

# *Computing critical points using Gröbner Bases: Complexity and Applications*

Jean-Charles Faugère   Mohab Safey El Din  
Pierre-Jean Spaenlehauer

UPMC – CNRS – INRIA Paris - Rocquencourt  
LIP6 – SALSA team

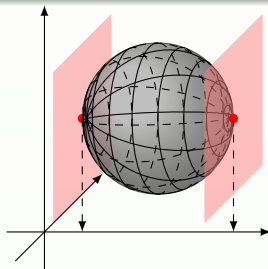
Séminaire Algorithms  
January 31, 2011



# Problem statement

$$(x - 2)^2 + (y - 2)^2 + z^2 - 1 = 0.$$

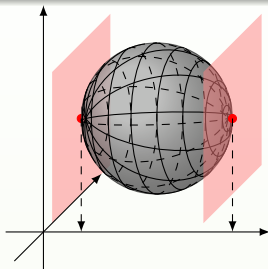
$$M = \begin{bmatrix} 2(x - 2) & 2(y - 2) & 2z \\ 1 & 0 & 0 \end{bmatrix}$$



## *Problem statement*

$$(x - 2)^2 + (y - 2)^2 + z^2 - 1 = 0.$$

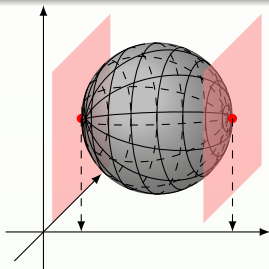
$$M = [2(y - 2) \quad 2z] = [0 \quad 0]$$



## Problem statement

$$(x - 2)^2 + (y - 2)^2 + z^2 - 1 = 0.$$

$$M = \begin{bmatrix} 2(y - 2) & 2z \\ 0 & 0 \end{bmatrix}$$



### Critical points

Let  $f_1, \dots, f_p \in \mathbb{Q}[x_1, \dots, x_n]$  be **polynomials** of degree  $D$  ( $p \leq n - 1$ ) and  $M$  be the  $p \times (n - 1)$  **matrix**

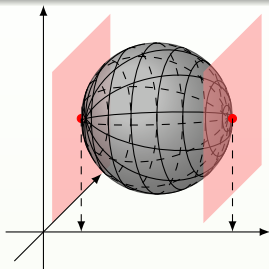
$$\begin{bmatrix} \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_p}{\partial x_2} & \cdots & \frac{\partial f_p}{\partial x_n} \end{bmatrix}.$$

Compute the set of points  $\mathbf{x} \in \mathbb{R}^n$  such that  $f_1(\mathbf{x}) = \cdots = f_p(\mathbf{x}) = 0$  and  $\text{Rank}(M) < p$ .

## Problem statement

$$(x - 2)^2 + (y - 2)^2 + z^2 - 1 = 0.$$

$$M = \begin{bmatrix} 2(y - 2) & 2z \end{bmatrix} = \begin{bmatrix} 0 & 0 \end{bmatrix}$$



### Critical points

Let  $f_1, \dots, f_p \in \mathbb{Q}[x_1, \dots, x_n]$  be **polynomials** of degree  $D$  ( $p \leq n - 1$ ) and  $M$  be the  $p \times (n - 1)$  **matrix**

$$\begin{bmatrix} \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_p}{\partial x_2} & \cdots & \frac{\partial f_p}{\partial x_n} \end{bmatrix}.$$

Compute the set of points  $\mathbf{x} \in \mathbb{R}^n$  such that  $f_1(\mathbf{x}) = \cdots = f_p(\mathbf{x}) = 0$  and  $\text{Rank}(M) < p$ .

$K_0$  is an **algebraic variety**.

$\rightsquigarrow$  **Polynomial system solving**.

## Polynomial Minimization

$$\begin{cases} \min_{(x_1, \dots, x_n) \in \mathbb{R}^n} x_1 \\ \text{s.t. } f_1(x_1, \dots, x_n) = \dots = f_p(x_1, \dots, x_n) = 0. \end{cases}$$

**Assumption:** the minimum is reached on the feasible region.

exact solution/certified numerical solution.

## Polynomial Minimization

$$\begin{cases} \min_{(x_1, \dots, x_n) \in \mathbb{R}^n} \ell(x_1, \dots, x_n) \\ \text{s.t. } f_1(x_1, \dots, x_n) = \dots = f_p(x_1, \dots, x_n) = 0. \end{cases}$$

**Assumption:** the minimum is reached on the feasible region.

exact solution/certified numerical solution.

## Polynomial Minimization

$$\begin{cases} \min_{(x_1, \dots, x_n) \in \mathbb{R}^n} \ell(x_1, \dots, x_n) \\ \text{s.t. } f_1(x_1, \dots, x_n) = \dots = f_p(x_1, \dots, x_n) = 0. \end{cases}$$

**Assumption:** the minimum is reached on the feasible region.

**exact** solution/**certified** numerical solution.

Other applications:

- **Sampling points**
- **Connectivity queries**
- **Quantifier elimination**
- ...

Canny, Grigoriev, Vorobjov, Basu, Pollack, Roy, Bank, Giusti, Heintz, Pardo, Rouillier, Safey, Schost, Hong, ...

## Motivations (II)

Generically, **nb. crit. points**:  $\binom{n-1}{p-1} D^p (D-1)^{n-p}$ .

Generically, **nb. crit. points**:  $\binom{n-1}{p-1} D^p (D-1)^{n-p}$ .

