensional subspace ($I_{\leq d}$ in the affine case).

Definition

Let V be a k-subspace of $K[\underline{x}]$. A subset B of $V \setminus \{0\}$ is called a **staggered linear basis** of V, if B generates V and B is staggered, that is, for all $f \neq g \in B$, $\mathrm{LM}(f) \neq \mathrm{LM}(g)$.

Theorem

Let B be a **staggered linear** *basis for an ideal I in $K[\underline{x}]$. Then, the set*

$$G = \{f \in B \mid \text{ for all } f \neq g \in B, \mathrm{LM}(g) \text{ does not divide } \mathrm{LM}(f)\}$$

is a minimal **Groebner basis** *for I.*

Gradation

Definition

Let I be an ideal and $G = \{g_1, \ldots, g_m\}$ a set of generators of I. G is a d-**Groebner basis** of I if $\mathrm{LM}(I) \cap R_{\leq d} \subseteq \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_m) \rangle$.

Gradation

Definition

Let I be an ideal and $G = \{g_1, \ldots, g_m\}$ a set of generators of I. G is a *d*-**Groebner basis** of I if $\mathrm{LM}(I) \cap R_{\leq d} \subseteq \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_m)\rangle$.

Proposition

Let B be a **staggered** *linear basis for $I_{\leq d}$. Then, the set*

$$\{f \in B \mid \textit{ for all } f \neq g \in B, \mathrm{LM}(g) \textit{ does not divide } \mathrm{LM}(f)\}$$

*is a minimal d-*__Groebner basis__ *for I.*

Gradation

Definition

Let I be an ideal and $G = \{g_1, \ldots, g_m\}$ a set of generators of I. G is a d-**Groebner basis** of I if $\mathrm{LM}(I) \cap R_{\leq d} \subseteq \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_m) \rangle$.

Proposition

Let B be a **staggered** *linear basis for $I_{\leq d}$. Then, the set*

$$\{f \in B \mid \text{ for all } f \neq g \in B, \mathrm{LM}(g) \text{ does not divide } \mathrm{LM}(f)\}$$

*is a minimal d-***Groebner basis** *for I.*

Proposition

Let I be an ideal of $K[\underline{x}]$. **There exists** *d_0 such that for all $d \geq d_0$, every d-Groebner basis of I is a* **Groebner basis of** *I.*

Macaulay Matrix

Definition

Given $F = \{f_1, \ldots, f_m\} \subset R$ and $d \geq 0$

- the **Maucalay matrix** of F in degree d, denoted by $\mathcal{M}_d(F)$, is the matrix whose columns are indexed by monomials of degree $\leq d$ and the rows correspond to polynomial $x^\alpha f_i$ with $\deg(x^\alpha f_i) = d$.

Macaulay Matrix

Definition

Given $F = \{f_1, \ldots, f_m\} \subset R$ and $d \geq 0$

- the **Maucalay matrix** of F in degree d, denoted by $\mathcal{M}_d(F)$, is the matrix whose columns are indexed by monomials of degree $\leq d$ and the rows correspond to polynomial $x^\alpha f_i$ with $\deg(x^\alpha f_i) = d$.
- Similarly define $\mathcal{M}_{\leq d}(F)$.

Macaulay Matrix

Definition

Given $F = \{f_1, \ldots, f_m\} \subset R$ and $d \geq 0$

- the **Maucalay matrix** of F in degree d, denoted by $\mathcal{M}_d(F)$, is the matrix whose columns are indexed by monomials of degree $\leq d$ and the rows correspond to polynomial $x^\alpha f_i$ with $\deg(x^\alpha f_i) = d$.
- Similarly define $\mathcal{M}_{\leq d}(F)$.
- Given a matrix M whose columns are indexed by monomials, we can define the polynomial representation of M denoted by $\mathcal{P}(M)$.

Macaulay Matrix

Definition

Given $F = \{f_1, \ldots, f_m\} \subset R$ and $d \geq 0$

- the **Maucalay matrix** of F in degree d, denoted by $\mathcal{M}_d(F)$, is the matrix whose columns are indexed by monomials of degree $\leq d$ and the rows correspond to polynomial $x^\alpha f_i$ with $\deg(x^\alpha f_i) = d$.
- Similarly define $\mathcal{M}_{\leq d}(F)$.
- Given a matrix M whose columns are indexed by monomials, we can define the polynomial representation of M denoted by $\mathcal{P}(M)$.

- Given F homogeneous, $\{x^\alpha f_i : \deg(x^\alpha f_i) \leq d\}$ is a linear basis for $I_{\leq d}$.

