Gröbner basis computation

Robin Kouba from PolSys team
Supervisors: Mohab Safey El Din and Vincent Neiger

Sorbonne Université - CNRS - LIP6

December 11, 2025

Algebraic Numbers and Polynomial Systems

$$\begin{cases} x^2 + y^2 &= 5 \\ x + y &= 1 \end{cases} \implies 2y^2 - 2y - 4 = 0$$

Algebraic Numbers and Polynomial Systems

$$\begin{cases} x^2 + y^2 &= 5 \\ x + y &= 1 \end{cases} \implies 2y^2 - 2y - 4 = 0$$

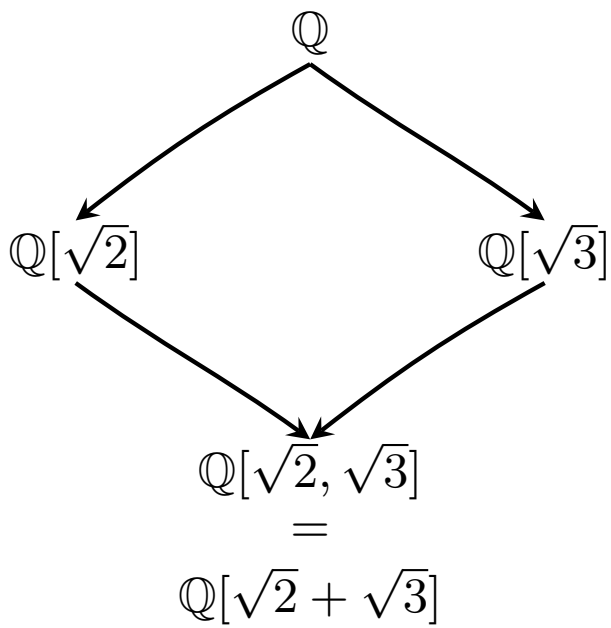
y and x are algebraic

Algebraic Numbers and Polynomial Systems

$$\begin{cases} x^2 + y^2 &= 5 \\ x + y &= 1 \end{cases} \implies 2y^2 - 2y - 4 = 0$$

y and x are algebraic

Évariste Galois
(1811–1832)



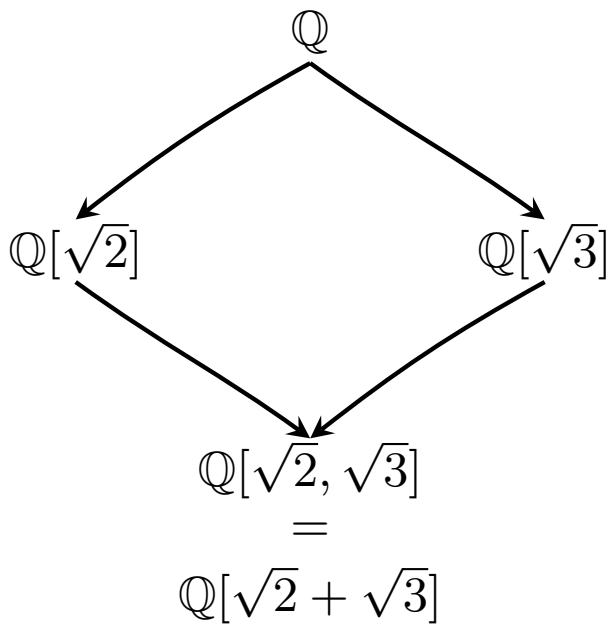
Primitive Element Theorem

Algebraic Numbers and Polynomial Systems

$$\begin{cases} x^2 + y^2 &= 5 \\ x + y &= 1 \end{cases} \implies 2y^2 - 2y - 4 = 0$$

y and x are algebraic

Évariste Galois
(1811–1832)



$$\begin{cases} x_1^2 - 2 &= 0 \\ x_2^2 - 3 &= 0 \\ x_3 - (x_1 + x_2) &= 0 \end{cases}$$

Primitive Element Theorem

The Legacies of Sylvester and Macaulay

$f = \sum_{k=0}^{d} a_k X^k$, $g = \sum_{k=0}^{e} b_k X^k$ in $\mathcal{R}[X]$

$$\begin{pmatrix} a_d & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & \ddots & & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & 0 \\ 0 & \cdots & 0 & a_d & \cdots & \cdots & a_0 \\ b_e & \cdots & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & \ddots & & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & 0 \\ 0 & \cdots & 0 & b_e & \cdots & \cdots & b_0 \end{pmatrix}$$

$$\begin{array}{c} \mathcal{R}[X]_{<e} \oplus \mathcal{R}[X]_{<d} \longrightarrow \mathcal{R}[X]_{<d+e} \\ (U, V) \longmapsto UF + VG \end{array}$$