**Geometric algorithms**: Basu, Pollack, Roy, Bank, Giusti, Heintz, M'Bakop, Pardo, Schost, Safey,...

Generically, **nb. crit. points**:  $\binom{n-1}{p-1} D^p (D-1)^{n-p}$ .

**Geometric algorithms**: Basu, Pollack, Roy, Bank, Giusti, Heintz, M'Bakop, Pardo, Schost, Safey,...

Gröbner basis → well-suited for **determinantal ideals** (Faugère, Safey, S. ISSAC 2010).  
Experimentally, computing critical points with **GB algorithms** (RAGlib, FGb in Maple) can solve large problems.

## Motivations (II)

Generically, **nb. crit. points**:  $\binom{n-1}{p-1} D^p (D-1)^{n-p}$ .

**Geometric algorithms**: Basu, Pollack, Roy, Bank, Giusti, Heintz, M'Bakop, Pardo, Schost, Safey,...

Gröbner basis → well-suited for **determinantal ideals** (Faugère, Safey, S. ISSAC 2010).  
Experimentally, computing critical points with **GB algorithms** (RAGlib, FGb in Maple) can solve large problems.

### Goal 1

Arithmetic complexity **polynomial** in the number of **critical points**.

## Motivations (II)

Generically, **nb. crit. points**:  $\binom{n-1}{p-1} D^p (D-1)^{n-p}$ .

**Geometric algorithms**: Basu, Pollack, Roy, Bank, Giusti, Heintz, M'Bakop, Pardo, Schost, Safey,...

Gröbner basis → well-suited for **determinantal ideals** (Faugère, Safey, S. ISSAC 2010).  
Experimentally, computing critical points with **GB algorithms** (RAGlib, FGb in Maple) can solve large problems.

### Goal 1

Arithmetic complexity **polynomial** in the number of **critical points**.

### Goal 2

Use the **structure** of  $\langle \mathbf{F}, \text{MaxMinors}(M) \rangle$  to speed-up the computations.

We focus on the zero-dimensional case

$$\mathcal{I} = \langle \mathbf{F}, \text{MaxMinors}(\mathbf{M}) \rangle$$

$$\mathbf{F}, \text{MaxMinors}(\mathbf{M}) = 0$$

⇓

“grevlex” Gb

⇓

“lex” Gb

**Row Echelon** forms of  
**Macaulay matrices** up to  
degree  $\mathbb{D}_{\text{reg}}$

**Linear algebra** in  $\frac{\mathbb{Q}[\mathbf{X}]}{\mathcal{I}}$   
as  $\mathbb{Q}$ -vect. space of dim.  
 $\text{Deg}(\mathcal{I})$

**Complexity**

$$O\left(\binom{n+\mathbb{D}_{\text{reg}}}{n}^\omega\right)$$

$$O(n \text{Deg}(\mathcal{I})^\omega)$$

$$\mathcal{I} = \langle f_1, \dots, f_p, \text{MaxMinors}(M) \rangle$$

Complexity of **grevlex GB**:  $O\left(\binom{n+\mathbb{D}_{\text{reg}}}{n}^\omega\right)$ .

## Bounds on $\mathbb{D}_{\text{reg}}$

- $f_1, \dots, f_p$  generic and hom.:  $\mathbb{D}_{\text{reg}} = D(p-1) + (D-2)n + 2$ .
- $f_1, \dots, f_p$  generic:  $\mathbb{D}_{\text{reg}} \leq D(p-1) + (D-2)n + 2$ .

$$\mathcal{I} = \langle f_1, \dots, f_p, \text{MaxMinors}(M) \rangle$$

Complexity of **grevlex GB**:  $O\left(\binom{n+\mathbb{D}_{\text{reg}}}{n}^\omega\right)$ .

## Bounds on $\mathbb{D}_{\text{reg}}$

- $f_1, \dots, f_p$  generic and hom.:  $\mathbb{D}_{\text{reg}} = D(p-1) + (D-2)n + 2$ .
- $f_1, \dots, f_p$  generic:  $\mathbb{D}_{\text{reg}} \leq D(p-1) + (D-2)n + 2$ .

## Complexity

When  $D$  and  $p$  are constant, the **arithmetic complexity** of computing a **lex GB** of  $\mathcal{I}$  is **upper** bounded by:

- $O(n^{2p\omega})$  if  $D = 2$ ;
- $O\left(\frac{1}{\sqrt{n}}((D-1)e)^{n\omega}\right)$  if  $D > 2$ .

$\rightsquigarrow$  **polynomial in  $\text{DEG}(\mathcal{I})$ .**

	System	→	grevlex GB	→	lex GB.
<i>Complexity</i>				<i>Change of ordering</i>	
	$O\left(\binom{n + \mathbb{D}_{\text{reg}}}{\mathbb{D}_{\text{reg}}}\omega\right)$				$O(n \cdot \text{DEG}^\omega)$

## Step 1:

- Start with an **affine** critical point system  $f_1, \dots, f_p, \text{MaxMinors}(M)$ .
- Consider the **homogeneous part of highest degree**  
 $\rightsquigarrow f_1^{(h)}, \dots, f_p^{(h)}, \text{MaxMinors}(M^{(h)})$
- Homogeneous system is 0-dim  
 $\rightarrow \mathbb{D}_{\text{reg}} \text{ affine} \leq \mathbb{D}_{\text{reg}} \text{ hom. and DEG affine} \leq \text{DEG hom.}$

