Régularisation du calcul de bases de Gröbner pour des systèmes avec poids et déterminantiels, et application en imagerie médicale

Thibaut VERRON

sous la direction de Jean-Charles FAUGÈRE

et Mohab SAFEY EL DIN

Sorbonne Universités, UPMC Univ. Paris 06, LIP6, CNRS, Inria Paris, Équipe POLSYS

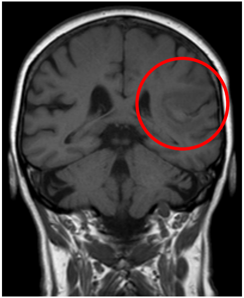
26 septembre 2016

An example: the contrast optimisation problem (1)

(N)MRI = (Nuclear) Magnetic Resonance Imagery

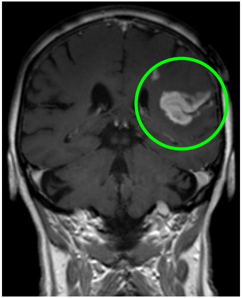
1. Apply a magnetic field to a body
2. Measure the radio waves emitted in reaction

Goal = optimize the contrast = distinguish two biological matters from this measure



?

Bad contrast (not enhanced)



✓

Good contrast (enhanced)

Known methods:

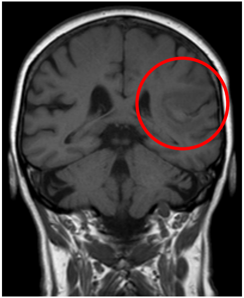
- inject contrast agents to the patient: potentially toxic
- make the field variable to exploit differences in relaxation times
  $\Longrightarrow$ requires finding optimal settings depending on the relaxation parameters

An example: the contrast optimisation problem (1)

(N)MRI = (Nuclear) Magnetic Resonance Imagery

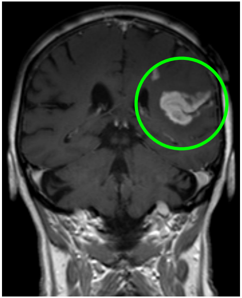
1. Apply a magnetic field to a body
2. Measure the radio waves emitted in reaction

Goal = optimize the contrast = distinguish two biological matters from this measure



?

Bad contrast (not enhanced)



✓

Good contrast (enhanced)

Examples of relaxation parameters:

- Water: $\gamma = \Gamma = 0.01\,\mathrm{Hz}$
- Cerebrospinal fluid: $\gamma = 0.02\,\mathrm{Hz}$, $\Gamma = 0.10\,\mathrm{Hz}$
- Fat: $\gamma = 0.15\,\mathrm{Hz}$, $\Gamma = 0.31\,\mathrm{Hz}$

An example: the contrast optimization problem (2)

The Bloch equations

$$\begin{cases} \dot{y}_i &= -\Gamma_i y_i - u z_i \\ \dot{z}_i &= -\gamma_i(1 - z_i) + u y_i \end{cases}$$

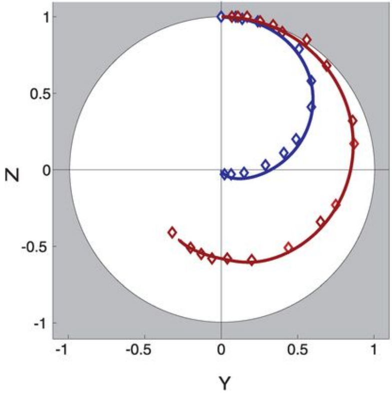
$(i = 1, 2)$

Saturation method

Find a path u so that after some time T:

- matter 1 saturated: $y_1(T) = z_1(T) = 0$
- matter 2 "maximized": $|(y_2(T), z_2(T))|$ maximal

Glaser's team, 2012 : method from Optimal Control Theory



An example: the contrast optimization problem (2)

The Bloch equations

$$\begin{cases} \dot{y}_i &= -\Gamma_i y_i - u z_i \\ \dot{z}_i &= -\gamma_i (1 - z_i) + u y_i \end{cases}$$

$(i = 1, 2)$

Saturation method

Find a path u so that after some time T:

- matter 1 saturated: $y_1(T) = z_1(T) = 0$
- matter 2 "maximized": $|(y_2(T), z_2(T))|$ maximal

Glaser's team, 2012 : method from Optimal Control Theory

Problem: analyze the behavior of the control through algebraic invariants

- Example: singular feedback control: $u = \dfrac{D'}{D}$ (D, D' polynomials in y, z, γ, Γ)
- Geometry of $\{D = 0\}$?
- Study of the singular points of $\{D = 0\}$ for each value of $\gamma_1, \Gamma_1, \gamma_2, \Gamma_2$
- Examples with water: Bonnard, Chyba, Jacquemard, Marriott, 2013
  - Water/Fat : 1 point
  - Water/Cerebrospinal fluid : 1 point

An example: the contrast optimization problem (2)

The Bloch equations

$$\begin{cases} \dot{y}_i & = -\Gamma_i y_i - u z_i \\ \dot{z}_i & = -\gamma_i (1 - z_i) + u y_i \end{cases}$$

$(i = 1, 2)$

Saturation method

Find a path u so that after some time T:

- matter 1 saturated: $y_1(T) = z_1(T) = 0$
- matter 2 "maximized": $|(y_2(T), z_2(T))|$ maximal

Glaser's team, 2012 : method from Optimal Control Theory

Problem: analyze the behavior of the control through algebraic invariants

- Example: singular feedback control: $u = \dfrac{D'}{D}$ (D, D' polynomials in y, z, γ, Γ)
- Geometry of $\{D = 0\}$?
- Study of the singular points of $\{D = 0\}$ for each value of $\gamma_1, \Gamma_1, \gamma_2, \Gamma_2$
- Examples with water: Bonnard, Chyba, Jacquemard, Marriott, 2013
  - Water/Fat : 1 point
  - Water/Cerebrospinal fluid : 1 point

Questions

- Is there always 1 singular point for pairs involving water?
- If not, how many possible families of parameters can we separate?

An example: the polynomial system

The D invariant: equation of a determinantal system

- 4 variables $(y_i, z_i,\ i = 1,2)$ and 4 parameters $(\gamma_i, \Gamma_i,\ i = 1,2)$
- $$M := \begin{pmatrix} -\Gamma_1 y_1 & -z_1 - 1 & -\Gamma_1 + (\gamma_1 - \Gamma_1) z_1 & (2\gamma_1 - 2\Gamma_1) y_1 \\ -\gamma_1 z_1 & y_1 & (\gamma_1 - \Gamma_1) y_1 & 2\Gamma_1 - \gamma_1 - (2\gamma_1 - 2\Gamma_1) z_1 \\ -\Gamma_2 y_2 & -z_2 - 1 & -\Gamma_2 + (\gamma_2 - \Gamma_2) z_2 & (2\gamma_2 - 2\Gamma_2) y_2 \\ -\gamma_2 z_2 & y_2 & (\gamma_2 - \Gamma_2) y_2 & 2\Gamma_2 - \gamma_2 - (2\gamma_2 - 2\Gamma_2) z_2 \end{pmatrix}$$
- $D :=$ determinant(M)
- $$\mathcal{V} := \left\{ D = \frac{\partial D}{\partial y_1} = \frac{\partial D}{\partial z_1} = \frac{\partial D}{\partial y_2} = \frac{\partial D}{\partial z_2} = 0 \right\}$$

Polynomial system with structure

- 5 equations of degree 8 in 4 variables and 4 parameters
- Homogeneous in γ, Γ, degree 4
- Roots of D = points where M has rank ≤ 3 : determinantal system
- $\mathcal{V}$ = singularities and critical points of the determinantal variety

Polynomial system solving

Applications:

- Control theory
- Cryptography
- Physics, industry...

Polynomial equations

$$f_1(\mathbf{X}) = \cdots = f_m(\mathbf{X}) = 0$$

- Numerical: give approximations of the solutions
  - Newton's method
  - Homotopy continuation method
- Symbolic: give exact solutions
  - Gröbner bases
  - Resultant method
  - Triangular sets
  - Geometric resolution

Examples of solutions:

- Find all the solutions if finite (dimension 0)
- Eliminate some variables (dimension > 0)
- ...

Difficult problem

- Exponential number of solutions
- NP-complete (at least on finite fields)

What is the goal for the contrast optimization example?

The D invariant: equation of a determinantal system

- 4 variables $(y_i, z_i,\ i = 1,2)$ and 4 parameters $(\gamma_i, \Gamma_i,\ i = 1,2)$
- $M := \begin{pmatrix} -\Gamma_1 y_1 & -z_1 - 1 & -\Gamma_1 + (\gamma_1 - \Gamma_1) z_1 & (2\gamma_1 - 2\Gamma_1) y_1 \\ -\gamma_1 z_1 & y_1 & (\gamma_1 - \Gamma_1) y_1 & 2\Gamma_1 - \gamma_1 - (2\gamma_1 - 2\Gamma_1) z_1 \\ -\Gamma_2 y_2 & -z_2 - 1 & -\Gamma_2 + (\gamma_2 - \Gamma_2) z_2 & (2\gamma_2 - 2\Gamma_2) y_2 \\ -\gamma_2 z_2 & y_2 & (\gamma_2 - \Gamma_2) y_2 & 2\Gamma_2 - \gamma_2 - (2\gamma_2 - 2\Gamma_2) z_2 \end{pmatrix}$
- $D := \text{determinant}(M)$
- $\mathcal{V} := \left\{ D = \dfrac{\partial D}{\partial y_1} = \dfrac{\partial D}{\partial z_1} = \dfrac{\partial D}{\partial y_2} = \dfrac{\partial D}{\partial z_2} = 0 \right\}$

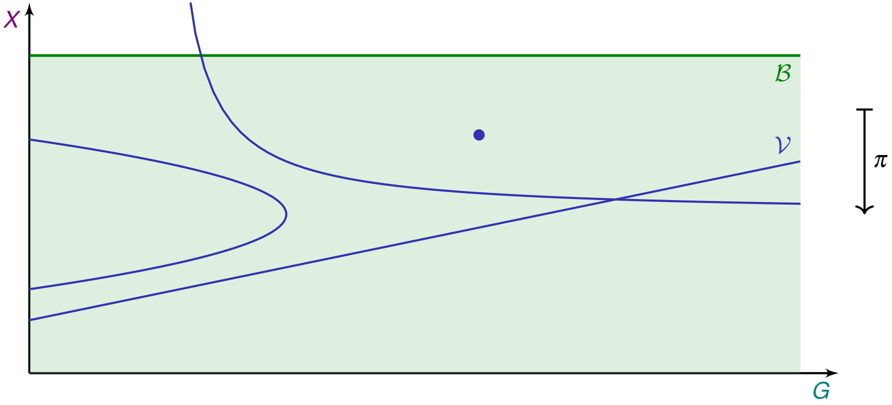
The Bloch ball: inequalities $\rightsquigarrow$ real semi-algebraic set

- $\mathcal{B} := \left\{ \begin{array}{l} {y_1}^2 + (z_1 + 1)^2 \leq 1 \\ {y_2}^2 + (z_2 + 1)^2 \leq 1 \end{array} \right\}$

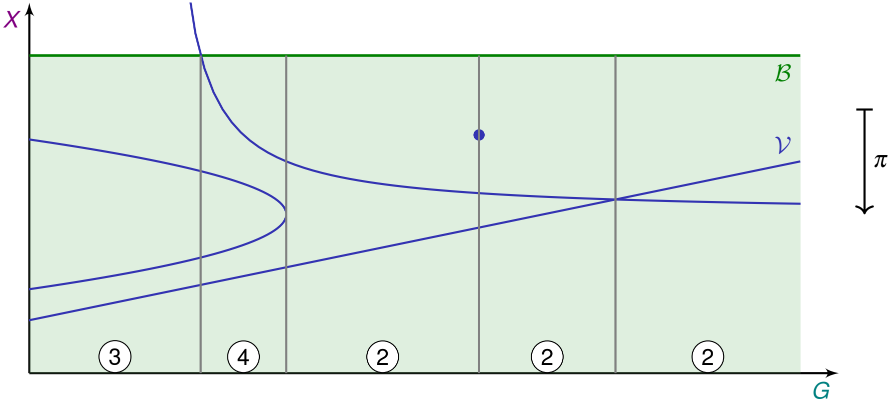
Goal

Classification of the real fibers of the projection of $\mathcal{V} \cap \mathcal{B}$ onto the parameter space