The Legacies of Sylvester and Macaulay

$f = \sum_{k=0}^{d} a_k X^k$, $g = \sum_{k=0}^{e} b_k X^k$ in $\mathcal{R}[X]$

$$\begin{pmatrix}
a_d & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\
0 & \ddots & & & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & & & \ddots & 0 \\
0 & \cdots & 0 & a_d & \cdots & \cdots & a_0 \\
b_e & \cdots & \cdots & b_0 & 0 & \cdots & 0 \\
0 & \ddots & & & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & & & \ddots & 0 \\
0 & \cdots & 0 & b_e & \cdots & \cdots & b_0
\end{pmatrix}$$

$$\begin{aligned}\mathcal{R}[X]_{<e} \oplus \mathcal{R}[X]_{<d} &\longrightarrow \mathcal{R}[X]_{<d+e} \\ (U, V) &\longmapsto UF + VG\end{aligned}$$

Euclid Algorithm

$\mathsf{GCD}(f, g)$

$$f = qg + r$$

new leading monomial

The Legacies of Sylvester and Macaulay

$f = \sum_{k=0}^{d} a_k X^k$, $g = \sum_{k=0}^{e} b_k X^k$ in $\mathcal{R}[X]$

$$\begin{pmatrix} a_d & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & \ddots & & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & 0 \\ 0 & \cdots & 0 & a_d & \cdots & \cdots & a_0 \\ b_e & \cdots & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & \ddots & & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & 0 \\ 0 & \cdots & 0 & b_e & \cdots & \cdots & b_0 \end{pmatrix}$$

$$\begin{aligned} \mathcal{R}[X]_{<e} \oplus \mathcal{R}[X]_{<d} &\longrightarrow \mathcal{R}[X]_{<d+e} \\ (U, V) &\longmapsto UF + VG \end{aligned}$$

Euclid Algorithm

$\mathsf{GCD}(f, g)$

$$f = qg + r$$

new leading monomial

bivariate case is doable using resultant

Why Solve Polynomial Systems in 2026?

Biology: Lotka–Volterra Predation Equations

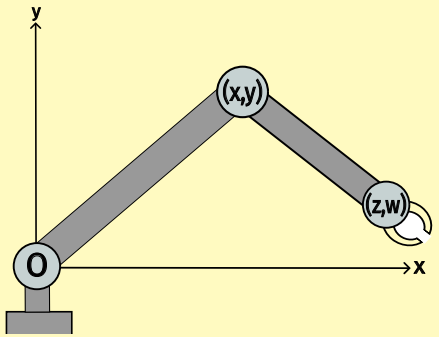
$$\begin{cases} \dfrac{dx(t)}{dt} = \alpha x(t) - \beta x(t) y(t), \\ \dfrac{dy(t)}{dt} = \delta x(t) y(t) - \gamma y(t). \end{cases}$$

Why Solve Polynomial Systems in 2026?

Biology: Lotka–Volterra Predation Equations

$$\begin{cases} \dfrac{dx(t)}{dt} = \alpha x(t) - \beta x(t) y(t), \\ \dfrac{dy(t)}{dt} = \delta x(t) y(t) - \gamma y(t). \end{cases}$$

Robotics

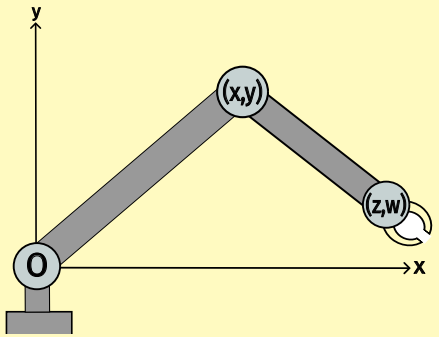


Why Solve Polynomial Systems in 2026?

Biology: Lotka–Volterra Predation Equations

$$\begin{cases} \dfrac{dx(t)}{dt} = \alpha x(t) - \beta x(t) y(t), \\ \dfrac{dy(t)}{dt} = \delta x(t) y(t) - \gamma y(t). \end{cases}$$

Robotics



Application to **cryptography**

public key: a polynomial system $(f_1, \ldots, f_\ell)$

private key : a solution to the system $\zeta \in \mathbb{K}^n$ s.t. $f_1(\zeta) = \cdots = f_\ell(\zeta) = 0$

$$\text{message} \xrightarrow{\text{encryption}} \text{message} + \text{combination of the } f_i$$

$$\text{ciphertext} \xrightarrow{\text{decryption}} \text{ciphertext}(x = \zeta) = \text{message}$$

Some Foundational Problems and Historical Solutions

Ideal membership and elimination problem:

Knowing if a polynomial f lies in I, or in $I \cap \mathbb{K}[x_\ell, \ldots, x_n]$.

Some Foundational Problems and Historical Solutions

Ideal membership and elimination problem:

Knowing if a polynomial f lies in I, or in $I \cap \mathbb{K}[x_\ell, \ldots, x_n]$.