	System	→	grevlex GB	→	lex GB.
<i>Complexity</i>				<i>Change of ordering</i>	
			$O\left(\binom{n + \mathbb{D}_{\text{reg}}}{\mathbb{D}_{\text{reg}}}\omega\right)$		$O(n \cdot \text{DEG}^\omega)$

## Step 1:

- Start with an **affine** critical point system  $f_1, \dots, f_p, \text{MaxMinors}(M)$ .
  - Consider the **homogeneous part of highest degree**  
 $\rightsquigarrow f_1^{(h)}, \dots, f_p^{(h)}, \text{MaxMinors}(M^{(h)})$
  - Homogeneous system is 0-dim  
 $\rightarrow \mathbb{D}_{\text{reg}} \text{ affine} \leq \mathbb{D}_{\text{reg}} \text{ hom. and DEG affine} \leq \text{DEG hom.}$
- $\Rightarrow$  for the analysis, we can assume that  $f_1, \dots, f_p$  are **homogeneous**.

	System	→	grevlex GB	→	lex GB.
<i>Complexity</i>				<i>Change of ordering</i>	
	$O\left(\binom{n + \mathbb{D}_{\text{reg}}}{\mathbb{D}_{\text{reg}}}\omega\right)$				$O(n \cdot \text{DEG}^\omega)$

## Step 1:

- Start with an **affine** critical point system  $f_1, \dots, f_p, \text{MaxMinors}(M)$ .
- Consider the **homogeneous part of highest degree**  
 $\rightsquigarrow f_1^{(h)}, \dots, f_p^{(h)}, \text{MaxMinors}(M^{(h)})$
- Homogeneous system is 0-dim  
 $\rightarrow \mathbb{D}_{\text{reg}} \text{ affine} \leq \mathbb{D}_{\text{reg}} \text{ hom. and DEG affine} \leq \text{DEG hom.}$

$\Rightarrow$  for the analysis, we can assume that  $f_1, \dots, f_p$  are **homogeneous**.

## Step 2:

- Find  $\mathbb{D}_{\text{reg}}$  is the **homogeneous** setting.

## *Something special happens with minors...*

We consider **maximal minors** of polynomial matrices.

*Bernstein/Sturmfels/Zelevinski 1993, ...*

Let  $\mathbf{U} = (u_{i,j})$  be an  $p \times (n - 1)$  matrix whose entries are **indeterminates**. The set of **maximal minors** of  $\mathbf{U}$  is a universal Gröbner basis.

$\rightsquigarrow$  This gives the intuition that good things may happen in **Gröbner bases** computations.

# Something special happens with minors...

We consider **maximal minors** of polynomial matrices.

*Bernstein/Sturmfels/Zelevinski 1993, ...*

Let  $\mathbf{U} = (u_{i,j})$  be an  $p \times (n-1)$  matrix whose entries are **indeterminates**. The set of **maximal minors** of  $\mathbf{U}$  is a universal Gröbner basis.

$\rightsquigarrow$  This gives the intuition that good things may happen in **Gröbner bases** computations.

**MaxMinors(M)** (*Faugère/Safey/S.*)

Let  $M$  with be an  $p \times (n-1)$  matrix whose entries are linear forms in  $\mathbb{Q}[x_0, \dots, x_{n-1-p}]$ . A *grevlex* Gröbner basis  $\text{Minors}(M, p)$  is a linear combination of the  $p \times p$  minors.

Here  $\mathbb{D}_{\text{reg}} = p$  (to be compared with Macaulay's bound  $(n-p)p(D-1)+1$ ).

Generating series of the **rank defects** of successive **Macaulay matrices**.

Generating series of the **rank defects** of successive **Macaulay matrices**.

- $\mathbb{Q}[\mathbf{X}]_d = \{f \in \mathbb{Q}[\mathbf{X}] \mid \deg(f) = d, f \text{ homogeneous} \}$
- $\mathbb{Q}[\mathbf{X}] = \bigoplus_{d \geq 0} \mathbb{Q}[\mathbf{X}]_d$

Generating series of the **rank defects** of successive Macaulay matrices.

- $\mathbb{Q}[\mathbf{X}]_d = \{f \in \mathbb{Q}[\mathbf{X}] \mid \deg(f) = d, f \text{ homogeneous}\}$
- $\mathbb{Q}[\mathbf{X}] = \bigoplus_{d \geq 0} \mathbb{Q}[\mathbf{X}]_d$

Let  $I$  be a **homogeneous** ideal of  $\mathbb{Q}[\mathbf{X}] = \mathbb{Q}[x_1, \dots, x_n]$ .

- $I_d = \{f \in I \mid \deg(f) = d, f \text{ homogeneous}\}, I = \bigoplus_{d \geq 0} I_d$
- $\frac{\mathbb{Q}[\mathbf{X}]_d}{I_d}$  is a finite dimensional  $\mathbb{Q}$ -vector space.

Generating series of the **rank defects** of successive Macaulay matrices.

- $\mathbb{Q}[\mathbf{X}]_d = \{f \in \mathbb{Q}[\mathbf{X}] \mid \deg(f) = d, f \text{ homogeneous}\}$
- $\mathbb{Q}[\mathbf{X}] = \bigoplus_{d \geq 0} \mathbb{Q}[\mathbf{X}]_d$

Let  $I$  be a **homogeneous** ideal of  $\mathbb{Q}[\mathbf{X}] = \mathbb{Q}[x_1, \dots, x_n]$ .