Real roots classification problem



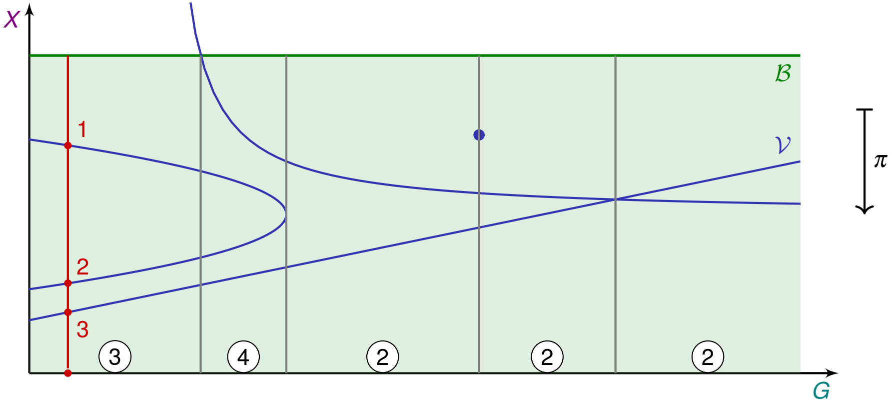
Real roots classification problem



Goal

Partition of the parameter space depending on the number of points of $\mathcal{V} \cap \mathcal{B}$ above

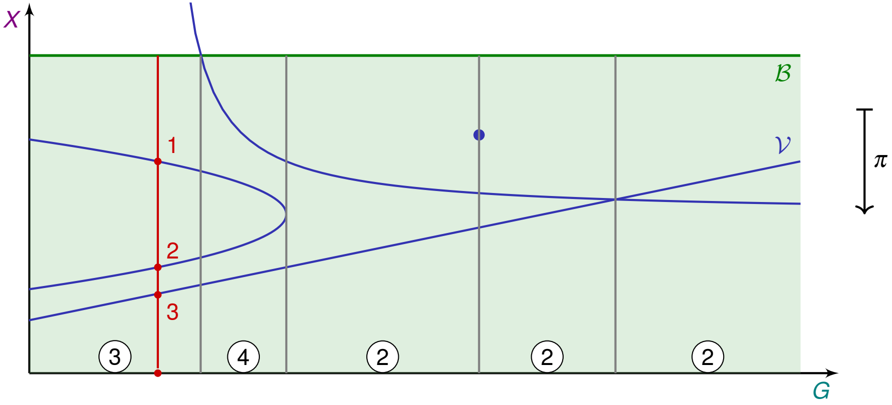
Real roots classification problem



Goal

Partition of the parameter space depending on the number of points of $\mathcal{V} \cap \mathcal{B}$ above

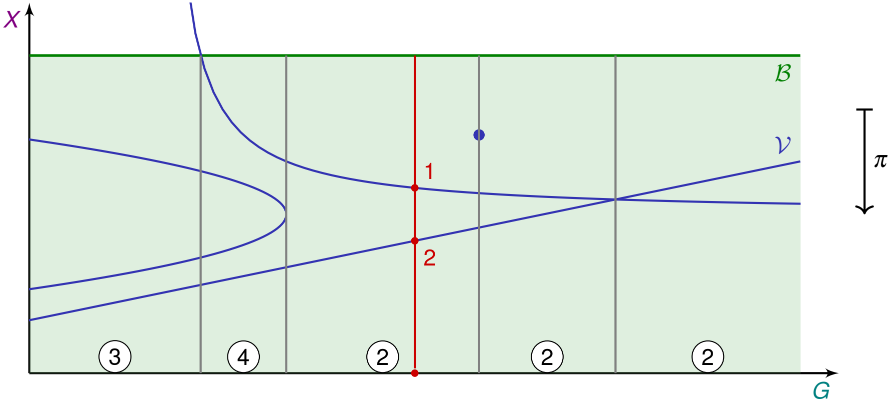
Real roots classification problem



Goal

Partition of the parameter space depending on the number of points of $\mathcal{V} \cap \mathcal{B}$ above

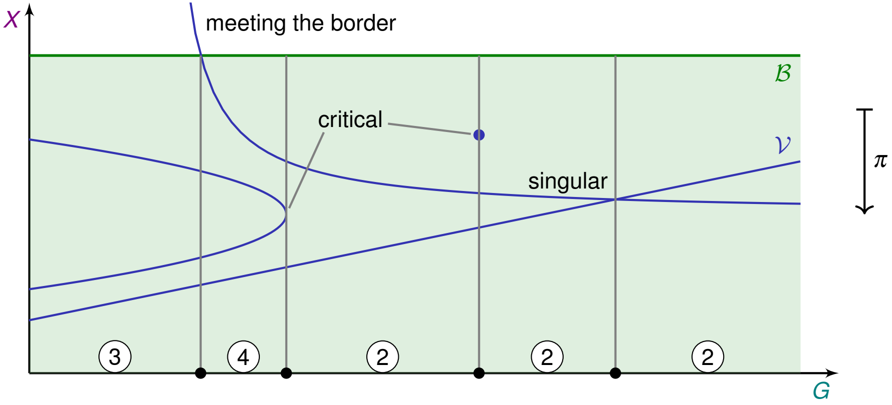
Real roots classification problem



Goal

Partition of the parameter space depending on the number of points of $\mathcal{V} \cap \mathcal{B}$ above

Real roots classification problem



Goal

Partition of the parameter space depending on the number of points of $\mathcal{V} \cap \mathcal{B}$ above

- Projections ($\Longleftrightarrow$ elimination)
- Critical and singular points

Algebraic regularity

How to compute singular and critical points?

- Definition depends on the dimension of irreducible components
- Can be characterized globally using the rank of a truncated Jacobian matrix for equidimensional varieties

Definition

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

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

Properties

- F regular $\iff$ $V(F)$ equidimensional with dimension $n-m$
- Regular sequences are generic (amongst systems of polynomials with given degrees)

Algebraic regularity

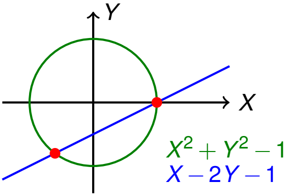
How to compute singular and critical points?

- Definition depends on the dimension of irreducible components
- Can be characterized globally using the rank of a truncated Jacobian matrix for equidimensional varieties

Definition

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

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



Properties

- F regular $\iff$ $V(F)$ equidimensional with dimension $n - m$
- Regular sequences are generic (amongst systems of polynomials with given degrees)

Regularity of the computations

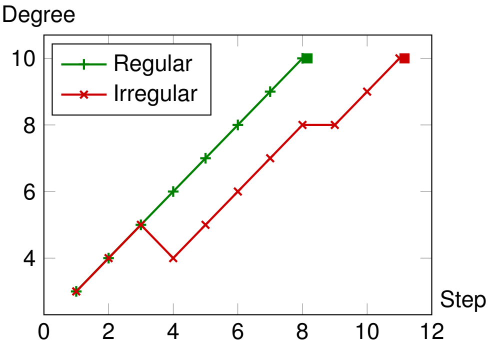
Gröbner basis algorithms (e.g. F_5)

- Compute a basis by iteratively building and reducing matrices of polynomials of same degree
- Normal strategy: perform lowest-degree reductions first
- Degree = indicator of progress

Regularity of the computations

Gröbner basis algorithms (e.g. F_5)

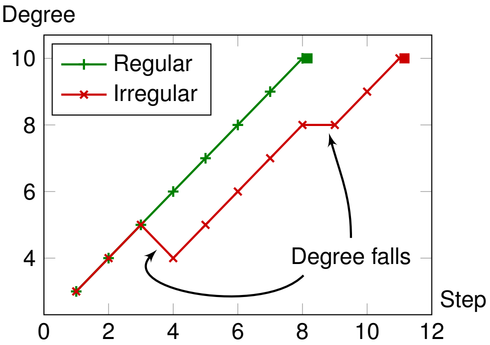
- Compute a basis by iteratively building and reducing matrices of polynomials of same degree
- Normal strategy: perform lowest-degree reductions first
- Degree = indicator of progress



Regularity of the computations

Gröbner basis algorithms (e.g. F_5)

- Compute a basis by iteratively building and reducing matrices of polynomials of same degree
- Normal strategy: perform lowest-degree reductions first
- Degree = indicator of progress



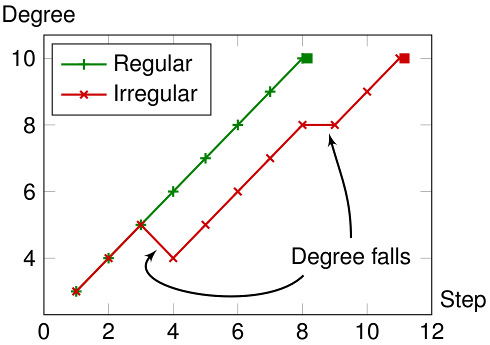
Degree fall?

- Definition: reduction resulting in a lower degree polynomial
- Example: $X\cdot(Y-1)-Y\cdot(X-1)=XY-YX+Y-X$
- Consequence: "next d" $< d+1$

Regularity of the computations

Gröbner basis algorithms (e.g. F_5)

- Compute a basis by iteratively building and reducing matrices of polynomials of same degree
- Normal strategy: perform lowest-degree reductions first
- Degree = indicator of progress

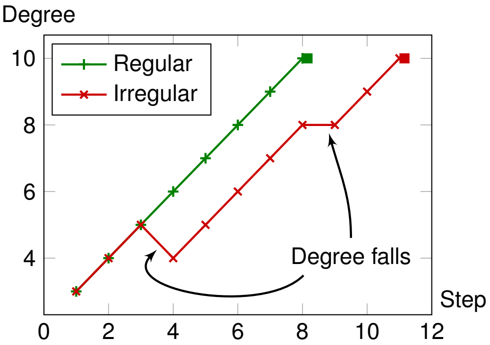


Regular sequences $\Longrightarrow$ algorithmic regularity!

- F_5-criterion: no reduction to zero in F_5 ($\Longleftrightarrow$ all matrices have full-rank)
- Degree falls $\Longleftrightarrow$ Reduction to zero of the highest degree components

$\rightsquigarrow$ Regularity in the affine sense = regularity of the highest degree components

Regularity of the computations



Gröbner basis algorithms (e.g. F_5)

- Compute a basis by iteratively building and reducing matrices of polynomials of same degree
- Normal strategy: perform lowest-degree reductions first
- Degree = indicator of progress

Regular sequences $\Longrightarrow$ algorithmic regularity!

- F_5-criterion: no reduction to zero in F_5 ($\iff$ all matrices have full-rank)
- Degree falls $\iff$ Reduction to zero of the highest degree components

$\rightsquigarrow$ Regularity in the affine sense = regularity of the highest degree components

This notion depends on the homogeneous structure!

Complexity for generic homogeneous systems if $n = m$

Homogeneous, generic (regular sequence),
with degree $(d_1, \dots, d_n)$

Initial system

F$_5$

Highest degree $d_{\max} \leq \sum_{i=1}^{n} (d_i - 1) + 1$ (Macaulay's bound)

Size of the matrix at degree d: $\binom{n+d-1}{d}$

$$\boxed{C_{F_5} = O\left(d_{\max} \binom{n + d_{\max} - 1}{d_{\max}}^3\right)}$$

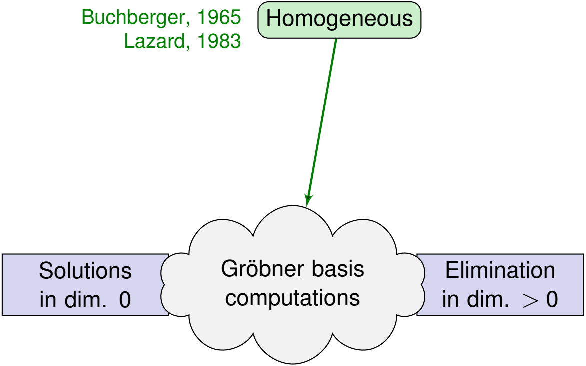
GREVLEX basis

FGLM

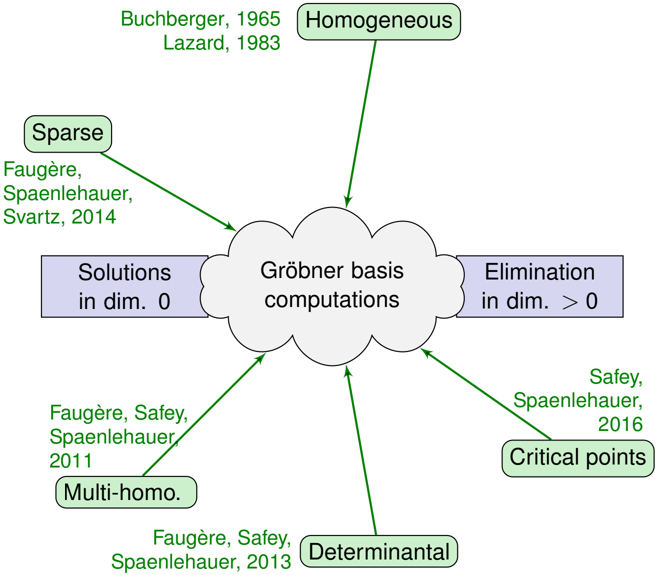
Number of solutions $= \prod_{i=1}^{n} d_i$ (Bézout's bound)