Macaulay Matrix

Definition

Given $F = \{f_1, \ldots, f_m\} \subset R$ and $d \geq 0$

- the **Maucalay matrix** of F in degree d, denoted by $\mathcal{M}_d(F)$, is the matrix whose columns are indexed by monomials of degree $\leq d$ and the rows correspond to polynomial $x^\alpha f_i$ with $\deg(x^\alpha f_i) = d$.
- Similarly define $\mathcal{M}_{\leq d}(F)$.
- Given a matrix M whose columns are indexed by monomials, we can define the polynomial representation of M denoted by $\mathcal{P}(M)$.

- Given F homogeneous, $\{x^\alpha f_i : \deg(x^\alpha f_i) \leq d\}$ is a linear basis for $I_{\leq d}$.
- An echelon form of $\mathcal{M}_{\leq d}(F)$ is a staggered linear basis for $I_{\leq d}$.

Lazard's Algorithm (XL)

Require: P a list of polynomials.

$G :=$ `echelon`(P)
$A := X \times G$
while no solution found **do**
    $H := \{xg \mid (x, g) \in A\}$
    $\widetilde{H} :=$ `echelon`$(H \cup G)$
    $\widetilde{H}^+ := \left\{h \in \widetilde{H} \mid \mathsf{LM}(h) \notin \mathsf{LM}(G)\right\}$
    $G := G \cup \widetilde{H}^+$
    $A := X \times \widetilde{H}^+$
return G

Non-Homogeneous Case

- Let $F = \{f_1, \ldots, f_m\} \subset R$ and $d \geq 0$

Non-Homogeneous Case

- Let $F = \{f_1, \ldots, f_m\} \subset R$ and $d \geq 0$
- Let $M = \mathcal{M}_{\leq d}$.

Non-Homogeneous Case

- Let $F = \{f_1, \dots, f_m\} \subset R$ and $d \geq 0$
- Let $M = \mathcal{M}_{\leq d}$.
- Let $\tilde{M}$ be an echelon form of M.

Non-Homogeneous Case

- Let $F = \{f_1, \dots, f_m\} \subset R$ and $d \geq 0$
- Let $M = \mathcal{M}_{\leq d}$.
- Let $\tilde{M}$ be an echelon form of M.
- Add new rows to $\tilde{M}$ for all $f \in \mathcal{P}(\tilde{M})$ and u monomial s.t. $\deg(uf) \leq d$ and $uf \notin \text{rowsp}(\tilde{M})$

Non-Homogeneous Case

- Let $F = \{f_1, \ldots, f_m\} \subset R$ and $d \geq 0$
- Let $M = \mathcal{M}_{\leq d}$.
- Let $\tilde{M}$ be an echelon form of M.
- Add new rows to $\tilde{M}$ for all $f \in \mathcal{P}(\tilde{M})$ and u monomial s.t. $\deg(uf) \leq d$ and $uf \notin \operatorname{rowsp}(\tilde{M})$
- Repeat the process successively until there is nothing more to add.

Non-Homogeneous Case

- Let $F = \{f_1, \ldots, f_m\} \subset R$ and $d \geq 0$
- Let $M = \mathcal{M}_{\leq d}$.
- Let $\tilde{M}$ be an echelon form of M.
- Add new rows to $\tilde{M}$ for all $f \in \mathcal{P}(\tilde{M})$ and u monomial s.t. $\deg(uf) \leq d$ and $uf \notin \text{rowsp}(\tilde{M})$
- Repeat the process successively until there is nothing more to add.
- We will refer to the resulting matrix as the Saturated Macaulay matrix of F, and denote it by $\mathcal{SM}_{\leq d}(F)$

Non-Homogeneous Case

- Let $F = \{f_1, \dots, f_m\} \subset R$ and $d \geq 0$
- Let $M = \mathcal{M}_{\leq d}$.
- Let $\tilde{M}$ be an echelon form of M.
- Add new rows to $\tilde{M}$ for all $f \in \mathcal{P}(\tilde{M})$ and u monomial s.t. $\deg(uf) \leq d$ and $uf \notin \operatorname{rowsp}(\tilde{M})$
- Repeat the process successively until there is nothing more to add.
- We will refer to the resulting matrix as the Saturated Macaulay matrix of F, and denote it by $\mathcal{SM}_{\leq d}(F)$
- There exists an integer d_0 such that for all $d \geq d_0$, $\mathcal{P}(\mathcal{SM}_{\leq d}(F))$ is a staggered linear basis for $I_{\leq d}$.

The Mutant-XL Algorithm [DCS+08]

Require: P a finite subsets of $K[\underline{x}]$ in row echelon form

$G := P$

$A := X \times G$

while no solution found **do**

 $d := \min\{\deg(x,g) \mid (x,g) \in A\}$

 $B := \{(x,g) \in A \mid \deg(x,g) = d\}$

 $A := A \setminus B$

 $H := \{xg \mid (x,g) \in B\}$

 $\widetilde{H} := \texttt{echelon}(H \cup G)$

 $\widetilde{H}^{+} := \left\{h \in \widetilde{H} \mid \mathrm{LM}(h) \notin \mathrm{LM}(G)\right\}$

 $G := G \cup \widetilde{H}^{+}$

 $A := A \cup (X \times \widetilde{H}^{+})$

return G

Termination Condition

- Check Buchberger's criterion.