- $I_d = \{f \in I \mid \deg(f) = d, f \text{ homogeneous}\}$ ,  $I = \bigoplus_{d \geq 0} I_d$
- $\frac{\mathbb{Q}[\mathbf{X}]_d}{I_d}$  is a finite dimensional  $\mathbb{Q}$ -vector space.

**Hilbert series of  $I$ :**  $HS_I(t) = \sum_{d=0} \dim \left( \frac{\mathbb{Q}[\mathbf{X}]_d}{I_d} \right) t^d$

- $\dim(I)$  and  $\text{DEG}(I)$  ( $= P(1)$ ) can be read on  $HS_I(t) = \frac{P(t)}{(1-t)^{\dim(I)}}$ .
- If  $I$  has dimension 0,  $\mathbb{D}_{\text{reg}}(I) = \deg(HS_I(t)) + 1$ .

Generating series of the **rank defects** of successive Macaulay matrices.

- $\mathbb{Q}[\mathbf{X}]_d = \{f \in \mathbb{Q}[\mathbf{X}] \mid \deg(f) = d, f \text{ homogeneous}\}$
- $\mathbb{Q}[\mathbf{X}] = \bigoplus_{d \geq 0} \mathbb{Q}[\mathbf{X}]_d$

Let  $I$  be a **homogeneous** ideal of  $\mathbb{Q}[\mathbf{X}] = \mathbb{Q}[x_1, \dots, x_n]$ .

- $I_d = \{f \in I \mid \deg(f) = d, f \text{ homogeneous}\}$ ,  $I = \bigoplus_{d \geq 0} I_d$
- $\frac{\mathbb{Q}[\mathbf{X}]_d}{I_d}$  is a finite dimensional  $\mathbb{Q}$ -vector space.

**Hilbert series of  $I$ :**  $HS_I(t) = \sum_{d=0} \dim \left( \frac{\mathbb{Q}[\mathbf{X}]_d}{I_d} \right) t^d$

- $\dim(I)$  and  $\text{DEG}(I)$  ( $= P(1)$ ) can be read on  $HS_I(t) = \frac{P(t)}{(1-t)^{\dim(I)}}$ .
- If  $I$  has dimension 0,  $\mathbb{D}_{\text{reg}}(I) = \deg(HS_I(t)) + 1$ .
- If  $f$  is homogeneous of degree  $D$  and does not belong to any prime associated to  $I$ ,  $HS_{I+\langle f \rangle}(t) = (1 - t^D)HS_I(t)$ .

$f_1, \dots, f_p$  homogeneous.  $\mathcal{I} = \langle f_1, \dots, f_p, \text{MaxMinors}(M) \rangle$ .

## Goal:

- obtain an explicit formula for  $\text{HS}_{\mathcal{I}}(t)$ .

$f_1, \dots, f_p$  homogeneous.  $\mathcal{I} = \langle f_1, \dots, f_p, \text{MaxMinors}(M) \rangle$ .

## Goal:

- obtain an explicit formula for  $\text{HS}_{\mathcal{I}}(t)$ .

## Strategy:

- Start with the  $p \times (n-1)$  matrix  $\mathbf{U} = (u_{i,j})$  whose entries are **independent variables**. Let  $\mathcal{U}$  be the ideal generated by the maximal minors of  $\mathbf{U}$ .  
**Abhyankar's formula**  $\rightsquigarrow \text{HS}_{\mathcal{U}}(t)$ .
- $\mathcal{I} = (\mathcal{U} + \langle \{u_{i,j} - \frac{\partial f_i}{\partial x_j}\}, f_1, \dots, f_p \rangle) \cap \mathbb{Q}[\mathbf{X}]$ .  
Handle the fact that  $u_{i,j} - \frac{\partial f_i}{\partial x_j}$  is **not homogeneous**.
- Obtain a **relation** between the **Hilbert series** of  $\mathcal{U}$  and  $\mathcal{I}$

# Determinantal ideals

$\mathbf{U} = (u_{i,j})$ :  $p \times (n - 1)$  matrix whose entries are **independent variables**.

$$\mathcal{U} = \langle \text{MaxMinors}(\mathbf{U}) \rangle.$$

## Abhyankar's formula

Abhyankar 1988, Conca/Herzog 1994.

$$\text{HS}_{\mathcal{U}}(t) = \frac{\det(A(t))}{t^{\binom{p-1}{2}}(1-t)^{n(p-1)}},$$

where  $A(t)$  is the  $(p - 1) \times (p - 1)$  matrix where  $A_{i,j}(t) = \sum \binom{p-i}{\ell} \binom{n-1-j}{\ell} t^{\ell}$ .

## Properties of $\mathcal{U}$

- $\text{codim}(\mathcal{U}) = n - p$ .
- $\text{DEG}(\mathcal{U}) = \binom{n-1}{p-1}$ .

## *Additional property*

*Theorem (Macaulay, Hochster, Eagon)*

Determinantal rings are **Cohen-Macaulay**.

