# Polynomial Division and Elimination Theory Over Finite Fields

Giulio Crisanti

Domodossola, 15/07/25

Based on upcoming work with

Vsevolod Chestnov

Centre for Theoretical Physics · Higgs

The University of Edinburgh

# Introduction and Motivation (1/1)

## Motivating Example

Consider

$$f(x) = x^3 + ax^2 - (5 + 2a)x + 1 \qquad\qquad p(x) = x^2 - 2x - 1$$

For $x^*$ s.t. $p(x^*) = 0$ what is $f(x^*)$ ?

# Introduction and Motivation (1/1)

## Motivating Example

Consider

$$f(x) = x^3 + ax^2 - (5+2a)x + 1 \qquad\qquad p(x) = x^2 - 2x - 1$$

For $x^*$ s.t. $p(x^*) = 0$ what is $f(x^*)$ ?

Normal Approach: $x^* = 1 \pm \sqrt{2}$ $\longrightarrow$

$$\begin{aligned} f(x^*) &= (1 \pm \sqrt{2})^3 + a(1 \pm \sqrt{2})^2 - (5+2a)(1 \pm \sqrt{2}) + 1 \\ &= 7 \pm 5\sqrt{2} + a(3 \pm 2\sqrt{2}) - (5+2a)(1 \pm \sqrt{2}) + 1 \\ &= 3 + a \end{aligned}$$

# Introduction and Motivation (1/1)

## Motivating Example

Consider

$$f(x) = x^3 + ax^2 - (5+2a)x + 1 \qquad\qquad p(x) = x^2 - 2x - 1$$

For $x^*$ s.t. $p(x^*) = 0$ what is $f(x^*)$ ?

Normal Approach: $x^* = 1 \pm \sqrt{2}$ → 

$$\begin{aligned} f(x^*) &= (1 \pm \sqrt{2})^3 + a(1 \pm \sqrt{2})^2 - (5+2a)(1 \pm \sqrt{2}) + 1 \\ &= 7 \pm 5\sqrt{2} + a(3 \pm 2\sqrt{2}) - (5+2a)(1 \pm \sqrt{2}) + 1 \\ &= 3 + a \end{aligned}$$

→ Rational Expression!

What if this example was more complicated (quintics and beyond)? Is there a fully rational way to obtain this result? Yes! — Polynomial division

# Introduction and Motivation (1/1)

## Motivating Example

Consider

$$f(x) = x^3 + ax^2 - (5+2a)x + 1 \qquad\qquad p(x) = x^2 - 2x - 1$$

For $x^*$ s.t. $p(x^*) = 0$ what is $f(x^*)$ ?

Normal Approach: $x^* = 1 \pm \sqrt{2}$ $\longrightarrow$

$$\begin{aligned} f(x^*) &= (1 \pm \sqrt{2})^3 + a(1 \pm \sqrt{2})^2 - (5+2a)(1 \pm \sqrt{2}) + 1 \\ &= 7 \pm 5\sqrt{2} + a(3 \pm 2\sqrt{2}) - (5+2a)(1 \pm \sqrt{2}) + 1 \\ &= 3 + a \end{aligned}$$

Rational Expression!

What if this example was more complicated (quintics and beyond)? Is there a fully rational way to obtain this result? Yes! — Polynomial division

$$f(x) = 3 + a \mod p(x)$$

Philosophy: Polynomial division can often solve problems without *explicitly* needing to solve polynomial systems

# Review of Polynomial Division (1/2)

## Quick Summary

Polynomial division allows us to decompose functions as

$$f(x) = q(x)p(x) + r(x)$$

$$\updownarrow$$

$$f(x) = r(x) \mod p(x)$$

# Review of Polynomial Division (1/2)

## Quick Summary

Polynomial division allows us to decompose functions as

$$f(x) = q(x)p(x) + r(x)$$

$\deg(r) < \deg(p)$

$$f(x) = r(x) \mod p(x)$$

# Review of Polynomial Division (1/2)

## Quick Summary

Polynomial division allows us to decompose functions as

$$f(x) = q(x)p(x) + r(x)$$

$\deg(r) < \deg(p)$

$$f(x) = r(x) \mod p(x)$$

Can always be done — best seen by example!

$$f(x) = x^3 + ax^2 - (5 + 2a)x + 1$$

$$p(x) = x^2 - 2x - 1 \longrightarrow x^2 = p(x) + 2x + 1$$

# Review of Polynomial Division (1/2)

## Quick Summary

Polynomial division allows us to decompose functions as

$$f(x) = q(x)p(x) + r(x)$$

$\deg(r) < \deg(p)$

$\updownarrow$

$$f(x) = r(x) \mod p(x)$$

Can always be done — best seen by example!

$$f(x) = x^3 + ax^2 - (5 + 2a)x + 1 \qquad p(x) = x^2 - 2x - 1 \longrightarrow x^2 = p(x) + 2x + 1$$

$$\begin{aligned}
f(x) &= x\left(p(x) + 2x + 1\right) + a\left(p(x) + 2x + 1\right) - (5 + 2a)x + 1 \\
&= p(x)(x + a) + 2x^2 + x + 2ax + a - 5x - 2ax + 1 \\
&= p(x)(x + a) + 2x^2 + a - 4x + 1 \\
&= p(x)(x + a) + 2(p(x) + 2x + 1) + a - 4x + 1 \\
&= p(x)(x + a + 2) + 4x + 2 + a - 4x + 1 \\
&= p(x)(x + a + 2) + a + 3
\end{aligned}$$

# Review of Polynomial Division (2/2)

## How does polynomial division solve the problem from a few slides back?

For $x^*$ s.t. $p(x^*) = 0$ what is $f(x^*)$?

$$f(x) = q(x)p(x) + r(x)$$

# Review of Polynomial Division (2/2)

## How does polynomial division solve the problem from a few slides back?

For $x^*$ s.t. $p(x^*) = 0$ what is $f(x^*)$?

$$f(x) = q(x)p(x) + r(x)$$

$$\downarrow$$

$$f(x^*) = q(x^*)p(x^*) + r(x^*) = r(x^*) = 3 + a$$

# Review of Polynomial Division (2/2)

## How does polynomial division solve the problem from a few slides back?

For $x^*$ s.t. $p(x^*) = 0$ what is $f(x^*)$?

$$f(x) = q(x)p(x) + r(x)$$

$$f(x^*) = q(x^*)\cancel{p(x^*)}^{\,0} + r(x^*) = r(x^*) = 3 + a$$

# Review of Polynomial Division (2/2)

## How does polynomial division solve the problem from a few slides back?

For $x^*$ s.t. $p(x^*) = 0$ what is $f(x^*)$?

$$f(x) = q(x)p(x) + r(x)$$

$$f(x^*) = q(x^*)\underbrace{p(x^*)}_{0} + r(x^*) = r(x^*) = 3 + a$$

## What about for irrational solutions?

$$\tilde{f}(x) = f(x) + x$$

# Review of Polynomial Division (2/2)

## How does polynomial division solve the problem from a few slides back?

For $x^*$ s.t. $p(x^*) = 0$ what is $f(x^*)$?

$$f(x) = q(x)p(x) + r(x)$$

$$f(x^*) = q(x^*)\underbrace{p(x^*)}_{0} + r(x^*) = r(x^*) = 3 + a$$

## What about for irrational solutions?

$$\tilde{f}(x) = f(x) + x \longrightarrow \tilde{r}(x) = r(x) + x = 3 + a + x$$

# Review of Polynomial Division (2/2)

## How does polynomial division solve the problem from a few slides back?

For $x^*$ s.t. $p(x^*) = 0$ what is $f(x^*)$?

$$f(x) = q(x)p(x) + r(x)$$

$$f(x^*) = q(x^*)\underbrace{p(x^*)}_{0} + r(x^*) = r(x^*) = 3 + a$$

## What about for irrational solutions?

$$\tilde{f}(x) = f(x) + x \longrightarrow \tilde{r}(x) = r(x) + x = 3 + a + x$$

$$\tilde{f}(x^*) = \tilde{r}(x^*) = 3 + a + x^* = 4 \pm \sqrt{2}$$

no root cancellations needed

# Review of Polynomial Division (2/2)

## How does polynomial division solve the problem from a few slides back?

For $x^*$ s.t. $p(x^*) = 0$ what is $f(x^*)$?

$$f(x) = q(x)p(x) + r(x)$$

$$f(x^*) = q(x^*)\underbrace{p(x^*)}_{0} + r(x^*) = r(x^*) = 3 + a$$

## What about for irrational solutions?

$$\tilde{f}(x) = f(x) + x \longrightarrow \tilde{r}(x) = r(x) + x = 3 + a + x$$

$$\tilde{f}(x^*) = \tilde{r}(x^*) = 3 + a + x^* = 4 \pm \sqrt{2}$$

no root cancellations needed

## Can also apply the same techniques to rational functions

Define inverses as: $\frac{1}{g(x)} := g_{\text{inv}}(x) \mod p(x) \longleftrightarrow g(x)g_{\text{inv}}(x) = 1 \mod p(x)$

# Review of Polynomial Division (2/2)

## How does polynomial division solve the problem from a few slides back?

For $x^*$ s.t. $p(x^*) = 0$ what is $f(x^*)$?

$$f(x) = q(x)p(x) + r(x)$$

$$f(x^*) = q(x^*)\underbrace{p(x^*)}_{0} + r(x^*) = r(x^*) = 3 + a$$

## What about for irrational solutions?

$$\tilde{f}(x) = f(x) + x \longrightarrow \tilde{r}(x) = r(x) + x = 3 + a + x \qquad \tilde{f}(x^*) = \tilde{r}(x^*) = 3 + a + x^* = 4 \pm \sqrt{2}$$

no root cancellations needed

## Can also apply the same techniques to rational functions

Define inverses as: $$\frac{1}{g(x)} := g_{\text{inv}}(x) \mod p(x) \longleftrightarrow g(x)g_{\text{inv}}(x) = 1 \mod p(x)$$

Eg: $$\frac{1}{1+x^3} = \frac{13}{14} - \frac{5x}{14} \mod p(x)$$

# Review of Polynomial Division (2/2)

## How does polynomial division solve the problem from a few slides back?

For $x^*$ s.t. $p(x^*) = 0$ what is $f(x^*)$?

