A Symbolic Homotopy Algorithm for Solving Composable Polynomial Systems

Thi Xuan Vu

Université de Lille, France

An example

Computing the zeros of

$$\begin{cases} f_1 & = x_1 + x_2 - x_1 x_2 - 1 = 0 \\ f_2 & = x_1^2 x_2^2 + x_1 x_2 = 0 \end{cases}$$

An example

Computing the zeros of

$$\begin{cases} f_1 & = x_1 + x_2 - x_1 x_2 - 1 = 0 \\ f_2 & = x_1^2 x_2^2 + x_1 x_2 = 0 \end{cases}$$

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

An example

Computing the zeros of

$$\begin{cases} f_1 &= x_1 + x_2 - x_1 x_2 - 1 = 0 \\ f_2 &= x_1^2 x_2^2 + x_1 x_2 = 0 \end{cases}$$

$$\begin{cases} f_1 &= x_1 + x_2 - x_1 x_2 - 1 = h_1(g_1, g_2) \\ f_2 &= (x_1 x_2)^2 + x_1 x_2 = h_2(g_1, g_2) \end{cases}$$

with $\begin{cases} g_1 &= x_1 + x_2 \\ g_2 &= x_1 x_2 \end{cases}$ and $\begin{cases} h_1 &= y_1 - y_2 - 1 \\ h_2 &= y_2^2 + y_2 \end{cases}$

An example

Computing the zeros of

$$\begin{cases} f_1 & = x_1 + x_2 - x_1 x_2 - 1 = 0 \\ f_2 & = x_1^2 x_2^2 + x_1 x_2 = 0 \end{cases}$$

$$\begin{cases} f_1 & = x_1 + x_2 - x_1 x_2 - 1 = h_1(g_1, g_2) \\ f_2 & = (x_1 x_2)^2 + x_1 x_2 = h_2(g_1, g_2) \end{cases}$$

with $\begin{cases} g_1 & = x_1 + x_2 \\ g_2 & = x_1 x_2 \end{cases}$ and $\begin{cases} h_1 & = y_1 - y_2 - 1 \\ h_2 & = y_2^2 + y_2 \end{cases}$

$$\boldsymbol{F} = \boldsymbol{H}(\boldsymbol{G}) = \boldsymbol{H} \circ \boldsymbol{G}$$

An example

Computing the zeros of

$$\begin{cases} f_1 &= x_1 + x_2 - x_1x_2 - 1 = 0 \\ f_2 &= x_1^2x_2^2 + x_1x_2 = 0 \end{cases}$$

$$\begin{cases} f_1 &= x_1 + x_2 - x_1x_2 - 1 = h_1(g_1, g_2) \\ f_2 &= (x_1x_2)^2 + x_1x_2 = h_2(g_1, g_2) \end{cases}$$

with $\begin{cases} g_1 &= x_1 + x_2 \\ g_2 &= x_1x_2 \end{cases}$ and $\begin{cases} h_1 &= y_1 - y_2 - 1 \\ h_2 &= y_2^2 + y_2 \end{cases}$

$$\boldsymbol{F} = \boldsymbol{H}(\boldsymbol{G}) = \boldsymbol{H} \circ \boldsymbol{G}$$

this type of equations appears frequenly in

- invariant theory (e.g., symmetric groups),
- cryptology,
- decoupling problem, ...

Our problem and the main result

Given: polynomials $\boldsymbol{F} = (f_1, \dots, f_n)$, $\boldsymbol{H} = (h_1, \dots, h_n)$ and $\boldsymbol{G} = (g_1, \dots, g_n)$ s.t

$$\boldsymbol{F} = \boldsymbol{H}(\boldsymbol{G}) = \boldsymbol{H} \circ \boldsymbol{G}$$

Solve: $\boldsymbol{F}(x_1, \dots, x_n) = 0$

Our problem and the main result

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

$$\boldsymbol{F} = \boldsymbol{H}(\boldsymbol{G}) = \boldsymbol{H} \circ \boldsymbol{G}$$

Solve: $\boldsymbol{F}(x_1, \ldots, x_n) = 0$

Theorem

There exists a randomized of Monte Carlo type algorithm to compute a parametrization of the isolated points of $\boldsymbol{F} = 0$ with the complexity

$$((L_H + L_G)nCD)^{O(1)}$$

operations in $\mathbb{Q}$. Moreover, the number of points we have to compute is bounded by $C \cdot D$.

