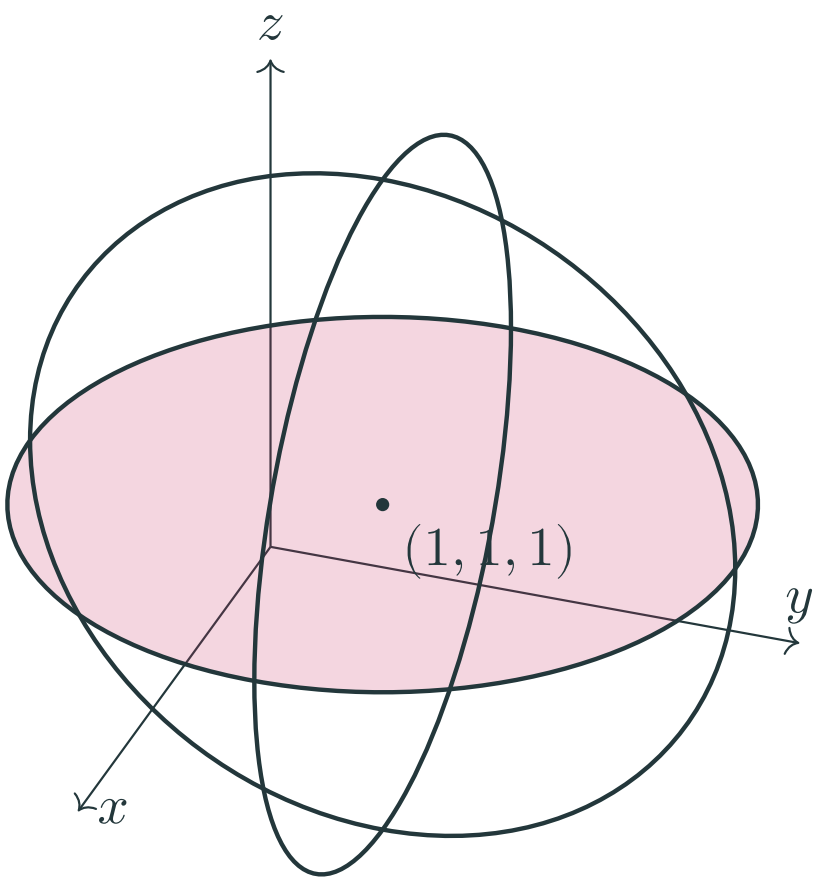
On the (De)composable Polynomials

Thi Xuan Vu

University of Lille, France

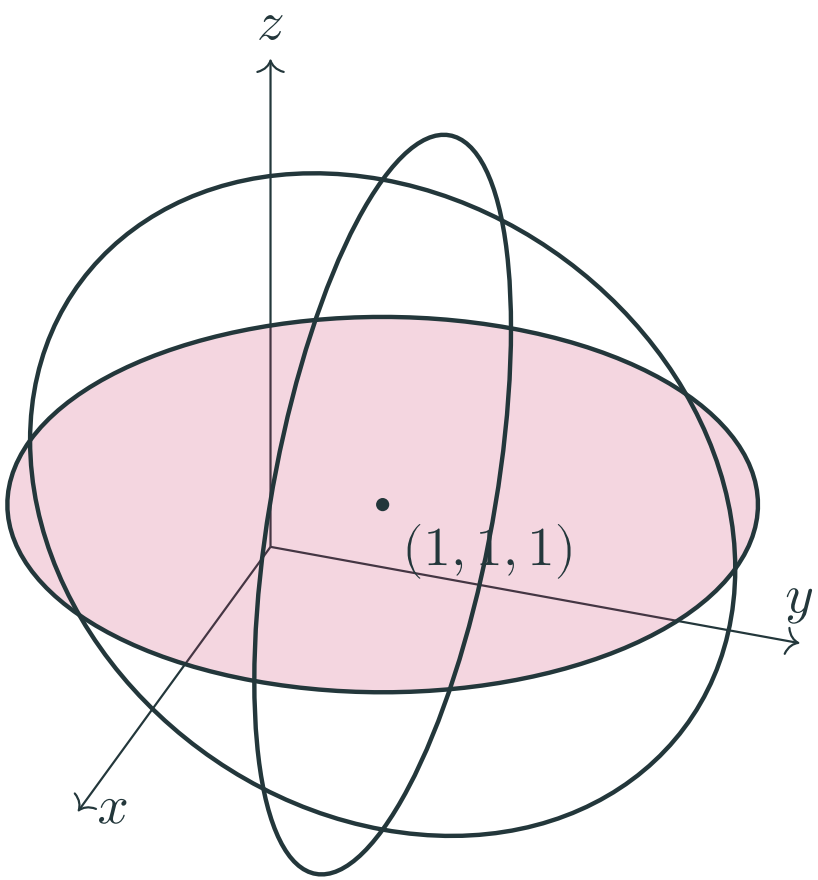
Computing representation in subrings of multivariate polynomial rings

An Example



$$(x-1)^2 + (y-1)^2 + (z-1)^2 = 4$$

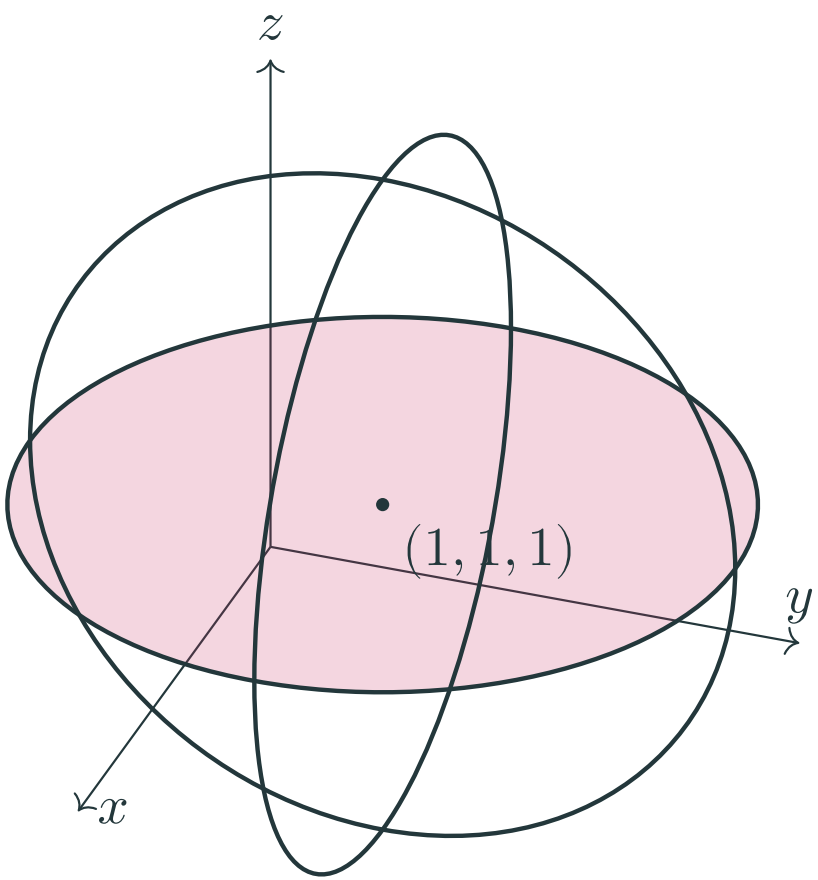
An Example



$$(x-1)^2 + (y-1)^2 + (z-1)^2 = 4$$

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

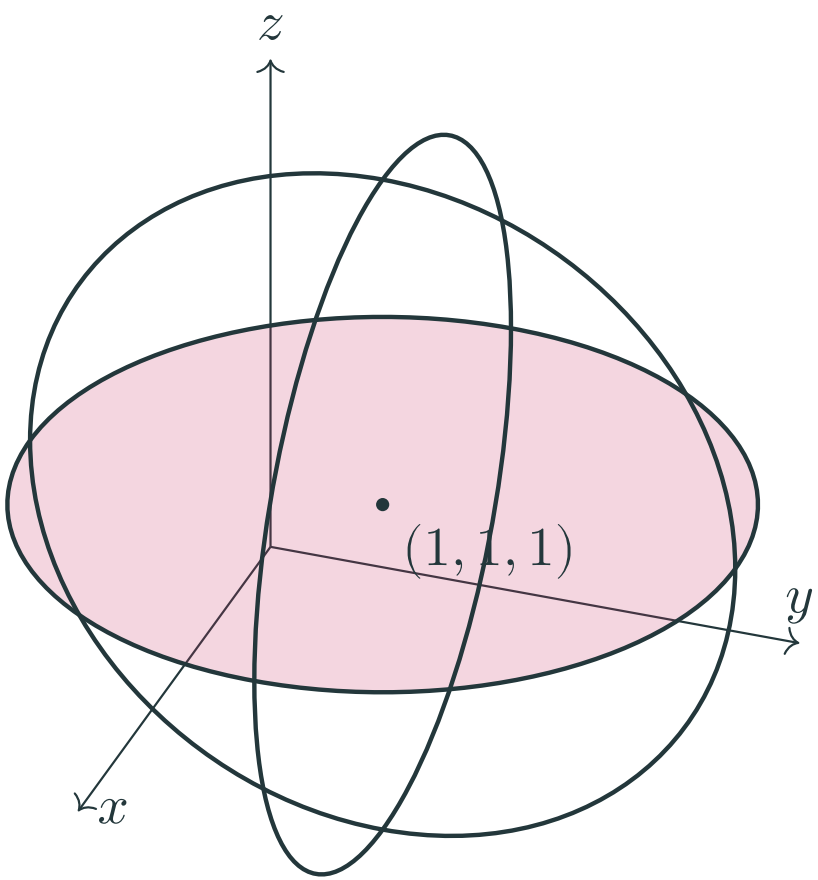
An Example



$$(x-1)^2+(y-1)^2+(z-1)^2=4$$

- symmetric
- $x^2+y^2+z^2-2(x+y+z)-1=0$
- $(x+y+z)^2-2(xy+yz+zx)-2(x+y+z)-1=0$

An Example



$$(x-1)^2+(y-1)^2+(z-1)^2=4$$

- symmetric
- $x^2+y^2+z^2-2(x+y+z)-1=0$
- $(x+y+z)^2-2(xy+yz+zx)-2(x+y+z)-1=0$
- $e_1^2-2e_2-2e_1-1=0$

e_k: elementary symmetric polynomial of degree k.

Unique Representation in Subrings

Theorem [Fundamental Thm of symm. polynomials]

For any symmetric polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$, there is a unique polynomial $h \in \mathbb{K}[y_1, \ldots, y_n]$ such that

$$h(e_1(x_1, \ldots, x_n), \ldots, e_n(x_1, \ldots, x_n)) = f.$$

Unique Representation in Subrings

Theorem [Fundamental Thm of symm. polynomials]

For any symmetric polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$, there is a unique polynomial $h \in \mathbb{K}[y_1, \ldots, y_n]$ such that

$$h(e_1(x_1, \ldots, x_n), \ldots, e_n(x_1, \ldots, x_n)) = f.$$

Given f, compute h algorithmically?

Unique Representation in Subrings

Theorem [Fundamental Thm of symm. polynomials]

For any symmetric polynomial $f \in \mathbb{K}[x_1, \dots, x_n]$, there is a unique polynomial $h \in \mathbb{K}[y_1, \dots, y_n]$ such that

$$h(e_1(x_1, \dots, x_n), \dots, e_n(x_1, \dots, x_n)) = f.$$

Given f, compute h algorithmically?

In general, given

- n algebraically independent polynomials $g_1, \dots, g_n$ in $\mathbb{K}[x_1, \dots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \dots, g_n]$, where $\mathbb{K}[g_1, \dots, g_n]$ is the subring of $\mathbb{K}[x_1, \dots, x_n]$ generated by $(g_1, \dots, g_n)$

Unique Representation in Subrings

Theorem [Fundamental Thm of symm. polynomials]

For any symmetric polynomial $f \in \mathbb{K}[x_1, \dots, x_n]$, there is a unique polynomial $h \in \mathbb{K}[y_1, \dots, y_n]$ such that

$$h(e_1(x_1, \dots, x_n), \dots, e_n(x_1, \dots, x_n)) = f.$$

Given f, compute h algorithmically?

In general, given

- n algebraically independent polynomials $g_1, \dots, g_n$ in $\mathbb{K}[x_1, \dots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \dots, g_n]$, where $\mathbb{K}[g_1, \dots, g_n]$ is the subring of $\mathbb{K}[x_1, \dots, x_n]$ generated by $(g_1, \dots, g_n)$

There is a unique polynomial $h \in \mathbb{K}[y_1, \dots, y_n]$ such that

$$h(g_1, \dots, g_n) = f$$

Algebraic Independence

Let $g_1, \dots, g_n$ be polynomials in $\mathbb{K}[x_1, \dots, x_n]$

Definition

$g_1, \dots, g_n$ are called algebraically independent (A. ID) if there is no non-zero polynomial $A \in \mathbb{K}[y_1, \dots, y_n]$ such that $A(g_1, \dots, g_n) = 0$.

Algebraic Independence

Let $g_1, \dots, g_n$ be polynomials in $\mathbb{K}[x_1, \dots, x_n]$

Definition

$g_1, \dots, g_n$ are called algebraically independent (A. ID) if there is no non-zero polynomial $A \in \mathbb{K}[y_1, \dots, y_n]$ such that $A(g_1, \dots, g_n) = 0$.

Example:

- elementary symmetric polys $(x + y + z, xy + yz + zx, xyz)$ are A. ID

Algebraic Independence

Let $g_1, \dots, g_n$ be polynomials in $\mathbb{K}[x_1, \dots, x_n]$

Definition

$g_1, \dots, g_n$ are called algebraically independent (A. ID) if there is no non-zero polynomial $A \in \mathbb{K}[y_1, \dots, y_n]$ such that $A(g_1, \dots, g_n) = 0$.