$$f(x) = q(x)p(x) + r(x)$$

$$f(x^*) = q(x^*)\underbrace{p(x^*)}_{0} + r(x^*) = r(x^*) = 3 + a$$

## What about for irrational solutions?

$$\tilde{f}(x) = f(x) + x \longrightarrow \tilde{r}(x) = r(x) + x = 3 + a + x \qquad \tilde{f}(x^*) = \tilde{r}(x^*) = 3 + a + x^* = 4 \pm \sqrt{2}$$

no root cancellations needed

## Can also apply the same techniques to rational functions

Define inverses as: $$\frac{1}{g(x)} := g_{\text{inv}}(x) \mod p(x) \longleftrightarrow g(x)g_{\text{inv}}(x) = 1 \mod p(x)$$

Eg: $$\frac{1}{1+x^3} = \frac{13}{14} - \frac{5x}{14} \mod p(x) \longrightarrow \frac{1}{1+(x^*)^3} = \frac{13}{14} - \frac{5x^*}{14} = \frac{1}{14}\left(8 \mp 5\sqrt{2}\right)$$

# Towards Finite Fields

## Polynomial division as row reduction

If all we care about is the remainder, we can work modulo $p(x)$ from the beginning

$$x^2 = p(x) + 2x + 1 \longrightarrow x^2 = 2x + 1 \mod p(x)$$

# Towards Finite Fields

## Polynomial division as row reduction

If all we care about is the remainder, we can work modulo $p(x)$ from the beginning

$$x^2 = p(x) + 2x + 1 \longrightarrow x^2 = 2x + 1 \mod p(x)$$

Can generate a linear system of equations this way

$$x^2 - 2x - 1 = 0 \mod p(x)$$
$$x^3 - 2x^2 - x = 0 \mod p(x)$$
$$\vdots$$

# Towards Finite Fields

## Polynomial division as row reduction

If all we care about is the remainder, we can work modulo $p(x)$ from the beginning

$$x^2 = p(x) + 2x + 1 \longrightarrow x^2 = 2x + 1 \mod p(x)$$

Can generate a linear system of equations this way

$$x^2 - 2x - 1 = 0 \mod p(x)$$
$$x^3 - 2x^2 - x = 0 \mod p(x)$$
$$\vdots$$
$$f(x) - x^3 - ax^2 + (5 + 2a)x + 1 = 0 \mod p(x)$$

# Towards Finite Fields

## Polynomial division as row reduction

If all we care about is the remainder, we can work modulo $p(x)$ from the beginning

$$x^2 = p(x) + 2x + 1 \longrightarrow x^2 = 2x + 1 \mod p(x)$$

Can generate a linear system of equations this way

$$x^2 - 2x - 1 = 0 \mod p(x)$$
$$x^3 - 2x^2 - x = 0 \mod p(x)$$
$$\vdots$$
$$f(x) - x^3 - ax^2 + (5 + 2a)x + 1 = 0 \mod p(x)$$

Cast in matrix form:

$$\begin{bmatrix} -1 & 1 & a & -(5+2a) & 1 \\ 0 & -1 & 2 & 1 & 0 \\ 0 & 0 & -1 & 2 & 1 \end{bmatrix} \begin{bmatrix} f(x) \\ x^3 \\ x^2 \\ x \\ 1 \end{bmatrix} = \mathbf{0}$$

# Towards Finite Fields

## Polynomial division as row reduction

If all we care about is the remainder, we can work modulo $p(x)$ from the beginning

$$x^2 = p(x) + 2x + 1 \longrightarrow x^2 = 2x + 1 \mod p(x)$$

Can generate a linear system of equations this way

$$x^2 - 2x - 1 = 0 \mod p(x)$$
$$x^3 - 2x^2 - x = 0 \mod p(x)$$
$$\vdots$$
$$f(x) - x^3 - ax^2 + (5 + 2a)x + 1 = 0 \mod p(x)$$

Cast in matrix form:

$$\begin{bmatrix} -1 & 1 & a & -(5+2a) & 1 \\ 0 & -1 & 2 & 1 & 0 \\ 0 & 0 & -1 & 2 & 1 \end{bmatrix} \begin{bmatrix} f(x) \\ x^3 \\ x^2 \\ x \\ 1 \end{bmatrix} = \mathbf{0} \xrightarrow{\text{RowRed}} \begin{bmatrix} 1 & 0 & 0 & 0 & -3-a \\ 0 & 1 & 0 & -5 & -2 \\ 0 & 0 & 1 & -2 & -1 \end{bmatrix} \begin{bmatrix} f(x) \\ x^3 \\ x^2 \\ x \\ 1 \end{bmatrix} = \mathbf{0}$$

# Towards Finite Fields

## Polynomial division as row reduction

If all we care about is the remainder, we can work modulo $p(x)$ from the beginning

$$x^2 = p(x) + 2x + 1 \longrightarrow x^2 = 2x + 1 \mod p(x)$$

Can generate a linear system of equations this way

$$x^2 - 2x - 1 = 0 \mod p(x)$$

$$x^3 - 2x^2 - x = 0 \mod p(x)$$

$$\vdots$$

$$f(x) - x^3 - ax^2 + (5 + 2a)x + 1 = 0 \mod p(x)$$

Cast in matrix form:

$$\begin{bmatrix} -1 & 1 & a & -(5+2a) & 1 \\ 0 & -1 & 2 & 1 & 0 \\ 0 & 0 & -1 & 2 & 1 \end{bmatrix} \begin{bmatrix} f(x) \\ x^3 \\ x^2 \\ x \\ 1 \end{bmatrix} = \mathbf{0} \xrightarrow{\text{RowRed}} \begin{bmatrix} 1 & 0 & 0 & 0 & -3-a \\ 0 & 1 & 0 & -5 & -2 \\ 0 & 0 & 1 & -2 & -1 \end{bmatrix} \begin{bmatrix} f(x) \\ x^3 \\ x^2 \\ x \\ 1 \end{bmatrix} = \mathbf{0}$$

(First row of reduced matrix:) $f(x) - 3 - a = 0 \mod p(x)$

# Towards Finite Fields

## Polynomial division as row reduction

If all we care about is the remainder, we can work modulo $p(x)$ from the beginning

$$x^2 = p(x) + 2x + 1 \longrightarrow x^2 = 2x + 1 \mod p(x)$$

Can generate a linear system of equations this way

$$x^2 - 2x - 1 = 0 \mod p(x)$$
$$x^3 - 2x^2 - x = 0 \mod p(x)$$
$$\vdots$$
$$f(x) - x^3 - ax^2 + (5+2a)x + 1 = 0 \mod p(x)$$

Cast in matrix form:

$$\begin{bmatrix} -1 & 1 & a & -(5+2a) & 1 \\ 0 & -1 & 2 & 1 & 0 \\ 0 & 0 & -1 & 2 & 1 \end{bmatrix} \begin{bmatrix} f(x) \\ x^3 \\ x^2 \\ x \\ 1 \end{bmatrix} = \mathbf{0} \xrightarrow{\text{RowRed}} \begin{bmatrix} 1 & 0 & 0 & 0 & -3-a \\ 0 & 1 & 0 & -5 & -2 \\ 0 & 0 & 1 & -2 & -1 \end{bmatrix} \begin{bmatrix} f(x) \\ x^3 \\ x^2 \\ x \\ 1 \end{bmatrix} = \mathbf{0}$$

(first row of the reduced matrix:) $f(x) - 3 - a = 0 \mod p(x)$

Useful because there exist very quick ways to do row reduction: Sample over finite fields and reconstruct output

# Finite Field Reconstruction

## Operations on Matrices

$$\mathbb{M}(a_1, \cdots, a_n)$$

# Finite Field Reconstruction

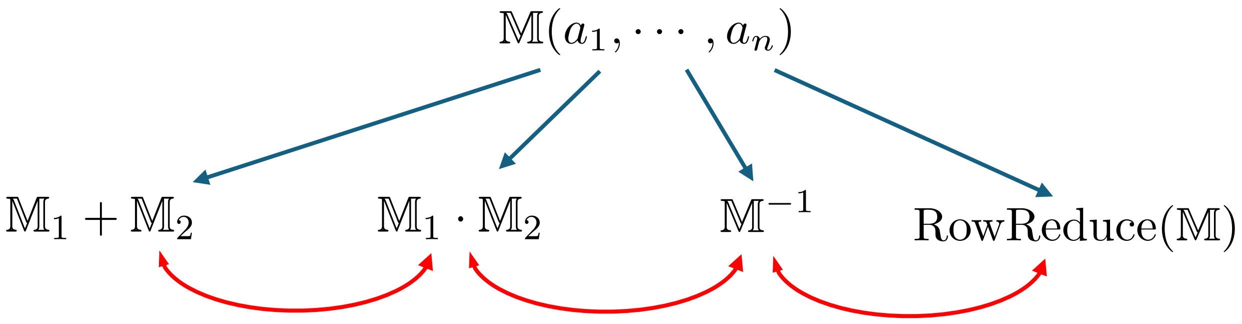
## Operations on Matrices

$$\mathbb{M}(a_1, \cdots, a_n)$$

$$\mathbb{M}_1 + \mathbb{M}_2 \qquad \mathbb{M}_1 \cdot \mathbb{M}_2 \qquad \mathbb{M}^{-1} \qquad \mathrm{RowReduce}(\mathbb{M})$$

# Finite Field Reconstruction

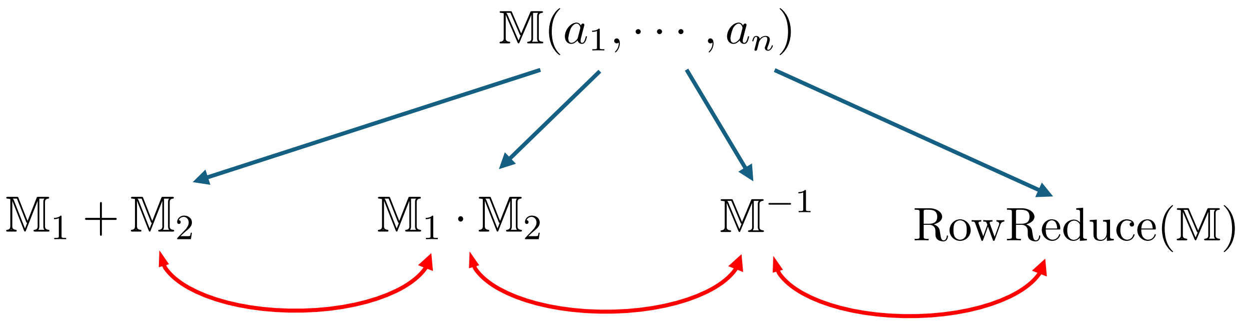
## Operations on Matrices




Algebraic post processing simplification — can become very intensive!

