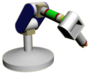
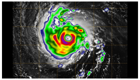
Computer algebra algorithms for solving polynomial systems, software and applications

Thibaut Verron

Johannes Kepler University, Institute for Algebra, Linz, Austria

Non-linear modelization and computer algebra





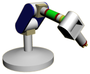
Applications → Robotics | Cryptography | Dynamical systems | …

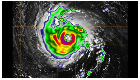
↓

System of polynomial equations (and inequations)

↓

Solutions





Applications → Robotics | Cryptography | Dynamical systems | …

↓

System of polynomial equations (and inequations)

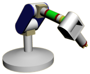
↓

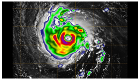
Solutions

Many tools:

- Numeric
  - Ex: Newton iteration, homotopy...
  - Trade precision for speed
- Computer Algebra
  - Ex: Resultants, Gröbner bases...
  - Exact, exhaustive and certifiable
- Hybrid

Non-linear modelization and computer algebra





Applications → Robotics, Cryptography, Dynamical systems …

↓

System of polynomial equations (and inequations)

↓

Solutions

Many tools:

- Numeric
  - Ex: Newton iteration, homotopy...
  - Trade precision for speed
- Computer Algebra
  - Ex: Resultants, Gröbner bases...
  - Exact, exhaustive and certifiable
- Hybrid

Generic and structured systems

Goal: exact, exhaustive and certified results

- Replace or supplement numeric calculations with symbolic manipulations
- Difficulty: intrinsic complexity of the objects being computed

Examples:

- NP-complete problem over finite fields
- Bézout bound: number of solutions exponential (product of the degrees)
- Worst case: doubly exponential space complexity [Mayr, Meyer 1984]
- For generic system, singly exponential bounds (time and space)

In practice, systems from applications are...

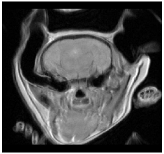
- ... not generic
- ... not instances of the worst case complexity

Key question: identify underlying structures to recover the generic complexity

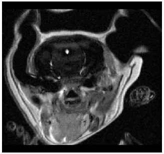
An example: algebraic classification for magnetic resonance imagery

(With B. Bonnard, J.-C. Faugère, A. Jacquemard and M. Safey El Din)

- Context: Magnetic Resonance Imagery
- Goal: optimize contrast



Bad contrast



Optimized

- Optimal control approach: the Bloch model

$$\begin{cases} \dfrac{\mathrm{d}}{\mathrm{d}t} y_i = -\Gamma_i\, y_i - u\, z_i \\ \dfrac{\mathrm{d}}{\mathrm{d}t} z_i = -\gamma_i\, (1 - z_i) + u\, y_i \end{cases} \qquad (i = 1, 2, \ldots, n)$$

y_i, z_i : $2n$ dynamic variables

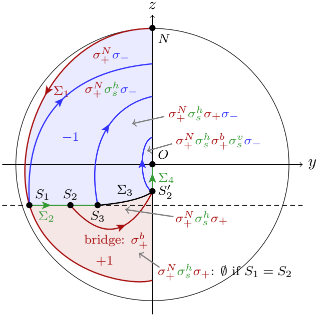
Bloch ball: $y_i^2 + z_i^2 \leq 1$

u : control function

γ_i, Γ_i : $2n$ physical parameters fixed by the experimental setting

$\gamma_i > 0, \Gamma_i > 0, 2\,\Gamma_i \geq \gamma_i$

Semi-algebraic classification problem for MRI



Problem: classification of optimal trajectories

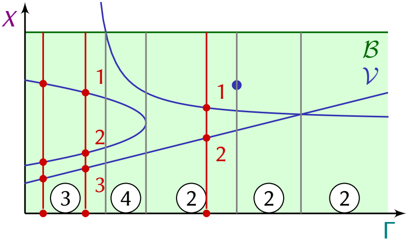
- Control of a single particle: done
- For two particles: more complicated
- Classify some algebraic invariants instead
- Used for choosing simulations to run

Example of algebraic invariant:

- Linked to equilibrium points
- Equations:

$$\mathcal{V} = \left\{ D = \frac{\partial D}{\partial y_1} = \frac{\partial D}{\partial z_1} = \frac{\partial D}{\partial y_2} = \frac{\partial D}{\partial z_2} = 0 \right\}$$

- D : determinant of 4 vector fields
- Inequalities: $\mathcal{B} = \{ y_i^2 + z_i^2 \leq 1 \}$
- Classification question: real points of $\mathcal{V} \cap \mathcal{B}$ depending on γ_i, Γ_i



Results for the MRI classification problem

State of the art:

- Existing tools can't solve the problem efficiently
- 1000s on the case of water (easier: $\gamma_1 = \Gamma_1 = 1$), full problem out of reach
- Complicated output for further steps

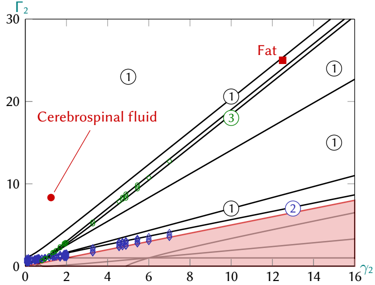
Results:

- Dedicated algorithm exploiting the structure of the system (determinants of matrices)
- Implemented in Maple
- Used to give full classification to the application
- 10s on the case of water, 4h on the full problem

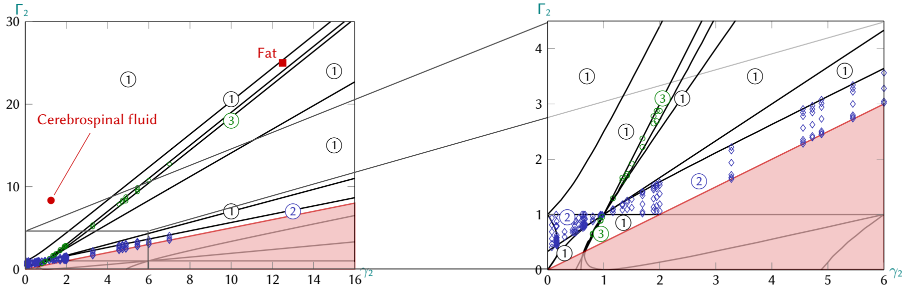
Tools:

- Real geometry: Whitney stratification, Thom's isotopy theorem, critical points
- Algebra: determinantal ideals, incidence varieties
- Computer Algebra: polynomial elimination

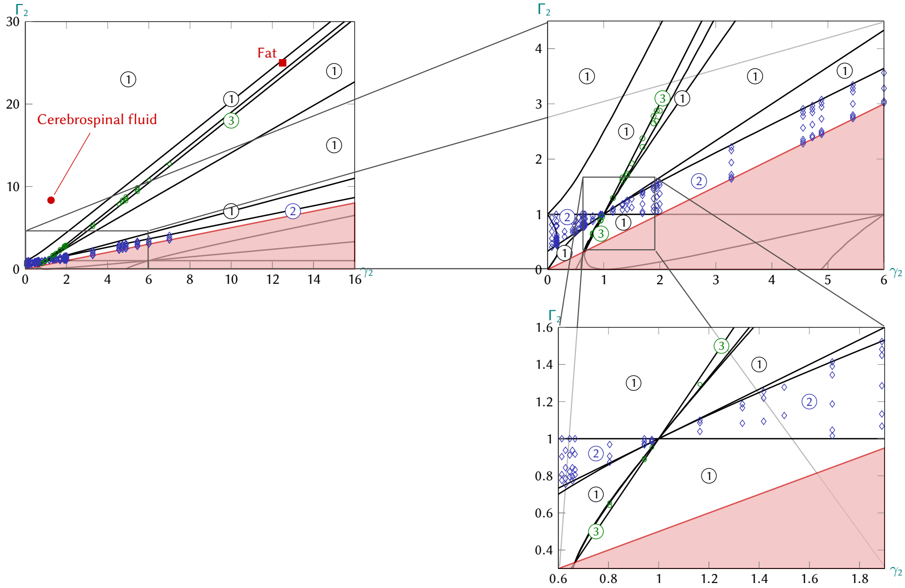
Classification in the case of water ($\gamma_1 = \Gamma_1 = 1$)