Termination Condition

- Check Buchberger's criterion.
- In certain cases, if we know something about the ideal or about its Groebner bases, it is possible decide termination more efficiently.

Termination Condition

- Check Buchberger's criterion.
- In certain cases, if we know something about the ideal or about its Groebner bases, it is possible decide termination more efficiently.
- In the homogeneous zero-dimensional case, check if $I_d = R_d$.

Termination Condition

- Check Buchberger's criterion.
- In certain cases, if we know something about the ideal or about its Groebner bases, it is possible decide termination more efficiently.
- In the homogeneous zero-dimensional case, check if $I_d = R_d$.
- In the case of a single solution, check if there are n linear equations.

Termination Condition

- Check Buchberger's criterion.
- In certain cases, if we know something about the ideal or about its Groebner bases, it is possible decide termination more efficiently.
- In the homogeneous zero-dimensional case, check if $I_d = R_d$.
- In the case of a single solution, check if there are n linear equations.
- Perhaps we can estimate a suitable d.

The F4 Algorithm [Fau99]

Require: F is a finite subset of $K[\underline{x}]$

$G := F$

$B := \{\{g_1, g_2\} \mid g_1, g_2 \in G, g_1 \neq g_2\}$

while $B \neq \emptyset$ **do**

  let B^* be a nonempty subset of B

  $B := B \setminus B^*$

  $L := \left\{ \frac{\mathrm{lcm}(\mathrm{LM}(f),\mathrm{LM}(g))}{\mathrm{LM}(f)} \cdot f \mid \{f, g\} \in B^* \right\}$

  $H := \texttt{basic\_symb\_pre\_proc}(L, G)$

  $\widetilde{H} :=$ a row echelon form of H

  $\widetilde{H}^+ := \{h \in \widetilde{H} \mid \mathrm{LM}(h) \notin \mathrm{LM}(H)\}$

  $G := G \cup \widetilde{H}^+$

  $B := B \cup \{\{h, g\} \mid h \in \widetilde{H}^+, g \in G, h \neq g\}$

return G

`basic_symb_pre_proc`(L, G)

Require: L and G are finite subsets of $K[\underline{x}]$

$H := L$

$\mathit{done} := \mathrm{LM}(H)$

while $\mathrm{M}(H) \neq \mathit{done}$ **do**

    let t be an element of $(\mathrm{M}(H) \setminus \mathit{done})$

    $\mathit{done} = \mathit{done} \cup \{t\}$

    if there exist $g \in G$ s.t. $\mathrm{LM}(g) \mid t$ **then**

        choose $g \in G$ s.t. $\mathrm{LM}(g) \mid t$

        $H := H \cup \{\frac{t}{\mathrm{LM}(g)} * g\}$

return H

N. Courtois, A. Klimov, J. Patarin, and A.Shamir.
Efficient algorithms for solving overdefined systems of multivariate polynomial equations.
EUROCRYPT 2000, LNCS, 1807:392–407, 2000.

Jintai Ding, Daniel Cabarcas, Dieter Schmidt, Johannnes Buchmann, and Stefan Tohaneanu.
Mutant Gröbner Basis Algorithm.
In *Proceedings of the 1st international conference on Symbolic Computation and Cryptography (SCC08)*, pages 23–32, Beijing, China, April 2008. LMIB.

J. C. Faugere.
A new efficient algorithm for computing grobner bases (f4).
Journal of Pure and Applied Algebra, 139:61–88, 1999.

D. Lazard.
Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations.
In *Computer algebra*, volume 162 of *LNCS*, pages 146–156, Berlin, 1983. Springer.
Proceedings Eurocal'83, London, 1983.

Thanks

Daniel Cabarcas – dcabarc@unal.edu.co

UNIVERSIDAD
NACIONAL
DE COLOMBIA

Solving Non-linear Equations with Linear Algebra

Part III - Computational Complexity

Daniel Cabarcas

Universidad Nacional de Colombia sede Medellín

CIMPA-ICTP Research in Pairs
2023

Minicourse Outline

- Motivation.
- Groebner bases and elimination theory.
- Linear algebra to compute Groebner bases.
- Computational Complexity of Groebner bases computation.

Outline for Today

Outline for Today

1. Avoid Zero Reductions

2. Solving Degree

3. Matrix Reduction Algorithms

Reduction to Zero

Definition

Given $<$, $G = \{g_1, \ldots, g_m\} \subset K[\underline{x}]$, and $f \in K[\underline{x}]$, we say that f **reduces to zero modulo** G, denoted $f \to_G 0$, if $f = a_1 g_1 + \cdots + a_m g_m$, for some $a_i \in K[\underline{x}]$ s.t. $\mathrm{LM}(f) \geq \mathrm{LM}(a_i g_i)$ for all i.