Compute with algebraic numbers:

It means compute in a quotient ring

$$\mathbb{K}[x_1, \ldots, x_n]/I.$$

Some Foundational Problems and Historical Solutions

Ideal membership and elimination problem:
Knowing if a polynomial f lies in I, or in $I \cap \mathbb{K}[x_\ell, \ldots, x_n]$.

Compute with algebraic numbers:
It means compute in a quotient ring

$$\mathbb{K}[x_1, \ldots, x_n]/I.$$

The Weak Hilbert Nullstellensatz

Let $\mathbb{K}$ be an algebraically closed field and let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal which associated variety is empty. Then $I = \mathbb{K}[x_1, \ldots, x_n]$.

Knowing if the varity is empty is knowing if 1 lies in I or not.

Some Quantitative Bounds

Ideal membership:

[Greta Hermann, 1926]

Doubly exponentiel in the number of variables

Some Quantitative Bounds

Ideal membership:

[Greta Hermann, 1926]

Doubly exponentiel in the number of variables

Zero-dimensional systems:

[Bézout Theorem]

Number of solutions $\leq \delta^n$
with δ the degree of the input polynomials

Some Quantitative Bounds

Ideal membership:

[Greta Hermann, 1926]

Doubly exponentiel in the number of variables

Zero-dimensional systems:

[Bézout Theorem]

Number of solutions $\leq \delta^n$ with δ the degree of the input polynomials

Existence of a solution:

NP-Hard problem

[Cook-Levin Theorem] and [Michael, Garey, 1979]

Some Quantitative Bounds

Ideal membership:

[Greta Hermann, 1926]

Doubly exponentiel in the number of variables

Zero-dimensional systems:

[Bézout Theorem]

Number of solutions $\leq \delta^n$ with δ the degree of the input polynomials

Existence of a solution:

NP-Hard problem

[Cook-Levin Theorem] and [Michael, Garey, 1979]

- Hard problem for cryptography
- Lots of applications

From Euclid to Gröbner Bases

For $f_1, \ldots, f_\ell \in \mathbb{K}[X]$,
let $g = \gcd(f_1, \ldots, f_\ell)$.
Then
$\langle x^{\deg(g)} \rangle = \langle \{ x^{\deg f} \mid f \in I \} \rangle$.

$\Longrightarrow$ **admissible monomial ordering**

From Euclid to Gröbner Bases

For $f_1, \ldots, f_\ell \in \mathbb{K}[X]$,
let $g = \gcd(f_1, \ldots, f_\ell)$.
Then
$\langle x^{\deg(g)} \rangle = \langle \{ x^{\deg f} \mid f \in I \} \rangle$.

$\Longrightarrow$ **admissible monomial ordering**

Definition of grevlex

For $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$, $\mathbf{x}^{\boldsymbol{\alpha}} \prec_{grlex} \mathbf{x}^{\boldsymbol{\beta}}$ if and only if

- $\deg(\mathbf{x}^{\boldsymbol{\beta}}) > \deg(\mathbf{x}^{\boldsymbol{\alpha}})$,
- $\deg(\mathbf{x}^{\boldsymbol{\beta}}) = \deg(\mathbf{x}^{\boldsymbol{\alpha}})$ and the rightmost nonzero entry of $\boldsymbol{\beta} - \boldsymbol{\alpha} \in \mathbb{Z}^n$ is negative.

From Euclid to Gröbner Bases

For $f_1, \ldots, f_\ell \in \mathbb{K}[X]$,
let $g = \gcd(f_1, \ldots, f_\ell)$.
Then
$\langle x^{\deg(g)} \rangle = \langle \{ x^{\deg f} \mid f \in I \} \rangle$.

$\Longrightarrow$ **admissible monomial ordering**

Definition of grevlex

For $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$, $\mathbf{x}^{\boldsymbol{\alpha}} \prec_{grlex} \mathbf{x}^{\boldsymbol{\beta}}$ if and only if

- $\deg(\mathbf{x}^{\boldsymbol{\beta}}) > \deg(\mathbf{x}^{\boldsymbol{\alpha}})$,
- $\deg(\mathbf{x}^{\boldsymbol{\beta}}) = \deg(\mathbf{x}^{\boldsymbol{\alpha}})$ and the rightmost nonzero entry of $\boldsymbol{\beta} - \boldsymbol{\alpha} \in \mathbb{Z}^n$ is negative.