Example:

- elementary symmetric polys $(x + y + z, xy + yz + zx, xyz)$ are A. ID
- (x, y) are A. ID

Algebraic Independence

Let $g_1, \dots, g_n$ be polynomials in $\mathbb{K}[x_1, \dots, x_n]$

Definition

$g_1, \dots, g_n$ are called algebraically independent (A. ID) if there is no non-zero polynomial $A \in \mathbb{K}[y_1, \dots, y_n]$ such that $A(g_1, \dots, g_n) = 0$.

Example:

- elementary symmetric polys $(x + y + z, xy + yz + zx, xyz)$ are A. ID
- (x, y) are A. ID
- but $(x, y, x^2 + y^3)$ are not A. ID since

$$A(x, y, x^2 + y^3) = 0 \text{ with } A = y_1^2 + y_2^3 - y_3$$

Our First Problem

Given

- n algebraically independent polynomials $g_1, \ldots, g_n$ in $\mathbb{K}[x_1, \ldots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \ldots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \ldots, y_n]$ such that

$$h(g_1, \ldots, g_n) = f$$

Our First Problem

Given

- n algebraically independent polynomials $g_1, \dots, g_n$ in $\mathbb{K}[x_1, \dots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \dots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \dots, y_n]$ such that

$$h(g_1, \dots, g_n) = f$$

Theorem [V., 2025]

There exists a randomized algorithm to compute h with the complexity being $O\tilde{}((nL_1 + n^4 + L_2) \cdot \mathcal{M}(\Delta, n))$ operations in $\mathbb{K}$.

with $\deg(h) \leq \Delta$ and

- L_1 and L_2 are the sizes of $(g_1, \dots, g_n)$ and f respectively
- $\mathcal{M}(\Delta, n)$: the cost of multiplying n-variate polynomials of total degree Δ

State of The Art

Gröbner basis strategy (eliminate x_i's):

- consider polynomial ring $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_n]$ and a monomial order $[x_1, \dots, x_n] \succ [y_1, \dots, y_n]$
- $\mathfrak{B} = GB(g_1 - y_1, \dots, g_n - y_n)$ w.r.t $\succ$
- $h = \text{Remainder}(f, \mathfrak{B})$

State of The Art

Gröbner basis strategy (eliminate x_i's):

- consider polynomial ring $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_n]$ and a monomial order $[x_1, \dots, x_n] \succ [y_1, \dots, y_n]$
- $\mathfrak{B} = GB(g_1 - y_1, \dots, g_n - y_n)$ w.r.t $\succ$
- $h =$ Remainder$(f, \mathfrak{B})$

Strategy	Applicable To	Complexity
Gröbner basis	General	Not fully analyzed
Gaudry et al. (2006)	f symmetric, $g_i = e_i$	$4^n (n!)^2 L_2 + 2$
Bläser–Jindal (2018)	f symmetric, $g_i = e_i$	$\tilde{O}(d^2 L_2 + d^2 n^2)$
Chaugule et al. (2023)	f symmetric, various bases	$\tilde{O}(d^2 L_2 + d^2 n^2)$
Vu (2025)	General	$\tilde{O}((nL_1 + n^4 + L_2)\, \mathcal{M}(\Delta, n))$

L_1 and L_2: sizes of $(g_1, \dots, g_n)$ and f; $\quad d = \deg(f)$; $\quad \Delta = \deg(h)$

Our Main Tool: the Hensel-Newton Lifting

Hensel's lemma (lifting roots modulo powers) + Newton iteration

Let

- $\boldsymbol{P} = (p_1, \dots, p_n)$ be n polynomials in $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m]$
- $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$ be a solution of $P(x_1, \dots, x_n, 0, \dots, 0)$

Assume

- the Jacobian matrix of $\boldsymbol{P}(x_1, \dots, x_n, 0, \dots, 0)$ has full rank n at $\boldsymbol{\alpha}$

Then there is a unique $\boldsymbol{v} = (v_1, \dots, v_n)$ of power series in $\overline{\mathbb{K}}[[y_1, \dots, y_m]]$

$$\boldsymbol{v}(0, \dots, 0) = \boldsymbol{\alpha} \quad \text{and} \quad p_1(\boldsymbol{v}, \boldsymbol{y}) = \cdots = p_n(\boldsymbol{v}, \boldsymbol{y}) = 0.$$

Our Main Tool: the Hensel-Newton Lifting

Hensel's lemma (lifting roots modulo powers) + Newton iteration

Let

- $\boldsymbol{P} = (p_1, \dots, p_n)$ be n polynomials in $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m]$
- $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$ be a solution of $P(x_1, \dots, x_n, 0, \dots, 0)$

Assume

- the Jacobian matrix of $\boldsymbol{P}(x_1, \dots, x_n, 0, \dots, 0)$ has full rank n at $\boldsymbol{\alpha}$

Then there is a unique $\boldsymbol{v} = (v_1, \dots, v_n)$ of power series in $\overline{\mathbb{K}}[[y_1, \dots, y_m]]$

$$\boldsymbol{v}(0, \dots, 0) = \boldsymbol{\alpha} \quad \text{and} \quad p_1(\boldsymbol{v}, \boldsymbol{y}) = \cdots = p_n(\boldsymbol{v}, \boldsymbol{y}) = 0.$$

Example: Let $\boldsymbol{P} = (p_1, p_2) = (x_1 + x_2 - y_1 - 2, x_1^2 + x_2^2 - y_2 - 10)$ and

- $\boldsymbol{\alpha} = (-1, 3)$ is a root of $\boldsymbol{P}(x_1, x_2, 0, 0) = (x_1 + x_2 - 2, x_1^2 + x_2^2 - 10)$
- $\text{rank}(\text{jac})(\boldsymbol{\alpha}) = 2$ with $\text{jac} = \begin{pmatrix} 1 & 1 \\ 2x_1 & 2x_2 \end{pmatrix}$.

Then $v_1 = -1 + 3/4y_1 + -1/8y_2 + \cdots$ and $v_2 = 3 + 1/4y_1 + 1/8y_2 + \cdots$

Let

- $\boldsymbol{P} = (p_1, \dots, p_n)$ be n polynomials in $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m]$
- $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$ be a solution of $P(x_1, \dots, x_n, 0, \dots, 0)$

Assume

- the Jacobian matrix of $\boldsymbol{P}(x_1, \dots, x_n, 0, \dots, 0)$ has full rank n at $\boldsymbol{\alpha}$

Then there is a unique $\boldsymbol{v} = (v_1, \dots, v_n)$ of power series in $\overline{\mathbb{K}}[[y_1, \dots, y_m]]$

$$\boldsymbol{v}(0, \dots, 0) = \boldsymbol{\alpha} \quad \text{and} \quad p_1(\boldsymbol{v}, \boldsymbol{y}) = \cdots = p_n(\boldsymbol{v}, \boldsymbol{y}) = 0.$$

Moreover, we can compute the truncation of v to an arbitrary degree δ.

Let

- $\boldsymbol{P} = (p_1, \ldots, p_n)$ be n polynomials in $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$
- $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ be a solution of $P(x_1, \ldots, x_n, 0, \ldots, 0)$

Assume

- the Jacobian matrix of $\boldsymbol{P}(x_1, \ldots, x_n, 0, \ldots, 0)$ has full rank n at $\boldsymbol{\alpha}$

Then there is a unique $\boldsymbol{v} = (v_1, \ldots, v_n)$ of power series in $\overline{\mathbb{K}}[[y_1, \ldots, y_m]]$

$$\boldsymbol{v}(0, \ldots, 0) = \boldsymbol{\alpha} \quad \text{and} \quad p_1(\boldsymbol{v}, \boldsymbol{y}) = \cdots = p_n(\boldsymbol{v}, \boldsymbol{y}) = 0.$$

Moreover, we can compute the truncation of v to an arbitrary degree δ.

Lifting$(P, \boldsymbol{\alpha}, \delta)$:

1. Initialize $v^{(0)} = \boldsymbol{\alpha}$

Let

- $\boldsymbol{P} = (p_1, \dots, p_n)$ be n polynomials in $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m]$
- $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$ be a solution of $P(x_1, \dots, x_n, 0, \dots, 0)$

Assume

- the Jacobian matrix of $\boldsymbol{P}(x_1, \dots, x_n, 0, \dots, 0)$ has full rank n at $\boldsymbol{\alpha}$

Then there is a unique $\boldsymbol{v} = (v_1, \dots, v_n)$ of power series in $\overline{\mathbb{K}}[[y_1, \dots, y_m]]$

$$\boldsymbol{v}(0, \dots, 0) = \boldsymbol{\alpha} \quad \text{and} \quad p_1(\boldsymbol{v}, \boldsymbol{y}) = \cdots = p_n(\boldsymbol{v}, \boldsymbol{y}) = 0.$$

Moreover, we can compute the truncation of v to an arbitrary degree δ.

Lifting$(P, \boldsymbol{\alpha}, \delta)$:

1. Initialize $v^{(0)} = \boldsymbol{\alpha}$
2. For $k = 1$ to $\lceil \log_2(\delta) \rceil$ do:

$$\boldsymbol{v}^{(k)} = \begin{pmatrix} \boldsymbol{v}_1^{(k-1)} \\ \vdots \\ v_n^{(k-1)} \end{pmatrix} - \big(\mathsf{jac}(\boldsymbol{v}^{(k-1)}, \boldsymbol{y})\big)^{-1} \begin{pmatrix} p_1(\boldsymbol{v}^{(k-1)}, \boldsymbol{y}) \\ \vdots \\ p_n(\boldsymbol{v}^{(k-1)}, \boldsymbol{y}) \end{pmatrix}$$

Let

- $\boldsymbol{P} = (p_1, \dots, p_n)$ be n polynomials in $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m]$
- $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$ be a solution of $P(x_1, \dots, x_n, 0, \dots, 0)$

Assume

- the Jacobian matrix of $\boldsymbol{P}(x_1, \dots, x_n, 0, \dots, 0)$ has full rank n at $\boldsymbol{\alpha}$

Then there is a unique $\boldsymbol{v} = (v_1, \dots, v_n)$ of power series in $\overline{\mathbb{K}}[[y_1, \dots, y_m]]$

$$\boldsymbol{v}(0, \dots, 0) = \boldsymbol{\alpha} \quad \text{and} \quad p_1(\boldsymbol{v}, \boldsymbol{y}) = \cdots = p_n(\boldsymbol{v}, \boldsymbol{y}) = 0.$$

Moreover, we can compute the truncation of v to an arbitrary degree δ.

Lifting$(P, \boldsymbol{\alpha}, \delta)$:

1. Initialize $v^{(0)} = \boldsymbol{\alpha}$
2. For $k = 1$ to $\lceil \log_2(\delta) \rceil$ do:

$$\boldsymbol{v}^{(k)} = \begin{pmatrix} \boldsymbol{v}_1^{(k-1)} \\ \vdots \\ v_n^{(k-1)} \end{pmatrix} - \left(\mathsf{jac}(\boldsymbol{v}^{(k-1)}, \boldsymbol{y})\right)^{-1} \begin{pmatrix} p_1(\boldsymbol{v}^{(k-1)}, \boldsymbol{y}) \\ \vdots \\ p_n(\boldsymbol{v}^{(k-1)}, \boldsymbol{y}) \end{pmatrix}$$

3. Return $\boldsymbol{v}^{(\lceil \log_2(\delta) \rceil)}$

The First Version of Our Main Algorithm

Given

- n algebraically independent polynomials $g_1, \ldots, g_n$ in $\mathbb{K}[x_1, \ldots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \ldots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \ldots, y_n]$ such that

$$h(g_1, \ldots, g_n) = f$$

The First Version of Our Main Algorithm

Given

- n algebraically independent polynomials $g_1, \ldots, g_n$ in $\mathbb{K}[x_1, \ldots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \ldots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \ldots, y_n]$ such that

$$h(g_1, \ldots, g_n) = f$$

1. Consider polynomials $P = (g_1 - y_1, \ldots, g_n - y_n)$ in $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_n]$

The First Version of Our Main Algorithm

Given

- n algebraically independent polynomials $g_1, \ldots, g_n$ in $\mathbb{K}[x_1, \ldots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \ldots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \ldots, y_n]$ such that

$$h(g_1, \ldots, g_n) = f$$

1. Consider polynomials $P = (g_1 - y_1, \ldots, g_n - y_n)$ in $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_n]$
2. Let $\boldsymbol{\alpha}$ be a root of $P(x_1, \ldots, x_n, 0, \ldots, 0) = (g_1, \ldots, g_n)$

The First Version of Our Main Algorithm

Given

- n algebraically independent polynomials $g_1, \ldots, g_n$ in $\mathbb{K}[x_1, \ldots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \ldots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \ldots, y_n]$ such that

$$h(g_1, \ldots, g_n) = f$$

1. Consider polynomials $P = (g_1 - y_1, \ldots, g_n - y_n)$ in $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_n]$
2. Let $\boldsymbol{\alpha}$ be a root of $P(x_1, \ldots, x_n, 0, \ldots, 0) = (g_1, \ldots, g_n)$
3. $(v_1, \ldots, v_n) = \text{Lifting}(P, \alpha, \Delta)$ in $\mathbb{K}[y_1, \ldots, y_n]$, with $\Delta \geq \deg(h)$

The First Version of Our Main Algorithm

Given

- n algebraically independent polynomials $g_1, \ldots, g_n$ in $\mathbb{K}[x_1, \ldots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \ldots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \ldots, y_n]$ such that

$$h(g_1, \ldots, g_n) = f$$

1. Consider polynomials $P = (g_1 - y_1, \ldots, g_n - y_n)$ in $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_n]$
2. Let $\boldsymbol{\alpha}$ be a root of $P(x_1, \ldots, x_n, 0, \ldots, 0) = (g_1, \ldots, g_n)$
3. $(v_1, \ldots, v_n) = \text{Lifting}(P, \alpha, \Delta)$ in $\mathbb{K}[y_1, \ldots, y_n]$, with $\Delta \geq \deg(h)$
4. Compute $f(v_1, \ldots, v_n)$