Reduction to Zero

Definition

Given $<$, $G = \{g_1, \ldots, g_m\} \subset K[\underline{x}]$, and $f \in K[\underline{x}]$, we say that f **reduces to zero modulo** G, denoted $f \to_G 0$, if $f = a_1 g_1 + \cdots + a_m g_m$, for some $a_i \in K[\underline{x}]$ s.t. $\mathrm{LM}(f) \geq \mathrm{LM}(a_i g_i)$ for all i.

- The order of G does not matter
- Enough for Groebner bases

Reduction to Zero

Definition

Given $<$, $G = \{g_1, \ldots, g_m\} \subset K[\underline{x}]$, and $f \in K[\underline{x}]$, we say that f **reduces to zero modulo** G, denoted $f \to_G 0$, if $f = a_1 g_1 + \cdots + a_m g_m$, for some $a_i \in K[\underline{x}]$ s.t. $\mathrm{LM}(f) \geq \mathrm{LM}(a_i g_i)$ for all i.

- The order of G does not matter
- Enough for Groebner bases

Proposition

Let $f, g \in K[\underline{x}]$ be such that

$$\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g)) = \mathrm{LM}(f)\,\mathrm{LM}(g).$$

Then $S(f,g) \to_{\{f,g\}} 0$.

Syzygies

Definition

Let $F = (f_1, \ldots, f_m) \in K[\underline{x}]^m$. Then $H = (h_1, \ldots, h_m) \in K[\underline{x}]^m$ is called a **syzygy** of F if

$$F \cdot H = \sum_{i=1}^{m} f_i h_i = 0.$$

Syzygies

Definition

Let $F = (f_1, \ldots, f_m) \in K[\underline{x}]^m$. Then $H = (h_1, \ldots, h_m) \in K[\underline{x}]^m$ is called a **syzygy** of F if

$$F \cdot H = \sum_{i=1}^{m} f_i h_i = 0.$$

- The set of all syzygies of F forms an $K[\underline{x}]$-module graded by $\max \deg h_i f_i$.

Syzygies

Definition

Let $F = (f_1, \ldots, f_m) \in K[\underline{x}]^m$. Then $H = (h_1, \ldots, h_m) \in K[\underline{x}]^m$ is called a **syzygy** of F if

$$F \cdot H = \sum_{i=1}^{m} f_i h_i = 0.$$

- The set of all syzygies of F forms an $K[\underline{x}]$-module graded by $\max \deg h_i f_i$.
- We will denote by $S(F)$ the set of all syzygies of $(\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_m))$.

Syzygies

Definition

Let $F = (f_1, \ldots, f_m) \in K[\underline{x}]^m$. Then $H = (h_1, \ldots, h_m) \in K[\underline{x}]^m$ is called a **syzygy** of F if

$$F \cdot H = \sum_{i=1}^{m} f_i h_i = 0.$$

- The set of all syzygies of F forms an $K[\underline{x}]$-module graded by $\max \deg h_i f_i$.
- We will denote by $S(F)$ the set of all syzygies of $(\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_m))$.
- Note that S-polynomials are syzygies, lets denote them by

$$S_{ij} = \frac{\mathrm{lcm}(\mathrm{LM}(f_i), \mathrm{LM}(f_j))}{\mathrm{LT}(f_i)} e_j - \frac{\mathrm{lcm}(\mathrm{LM}(f_i), \mathrm{LM}(f_j))}{\mathrm{LT}(f_j)} e_i$$

Syzygies

Definition

Let $F = (f_1, \ldots, f_m) \in K[\underline{x}]^m$. Then $H = (h_1, \ldots, h_m) \in K[\underline{x}]^m$ is called a **syzygy** of F if

$$F \cdot H = \sum_{i=1}^{m} f_i h_i = 0.$$

- The set of all syzygies of F forms an $K[\underline{x}]$-module graded by $\max \deg h_i f_i$.
- We will denote by $S(F)$ the set of all syzygies of $(\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_m))$.
- Note that S-polynomials are syzygies, lets denote them by

$$S_{ij} = \frac{\mathrm{lcm}(\mathrm{LM}(f_i), \mathrm{LM}(f_j))}{\mathrm{LT}(f_i)} e_j - \frac{\mathrm{lcm}(\mathrm{LM}(f_i), \mathrm{LM}(f_j))}{\mathrm{LT}(f_j)} e_i$$

- $\{S_{ij} : 1 \leq i < j \leq m\}$ is a basis of $S(F)$.