$f_1 = x^2 + y - 1$ and $f_2 = xy + 2$, we compute:

$$S = yf_1 - xf_2 = y^2 - y - 2x$$

Gröbner bases

Definition

Let $\succ$ be an admissible monomial ordering and $G = \{g_1, \ldots, g_p\}$ a set of polynomials of $\mathbb{K}[x_1, \ldots, x_n]$ that generates the ideal I. The set G is a Gröbner basis of $(I, \succ)$ if:

$$\langle \mathrm{lm}_{\succ}(G) \rangle = \langle \mathrm{lm}_{\succ}(I) \rangle.$$

Gröbner bases

Definition

Let $\succ$ be an admissible monomial ordering and $G = \{g_1, \ldots, g_p\}$ a set of polynomials of $\mathbb{K}[x_1, \ldots, x_n]$ that generates the ideal I. The set G is a Gröbner basis of $(I, \succ)$ if:

$$\langle \mathrm{lm}_{\succ}(G) \rangle = \langle \mathrm{lm}_{\succ}(I) \rangle.$$

Elimination Theorem

Let G be a lexicographic Gröbner basis of an ideal I in $\mathbb{K}[x_1, \ldots, x_n]$ with $x_1 \succ \ldots \succ x_n$. Then

$$G \cap \mathbb{K}[x_\ell, \ldots, x_n] \text{ is a Gröbner basis of } I \cap \mathbb{K}[x_\ell, \ldots, x_n]$$

Gröbner bases

Definition

Let $\succ$ be an admissible monomial ordering and $G = \{g_1, \ldots, g_p\}$ a set of polynomials of $\mathbb{K}[x_1, \ldots, x_n]$ that generates the ideal I. The set G is a Gröbner basis of $(I, \succ)$ if:

$$\langle \mathrm{lm}_{\succ}(G) \rangle = \langle \mathrm{lm}_{\succ}(I) \rangle.$$

Elimination Theorem

Let G be a lexicographic Gröbner basis of an ideal I in $\mathbb{K}[x_1, \ldots, x_n]$ with $x_1 \succ \ldots \succ x_n$. Then

$$G \cap \mathbb{K}[x_\ell, \ldots, x_n] \text{ is a Gröbner basis of } I \cap \mathbb{K}[x_\ell, \ldots, x_n]$$

- Unic representation in the quotient ring
- Unicity of reduced Gröbner basis

Gröbner bases

Definition

Let $\succ$ be an admissible monomial ordering and $G = \{g_1, \ldots, g_p\}$ a set of polynomials of $\mathbb{K}[x_1, \ldots, x_n]$ that generates the ideal I. The set G is a Gröbner basis of $(I, \succ)$ if:

$$\langle \mathrm{lm}_{\succ}(G) \rangle = \langle \mathrm{lm}_{\succ}(I) \rangle.$$

Elimination Theorem

Let G be a lexicographic Gröbner basis of an ideal I in $\mathbb{K}[x_1, \ldots, x_n]$ with $x_1 \succ \ldots \succ x_n$. Then

$$G \cap \mathbb{K}[x_\ell, \ldots, x_n] \text{ is a Gröbner basis of } I \cap \mathbb{K}[x_\ell, \ldots, x_n]$$

- Unic representation in the quotient ring
- Unicity of reduced Gröbner basis

Worst case: [Mayr and Meyer, 1982]

Gröbner bases and linear algebra

Macaulay Matrices [Macaulay 1902]

$$\begin{pmatrix} \vdots \\ \mathrm{vect}(\boldsymbol{x}^{\boldsymbol{\alpha_i}} f_i) \\ \vdots \end{pmatrix} \xrightarrow[\text{form}]{\text{row echelon}} \text{Gröbner basis truncated to degree } D$$

for $\boldsymbol{\alpha_i}$ with $|\boldsymbol{\alpha_i}| \leq D - \delta$,
$\deg(f_i) = \delta$

Gröbner bases and linear algebra

Macaulay Matrices [Macaulay 1902]

$$\begin{pmatrix} \vdots \\ \mathrm{vect}(\mathbf{x}^{\boldsymbol{\alpha}_i} f_i) \\ \vdots \end{pmatrix} \xrightarrow[\text{form}]{\text{row echelon}} \text{Gröbner basis truncated to degree } D$$

for $\boldsymbol{\alpha}_i$ with $|\boldsymbol{\alpha}_i| \leq D - \delta$,
$\deg(f_i) = \delta$

Macaulay bound [Lazard, 1983]

If the sequence $(f_1, \ldots, f_n)$ in $\mathbb{K}[x_1, \ldots, x_n]$ is **regular**, a truncated Gröbner basis to degree $D = 1 + n(d-1)$ for the grevlex ordering is a Gröbner basis of $(\langle f_1, \ldots, f_\ell \rangle, \succ_{\mathrm{grlex}})$.