$$\boxed{C_{\mathrm{FGLM}} = O\left(n \left(\prod d_i\right)^3\right)}$$

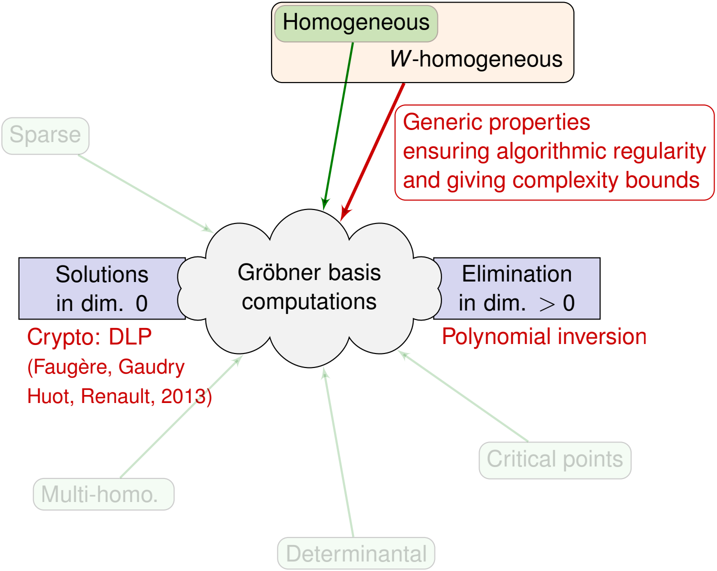
LEX basis



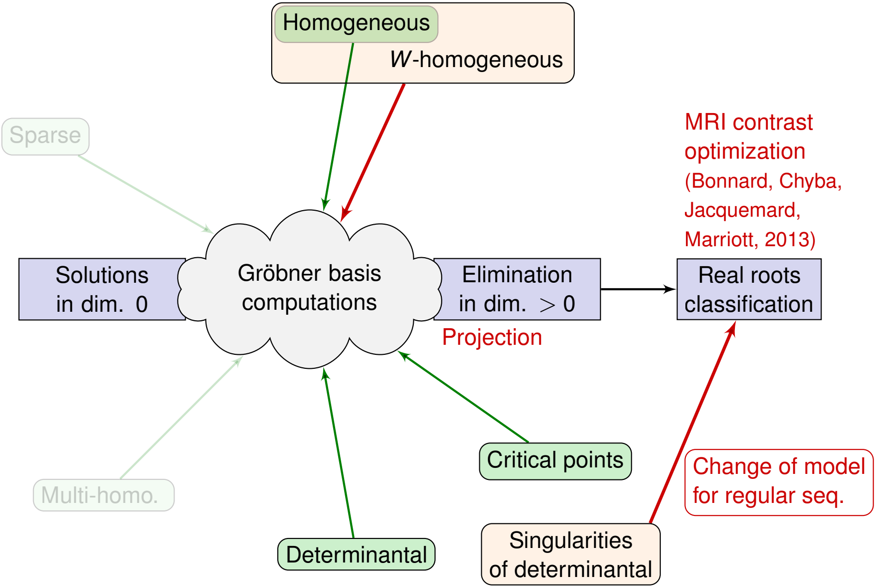
Buchberger, 1965
Lazard, 1983
Homogeneous
Solutions in dim. 0
Gröbner basis computations
Elimination in dim. > 0

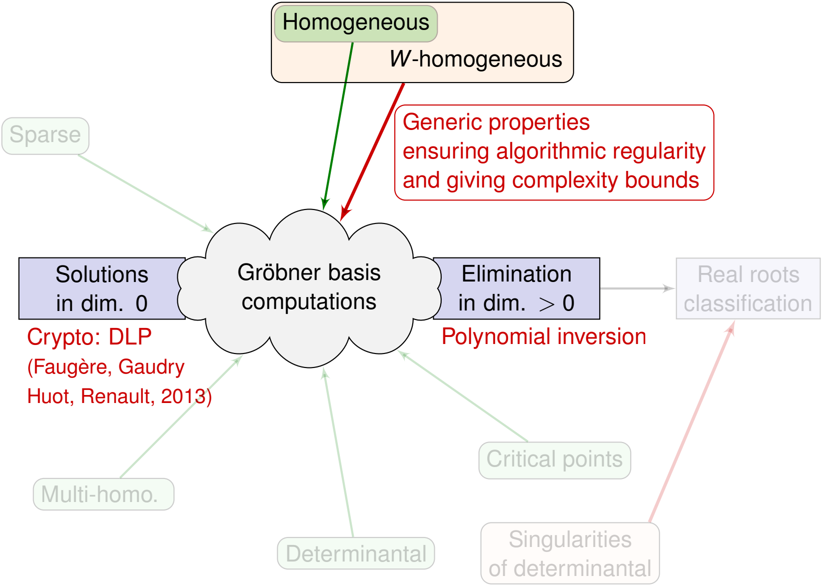

Buchberger, 1965
Lazard, 1983
Homogeneous
Sparse
Faugère, Spaenlehauer, Svartz, 2014
Solutions in dim. 0
Gröbner basis computations
Elimination in dim. > 0
Safey, Spaenlehauer, 2016
Critical points
Faugère, Safey, Spaenlehauer, 2011
Multi-homo.
Faugère, Safey, Spaenlehauer, 2013
Determinantal

Context and main results



Context and main results




Homogeneous
W-homogeneous
Generic properties
ensuring algorithmic regularity
and giving complexity bounds
Sparse
Solutions
in dim. 0
Gröbner basis
computations
Elimination
in dim. > 0
Real roots
classification
Crypto: DLP
(Faugère, Gaudry
Huot, Renault, 2013)
Polynomial inversion
Critical points
Multi-homo.
Determinantal
Singularities
of determinantal

Why the weights? An example (1)

Discrete Logarithm Problem on Edwards elliptic curves (Faugère, Gaudry, Huot, Renault 2013)

$$0 = \begin{bmatrix}41518\\33900\\8840\\22855\\29081\end{bmatrix} X_5^{16} + \begin{bmatrix}49874\\32136\\34252\\24932\\11782\end{bmatrix} X_1^8 + \begin{bmatrix}45709\\10698\\45336\\26076\\55993\end{bmatrix} X_1^7 X_2 + \begin{bmatrix}46659\\59796\\38267\\39647\\27683\end{bmatrix} X_1^6 X_2^2 + \begin{bmatrix}32367\\23164\\64111\\63692\\29095\end{bmatrix} X_1^5 X_2^3 + \begin{bmatrix}37627\\25182\\59951\\60422\\11080\end{bmatrix} X_1^4 X_2^4 +$$

$$\begin{bmatrix}27200\\38476\\28698\\5708\\47718\end{bmatrix} X_1^3 X_2^5 + \begin{bmatrix}64271\\43542\\57950\\52276\\9739\end{bmatrix} X_1^2 X_2^6 + \begin{bmatrix}49159\\11328\\33520\\65039\\27178\end{bmatrix} X_1 X_2^7 + \begin{bmatrix}59456\\49518\\46071\\49716\\33760\end{bmatrix} X_2^8 + \begin{bmatrix}17060\\60912\\64907\\61073\\37208\end{bmatrix} X_1^7 X_3 + \begin{bmatrix}55016\\15550\\19633\\28147\\25442\end{bmatrix} X_1^6 X_2 X_3 +$$

$$\begin{bmatrix}31264\\26817\\35757\\43106\\44133\end{bmatrix} X_1^5 X_2^2 X_3 + \begin{bmatrix}38258\\44188\\46688\\55434\\64632\end{bmatrix} X_1^4 X_2^3 X_3 + \begin{bmatrix}19475\\52270\\9282\\51171\\17150\end{bmatrix} X_1^3 X_2^4 X_3 + \begin{bmatrix}4467\\31828\\34222\\30753\\37662\end{bmatrix} X_1^2 X_2^5 X_3 + \text{2063 smaller monomials}$$

Goal: compute a Gröbner basis

Why the weights? An example (1)

Discrete Logarithm Problem on Edwards elliptic curves (Faugère, Gaudry, Huot, Renault 2013)

$$0 = \begin{bmatrix}41518\\33900\\8840\\22855\\29081\end{bmatrix} X_5^{16} + \begin{bmatrix}49874\\32136\\34252\\24932\\11782\end{bmatrix} X_1^8 + \begin{bmatrix}45709\\10698\\45336\\26076\\55993\end{bmatrix} X_1^7 X_2 + \begin{bmatrix}46659\\59796\\38267\\39647\\27683\end{bmatrix} X_1^6 X_2^2 + \begin{bmatrix}32367\\23164\\64111\\63692\\29095\end{bmatrix} X_1^5 X_2^3 + \begin{bmatrix}37627\\25182\\59951\\60422\\11080\end{bmatrix} X_1^4 X_2^4 +$$
$$\begin{bmatrix}27200\\38476\\28698\\5708\\47718\end{bmatrix} X_1^3 X_2^5 + \begin{bmatrix}64271\\43542\\57950\\52276\\9739\end{bmatrix} X_1^2 X_2^6 + \begin{bmatrix}49159\\11328\\33520\\65039\\27178\end{bmatrix} X_1 X_2^7 + \begin{bmatrix}59456\\49518\\46071\\49716\\33760\end{bmatrix} X_2^8 + \begin{bmatrix}17060\\60912\\64907\\61073\\37208\end{bmatrix} X_1^7 X_3 + \begin{bmatrix}55016\\15550\\19633\\28147\\25442\end{bmatrix} X_1^6 X_2 X_3 +$$
$$\begin{bmatrix}31264\\26817\\35757\\43106\\44133\end{bmatrix} X_1^5 X_2^2 X_3 + \begin{bmatrix}38258\\44188\\46688\\55434\\64632\end{bmatrix} X_1^4 X_2^3 X_3 + \begin{bmatrix}19475\\52270\\9282\\51171\\17150\end{bmatrix} X_1^3 X_2^4 X_3 + \begin{bmatrix}4467\\31828\\34222\\30753\\37662\end{bmatrix} X_1^2 X_2^5 X_3 + \text{2063 smaller monomials}$$

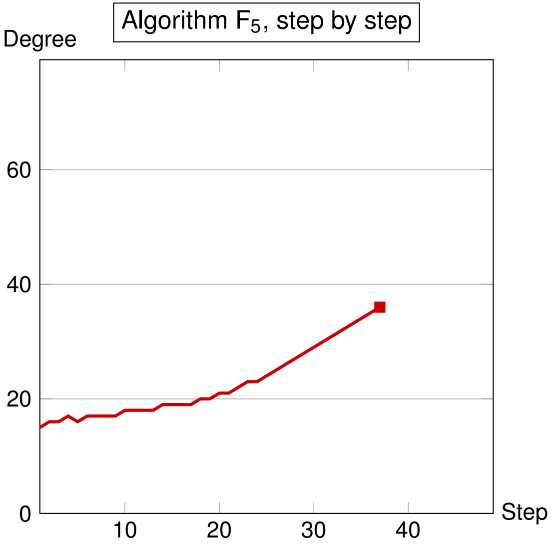
Goal: compute a Gröbner basis

Normal strategy (total degree):

- Difficult computation
- Non regular in the affine sense
- Non regular computation

Why the weights? An example (2)

Discrete Logarithm Problem on Edwards elliptic curves (Faugère, Gaudry, Huot, Renault 2013)



- Without weights:
  2 h (37 steps, $d_{\max} = 36$)
- With $W = (2, 2, 1, 1, 1)$:
  2 h (46 steps, $d_{\max} = 38$)
- With $W = (2, 2, 2, 2, 1)$:
  15 min (29 steps, $d_{\max} = 72$)

Why the weights? An example (3)

Discrete Logarithm Problem on Edwards elliptic curves (Faugère, Gaudry, Huot, Renault 2013)

$$0 = \begin{bmatrix} 41518 \\ 33900 \\ 8840 \\ 22855 \\ 29081 \end{bmatrix} X_5^{16} + \begin{bmatrix} 49874 \\ 32136 \\ 34252 \\ 24932 \\ 11782 \end{bmatrix} X_1^8 + \begin{bmatrix} 45709 \\ 10698 \\ 45336 \\ 26076 \\ 55993 \end{bmatrix} X_1^7 X_2 + \begin{bmatrix} 46659 \\ 59796 \\ 38267 \\ 39647 \\ 27683 \end{bmatrix} X_1^6 X_2^2 + \begin{bmatrix} 32367 \\ 23164 \\ 64111 \\ 63692 \\ 29095 \end{bmatrix} X_1^5 X_2^3 + \begin{bmatrix} 37627 \\ 25182 \\ 59951 \\ 60422 \\ 11080 \end{bmatrix} X_1^4 X_2^4 +$$

$$\begin{bmatrix} 27200 \\ 38476 \\ 28698 \\ 5708 \\ 47718 \end{bmatrix} X_1^3 X_2^5 + \begin{bmatrix} 64271 \\ 43542 \\ 57950 \\ 52276 \\ 9739 \end{bmatrix} X_1^2 X_2^6 + \begin{bmatrix} 49159 \\ 11328 \\ 33520 \\ 65039 \\ 27178 \end{bmatrix} X_1 X_2^7 + \begin{bmatrix} 59456 \\ 49518 \\ 46071 \\ 49716 \\ 33760 \end{bmatrix} X_2^8 + \begin{bmatrix} 17060 \\ 60912 \\ 64907 \\ 61073 \\ 37208 \end{bmatrix} X_1^7 X_3 + \begin{bmatrix} 55016 \\ 15550 \\ 19633 \\ 28147 \\ 25442 \end{bmatrix} X_1^6 X_2 X_3 +$$

$$\begin{bmatrix} 31264 \\ 26817 \\ 35757 \\ 43106 \\ 44133 \end{bmatrix} X_1^5 X_2^2 X_3 + \begin{bmatrix} 38258 \\ 44188 \\ 46688 \\ 55434 \\ 64632 \end{bmatrix} X_1^4 X_2^3 X_3 + \begin{bmatrix} 19475 \\ 52270 \\ 9282 \\ 51171 \\ 17150 \end{bmatrix} X_1^3 X_2^4 X_3 + \begin{bmatrix} 4467 \\ 31828 \\ 34222 \\ 30753 \\ 37662 \end{bmatrix} X_1^2 X_2^5 X_3 + \text{2063 smaller monomials}$$

Goal: compute a Gröbner basis

Normal strategy (total degree):

- Difficult computation
- Non regular in the affine sense
- Non regular computation

Alt. strategy: use weights

$=$ substitute $X_i \leftarrow X_i^{w_i}$ for $W = (w_1, \dots, w_5)$

What weights?