# Finite Field Reconstruction

## Operations on Matrices



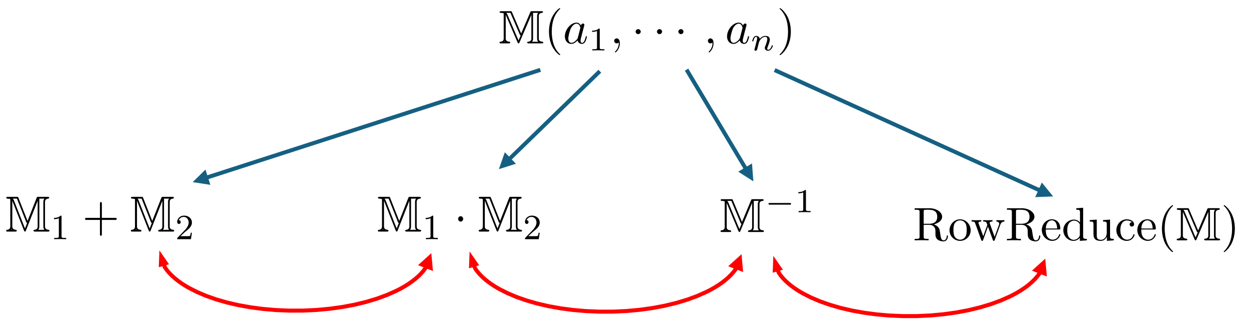

Algebraic post processing simplification — can become very intensive!

## Finite Fields Approach

Substitute numerical values for parameters → Perform all operations numerically mod primes → Reconstruct functional output from numerical sampling

# Finite Field Reconstruction

## Operations on Matrices




Algebraic post processing simplification — can become very intensive!

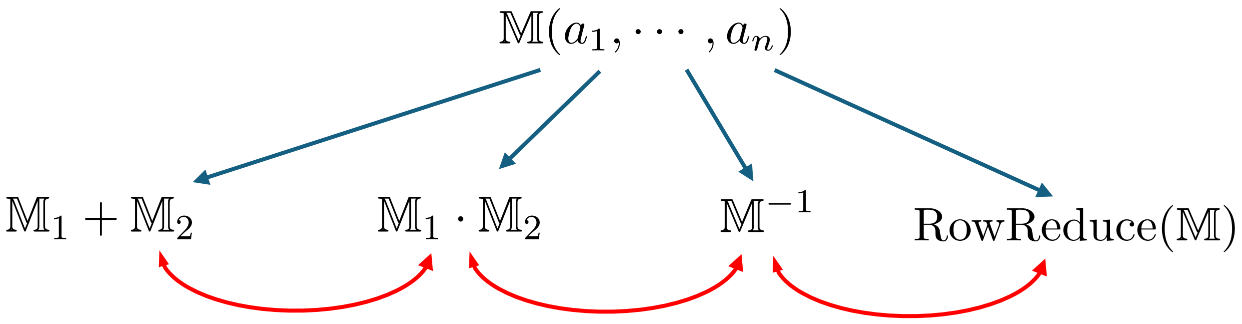
## Finite Fields Approach

Substitute numerical values for parameters → Perform all operations numerically mod primes → Reconstruct functional output from numerical sampling

Complicated cancellations will happen numerically — final reconstructed output already “simplified” [FiniteFlow, Peraro, 2019]

# Finite Field Reconstruction

## Operations on Matrices




Algebraic post processing simplification — can become very intensive!

## Finite Fields Approach

Substitute numerical values for parameters → Perform all operations numerically mod primes → Reconstruct functional output from numerical sampling

Complicated cancellations will happen numerically — final reconstructed output already "simplified"

[FiniteFlow, Peraro, 2019]

## What is reconstructed?

$$f(x) = x^3 + ax^2 - (5+2a)x + 1$$
$$p(x) = x^2 - 2x - 1$$

$$\begin{bmatrix} -1 & 1 & a & -(5+2a) & 1 \\ 0 & -1 & 2 & 1 & 0 \\ 0 & 0 & -1 & 2 & 1 \end{bmatrix} \begin{bmatrix} f(x) \\ x^3 \\ x^2 \\ x \\ 1 \end{bmatrix} = \mathbf{0}$$

# Finite Field Reconstruction

## Operations on Matrices

$$\mathbb{M}(a_1, \cdots, a_n)$$

$$\mathbb{M}_1 + \mathbb{M}_2 \qquad \mathbb{M}_1 \cdot \mathbb{M}_2 \qquad \mathbb{M}^{-1} \qquad \mathrm{RowReduce}(\mathbb{M})$$

Algebraic post processing simplification — can become very intensive!

## Finite Fields Approach

Substitute numerical values for parameters → Perform all operations numerically mod primes → Reconstruct functional output from numerical sampling

Complicated cancellations will happen numerically — final reconstructed output already "simplified"

[FiniteFlow, Peraro, 2019]

## What is reconstructed?

$$f(x) = x^3 + ax^2 - (5+2a)x + 1$$
$$p(x) = x^2 - 2x - 1$$

$$\begin{bmatrix} -1 & 1 & a & -(5+2a) & 1 \\ 0 & -1 & 2 & 1 & 0 \\ 0 & 0 & -1 & 2 & 1 \end{bmatrix} \begin{bmatrix} f(x) \\ x^3 \\ x^2 \\ x \\ 1 \end{bmatrix} = \mathbf{0}$$

parameters

variables

$$R = \mathbb{Q}[a][x]$$

Only need to reconstruct parameters!

# Multivariate Polynomial Division (1/3)

## Monomial Orderings

For one variable, sorting the monomials from “worst” to “best” is unambiguous

$$x^n > x^{n-1} > \cdots > x^3 > x^2 > x > 1$$

# Multivariate Polynomial Division (1/3)

## Monomial Orderings

For one variable, sorting the monomials from “worst” to “best” is unambiguous

$$x^n > x^{n-1} > \cdots > x^3 > x^2 > x > 1$$

For more than one variable there are multiple choices one can take

$$x > y$$

# Multivariate Polynomial Division (1/3)

## Monomial Orderings

For one variable, sorting the monomials from “worst” to “best” is unambiguous

$$x^n > x^{n-1} > \cdots > x^3 > x^2 > x > 1$$

For more than one variable there are multiple choices one can take

$x > y$ → Lexicographic: $\cdots > x^2 > xy^\infty > xy > x > y^\infty > \cdots > y > 1$

# Multivariate Polynomial Division (1/3)

## Monomial Orderings

For one variable, sorting the monomials from “worst” to “best” is unambiguous

$$x^n > x^{n-1} > \cdots > x^3 > x^2 > x > 1$$

For more than one variable there are multiple choices one can take

$x > y$

- Lexicographic: $\cdots > x^2 > xy^\infty > xy > x > y^\infty > \cdots > y > 1$
- Degree Lexicographic: $\cdots > y^3 > x^2 > xy > y^2 > x > y > 1$

# Multivariate Polynomial Division (1/3)

## Monomial Orderings

For one variable, sorting the monomials from "worst" to "best" is unambiguous

$$x^n > x^{n-1} > \cdots > x^3 > x^2 > x > 1$$

For more than one variable there are multiple choices one can take

Assume for rest of talk

$x > y$

- Lexicographic: $\cdots > x^2 > xy^\infty > xy > x > y^\infty > \cdots > y > 1$
- Degree Lexicographic: $\cdots > y^3 > x^2 > xy > y^2 > x > y > 1$

# Multivariate Polynomial Division (1/3)

## Monomial Orderings

For one variable, sorting the monomials from "worst" to "best" is unambiguous

$$x^n > x^{n-1} > \cdots > x^3 > x^2 > x > 1$$

For more than one variable there are multiple choices one can take

Assume for rest of talk

$x > y$

Lexicographic: $\cdots > x^2 > xy^\infty > xy > x > y^\infty > \cdots > y > 1$

Degree Lexicographic: $\cdots > y^3 > x^2 > xy > y^2 > x > y > 1$

## Is the division unique?

Unfortunately, this is not enough to uniquely determine a multivariate polynomial division

Consider $I = \langle xy - x, xy - y - 1 \rangle$. What is $x\,y = \ ? \mod I$

# Multivariate Polynomial Division (1/3)

## Monomial Orderings

For one variable, sorting the monomials from "worst" to "best" is unambiguous

$$x^n > x^{n-1} > \cdots > x^3 > x^2 > x > 1$$

For more than one variable there are multiple choices one can take

Assume for rest of talk

$x > y$

Lexicographic: $\cdots > x^2 > xy^\infty > xy > x > y^\infty > \cdots > y > 1$

Degree Lexicographic: $\cdots > y^3 > x^2 > xy > y^2 > x > y > 1$

## Is the division unique?

Unfortunately, this is not enough to uniquely determine a multivariate polynomial division

Consider $I = \langle xy - x, xy - y - 1 \rangle$. What is $x\,y = \;?\; \mod I$

$$xy = x \mod I$$

# Multivariate Polynomial Division (1/3)

## Monomial Orderings

For one variable, sorting the monomials from "worst" to "best" is unambiguous

$$x^n > x^{n-1} > \cdots > x^3 > x^2 > x > 1$$

For more than one variable there are multiple choices one can take

Assume for rest of talk

$x > y$

Lexicographic: $\cdots > x^2 > xy^\infty > xy > x > y^\infty > \cdots > y > 1$

Degree Lexicographic: $\cdots > y^3 > x^2 > xy > y^2 > x > y > 1$

## Is the division unique?

Unfortunately, this is not enough to uniquely determine a multivariate polynomial division

Consider $I = \langle xy - x, xy - y - 1 \rangle$. What is $x\,y = \ ? \mod I$

$xy = x \mod I$ $\qquad$ $xy = y + 1 \mod I$

Problem normally fixed by introducing Groebner Bases

[Buchberger, 1965]

# Multivariate Polynomial Division (2/3)

## Groebner Bases

A Groebner basis $G$ is a set of polynomials obtained from $I$ that has many nice properties

# Multivariate Polynomial Division (2/3)

## Groebner Bases

A Groebner basis $G$ is a set of polynomials obtained from $I$ that has many nice properties

For this talk: Roots of $G = 0$ are the same as $I = 0$, and polynomial division ambiguities fixed

# Multivariate Polynomial Division (2/3)

## Groebner Bases

A Groebner basis $G$ is a set of polynomials obtained from $I$ that has many nice properties