Gröbner bases and linear algebra

Macaulay Matrices [Macaulay 1902]

$$\begin{pmatrix} \vdots \\ \mathrm{vect}(\mathbf{x}^{\boldsymbol{\alpha_i}} f_i) \\ \vdots \end{pmatrix} \xrightarrow[\text{form}]{\text{row echelon}} \text{Gröbner basis truncated to degree } D$$

for $\boldsymbol{\alpha_i}$ with $|\boldsymbol{\alpha_i}| \leq D - \delta$,
$\deg(f_i) = \delta$

Macaulay bound [Lazard, 1983]

If the sequence $(f_1, \ldots, f_n)$ in $\mathbb{K}[x_1, \ldots, x_n]$ is **regular**, a truncated Gröbner basis to degree $D = 1 + n(d-1)$ for the grevlex ordering is a Gröbner basis of $(\langle f_1, \ldots, f_\ell \rangle, \succ_{\mathrm{grlex}})$.

Set $\langle f_1, \ldots, f_\ell \rangle = I$ an ideal of $\mathcal{R} = \mathbb{K}[x_1, ..x_n]$,

$$\mathrm{HS}_I(z) = \sum_{d=0} \dim(\mathcal{R}_d / I) z^d \quad \longrightarrow \quad \left(\sum_{i=0}^{\delta - 1} z^i \right)^n$$

F4 Algorithm

F4 Algorithm

- **S-polynomial** [Buchberger 1965]

For polynomials f_1, f_2,

$$S(f_1, f_2) = \frac{\mathrm{LCM}(\mathrm{lm}_{\succ}(f_1), \mathrm{lm}_{\succ}(f_2))}{\mathrm{lm}_{\succ}(f_1)} f_1 - \frac{\mathrm{LCM}(\mathrm{lm}_{\succ}(f_1), \mathrm{lm}_{\succ}(f_2))}{\mathrm{lm}_{\succ}(f_2)} f_2$$

F4 Algorithm

- **S-polynomial** [Buchberger 1965]

For polynomials f_1, f_2,

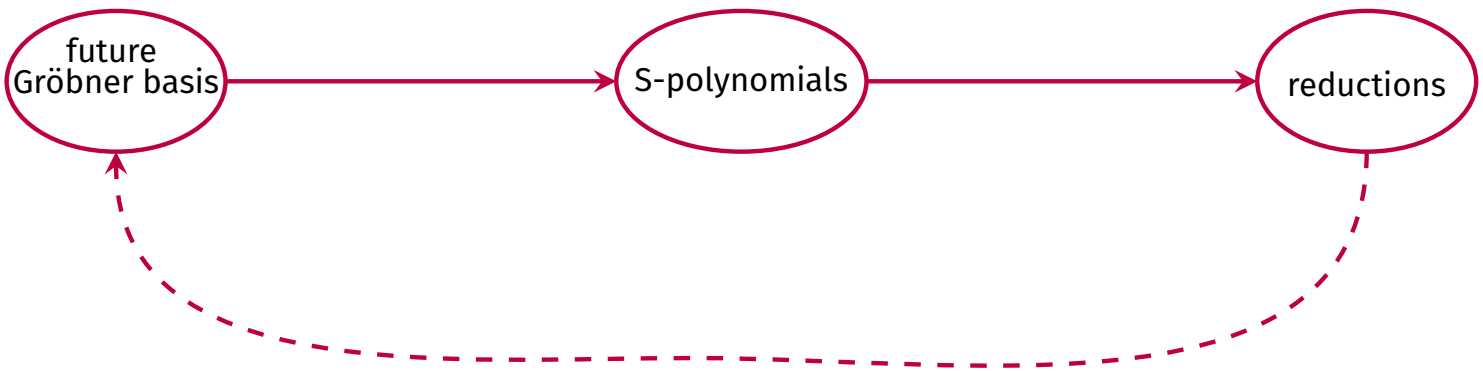
$$S(f_1, f_2) = \frac{\mathrm{LCM}(\mathrm{lm}_{\succ}(f_1), \mathrm{lm}_{\succ}(f_2))}{\mathrm{lm}_{\succ}(f_1)} f_1 - \frac{\mathrm{LCM}(\mathrm{lm}_{\succ}(f_1), \mathrm{lm}_{\succ}(f_2))}{\mathrm{lm}_{\succ}(f_2)} f_2$$

F4 Algorithm

- **S-polynomial** [Buchberger 1965]

For polynomials f_1, f_2,

$$S(f_1, f_2) = \frac{\mathrm{LCM}(\mathrm{lm}_\succ(f_1), \mathrm{lm}_\succ(f_2))}{\mathrm{lm}_\succ(f_1)} f_1 - \frac{\mathrm{LCM}(\mathrm{lm}_\succ(f_1), \mathrm{lm}_\succ(f_2))}{\mathrm{lm}_\succ(f_2)} f_2$$