- $W = (1,1,1,1,1)$: nothing changed
- $W = (2,2,1,1,1)$: better...
- $W = (2,2,2,2,1)$: regular!

Why the weights? An example (3)

Discrete Logarithm Problem on Edwards elliptic curves (Faugère, Gaudry, Huot, Renault 2013)

$$0 = \begin{bmatrix}41518\\33900\\8840\\22855\\29081\end{bmatrix} X_5^{16} + \begin{bmatrix}49874\\32136\\34252\\24932\\11782\end{bmatrix} X_1^{8} + \begin{bmatrix}45709\\10698\\45336\\26076\\55993\end{bmatrix} X_1^{7}X_2 + \begin{bmatrix}46659\\59796\\38267\\39647\\27683\end{bmatrix} X_1^{6}X_2^{2} + \begin{bmatrix}32367\\23164\\64111\\63692\\29095\end{bmatrix} X_1^{5}X_2^{3} + \begin{bmatrix}37627\\25182\\59951\\60422\\11080\end{bmatrix} X_1^{4}X_2^{4} +$$

$$\begin{bmatrix}27200\\38476\\28698\\5708\\47718\end{bmatrix} X_1^{3}X_2^{5} + \begin{bmatrix}64271\\43542\\57950\\52276\\9739\end{bmatrix} X_1^{2}X_2^{6} + \begin{bmatrix}49159\\11328\\33520\\65039\\27178\end{bmatrix} X_1X_2^{7} + \begin{bmatrix}59456\\49518\\46071\\49716\\33760\end{bmatrix} X_2^{8} + \begin{bmatrix}17060\\60912\\64907\\61073\\37208\end{bmatrix} X_1^{7}X_3 + \begin{bmatrix}55016\\15550\\19633\\28147\\25442\end{bmatrix} X_1^{6}X_2X_3 +$$

$$\begin{bmatrix}31264\\26817\\35757\\43106\\44133\end{bmatrix} X_1^{5}X_2^{2}X_3 + \begin{bmatrix}38258\\44188\\46688\\55434\\64632\end{bmatrix} X_1^{4}X_2^{3}X_3 + \begin{bmatrix}19475\\52270\\9282\\51171\\17150\end{bmatrix} X_1^{3}X_2^{4}X_3 + \begin{bmatrix}4467\\31828\\34222\\30753\\37662\end{bmatrix} X_1^{2}X_2^{5}X_3 + \text{2063 smaller monomials}$$

Goal: compute a Gröbner basis

Normal strategy (total degree):

- Difficult computation
- Non regular in the affine sense
- Non regular computation

Alt. strategy: use weights

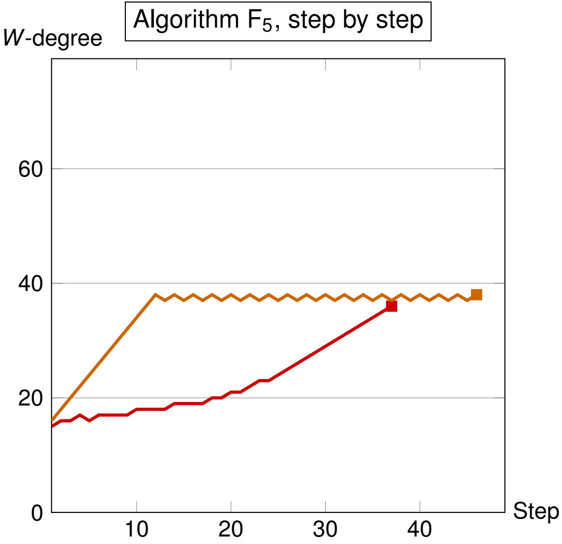
$=$ substitute $X_i \leftarrow X_i^{w_i}$ for $W = (w_1, \dots, w_5)$

What weights?

- $W = (1,1,1,1,1)$: nothing changed
- $W = (2,2,1,1,1)$: better...
- $W = (2,2,2,2,1)$: regular!

Why the weights? An example (4)

Discrete Logarithm Problem on Edwards elliptic curves (Faugère, Gaudry, Huot, Renault 2013)



- With $W = (1,1,1,1,1)$: 2 h (37 steps, $d_{\max} = 36$)
- With $W = (2,2,1,1,1)$: 2 h (46 steps, $d_{\max} = 38$)
- With $W = (2,2,2,2,1)$: 15 min (29 steps, $d_{\max} = 72$)

Why the weights? An example (5)

Discrete Logarithm Problem on Edwards elliptic curves (Faugère, Gaudry, Huot, Renault 2013)

$$0 = \begin{bmatrix}41518\\33900\\8840\\22855\\29081\end{bmatrix} X_5^{16} + \begin{bmatrix}49874\\32136\\34252\\24932\\11782\end{bmatrix} X_1^{8} + \begin{bmatrix}45709\\10698\\45336\\26076\\55993\end{bmatrix} X_1^{7}X_2 + \begin{bmatrix}46659\\59796\\38267\\39647\\27683\end{bmatrix} X_1^{6}X_2^{2} + \begin{bmatrix}32367\\23164\\64111\\63692\\29095\end{bmatrix} X_1^{5}X_2^{3} + \begin{bmatrix}37627\\25182\\59951\\60422\\11080\end{bmatrix} X_1^{4}X_2^{4} +$$

$$\begin{bmatrix}27200\\38476\\28698\\5708\\47718\end{bmatrix} X_1^{3}X_2^{5} + \begin{bmatrix}64271\\43542\\57950\\52276\\9739\end{bmatrix} X_1^{2}X_2^{6} + \begin{bmatrix}49159\\11328\\33520\\65039\\27178\end{bmatrix} X_1X_2^{7} + \begin{bmatrix}59456\\49518\\46071\\49716\\33760\end{bmatrix} X_2^{8} + \begin{bmatrix}17060\\60912\\64907\\61073\\37208\end{bmatrix} X_1^{7}X_3 + \begin{bmatrix}55016\\15550\\19633\\28147\\25442\end{bmatrix} X_1^{6}X_2X_3 +$$

$$\begin{bmatrix}31264\\26817\\35757\\43106\\44133\end{bmatrix} X_1^{5}X_2^{2}X_3 + \begin{bmatrix}38258\\44188\\46688\\55434\\64632\end{bmatrix} X_1^{4}X_2^{3}X_3 + \begin{bmatrix}19475\\52270\\9282\\51171\\17150\end{bmatrix} X_1^{3}X_2^{4}X_3 + \begin{bmatrix}4467\\31828\\34222\\30753\\37662\end{bmatrix} X_1^{2}X_2^{5}X_3 + \text{2063 smaller monomials}$$

Goal: compute a Gröbner basis

Normal strategy (total degree):

- Difficult computation
- Non regular in the affine sense
- Non regular computation

Alt. strategy: use weights

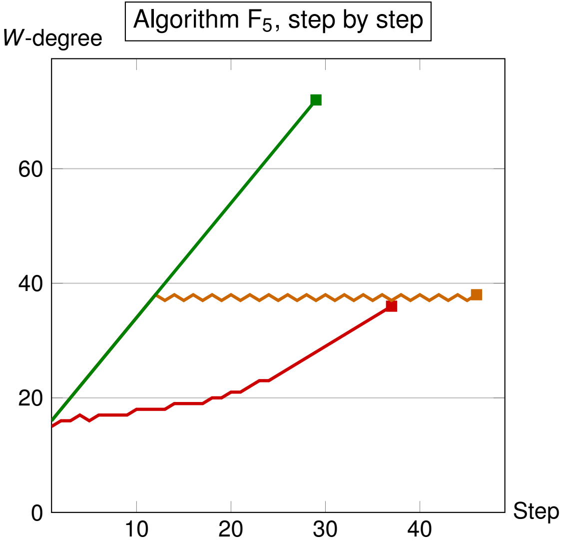
$=$ substitute $X_i \leftarrow X_i^{w_i}$ for $W = (w_1, \ldots, w_5)$

What weights?

- $W = (1,1,1,1,1)$: nothing changed
- $W = (2,2,1,1,1)$: better...
- $W = (2,2,2,2,1)$: regular!

Why the weights? An example (6)

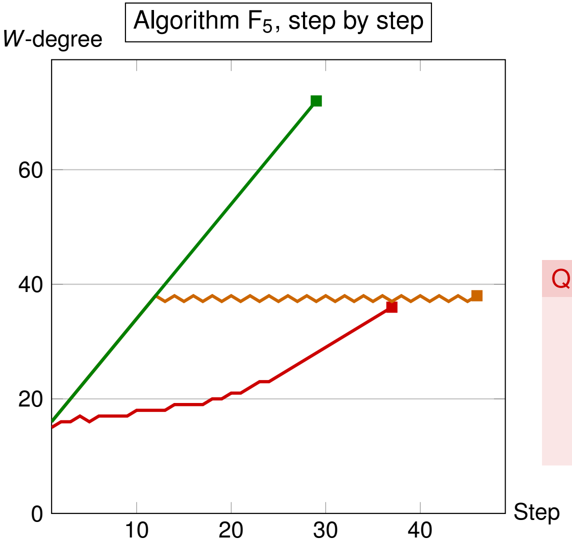
Discrete Logarithm Problem on Edwards elliptic curves (Faugère, Gaudry, Huot, Renault 2013)



- With $W = (1, 1, 1, 1, 1)$:
  2 h (37 steps, $d_{\max} = 36$)
- With $W = (2, 2, 1, 1, 1)$:
  2 h (46 steps, $d_{\max} = 38$)
- With $W = (2, 2, 2, 2, 1)$:
  15 min (29 steps, $d_{\max} = 72$)

Why the weights? An example (6)

Discrete Logarithm Problem on Edwards elliptic curves (Faugère, Gaudry, Huot, Renault 2013)



- With $W = (1, 1, 1, 1, 1)$:
  2 h (37 steps, $d_{\max} = 36$)
- With $W = (2, 2, 1, 1, 1)$:
  2 h (46 steps, $d_{\max} = 38$)
- With $W = (2, 2, 2, 2, 1)$:
  15 min (29 steps, $d_{\max} = 72$)

Questions

- Explain the regularity?
- Complexity bounds?
- Why does FGLM become a bottleneck?