The First Version of Our Main Algorithm

Given

- n algebraically independent polynomials $g_1, \ldots, g_n$ in $\mathbb{K}[x_1, \ldots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \ldots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \ldots, y_n]$ such that

$$h(g_1, \ldots, g_n) = f$$

1. Consider polynomials $P = (g_1 - y_1, \ldots, g_n - y_n)$ in $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_n]$
2. Let $\boldsymbol{\alpha}$ be a root of $P(x_1, \ldots, x_n, 0, \ldots, 0) = (g_1, \ldots, g_n)$
3. $(v_1, \ldots, v_n) = \text{Lifting}(P, \alpha, \Delta)$ in $\mathbb{K}[y_1, \ldots, y_n]$, with $\Delta \geq \deg(h)$
4. Compute $f(v_1, \ldots, v_n)$
5. $h =$ Truncation of $f(v_1, \ldots, v_n)$ at degree Δ

The First Version of Our Main Algorithm

Given

- n algebraically independent polynomials $g_1, \ldots, g_n$ in $\mathbb{K}[x_1, \ldots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \ldots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \ldots, y_n]$ such that

$$h(g_1, \ldots, g_n) = f$$

1. Consider polynomials $P = (g_1 - y_1, \ldots, g_n - y_n)$ in $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_n]$
2. Let $\boldsymbol{\alpha}$ be a root of $P(x_1, \ldots, x_n, 0, \ldots, 0) = (g_1, \ldots, g_n)$
3. $(v_1, \ldots, v_n) = \text{Lifting}(P, \alpha, \Delta)$ in $\mathbb{K}[y_1, \ldots, y_n]$, with $\Delta \geq \deg(h)$
4. Compute $f(v_1, \ldots, v_n)$
5. $h =$ Truncation of $f(v_1, \ldots, v_n)$ at degree Δ

⚠ The Jacobian matrix of $(g_1, \ldots, g_n)$ might **not** has full rank at $\boldsymbol{\alpha}$

The First Version of Our Main Algorithm

Given

- n algebraically independent polynomials $g_1, \ldots, g_n$ in $\mathbb{K}[x_1, \ldots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \ldots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \ldots, y_n]$ such that

$$h(g_1, \ldots, g_n) = f$$

1. Consider polynomials $P = (g_1 - y_1, \ldots, g_n - y_n)$ in $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_n]$
2. Let $\boldsymbol{\alpha}$ be a root of $P(x_1, \ldots, x_n, 0, \ldots, 0) = (g_1, \ldots, g_n)$
3. $(v_1, \ldots, v_n) = \text{Lifting}(P, \alpha, \Delta)$ in $\mathbb{K}[y_1, \ldots, y_n]$, with $\Delta \geq \deg(h)$
4. Compute $f(v_1, \ldots, v_n)$
5. $h =$ Truncation of $f(v_1, \ldots, v_n)$ at degree Δ

Example:

$g_1 = x_1 + x_1$ and $g_2 = x_1^2 + x_2^2$, $\boldsymbol{\alpha} = (0, 0)$ is a root of g_1, g_2, and jac $= \begin{pmatrix} 1 & 1 \\ 2x_1 & 2x_2 \end{pmatrix}$

Ensuring Full-rank Jacobian Matrices at Solutions

Lemma

Let

- $(g_1, \ldots, g_n)$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$
- $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ be a random point in $\overline{\mathbb{K}}^n$

Then

- $\boldsymbol{\alpha}$ is a root of $\boldsymbol{P} = (g_1 - g_1(\boldsymbol{\alpha}), \ldots, g_n - g_n(\boldsymbol{\alpha}))$ and
- the Jacobian matrix of $\boldsymbol{P}$ has full rank at $\boldsymbol{\alpha}$

Ensuring Full-rank Jacobian Matrices at Solutions

Lemma

Let

- $(g_1, \ldots, g_n)$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$
- $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ be a random point in $\overline{\mathbb{K}}^n$

Then

- $\boldsymbol{\alpha}$ is a root of $\boldsymbol{P} = (g_1 - g_1(\boldsymbol{\alpha}), \ldots, g_n - g_n(\boldsymbol{\alpha}))$ and
- the Jacobian matrix of $\boldsymbol{P}$ has full rank at $\boldsymbol{\alpha}$

Example: With $g_1 = x_1 + x_2, g_2 = x_1^2 + x_2^2$ and $\boldsymbol{\alpha} = (-1, 3)$. Then

- $\boldsymbol{P} = (x_1 + x_2 - g_1(\boldsymbol{\alpha}), x_1^2 + x_2^2 - g_2(\boldsymbol{\alpha})) = (x_1 + x_2 - 2, x_1^2 + x_2^2 - 10)$

Ensuring Full-rank Jacobian Matrices at Solutions

Lemma

Let

- $(g_1, \ldots, g_n)$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$
- $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ be a random point in $\overline{\mathbb{K}}^n$

Then

- $\boldsymbol{\alpha}$ is a root of $\boldsymbol{P} = (g_1 - g_1(\boldsymbol{\alpha}), \ldots, g_n - g_n(\boldsymbol{\alpha}))$ and
- the Jacobian matrix of $\boldsymbol{P}$ has full rank at $\boldsymbol{\alpha}$

Example: With $g_1 = x_1 + x_2, g_2 = x_1^2 + x_2^2$ and $\boldsymbol{\alpha} = (-1, 3)$. Then

- $\boldsymbol{P} = (x_1 + x_2 - g_1(\boldsymbol{\alpha}), x_1^2 + x_2^2 - g_2(\boldsymbol{\alpha})) = (x_1 + x_2 - 2, x_1^2 + x_2^2 - 10)$
- $\mathrm{jac}(\boldsymbol{P}) = \begin{pmatrix} 1 & 1 \\ 2x_1 & 2x_2 \end{pmatrix}$ and $\mathrm{jac}(\boldsymbol{P})(\boldsymbol{\alpha}) = \begin{pmatrix} 1 & 1 \\ 4 & 20 \end{pmatrix}$ has full rank 2.

The Main Algorithm

Given

- n algebraically independent polynomials $g_1, \ldots, g_n$ in $\mathbb{K}[x_1, \ldots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \ldots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \ldots, y_n]$ such that

$$h(g_1, \ldots, g_n) = f$$

The Main Algorithm

Given

- n algebraically independent polynomials $g_1, \dots, g_n$ in $\mathbb{K}[x_1, \dots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \dots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \dots, y_n]$ such that

$$h(g_1, \dots, g_n) = f$$

0. Take a random point $\boldsymbol{\alpha} \in \mathbb{K}^n$

The Main Algorithm

Given

- n algebraically independent polynomials $g_1, \dots, g_n$ in $\mathbb{K}[x_1, \dots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \dots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \dots, y_n]$ such that

$$h(g_1, \dots, g_n) = f$$

0. Take a random point $\boldsymbol{\alpha} \in \mathbb{K}^n$
1. Find $\boldsymbol{P} = (g_1 - y_1 - g_1(\boldsymbol{\alpha}), \dots, g_n - y_n - g_n(\boldsymbol{\alpha}))$ in $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_n]$

The Main Algorithm

Given

- n algebraically independent polynomials $g_1, \dots, g_n$ in $\mathbb{K}[x_1, \dots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \dots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \dots, y_n]$ such that

$$h(g_1, \dots, g_n) = f$$

0. Take a random point $\boldsymbol{\alpha} \in \mathbb{K}^n$
1. Find $\boldsymbol{P} = (g_1 - y_1 - g_1(\boldsymbol{\alpha}), \dots, g_n - y_n - g_n(\boldsymbol{\alpha}))$ in $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_n]$
2. $\boldsymbol{\alpha}$ is a root of $P(x_1, \dots, x_n, 0, \dots, 0)$

The Main Algorithm

Given

- n algebraically independent polynomials $g_1, \ldots, g_n$ in $\mathbb{K}[x_1, \ldots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \ldots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \ldots, y_n]$ such that

$$h(g_1, \ldots, g_n) = f$$

0. Take a random point $\boldsymbol{\alpha} \in \mathbb{K}^n$
1. Find $\boldsymbol{P} = (g_1 - y_1 - g_1(\boldsymbol{\alpha}), \ldots, g_n - y_n - g_n(\boldsymbol{\alpha}))$ in $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_n]$
2. $\boldsymbol{\alpha}$ is a root of $P(x_1, \ldots, x_n, 0, \ldots, 0)$
3. $(v_1, \ldots, v_n) =$ Lifting$(P, \boldsymbol{\alpha}, \Delta)$ in $\mathbb{K}[y_1, \ldots, y_n]$, with $\Delta \geq \deg(h)$

The Main Algorithm

Given

- n algebraically independent polynomials $g_1, \dots, g_n$ in $\mathbb{K}[x_1, \dots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \dots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \dots, y_n]$ such that

$$h(g_1, \dots, g_n) = f$$

0. Take a random point $\boldsymbol{\alpha} \in \mathbb{K}^n$
1. Find $\boldsymbol{P} = (g_1 - y_1 - g_1(\boldsymbol{\alpha}), \dots, g_n - y_n - g_n(\boldsymbol{\alpha}))$ in $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_n]$
2. $\boldsymbol{\alpha}$ is a root of $P(x_1, \dots, x_n, 0, \dots, 0)$
3. $(v_1, \dots, v_n) =$ Lifting$(P, \boldsymbol{\alpha}, \Delta)$ in $\mathbb{K}[y_1, \dots, y_n]$, with $\Delta \geq \deg(h)$
4. Compute $f(v_1, \dots, v_n)$

The Main Algorithm

Given

- n algebraically independent polynomials $g_1, \dots, g_n$ in $\mathbb{K}[x_1, \dots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \dots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \dots, y_n]$ such that

$$h(g_1, \dots, g_n) = f$$

0. Take a random point $\boldsymbol{\alpha} \in \mathbb{K}^n$
1. Find $\boldsymbol{P} = (g_1 - y_1 - g_1(\boldsymbol{\alpha}), \dots, g_n - y_n - g_n(\boldsymbol{\alpha}))$ in $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_n]$
2. $\boldsymbol{\alpha}$ is a root of $P(x_1, \dots, x_n, 0, \dots, 0)$
3. $(v_1, \dots, v_n) =$ Lifting$(P, \boldsymbol{\alpha}, \Delta)$ in $\mathbb{K}[y_1, \dots, y_n]$, with $\Delta \geq \deg(h)$
4. Compute $f(v_1, \dots, v_n)$
5. $h_{\text{trunc}} =$ Truncation of $f(v_1, \dots, v_n)$ at degree Δ

The Main Algorithm

Given

- n algebraically independent polynomials $g_1, \dots, g_n$ in $\mathbb{K}[x_1, \dots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \dots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \dots, y_n]$ such that

$$h(g_1, \dots, g_n) = f$$

0. Take a random point $\boldsymbol{\alpha} \in \mathbb{K}^n$
1. Find $\boldsymbol{P} = (g_1 - y_1 - g_1(\boldsymbol{\alpha}), \dots, g_n - y_n - g_n(\boldsymbol{\alpha}))$ in $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_n]$
2. $\boldsymbol{\alpha}$ is a root of $P(x_1, \dots, x_n, 0, \dots, 0)$
3. $(v_1, \dots, v_n) =$ Lifting$(P, \boldsymbol{\alpha}, \Delta)$ in $\mathbb{K}[y_1, \dots, y_n]$, with $\Delta \geq \deg(h)$
4. Compute $f(v_1, \dots, v_n)$
5. $h_{\text{trunc}} =$ Truncation of $f(v_1, \dots, v_n)$ at degree Δ
6. $h = h_{\text{trunc}}(y_1 + g_1(\boldsymbol{\alpha}), \dots, y_n + g_n(\boldsymbol{\alpha}))$

The Main Algorithm

Given

- n algebraically independent polynomials $g_1, \dots, g_n$ in $\mathbb{K}[x_1, \dots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \dots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \dots, y_n]$ such that

$$h(g_1, \dots, g_n) = f$$

0. Take a random point $\boldsymbol{\alpha} \in \mathbb{K}^n$
1. Find $\boldsymbol{P} = (g_1 - y_1 - g_1(\boldsymbol{\alpha}), \dots, g_n - y_n - g_n(\boldsymbol{\alpha}))$ in $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_n]$
2. $\boldsymbol{\alpha}$ is a root of $P(x_1, \dots, x_n, 0, \dots, 0)$
3. $(v_1, \dots, v_n) = \text{Lifting}(P, \boldsymbol{\alpha}, \Delta)$ in $\mathbb{K}[y_1, \dots, y_n]$, with $\Delta \geq \deg(h)$
4. Compute $f(v_1, \dots, v_n)$
5. $h_{\text{trunc}} = $ Truncation of $f(v_1, \dots, v_n)$ at degree Δ
6. $h = h_{\text{trunc}}(y_1 + g_1(\boldsymbol{\alpha}), \dots, y_n + g_n(\boldsymbol{\alpha}))$

Some Degree Bounds

Given $W = (w_1, \dots, w_n) \in \mathbb{N}^n_{>0}$, the *$W$-degree*:

$$\deg_W(x_1^{k_1} \cdots x_n^{k_n}) = w_1 k_1 + \cdots + w_n k_n.$$

Some Degree Bounds

Given $W = (w_1, \dots, w_n) \in \mathbb{N}^n_{>0}$, the *$W$-degree*:

$$\deg_W(x_1^{k_1} \cdots x_n^{k_n}) = w_1 k_1 + \cdots + w_n k_n.$$

A poly is called *W-homogeneous* if all monomials have the same W-degree.

Some Degree Bounds

Given $W = (w_1, \dots, w_n) \in \mathbb{N}^n_{>0}$, the *$W$-degree*:

$$\deg_W(x_1^{k_1} \cdots x_n^{k_n}) = w_1 k_1 + \cdots + w_n k_n.$$

A poly is called *W-homogeneous* if all monomials have the same W-degree.