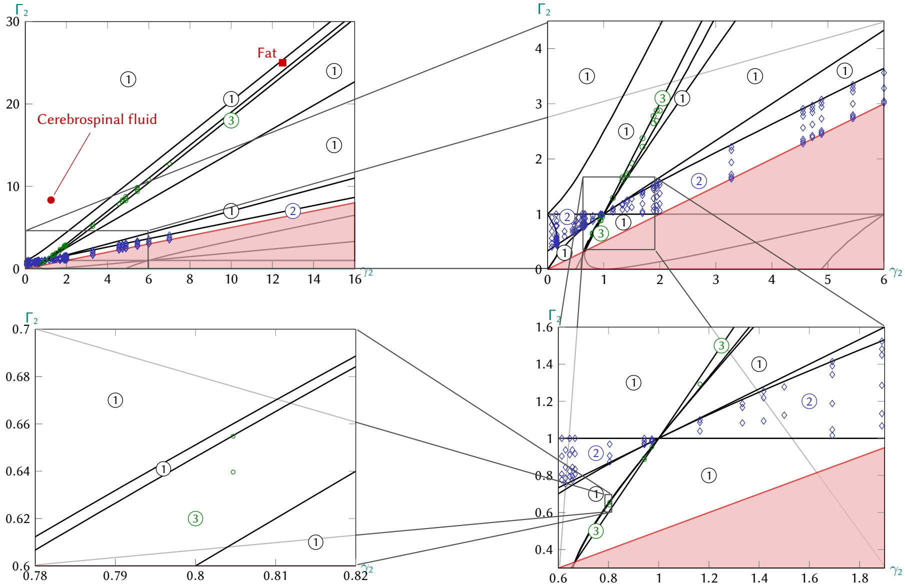
Classification in the case of water ($\gamma_1 = \Gamma_1 = 1$)



Classification in the case of water ($\gamma_1 = \Gamma_1 = 1$)



Classification in the case of water ($\gamma_1 = \Gamma_1 = 1$)



Main computer algebra building block : polynomial elimination

Polynomial elimination:

- Given an ideal $I \subset K[X_1, \ldots, X_n, G_1, \ldots, G_r]$
- Compute a basis of $I_G = I \cap K[G_1, \ldots, G_r]$

Computing eliminations allows to...

- ... compute projections of varieties
- ... solve if finitely many solutions (by iterating)
- ... compute unions and differences of varieties (by lifting)

Many tools: resultants, triangular sets, Gröbner bases

Main computer algebra building block : polynomial elimination

Polynomial elimination:

- Given an ideal $I \subset K[X_1, \dots, X_n, G_1, \dots, G_r]$
- Compute a basis of $I_G = I \cap K[G_1, \dots, G_r]$

Computing eliminations allows to...

- ... compute projections of varieties
- ... solve if finitely many solutions (by iterating)
- ... compute unions and differences of varieties (by lifting)

Many tools: resultants, triangular sets, Gröbner bases

$$\left\{\begin{array}{l} 2{X_1}^2 G_1 - 3{X_2}^2 G_2 - 3{G_2}^2 \\ X_1 G_1 + 2X_2 G_2 \\ X_1 X_2 + 4G_1 G_2 - 8{G_2}^2 \end{array}\right. \longrightarrow \left\{\begin{array}{l} X_1 X_2 + 4G_1 G_2 - 8{G_2}^2 \\ X_1 G_1 + 2X_2 G_2 \\ 32X_1 {G_2}^3 + 3X_1 {G_2}^2 - 12X_2 G_1 {G_2}^2 + 56X_2 {G_2}^3 \\ 3{X_2}^2 G_2 - 16G_1 {G_2}^2 + 32{G_2}^3 + 3{G_2}^2 \\ 6{G_1}^2 G_2 - 28G_1 {G_2}^2 + 32{G_2}^3 + 3{G_2}^2 \end{array}\right.$$