For this talk: Roots of $G = 0$ are the same as $I = 0$, and polynomial division ambiguities fixed

$$I = \langle xy - x, xy - y - 1 \rangle \longrightarrow G = \langle y^2 - 1, x - y - 1 \rangle \quad \text{(Lexicograhpic)}$$

Any possible combination of the elements of $G$ will result in the same polynomial remainder

# Multivariate Polynomial Division (2/3)

## Groebner Bases

A Groebner basis $G$ is a set of polynomials obtained from $I$ that has many nice properties

For this talk: Roots of $G = 0$ are the same as $I = 0$, and polynomial division ambiguities fixed

$$I = \langle xy - x, xy - y - 1 \rangle \longrightarrow G = \langle y^2 - 1, x - y - 1 \rangle \quad \text{(Lexicograhpic)}$$

Any possible combination of the elements of $G$ will result in the same polynomial remainder

$$xy \overset{2}{=} (y+1)y = y + y^2 \overset{1}{=} y + 1 \mod G$$

# Multivariate Polynomial Division (2/3)

## Groebner Bases

A Groebner basis $G$ is a set of polynomials obtained from $I$ that has many nice properties

For this talk: Roots of $G = 0$ are the same as $I = 0$, and polynomial division ambiguities fixed

$$I = \langle xy - x, xy - y - 1 \rangle \longrightarrow G = \langle y^2 - 1, x - y - 1 \rangle$$ (Lexicograhpic)

Any possible combination of the elements of $G$ will result in the same polynomial remainder

$$xy \overset{2}{=} (y+1)y = y + y^2 \overset{1}{=} y + 1 \mod G$$

$$\begin{aligned} xy^2 &\overset{1}{=} x \overset{2}{=} y + 1 \\ xy^2 &\overset{2}{=} (y+1)y^2 \overset{1}{=} y + 1 \end{aligned} \mod G$$

# Multivariate Polynomial Division (2/3)

## Groebner Bases

A Groebner basis $G$ is a set of polynomials obtained from $I$ that has many nice properties

For this talk: Roots of $G = 0$ are the same as $I = 0$, and polynomial division ambiguities fixed

$$I = \langle xy - x, xy - y - 1 \rangle \longrightarrow G = \langle y^2 - 1, x - y - 1 \rangle$$ (Lexicograhpic)

Any possible combination of the elements of $G$ will result in the same polynomial remainder

$$xy \overset{2}{=} (y+1)y = y + y^2 \overset{1}{=} y + 1 \mod G$$

$$\begin{aligned} xy^2 &\overset{1}{=} x \overset{2}{=} y + 1 \\ xy^2 &\overset{2}{=} (y+1)y^2 \overset{1}{=} y + 1 \end{aligned} \mod G$$

Groebner bases can be very difficult to calculate and are often computational bottlenecks!

# Multivariate Polynomial Division (2/3)

## Groebner Bases

A Groebner basis $G$ is a set of polynomials obtained from $I$ that has many nice properties

For this talk: Roots of $G = 0$ are the same as $I = 0$, and polynomial division ambiguities fixed

$$I = \langle xy - x, xy - y - 1 \rangle \longrightarrow G = \langle y^2 - 1, x - y - 1 \rangle$$ (Lexicograhpic)

Any possible combination of the elements of $G$ will result in the same polynomial remainder

$$xy \overset{2}{=} (y+1)y = y + y^2 \overset{1}{=} y + 1 \quad \mathrm{mod}\ G$$

$$\begin{aligned} xy^2 &\overset{1}{=} x \overset{2}{=} y + 1 \\ xy^2 &\overset{2}{=} (y+1)y^2 \overset{1}{=} y + 1 \end{aligned} \quad \mathrm{mod}\ G$$

Groebner bases can be very difficult to calculate and are often computational bottlenecks!

## Avoiding Groebner Bases

Claim: We can explicitly avoid computing a Groebner basis, and still obtain the correct result from polynomial division, using row reduction [Faugére, 1999] [Buchberger, 1985]

Allows us to compute polynomial divisions without needing to reconstruct the “intermediate” Groebner Basis

# Multivariate Polynomial Division (3/3)

## Row Reduction Again

We consider again $I = \langle xy - x, xy - y - 1 \rangle$ and let $f(x, y) = xy^2$

# Multivariate Polynomial Division (3/3)

## Row Reduction Again

We consider again $I = \langle xy - x, xy - y - 1 \rangle$ and let $f(x,y) = xy^2$

Seed a linear system by multiplying $I$ by $x^n y^m$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & -1 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} f(x) \\ x^2y^2 \\ x^2y \\ x^2 \\ xy^2 \\ xy \\ x \\ y^2 \\ y \\ 1 \end{bmatrix}$$

# Multivariate Polynomial Division (3/3)

## Row Reduction Again

We consider again $I = \langle xy - x, xy - y - 1 \rangle$ and let $f(x,y) = xy^2$

Seed a linear system by multiplying $I$ by $x^n y^m$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & -1 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} f(x) \\ x^2y^2 \\ x^2y \\ x^2 \\ xy^2 \\ xy \\ x \\ y^2 \\ y \\ 1 \end{bmatrix} \xrightarrow{\text{RowRed}} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & -2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -2 & -2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -2 & -2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} f(x) \\ x^2y^2 \\ x^2y \\ x^2 \\ xy^2 \\ xy \\ x \\ y^2 \\ y \\ 1 \end{bmatrix}$$

# Multivariate Polynomial Division (3/3)

## Row Reduction Again

We consider again $I = \langle xy - x, xy - y - 1 \rangle$ and let $f(x,y) = xy^2$

Seed a linear system by multiplying $I$ by $x^n y^m$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & -1 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} f(x) \\ x^2y^2 \\ x^2y \\ x^2 \\ xy^2 \\ xy \\ x \\ y^2 \\ y \\ 1 \end{bmatrix} \xrightarrow{\text{RowRed}} \left[\begin{array}{cccccccc:cc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & -2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -2 & -2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -2 & -2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right] \begin{bmatrix} f(x) \\ x^2y^2 \\ x^2y \\ x^2 \\ xy^2 \\ xy \\ x \\ y^2 \\ \hdashline y \\ 1 \end{bmatrix}$$

Irreducible monomials

Read off from top row: $f(x,y) = y + 1 \mod I$ No explicit Groebner Basis required!

# Multivariate Polynomial Division (3/3)

## Row Reduction Again

We consider again $I = \langle xy - x, xy - y - 1 \rangle$ and let $f(x,y) = xy^2$

Seed a linear system by multiplying $I$ by $x^n y^m$

$$
\begin{bmatrix}
1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & -1 \\
0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0
\end{bmatrix}
\begin{bmatrix} f(x) \\ x^2y^2 \\ x^2y \\ x^2 \\ xy^2 \\ xy \\ x \\ y^2 \\ y \\ 1 \end{bmatrix}
\xrightarrow{\text{RowRed}}
\left[\begin{array}{cccccccc:cc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & -2 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -2 & -2 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -2 & -2 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & -1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right]
\left[\begin{array}{c} f(x) \\ x^2y^2 \\ x^2y \\ x^2 \\ xy^2 \\ xy \\ x \\ y^2 \\ \hdashline y \\ 1 \end{array}\right]
$$

Irreducible monomials

Read off from top row: $f(x,y) = y + 1 \mod I$ No explicit Groebner Basis required!

Process can again be implemented in finite fields, with a reconstruction step at the end.

# Project Summary

## Program Overview

A (Mathematica) package that performs polynomial division over finite fields

# Project Summary

## Program Overview

A (Mathematica) package that performs polynomial division over finite fields

No intermediate reconstructions required — only reconstructs the final result, ensuring the numerical cancellations of complex intermediate stages

# Project Summary

## Program Overview

A (Mathematica) package that performs polynomial division over finite fields

No intermediate reconstructions required — only reconstructs the final result, ensuring the numerical cancellations of complex intermediate stages

Can handle polynomials or multivariate rational functions as input to arbitrary nested depth

# Project Summary

## Program Overview

A (Mathematica) package that performs polynomial division over finite fields

No intermediate reconstructions required — only reconstructs the final result, ensuring the numerical cancellations of complex intermediate stages

Can handle polynomials or multivariate rational functions as input to arbitrary nested depth

Functionality not present in Mathematica even with symbolic processing!

# Project Summary

## Program Overview

A (Mathematica) package that performs polynomial division over finite fields

No intermediate reconstructions required — only reconstructs the final result, ensuring the numerical cancellations of complex intermediate stages

Can handle polynomials or multivariate rational functions as input to arbitrary nested depth

Functionality not present in Mathematica even with symbolic processing!

Inputs and outputs:

$$I = \langle p_1(x_1, \cdots, x_n), \cdots, p_n(x_1, \cdots, x_n) \rangle \qquad f(x_1, \cdots, x_n)$$

# Project Summary

## Program Overview

A (Mathematica) package that performs polynomial division over finite fields

No intermediate reconstructions required — only reconstructs the final result, ensuring the numerical cancellations of complex intermediate stages

Can handle polynomials or multivariate rational functions as input to arbitrary nested depth

Functionality not present in Mathematica even with symbolic processing!

Inputs and outputs:

$$I = \langle p_1(x_1, \cdots, x_n), \cdots, p_n(x_1, \cdots, x_n) \rangle$$

$$f(x_1, \cdots, x_n)$$

Row reduction for companion matrix construction

$$M_{x_1}, \cdots, M_{x_n}$$

# Project Summary

## Program Overview

A (Mathematica) package that performs polynomial division over finite fields

No intermediate reconstructions required — only reconstructs the final result, ensuring the numerical cancellations of complex intermediate stages

Can handle polynomials or multivariate rational functions as input to arbitrary nested depth

Functionality not present in Mathematica even with symbolic processing!

Inputs and outputs:

$$I = \langle p_1(x_1, \cdots, x_n), \cdots, p_n(x_1, \cdots, x_n) \rangle$$

Row reduction for companion matrix construction

$$M_{x_1}, \cdots, M_{x_n}$$

$$f(x_1, \cdots, x_n)$$

Recursive parsing into companion matrix form

$$M_{f(x_1 \cdots x_n)}$$

# Project Summary

## Program Overview

A (Mathematica) package that performs polynomial division over finite fields

No intermediate reconstructions required — only reconstructs the final result, ensuring the numerical cancellations of complex intermediate stages

Can handle polynomials or multivariate rational functions as input to arbitrary nested depth

Functionality not present in Mathematica even with symbolic processing!