Example: With $W = (5, 2)$, $g_1 = x_1^2 + x_2^5$ is W-homogeneous with $\deg_W(g_1) = 10$ and $g_2 = x_2$ is W-homogeneous with $\deg_W(g_2) = 2$.

Some Degree Bounds

Given $W = (w_1, \dots, w_n) \in \mathbb{N}^n_{>0}$, the *$W$-degree*:

$$\deg_W(x_1^{k_1} \cdots x_n^{k_n}) = w_1 k_1 + \cdots + w_n k_n.$$

A poly is called *W-homogeneous* if all monomials have the same W-degree.

Example: With $W = (5, 2)$, $g_1 = x_1^2 + x_2^5$ is W-homogeneous with $\deg_W(g_1) = 10$ and $g_2 = x_2$ is W-homogeneous with $\deg_W(g_2) = 2$. Let $f = x_1^2$. Then $h = y_1 - y_2^5$ and $\deg_{W'}(h) = \deg_W(f) = 10$, where $W' = (\deg_W(g_1), \deg_W(g_2)) = (10, 2)$.

Some Degree Bounds

Given $W = (w_1, \dots, w_n) \in \mathbb{N}_{>0}^n$, the *W-degree*:

$$\deg_W(x_1^{k_1} \cdots x_n^{k_n}) = w_1 k_1 + \cdots + w_n k_n.$$

A poly is called *W-homogeneous* if all monomials have the same W-degree.

Example: With $W = (5, 2)$, $g_1 = x_1^2 + x_2^5$ is W-homogeneous with $\deg_W(g_1) = 10$ and $g_2 = x_2$ is W-homogeneous with $\deg_W(g_2) = 2$. Let $f = x_1^2$. Then $h = y_1 - y_2^5$ and $\deg_{W'}(h) = \deg_W(f) = 10$, where $W' = (\deg_W(g_1), \deg_W(g_2)) = (10, 2)$.

Lemma

Let $W = (w_1, \dots, w_n) \in \mathbb{N}_{>0}^n$ and

- $(g_1, \dots, g_n)$ be W-homogeneous, A. ID polynomials
- f be a polynomial in $\mathbb{K}[g_1, \dots, g_n]$

Let h be the poly such that $h(g_1, \dots, g_n) = f$. Then

$$\deg_{W'}(h) = \deg_W(f), \quad \text{where } W' = (\deg_W(g_1), \dots, \deg_W(g_n)).$$

Lemma

Let $W = (w_1, \dots, w_n) \in \mathbb{N}^n_{>0}$ and

- $(g_1, \dots, g_n)$ be W-homogeneous, A. ID polynomials
- f be a polynomial in $\mathbb{K}[g_1, \dots, g_n]$

Let h be the poly such that $h(g_1, \dots, g_n) = f$. Then

$$\deg_{W'}(h) = \deg_W(f), \quad \text{where } W' = (\deg_W(g_1), \dots, \deg_W(g_n)).$$

In particular, if $g_1, \dots, g_n$ are homogeneous (i.e, $W = (1, \dots, 1)$) A. ID polynomials

$$\deg(h) \leq \deg_{W'}(h) = \deg(f)$$

Lemma

Let $W = (w_1, \dots, w_n) \in \mathbb{N}_{>0}^n$ and

- $(g_1, \dots, g_n)$ be W-homogeneous, A. ID polynomials
- f be a polynomial in $\mathbb{K}[g_1, \dots, g_n]$

Let h be the poly such that $h(g_1, \dots, g_n) = f$. Then

$$\deg_{W'}(h) = \deg_W(f), \quad \text{where } W' = (\deg_W(g_1), \dots, \deg_W(g_n)).$$

In particular, if $g_1, \dots, g_n$ are homogeneous (i.e, $W = (1, \dots, 1)$) A. ID polynomials

$$\deg(h) \leq \deg_{W'}(h) = \deg(f)$$

$\Rightarrow$ invariant polynomials under finite pseudo-reflection groups

- symmetric groups,
- sign-symmetric groups,
- dihedral groups, ...

An Illustrative Example

Let $(g_1, g_2, g_3) = (x_1 + x_2 + x_3, x_1^2 + x_2^2 + x_3^2, x_1^3 + x_2^3 + x_3^3)$ and

- $f = x_1^3 + x_2^3 + x_3^3 - 2x_1x_2x_3 - x_1 - x_2 - x_3$

Find $h \in \mathbb{K}[y_1, y_2, y_3]$ such that $h(g_1, g_2, g_3) = f$

An Illustrative Example

Let $(g_1, g_2, g_3) = (x_1 + x_2 + x_3, x_1^2 + x_2^2 + x_3^2, x_1^3 + x_2^3 + x_3^3)$ and

- $f = x_1^3 + x_2^3 + x_3^3 - 2x_1x_2x_3 - x_1 - x_2 - x_3$

Find $h \in \mathbb{K}[y_1, y_2, y_3]$ such that $h(g_1, g_2, g_3) = f$ $\quad \deg(h) \leq \deg(f) = 3$

An Illustrative Example

Let $(g_1, g_2, g_3) = (x_1 + x_2 + x_3, x_1^2 + x_2^2 + x_3^2, x_1^3 + x_2^3 + x_3^3)$ and

- $f = x_1^3 + x_2^3 + x_3^3 - 2x_1x_2x_3 - x_1 - x_2 - x_3$

Find $h \in \mathbb{K}[y_1, y_2, y_3]$ such that $h(g_1, g_2, g_3) = f$ $\quad \deg(h) \leq \deg(f) = 3$

0. Take $\boldsymbol{\alpha} = (4, 6, 0)$

An Illustrative Example

Let $(g_1, g_2, g_3) = (x_1 + x_2 + x_3, x_1^2 + x_2^2 + x_3^2, x_1^3 + x_2^3 + x_3^3)$ and

- $f = x_1^3 + x_2^3 + x_3^3 - 2x_1x_2x_3 - x_1 - x_2 - x_3$

Find $h \in \mathbb{K}[y_1, y_2, y_3]$ such that $h(g_1, g_2, g_3) = f$ $\quad \deg(h) \leq \deg(f) = 3$

0. Take $\boldsymbol{\alpha} = (4, 6, 0)$
1. $\boldsymbol{P} = (g_1 - y_1 - g_1(\boldsymbol{\alpha}), g_2 - y_2 - g_2(\boldsymbol{\alpha}), g_3 - y_3 - g_3(\boldsymbol{\alpha})) =$
   $(x_1 + x_2 + x_3 - y_1 - 10, x_1^2 + x_2^2 + x_3^2 - y_2 - 52, x_1^3 + x_2^3 + x_3^3 - y_3 - 280)$

An Illustrative Example

Let $(g_1, g_2, g_3) = (x_1 + x_2 + x_3, x_1^2 + x_2^2 + x_3^2, x_1^3 + x_2^3 + x_3^3)$ and

- $f = x_1^3 + x_2^3 + x_3^3 - 2x_1x_2x_3 - x_1 - x_2 - x_3$

Find $h \in \mathbb{K}[y_1, y_2, y_3]$ such that $h(g_1, g_2, g_3) = f$ $\quad \deg(h) \leq \deg(f) = 3$

0. Take $\boldsymbol{\alpha} = (4, 6, 0)$
1. $\boldsymbol{P} = (g_1 - y_1 - g_1(\boldsymbol{\alpha}), g_2 - y_2 - g_2(\boldsymbol{\alpha}), g_3 - y_3 - g_3(\boldsymbol{\alpha})) =$
   $(x_1 + x_2 + x_3 - y_1 - 10, x_1^2 + x_2^2 + x_3^2 - y_2 - 52, x_1^3 + x_2^3 + x_3^3 - y_3 - 280)$
2. $\boldsymbol{\alpha}$ is a root of $P(x_1, x_2, x_3, 0, 0, 0)$

An Illustrative Example

Let $(g_1, g_2, g_3) = (x_1 + x_2 + x_3, x_1^2 + x_2^2 + x_3^2, x_1^3 + x_2^3 + x_3^3)$ and

- $f = x_1^3 + x_2^3 + x_3^3 - 2x_1x_2x_3 - x_1 - x_2 - x_3$

Find $h \in \mathbb{K}[y_1, y_2, y_3]$ such that $h(g_1, g_2, g_3) = f$ $\quad \deg(h) \leq \deg(f) = 3$

0. Take $\boldsymbol{\alpha} = (4, 6, 0)$
1. $\boldsymbol{P} = (g_1 - y_1 - g_1(\boldsymbol{\alpha}), g_2 - y_2 - g_2(\boldsymbol{\alpha}), g_3 - y_3 - g_3(\boldsymbol{\alpha})) =$
   $(x_1 + x_2 + x_3 - y_1 - 10, x_1^2 + x_2^2 + x_3^2 - y_2 - 52, x_1^3 + x_2^3 + x_3^3 - y_3 - 280)$
2. $\boldsymbol{\alpha}$ is a root of $P(x_1, x_2, x_3, 0, 0, 0)$
3. $(v_1, v_2, v_3) = \text{Lifting}(\boldsymbol{P}, \boldsymbol{\alpha}, 3)$
   $= (\frac{-1}{512}y_1y_2y_3 - \frac{11}{96}y_1^3 + \frac{33}{4096}y_2^3 - \frac{1}{55296}y_3^3 + \cdots, \frac{11}{2592}y_1y_2y_3 + \frac{1}{24}y_1^3 - \frac{197}{31104}y_2^3 +$
   $\frac{29}{1679616}y_3^3 + \cdots, \frac{-95}{41472}y_1y_2y_3 + \frac{7}{96}y_1^3 - \frac{1715}{995328}y_2^3 + \frac{11}{13436928}y_3^3 + \cdots)$

An Illustrative Example

Let $(g_1, g_2, g_3) = (x_1 + x_2 + x_3, x_1^2 + x_2^2 + x_3^2, x_1^3 + x_2^3 + x_3^3)$ and

- $f = x_1^3 + x_2^3 + x_3^3 - 2x_1x_2x_3 - x_1 - x_2 - x_3$

Find $h \in \mathbb{K}[y_1, y_2, y_3]$ such that $h(g_1, g_2, g_3) = f$ $\quad \deg(h) \leq \deg(f) = 3$

0. Take $\boldsymbol{\alpha} = (4, 6, 0)$
1. $\boldsymbol{P} = (g_1 - y_1 - g_1(\boldsymbol{\alpha}), g_2 - y_2 - g_2(\boldsymbol{\alpha}), g_3 - y_3 - g_3(\boldsymbol{\alpha})) =$
   $(x_1 + x_2 + x_3 - y_1 - 10, x_1^2 + x_2^2 + x_3^2 - y_2 - 52, x_1^3 + x_2^3 + x_3^3 - y_3 - 280)$
2. $\boldsymbol{\alpha}$ is a root of $P(x_1, x_2, x_3, 0, 0, 0)$
3. $(v_1, v_2, v_3) =$ Lifting$(\boldsymbol{P}, \boldsymbol{\alpha}, 3)$
   $= (\frac{-1}{512}y_1y_2y_3 - \frac{11}{96}y_1^3 + \frac{33}{4096}y_2^3 - \frac{1}{55296}y_3^3 + \cdots, \frac{11}{2592}y_1y_2y_3 + \frac{1}{24}y_1^3 - \frac{197}{31104}y_2^3 +$
   $\frac{29}{1679616}y_3^3 + \cdots, \frac{-95}{41472}y_1y_2y_3 + \frac{7}{96}y_1^3 - \frac{1715}{995328}y_2^3 + \frac{11}{13436928}y_3^3 + \cdots)$
4. Compute $f(v_1, v_2, v_3) = 270 + \frac{1}{3}y_3 + 10y_2 - 49y_1 + y_1y_2 - 10y_1^2 - \frac{1}{3}y_1^3 + \cdots$

An Illustrative Example

Let $(g_1, g_2, g_3) = (x_1 + x_2 + x_3, x_1^2 + x_2^2 + x_3^2, x_1^3 + x_2^3 + x_3^3)$ and

- $f = x_1^3 + x_2^3 + x_3^3 - 2x_1x_2x_3 - x_1 - x_2 - x_3$

Find $h \in \mathbb{K}[y_1, y_2, y_3]$ such that $h(g_1, g_2, g_3) = f$ $\quad \deg(h) \leq \deg(f) = 3$

0. Take $\boldsymbol{\alpha} = (4, 6, 0)$
1. $\boldsymbol{P} = (g_1 - y_1 - g_1(\boldsymbol{\alpha}), g_2 - y_2 - g_2(\boldsymbol{\alpha}), g_3 - y_3 - g_3(\boldsymbol{\alpha})) =$
   $(x_1 + x_2 + x_3 - y_1 - 10, x_1^2 + x_2^2 + x_3^2 - y_2 - 52, x_1^3 + x_2^3 + x_3^3 - y_3 - 280)$
2. $\boldsymbol{\alpha}$ is a root of $P(x_1, x_2, x_3, 0, 0, 0)$
3. $(v_1, v_2, v_3) =$ Lifting$(\boldsymbol{P}, \boldsymbol{\alpha}, 3)$
   $= (\frac{-1}{512}y_1y_2y_3 - \frac{11}{96}y_1^3 + \frac{33}{4096}y_2^3 - \frac{1}{55296}y_3^3 + \cdots, \frac{11}{2592}y_1y_2y_3 + \frac{1}{24}y_1^3 - \frac{197}{31104}y_2^3 +$
   $\frac{29}{1679616}y_3^3 + \cdots, \frac{-95}{41472}y_1y_2y_3 + \frac{7}{96}y_1^3 - \frac{1715}{995328}y_2^3 + \frac{11}{13436928}y_3^3 + \cdots)$
4. Compute $f(v_1, v_2, v_3) = 270 + \frac{1}{3}y_3 + 10y_2 - 49y_1 + y_1y_2 - 10y_1^2 - \frac{1}{3}y_1^3 + \cdots$
5. $h_{\text{trunc}} = -\frac{1}{3}y_1^3 - 10y_1^2 + y_1y_2 - 49y_1 + 10y_2 + \frac{1}{3}y_3 + 270$ `//* deg 3 truncation of` $f(\boldsymbol{v})$