- L_H, L_G: the sizes of straight-line programs of H and G
- $C = \deg(h_1) \cdots \deg(h_n)$
- $D = \deg(g_1) \cdots \deg(g_n)$

What do we mean by solving?

Given a system $\boldsymbol{F} = (f_1, \dots, f_n)$ in $\mathbb{Q}[x_1, \dots, x_n]$. A univariate representation of the isolated point set $Z \subset \mathbb{C}^n$ of $\boldsymbol{F} = 0$ are given by

- $(n+1)$ univariate polynomials $(q, v_1, \dots, v_n))$ in $\mathbb{Q}[T]$ s.t. q is square-free, $\deg(q) = |Z|$, $\deg(v_i) < \deg(q)$ and

$$q(T) = 0, \quad x_1 = v_1(T), \dots, x_n = v_n(T)$$

What do we mean by solving?

Given a system $\boldsymbol{F} = (f_1, \dots, f_n)$ in $\mathbb{Q}[x_1, \dots, x_n]$. A univariate representation of the isolated point set $Z \subset \mathbb{C}^n$ of $\boldsymbol{F} = 0$ are given by

- $(n+1)$ univariate polynomials $(q, v_1, \dots, v_n))$ in $\mathbb{Q}[T]$ s.t. q is square-free, $\deg(q) = |Z|$, $\deg(v_i) < \deg(q)$ and

$$q(T) = 0, \quad x_1 = v_1(T), \dots, x_n = v_n(T)$$

Example: $f_1 = x_1 + x_2 - x_1x_2 - 1$ and $f_2 = x_1^2x_2^2 + x_1x_2$

What do we mean by solving?

Given a system $\boldsymbol{F} = (f_1, \dots, f_n)$ in $\mathbb{Q}[x_1, \dots, x_n]$. A univariate representation of the isolated point set $Z \subset \mathbb{C}^n$ of $\boldsymbol{F} = 0$ are given by

- $(n+1)$ univariate polynomials $(q, v_1, \dots, v_n))$ in $\mathbb{Q}[T]$ s.t. q is square-free, $\deg(q) = |Z|$, $\deg(v_i) < \deg(q)$ and

$$q(T) = 0, \quad x_1 = v_1(T), \dots, x_n = v_n(T)$$

Example: $f_1 = x_1 + x_2 - x_1x_2 - 1$ and $f_2 = x_1^2x_2^2 + x_1x_2$

- the solutions of $f_1 = f_2 = 0$ are

$$(x_1, x_2) \in \{(1, -1), (1, 0), (-1, 1), (0, 1)\}$$

What do we mean by solving?

Given a system $\boldsymbol{F} = (f_1, \dots, f_n)$ in $\mathbb{Q}[x_1, \dots, x_n]$. A univariate representation of the isolated point set $Z \subset \mathbb{C}^n$ of $\boldsymbol{F} = 0$ are given by

- $(n+1)$ univariate polynomials $(q, v_1, \dots, v_n))$ in $\mathbb{Q}[T]$ s.t. q is square-free, $\deg(q) = |Z|$, $\deg(v_i) < \deg(q)$ and

$$q(T) = 0, \quad x_1 = v_1(T), \dots, x_n = v_n(T)$$

Example: $f_1 = x_1 + x_2 - x_1 x_2 - 1$ and $f_2 = x_1^2 x_2^2 + x_1 x_2$

- the solutions of $f_1 = f_2 = 0$ are

$$(x_1, x_2) \in \{(1, -1), (1, 0), (-1, 1), (0, 1)\}$$

- a representation for zeros of $f_1 = f_2 = 0$:

$$q(T) = T^4 - 4T^3 - T^2 + 16T - 12 = 0, \begin{cases} v_1(T) = \frac{2}{5}T^3 - \frac{9}{10}T^2 - \frac{21}{10}T + \frac{18}{5}, \\ v_2(T) = -\frac{2}{15}T^3 + \frac{3}{10}T^2 + \frac{31}{30}T - \frac{6}{5} \end{cases}$$

What do we mean by solving?