Inputs and outputs:

$$I = \langle p_1(x_1, \cdots, x_n), \cdots, p_n(x_1, \cdots, x_n) \rangle$$

Row reduction for companion matrix construction

$$M_{x_1}, \cdots, M_{x_n}$$

$$f(x_1, \cdots, x_n)$$

Recursive parsing into companion matrix form

$$M_{f(x_1 \cdots x_n)}$$

Finite Field Reconstruction

$$f(x_1, \cdots, x_n) = r(x_1, \cdots, x_n) \mod I$$

# Examples (1/5)

## Elimination Theory

Consider the following setup:

$$I = \langle p_1(x_1, \cdots, x_n), \cdots, p_n(x_1, \cdots, x_n) \rangle \qquad x_n > \cdots > x_1$$ (+ lexicograhpic ordering)

# Examples (1/5)

## Elimination Theory

Consider the following setup:

$$I = \langle p_1(x_1, \cdots, x_n), \cdots, p_n(x_1, \cdots, x_n) \rangle \qquad x_n > \cdots > x_1$$ (+ lexicograhpic ordering)

Polynomial division allows one to eliminate variables from a polynomial system:

$$x_1^m \mod I$$

# Examples (1/5)

## Elimination Theory

Consider the following setup:

$$I = \langle p_1(x_1, \cdots, x_n), \cdots, p_n(x_1, \cdots, x_n) \rangle \qquad x_n > \cdots > x_1 \quad \text{(+ lexicograhpic ordering)}$$

Polynomial division allows one to eliminate variables from a polynomial system:

$$x_1^m \mod I \rightarrow = x_1^m \qquad \text{(irreducible monomial)}$$

# Examples (1/5)

## Elimination Theory

Consider the following setup:

$$I = \langle p_1(x_1, \cdots, x_n), \cdots, p_n(x_1, \cdots, x_n) \rangle \qquad x_n > \cdots > x_1 \quad \text{(+ lexicograhpic ordering)}$$

Polynomial division allows one to eliminate variables from a polynomial system:

$$x_1^m \mod I \;\to\; = x_1^m \qquad \text{(irreducible monomial)}$$

$$x_1^m \mod I \;\to\; = r(x_1) = c_0 + \cdots c_a x_1^a \qquad a < m \qquad \text{(polynomially reduced)}$$

# Examples (1/5)

## Elimination Theory

Consider the following setup:

$$I = \langle p_1(x_1, \cdots, x_n), \cdots, p_n(x_1, \cdots, x_n) \rangle \qquad x_n > \cdots > x_1$$ (+ lexicograhpic ordering)

Polynomial division allows one to eliminate variables from a polynomial system:

$$x_1^m \mod I \;\to\; = x_1^m$$ (irreducible monomial)

$$x_1^m \mod I \;\to\; = r(x_1) = c_0 + \cdots c_a x_1^a \qquad a < m$$ (polynomially reduced)

only a function of $x_1$ because $\{x_n, \cdots, x_2\} > x_1^\infty$

# Examples (1/5)

## Elimination Theory

Consider the following setup:

$$I = \langle p_1(x_1, \cdots, x_n), \cdots, p_n(x_1, \cdots, x_n) \rangle \qquad x_n > \cdots > x_1 \quad \text{(+ lexicograhpic ordering)}$$

Polynomial division allows one to eliminate variables from a polynomial system:

$$x_1^m \mod I \rightarrow = x_1^m \qquad \text{(irreducible monomial)}$$

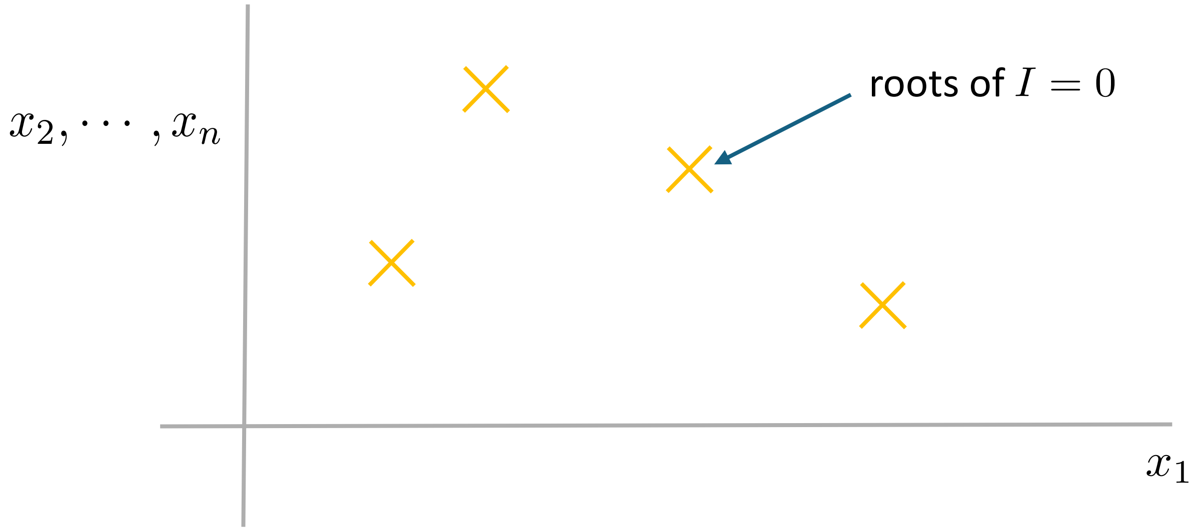
$$x_1^m \mod I \rightarrow = r(x_1) = c_0 + \cdots c_a x_1^a \qquad a < m \qquad \text{(polynomially reduced)}$$

only a function of $x_1$ because $\{x_n, \cdots, x_2\} > x_1^\infty$

Combining: $f(x_1) = x_1^m - r(x_1)$

$$\downarrow$$

$$f(x_1) = 0 \mod I$$



# Examples (1/5)

## Elimination Theory

Consider the following setup:

$$I = \langle p_1(x_1, \cdots, x_n), \cdots, p_n(x_1, \cdots, x_n) \rangle \qquad x_n > \cdots > x_1 \quad \text{(+ lexicograhpic ordering)}$$

Polynomial division allows one to eliminate variables from a polynomial system:

$$x_1^m \mod I \;\to\; = x_1^m \qquad \text{(irreducible monomial)}$$

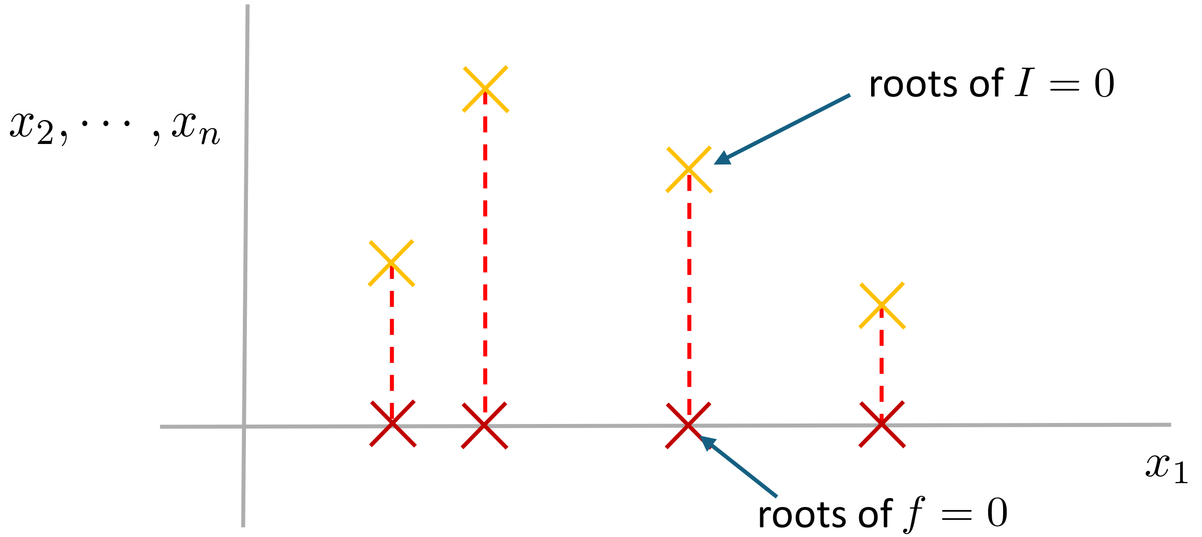
$$x_1^m \mod I \;\to\; = r(x_1) = c_0 + \cdots c_a x_1^a \qquad a < m \qquad \text{(polynomially reduced)}$$

only a function of $x_1$ because $\{x_n, \cdots, x_2\} > x_1^\infty$

equation for the roots in $x_1$ only

Combining: $f(x_1) = x_1^m - r(x_1)$

$$f(x_1) = 0 \mod I$$



# Examples (2/5)

## Elimination Benchmarking (Preliminary)

$$R = \mathbb{Q}[a, b, c, d][x, y, z]$$

$$I = \langle a + x^2y^2 + y^3 + z - 1, ax + cxy^2 + cy + z^2 - 2, a + bxy^2 + b + x^2y^2, -c + dxz + xyz + 1\rangle$$

Task: Eliminate $\{x, y, z\}$ $\longrightarrow$ $\mathcal{R}(a, b, c, d)$

# Examples (2/5)

## Elimination Benchmarking (Preliminary)

$$R = \mathbb{Q}[a,b,c,d][x,y,z]$$

$$I = \langle a + x^2y^2 + y^3 + z - 1, ax + cxy^2 + cy + z^2 - 2, a + bxy^2 + b + x^2y^2, -c + dxz + xyz + 1\rangle$$

Task: Eliminate $\{x,y,z\}$ ⟶ $\mathcal{R}(a,b,c,d)$

Finite Fields System Generation: Seed up to weight 17 ⟶ 2000 equations ⟶ 850 equations $\approx 1s$

| Resultant | Singular Time | Mathematica Time | Finite Fields Time (10 core) | Finite Fields Sample Points |
|---|---|---|---|---|
| $\mathcal{R}(3,5,7,d)$ | | | | |
| $\mathcal{R}(3,5,c,d)$ | | | | |
| $\mathcal{R}(3,b,c,d)$ | | | | |
| $\mathcal{R}(a,b,c,d)$ | | | | |

# Examples (2/5)

## Elimination Benchmarking (Preliminary)

$$R = \mathbb{Q}[a,b,c,d][x,y,z]$$

$$I = \langle a + x^2y^2 + y^3 + z - 1, ax + cxy^2 + cy + z^2 - 2, a + bxy^2 + b + x^2y^2, -c + dxz + xyz + 1\rangle$$