Other previous works

Structured

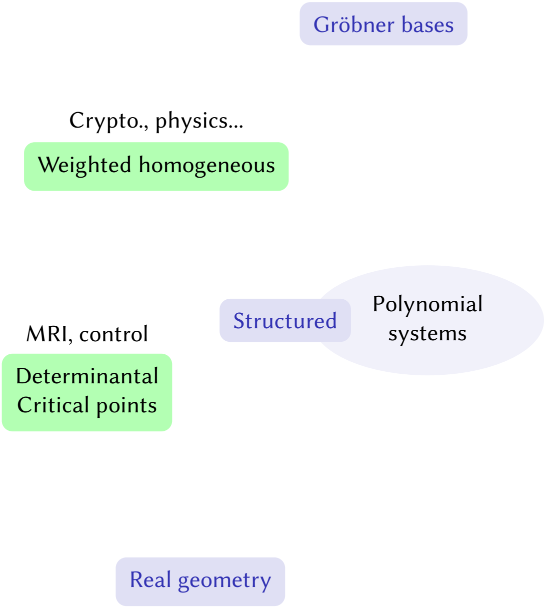
Polynomial systems

MRI, control

Determinantal
Critical points

Real geometry

Other previous works



Other previous works

Gröbner bases

GB over rings
Signature GB

Number theory

Gröbner bases on $\mathbb{Z}$

Crypto., physics...

Weighted homogeneous

Structured

Polynomial systems

Extended

MRI, control

Determinantal
Critical points

Real geometry

Other previous works

Gröbner bases

GB over rings
Signature GB

Number theory

Gröbner bases
on $\mathbb{Z}$

Crypto., physics...

Weighted homogeneous

Algebraic geometry

Gröbner bases
on Tate algebras

Structured

Polynomial
systems

Extended

MRI, control

Determinantal
Critical points

Power series
Valuations

Real geometry

Other previous works

Gröbner bases

GB over rings
Signature GB

Number theory

Gröbner bases on $\mathbb{Z}$

Crypto., physics...

Weighted homogeneous

Algebraic geometry

Gröbner bases on Tate algebras

Structured

Polynomial systems

Extended

MRI, control

Determinantal
Critical points

Power series
Valuations

Integral bases for Ore algebras

Summation

Real geometry

Tool for *e.g.* cryptography: weighted homogeneous systems

(With J.C. Faugère and M. Safey El Din)

Example: system from the discrete logarithm problem [Faugère, Gaudry, Huot, Renault, 2013]

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

$$\begin{bmatrix}27200\\38476\\28698\\5708\\47718\end{bmatrix} X_1^{3}X_2^{5} + \begin{bmatrix}64271\\43542\\57950\\52276\\9739\end{bmatrix} X_1^{2}X_2^{6} + \begin{bmatrix}49159\\11328\\33520\\65039\\27178\end{bmatrix} X_1X_2^{7} + \begin{bmatrix}59456\\49518\\46071\\49716\\33760\end{bmatrix} X_2^{8} + \text{2069 terms}$$

5 equations
5 unknowns
Degree 16

Tool for *e.g.* cryptography: weighted homogeneous systems

(With J.C. Faugère and M. Safey El Din)

Example: system from the discrete logarithm problem [Faugère, Gaudry, Huot, Renault, 2013]

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

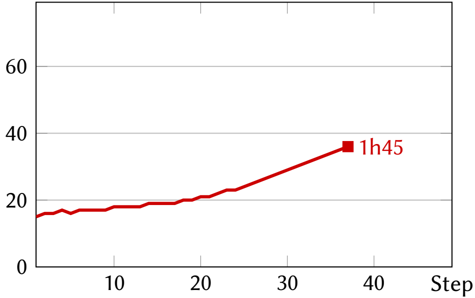
$$\begin{bmatrix}27200\\38476\\28698\\5708\\47718\end{bmatrix} X_1^3 X_2^5 + \begin{bmatrix}64271\\43542\\57950\\52276\\9739\end{bmatrix} X_1^2 X_2^6 + \begin{bmatrix}49159\\11328\\33520\\65039\\27178\end{bmatrix} X_1 X_2^7 + \begin{bmatrix}59456\\49518\\46071\\49716\\33760\end{bmatrix} X_2^8 + 2069 \text{ terms}$$

5 equations
5 unknowns
Degree 16

"Default" strategy:

- Irregular behavior
- Long calculation
- No complexity estimates

Degree of the polynomials at each step



Tool for *e.g.* cryptography: weighted homogeneous systems

(With J.C. Faugère and M. Safey El Din)

Example: system from the discrete logarithm problem [Faugère, Gaudry, Huot, Renault, 2013]

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

$$\begin{bmatrix}27200\\38476\\28698\\5708\\47718\end{bmatrix} X_1^{3}X_2^{5} + \begin{bmatrix}64271\\43542\\57950\\52276\\9739\end{bmatrix} X_1^{2}X_2^{6} + \begin{bmatrix}49159\\11328\\33520\\65039\\27178\end{bmatrix} X_1X_2^{7} + \begin{bmatrix}59456\\49518\\46071\\49716\\33760\end{bmatrix} X_2^{8} + 2069 \text{ terms}$$

5 equations
5 unknowns
Degree 16

"Default" strategy:

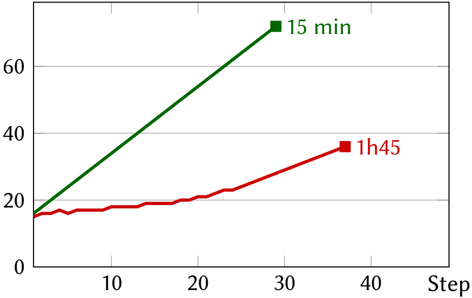
- Irregular behavior
- Long calculation
- No complexity estimates

With weights:

= Subst. $X_i \leftarrow X_i^2$ ($i = 1 \ldots 4$):

- Regular behavior
- Faster calculation

Degree of the polynomials at each step



Weighted homogeneous: results and future works

Results:

- Full algorithmic strategy taking advantage of generic regularity properties
- Full understanding of the graduation (syzygy module, Hilbert series)
- Characterization of generic properties (regularity, semi-regularity, Noether position)
- Complexity bounds divided by $\left(\prod w_i\right)^3$
- Can be used by any existing implementation without computational cost

Future work:

- Automatic detection of the best system of weights
- More general structures allowing the weights to be 0 (elimination)...
- ... or < 0 (variables with local ordering, saturation)
- Multi-graduation: weighted homogeneous for several systems of weights (physics)

Tool for number theory: modern algorithms for Gröbner bases over rings
(With M. Francis)

- Applications:
  - Number theory [Lichtblau, 2011]
  - Lattice-based cryptography [Francis, Dukkipati 2016]
  - Computation in finitely-presented groups [Sims, 1994]
- Example: intersection of two ideals in $\mathbb{Z}[\sqrt{-11}][x, y] \simeq \mathbb{Z}[x, y, z]/\langle z^2 + 11\rangle$?

  Non Euclidean (non factorial) → $\mathbb{Z}[\sqrt{-11}]$

  Euclidean ($\mathbb{Z}$) → $\mathbb{Z}$

- Algorithms developed in the late 80's and early 90's
- Impossible to mitigate coefficient growth with modular methods
- Many usual criteria when coefficients are in a field become more complicated over rings
- Recent surge of interest with focus on $\mathbb{Z}$ and Euclidean rings (Lichtblau, Eder, Popescu...)

Gröbner bases over $\mathbb{Z}$: results and future work

Question:

- Signatures: technique for recovering and exploiting info. on the module of syzygies [Faugère, 2002]
- Is it possible to compute Gröbner bases with signatures over $\mathbb{Z}$?
- State of the art: No, impossible [Eder, Popescu 2017]

Results:

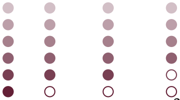
- New answer: Yes, with another definition!
- Proof of concept of two algorithms working over any principal ring
- Prototype implementation of the algorithms in Magma

Future work:

- Complete analysis of existing algorithms and criteria to identify what is or not possible
- Complexity analyses
- Competitive implementation of the algorithms

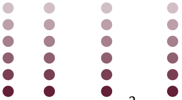
Tool for algebraic geometry: Gröbner bases over Tate algebras
(With X. Caruso and T. Vaccon)