Given a system $\boldsymbol{F} = (f_1, \dots, f_n)$ in $\mathbb{Q}[x_1, \dots, x_n]$. A univariate representation of the isolated point set $Z \subset \mathbb{C}^n$ of $\boldsymbol{F} = 0$ are given by

- $(n+1)$ univariate polynomials $(q, v_1, \dots, v_n))$ in $\mathbb{Q}[T]$ s.t. q is square-free, $\deg(q) = |Z|$, $\deg(v_i) < \deg(q)$ and

$$q(T) = 0, \quad x_1 = v_1(T), \dots, x_n = v_n(T)$$

Example: $f_1 = x_1 + x_2 - x_1x_2 - 1$ and $f_2 = x_1^2x_2^2 + x_1x_2$

- the solutions of $f_1 = f_2 = 0$ are

$$(x_1, x_2) \in \{(1, -1), (1, 0), (-1, 1), (0, 1)\}$$

- a representation for zeros of $f_1 = f_2 = 0$:

$$q(T) = T^4 - 4T^3 - T^2 + 16T - 12 = 0, \begin{cases} v_1(T) = \frac{2}{5}T^3 - \frac{9}{10}T^2 - \frac{21}{10}T + \frac{18}{5}, \\ v_2(T) = -\frac{2}{15}T^3 + \frac{3}{10}T^2 + \frac{31}{30}T - \frac{6}{5} \end{cases}$$

- $q(T) = 0$ has 4 solutions $T \in \{-2, 1, 2, 3\}$.

Solving $\boldsymbol{F} = \boldsymbol{H} \circ \boldsymbol{G} = \boldsymbol{H}(\boldsymbol{G}) = \boldsymbol{0}$

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

A very first naive try: solving $\boldsymbol{F} = 0$ directly

Solving $\boldsymbol{F} = \boldsymbol{H} \circ \boldsymbol{G} = \boldsymbol{H}(\boldsymbol{G}) = \mathbf{0}$

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

A very first naive try: solving $\boldsymbol{F} = 0$ directly, but

- the complexity depends on the Bézout bound $M = \deg(f_1) \cdots \deg(f_n)$
  - in many cases, M is **not** a good bound

Solving $F = H \circ G = H(G) = 0$

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

A very first naive try: solving $F = 0$ directly, but

- the complexity depends on the Bézout bound $M = \deg(f_1) \cdots \deg(f_n)$
  - in many cases, M is **not** a good bound

Example

With $f_1 = x_1 + x_2 - x_1x_2 - 1$ and $f_2 = x_1^2x_2^2 + x_1x_2$, $f_1 = f_2 = 0$ has **4** solutions and $M = \deg(f_1) \cdot \deg(f_2) = 2 \cdot 4 = 8$

Solving $F = H \circ G = H(G) = 0$

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

A very first naive try: solving $F = 0$ directly, but

- the complexity depends on the Bézout bound $M = \deg(f_1) \cdots \deg(f_n)$
  - in many cases, M is **not** a good bound
- not taking the **composable** structure

Solving $F = H \circ G = H(G) = 0$

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

A very first naive try: solving $F = 0$ directly, but

- the complexity depends on the Bézout bound $M = \deg(f_1) \cdots \deg(f_n)$
  - in many cases, M is **not** a good bound
- not taking the **composable** structure

Our very natural try: decomposing using new variables $(y_1, \ldots, y_n)$

Solving $F = H \circ G = H(G) = 0$

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

A very first naive try: solving $F = 0$ directly, but

- the complexity depends on the Bézout bound $M = \deg(f_1) \cdots \deg(f_n)$
  - in many cases, M is **not** a good bound
- not taking the **composable** structure

Our very natural try: decomposing using new variables $(y_1, \dots, y_n)$

$$\boxed{F(x_1, \dots, x_n) = 0 \Leftrightarrow \begin{cases} H(y_1, \dots, y_n) & = 0 \\ G(x_1, \dots, x_n) & = Y \end{cases}}$$

$$\boldsymbol{F}(x_1, \dots, x_n) = 0 \Leftrightarrow \begin{cases} \boldsymbol{H}(y_1, \dots, y_n) & = 0 \\ \boldsymbol{G}(x_1, \dots, x_n) & = \boldsymbol{Y} \end{cases}$$

The Simpler Step - Solving

$$h_1(y_1, \dots, y_n) = \dots = h_n(y_1, \dots, y_n) = 0$$

$$\boldsymbol{F}(x_1, \dots, x_n) = 0 \Leftrightarrow \begin{cases} \boldsymbol{H}(y_1, \dots, y_n) & = 0 \\ \boldsymbol{G}(x_1, \dots, x_n) & = \boldsymbol{Y} \end{cases}$$