Task: Eliminate $\{x,y,z\} \longrightarrow \mathcal{R}(a,b,c,d)$

Finite Fields System Generation: Seed up to weight 17 ⟶ 2000 equations ⟶ 850 equations $\approx 1s$

| Resultant | Singular Time | Mathematica Time | Finite Fields Time (10 core) | Finite Fields Sample Points |
|---|---|---|---|---|
| $\mathcal{R}(3,5,7,d)$ | $\approx 0.027s$ | $\approx 0.016s$ | $\approx 0.15s$ | $3$ |
| $\mathcal{R}(3,5,c,d)$ | | | | |
| $\mathcal{R}(3,b,c,d)$ | | | | |
| $\mathcal{R}(a,b,c,d)$ | | | | |

# Examples (2/5)

## Elimination Benchmarking (Preliminary)

$$R = \mathbb{Q}[a,b,c,d][x,y,z]$$

$$I = \langle a + x^2y^2 + y^3 + z - 1, ax + cxy^2 + cy + z^2 - 2, a + bxy^2 + b + x^2y^2, -c + dxz + xyz + 1\rangle$$

Task: Eliminate $\{x,y,z\} \longrightarrow \mathcal{R}(a,b,c,d)$

Finite Fields System Generation: Seed up to weight 17 $\longrightarrow$ 2000 equations $\longrightarrow$ 850 equations $\approx 1s$

| Resultant | Singular Time | Mathematica Time | Finite Fields Time (10 core) | Finite Fields Sample Points |
|---|---|---|---|---|
| $\mathcal{R}(3,5,7,d)$ | $\approx 0.027s$ | $\approx 0.016s$ | $\approx 0.15s$ | 3 |
| $\mathcal{R}(3,5,c,d)$ | $> 10h$ | $\approx 2s$ | $\approx 0.2s$ | 27 |
| $\mathcal{R}(3,b,c,d)$ | | | | |
| $\mathcal{R}(a,b,c,d)$ | | | | |

# Examples (2/5)

## Elimination Benchmarking (Preliminary)

$$R = \mathbb{Q}[a, b, c, d][x, y, z]$$

$$I = \langle a + x^2y^2 + y^3 + z - 1, ax + cxy^2 + cy + z^2 - 2, a + bxy^2 + b + x^2y^2, -c + dxz + xyz + 1\rangle$$

Task: Eliminate $\{x, y, z\} \longrightarrow \mathcal{R}(a, b, c, d)$

Finite Fields System Generation: Seed up to weight 17 $\longrightarrow$ 2000 equations $\longrightarrow$ 850 equations $\approx 1s$

| Resultant | Singular Time | Mathematica Time | Finite Fields Time (10 core) | Finite Fields Sample Points |
|---|---|---|---|---|
| $\mathcal{R}(3, 5, 7, d)$ | $\approx 0.027s$ | $\approx 0.016s$ | $\approx 0.15s$ | 3 |
| $\mathcal{R}(3, 5, c, d)$ | $> 10h$ | $\approx 2s$ | $\approx 0.2s$ | 27 |
| $\mathcal{R}(3, b, c, d)$ | ? | $\approx 3h$ | $\approx 0.3s$ | 523 |
| $\mathcal{R}(a, b, c, d)$ | | | | |

# Examples (2/5)

## Elimination Benchmarking (Preliminary)

$$R = \mathbb{Q}[a,b,c,d][x,y,z]$$

$$I = \langle a + x^2y^2 + y^3 + z - 1, ax + cxy^2 + cy + z^2 - 2, a + bxy^2 + b + x^2y^2, -c + dxz + xyz + 1\rangle$$

Task: Eliminate $\{x,y,z\} \longrightarrow \mathcal{R}(a,b,c,d)$

Finite Fields System Generation: Seed up to weight 17 $\longrightarrow$ 2000 equations $\longrightarrow$ 850 equations $\approx 1s$

| Resultant | Singular Time | Mathematica Time | Finite Fields Time (10 core) | Finite Fields Sample Points |
|---|---|---|---|---|
| $\mathcal{R}(3,5,7,d)$ | $\approx 0.027s$ | $\approx 0.016s$ | $\approx 0.15s$ | 3 |
| $\mathcal{R}(3,5,c,d)$ | $> 10h$ | $\approx 2s$ | $\approx 0.2s$ | 27 |
| $\mathcal{R}(3,b,c,d)$ | ? | $\approx 3h$ | $\approx 0.3s$ | 523 |
| $\mathcal{R}(a,b,c,d)$ | ? | $> 7d$ | $\approx 3s$ | 6769 |

# Examples (2/5)

## Elimination Benchmarking (Preliminary)

$$R = \mathbb{Q}[a,b,c,d][x,y,z]$$

$$I = \langle a + x^2y^2 + y^3 + z - 1, ax + cxy^2 + cy + z^2 - 2, a + bxy^2 + b + x^2y^2, -c + dxz + xyz + 1 \rangle$$

Task: Eliminate $\{x,y,z\}$ $\longrightarrow$ $\mathcal{R}(a,b,c,d)$

Finite Fields System Generation: Seed up to weight 17 $\longrightarrow$ 2000 equations $\longrightarrow$ 850 equations $\approx 1s$

| Resultant | Singular Time | Mathematica Time | Finite Fields Time (10 core) | Finite Fields Sample Points |
|---|---|---|---|---|
| $\mathcal{R}(3,5,7,d)$ | $\approx 0.027s$ | $\approx 0.016s$ | $\approx 0.15s$ | $3$ |
| $\mathcal{R}(3,5,c,d)$ | $> 10h$ | $\approx 2s$ | $\approx 0.2s$ | $27$ |
| $\mathcal{R}(3,b,c,d)$ | $?$ | $\approx 3h$ | $\approx 0.3s$ | $523$ |
| $\mathcal{R}(a,b,c,d)$ | $?$ | $> 7d$ | $\approx 3s$ | $6769$ |

The Finite Fields approach is solving a larger set of equations, but isn't slowed down by intermediate cancellations

# Examples (3/5)

## Landau Singularities of Feynman (Euler) Integrals

A Feynman integral can be defined as an Euler/Twisted Period Integral

$$I(s_{ij}, m) = \int_0^\infty \mathcal{G}(x, s_{ij}, m)^{-d/2} \, \frac{dx_1}{x_1} \wedge \cdots \wedge \frac{dx_n}{x_n}$$

# Examples (3/5)

## Landau Singularities of Feynman (Euler) Integrals

A Feynman integral can be defined as an Euler/Twisted Period Integral

$$I(s_{ij}, m) = \int_0^\infty \mathcal{G}(x, s_{ij}, m)^{-d/2} \frac{dx_1}{x_1} \wedge \cdots \wedge \frac{dx_n}{x_n}$$

Parameters (Mandelstam variables)

Integration variables

[Lee, 2013]

# Examples (3/5)

## Landau Singularities of Feynman (Euler) Integrals

A Feynman integral can be defined as an Euler/Twisted Period Integral

Twist: polynomial raised to a non integer (generic) power

$$I(s_{ij}, m) = \int_0^\infty \mathcal{G}(x, s_{ij}, m)^{-d/2} \frac{dx_1}{x_1} \wedge \cdots \wedge \frac{dx_n}{x_n}$$

Parameters (Mandelstam variables)

Integration variables

[Lee, 2013]

# Examples (3/5)

## Landau Singularities of Feynman (Euler) Integrals

A Feynman integral can be defined as an Euler/Twisted Period Integral

Twist: polynomial raised to a non integer (generic) power

$$I(s_{ij}, m) = \int_0^\infty \mathcal{G}(x, s_{ij}, m)^{-d/2} \frac{dx_1}{x_1} \wedge \cdots \wedge \frac{dx_n}{x_n}$$

Parameters (Mandelstam variables)    Integration variables

[Lee, 2013]

Parametric representations allow us to associate an Euler characteristic $\chi$ to a given Feynman integral

[Lee, 2013]
[Mastrolia, Mizera 2018]

Computing $\chi$ is algorithmically simple: $\omega = \mathrm{d}\log\left(\mathcal{G}(z)^{-d/2}\right)$ $\qquad \chi = \#\text{ solutions to } \omega = 0$

# Examples (3/5)

## Landau Singularities of Feynman (Euler) Integrals

A Feynman integral can be defined as an Euler/Twisted Period Integral

Twist: polynomial raised to a non integer (generic) power

$$I(s_{ij}, m) = \int_0^\infty \mathcal{G}(x, s_{ij}, m)^{-d/2} \frac{dx_1}{x_1} \wedge \cdots \wedge \frac{dx_n}{x_n}$$

Parameters (Mandelstam variables) Integration variables

[Lee, 2013]

Parametric representations allow us to associate an Euler characteristic $\chi$ to a given Feynman integral [Lee, 2013] [Mastrolia, Mizera 2018]

Computing $\chi$ is algorithmically simple: $\omega = \mathrm{d}\log\left(\mathcal{G}(z)^{-d/2}\right)$ $\chi = \#\ \text{solutions to}\ \omega = 0$

For what values of $\{s_{ij}, m\}$ does $I$ diverge? ⟶ Landau Analysis [Landau, 1960] [Cutkosky, 1960]

[Abreu, Berghoff, Bourjaily, Britto, Correia, Duhr, Fevola, Gardi, Giroux, Hannesdottir, Helmer, McLeod, Mizera, Panzer, Papathanasiou, Schwartz, Tellander, Telen, Vergu, 2017-2025]

# Examples (3/5)

## Landau Singularities of Feynman (Euler) Integrals

A Feynman integral can be defined as an Euler/Twisted Period Integral

Twist: polynomial raised to a non integer (generic) power

$$I(s_{ij}, m) = \int_0^\infty \mathcal{G}(x, s_{ij}, m)^{-d/2} \frac{dx_1}{x_1} \wedge \cdots \wedge \frac{dx_n}{x_n}$$

Parameters (Mandelstam variables)

Integration variables

[Lee, 2013]

Parametric representations allow us to associate an Euler characteristic $\chi$ to a given Feynman integral [Lee, 2013] [Mastrolia, Mizera 2018]

Computing $\chi$ is algorithmically simple: $\omega = \mathrm{d}\log\left(\mathcal{G}(z)^{-d/2}\right)$ $\chi = \#\ \text{solutions to}\ \omega = 0$