- Tate series = convergent series over a complete valued ring (*e.g.* $\mathbb{Z}_p$ or $\mathbb{Q}_p$)
  $\iff$ the valuation of the coefficients goes to infinity
- Introduced by Tate in 1971 for rigid geometry
  (p-adic equivalent of the bridge between algebraic and analytic geometry over $\mathbb{C}$)
- No existing implementation of arithmetic or ideal operations



$$\sum_{i,j=0}^{\infty} p^{i+j} X^i Y^j = 1 + pX + pY + p^2 X^2 + \cdots$$

Tate series



$$\sum_{i=0}^{\infty} X^i = 1 + 1X + 1X^2 + 1X^3 + \cdots$$

Not a Tate series

Tate algebras: results and future work

Features of those systems:

- In the valued case, there is no difference between ring and field
- Main difficulty: in Tate series, we need to order terms (with coefficients)...
- ... in a mixed ordering: $pX < 1 < X$

Results:

- Definitions and algorithms for Gröbner bases over Tate algebras
- Implementation of arithmetic and Gröbner basis algorithms in Sage (included in Sage since version 8.5 [2019])
- Signature-based algorithms over Tate algebras

Future work:

- More efficient algorithms for reductions
- More optimized implementation

Previous works and research project

Gröbner bases

GB over rings
Signature GB

Number theory

Gröbner bases on $\mathbb{Z}$

More criteria
Better implementation

Crypto., physics...

Weighted homogeneous

More general weights
Automatic detection

Algebraic geometry

Gröbner bases on Tate algebras

Faster reductions

Structured — Polynomial systems — Extended

MRI, control

Determinantal
Critical points

Rectangular matrices
Complexity bounds
Other classifications

Power series
Valuations

Integral bases for Ore algebras — Summation

Real geometry

Previous works and research project

Generic complexity
and strategy questions

Gröbner bases

GB over rings
Signature GB

Number theory

Gröbner bases
on $\mathbb{Z}$

More criteria
Better implementation

Crypto., physics...

Weighted homogeneous

More general weights
Automatic detection

Algebraic geometry

Gröbner bases
on Tate algebras

Faster reductions

Structured

Polynomial
systems

Extended

MRI, control

Determinantal
Critical points

Rectangular matrices
Complexity bounds
Other classifications

Power series
Valuations

Integral bases
for Ore algebras

Summation

Real geometry

Example of general questions: complexity and strategy for elimination?

Complexity and strategy for a system with finitely many solutions:

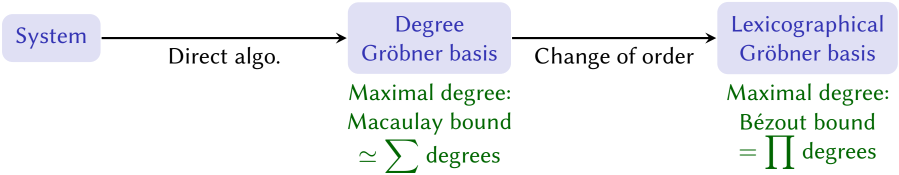
System → (Direct algo.) → Degree Gröbner basis → (Change of order) → Lexicographical Gröbner basis

Degree Gröbner basis — Maximal degree: Macaulay bound $\simeq \sum$ degrees

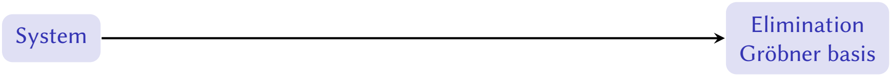
Lexicographical Gröbner basis — Maximal degree: Bézout bound $= \prod$ degrees

Example of general questions: complexity and strategy for elimination?

Complexity and strategy for a system with finitely many solutions:



What about polynomial elimination?



Example of general questions: complexity and strategy for elimination?

Complexity and strategy for a system with finitely many solutions:

System → (Direct algo.) → Degree Gröbner basis → (Change of order) → Lexicographical Gröbner basis

Degree Gröbner basis — Maximal degree: Macaulay bound $\simeq \sum$ degrees

Lexicographical Gröbner basis — Maximal degree: Bézout bound $= \prod$ degrees

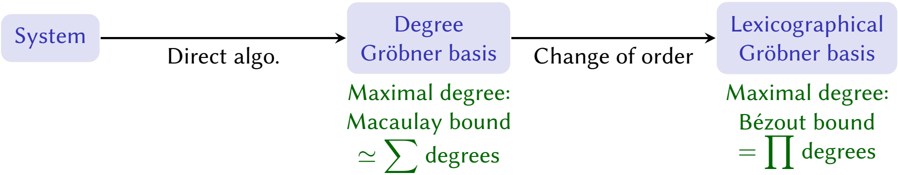
What about polynomial elimination?