An Illustrative Example

Let $(g_1, g_2, g_3) = (x_1 + x_2 + x_3, x_1^2 + x_2^2 + x_3^2, x_1^3 + x_2^3 + x_3^3)$ and

- $f = x_1^3 + x_2^3 + x_3^3 - 2x_1x_2x_3 - x_1 - x_2 - x_3$

Find $h \in \mathbb{K}[y_1, y_2, y_3]$ such that $h(g_1, g_2, g_3) = f$ $\quad \deg(h) \leq \deg(f) = 3$

0. Take $\boldsymbol{\alpha} = (4, 6, 0)$
1. $\boldsymbol{P} = (g_1 - y_1 - g_1(\boldsymbol{\alpha}), g_2 - y_2 - g_2(\boldsymbol{\alpha}), g_3 - y_3 - g_3(\boldsymbol{\alpha})) =$
   $(x_1 + x_2 + x_3 - y_1 - 10, x_1^2 + x_2^2 + x_3^2 - y_2 - 52, x_1^3 + x_2^3 + x_3^3 - y_3 - 280)$
2. $\boldsymbol{\alpha}$ is a root of $P(x_1, x_2, x_3, 0, 0, 0)$
3. $(v_1, v_2, v_3) =$ Lifting$(\boldsymbol{P}, \boldsymbol{\alpha}, 3)$
   $= (\frac{-1}{512}y_1y_2y_3 - \frac{11}{96}y_1^3 + \frac{33}{4096}y_2^3 - \frac{1}{55296}y_3^3 + \cdots, \frac{11}{2592}y_1y_2y_3 + \frac{1}{24}y_1^3 - \frac{197}{31104}y_2^3 +$
   $\frac{29}{1679616}y_3^3 + \cdots, \frac{-95}{41472}y_1y_2y_3 + \frac{7}{96}y_1^3 - \frac{1715}{995328}y_2^3 + \frac{11}{13436928}y_3^3 + \cdots)$
4. Compute $f(v_1, v_2, v_3) = 270 + \frac{1}{3}y_3 + 10y_2 - 49y_1 + y_1y_2 - 10y_1^2 - \frac{1}{3}y_1^3 + \cdots$
5. $h_{\text{trunc}} = -\frac{1}{3}y_1^3 - 10y_1^2 + y_1y_2 - 49y_1 + 10y_2 + \frac{1}{3}y_3 + 270$ `//* deg 3 truncation of` $f(\boldsymbol{v})$
6. $h = h_{\text{trunc}}(y_1 + g_1(\boldsymbol{\alpha}), y_2 + g_2(\boldsymbol{\alpha}), y_3 + g_3(\boldsymbol{\alpha})) = -\frac{1}{3}y_1^3 + y_1y_2 - y_1 + \frac{1}{3}y_3$

Even We Do Not Have The Degree Bounds?

Given: n algebraically independent polynomials $g_1, \dots, g_n$ in $\mathbb{K}[x_1, \dots, x_n]$ and a polynomial $f \in \mathbb{K}[g_1, \dots, g_n]$. Compute $h \in \mathbb{K}[y_1, \dots, y_n]$ such that $h(g_1, \dots, g_n) = f$.

0. Take a random point $\alpha \in \mathbb{K}^n$
1. Compute $P = (g_1 - y_1 - g_1(\alpha), \dots, g_n - y_n - g_n(\alpha))$ in $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_n]$
2. α is a root of $P(x_1, \dots, x_n, 0, \dots, 0)$
3. $(v_1, \dots, v_n) =$ Lifting(P, α, Δ) in $\mathbb{K}[y_1, \dots, y_n]$, with $\Delta \geq \deg(h)$
4. Compute $f(v_1, \dots, v_n)$
5. $h_{\text{trunc}} =$ Truncation of $f(v_1, \dots, v_n)$ at degree Δ
6. $h = h_{\text{trunc}}(y_1 + g_1(\alpha), \dots, y_n + g_n(\alpha))$

a bound $\deg(h) \leq \Delta$ is known in advance

Even We Do Not Have The Degree Bounds?

Given: n algebraically independent polynomials $g_1, \dots, g_n$ in $\mathbb{K}[x_1, \dots, x_n]$ and a polynomial $f \in \mathbb{K}[g_1, \dots, g_n]$. Compute $h \in \mathbb{K}[y_1, \dots, y_n]$ such that $h(g_1, \dots, g_n) = f$.

0. Take a random point $\alpha \in \mathbb{K}^n$
1. Compute $P = (g_1 - y_1 - g_1(\alpha), \dots, g_n - y_n - g_n(\alpha))$ in $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_n]$
2. α is a root of $P(x_1, \dots, x_n, 0, \dots, 0)$
3. $(v_1, \dots, v_n) =$ Lifting(P, α, δ) in $\mathbb{K}[y_1, \dots, y_n]$, with $\delta \in \{2, 4, 8, 16, \dots\}$
4. Compute $f(v_1, \dots, v_n)$
5. $h_{\text{trunc}} =$ Truncation of $f(v_1, \dots, v_n)$ at degree δ
6. $\overline{h} = h_{\text{trunc}}(y_1 + g_1(\alpha), \dots, y_n + g_n(\alpha))$

What if we do not know a bound for $\deg(h)$?

- use Lifting(P, α, δ) several times, for $\delta \in \{2, 4, 8, 16, \dots\}$
- for each δ,
  - run steps 4., 5., and 6.
  - add step 7. check if $\overline{h}(g_1, \dots, g_n)$ equals f

Done: Given

- n algebraically independent polynomials $g_1, \ldots, g_n$ in $\mathbb{K}[x_1, \ldots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \ldots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \ldots, y_n]$ such that $h(g_1, \ldots, g_n) = f$

Done: Given

- n algebraically independent polynomials $g_1, \dots, g_n$ in $\mathbb{K}[x_1, \dots, x_n]$
- a polynomial $f \in \mathbb{K}[g_1, \dots, g_n]$

Compute the unique polynomial $h \in \mathbb{K}[y_1, \dots, y_n]$ such that $h(g_1, \dots, g_n) = f$

Todo:

- faster algorithms; tight degree bounds for $\deg(h)$?
- extend to invariant rational functions
- compute the Hironaka decomposition of the invariant ring

$$f = \sum_{j=1}^{r} F_j(g_1, \dots, g_n) \cdot \sigma_j$$

- decomposing multivariate polynomials

given f; finding h and $g_1, \dots, g_n$

and solve decomposale polynomial systems?

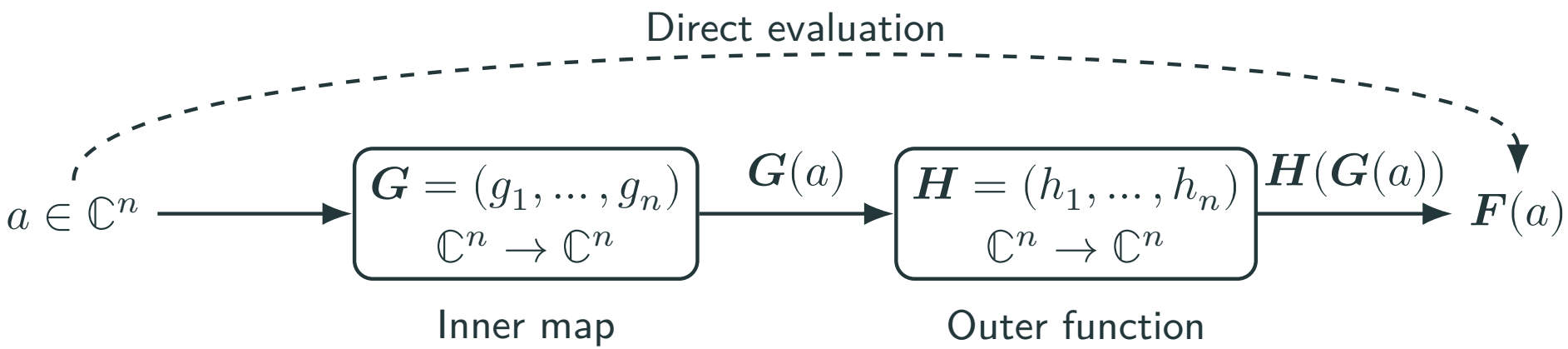
Solving composable polynomial systems

Given: polynomials $\boldsymbol{F} = (f_1, \ldots, f_n)$, $\boldsymbol{H} = (h_1, \ldots, h_n)$ and $\boldsymbol{G} = (g_1, \ldots, g_n)$ with

$$f_i = h_i(g_1, \ldots, g_n) \quad \text{for } i = 1, \ldots, n$$

Solve $f_1 = \cdots = f_n = 0$?

$$\begin{aligned} f_1 &= h_1(g_1(x_1, \ldots, x_n), \ldots, g_n(x_1, \ldots, x_n)) \\ &\vdots \\ f_n &= h_n(g_1(x_1, \ldots, x_n), \ldots, g_n(x_1, \ldots, x_n)) \end{aligned}$$



Main Result

Let

- $\boldsymbol{F} = (f_1, \ldots, f_n)$: polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$ with $f_i = h_i(g_1, \ldots, g_n)$
- L_h and L_g: sizes of $\boldsymbol{H}$ and $\boldsymbol{G}$ respectively
- $C = \deg(h_1) \cdots \deg(h_n)$ and $E = (\deg(h_1) + 1) \cdots (\deg(h_n) + 1)$
- $D = \deg(g_1) \cdots \deg(g_n)$ and $J = (\deg(g_1) + 1) \cdots (\deg(g_n) + 1)$.

Theorem

There exists a randomized algorithm to compute a zero-dimensional parametrization of the non-singular points of $\boldsymbol{F} = 0$ with the complexity

$$\tilde{O}(n(L_h + L_g + n^2)(CE + DJ + DC))$$

operations in $\mathbb{Q}$.

Main Result

Let

- $\boldsymbol{F} = (f_1, \ldots, f_n)$: polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$ with $f_i = h_i(g_1, \ldots, g_n)$
- L_h and L_g: sizes of $\boldsymbol{H}$ and $\boldsymbol{G}$ respectively
- $C = \deg(h_1) \cdots \deg(h_n)$ and $E = (\deg(h_1) + 1) \cdots (\deg(h_n) + 1)$
- $D = \deg(g_1) \cdots \deg(g_n)$ and $J = (\deg(g_1) + 1) \cdots (\deg(g_n) + 1)$.

Theorem

There exists a randomized algorithm to compute a zero-dimensional parametrization of the non-singular points of $\boldsymbol{F} = 0$ with the complexity

$$\tilde{O}(n(L_h + L_g + n^2)(CE + DJ + DC))$$

operations in $\mathbb{Q}$.

Note: • size of $\boldsymbol{F}$ is $O(L_h + L_g)$ • most of the cases $C \cdot D \ll \deg(f_1) \cdots \deg(f_n)$

Zero-dimensional Parametrizations

Let $V \subset \mathbb{C}^n$ be a finite set defined by polynomials in $\mathbb{Q}[x_1, \dots, x_n]$.

Rational Univariate Representation (R.U.R)

A R.U.R $\mathscr{R} = ((q, v_1, \dots, v_n), \lambda)$ of V

- a square-free poly $q \in \mathbb{Q}[T]$ with $\deg(q) = |V|$
- polynomials $v_1, \dots, v_n \in \mathbb{Q}[T]$, with $\deg(v_i) < \deg(q)$

$$q(T) = 0, \;\; x_i = \frac{v_i(T)}{q'(T)} \text{ with } \;\; q' = \frac{\partial q}{\partial T}$$

- a linear form $\lambda = \lambda_1 x_1 + \cdots + \lambda_n x_n$ with $\lambda_i \in \mathbb{Q}$

$$\lambda(v_1, \dots, v_n) \equiv T q' \pmod{q}$$

For $V = \{(1,0), (0,1)\}$,

- $q(T) = T^2 - 4T + 3$
- $v_1(T) = T - 3$
- $v_2(T) = T - 1$
- $\lambda = x_1 + 3x_2$

$T = 1, \; (x_1, x_2) = (1, 0)$

- $\frac{v_1(1)}{q'(1)} = \frac{-2}{-2} = 1$
- $\frac{v_2(1)}{q'(1)} = \frac{0}{-2} = 0$

$T = 3, \; (x_1, x_2) = (0, 1)$

Zero-dimensional Parametrizations

Let $V \subset \mathbb{C}^n$ be a finite set defined by polynomials in $\mathbb{Q}[x_1, \dots, x_n]$.