Weighted homogeneous systems: definition

Definition (e.g. [Robbiano 1986], [Becker and Weispfenning 1993])

System of weights: $W = (w_1, \ldots, w_n) \in \mathbb{N}^n$

Weighted degree (or W-degree): $\deg_W(X_1^{\alpha_1} \ldots X_n^{\alpha_n}) = \sum_{i=1}^{n} w_i \alpha_i$

Weighted homogeneous polynomial: poly. containing only monomials of same W-degree

→ Example: physical equations: $\underset{\text{Weight 3}}{\text{Volume}} = \underset{\text{Weight 2}}{\text{Area}} \times \underset{\text{Weight 1}}{\text{Height}}$

Given a general (non-weighted-homogeneous) system and a system of weights

Computational strategy: weighted-homogenize it as in the homogeneous case

Complexity estimates: consider the highest W-degree components of the system

- Enough to study weighted homogeneous systems

Weighted homogeneous systems: definition

Definition (e.g. [Robbiano 1986], [Becker and Weispfenning 1993])

System of weights: $W = (w_1, \dots, w_n) \in \mathbb{N}^n$

Weighted degree (or W-degree): $\deg_W(X_1^{\alpha_1} \dots X_n^{\alpha_n}) = \sum_{i=1}^n w_i \alpha_i$

Weighted homogeneous polynomial: poly. containing only monomials of same W-degree

$\rightarrow$ Example: physical equations: $\underset{\text{Weight 3}}{\underset{\uparrow}{\text{Volume}}} = \underset{\text{Weight 2}}{\underset{\uparrow}{\text{Area}}} \times \underset{\text{Weight 1}}{\underset{\uparrow}{\text{Height}}}$

Given a general (non-weighted-homogeneous) system and a system of weights

Computational strategy: weighted-homogenize it as in the homogeneous case

Complexity estimates: consider the highest W-degree components of the system

- Enough to study weighted homogeneous systems

Strategy and complexity for W-homogeneous systems

$$W = (w_1, \ldots, w_n)$$

$F(X_1, \ldots, X_n)$ ← W-homogeneous, generic (simultaneous Noether position), with W-degree $(d_1, \ldots, d_n)$

$\downarrow$

$F(X_1^{w_1}, \ldots, X_n^{w_n})$ ← Homogeneous, in SNP ($\Longrightarrow$ regular), with total degree $(d_1, \ldots, d_n)$

$\downarrow$

F_5 ←

Highest W-degree

$$\leq \sum_{i=1}^{n}(d_i - 1) + 1 - \sum_{i=1}^{n}(w_i - 1) + w_n - 1$$

$$\leq \sum_{i=1}^{n}(d_i - w_i) + w_n$$

Size of the matrix at W-degree $d \simeq \frac{1}{\prod_{i=1}^{n} w_i}\binom{n+d-1}{d}$

$\downarrow$

W-GRevLex basis

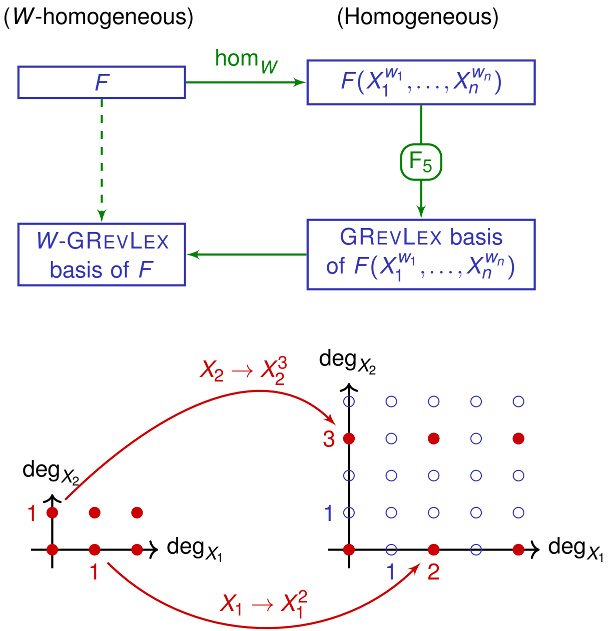
$\downarrow$

FGLM ← Number of solutions $= \frac{\prod_{i=1}^{n} d_i}{\prod_{i=1}^{n} w_i}$ (weighted Bézout bound)

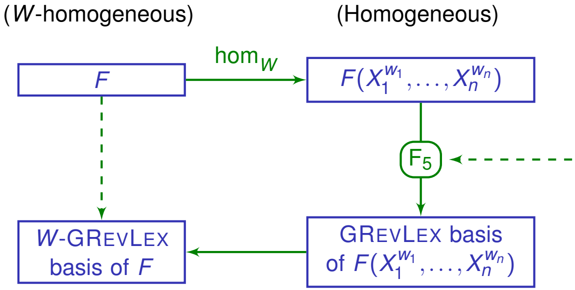
$\downarrow$

Lex basis

Why is the strategy correct?



Why is the strategy correct?

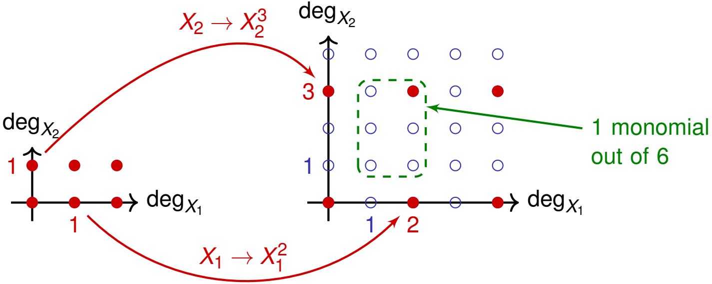


Reduces matrices of monomials degree by degree

→ Size of the matrices $\simeq$ divided by $\prod w_i$

→ Regular computations ?

→ Max W-degree $d_{\max}$?



Regularity: homogeneous vs W-homogeneous

Properties of regular sequences

	Homogeneous	W-homogeneous
F_5 Criterion?	Yes	Yes
Generic?	Yes	If $\neq \varnothing$
Bézout's bound	$\deg(\langle F \rangle) = \prod_{i=1}^{n} d_i$	$\deg(\langle F \rangle) = \frac{\prod_{i=1}^{n} d_i}{\prod_{i=1}^{n} w_i}$
Macaulay's bound	$d_{\max} \leq \sum_{i=1}^{n} (d_i - 1) + 1$	$d_{\max} \leq \sum_{i=1}^{n} (d_i - w_i) + \max\{w_j\}$
Macaulay's bound reached?	Yes	Not always

Macaulay's bound requires to know how each variable participates in the computations

Simultaneous Noether position

- "$f_1, \ldots, f_i$ depend on $X_1, \ldots, X_i$" for all i
- SNP is "as generic as possible" too
- Weighted Macaulay's bound if in SNP: $d_{\max} \leq \sum_{i=1}^{n} (d_i - w_i) + w_n$

Regularity: homogeneous vs W-homogeneous

Properties of regular sequences

	Homogeneous	W-homogeneous
F_5 Criterion?	Yes	Yes
Generic?	Yes	If $\neq \varnothing$
Bézout's bound	$\deg(\langle F \rangle) = \prod_{i=1}^{n} d_i$	$\deg(\langle F \rangle) = \frac{\prod_{i=1}^{n} d_i}{\prod_{i=1}^{n} w_i}$
Macaulay's bound	$d_{\max} \leq \sum_{i=1}^{n} (d_i - 1) + 1$	$d_{\max} \leq \sum_{i=1}^{n} (d_i - w_i) + \max\{w_j\}$
Macaulay's bound reached?	Yes	Not always

Macaulay's bound requires to know how each variable participates in the computations

Simultaneous Noether position

- "$f_1, \ldots, f_i$ depend on $X_1, \ldots, X_i$" for all i
- SNP is "as generic as possible" too
- Weighted Macaulay's bound if in SNP: $d_{\max} \leq \sum_{i=1}^{n} (d_i - w_i) + w_n$

Regularity: homogeneous vs W-homogeneous

Properties of regular sequences

	Homogeneous	W-homogeneous
F_5 Criterion?	Yes	Yes
Generic?	Yes	If $\neq \varnothing$
Bézout's bound	$\deg(\langle F \rangle) = \prod_{i=1}^{n} d_i$	$\deg(\langle F \rangle) = \frac{\prod_{i=1}^{n} d_i}{\prod_{i=1}^{n} w_i}$
Macaulay's bound	$d_{\max} \leq \sum_{i=1}^{n} (d_i - 1) + 1$	$d_{\max} \leq \sum_{i=1}^{n} (d_i - w_i) + \max\{w_j\}$
Macaulay's bound reached?	Yes	Not always

Macaulay's bound requires to know how each variable participates in the computations

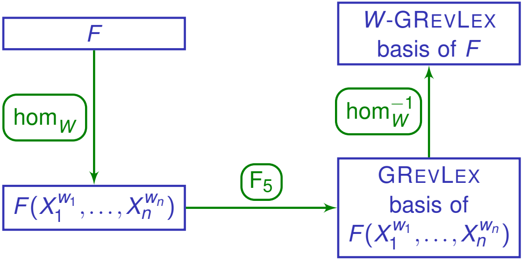
Simultaneous Noether position

- "$f_1, \dots, f_i$ depend on $X_1, \dots, X_i$" for all i
- SNP is "as generic as possible" too
- Weighted Macaulay's bound if in SNP: $d_{\max} \leq \sum_{i=1}^{n} (d_i - w_i) + w_n$

What about FGLM?

Two-step strategy for 0-dimensional systems

- F_5 algorithm on the homogenized system
- FGLM algorithm on the weighted homogeneous system

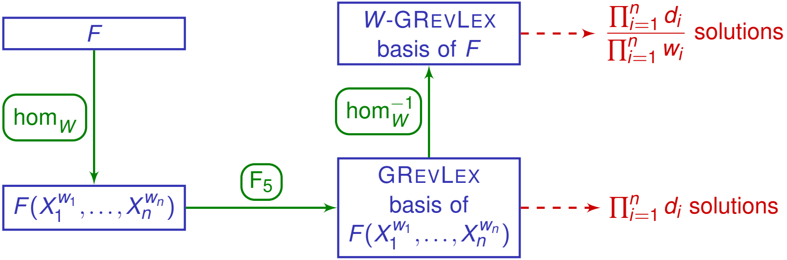


$$\boxed{O\left(\frac{d_{\max}}{(\prod w_i)^3}\binom{n+d_{\max}-1}{d_{\max}}^3\right)}$$

What about FGLM?

Two-step strategy for 0-dimensional systems

- F_5 algorithm on the homogenized system
- FGLM algorithm on the weighted homogeneous system

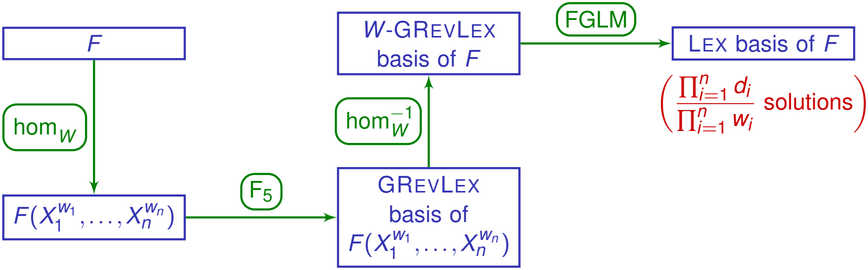


$$\boxed{O\left(\frac{d_{\max}}{(\prod w_i)^3}\binom{n+d_{\max}-1}{d_{\max}}^3\right)}$$

What about FGLM?

Two-step strategy for 0-dimensional systems

- F_5 algorithm on the homogenized system
- FGLM algorithm on the weighted homogeneous system

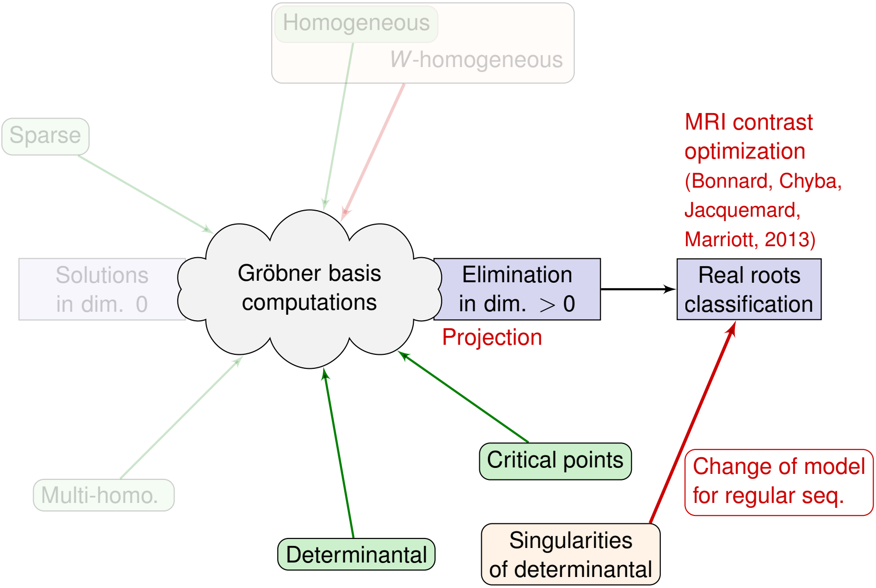


$$\boxed{O\left(\frac{d_{\max}}{(\prod w_i)^3}\binom{n+d_{\max}-1}{d_{\max}}^3\right)} \qquad \boxed{O\left(n\left(\frac{\prod d_i}{\prod w_i}\right)^3\right)}$$

Benchmarks

System	Normal (s)	Weighted (s)	Speed-up
DLP Edwards $n = 5$, GREVLEX (F_5, FGb)	6461.2	935.4	6.9
DLP Edwards $n = 5$, GREVLEX (F_4, Magma)	56 195.0	6044.0	9.3
Invariant relations, Cyclic $n = 5$, GREVLEX (F_4, Magma)	$>$75 000	392.7	$>$191
Monomial relations, $n = 26$, $m = 52$, GREVLEX (F_4, Magma)	14 630.6	0.2	73 153
DLP Edwards $n = 5$, LEX (Sparse-FGLM, FGb)	6835.6	2164.4	3.2
Invariant relations, Cyclic $n = 5$, ELIM (F_4, Magma)	NA	382.5	NA
Monomial relations, $n = 26$, $m = 52$, ELIM (F_4, Magma)	17 599.5	8054.2	2.2