*Theorem (Macaulay, Hochster, Eagon)*

Determinantal rings are **Cohen-Macaulay**.

$$\mathcal{I} = \left( \mathcal{U} + \left\langle u_{i,j} - \frac{\partial f_i}{\partial x_j} \right\rangle + \langle f_1, \dots, f_p \rangle \right) \cap \mathbb{Q}[\mathbf{X}]$$

## *Additional property*

*Theorem (Macaulay, Hochster, Eagon)*

Determinantal rings are **Cohen-Macaulay**.

$$\mathcal{I} = \left( \mathcal{U} + \left\langle u_{ij} - \frac{\partial f_i}{\partial x_j} \right\rangle + \langle f_1, \dots, f_p \rangle \right) \cap \mathbb{Q}[\mathbf{X}]$$

*Lemma*

**Algebraic Sard's Theorem**  $\Rightarrow \dim(\mathcal{I}) = 0$ .

## Additional property

Theorem (Macaulay, Hochster, Eagon)

Determinantal rings are **Cohen-Macaulay**.

$$\mathcal{I} = \left( \mathcal{U} + \left\langle u_{i,j} - \frac{\partial f_i}{\partial x_j} \right\rangle + \langle f_1, \dots, f_p \rangle \right) \cap \mathbb{Q}[\mathbf{X}]$$

Lemma

**Algebraic Sard's Theorem**  $\Rightarrow \dim(\mathcal{I}) = 0$ .

$\rightsquigarrow (\mathcal{U} + \langle \{u_{i,j} - \frac{\partial f_i}{\partial x_j}\}, f_1, \dots, f_p \rangle) = \mathcal{I} + \langle u_{i,j} - \frac{\partial f_i}{\partial x_j} \rangle \subset \mathbb{Q}[\mathbf{X}, \mathbf{U}]$  has dimension 0.

$\rightsquigarrow \langle \{u_{i,j} - \frac{\partial f_i}{\partial x_j}\}, f_1, \dots, f_p \rangle$  has codimension  $np$  as an ideal of  $\mathbb{Q}[\mathbf{X}, \mathbf{U}]/\mathcal{U}$ .

## Additional property

Theorem (Macaulay, Hochster, Eagon)

Determinantal rings are **Cohen-Macaulay**.

$$\mathcal{I} = \left( \mathcal{U} + \left\langle u_{i,j} - \frac{\partial f_i}{\partial x_j} \right\rangle + \langle f_1, \dots, f_p \rangle \right) \cap \mathbb{Q}[\mathbf{X}]$$

Lemma

**Algebraic Sard's Theorem**  $\Rightarrow \dim(\mathcal{I}) = 0$ .

$\rightsquigarrow (\mathcal{U} + \langle \{u_{i,j} - \frac{\partial f_i}{\partial x_j}\}, f_1, \dots, f_p \rangle) = \mathcal{I} + \langle u_{i,j} - \frac{\partial f_i}{\partial x_j} \rangle \subset \mathbb{Q}[\mathbf{X}, \mathbf{U}]$  has dimension 0.

$\rightsquigarrow \langle \{u_{i,j} - \frac{\partial f_i}{\partial x_j}\}, f_1, \dots, f_p \rangle$  has codimension  $np$  as an ideal of  $\mathbb{Q}[\mathbf{X}, \mathbf{U}]/\mathcal{U}$ .

$\rightsquigarrow$  **regular sequence** in  $\mathbb{Q}[\mathbf{X}, \mathbf{U}]/\mathcal{U}$  (Unmixedness Theorem).

If  $u_{i,j} - \frac{\partial f_i}{\partial x_j}$  were homogeneous, we could conclude.

# Back to the “homogeneous” case

We consider  $\mathcal{U}$  as an ideal of  $\mathbb{Q}[\mathbf{U}, \mathbf{X}]$ .

- $\text{HS}_{\mathcal{U}}(t)$  is known and  $u_{i,j} - \frac{\partial f_i}{\partial x_j}$  is **not homogeneous**.
- $\rightsquigarrow$  we consider all variables  $u_{i,j}$  as variables of **weight  $D - 1$**   
With such a weight,  $u_{i,j} - \frac{\partial f_i}{\partial x_j}$  may be seen as a “homogeneous” polynomial.
- quasi-homogeneous polynomial  $f$  of weight degree  $d$  and type  $(D - 1, 1)$ :  
 $f(\lambda^{D-1}\mathbf{U}, \lambda\mathbf{X}) = \lambda^d f(\mathbf{U}, \mathbf{X})$

This allows to define a grading of the polynomial ring  $\mathbb{Q}[\mathbf{U}, \mathbf{X}]$ .  
We use this grading

# Abhyankar's formula with weights and properties of $\mathcal{U}$

- $\mathbb{Q}[\mathbf{U}, \mathbf{X}] = \bigoplus_{d \in \mathbb{N}} \mathbb{Q}[\mathbf{U}, \mathbf{X}]_d$  (with weight degrees)
- **Quasi-homogeneous ideals** are those which are generated by a set of quasi-homogeneous set of polynomials.
- $\rightsquigarrow$  **weighted Hilbert series**  $\text{wHS}_I(t) = \sum_{d \in \mathbb{N}} \dim \left( \frac{\mathbb{Q}[\mathbf{U}, \mathbf{X}]_d}{I_d} \right) t^d$ .

# Abhyankar's formula with weights and properties of $\mathcal{U}$

- $\mathbb{Q}[\mathbf{U}, \mathbf{X}] = \bigoplus_{d \in \mathbb{N}} \mathbb{Q}[\mathbf{U}, \mathbf{X}]_d$  (with weight degrees)
- **Quasi-homogeneous ideals** are those which are generated by a set of quasi-homogeneous set of polynomials.
- $\rightsquigarrow$  **weighted Hilbert series**  $\text{wHS}_I(t) = \sum_{d \in \mathbb{N}} \dim \left( \frac{\mathbb{Q}[\mathbf{U}, \mathbf{X}]_d}{I_d} \right) t^d$ .