Rational Univariate Representation (R.U.R)

A R.U.R $\mathscr{R} = ((q, v_1, \dots, v_n), \lambda)$ of V

- a square-free poly $q \in \mathbb{Q}[T]$ with $\deg(q) = |V|$
- polynomials $v_1, \dots, v_n \in \mathbb{Q}[T]$, with $\deg(v_i) < \deg(q)$

$$q(T) = 0, \; x_i = \frac{v_i(T)}{q'(T)} \text{ with } \; q' = \frac{\partial q}{\partial T}$$

- a linear form $\lambda = \lambda_1 x_1 + \cdots + \lambda_n x_n$ with $\lambda_i \in \mathbb{Q}$

$$\lambda(v_1, \dots, v_n) \equiv T q' \pmod{q}$$

For $V = \{(1,0), (0,1)\}$,

- $q(T) = T^2 - 4T + 3$
- $v_1(T) = T - 3$
- $v_2(T) = T - 1$
- $\lambda = x_1 + 3x_2$

$T = 1, \; (x_1, x_2) = (1, 0)$

- $\frac{v_1(1)}{q'(1)} = \frac{-2}{-2} = 1$
- $\frac{v_2(1)}{q'(1)} = \frac{0}{-2} = 0$

$T = 3, \; (x_1, x_2) = (0, 1)$

Define:

$w_i \equiv (q')^{-1} v_i \pmod{q}$

Geometric Resolution $\mathscr{S} = ((q, w_1, \dots, w_n), \lambda)$ of V

$$q(T) = 0, \quad x_i = w_i(T), \quad \lambda(w_1, \dots, w_n) = T$$

$w_1(T) = \frac{3}{2} - \frac{T}{2}, \quad w_2(T) = -\frac{1}{2} + \frac{T}{2}$

$\mathscr{S} \leftarrow$ RUR_to_GR($\mathscr{R}$) $\quad \tilde{O}(n \deg(q))$

Global Newton-Hensel Lifting

Let $(\zeta_1(x_1,\dots,x_n,T),\dots,\zeta_n(x_1,\dots,x_n,T)) \subset \mathbb{Q}[x_1,\dots,x_n,T]^n$

Given $q(U), v_1(U),\dots,v_n(U)$-univar. polynomials

$$q(U)=0,\ \begin{cases} x_1 & = v_1(U) \\ & \cdots \\ x_n & = v_n(U), \end{cases} \qquad \boldsymbol{\zeta}(\boldsymbol{v}) = 0 \bmod \langle T^m, q(U)\rangle$$

$$\begin{cases} \zeta_1 = x_1 + x_2 - T - 1 \\ \zeta_2 = x_1 x_2 - T \\ q(U) = U^2 - 4U + 3 \\ v_1(U) = 3/2 - U/2 \\ v_2(U) = -1/2 + U/2 \end{cases}$$

$\zeta_i(v_1, v_2) \equiv -T \bmod q(U)$

Global Newton-Hensel Lifting

Let $(\zeta_1(x_1,\dots,x_n,T),\dots,\zeta_n(x_1,\dots,x_n,T)) \subset \mathbb{Q}[x_1,\dots,x_n,T]^n$

Given $q(U), v_1(U),\dots,v_n(U)$-univar. polynomials

$$q(U)=0,\ \begin{cases} x_1 &= v_1(U) \\ &\cdots \\ x_n &= v_n(U), \end{cases} \qquad \boldsymbol{\zeta}(\boldsymbol{v}) = 0 \bmod \langle T^m, q(U)\rangle$$

$$\begin{cases} \zeta_1 = x_1 + x_2 - T - 1 \\ \zeta_2 = x_1 x_2 - T \\ q(U) = U^2 - 4U + 3 \\ v_1(U) = 3/2 - U/2 \\ v_2(U) = -1/2 + U/2 \end{cases}$$

$\zeta_i(v_1, v_2) \equiv -T \bmod q(U)$

Compute bivar. polynomials $Q(U,T), V_1(U,T),\dots,V_n(U,T)$

$$Q(U,T)=0,\ \begin{cases} x_1 &= V_1(U) \\ &\cdots \\ x_n &= V_n(U), \end{cases} \qquad \boldsymbol{\zeta}(\boldsymbol{V}) = 0 \bmod \langle T^\delta, Q(U,T)\rangle \text{ with } \delta \geq m$$

Then $Q(U,T) = U^2 - 4U + 3 + 2T(5-U),\ V_1 = \frac{3}{2} - \frac{U}{2} + \frac{3T}{2},\ V_2 = -\frac{1}{2} + \frac{U}{2} - \frac{T}{2}$

with $\zeta_1(V_1, V_2) = -1/4(U^2 - 4U + 3 - 4UT + 10T + 3T^2) \equiv T^2 \bmod Q(U,T)$

Given: ◇ polynomials $\boldsymbol{\zeta} = (f_1, \ldots, f_n)$ in $\mathbb{Q}[x_1, \ldots, x_n, T]$

◇ monic poly. $q(U)$ and polys. $\boldsymbol{v} = (v_i(U))_{i=1}^{n}$ with $\deg(v_i) < \deg(q)$

◇ linear form $\lambda = \lambda_1 x_1 + \cdots + \lambda_n x_n$ and $\delta \in \mathbb{N}_{\geq 0}$

Assumptions: ◇ the Jacobian matrix of $\boldsymbol{\zeta}$ w.r.t $\boldsymbol{X}$ is invertible at $\boldsymbol{v}$ mod $q(U)$

◇ $\boldsymbol{\zeta}(\boldsymbol{v}) \equiv 0 \pmod{\langle T^m, q(U)\rangle}$

◇ $\lambda(\boldsymbol{v}) \equiv U \bmod q(U)$

GLS_Lifting$(\boldsymbol{\zeta}, q, \boldsymbol{v}, \lambda, \delta)$

◇ $\boldsymbol{V} \leftarrow \boldsymbol{v}$, $Q \leftarrow q$, $k \leftarrow m$, $J \leftarrow \frac{\partial \boldsymbol{\zeta}}{\partial \boldsymbol{X}}$ `// Initialize`

Given: ◇ polynomials $\boldsymbol{\zeta} = (f_1, \ldots, f_n)$ in $\mathbb{Q}[x_1, \ldots, x_n, T]$

◇ monic poly. $q(U)$ and polys. $\boldsymbol{v} = (v_i(U))_{i=1}^{n}$ with $\deg(v_i) < \deg(q)$

◇ linear form $\lambda = \lambda_1 x_1 + \cdots + \lambda_n x_n$ and $\delta \in \mathbb{N}_{\geq 0}$

Assumptions: ◇ the Jacobian matrix of $\boldsymbol{\zeta}$ w.r.t $\boldsymbol{X}$ is invertible at $\boldsymbol{v}$ mod $q(U)$

◇ $\boldsymbol{\zeta}(\boldsymbol{v}) \equiv 0 \pmod{\langle T^m, q(U)\rangle}$

◇ $\lambda(\boldsymbol{v}) \equiv U \bmod q(U)$

GLS_Lifting$(\boldsymbol{\zeta}, q, \boldsymbol{v}, \lambda, \delta)$

◇ $\boldsymbol{V} \leftarrow \boldsymbol{v}$, $Q \leftarrow q$, $k \leftarrow m$, $J \leftarrow \frac{\partial \boldsymbol{\zeta}}{\partial \boldsymbol{X}}$ `// Initialize`

◇ ***while*** $k < \delta$ ***do*** `// Update` (Q, V)

$$\boldsymbol{V} \leftarrow \boldsymbol{V} - J(\boldsymbol{V})^{-1}\boldsymbol{\zeta}(\boldsymbol{V}) \mod \langle T^k, Q\rangle$$
$$\Delta \leftarrow \lambda(\boldsymbol{V}) - U$$
$$\boldsymbol{V} \leftarrow \boldsymbol{V} - \left(\frac{\partial \boldsymbol{V}}{\partial U} \cdot \Delta \mod \langle T^k, Q\rangle\right)$$
$$Q \leftarrow Q - \left(\frac{\partial Q}{\partial U} \cdot \Delta \mod \langle T^k, Q\rangle\right)$$
$$k \leftarrow 2k$$

Given: ◇ polynomials $\boldsymbol{\zeta} = (f_1, \ldots, f_n)$ in $\mathbb{Q}[x_1, \ldots, x_n, T]$

◇ monic poly. $q(U)$ and polys. $\boldsymbol{v} = (v_i(U))_{i=1}^n$ with $\deg(v_i) < \deg(q)$

◇ linear form $\lambda = \lambda_1 x_1 + \cdots + \lambda_n x_n$ and $\delta \in \mathbb{N}_{\geq 0}$

Assumptions: ◇ the Jacobian matrix of $\boldsymbol{\zeta}$ w.r.t $\boldsymbol{X}$ is invertible at $\boldsymbol{v}$ mod $q(U)$

◇ $\boldsymbol{\zeta}(\boldsymbol{v}) \equiv 0 \pmod{\langle T^m, q(U)\rangle}$

◇ $\lambda(\boldsymbol{v}) \equiv U \bmod q(U)$

GLS_Lifting$(\boldsymbol{\zeta}, q, \boldsymbol{v}, \lambda, \delta)$

◇ $\boldsymbol{V} \leftarrow \boldsymbol{v}$, $Q \leftarrow q$, $k \leftarrow m$, $J \leftarrow \frac{\partial \boldsymbol{\zeta}}{\partial \boldsymbol{X}}$ `// Initialize`

◇ ***while*** $k < \delta$ ***do*** `// Update` (Q, V)

$$\boldsymbol{V} \leftarrow \boldsymbol{V} - J(\boldsymbol{V})^{-1}\boldsymbol{\zeta}(\boldsymbol{V}) \mod \langle T^k, Q\rangle$$
$$\Delta \leftarrow \lambda(\boldsymbol{V}) - U$$
$$\boldsymbol{V} \leftarrow \boldsymbol{V} - \left(\frac{\partial \boldsymbol{V}}{\partial U} \cdot \Delta \mod \langle T^k, Q\rangle\right)$$
$$Q \leftarrow Q - \left(\frac{\partial Q}{\partial U} \cdot \Delta \mod \langle T^k, Q\rangle\right)$$
$$k \leftarrow 2k$$

◇ ***end while***

Given: ◇ polynomials $\boldsymbol{\zeta} = (f_1, \ldots, f_n)$ in $\mathbb{Q}[x_1, \ldots, x_n, T]$

◇ monic poly. $q(U)$ and polys. $\boldsymbol{v} = (v_i(U))_{i=1}^n$ with $\deg(v_i) < \deg(q)$

◇ linear form $\lambda = \lambda_1 x_1 + \cdots + \lambda_n x_n$ and $\delta \in \mathbb{N}_{\geq 0}$

Assumptions: ◇ the Jacobian matrix of $\boldsymbol{\zeta}$ w.r.t $\boldsymbol{X}$ is invertible at $\boldsymbol{v}$ mod $q(U)$

◇ $\boldsymbol{\zeta}(\boldsymbol{v}) \equiv 0 \pmod{\langle T^m, q(U)\rangle}$

◇ $\lambda(\boldsymbol{v}) \equiv U \bmod q(U)$

GLS_Lifting$(\boldsymbol{\zeta}, q, \boldsymbol{v}, \lambda, \delta)$

◇ $\boldsymbol{V} \leftarrow \boldsymbol{v}$, $Q \leftarrow q$, $k \leftarrow m$, $J \leftarrow \frac{\partial \boldsymbol{\zeta}}{\partial \boldsymbol{X}}$ // Initialize

◇ ***while*** $k < \delta$ ***do*** // Update (Q, V)

$\boldsymbol{V} \leftarrow \boldsymbol{V} - J(\boldsymbol{V})^{-1}\boldsymbol{\zeta}(\boldsymbol{V}) \mod \langle T^k, Q\rangle$

$\Delta \leftarrow \lambda(\boldsymbol{V}) - U$

$\boldsymbol{V} \leftarrow \boldsymbol{V} - \left(\frac{\partial \boldsymbol{V}}{\partial U} \cdot \Delta \mod \langle T^k, Q\rangle\right)$

$Q \leftarrow Q - \left(\frac{\partial Q}{\partial U} \cdot \Delta \mod \langle T^k, Q\rangle\right)$

$k \leftarrow 2k$

◇ ***end while***

◇ return $(Q, \boldsymbol{V})$

a particular case of Alg. 1, Giusti–Lecerf–Salvy, 2001

$\tilde{O}((nL + n^\omega)\deg(q)\delta)$

L: size of $\boldsymbol{\zeta}$

Symbolic Homotopy Continuation

Given: polynomials $\boldsymbol{H} = (h_1, \ldots, h_n)$ in $\mathbb{Q}[x_1, \ldots, x_n]$ of size L

Compute: a zero-dimensional parametrization of the isolated points of $\boldsymbol{H} = 0$

Denote: $C = \deg(h_1) \cdots \deg(h_n)$ and $E = (\deg(h_1) + 1) \cdots (\deg(h_n) + 1)$

Symbolic_Homotopy($\boldsymbol{H}$)

- construct "start system" p_i as product of $\deg(h_i)$ random linear forms

Symbolic Homotopy Continuation

Given: polynomials $\boldsymbol{H} = (h_1, \ldots, h_n)$ in $\mathbb{Q}[x_1, \ldots, x_n]$ of size L

Compute: a zero-dimensional parametrization of the isolated points of $\boldsymbol{H} = 0$

Denote: $C = \deg(h_1) \cdots \deg(h_n)$ and $E = (\deg(h_1) + 1) \cdots (\deg(h_n) + 1)$

Symbolic_Homotopy($\boldsymbol{H}$)

- construct "start system" p_i as product of $\deg(h_i)$ random linear forms
- compute a RUR $\mathscr{R}_0 = (q_0, (v_{0,1}, \ldots, v_{0,n}), u)$ of $\boldsymbol{P} = (p_1, \ldots, p_n)$

$q_0, v_{0,i} \in \mathbb{Q}[U]$; `Gaussian elimination + interpolation`; $O(Cn^3)$

Symbolic Homotopy Continuation

Given: polynomials $\boldsymbol{H} = (h_1, \ldots, h_n)$ in $\mathbb{Q}[x_1, \ldots, x_n]$ of size L

Compute: a zero-dimensional parametrization of the isolated points of $\boldsymbol{H} = 0$

Denote: $C = \deg(h_1) \cdots \deg(h_n)$ and $E = (\deg(h_1) + 1) \cdots (\deg(h_n) + 1)$

Symbolic_Homotopy($\boldsymbol{H}$)

- construct "start system" p_i as product of $\deg(h_i)$ random linear forms
- compute a RUR $\mathscr{R}_0 = (q_0, (v_{0,1}, \ldots, v_{0,n}), u)$ of $\boldsymbol{P} = (p_1, \ldots, p_n)$