F4 exemple

In $\mathbb{Z}/7\mathbb{Z}[x, y, z]$,

$$f_1 = x^2 + 2xy + 5y^2 + xz + 6yz + 3z^2,$$

$$f_2 = xy + 3y^2 + 4xz + 2yz + z^2,$$

$$f_3 = y^2 + 4xz + 2yz + 3z^2.$$

F4 exemple

In $\mathbb{Z}/7\mathbb{Z}[x, y, z]$,

$f_1 = x^2 + 2xy + 5y^2 + xz + 6yz + 3z^2$,

$f_2 = xy + 3y^2 + 4xz + 2yz + z^2$,

$f_3 = y^2 + 4xz + 2yz + 3z^2$.

$$
\begin{array}{c}
 & \begin{array}{cccccccccc} x^3 & x^2y & xy^2 & y^3 & x^2z & xyz & y^2z & xz^2 & yz^2 & z^3 \end{array} \\
\begin{array}{r} S_{f_1,f_2} \\ S_{f_2,f_3} \end{array} & \left(\begin{array}{cccccccccc} 0 & 0 & 6 & 5 & 3 & 6 & 6 & 6 & 3 & 0 \\ 0 & 0 & 0 & 3 & 3 & 2 & 2 & 4 & 1 & 0 \\ \hline & & & & & & & & & \\ & & & & & & & & & \\ & & & & & & & & & \end{array}\right)
\end{array}
$$

F4 exemple

In $\mathbb{Z}/7\mathbb{Z}[x, y, z]$,

$f_1 = x^2 + 2xy + 5y^2 + xz + 6yz + 3z^2$,

$f_2 = xy + 3y^2 + 4xz + 2yz + z^2$,

$f_3 = y^2 + 4xz + 2yz + 3z^2$.

	x^3	x^2y	xy^2	y^3	x^2z	xyz	y^2z	xz^2	yz^2	z^3
S_{f_1,f_2}	0	0	6	5	3	6	6	6	3	0
S_{f_2,f_3}	0	0	0	3	3	2	2	4	1	0
xf_3	0	0	1	0	4	2	0	3	0	0
yf_3	0	0	0	1	0	4	2	0	3	0
zf_1	0	0	0	0	1	2	5	1	6	3
zf_2	0	0	0	0	0	1	3	4	2	1

F4 exemple

In $\mathbb{Z}/7\mathbb{Z}[x, y, z]$,

$f_1 = x^2 + 2xy + 5y^2 + xz + 6yz + 3z^2$,

$f_2 = xy + 3y^2 + 4xz + 2yz + z^2$,

$f_3 = y^2 + 4xz + 2yz + 3z^2$.

$$
\begin{array}{c}
\begin{array}{cccccccccc}
x^3 & x^2y & xy^2 & y^3 & x^2z & xyz & y^2z & xz^2 & yz^2 & z^3
\end{array} \\
\left(\begin{array}{cccccccccc}
0 & 0 & 1 & 0 & 0 & 0 & 0 & 6 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 4 & 0 & 2 \\
\hline
0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 2 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 5 & 0 & 6 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 6 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 6
\end{array}\right)
\end{array}
$$

F4 Tracer

In Software [msolve 2021]**:** F4 is **traced** [Traverso 1989]

1. F4 over $\mathbb{Q} \Longrightarrow$ F4 over $\mathbb{Z}/p_i\mathbb{Z}$ for all $(p_i)_{i\in\{1,\ldots,r\}}$ prime integers
2. For $p_2, \ldots, p_r$**,** re-use information from the computation for p_1

F4 Tracer

In Software [msolve 2021]**:** F4 is **traced** [Traverso 1989]

1. F4 over $\mathbb{Q} \Longrightarrow$ F4 over $\mathbb{Z}/p_i\mathbb{Z}$ for all $(p_i)_{i\in\{1,\dots,r\}}$ prime integers
2. For $p_2, \dots, p_r$, re-use information from the computation for p_1

Upper triangular

Reductors

S-polynomials

$$\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right) \Longrightarrow \left(\begin{array}{c|c} Id & A^{-1}B \\ \hline 0 & M \end{array}\right)$$

F4 Tracer

In Software [msolve 2021]**:** F4 is **traced** [Traverso 1989]

1. F4 over $\mathbb{Q} \Longrightarrow$ F4 over $\mathbb{Z}/p_i\mathbb{Z}$ for all $(p_i)_{i\in\{1,\dots,r\}}$ prime integers
2. For $p_2, \dots, p_r$, re-use information from the computation for p_1