## First Properties (well-known)

In  $\mathbb{Q}[\mathbf{U}]$ , the weighted Hilbert series of the ideal  $\mathcal{U}$  (with  $u_{i,j}$  of weight  $D - 1$ ) is

$$\text{wHS}_{\mathcal{U}}(t^{D-1})$$

In  $\mathbb{Q}[\mathbf{X}, \mathbf{U}]$ , The weighted Hilbert series of the ideal  $\mathcal{U}$  (with  $u_{i,j}$  of weight  $D - 1$ ) is

$$\text{wHS}_{\mathcal{U}}(t^{D-1}) / (1 - t)^n.$$

(Milnor, Olinik, Walreich, see “Poincaré series of a graded algebra”, Bourbaki)

# Abhyankar's formula with weights and properties of $\mathcal{U}$

- $\mathbb{Q}[\mathbf{U}, \mathbf{X}] = \bigoplus_{d \in \mathbb{N}} \mathbb{Q}[\mathbf{U}, \mathbf{X}]_d$  (with weight degrees)
- **Quasi-homogeneous ideals** are those which are generated by a set of quasi-homogeneous set of polynomials.
- $\rightsquigarrow$  **weighted Hilbert series**  $\text{wHS}_{\mathcal{I}}(t) = \sum_{d \in \mathbb{N}} \dim \left( \frac{\mathbb{Q}[\mathbf{U}, \mathbf{X}]_d}{I_d} \right) t^d$ .

## First Properties (well-known)

In  $\mathbb{Q}[\mathbf{U}]$ , the weighted Hilbert series of the ideal  $\mathcal{U}$  (with  $u_{i,j}$  of weight  $D - 1$ ) is

$$\text{wHS}_{\mathcal{U}}(t^{D-1})$$

In  $\mathbb{Q}[\mathbf{X}, \mathbf{U}]$ , The weighted Hilbert series of the ideal  $\mathcal{U}$  (with  $u_{i,j}$  of weight  $D - 1$ ) is

$$\text{wHS}_{\mathcal{U}}(t^{D-1}) / (1 - t)^n.$$

(Milnor, Olinik, Walreich, see "Poincaré series of a graded algebra", Bourbaki)

$$\rightsquigarrow \text{In } \mathbb{Q}[\mathbf{X}, \mathbf{U}], \quad \text{wHS}_{\mathcal{U}}(t) = \frac{\det(A(t^{D-1}))}{t^{(D-1)\binom{p-1}{2}} (1 - t^{D-1})^{n(p-1)} (1 - t)^n}.$$

# Adding a regular sequence

$$\mathcal{I} = \langle f_1, \dots, f_p, \text{MaxMinors}(M) \rangle.$$

$(\{u_{i,j} - \frac{\partial f_i}{\partial x_j}\}, f_1, \dots, f_p)$  is a  $\mathbb{Q}[\mathbf{X}, \mathbf{U}]/\mathcal{U}$ -**regular sequence**:

$$\text{wHS}_{\mathcal{U} + \langle \{u_{i,j} - \frac{\partial f_i}{\partial x_j}\}, f_1, \dots, f_p \rangle}(t) = (1 - t^{D-1})^{(n-1)p} (1 - t^D)^p \text{HS}_{\mathcal{U}}(t^{D-1})$$

# Adding a regular sequence

$$\mathcal{I} = \langle f_1, \dots, f_p, \text{MaxMinors}(M) \rangle.$$

$(\{u_{i,j} - \frac{\partial f_i}{\partial x_j}\}, f_1, \dots, f_p)$  is a  $\mathbb{Q}[\mathbf{X}, \mathbf{U}]/\mathcal{U}$ -**regular sequence**:

$$\begin{aligned} \text{wHS}_{\mathcal{U} + \langle \{u_{i,j} - \frac{\partial f_i}{\partial x_j}\}, f_1, \dots, f_p \rangle}(t) &= (1 - t^{D-1})^{(n-1)p} (1 - t^D)^p \text{HS}_{\mathcal{U}}(t^{D-1}) \\ &= \frac{(1 - t^{D-1})^{(n-1)p} (1 - t^D)^p \det(A(t^{D-1}))}{(1 - t^{D-1})^{n(p-1)} (1 - t)^n t^{(D-1)\binom{p-1}{2}}} \end{aligned}$$

# Adding a regular sequence

$$\mathcal{I} = \langle f_1, \dots, f_p, \text{MaxMinors}(M) \rangle.$$

$(\{u_{i,j} - \frac{\partial f_i}{\partial x_j}\}, f_1, \dots, f_p)$  is a  $\mathbb{Q}[\mathbf{X}, \mathbf{U}]/\mathcal{U}$ -**regular sequence**:

$$\begin{aligned} \text{wHS}_{\mathcal{U} + \langle \{u_{i,j} - \frac{\partial f_i}{\partial x_j}\}, f_1, \dots, f_p \rangle}(t) &= (1 - t^{D-1})^{(n-1)p} (1 - t^D)^p \text{HS}_{\mathcal{U}}(t^{D-1}) \\ &= \frac{(1 - t^{D-1})^{(n-1)p} (1 - t^D)^p \det(A(t^{D-1}))}{(1 - t^{D-1})^{n(p-1)} (1 - t)^n t^{(D-1)\binom{p-1}{2}}} \\ &= \frac{(1 - t^{D-1})^{n-p} (1 - t^D)^p \det(A(t^{D-1}))}{(1 - t)^n t^{(D-1)\binom{p-1}{2}}} \end{aligned}$$