Syzygies and Groebner Basis

Theorem

Let $G = (g_1, \dots, g_m)$ *be a basis for an ideal* I*, and* B *a homogeneous basis for* $S(G)$*. Then* G *is a GB iff, for all* $S \in B$*,*

$$S \cdot G \to_G 0.$$

Remove Zero-Reductions

Proposition

Let $G = (g_1, \ldots, g_m)$ *and* $S \subseteq \{S_{ij} : 1 \leq i < j \leq m\}$ *be a basis for* $S(G)$. *Suppose* i, j, k *are such that*

$$\mathrm{LT}(g_k) \mid \mathrm{lcm}(\mathrm{LM}(g_i), \mathrm{LM}(g_j)).$$

Then, if $S_{ik}, S_{jk} \in S$, *then* $S - \{S_{ij}\}$ *is also a basis for* $S(G)$.

Improved Buchberger Algorithm

Require: F is a finite subset of $K[\underline{x}]$

$G := \emptyset$
$B := \emptyset$
for all f in F **do**
    $(G, B) := \texttt{update}(G, B, f)$
while $B \neq \emptyset$ **do**
    let $\{g_1, g_2\}$ be an element of B
    $B := B \setminus \{\{g_1, g_2\}\}$
    $h := \mathrm{S}(g_1, g_2)$
    $r := \texttt{normal\_form}(h, G)$
    if $r \neq 0$ **then**
        $(G, B) := \texttt{update}(G, B, r)$
return G

update(G, B, h)

Require: G subset of $K[\underline{x}]$, B a set of pairs, $0 \neq h \in K[\underline{x}]$.

$C := \{\{h, g\} \mid g \in G\}$
for all $\{h, g_1\} \in C$ **do**
    if (LM(h) and LM($g1$) are NOT disjoint) **and** (there exist $\{h, g_2\} \in C \setminus \{\{h, g_1\}\}$ **s.t.** $\mathrm{lcm}(\mathrm{LM}(h), \mathrm{LM}(g_2)) \mid \mathrm{lcm}(\mathrm{LM}(h), \mathrm{LM}(g_1))$) **then**
        $C := C \setminus \{h, g_1\}$
for all $\{h, g\} \in C$ **do**
    if LM(h) and LM(g) are disjoint **then**
        $C := C \setminus \{h, g\}$
for all $\{g_1, g_2\} \in B$ **do**
    if ($\mathrm{LM}(h) \mid \mathrm{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(g_2))$) **and** ($\mathrm{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(h)) \neq \mathrm{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(g_2))$) **and** ($\mathrm{lcm}(\mathrm{LM}(h), \mathrm{LM}(g_2)) \neq \mathrm{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(g_2))$) **then**
        $B := B \setminus \{g_1, g_2\}$
$B := B \cup C$
for all $g \in G$ **do**
    if $\mathrm{LM}(h) \mid \mathrm{LM}(g)$ **then**
        $G := G \setminus \{g\}$

The F4 Algorithm with update

Require: F is a finite subset of $K[\underline{x}]$

$G := \emptyset$

$B := \emptyset$

for all $f \in F$ **do**

  $(G, B) := \texttt{update}(G, B, f)$

while $B \neq \emptyset$ **do**

  let B^* be a nonempty subset of B

  $B := B \setminus B^*$

  $L := \left\{ \frac{\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LM}(f)} \cdot f \mid \{f, g\} \in B^* \right\}$

  $H := \texttt{basic\_symb\_pre\_proc}(L, G)$

  $\widetilde{H} :=$ a row echelon form of H

  $\widetilde{H}^+ := \{h \in \widetilde{H} \mid \mathrm{LM}(h) \notin \mathrm{LM}(H)\}$

  for all $h \in \widetilde{H}^+$ **do**

    $(G, B) := \texttt{update}(G, B, h)$

return G

The F5 Algorithm [Fau02] (Matrix Version)

Signature

Given $F = (f_1, \ldots, f_m)$, each row tf_i of the Macaulay matrix $\mathcal{M}_d(F)$ is labeled with a signature (t, f_i).

The F5 Algorithm [Fau02] (Matrix Version)

Signature

Given $F = (f_1, \ldots, f_m)$, each row tf_i of the Macaulay matrix $\mathcal{M}_d(F)$ is labeled with a signature (t, f_i).

- Keep labels throughout Gaussian elimination.
- Reduce only downwards during Gaussian and do not switch rows.
- An order among signatures is preserved.

The F5 Algorithm [Fau02] (Matrix Version)

Signature

Given $F = (f_1, \ldots, f_m)$, each row tf_i of the Macaulay matrix $\mathcal{M}_d(F)$ is labeled with a signature (t, f_i).

- Keep labels throughout Gaussian elimination.
- Reduce only downwards during Gaussian and do not switch rows.
- An order among signatures is preserved.

Rewritten Criterion

Given an echelon form $\tilde{M}$ of the Macaulay matrix $\mathcal{M}_d(F)$, use the non-zero rows of $\tilde{M}$ to construct $\mathcal{M}_{d+1}(F)$, avoiding repetitions.