Upper triangular

Reductors

S-polynomials

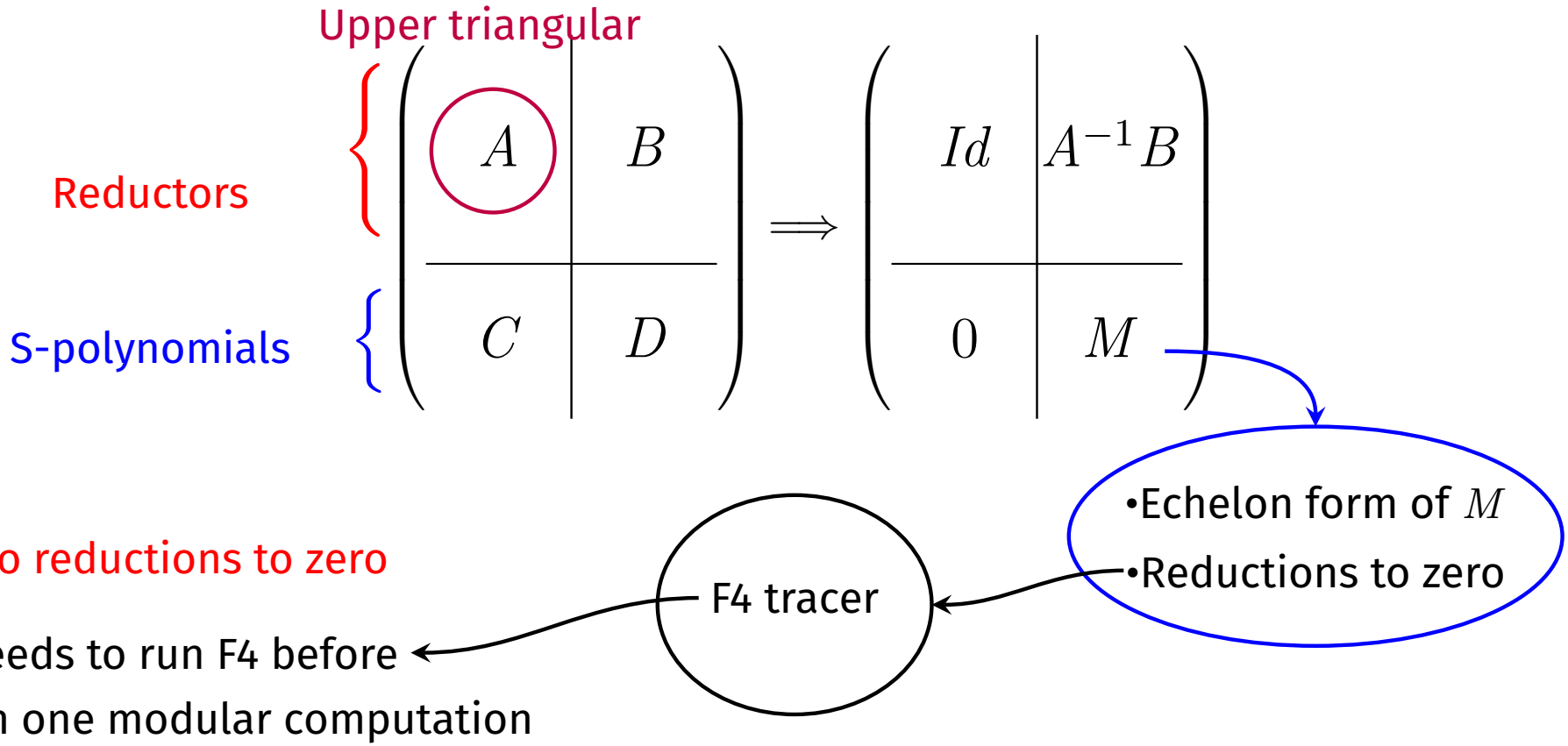
$$\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right) \Longrightarrow \left(\begin{array}{c|c} Id & A^{-1}B \\ \hline 0 & M \end{array}\right)$$

- Echelon form of M
- Reductions to zero

F4 Tracer

In Software [msolve 2021]**:** F4 is **traced** [Traverso 1989]