For what values of $\{s_{ij}, m\}$ does $I$ diverge? ⟶ Landau Analysis [Landau, 1960] [Cutkosky, 1960] [Abreu, Berghoff, Bourjaily, Britto, Correia, Duhr, Fevola, Gardi, Giroux, Hannesdottir, Helmer, McLeod, Mizera, Panzer, Papathanasiou, Schwartz, Tellander, Telen, Vergu, 2017-2025]

The Landau Variety can be defined as the values of $\{s_{ij}, m\}$ for which the Euler characteristic drops in value

[Chestnov, Matsubara-Heo, Munch, Takayama, 2023] [Mizera, Fevola, Telen, 2023/24]

# Examples (4/5)

## Computing Euler Characteristics for Landau Analysis

Computing $\chi$ : $\omega = \mathrm{d}\log\left(G(z)^{-d/2}\right)$ $\chi = \#\text{ solutions to }\omega = 0$ $\omega = -\frac{d}{2}\left(\frac{\partial_1 G}{G}dx_1 + \cdots + \frac{\partial_n G}{G}dx_n\right)$

# Examples (4/5)

## Computing Euler Characteristics for Landau Analysis

Computing $\chi$ : $\omega = \mathrm{d}\log\left(G(z)^{-d/2}\right)$ $\chi = \#\text{ solutions to } \omega = 0$ $\omega = -\frac{d}{2}\left(\frac{\partial_1 G}{G}dx_1 + \cdots + \frac{\partial_n G}{G}dx_n\right)$

$$\omega = 0 \longrightarrow \boxed{\begin{array}{c} \frac{\partial_1 G}{G} = 0 \\ \vdots \\ \frac{\partial_n G}{G} = 0 \end{array}}$$

# Examples (4/5)

## Computing Euler Characteristics for Landau Analysis

Computing $\chi$ : $\omega = \mathrm{d}\log\left(G(z)^{-d/2}\right)$ $\quad \chi = \#$ solutions to $\omega = 0$ $\quad \omega = -\frac{d}{2}\left(\frac{\partial_1 G}{G}dx_1 + \cdots + \frac{\partial_n G}{G}dx_n\right)$

$$\omega = 0 \longrightarrow \begin{array}{c} \frac{\partial_1 G}{G} = 0 \\ \vdots \\ \frac{\partial_n G}{G} = 0 \end{array} \longrightarrow \left.\begin{array}{r} \partial_1 G = 0 \\ \vdots \\ \partial_n G = 0 \\ 1 - x_0 G = 0 \end{array}\right\}$$

system of polynomial equations!

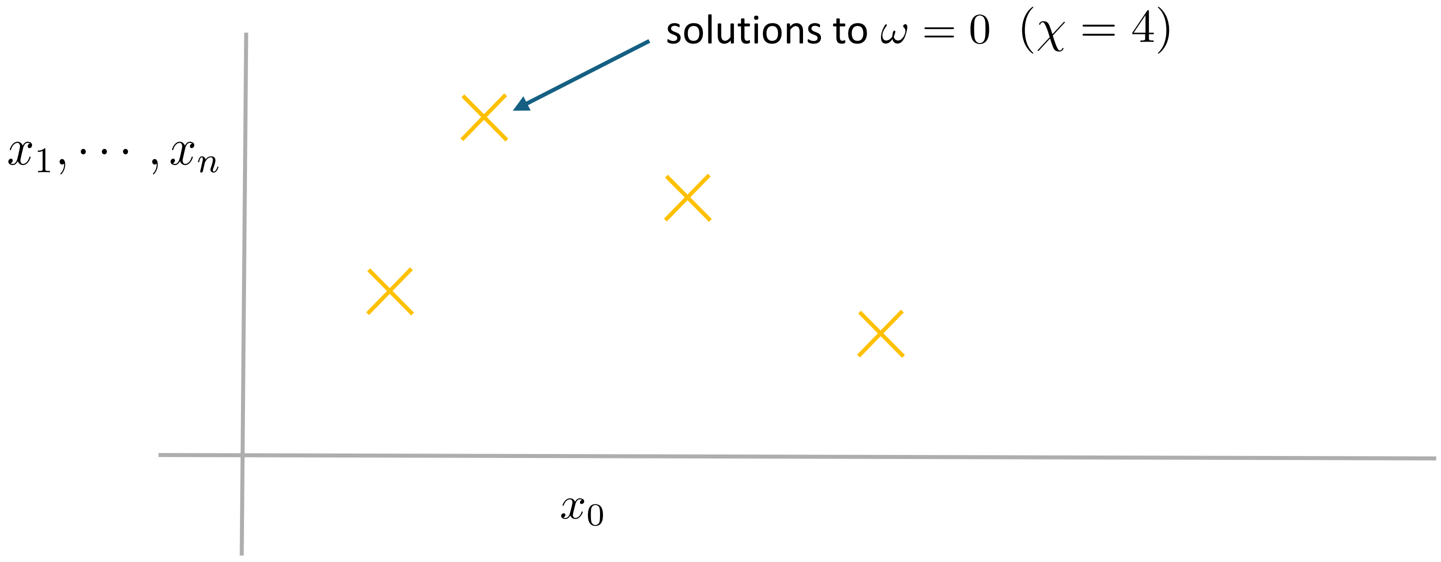
# Examples (4/5)

## Computing Euler Characteristics for Landau Analysis

**Computing $\chi$ :** $\omega = \mathrm{d}\log\left(G(z)^{-d/2}\right)$ $\chi = \#\ \text{solutions to } \omega = 0$ $\omega = -\frac{d}{2}\left(\frac{\partial_1 G}{G}dx_1 + \cdots + \frac{\partial_n G}{G}dx_n\right)$

$$\omega = 0 \longrightarrow \begin{cases} \frac{\partial_1 G}{G} = 0 \\ \vdots \\ \frac{\partial_n G}{G} = 0 \end{cases} \longrightarrow \begin{cases} \partial_1 G = 0 \\ \vdots \\ \partial_n G = 0 \\ 1 - x_0 G = 0 \end{cases}$$

system of polynomial equations!



# Examples (4/5)

## Computing Euler Characteristics for Landau Analysis

Computing $\chi$:

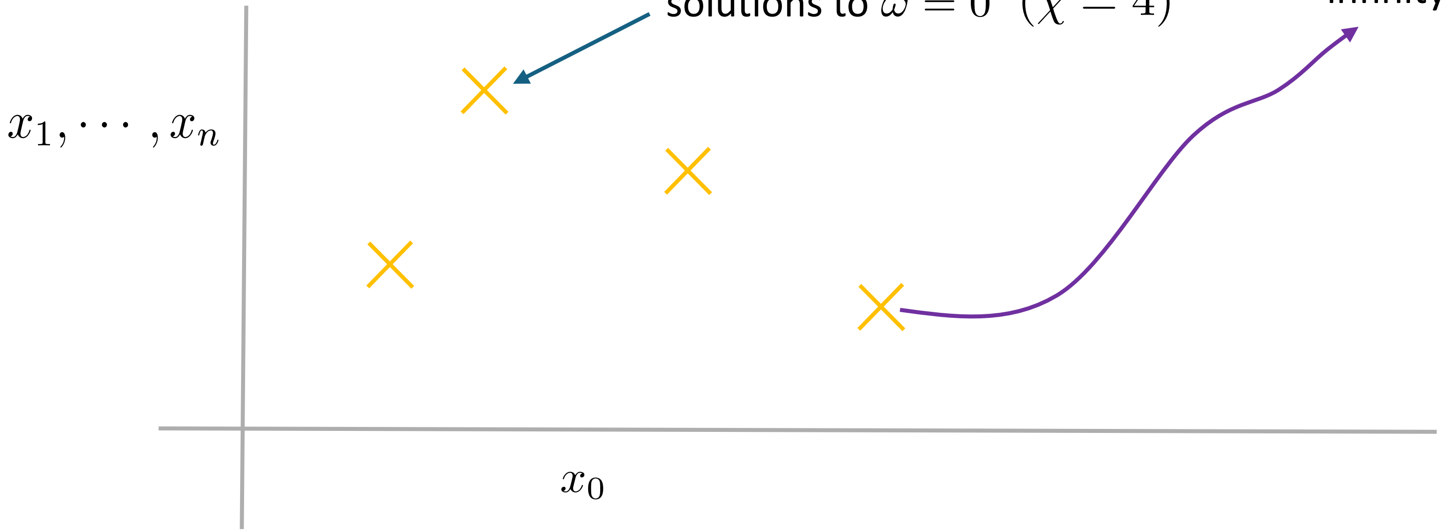
$$\omega = \mathrm{d}\log\left(G(z)^{-d/2}\right) \qquad \chi = \#\ \text{solutions to}\ \omega = 0 \qquad \omega = -\frac{d}{2}\left(\frac{\partial_1 G}{G}dx_1 + \cdots + \frac{\partial_n G}{G}dx_n\right)$$

$$\omega = 0 \longrightarrow \begin{cases} \dfrac{\partial_1 G}{G} = 0 \\ \vdots \\ \dfrac{\partial_n G}{G} = 0 \end{cases} \longrightarrow \begin{cases} \partial_1 G = 0 \\ \vdots \\ \partial_n G = 0 \\ 1 - x_0 G = 0 \end{cases}$$

system of polynomial equations!

as the degenerate configuration is approached some solutions fly off to infinity

solutions to $\omega = 0 \quad (\chi = 4)$



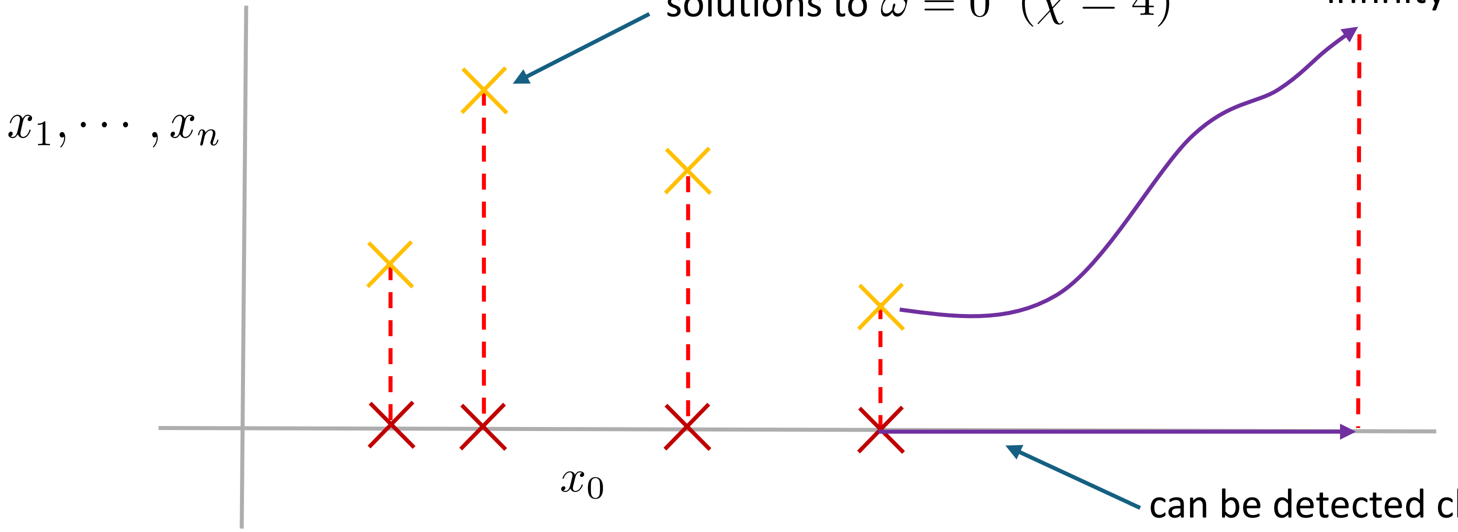
# Examples (4/5)