System → Elimination Gröbner basis

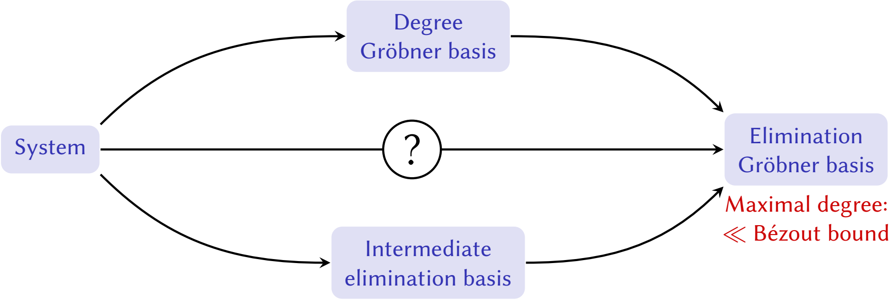
Elimination Gröbner basis — Maximal degree: $\ll$ Bézout bound

Example of general questions: complexity and strategy for elimination?

Complexity and strategy for a system with finitely many solutions:



What about polynomial elimination?



Previous works and research project

Generic complexity and strategy questions

Gröbner bases

GB over rings
Signature GB

Number theory

Gröbner bases on $\mathbb{Z}$

More criteria
Better implementation

Crypto., physics...

Weighted homogeneous

More general weights
Automatic detection

Algebraic geometry

Gröbner bases on Tate algebras

Faster reductions

Structured

Polynomial systems

Extended

MRI, control

Determinantal
Critical points

Rectangular matrices
Complexity bounds
Other classifications

Power series
Valuations

Integral bases for Ore algebras

Summation

Real geometry

Previous works and research project

Generic complexity and strategy questions

Gröbner bases

Non-commutative case

GB over rings
Signature GB

Number theory

Gröbner bases on $\mathbb{Z}$

More criteria
Better implementation

Crypto., physics...

Weighted homogeneous

More general weights
Automatic detection

Algebraic geometry

Gröbner bases on Tate algebras

Faster reductions

Structured

Polynomial systems

Extended

MRI, control

Determinantal
Critical points

Rectangular matrices
Complexity bounds
Other classifications

Power series
Valuations

Integral bases for Ore algebras

Summation

Real geometry

Previous works and research project

Generic complexity and strategy questions

Gröbner bases

Non-commutative case

GB over rings
Signature GB

Number theory

Gröbner bases on $\mathbb{Z}$

More criteria
Better implementation

Crypto., physics...

Weighted homogeneous

More general weights
Automatic detection

Algebraic geometry

Gröbner bases on Tate algebras

Faster reductions

Structured

Polynomial systems

Extended

MRI, control

Determinantal
Critical points

Power series
Valuations

Rectangular matrices
Complexity bounds
Other classifications

More systems from more applications

Integral bases for Ore algebras

Summation

Real geometry

Thank you for your attention!

Image credits

- Robotic arm p. 2: public domain, via Wikimedia Commons
- Credit cards p. 2: Lotus Heads via Wikimedia Commons (CC-by SA 3.0)
- Hurricane model p. 2: NASA
- Mouse head MRI p.4:
  - Éric Van Reeth et al. (2016). 'Optimal Control Design of Preparation Pulses for Contrast Optimization in MRI'. In: Submitted IEEE transactions on medical imaging
- Optimal trajectories of a single spin p.5:
  - Bernard Bonnard et al. (2020). 'Time minimal saturation of a pair of spins and application in Magnetic Resonance Imaging'. In: *Mathematical Control & Related Fields* 10.1, 47–88. ISSN: 2156-8499. DOI: 10.3934/mcrf.2019029. URL: https://www.archives-ouvertes.fr/hal-01764022