Singularities of determinantal systems



The D invariant: equation of a determinantal system

- 4 variables $(y_i, z_i,\ i=1,2)$ and 4 parameters $(\gamma_i, \Gamma_i,\ i=1,2)$
- $$M := \begin{pmatrix} -\Gamma_1 y_1 & -z_1 - 1 & -\Gamma_1 + (\gamma_1 - \Gamma_1) z_1 & (2\gamma_1 - 2\Gamma_1) y_1 \\ -\gamma_1 z_1 & y_1 & (\gamma_1 - \Gamma_1) y_1 & 2\Gamma_1 - \gamma_1 - (2\gamma_1 - 2\Gamma_1) z_1 \\ -\Gamma_2 y_2 & -z_2 - 1 & -\Gamma_2 + (\gamma_2 - \Gamma_2) z_2 & (2\gamma_2 - 2\Gamma_2) y_2 \\ -\gamma_2 z_2 & y_2 & (\gamma_2 - \Gamma_2) y_2 & 2\Gamma_2 - \gamma_2 - (2\gamma_2 - 2\Gamma_2) z_2 \end{pmatrix}$$
- $D := \mathrm{determinant}(M)$
- $$\mathcal{V} := \left\{ D = \frac{\partial D}{\partial y_1} = \frac{\partial D}{\partial z_1} = \frac{\partial D}{\partial y_2} = \frac{\partial D}{\partial z_2} = 0 \right\}$$

The Bloch ball: inequalities $\rightsquigarrow$ real semi-algebraic set

- $$\mathcal{B} := \left\{ \begin{array}{l} {y_1}^2 + (z_1+1)^2 \leq 1 \\ {y_2}^2 + (z_2+1)^2 \leq 1 \end{array} \right\}$$

Goal

Classification of the real fibers of the projection of $\mathcal{V} \cap \mathcal{B}$ onto the parameter space

State of the art and contributions

State of the art:

- General tool: Cylindrical Algebraic Decomposition
  Collins, 1975
- Specific tools for roots classification
  Yang, Hou, Xia, 2001
  Lazard, Rouillier, 2007

State of the art and contributions

State of the art:

- General tool: Cylindrical Algebraic Decomposition
  Collins, 1975
- Specific tools for roots classification
  Yang, Hou, Xia, 2001
  Lazard, Rouillier, 2007

Problem

- None of these algorithms can solve the problem efficiently:
  - 1050 s in the case of water ($\gamma_1 = \Gamma_1 = 1 \to 2$ parameters)
  - > 24 h in the general case (3 parameters)
- Can we exploit the determinantal structure to go further?

State of the art and contributions

State of the art:

- General tool: Cylindrical Algebraic Decomposition
  Collins, 1975
- Specific tools for roots classification
  Yang, Hou, Xia, 2001
  Lazard, Rouillier, 2007

Problem

- None of these algorithms can solve the problem efficiently:
  - 1050 s in the case of water ($\gamma_1 = \Gamma_1 = 1 \to 2$ parameters)
  - > 24 h in the general case (3 parameters)
- Can we exploit the determinantal structure to go further?

Main results

- Dedicated strategy for real roots classification for determinantal systems
- Can use existing tools for elimination
- Main refinements:
  - Rank stratification
  - Incidence varieties

State of the art and contributions

State of the art:

- General tool: Cylindrical Algebraic Decomposition
  Collins, 1975
- Specific tools for roots classification
  Yang, Hou, Xia, 2001
  Lazard, Rouillier, 2007

Problem

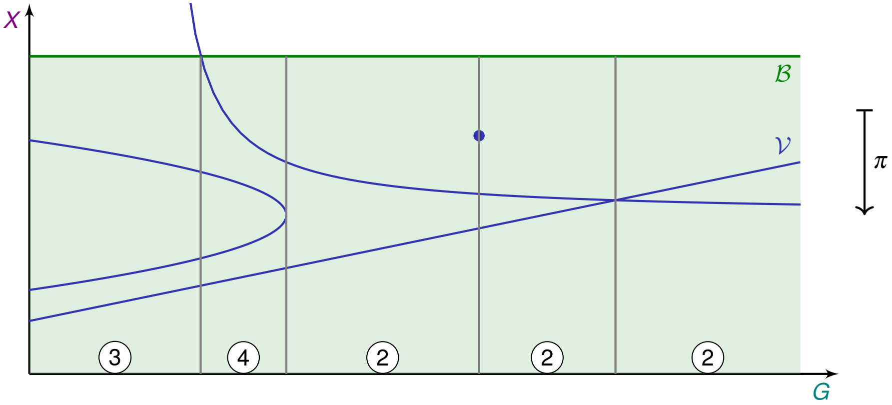
- None of these algorithms can solve the problem efficiently:
  - 1050 s in the case of water ($\gamma_1 = \Gamma_1 = 1 \to 2$ parameters)
  - $>$ 24 h in the general case (3 parameters)
- Can we exploit the determinantal structure to go further?

Main results

- Dedicated strategy for real roots classification for determinantal systems
- Can use existing tools for elimination
- Main refinements:
  - Rank stratification
  - Incidence varieties

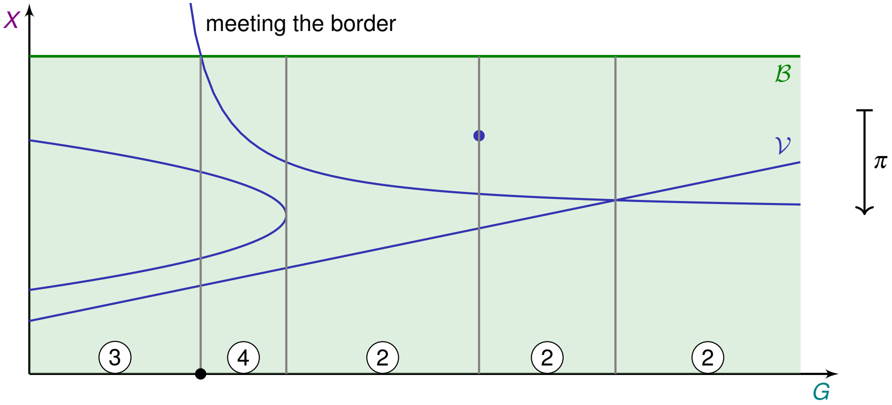
- Faster than general algorithms:
  - 10 s in the case of water
  - 4 h in the general case
- Results for the application
  - Full classification
  - Answers to the experimental questions for water: there can be 1, 2 or 3 singularities

Classification strategy



In our case, the only points where the number of roots may change are projections of:

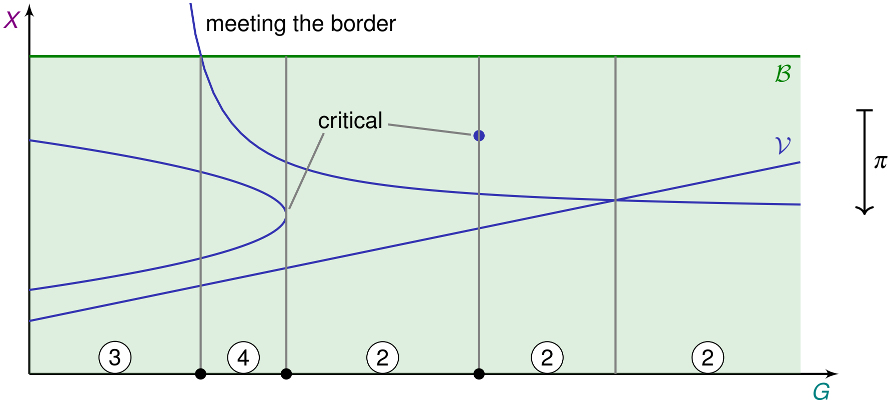
Classification strategy



In our case, the only points where the number of roots may change are projections of:

- points where $\mathcal{V}$ meets the border of the semi-algebraic domain

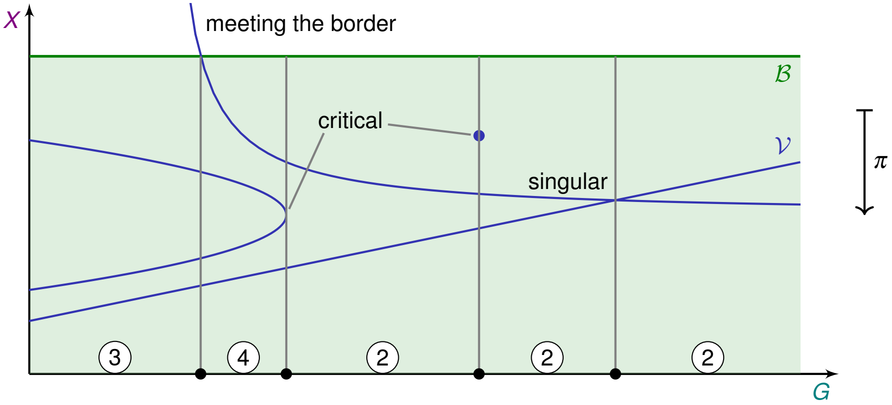
Classification strategy



In our case, the only points where the number of roots may change are projections of:

- points where $\mathcal{V}$ meets the border of the semi-algebraic domain
- critical points of π restricted to $\mathcal{V}$

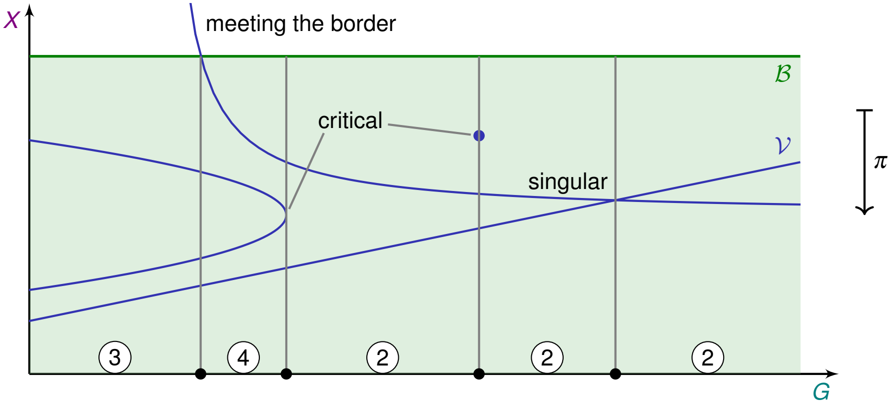
Classification strategy



In our case, the only points where the number of roots may change are projections of:

- points where $\mathcal{V}$ meets the border of the semi-algebraic domain
- critical points of π restricted to $\mathcal{V}$
- singular points of $\mathcal{V}$

Classification strategy



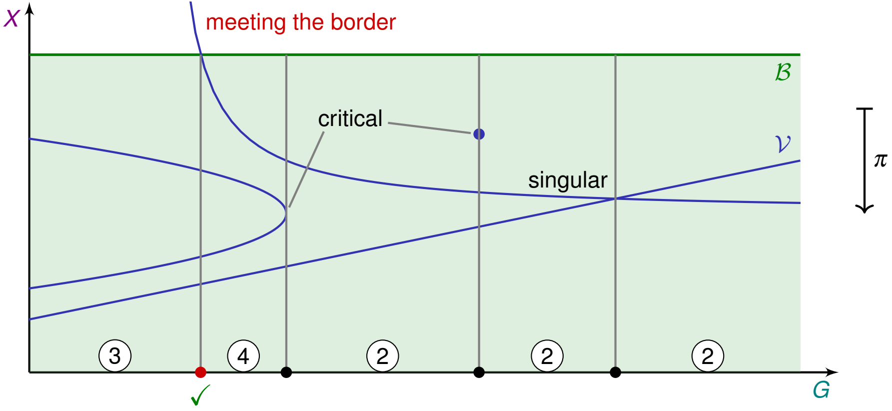
In our case, the only points where the number of roots may change are projections of:

- points where $\mathcal{V}$ meets the border of the semi-algebraic domain
- critical points of π restricted to $\mathcal{V}$
- singular points of $\mathcal{V}$

$\Big\} =: K(\pi, \mathcal{V})$

We want to compute $P \in \mathbb{Q}[G]$ with $P \neq 0$ and P vanishing at all these points

Classification strategy

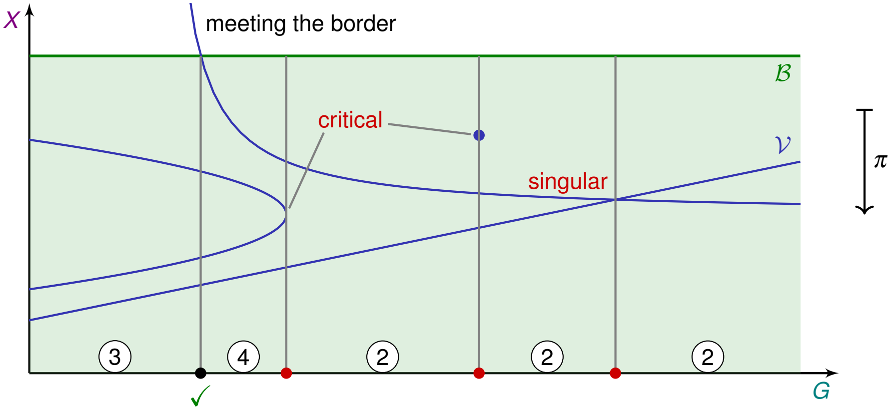


Intersection with the border

For each inequality $f > 0$ defining $\mathcal{B}$

1. Add $f = 0$ to the equations of $\mathcal{V}$
2. Compute the image of the variety through π (eliminate **X**)

Classification strategy



Critical and singular points

$$(\mathbf{X},\mathbf{G}) \in K(\pi,\mathcal{V}) \iff \mathrm{Jac}(F,\mathbf{X}) \text{ has rank } < d$$

Requirements

- F generates the ideal of $\mathcal{V}$ $\implies$ radical
- $\mathcal{V}$ is equidimensional with codimension d

Can we find a regular sequence for F?