  $q_0, v_{0,i} \in \mathbb{Q}[U]$; `Gaussian elimination + interpolation`; $O(Cn^3)$
- define a homotopy $\boldsymbol{R}(\boldsymbol{X}, T) = (1 - T) \cdot \boldsymbol{H}(\boldsymbol{X}) + T \cdot \boldsymbol{P}(\boldsymbol{X})$

Symbolic Homotopy Continuation

Given: polynomials $\boldsymbol{H} = (h_1, \ldots, h_n)$ in $\mathbb{Q}[x_1, \ldots, x_n]$ of size L

Compute: a zero-dimensional parametrization of the isolated points of $\boldsymbol{H} = 0$

Denote: $C = \deg(h_1) \cdots \deg(h_n)$ and $E = (\deg(h_1) + 1) \cdots (\deg(h_n) + 1)$

Symbolic_Homotopy($\boldsymbol{H}$)

- construct "start system" p_i as product of $\deg(h_i)$ random linear forms
- compute a RUR $\mathscr{R}_0 = (q_0, (v_{0,1}, \ldots, v_{0,n}), u)$ of $\boldsymbol{P} = (p_1, \ldots, p_n)$

  $q_0, v_{0,i} \in \mathbb{Q}[U]$; `Gaussian elimination + interpolation`; $O(Cn^3)$
- define a homotopy $\boldsymbol{R}(\boldsymbol{X}, T) = (1 - T) \cdot \boldsymbol{H}(\boldsymbol{X}) + T \cdot \boldsymbol{P}(\boldsymbol{X})$
- lift $\mathscr{R}_0$ along $\boldsymbol{R}$ to a RUR $\mathscr{R}$ in $\mathbb{Q}[[T]]/\langle T^{2E} \rangle$

  $\mathscr{R} \leftarrow$ GLS_Lifting$(\boldsymbol{R}, q_0, \boldsymbol{v}_0, u, E)$; E: degree of homotopy curve $\quad O((nL' + n^\omega)CE)$

Symbolic Homotopy Continuation

Given: polynomials $\boldsymbol{H} = (h_1, \ldots, h_n)$ in $\mathbb{Q}[x_1, \ldots, x_n]$ of size L

Compute: a zero-dimensional parametrization of the isolated points of $\boldsymbol{H} = 0$

Denote: $C = \deg(h_1) \cdots \deg(h_n)$ and $E = (\deg(h_1) + 1) \cdots (\deg(h_n) + 1)$

Symbolic_Homotopy($\boldsymbol{H}$)

- construct "start system" p_i as product of $\deg(h_i)$ random linear forms
- compute a RUR $\mathscr{R}_0 = (q_0, (v_{0,1}, \ldots, v_{0,n}), u)$ of $\boldsymbol{P} = (p_1, \ldots, p_n)$

  $q_0, v_{0,i} \in \mathbb{Q}[U]$; `Gaussian elimination + interpolation`; $O(Cn^3)$
- define a homotopy $\boldsymbol{R}(\boldsymbol{X}, T) = (1 - T) \cdot \boldsymbol{H}(\boldsymbol{X}) + T \cdot \boldsymbol{P}(\boldsymbol{X})$
- lift $\mathscr{R}_0$ along $\boldsymbol{R}$ to a RUR $\mathscr{R}$ in $\mathbb{Q}[[T]]/\langle T^{2E} \rangle$

  $\mathscr{R} \leftarrow$ GLS_Lifting($\boldsymbol{R}, q_0, \boldsymbol{v}_0, u, E$); E: degree of homotopy curve $\quad O((nL' + n^\omega)CE)$
- rational reconstruction on $\mathscr{R}$ to obtain RUR $\mathscr{S} \subset \mathbb{Q}(T)$ $\quad \tilde{O}(CEn)$

Symbolic Homotopy Continuation

Given: polynomials $\boldsymbol{H} = (h_1, \ldots, h_n)$ in $\mathbb{Q}[x_1, \ldots, x_n]$ of size L

Compute: a zero-dimensional parametrization of the isolated points of $\boldsymbol{H} = 0$

Denote: $C = \deg(h_1) \cdots \deg(h_n)$ and $E = (\deg(h_1) + 1) \cdots (\deg(h_n) + 1)$

Symbolic_Homotopy($\boldsymbol{H}$)

- construct "start system" p_i as product of $\deg(h_i)$ random linear forms
- compute a RUR $\mathscr{R}_0 = (q_0, (v_{0,1}, \ldots, v_{0,n}), u)$ of $\boldsymbol{P} = (p_1, \ldots, p_n)$

  $q_0, v_{0,i} \in \mathbb{Q}[U]$; `Gaussian elimination + interpolation`; $O(Cn^3)$
- define a homotopy $\boldsymbol{R}(\boldsymbol{X}, T) = (1 - T) \cdot \boldsymbol{H}(\boldsymbol{X}) + T \cdot \boldsymbol{P}(\boldsymbol{X})$
- lift $\mathscr{R}_0$ along $\boldsymbol{R}$ to a RUR $\mathscr{R}$ in $\mathbb{Q}[[T]]/\langle T^{2E} \rangle$

  $\mathscr{R} \leftarrow$ GLS_Lifting$(\boldsymbol{R}, q_0, \boldsymbol{v}_0, u, E)$; E: degree of homotopy curve $\quad O((nL' + n^\omega)CE)$
- rational reconstruction on $\mathscr{R}$ to obtain RUR $\mathscr{S} \subset \mathbb{Q}(T)$ $\quad \tilde{O}(CEn)$
- deduce a RUR $\mathscr{R}_1$ over k $\quad \tilde{O}(CEn)$

Symbolic Homotopy Continuation

Given: polynomials $\boldsymbol{H} = (h_1, \ldots, h_n)$ in $\mathbb{Q}[x_1, \ldots, x_n]$ of size L

Compute: a zero-dimensional parametrization of the isolated points of $\boldsymbol{H} = 0$

Denote: $C = \deg(h_1) \cdots \deg(h_n)$ and $E = (\deg(h_1) + 1) \cdots (\deg(h_n) + 1)$

Symbolic_Homotopy($\boldsymbol{H}$)

- construct "start system" p_i as product of $\deg(h_i)$ random linear forms
- compute a RUR $\mathscr{R}_0 = (q_0, (v_{0,1}, \ldots, v_{0,n}), u)$ of $\boldsymbol{P} = (p_1, \ldots, p_n)$

  $q_0, v_{0,i} \in \mathbb{Q}[U]$; `Gaussian elimination + interpolation`; $O(Cn^3)$
- define a homotopy $\boldsymbol{R}(\boldsymbol{X}, T) = (1 - T) \cdot \boldsymbol{H}(\boldsymbol{X}) + T \cdot \boldsymbol{P}(\boldsymbol{X})$
- lift $\mathscr{R}_0$ along $\boldsymbol{R}$ to a RUR $\mathscr{R}$ in $\mathbb{Q}[[T]]/\langle T^{2E} \rangle$

  $\mathscr{R} \leftarrow$ GLS_Lifting$(\boldsymbol{R}, q_0, \boldsymbol{v}_0, u, E)$; E: degree of homotopy curve $\quad O((nL' + n^\omega)CE)$
- rational reconstruction on $\mathscr{R}$ to obtain RUR $\mathscr{S} \subset \mathbb{Q}(T)$ $\quad \tilde{O}(CEn)$
- deduce a RUR $\mathscr{R}_1$ over k $\quad \tilde{O}(CEn)$
- Remove non-isolated points in $V(\boldsymbol{H})$ $\quad \tilde{O}(C^6(n^4 + nL'))$

[*] Remove singular points $\tilde{O}(C^2(n^3 + nL'))$

Our problem:

$$\begin{cases} f_1 & = h_1(g_1(x_1, \dots, x_n), \dots, g_n(x_1, \dots, x_n)) \\ & \vdots \\ f_n & = h_n(g_1(x_1, \dots, x_n), \dots, g_n(x_1, \dots, x_n)) \end{cases}$$

Done:

$$\begin{cases} h_1(y_1, \dots, y_n) & = 0 \\ & \vdots \\ h_n(y_1, \dots, y_n) & = 0 \end{cases}$$

- $(q_h(T), v_1(T), \dots, v_n(T), \mu)$: a geometric resolution of $\boldsymbol{H} = 0$

Our problem:

$$\begin{cases} f_1 &= h_1(g_1(x_1,\dots,x_n),\dots,g_n(x_1,\dots,x_n)) \\ &\vdots \\ f_n &= h_n(g_1(x_1,\dots,x_n),\dots,g_n(x_1,\dots,x_n)) \end{cases}$$

Done:

$$\begin{cases} h_1(y_1,\dots,y_n) &= 0 \\ &\vdots \\ h_n(y_1,\dots,y_n) &= 0 \end{cases}$$

Remain:

$$q_h(T)=0,\quad \begin{cases} g_1(x_1,\dots,x_n) &= v_1(T) \\ &\vdots \\ g_n(x_1,\dots,x_n) &= v_n(T) \end{cases}$$

- $(q_h(T), v_1(T),\dots,v_n(T),\mu)$: a geometric resolution of $\boldsymbol{H}=0$

$$q_h(T)=0,\quad \begin{cases} y_1 &= v_1(T) \\ &\vdots \\ y_n &= v_n(T) \end{cases} \qquad \mu(v_1,\dots,v_n)\equiv T \bmod q_h(T),\quad \deg(q_h)\le C$$

Solving the inner system

$$g_1(x_1, \dots, x_n) - v_1(T) = \cdots = g_n(x_1, \dots, x_n) - v_n(T) = 0$$

Find: $Q(U,T) \in \mathbb{Q}[U,T]$, $\boldsymbol{V} = (V_1, \dots, V_n) \in \mathbb{Q}[U,T]^n$, $\lambda = \lambda_1 x_1 + \cdots + \lambda_n x_n$

`with` $\boldsymbol{G}(V_1, \dots, V_n) - \boldsymbol{V}(T) \equiv 0$ and $\lambda(V_1, \dots, V_n) \equiv U \bmod \langle T^C, Q(U,T) \rangle$

Main idea: GLS_Lifting, with full-rank Jacobian?

Solving the inner system

$$g_1(x_1, \dots, x_n) - v_1(T) = \cdots = g_n(x_1, \dots, x_n) - v_n(T) = 0$$

Find: $Q(U,T) \in \mathbb{Q}[U,T]$, $\boldsymbol{V} = (V_1, \dots, V_n) \in \mathbb{Q}[U,T]^n$, $\lambda = \lambda_1 x_1 + \cdots + \lambda_n x_n$

`with` $\boldsymbol{G}(V_1, \dots, V_n) - \boldsymbol{V}(T) \equiv 0$ and $\lambda(V_1, \dots, V_n) \equiv U \bmod \langle T^C, Q(U,T) \rangle$

Main idea: GLS_Lifting, with full-rank Jacobian?

random shift $S := T - s_0, s_0 \in \mathbb{Q}$

Solving the inner system

$$g_1(x_1, \ldots, x_n) - v_1(T) = \cdots = g_n(x_1, \ldots, x_n) - v_n(T) = 0$$

Find: $Q(U,T) \in \mathbb{Q}[U,T]$, $\boldsymbol{V} = (V_1, \ldots, V_n) \in \mathbb{Q}[U,T]^n$, $\lambda = \lambda_1 x_1 + \cdots + \lambda_n x_n$

`with` $\boldsymbol{G}(V_1, \ldots, V_n) - \boldsymbol{V}(T) \equiv 0$ and $\lambda(V_1, \ldots, V_n) \equiv U \bmod \langle T^C, Q(U,T) \rangle$

Main idea: GLS_Lifting, with full-rank Jacobian?

random shift $S := T - s_0, s_0 \in \mathbb{Q}$

Parametric$(\boldsymbol{G}, \boldsymbol{V}, C)$ $\quad D = \deg(g_1) \cdots \deg(g_n) \quad J = (\deg(g_1)+1) \cdots (\deg(g_n)+1)$

1. $\boldsymbol{P}(\boldsymbol{X}, S) \leftarrow \boldsymbol{G}(\boldsymbol{X}) - \boldsymbol{V}(S + s_0)$
2. $(\overline{q}, (\overline{w}_1, \ldots, \overline{w}_n), \lambda) \leftarrow$ geometric resolution of $\boldsymbol{P}(\boldsymbol{X}, 0)$ `//* in` $\mathbb{Q}[U]$ $\quad \tilde{O}(DJn(L_g + n^2))$
3. $(Q_{\text{shift}}, (V_{1,\text{shift}}, \ldots, V_{n,\text{shift}})) \leftarrow$ GLS_Lifting$(\boldsymbol{P}, \overline{q}, \overline{\boldsymbol{w}}, \lambda, 2C)$ $\quad \tilde{O}(n(L_g + n^2)\, D\, C)$
4. $Q_{\text{poly}} \leftarrow \text{RationalReconstruct}(Q_{\text{shift}}, C)$; $V_{i,\text{poly}} \leftarrow \text{RationalReconstruct}(V_{i,\text{shift}}, C)$
5. $Q(U,T) \leftarrow Q_{\text{poly}}(U, T - s_0)$; $V_i(U,T) \leftarrow V_{i,\text{poly}}(U, T - s_0)$

Our problem:

$$\begin{cases} f_1 &= h_1(g_1(x_1, \dots, x_n), \dots, g_n(x_1, \dots, x_n)) \\ &\vdots \\ f_n &= h_n(g_1(x_1, \dots, x_n), \dots, g_n(x_1, \dots, x_n)) \end{cases}$$

Done:

$$\begin{cases} h_1(y) &= 0 \\ &\vdots \\ h_n(y) &= 0 \end{cases}$$

Remain:

$$q_h(T) = 0, \quad \begin{cases} g_1(x) &= v_1(T) \\ &\vdots \\ g_n(x) &= v_n(T) \end{cases}$$

Our problem:

$$\begin{cases} f_1 &= h_1(g_1(x_1,\dots,x_n),\dots,g_n(x_1,\dots,x_n)) \\ &\vdots \\ f_n &= h_n(g_1(x_1,\dots,x_n),\dots,g_n(x_1,\dots,x_n)) \end{cases}$$

Done:

$$\begin{cases} h_1(y) &= 0 \\ &\vdots \\ h_n(y) &= 0 \end{cases}$$

Remain:

$$q_h(T) = 0, \quad \begin{cases} g_1(x) &= v_1(T) \\ &\vdots \\ g_n(x) &= v_n(T) \end{cases}$$

Done:

$$\begin{cases} g_1(x) &= v_1(T) \\ &\vdots \\ g_n(x) &= v_n(T) \end{cases}$$

Remain of Remain:

$$q_h(T) = 0,$$

$$Q(U,T) = 0, \quad \begin{cases} x_1 &= V_1(U,T) \\ &\vdots \\ x_n &= V_n(U,T) \end{cases}$$

Remain of Remain:

$$q_h(T) = 0, \quad Q(U,T) = 0$$

$$\begin{cases} x_1 & = V_1(U,T) \\ & \vdots \\ x_n & = V_n(U,T) \end{cases}$$

1. $(\Psi_{\text{prec}}(S), v(S), \tau(S), U) \leftarrow$ a geometric resolution of $Q(U,T) = q_h(T) = 0$

   /* Symbolic_Homotopy(Q, q_h) */

2. $W_{i,\text{prec}}(S) \leftarrow V_i(v(S), \tau(S))$

Sum Up – The Main Algorithm

Given: $\boldsymbol{H} = (h_1, \ldots, h_n) \in \mathbb{Q}[y_1, \ldots, y_n]^n$, $\boldsymbol{G} = (g_1, \ldots, g_n) \in \mathbb{Q}[x_1, \ldots, x_n]^n$

Compute: a zero-dimensional parametrization $(\Psi(S), (W_1(S), \ldots, W_n(S), \lambda))$ of isolated/regular points of $\boldsymbol{H}(\boldsymbol{G}(\boldsymbol{X})) = 0$.