The F5 Algorithm (Matrix Version)

Notation

$\mathcal{M}_{d,i}(F)$ denotes the Macaulay matrix of $(f_1, \ldots, f_i)$ of degree d.

The F5 Algorithm (Matrix Version)

Notation

$\mathcal{M}_{d,i}(F)$ denotes the Macaulay matrix of $(f_1, \ldots, f_i)$ of degree d.

Theorem (F5 Criterion)

For all $j < m$, if we have a row labeled (t, f_j) in the echelon form of $\mathcal{M}_{D-d_m,m-1}$ that has leading term t', then the row (t', f_m) in $\mathcal{M}_{D,m}$ is redundant.

Index of Regularity

Definition

- The **Hilbert function** of $K[\underline{x}]/I$ is defined by $\mathrm{HF}_{K[\underline{x}]/I}(d) = \dim(K[\underline{x}]_d/I_d)$.

Index of Regularity

Definition

- The **Hilbert function** of $K[\underline{x}]/I$ is defined by $\mathrm{HF}_{K[\underline{x}]/I}(d) = \dim(K[\underline{x}]_d/I_d)$.
- The **Hilbert series** of $K[\underline{x}]/I$ is the power series whose coefficients are the Hilbert function

$$\mathrm{HS}_{K[\underline{x}]/I}(z) = \sum_{d=0}^{\infty} \mathrm{HF}_{K[\underline{x}]/I}(d) z^d.$$

Index of Regularity

Definition

- The **Hilbert function** of $K[\underline{x}]/I$ is defined by $\mathrm{HF}_{K[\underline{x}]/I}(d) = \dim(K[\underline{x}]_d/I_d)$.
- The **Hilbert series** of $K[\underline{x}]/I$ is the power series whose coefficients are the Hilbert function

$$\mathrm{HS}_{K[\underline{x}]/I}(z) = \sum_{d=0}^{\infty} \mathrm{HF}_{K[\underline{x}]/I}(d) z^d.$$

- There exists D such that for $d \geq D$, HF is a polynomial in d.

Index of Regularity

Definition

- The **Hilbert function** of $K[\underline{x}]/I$ is defined by $\mathrm{HF}_{K[\underline{x}]/I}(d) = \dim(K[\underline{x}]_d/I_d)$.
- The **Hilbert series** of $K[\underline{x}]/I$ is the power series whose coefficients are the Hilbert function

$$\mathrm{HS}_{K[\underline{x}]/I}(z) = \sum_{d=0}^{\infty} \mathrm{HF}_{K[\underline{x}]/I}(d) z^d.$$

- There exists D such that for $d \geq D$, HF is a polynomial in d.
- The smallest such D is called the **index or regularity**.

Index of Regularity

Definition

- The **Hilbert function** of $K[\underline{x}]/I$ is defined by $\mathrm{HF}_{K[\underline{x}]/I}(d) = \dim(K[\underline{x}]_d/I_d)$.
- The **Hilbert series** of $K[\underline{x}]/I$ is the power series whose coefficients are the Hilbert function

$$\mathrm{HS}_{K[\underline{x}]/I}(z) = \sum_{d=0}^{\infty} \mathrm{HF}_{K[\underline{x}]/I}(d) z^d.$$

- There exists D such that for $d \geq D$, HF is a polynomial in d.
- The smallest such D is called the **index or regularity**.
- The index or regularity is the largest degree of any polynomial in the reduced GB of I.

Regular

Definition

A sequence $F = (f_1, \dots f_m)$ of non-zero homogeneous polynomials is called **regular** if for $i = 2, \dots, m$, for all $g \in K[\underline{x}]$, $gf_i \in \langle f_1, \dots, f_{i-1} \rangle$ implies $g \in \langle f_1, \dots, f_{i-1} \rangle$.

Regular

Definition

A sequence $F = (f_1, \ldots f_m)$ of non-zero homogeneous polynomials is called **regular** if for $i = 2, \ldots, m$, for all $g \in K[\underline{x}]$, $gf_i \in \langle f_1, \ldots, f_{i-1} \rangle$ implies $g \in \langle f_1, \ldots, f_{i-1} \rangle$.

In other words:

- f_i is not a zero divisor in $K[\underline{x}] / \langle f_1, \ldots, f_{i-1} \rangle$.

Regular

Definition

A sequence $F = (f_1, \ldots f_m)$ of non-zero homogeneous polynomials is called **regular** if for $i = 2, \ldots, m$, for all $g \in K[\underline{x}]$, $gf_i \in \langle f_1, \ldots, f_{i-1} \rangle$ implies $g \in \langle f_1, \ldots, f_{i-1} \rangle$.

In other words:

- f_i is not a zero divisor in $K[\underline{x}] / \langle f_1, \ldots, f_{i-1} \rangle$.

Proposition

F is **regular** *iff the syzygy module of F is* **generated by** $\{f_i e_j - f_j e_i : 1 \leq i < j \leq m\}$.