# Adding a regular sequence

$$\mathcal{I} = \langle f_1, \dots, f_p, \text{MaxMinors}(M) \rangle.$$

$(\{u_{i,j} - \frac{\partial f_i}{\partial x_j}\}, f_1, \dots, f_p)$  is a  $\mathbb{Q}[\mathbf{X}, \mathbf{U}]/\mathcal{U}$ -**regular sequence**:

$$\begin{aligned} \text{wHS}_{\mathcal{U} + \langle \{u_{i,j} - \frac{\partial f_i}{\partial x_j}\}, f_1, \dots, f_p \rangle}(t) &= (1 - t^{D-1})^{(n-1)p} (1 - t^D)^p \text{HS}_{\mathcal{U}}(t^{D-1}) \\ &= \frac{(1 - t^{D-1})^{(n-1)p} (1 - t^D)^p \det(A(t^{D-1}))}{(1 - t^{D-1})^{n(p-1)} (1 - t)^n t^{(D-1)\binom{p-1}{2}}} \\ &= \frac{(1 - t^{D-1})^{n-p} (1 - t^D)^p \det(A(t^{D-1}))}{(1 - t)^n t^{(D-1)\binom{p-1}{2}}} \\ &= \text{HS}_{\mathcal{I}}(t). \end{aligned}$$

**Problem:** under which conditions is the **Hilbert series** equal to

$$\text{HS}_{\mathcal{I}}(t) = \frac{(1 - t^{D-1})^{n-p} (1 - t^D)^p \det(A(t^{D-1}))}{(1 - t)^n t^{(D-1)\binom{p-1}{2}}}$$

# Genericity ?

**Problem:** under which conditions is the **Hilbert series** equal to

$$\text{HS}_{\mathcal{I}}(t) = \frac{(1 - t^{D-1})^{n-p} (1 - t^D)^p \det(A(t^{D-1}))}{(1 - t)^n t^{(D-1)\binom{p-1}{2}}}$$

*Theorem (Eisenbud, Conca, Herzog)*

Let  $B$  be a  $p \times (n - 1)$  matrix whose entries are **homogeneous** polynomials in  $\mathbb{K}[X]$ :

$$B = \begin{bmatrix} f_{1,1} & \dots & f_{1,n-1} \\ \vdots & \ddots & \vdots \\ f_{p,1} & \dots & f_{p,n-1} \end{bmatrix}$$

If  $\text{codim}(\langle \text{MaxMinors}(B) \rangle) = n - p$ , then

$$\text{HS}_{\langle \text{MaxMinors}(B) \rangle}(t) = \frac{\det(A(t))}{t^{\binom{p-1}{2}} (1 - t)^{\dim(\langle \text{MaxMinors}(B) \rangle)}}.$$

# Genericity ?

**Problem:** under which conditions is the **Hilbert series** equal to

$$\text{HS}_{\mathcal{I}}(t) = \frac{(1 - t^{D-1})^{n-p} (1 - t^D)^p \det(A(t^{D-1}))}{(1 - t)^n t^{(D-1)\binom{p-1}{2}}}$$

*Theorem (Eisenbud, Conca, Herzog)*

Let  $B$  be a  $p \times (n-1)$  matrix whose entries are **homogeneous** polynomials in  $\mathbb{K}[X]$ :

$$B = \begin{bmatrix} f_{1,1} & \dots & f_{1,n-1} \\ \vdots & \ddots & \vdots \\ f_{p,1} & \dots & f_{p,n-1} \end{bmatrix}$$

If  $\text{codim}(\langle \text{MaxMinors}(B) \rangle) = n - p$ , then

$$\text{HS}_{\langle \text{MaxMinors}(B) \rangle}(t) = \frac{\det(A(t))}{t^{\binom{p-1}{2}} (1 - t)^{\dim(\langle \text{MaxMinors}(B) \rangle)}}.$$

$\rightsquigarrow$  **Answer:** Equivalent to  $\dim(\mathcal{I}) = 0$ .

## Degree and regularity

$$\mathrm{HS}_{\mathcal{I}}(t) = \frac{(1 - t^{D-1})^{n-p} (1 - t^D)^p \det(A(t^{D-1}))}{(1 - t)^n t^{(D-1)\binom{p-1}{2}}}.$$

### Homogeneous

$$\mathbb{D}_{\mathrm{reg}} = \deg(\mathrm{HS}_{\mathcal{I}}(t)) + 1 = D(p-1) + (D-2)n + 2.$$

$$\mathrm{DEG}(\mathcal{I}) = \mathrm{HS}_{\mathcal{I}}(1) = \binom{n-1}{p-1} D^p (D-1)^{n-p}.$$

## Degree and regularity

$$\mathrm{HS}_{\mathcal{I}}(t) = \frac{(1 - t^{D-1})^{n-p} (1 - t^D)^p \det(A(t^{D-1}))}{(1 - t)^n t^{(D-1)\binom{p-1}{2}}}.$$

### Homogeneous

$$\mathbb{D}_{\mathrm{reg}} = \deg(\mathrm{HS}_{\mathcal{I}}(t)) + 1 = D(p-1) + (D-2)n + 2.$$

$$\mathrm{DEG}(\mathcal{I}) = \mathrm{HS}_{\mathcal{I}}(1) = \binom{n-1}{p-1} D^p (D-1)^{n-p}.$$

Back to the non-homogeneous case

↪ consider the homogeneous part of highest degree:

## Degree and regularity

$$\text{HS}_{\mathcal{I}}(t) = \frac{(1 - t^{D-1})^{n-p} (1 - t^D)^p \det(A(t^{D-1}))}{(1 - t)^n t^{(D-1)\binom{p-1}{2}}}.$$

### Homogeneous

$$\mathbb{D}_{\text{reg}} = \deg(\text{HS}_{\mathcal{I}}(t)) + 1 = D(p-1) + (D-2)n + 2.$$

$$\text{DEG}(\mathcal{I}) = \text{HS}_{\mathcal{I}}(1) = \binom{n-1}{p-1} D^p (D-1)^{n-p}.$$

Back to the non-homogeneous case

↪ consider the homogeneous part of highest degree:

### Non-homogeneous

$$\mathbb{D}_{\text{reg}} \leq D(p-1) + (D-2)n + 2.$$

$$\text{DEG}(\mathcal{I}) \leq \binom{n-1}{p-1} D^p (D-1)^{n-p}.$$

Bounds are **reached** in practice !

$\mathbb{D}_{\text{reg}}$  independant of  $n$  when  $D = 2$ .

	System	→	grevlex GB	→	lex GB.
<i>Complexity</i>				<i>Change of ordering</i>	
			$O\left(\binom{n + D_{\text{reg}}}{D_{\text{reg}}}\right)^\omega$		$O(n \cdot \text{DEG}^\omega)$

	System	→	grevlex GB	→	lex GB.
<i>Complexity</i>				<i>Change of ordering</i>	
	$O\left(\binom{n + D_{\text{reg}}}{D_{\text{reg}}}\omega\right)$				$O(n \cdot \text{DEG}^\omega)$

First analysis: how does the complexity behave when  $n$  grows ?

## Complexity of grevlex GB

$\omega$  feasible exponent for computing the row echelon form.

$$\begin{array}{l|l} \text{if } D = 2 & O(n^{2p\omega}), \text{ polynomial in } n. \\ \text{if } D > 2 & O((D-1)e)^{n\omega} \end{array}$$

## Complexity of change of ordering

$$O\left(n \binom{n-1}{p-1}^\omega D^{p\omega} (D-1)^{(n-p)\omega}\right)$$

↪ upper bounded by the complexity of grevlex GB

## Complexity (II)

The number of arithmetic operations for computing a lex GB of  $\mathcal{I}$  is upper bounded by

$$O\left(\text{DEG}(\mathcal{I})^{\frac{\log(D)+\log(2)+1}{\log(D-1)}\omega}\right).$$

## Complexity (II)

The number of arithmetic operations for computing a lex GB of  $\mathcal{I}$  is upper bounded by

$$O\left(\text{DEG}(\mathcal{I})^{\frac{\log(D)+\log(2)+1}{\log(D-1)}\omega}\right).$$

$$\frac{\log(D) + \log(2) + 1}{\log(D - 1)} < 4.03 \text{ for } D > 2,$$

## Complexity (II)

The number of arithmetic operations for computing a lex GB of  $\mathcal{I}$  is upper bounded by

$$O\left(\text{DEG}(\mathcal{I})^{\frac{\log(D)+\log(2)+1}{\log(D-1)}\omega}\right).$$

$$\frac{\log(D) + \log(2) + 1}{\log(D - 1)} < 4.03 \text{ for } D > 2,$$

↪ complexity is **polynomial** in the number of **critical points**.

# Complexity (II)

The number of arithmetic operations for computing a lex GB of  $\mathcal{I}$  is upper bounded by

$$O\left(\text{DEG}(\mathcal{I})^{\frac{\log(D)+\log(2)+1}{\log(D-1)}\omega}\right).$$

$$\frac{\log(D) + \log(2) + 1}{\log(D - 1)} < 4.03 \text{ for } D > 2,$$

↪ complexity is **polynomial** in the number of **critical points**.

$$\lim_{D \rightarrow \infty} \frac{\log(D) + \log(2) + 1}{\log(D - 1)} = 1.$$

$$\text{Numerical evaluations: } \frac{\log\left(\binom{n+\mathbb{D}_{\text{reg}}}{n}\right)}{\log(\text{DEG}(\mathcal{I}))} \approx 1.3$$

## Conclusion

- New **complexity** estimates.
- Understanding of the experimental behaviour.
- A new family of **structured systems** solvable in **polynomial** arithmetic complexity with **Gröbner bases**.
- **Hilbert series**  $\rightsquigarrow$  first step towards a dedicated GB algorithm.

## Conclusion

- New **complexity** estimates.
- Understanding of the experimental behaviour.
- A new family of **structured systems** solvable in **polynomial** arithmetic complexity with **Gröbner bases**.
- **Hilbert series**  $\rightsquigarrow$  first step towards a dedicated GB algorithm.

## Work in progress

- **Mixed** degrees.
- $F_5$ /**Reductions to zero**.

$\rightsquigarrow$  tools from **homological algebra**.

## Cryptology and Information Theory

- Cryptanalysis of **HFE** (Kipnis, Shamir, Bettale, Perret, Faugère, ...).
  - Courtois authentication scheme (Courtois, Perret, Faugère, Levy-dit-Vehel, Safey El Din, S., ...).
  - **Rank metric** decoding (Gabidulin, Loidreau, Ourivski, Johannsson, ...).
- 
- **Multihomogeneous** systems.
  - **Enumerative geometry**: Schubert calculus, Secant conjecture, ...
  - **Polar/Bipolar** varieties.
  - Global optimization (cf. **Aurelien's** talk),...