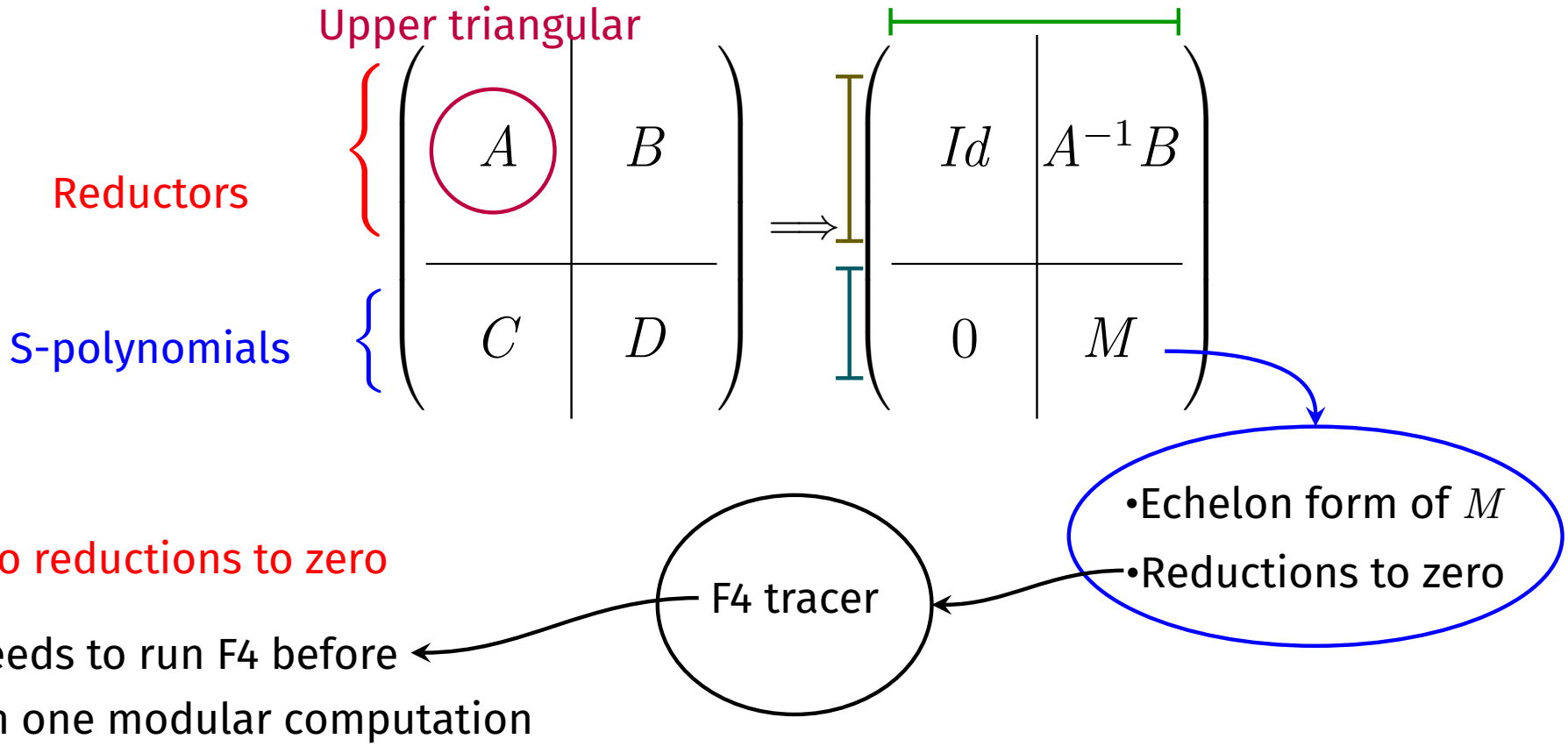
1. F4 over $\mathbb{Q} \Longrightarrow$ F4 over $\mathbb{Z}/p_i\mathbb{Z}$ for all $(p_i)_{i\in\{1,\ldots,r\}}$ prime integers
2. For $p_2, \ldots, p_r$, re-use information from the computation for p_1



F4 Tracer

In Software [msolve 2021]**:** F4 is **traced** [Traverso 1989]

1. F4 over $\mathbb{Q} \Longrightarrow$ F4 over $\mathbb{Z}/p_i\mathbb{Z}$ for all $(p_i)_{i\in\{1,\dots,r\}}$ prime integers
2. For $p_2, \dots, p_r$, re-use information from the computation for p_1



Complexity: $\mathcal{O}\left(\sharp(\text{new GB elements}) \times \sharp(\text{reductors}) \times \sharp(\text{support})\right)$

F5 Algorithm

A new signature system $\longrightarrow$

- No reductions to zero in the regular case
- Must compute Gröbner basis of $\langle f_1, \ldots, f_i \rangle$
- No fast linear algebra

F5 Algorithm

A new signature system $\longrightarrow$

- No reductions to zero in the regular case
- Must compute Gröbner basis of $\langle f_1, \ldots, f_i \rangle$
- No fast linear algebra

[Bardet, Faugère, Salvy, 2015]

Under generic assumptions, computing a grevlex Gröbner basis of $\langle f_1, \ldots, f_n \rangle \subset \mathbb{K}[x_1, \ldots x_n]$ takes

$$\underset{n \to +\infty}{\widetilde{\mathcal{O}}} \left(\delta^{3n} 3^n \right)$$

arithmetic operations in $\mathbb{K}$.

Conclusion

- Multivariate polynomial systems can encode a wide variety of situations.
- Gröbner bases are very helpful for eliminating variables and finding solutions to zero-dimensional systems.
- $F4/F5$ is a family of algorithms that compute Gröbner bases for which efficient implementations exist and have proven effective [msolve 2021], [GBLA 2016].

The work in my thesis:

- Understand the complexity of such algorithms in order to improve them.
- Use univariate polynomial matrix transformations (Popov forms) as a generalisation of echelon form to obtain new versions of these algorithms.