The Simpler Step - Solving

$$h_1(y_1, \dots, y_n) = \cdots = h_n(y_1, \dots, y_n) = 0$$

- using symbolic homotopy techniques

$$\boldsymbol{F}(x_1, \dots, x_n) = 0 \Leftrightarrow \begin{cases} \boldsymbol{H}(y_1, \dots, y_n) & = 0 \\ \boldsymbol{G}(x_1, \dots, x_n) & = \boldsymbol{Y} \end{cases}$$

The Simpler Step - Solving

$$h_1(y_1, \dots, y_n) = \cdots = h_n(y_1, \dots, y_n) = 0$$

- using symbolic homotopy techniques
- this gives a univariate repr. $(q_h(T), v_1(T), \dots, v_n(T))$ of $\boldsymbol{H}(\boldsymbol{Y}) = 0$, i.e.,

$$q_h(T) = 0, \begin{cases} y_1 & = v_1(T) \\ & \vdots \\ y_n & = v_n(T) \end{cases} \quad \text{with} \quad \deg(v_i) < \deg(q_h) \leq C$$

$$\boldsymbol{F}(x_1, \ldots, x_n) = 0 \Leftrightarrow \begin{cases} \boldsymbol{H}(y_1, \ldots, y_n) & = 0 \\ \boldsymbol{G}(x_1, \ldots, x_n) & = \boldsymbol{Y} \end{cases}$$

The Simpler Step - Solving

$$h_1(y_1, \ldots, y_n) = \cdots = h_n(y_1, \ldots, y_n) = 0$$

- using symbolic homotopy techniques
- this gives a univariate repr. $(q_h(T), v_1(T), \ldots, v_n(T))$ of $\boldsymbol{H}(\boldsymbol{Y}) = 0$, i.e.,

$$q_h(T) = 0, \begin{cases} y_1 & = v_1(T) \\ & \vdots \\ y_n & = v_n(T) \end{cases} \text{with} \quad \deg(v_i) < \deg(q_h) \leq C$$

The More Challenging Step - Solving

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

$$\boldsymbol{F}(x_1, \dots, x_n) = 0 \Leftrightarrow \begin{cases} \boldsymbol{H}(y_1, \dots, y_n) & = 0 \\ \boldsymbol{G}(x_1, \dots, x_n) & = \boldsymbol{Y} \end{cases}$$

The Simpler Step - Solving

$$h_1(y_1, \dots, y_n) = \cdots = h_n(y_1, \dots, y_n) = 0$$

- using symbolic homotopy techniques
- this gives a univariate repr. $(q_h(T), v_1(T), \dots, v_n(T))$ of $\boldsymbol{H}(\boldsymbol{Y}) = 0$, i.e.,

$$q_h(T) = 0, \begin{cases} y_1 & = v_1(T) \\ & \vdots \\ y_n & = v_n(T) \end{cases} \quad \text{with} \quad \deg(v_i) < \deg(q_h) \leq C$$

The More Challenging Step - Solving

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

- ignoring $q_h(T)$ and studying

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

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

Step 1: Computing a univar. repr. $q(U), w_1(U), \dots, w_n(U)$ of $\boldsymbol{G}(\boldsymbol{X}) - \boldsymbol{v}(0) = 0$

$$q(U) = 0,\ x_1 = w_1(U), \dots, x_n = w_n(U),\ \boldsymbol{G}(\boldsymbol{w}) - \boldsymbol{v}(0) = 0 \text{ mod } q(U)$$

`//* symbolic homotopy techniques`

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

Step 1: Computing a univar. repr. $q(U), w_1(U), \dots, w_n(U)$ of $\boldsymbol{G}(\boldsymbol{X}) - \boldsymbol{v}(0) = 0$

$$q(U) = 0,\ x_1 = w_1(U), \dots, x_n = w_n(U),\ \boldsymbol{G}(\boldsymbol{w}) - \boldsymbol{v}(0) = 0 \text{ mod } q(U)$$

```
//* symbolic homotopy techniques
```

Step 2: **Lifting** this univar. repr. to a representation

$$(Q(U,T), W_1(U,T), \dots, W_n(U,T)),$$

upto degree δ, for "symbolic" variable T

$$Q(U,T) = 0,\ \begin{cases} x_1 & = W_1(U,T) \\ & \dots \\ x_n & = W_n(U,T) \end{cases},\ \ \boldsymbol{G}(\boldsymbol{W}) - \boldsymbol{v}(T) = 0 \text{ mod } \langle T^\delta, Q(U,T) \rangle \ \ (\delta \in \mathbb{N}_{\geq 1})$$