Solve_h_circ_g(h,g)

1. $(q_h(T), v_1(T), \ldots, v_n(T), \mu) \leftarrow$ a geometric resolution of $\boldsymbol{H} = 0$

   /* Symbolic_Homotopy → RUR_to_GR */

2. $C \leftarrow \deg(q_h)$ $\qquad C \leq \prod \deg(h_i)$

3. $(Q(U,T), V_1(U,T), \ldots, V_n(U,T), \lambda) \leftarrow$ Parametric$(\boldsymbol{G}, \boldsymbol{V}, C)$

4. $(\Psi_{\text{prec}}(S), \upsilon(S), \tau(S), U) \leftarrow$ a geometric resolution of $Q(U,T) = q_h(T) = 0$

   /* Symbolic_Homotopy → RUR_to_GR */

5. $W_{i,\text{prec}}(S) \leftarrow V_i(\upsilon(S), \tau(S))$

6. $(\Psi(S), (W_1(S), \ldots, W_n(S), \lambda)) \leftarrow$ Remove $(\Psi_{\text{prec}}(S), (\boldsymbol{W}_{\text{prec}}(S), \lambda))$

An Example $f_1 = h_1(g_1, g_2),\ f_2 = h_2(g_1, g_2)$

Solve:

$$\begin{cases} f_1 &= x_1 + x_2 - x_1 x_2 - 1 \\ f_2 &= x_1^2 x_2^2 + x_1 x_2 \end{cases}$$

Outer system:

$$\begin{cases} h_1 &= y_1 - y_2 \\ h_2 &= y_2^2 + y_2 \end{cases}$$

Inner system:

$$\begin{cases} g_1 &= x_1 + x_2 \\ g_2 &= x_1 x_2 \end{cases}$$

An Example $f_1 = h_1(g_1, g_2),\ f_2 = h_2(g_1, g_2)$

Solve:

$$\begin{cases} f_1 &= x_1 + x_2 - x_1x_2 - 1 \\ f_2 &= x_1^2x_2^2 + x_1x_2 \end{cases}$$

Outer system:

$$\begin{cases} h_1 &= y_1 - y_2 \\ h_2 &= y_2^2 + y_2 \end{cases}$$

Inner system:

$$\begin{cases} g_1 &= x_1 + x_2 \\ g_2 &= x_1x_2 \end{cases}$$

- GR of $h_1 = h_2 = 0$:

$$q_h(T) = T^2 + T, \quad v_1(T) = T + 1, \quad v_2(T) = T$$

An Example $f_1 = h_1(g_1, g_2),\ f_2 = h_2(g_1, g_2)$

Solve:

$$\begin{cases} f_1 &= x_1 + x_2 - x_1x_2 - 1 \\ f_2 &= x_1^2x_2^2 + x_1x_2 \end{cases}$$

Outer system:

$$\begin{cases} h_1 &= y_1 - y_2 \\ h_2 &= y_2^2 + y_2 \end{cases}$$

Inner system:

$$\begin{cases} g_1 &= x_1 + x_2 \\ g_2 &= x_1x_2 \end{cases}$$

◇ GR of $h_1 = h_2 = 0$:

$$q_h(T) = T^2 + T, \quad v_1(T) = T + 1, \quad v_2(T) = T$$

◇ Parametric$(\boldsymbol{G}, \boldsymbol{V}, C)$, with $C = \deg(g_1) \cdot \deg(g_2) = 2$:

$$\lambda = x_1 + 3x_2$$

$$Q(U, T) = U^2 - (4T + 4)U + (3T^2 + 10T + 3)$$

$$V_1(U, T) = \tfrac{3}{2} - \tfrac{U}{2} + \tfrac{3T}{2} \quad V_2(U, T) = -\tfrac{1}{2} + \tfrac{U}{2} - \tfrac{T}{2}$$

An Example $f_1 = h_1(g_1, g_2),\ f_2 = h_2(g_1, g_2)$

Solve:

$$\begin{cases} f_1 &= x_1 + x_2 - x_1x_2 - 1 \\ f_2 &= x_1^2x_2^2 + x_1x_2 \end{cases}$$

Outer system:

$$\begin{cases} h_1 &= y_1 - y_2 \\ h_2 &= y_2^2 + y_2 \end{cases}$$

Inner system:

$$\begin{cases} g_1 &= x_1 + x_2 \\ g_2 &= x_1x_2 \end{cases}$$

- GR of $h_1 = h_2 = 0$:

$$q_h(T) = T^2 + T, \quad v_1(T) = T + 1, \quad v_2(T) = T$$

- Parametric$(\boldsymbol{G}, \boldsymbol{V}, C)$, with $C = \deg(g_1) \cdot \deg(g_2) = 2$:

$$\lambda = x_1 + 3x_2$$

$$Q(U, T) = U^2 - (4T + 4)U + (3T^2 + 10T + 3)$$

$$V_1(U, T) = \tfrac{3}{2} - \tfrac{U}{2} + \tfrac{3T}{2} \quad V_2(U, T) = -\tfrac{1}{2} + \tfrac{U}{2} - \tfrac{T}{2}$$

- GR of $Q(U, T) = q_h(T) = 0$:

$$\Psi(S) = S^4 - 4S^3 - S^2 + 16S - 12$$

$$\upsilon(S) = S, \quad \tau(S) = \tfrac{4}{15}S^3 - \tfrac{9}{15}S^2 - \tfrac{16}{15}S - \tfrac{21}{15}$$

An Example $f_1 = h_1(g_1, g_2),\ f_2 = h_2(g_1, g_2)$

Solve:
$$\begin{cases} f_1 &= x_1 + x_2 - x_1x_2 - 1 \\ f_2 &= x_1^2x_2^2 + x_1x_2 \end{cases}$$

Outer system:
$$\begin{cases} h_1 &= y_1 - y_2 \\ h_2 &= y_2^2 + y_2 \end{cases}$$

Inner system:
$$\begin{cases} g_1 &= x_1 + x_2 \\ g_2 &= x_1x_2 \end{cases}$$

◇ GR of $h_1 = h_2 = 0$:

$$q_h(T) = T^2 + T, \quad v_1(T) = T + 1, \quad v_2(T) = T$$

◇ Parametric$(\boldsymbol{G}, \boldsymbol{V}, C)$, with $C = \deg(g_1) \cdot \deg(g_2) = 2$:

$$\lambda = x_1 + 3x_2$$
$$Q(U, T) = U^2 - (4T + 4)U + (3T^2 + 10T + 3)$$
$$V_1(U, T) = \tfrac{3}{2} - \tfrac{U}{2} + \tfrac{3T}{2} \quad V_2(U, T) = -\tfrac{1}{2} + \tfrac{U}{2} - \tfrac{T}{2}$$

◇ GR of $Q(U, T) = q_h(T) = 0$:

$$\Psi(S) = S^4 - 4S^3 - S^2 + 16S - 12$$
$$\upsilon(S) = S, \quad \tau(S) = \tfrac{4}{15}S^3 - \tfrac{9}{15}S^2 - \tfrac{16}{15}S - \tfrac{21}{15}$$

◇ Final GR of $f_1 = f_2 = 0$:

$$\lambda = x_1 + 3x_2, \quad \Psi(S) = S^4 - 4S^3 - S^2 + 16S - 12$$
$$W_1(S) = \tfrac{2}{5}S^3 - \tfrac{9}{10}S^2 - \tfrac{21}{10}S + \tfrac{18}{5}, \quad W_2(S) = -\tfrac{2}{15}S^3 + \tfrac{3}{10}S^2 + \tfrac{31}{30}S - \tfrac{6}{5}$$

Solve:

$$\begin{cases} f_1 &= x_1 + x_2 - x_1x_2 - 1 \\ f_2 &= x_1^2x_2^2 + x_1x_2 \end{cases}$$

Outer system:

$$\begin{cases} h_1 &= y_1 - y_2 \\ h_2 &= y_2^2 + y_2 \end{cases}$$

Inner system:

$$\begin{cases} g_1 &= x_1 + x_2 \\ g_2 &= x_1x_2 \end{cases}$$

◇ a GR of $f_1 = f_2 = 0$:

$$\lambda = x_1 + 3x_2,\ \Psi(S) = S^4 - 4S^3 - S^2 + 16S - 12 = 0,\ \begin{cases} W_1(S) = \frac{2}{5}S^3 - \frac{9}{10}S^2 - \frac{21}{10}S + \frac{18}{5}, \\ W_2(S) = -\frac{2}{15}S^3 + \frac{3}{10}S^2 + \frac{31}{30}S - \frac{6}{5} \end{cases}$$

Solve:

$$\begin{cases} f_1 &= x_1 + x_2 - x_1x_2 - 1 \\ f_2 &= x_1^2x_2^2 + x_1x_2 \end{cases}$$

Outer system:

$$\begin{cases} h_1 &= y_1 - y_2 \\ h_2 &= y_2^2 + y_2 \end{cases}$$

Inner system:

$$\begin{cases} g_1 &= x_1 + x_2 \\ g_2 &= x_1x_2 \end{cases}$$

◇ a GR of $f_1 = f_2 = 0$:

$$\lambda = x_1 + 3x_2,\ \Psi(S) = S^4 - 4S^3 - S^2 + 16S - 12 = 0,\ \begin{cases} W_1(S) = \frac{2}{5}S^3 - \frac{9}{10}S^2 - \frac{21}{10}S + \frac{18}{5}, \\ W_2(S) = -\frac{2}{15}S^3 + \frac{3}{10}S^2 + \frac{31}{30}S - \frac{6}{5} \end{cases}$$

◇ $\Psi(S) = 0$ has 4 solutions $S \in \{-2, 1, 2, 3\}$. The solutions of $f_1 = f_2 = 0$ are

$$(x_1, x_2) = (W_1(S), W_2(S) \in \{(1, -1), (1, 0), (-1, 1), (0, 1)\}$$

Solve:
$$\begin{cases} f_1 &= x_1 + x_2 - x_1x_2 - 1 \\ f_2 &= x_1^2x_2^2 + x_1x_2 \end{cases}$$

Outer system:
$$\begin{cases} h_1 &= y_1 - y_2 \\ h_2 &= y_2^2 + y_2 \end{cases}$$

Inner system:
$$\begin{cases} g_1 &= x_1 + x_2 \\ g_2 &= x_1x_2 \end{cases}$$

◇ a GR of $f_1 = f_2 = 0$:

$$\lambda = x_1 + 3x_2,\ \Psi(S) = S^4 - 4S^3 - S^2 + 16S - 12 = 0,\ \begin{cases} W_1(S) = \frac{2}{5}S^3 - \frac{9}{10}S^2 - \frac{21}{10}S + \frac{18}{5}, \\ W_2(S) = -\frac{2}{15}S^3 + \frac{3}{10}S^2 + \frac{31}{30}S - \frac{6}{5} \end{cases}$$

◇ $\Psi(S) = 0$ has 4 solutions $S \in \{-2, 1, 2, 3\}$. The solutions of $f_1 = f_2 = 0$ are

$$(x_1, x_2) = (W_1(S), W_2(S) \in \{(1, -1), (1, 0), (-1, 1), (0, 1)\}$$

Final Remark: Solving the $f_1 = f_2 = 0$ directly gives a bound

$$\deg(f_1) \cdot \deg(f_2) = 8 > 4$$

on the number of points we need to compute.

Done: a polynomial time (in the sizes of the input and the output) algorithm to compute a zero-dimensional parametrization of a system composable polynomials

$$f_1 = h_1(g_1, \dots, g_n), \dots, f_n = h_n(g_1, \dots, g_n)$$

Done: a polynomial time (in the sizes of the input and the output) algorithm to compute a zero-dimensional parametrization of a system composable polynomials

$$f_1 = h_1(g_1, \dots, g_n), \dots, f_n = h_n(g_1, \dots, g_n)$$

Todo:

- hybrid numeric-symbolic algorithms
- exploiting the sparsity
- real solutions (emptiness, connectivity of real algebraic sets, ...)
- applications in optimization, cryptology, ...