Determinantal systems

- $A = k \times k$-matrix filled with polynomials in n variables **X** and t parameters **G**
- $1 \leq r < k$ target rank
- Determinantal variety: $V_{\leq r}(A) = \{(\mathbf{x}, \mathbf{g}) : \operatorname{rank}(A(\mathbf{x}, \mathbf{g})) \leq r\}$

Our system: $n = 4$, $k = 4$, $r = 3$, $\mathcal{V} = K(\pi, V_{\leq r}(M))$

Properties of determinantal systems

Determinantal systems

- $A =$ $k \times k$-matrix filled with polynomials in n variables $\mathbf{X}$ and t parameters $\mathbf{G}$
- $1 \leq r < k$ target rank
- Determinantal variety: $V_{\leq r}(A) = \{(\mathbf{x}, \mathbf{g}) : \mathrm{rank}(A(\mathbf{x}, \mathbf{g})) \leq r\}$

Our system: $n = 4$, $k = 4$, $r = 3$, $\mathcal{V} = K(\pi, V_{\leq r}(M))$

For a generic matrix A with the same parameters

- $V_{\leq r}(A)$ equidimensional with codimension $(k - r)^2$
- $\mathrm{Sing}(V_{\leq r}(A)) = V_{\leq r-1}(A)$, t-equidimensional
- $\mathrm{Crit}(\pi, V_{\leq r}(A))$ has dimension $< t$
- Natural stratification : $K(\pi, V_{\leq r}(A)) = \mathrm{Sing}(V_{\leq r}(A)) \cup \mathrm{Crit}(\pi, V_{\leq r}(A))$

Properties of determinantal systems

Determinantal systems

- $A = k \times k$-matrix filled with polynomials in n variables $\mathbf{X}$ and t parameters $\mathbf{G}$
- $1 \leq r < k$ target rank
- Determinantal variety: $V_{\leq r}(A) = \{(\mathbf{x}, \mathbf{g}) : \mathrm{rank}(A(\mathbf{x}, \mathbf{g})) \leq r\}$

Our system: $n = 4$, $k = 4$, $r = 3$, $\mathcal{V} = K(\pi, V_{\leq r}(M))$

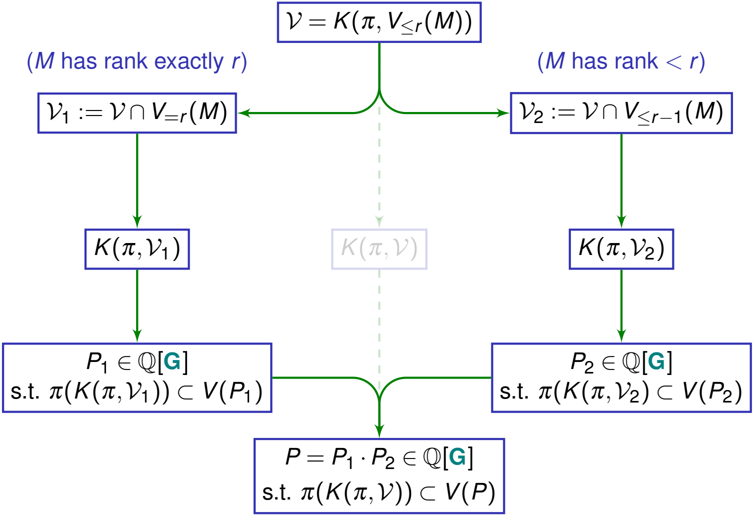
For our specific matrix M

- $V_{\leq r-1}(M) \subset \mathcal{V}$ (always true)
- $V_{\leq r-1}(M)$ is equidimensional with dimension t
- $\mathcal{V} \setminus V_{\leq r-1}(M)$ has dimension $< t$
- Rank stratification : $\mathcal{V} = (\mathcal{V} \cap V_{\leq r-1}(M)) \cup (\mathcal{V} \setminus V_{\leq r-1}(M))$

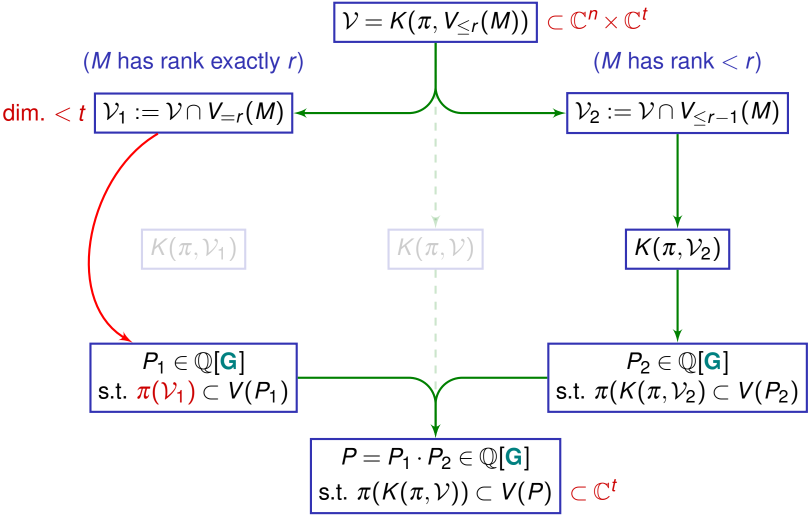
Rank stratification

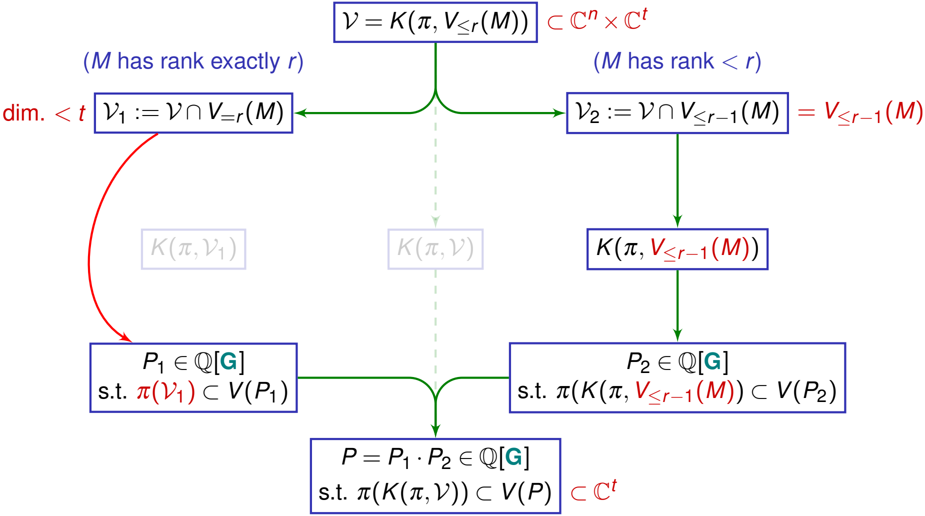
$$\begin{tikzcd} \boxed{\mathcal{V} = K(\pi, V_{\leq r}(M))} \arrow[d, dashed] \\ \boxed{K(\pi,\mathcal{V})} \arrow[d, dashed] \\ \boxed{\begin{array}{c} P \in \mathbb{Q}[\mathbf{G}] \\ \text{s.t. } \pi(K(\pi,\mathcal{V})) \subset V(P) \end{array}} \end{tikzcd}$$

Rank stratification



Rank stratification




$\mathcal{V} = K(\pi, V_{\leq r}(M))$ $\subset \mathbb{C}^n \times \mathbb{C}^t$
(M has rank exactly r)
(M has rank $< r$)
dim. $< t$
$\mathcal{V}_1 := \mathcal{V} \cap V_{=r}(M)$
$\mathcal{V}_2 := \mathcal{V} \cap V_{\leq r-1}(M)$ $= V_{\leq r-1}(M)$
$K(\pi, \mathcal{V}_1)$
$K(\pi, \mathcal{V})$
$K(\pi, V_{\leq r-1}(M))$
$P_1 \in \mathbb{Q}[\mathbf{G}]$ s.t. $\pi(\mathcal{V}_1) \subset V(P_1)$
$P_2 \in \mathbb{Q}[\mathbf{G}]$ s.t. $\pi(K(\pi, V_{\leq r-1}(M)) \subset V(P_2)$
$P = P_1 \cdot P_2 \in \mathbb{Q}[\mathbf{G}]$ s.t. $\pi(K(\pi, \mathcal{V})) \subset V(P)$ $\subset \mathbb{C}^t$

Change of model: incidence varieties

Reminder: $k =$ size of the matrix; $r =$ target rank

Possible modelizations for determinantal varieties

- Minors: $\operatorname{rank}(A) \leq r \iff$ all $r+1$-minors of A are 0
- Incidence system: $\operatorname{rank}(A) \leq r \iff \exists L, A \cdot L = 0$ and $\operatorname{rank}(L) = k - r$

Minors:

- $\binom{k}{r+1}^2$ equations
- Codimension $(k-r)^2$

Incidence system:

- $k(k-r)$ new variables (entries of the matrix L)
- $(k-r)^2 + k(k-r)$ equations
- Codimension: $(k-r)^2 + k(k-r)$

Change of model: incidence varieties

Reminder: $k =$ size of the matrix; $r =$ target rank

Possible modelizations for determinantal varieties

- Minors: $\mathrm{rank}(A) \leq r \iff$ all $r+1$-minors of A are 0
- Incidence system: $\mathrm{rank}(A) \leq r \iff \exists L, A \cdot L = 0$ and $\mathrm{rank}(L) = k - r$

Minors:

- $\binom{k}{r+1}^2$ equations
- Codimension $(k-r)^2$

Incidence system:

- $k(k-r)$ new variables (entries of the matrix L)
- $(k-r)^2 + k(k-r)$ equations
- Codimension: $(k-r)^2 + k(k-r)$

Properties of the incidence system (generically and in our situation)

- It forms a regular sequence (codimension = length)
- It defines a radical ideal

Consequence for the strategy

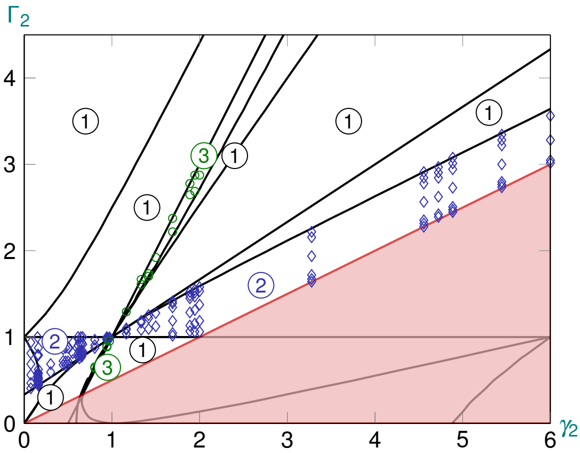
$K(\pi, V_{\leq r-1}(M))$ can be computed with the incidence system,
using maximal minors of the Jacobian matrix

Experimental results: timings

- Computations run on the matrix of the contrast optimization problem
  - Water: $\Gamma_1 = \gamma_1 = 1 \implies$ 2 parameters
  - General: $\gamma_1 = 1 \implies$ 3 parameters
- Results obtained with Maple
- Source code and full results available at `mercurey.gforge.inria.fr`

Elimination tool	Water (direct)	Water (det. strat.)	General (direct)	General (det. strat.)
Gröbner bases (`FGb`)	100 s	10 s	$>$24 h	46×200 s
Gröbner bases (`F5`)	-	1 s	-	110 s
Regular chains (`RegularChains`)	1050 s	-	$>$24 h	90×200 s

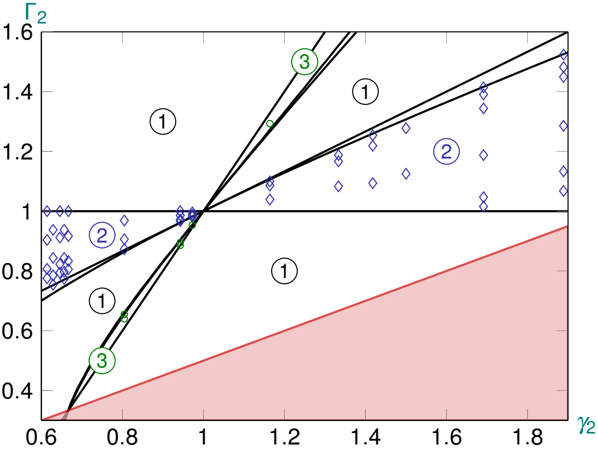
Experimental results: answers



Answers to the questions

- There can be 1, 2 or 3 singular points in the fibers
- We can separate 3 families of biological matters