Index of Regularity of Regular Sequence

Theorem

F is regular **iff** *the following is a short exact sequence*

$$0 \longrightarrow \left(\frac{R}{\langle P_{i-1}\rangle}\right)_{d-d_i} \xrightarrow{\times f_i} \left(\frac{R}{\langle P_{i-1}\rangle}\right)_{d} \xrightarrow{\pi} \left(\frac{R}{\langle P_{i}\rangle}\right)_{d} \longrightarrow 0\,,$$

iff *the Hilbert series of F is*

$$\mathrm{HS}_{K[\underline{x}]/I}(z) = \frac{\prod_{i=1}^{m}(1-z^{d_i})}{(1-z)^n}.$$

Index of Regularity of Regular Sequence

Theorem

F is regular **iff** *the following is a short exact sequence*

$$0 \longrightarrow \left(\frac{R}{\langle P_{i-1}\rangle}\right)_{d-d_i} \xrightarrow{\times f_i} \left(\frac{R}{\langle P_{i-1}\rangle}\right)_{d} \xrightarrow{\pi} \left(\frac{R}{\langle P_{i}\rangle}\right)_{d} \longrightarrow 0\,,$$

iff *the Hilbert series of F is*

$$\mathrm{HS}_{K[\underline{x}]/I}(z) = \frac{\prod_{i=1}^{m}(1-z^{d_i})}{(1-z)^n}.$$

- In this case the index of regularity is

$$\sum_{i=1}^{m} d_i - m + 1.$$

Semi-Regularity

- Semi-regular extend the notion of regularity when there are more equations than variables [BFS04].

Semi-Regularity

- Semi-regular extend the notion of regularity when there are more equations than variables [BFS04].
- $f_1, \ldots f_m$ homogeneous and $I = \langle f_1, \ldots f_m \rangle$ zero dimensional.

Semi-Regularity

- Semi-regular extend the notion of regularity when there are more equations than variables [BFS04].
- $f_1, \ldots f_m$ homogeneous and $I = \langle f_1, \ldots f_m \rangle$ zero dimensional.
- Thus $\dim(K[\underline{x}]/I) < \infty$

Semi-Regularity

- Semi-regular extend the notion of regularity when there are more equations than variables [BFS04].
- $f_1, \ldots f_m$ homogeneous and $I = \langle f_1, \ldots f_m \rangle$ zero dimensional.
- Thus $\dim(K[\underline{x}]/I) < \infty$
- and the Hilbert series

$$\mathrm{HS}_{K[\underline{x}]/I}(z)$$

  is a polynomial.

Semi-Regularity

Definition

Let $P = (p_1, \ldots, p_m)$ be a sequence of homogeneous polynomials, $d \geq 0$. P is ***d*-regular** if for all $g \in R$ and all $1 \leq i \leq m$, $gp_i \in \langle P_{i-1} \rangle$ and $\deg(gp_i) < d$ imply $g \in \langle P_{i-1} \rangle$.

Semi-Regularity

Definition

Let $P = (p_1, \ldots, p_m)$ be a sequence of homogeneous polynomials, $d \geq 0$. P is **d-regular** if for all $g \in R$ and all $1 \leq i \leq m$, $gp_i \in \langle P_{i-1} \rangle$ and $\deg(gp_i) < d$ imply $g \in \langle P_{i-1} \rangle$.

Definition

Let I be a homogeneous ideal in R. The **degree of regularity** of I is

$$\min \{d \geq 0 \mid \dim(I_d) = \dim(R_d)\} \; .$$

Semi-Regularity

Definition

A homogeneous sequence of polynomials $P = (p_1, \ldots, p_m)$ in $K[\underline{x}]$ is **semi-regular** if it is D-regular, where D is the degree of regularity of $\langle P \rangle$.

Semi-Regularity

Definition

A homogeneous sequence of polynomials $P = (p_1, \ldots, p_m)$ in $K[\underline{x}]$ is **semi-regular** if it is D-regular, where D is the degree of regularity of $\langle P \rangle$.

Theorem

P is semi-regular

- **iff** *the Hilbert series of $K[\underline{x}]/I$ is*

$$\mathrm{HS}_{K[\underline{x}]/I}(z) = \left[\frac{\prod_{i=1}^{m}(1 - z^{d_i})}{(1 - z)^n}\right]_+ .$$

- **iff** *the ideal I has dimension 0 and every syzygy of F of degree at most $\deg(\mathrm{HS}_{K[\underline{x}]/I})$ is in the module generated by the trivial syzygies $\langle f_i e_j - f_j e_i \rangle$.*

First Fall Degree

Notation

- F^{top} is the highest degree part of each poly in F.
- $\text{Syz}(.)$ is the module of syzygies.
- $\text{Triv}(.)$ is the submodule generated by

$$\{f_i e_j - f_j e_i : 1 \leq i < j \leq m\} \cup \{f_i^{q-1} e_i : 1 \leq im\}.$$