## Computing Euler Characteristics for Landau Analysis

Computing $\chi$: $\omega = \mathrm{d}\log\left(G(z)^{-d/2}\right)$ $\chi = \#$ solutions to $\omega = 0$ $\omega = -\frac{d}{2}\left(\frac{\partial_1 G}{G}dx_1 + \cdots + \frac{\partial_n G}{G}dx_n\right)$

$$\omega = 0 \longrightarrow \begin{cases} \frac{\partial_1 G}{G} = 0 \\ \vdots \\ \frac{\partial_n G}{G} = 0 \end{cases} \longrightarrow \begin{cases} \partial_1 G = 0 \\ \vdots \\ \partial_n G = 0 \\ 1 - x_0 G = 0 \end{cases}$$

system of polynomial equations!

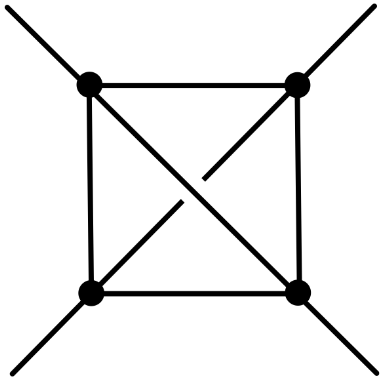


# Examples (5/5)

Computing Euler Characteristics for Landau Analysis: Three loop envelope (preliminary)

# Examples (5/5)

## Computing Euler Characteristics for Landau Analysis: Three loop envelope (preliminary)

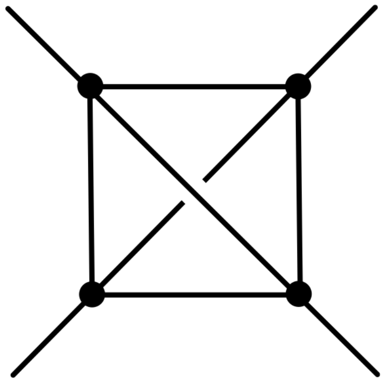


[Correia, Sever, Zhibodeev, 2021]

Horrendous integral: $\chi = 60(!)$ in the top (max cut) sector alone

# Examples (5/5)

## Computing Euler Characteristics for Landau Analysis: Three loop envelope (preliminary)



[Correia, Sever, Zhibodeov, 2021]

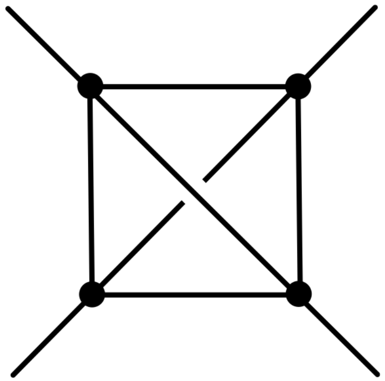
Horrendous integral: $\chi = 60(!)$ in the top (max cut) sector alone

SOFIA/PLD most complicated letter found: $27(m^2)^3 + 4s^2t + 4st^2$

[Fevola, Mizera, Telen, 2023]
[Correia, Giroux, Mizera, 2025]

# Examples (5/5)

## Computing Euler Characteristics for Landau Analysis: Three loop envelope (preliminary)



[Correia, Sever, Zhibodeov, 2021]

Horrendous integral: $\chi = 60(!)$ in the top (max cut) sector alone

SOFIA/PLD most complicated letter found: $27(m^2)^3 + 4s^2t + 4st^2$

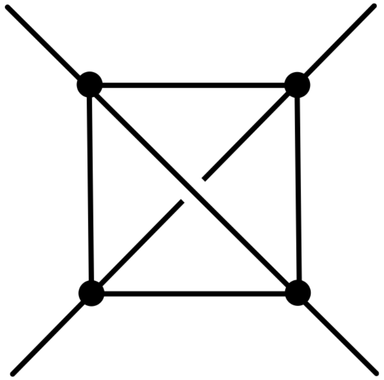
[Fevola, Mizera, Telen, 2023]
[Correia, Giroux, Mizera, 2025]

## Euler characteristic strategy

Two new simple letters: $\{s^2 + st + t^2, m^2s^2 + m^2st + s^2t + m^2t^2 + st^2\}$

# Examples (5/5)

## Computing Euler Characteristics for Landau Analysis: Three loop envelope (preliminary)



[Correia, Sever, Zhibodeev, 2021]

Horrendous integral: $\chi = 60(!)$ in the top (max cut) sector alone

SOFIA/PLD most complicated letter found: $27(m^2)^3 + 4s^2t + 4st^2$

[Fevola, Mizera, Telen, 2023]
[Correia, Giroux, Mizera, 2025]

## Euler characteristic strategy

Two new simple letters: $\{s^2 + st + t^2, m^2s^2 + m^2st + s^2t + m^2t^2 + st^2\}$

Four new complicated letters:

$$\{27\, m2^4 s^2 + 108\, m2^4 s\, t + 162\, m2^3 s^2 t + 54\, m2^2 s^3 t + 4\, m2\, s^4 t + 108\, m2^4 t^2 + 162\, m2^3 s\, t^2 + 45\, m2^2 s^2 t^2 -$$
$$6\, m2\, s^3 t^2 - s^4 t^2 - 18\, m2^2 s\, t^3 - 20\, m2\, s^2 t^3 - 2\, s^3 t^3 - 9\, m2^2 t^4 - 10\, m2\, s\, t^4 - s^2 t^4,\ 108\, m2^4 s^2 - 9\, m2^2 s^4 + 108\, m2^4 s\, t + 162\, m2^3 s^2 t -$$
$$18\, m2^2 s^3 t - 10\, m2\, s^4 t + 27\, m2^4 t^2 + 162\, m2^3 s\, t^2 + 45\, m2^2 s^2 t^2 - 20\, m2\, s^3 t^2 - s^4 t^2 + 54\, m2^2 s\, t^3 - 6\, m2\, s^2 t^3 - 2\, s^3 t^3 + 4\, m2\, s\, t^4 - s^2 t^4,$$
$$27\, m2^4 s^2 - 54\, m2^4 s\, t + 162\, m2^3 s^2 t - 54\, m2^2 s^3 t + 4\, m2\, s^4 t + 27\, m2^4 t^2 + 162\, m2^3 s\, t^2 - 117\, m2^2 s^2 t^2 + 22\, m2\, s^3 t^2 - s^4 t^2 - 54\, m2^2 s\, t^3 + 22\, m2\, s^2 t^3 - 2\, s^3 t^3 + 4\, m2\, s\, t^4 - s^2 t^4,$$
$$65\,536\, m2^{12} + 270\,336\, m2^{10} s^2 + 33\,024\, m2^8 s^4 + 1024\, m2^6 s^6 + 270\,336\, m2^{10} s\, t - 458\,752\, m2^9 s^2 t + 66\,048\, m2^8 s^3 t - 1\,276\,416\, m2^7 s^4 t + 3072\, m2^6 s^5 t - 137\,472\, m2^5 s^6 t -$$
$$4096\, m2^3 s^8 t + 270\,336\, m2^{10} t^2 - 458\,752\, m2^9 s\, t^2 + 99\,072\, m2^8 s^2 t^2 - 2\,552\,832\, m2^7 s^3 t^2 - 3\,427\,584\, m2^6 s^4 t^2 - 412\,416\, m2^5 s^5 t^2 + 149\,472\, m2^4 s^6 t^2 - 16\,384\, m2^3 s^7 t^2 +$$
$$768\, m2^2 s^8 t^2 + 66\,048\, m2^8 s\, t^3 - 2\,552\,832\, m2^7 s^2 t^3 - 6\,860\,288\, m2^6 s^3 t^3 - 687\,360\, m2^5 s^4 t^3 + 448\,416\, m2^4 s^5 t^3 - 49\,888\, m2^3 s^6 t^3 + 3072\, m2^2 s^7 t^3 - 48\, m2\, s^8 t^3 +$$
$$33\,024\, m2^8 t^4 - 1\,276\,416\, m2^7 s\, t^4 - 3\,427\,584\, m2^6 s^2 t^4 - 687\,360\, m2^5 s^3 t^4 + 597\,888\, m2^4 s^4 t^4 - 92\,320\, m2^3 s^5 t^4 + 6144\, m2^2 s^6 t^4 - 192\, m2\, s^7 t^4 + s^8 t^4 +$$
$$3072\, m2^6 s\, t^5 - 412\,416\, m2^5 s^2 t^5 + 448\,416\, m2^4 s^3 t^5 - 92\,320\, m2^3 s^4 t^5 + 7680\, m2^2 s^5 t^5 - 336\, m2\, s^6 t^5 + 4\, s^7 t^5 + 1024\, m2^6 t^6 - 137\,472\, m2^5 s\, t^6 + 149\,472\, m2^4 s^2 t^6 -$$
$$49\,888\, m2^3 s^3 t^6 + 6144\, m2^2 s^4 t^6 - 336\, m2\, s^5 t^6 + 6\, s^6 t^6 - 16\,384\, m2^3 s^2 t^7 + 3072\, m2^2 s^3 t^7 - 192\, m2\, s^4 t^7 + 4\, s^5 t^7 - 4096\, m2^3 s\, t^8 + 768\, m2^2 s^2 t^8 - 48\, m2\, s^3 t^8 + s^4 t^8\}$$

Thank you for listening!