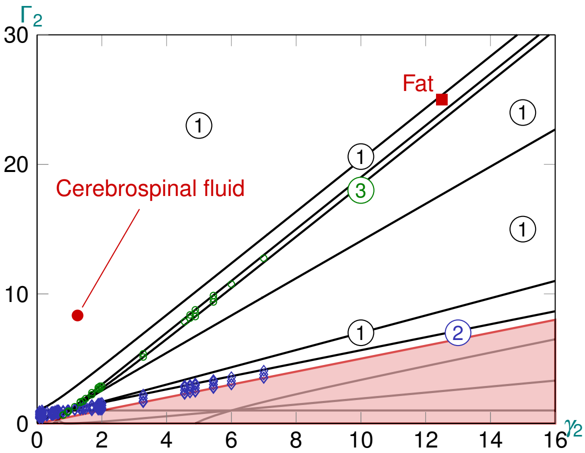
Experimental results: answers (zoom in)



Answers to the questions

- There can be 1, 2 or 3 singular points in the fibers
- We can separate 3 families of biological matters

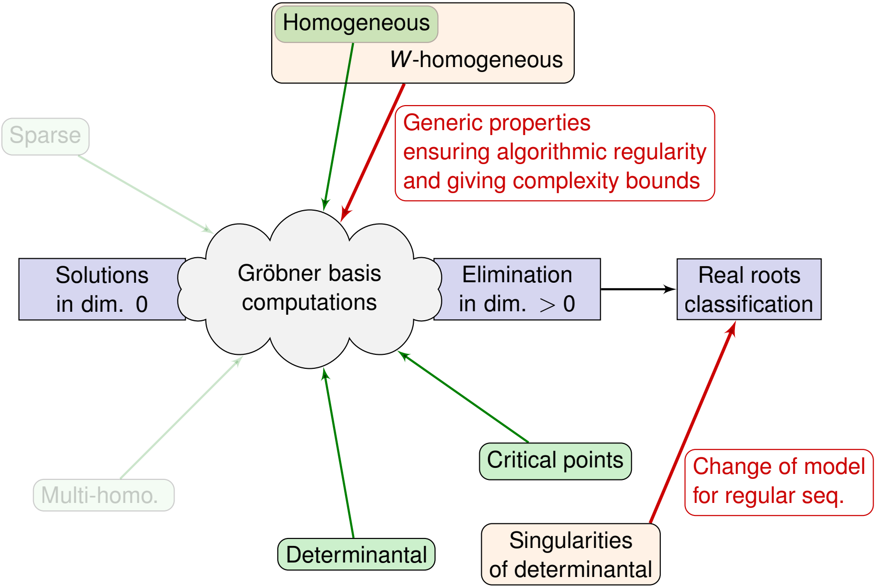
Experimental results: answers (zoom out)



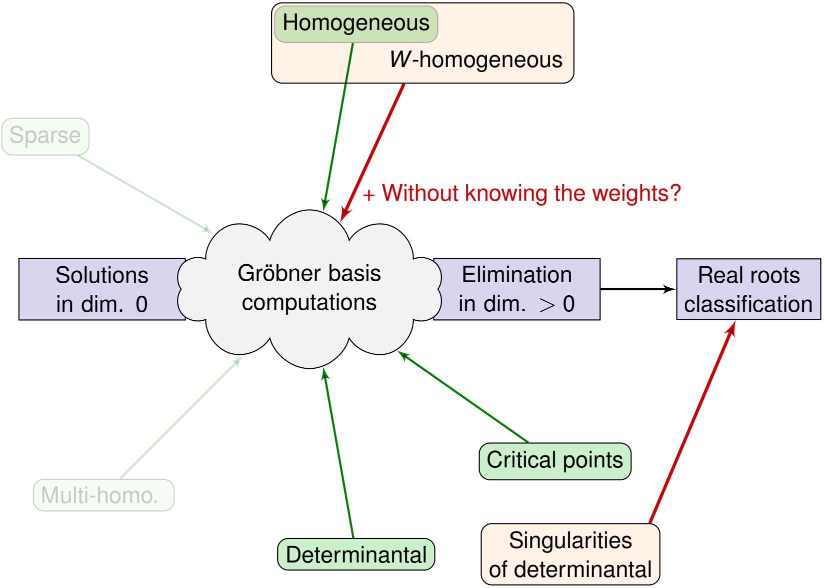
Answers to the questions

- There can be 1, 2 or 3 singular points in the fibers
- We can separate 3 families of biological matters

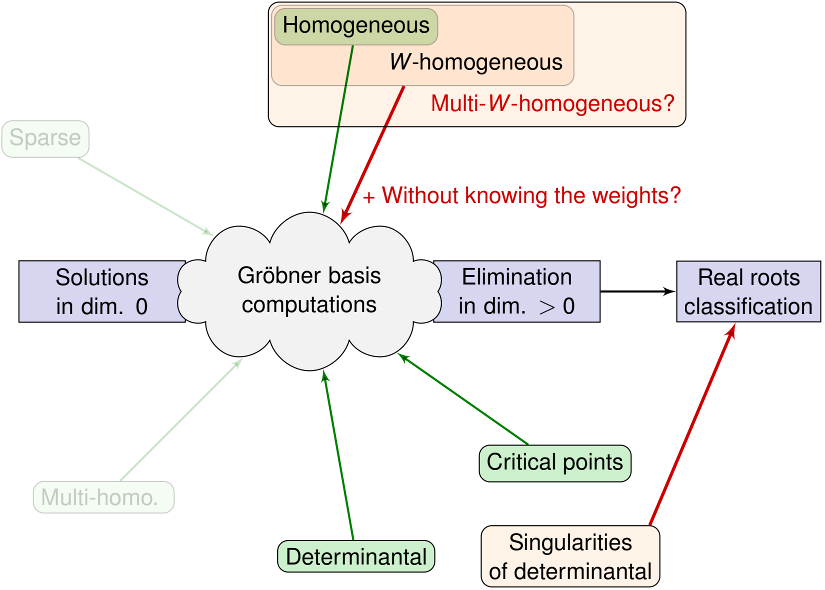
Conclusion


Homogeneous
W-homogeneous
Generic properties
ensuring algorithmic regularity
and giving complexity bounds
Sparse
Solutions
in dim. 0
Gröbner basis
computations
Elimination
in dim. > 0
Real roots
classification
Critical points
Change of model
for regular seq.
Multi-homo.
Determinantal
Singularities
of determinantal

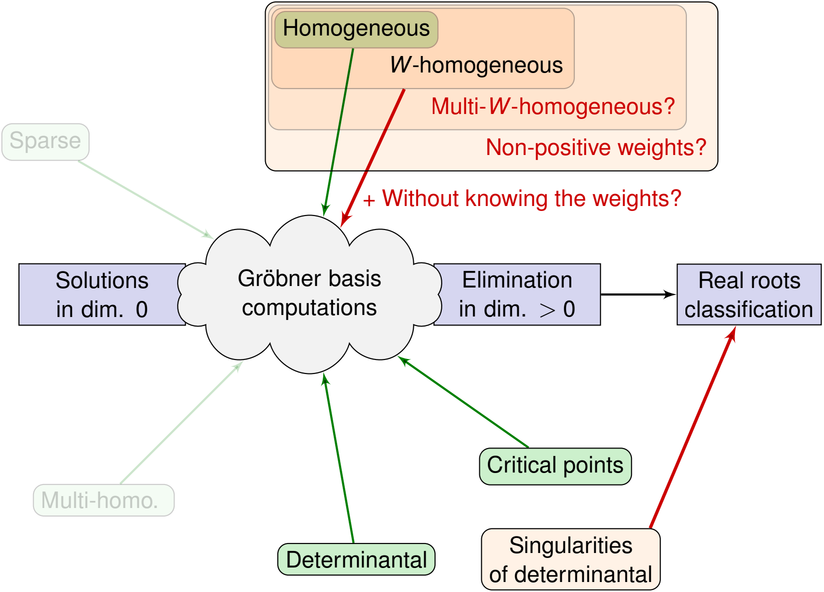
Conclusion... and perspectives



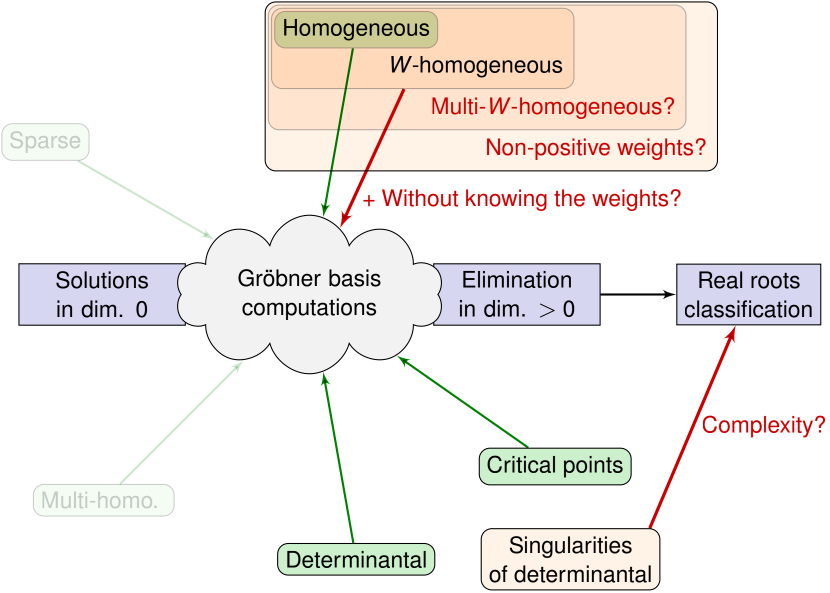
Conclusion... and perspectives



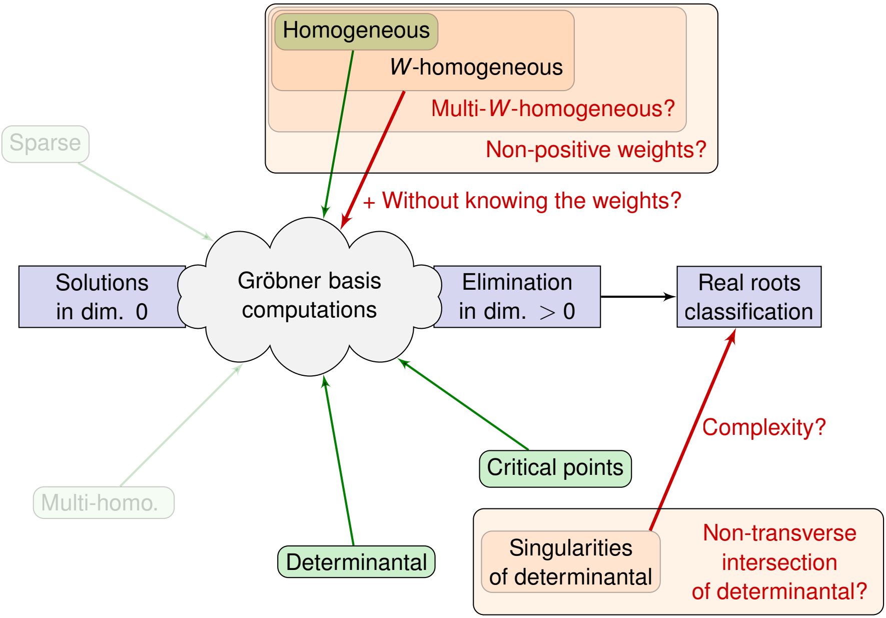
Conclusion... and perspectives



Conclusion... and perspectives



Conclusion... and perspectives



Thank you for your attention!

Publications:

- Jean-Charles Faugère, Mohab Safey El Din and Thibaut Verron (2013). 'On the complexity of computing Gröbner bases for quasi-homogeneous systems'. In: *Proceedings of the 2013 International Symposium on Symbolic and Algebraic Computation*. ISSAC '13. Boston, USA: ACM
- Jean-Charles Faugère, Mohab Safey El Din and Thibaut Verron (2016). 'On the complexity of computing Gröbner bases for weighted homogeneous systems'. In: *Journal of Symbolic Computation* 76, pp. 107–141. ISSN: 0747-7171. DOI: `http://dx.doi.org/10.1016/j.jsc.2015.12.001`. URL: `http://www.sciencedirect.com/science/article/pii/S0747717115001273`
- Bernard Bonnard, Jean-Charles Faugère, Alain Jcquemard, Mohab Safey El Din and Thibaut Verron (2016). 'Determinantal sets, singularities and application to optimal control in medical imagery'. In: *Proceedings of the 2016 International Symposium on Symbolic and Algebraic Computation*. ISSAC '16. Waterloo, Canada