Definition

Let $F \subseteq K[\underline{x}]$. The first fall degree of F is

$$d_{ff}(F) = \min\{d \in \mathbb{N} : \text{Syz}(F^{\text{top}})_d / \text{Triv}(F^{\text{top}})_d \neq 0\}.$$

Last Fall Degree

Matrix Reduction Algorithms

- For small systems we can use a fast matrix reduction algorithm such as Strassen. In this case the time complexity is

$$O\left(\binom{n+D}{n}\right)^{2.81}$$

Matrix Reduction Algorithms

- For small systems we can use a fast matrix reduction algorithm such as Strassen. In this case the time complexity is

$$O\left(\binom{n+D}{n}\right)^{2.81}$$

- For larger systems a sparse linear algebra algorithm is required, e.g. [FL10].

Matrix Reduction Algorithms

- For small systems we can use a fast matrix reduction algorithm such as Strassen. In this case the time complexity is

$$O\left(\binom{n+D}{n}\right)^{2.81}$$

- For larger systems a sparse linear algebra algorithm is required, e.g. [FL10].
- The complexity of such algorithms depends on the sparsity of the matrix.

Matrix Reduction Algorithms

- For small systems we can use a fast matrix reduction algorithm such as Strassen. In this case the time complexity is

$$O\left(\binom{n+D}{n}\right)^{2.81}$$

- For larger systems a sparse linear algebra algorithm is required, e.g. [FL10].
- The complexity of such algorithms depends on the sparsity of the matrix.
- There are hybrid algorithms such as crossbread that can be faster for small fields [JV18].

Matrix Reduction Algorithms

- For small systems we can use a fast matrix reduction algorithm such as Strassen. In this case the time complexity is

$$O\left(\binom{n+D}{n}\right)^{2.81}$$

- For larger systems a sparse linear algebra algorithm is required, e.g. [FL10].
- The complexity of such algorithms depends on the sparsity of the matrix.
- There are hybrid algorithms such as crossbread that can be faster for small fields [JV18].
- Quantum algorithms [BY18].

Matrix Reduction Algorithms

- For small systems we can use a fast matrix reduction algorithm such as Strassen. In this case the time complexity is

$$O\left(\binom{n+D}{n}\right)^{2.81}$$

- For larger systems a sparse linear algebra algorithm is required, e.g. [FL10].
- The complexity of such algorithms depends on the sparsity of the matrix.
- There are hybrid algorithms such as crossbread that can be faster for small fields [JV18].
- Quantum algorithms [BY18].
- Fukuoka MQ Challenge

References I

Magali Bardet, Jean-Charles Faugère, and Bruno Salvy.
On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations.
In *Proceedings of the International Conference on Polynomial System Solving*, pages 71–74, 2004.

Daniel J. Bernstein and Bo-Yin Yang.
Asymptotically faster quantum algorithms to solve multivariate quadratic equations.
In Tanja Lange and Rainer Steinwandt, editors, *Post-Quantum Cryptography*, pages 487–506, Cham, 2018. Springer International Publishing.

J. C. Faugere.
A new efficient algorithm for computing grobner bases without reduction to zero (f5).
ISSAC 2002, ACM Press, pages 75–83, 2002.

Jean-Charles Faugère and Sylvain Lachartre.
Parallel gaussian elimination for gröbner bases computations in finite fields.
In *Proceedings of the 4th International Workshop on Parallel and Symbolic Computation*, PASCO '10, page 89–97, New York, NY, USA, 2010. Association for Computing Machinery.

Antoine Joux and Vanessa Vitse.
A crossbred algorithm for solving boolean polynomial systems.
In Jerzy Kaczorowski, Josef Pieprzyk, and Jacek Pomykała, editors, *Number-Theoretic Methods in Cryptology*, pages 3–21, Cham, 2018. Springer International Publishing.

Additional References

- Cox, D., Little, J., & OShea, D. Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra. Springer Science & Business Media. 2013.
- Cabarcas, D.. An Implementation of Faugère's F4 Algorithm for Computing Gröbner Bases. Master's thesis, University of Cincinnati, 2010.
- Cabarcas, D. Gröbner Bases Computation and Mutant Polynomials. PhD Dissertation, University of Cincinnati, 2011.
- Albrecht, M. Algorithmic Algebraic Techniques and their Application to Block Cipher Cryptanalysis. 2010. PhD Dissertation, Royal Holloway, University of London.
- Spaenlehauer, P. Résolution de systèmes multi-homogènes et déterminantiels algorithmes - complexité - applications. 2012. PhD Dissertation, l'Université Pierre et Marie Curie - Paris 6.

Thanks

Daniel Cabarcas – dcabarc@unal.edu.co

UNIVERSIDAD NACIONAL DE COLOMBIA