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

Step 1: Computing a univar. repr. $q(U), w_1(U), \ldots, w_n(U)$ of $\boldsymbol{G}(\boldsymbol{X}) - \boldsymbol{v}(0) = 0$

$$q(U) = 0,\ x_1 = w_1(U), \ldots, x_n = w_n(U),\ \boldsymbol{G}(\boldsymbol{w}) - \boldsymbol{v}(0) = 0 \text{ mod } q(U)$$

```
//* symbolic homotopy techniques
```

Step 2: **Lifting** this univar. repr. to a representation

$$(Q(U,T), W_1(U,T), \ldots, W_n(U,T)),$$

upto degree δ, for "symbolic" variable T

$$Q(U,T) = 0,\ \begin{cases} x_1 & = W_1(U,T) \\ & \cdots \\ x_n & = W_n(U,T) \end{cases},\ \boldsymbol{G}(\boldsymbol{W}) - \boldsymbol{v}(T) = 0 \text{ mod } \langle T^\delta, Q(U,T)\rangle \quad (\delta \in \mathbb{N}_{\geq 1})$$

In particular, $Q(U,0) = q(U), W_1(U,0) = w_1(U), \ldots, W_n(U,0) = w_n(U)$

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

Step 1: Computing a univar. repr. $q(U), w_1(U), \dots, w_n(U)$ of $\boldsymbol{G}(\boldsymbol{X}) - \boldsymbol{v}(0) = 0$

$$q(U) = 0,\ x_1 = w_1(U), \dots, x_n = w_n(U),\ \boldsymbol{G}(\boldsymbol{w}) - \boldsymbol{v}(0) = 0 \text{ mod } q(U)$$

Step 2 Lifting:

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

Step 1: Computing a univar. repr. $q(U), w_1(U), \ldots, w_n(U)$ of $\boldsymbol{G}(\boldsymbol{X}) - \boldsymbol{v}(0) = 0$

$$q(U) = 0,\ x_1 = w_1(U), \ldots, x_n = w_n(U),\ \boldsymbol{G}(\boldsymbol{w}) - \boldsymbol{v}(0) = 0 \text{ mod } q(U)$$

Step 2 Lifting:

- $\boldsymbol{\zeta} := \boldsymbol{G}(\boldsymbol{X}) - \boldsymbol{v}(T)$
- $\boldsymbol{W} \leftarrow \boldsymbol{w}$, $Q \leftarrow q$, $k \leftarrow 0$, $J \leftarrow \frac{\partial \boldsymbol{G}}{\partial \boldsymbol{X}}$ `//* Initialize`

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

Step 1: Computing a univar. repr. $q(U), w_1(U), \dots, w_n(U)$ of $\boldsymbol{G}(\boldsymbol{X}) - \boldsymbol{v}(0) = 0$

$$q(U) = 0,\ x_1 = w_1(U), \dots, x_n = w_n(U),\ \boldsymbol{G}(\boldsymbol{w}) - \boldsymbol{v}(0) = 0 \text{ mod } q(U)$$

Step 2 Lifting:

- $\boldsymbol{\zeta} := \boldsymbol{G}(\boldsymbol{X}) - \boldsymbol{v}(T)$
- $\boldsymbol{W} \leftarrow \boldsymbol{w},\ Q \leftarrow q,\ k \leftarrow 0,\ J \leftarrow \frac{\partial \boldsymbol{G}}{\partial \boldsymbol{X}}$ `//* Initialize`
- **while** $k < \delta$ **do**: `//* Update` $(\boldsymbol{Q}, \boldsymbol{V})$

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

$$\Delta \leftarrow \lambda(\boldsymbol{W}) - U$$ `//*` λ: a linear form in $\boldsymbol{X}$

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

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

$$k \leftarrow 2k$$

- **end while**
- **return** $(Q, \boldsymbol{W})$

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

Step 1: Computing a univar. repr. $q(U), w_1(U), \dots, w_n(U)$ of $\boldsymbol{G}(\boldsymbol{X})-\boldsymbol{v}(0)=0$

$$q(U)=0,\ x_1=w_1(U),\dots,x_n=w_n(U),\ \boldsymbol{G}(\boldsymbol{w})-\boldsymbol{v}(0)=0 \text{ mod } q(U)$$

Step 2 Lifting:

- $\boldsymbol{\zeta} := \boldsymbol{G}(\boldsymbol{X})-\boldsymbol{v}(T)$
- $\boldsymbol{W}\leftarrow \boldsymbol{w}$, $Q\leftarrow q$, $k\leftarrow 0$, $J\leftarrow \frac{\partial \boldsymbol{G}}{\partial \boldsymbol{X}}$ `//* Initialize`
- **while** $k<\delta$ **do**: `//* Update` $(\boldsymbol{Q},\boldsymbol{V})$

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

$$\varDelta \leftarrow \lambda(\boldsymbol{W})-U$$ `//*` λ: a linear form in $\boldsymbol{X}$

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

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

$$k\leftarrow 2k$$

- **end while**
- **return** $(Q,\boldsymbol{W})$

Requirement: Jacobian matrix J of $\boldsymbol{G}$ w.r.t $\boldsymbol{X}$ is invertible at $\boldsymbol{w}$ mod $q(U)$

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

Step 0: random shift $T := T + s_0, s_0 \in \mathbb{Q}$

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

Step 0: random shift $T := T + s_0, s_0 \in \mathbb{Q}$

Step 1': Computing a univar. repr. $q(U), w_1(U), \dots, w_n(U)$

$$q(U) = 0,\ x_1 = w_1(U), \dots, x_n = w_n(U),\ \boldsymbol{G}(\boldsymbol{w}) - \boldsymbol{v}(0 + s_0) = 0 \text{ mod } q(U)$$

Step 2: **Lifting** this univar. repr. to a representation

$$(Q(U,T), W_1(U,T), \dots, W_n(U,T)),$$

upto degree δ, for "symbolic" variable T

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

Step 0: random shift $T := T + s_0, s_0 \in \mathbb{Q}$

Step 1': Computing a univar. repr. $q(U), w_1(U), \dots, w_n(U)$

$$q(U) = 0,\ x_1 = w_1(U), \dots, x_n = w_n(U),\ \boldsymbol{G}(\boldsymbol{w}) - \boldsymbol{v}(0 + s_0) = 0 \bmod q(U)$$

Step 2: **Lifting** this univar. repr. to a representation

$$(Q(U,T), W_1(U,T), \dots, W_n(U,T)),$$

upto degree δ, for "symbolic" variable T

Step 3: Shift back

A summary - Roadmap to Solve: $\boldsymbol{F} = \boldsymbol{H}(\boldsymbol{G}) = \boldsymbol{H} \circ \boldsymbol{G} = 0$

A summary - Roadmap to Solve: $F = H(G) = H \circ G = 0$

Compute a univ. repr.

$q_h(T), v_1(T), \dots, v_n(T)$ of

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

$\tilde{O}(n(L_h + n^2) C\, E)$

$C = \deg(h_1) \cdots \deg(h_n)$

$E = (\deg(h_1) + 1) \cdots (\deg(h_n) + 1)$

A summary - Roadmap to Solve: $F = H(G) = H \circ G = 0$

Compute a univ. repr.

$q_h(T), v_1(T), \dots, v_n(T)$ of

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

$$\tilde{O}(n(L_h + n^2) C\, E)$$

$$C = \deg(h_1) \cdots \deg(h_n)$$

$$E = (\deg(h_1) + 1) \cdots (\deg(h_n) + 1)$$

Compute a bivar. repr.

$Q(U, T), W_1(U, T), \dots, W_n(U, T)$ of

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

$$\tilde{O}(n(L_g + n^2) D\, J)$$

$$D = \deg(g_1) \cdots \deg(g_n)$$

$$J = (\deg(g_1) + 1) \cdots (\deg(g_n) + 1)$$

A summary - Roadmap to Solve: $\boldsymbol{F} = \boldsymbol{H}(\boldsymbol{G}) = \boldsymbol{H} \circ \boldsymbol{G} = 0$

Compute a univ. repr.

$q_h(T), v_1(T), \dots, v_n(T)$ of

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

$\tilde{O}(n(L_h + n^2) C\, E)$

$C = \deg(h_1) \cdots \deg(h_n)$

$E = (\deg(h_1) + 1) \cdots (\deg(h_n) + 1)$

Compute a bivar. repr.

$Q(U,T), W_1(U,T), \dots, W_n(U,T)$ of

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

$\tilde{O}(n(L_g + n^2) D\, J)$

$D = \deg(g_1) \cdots \deg(g_n)$

$J = (\deg(g_1) + 1) \cdots (\deg(g_n) + 1)$

$\rightsquigarrow$ bivariate representation of $\boldsymbol{F} = 0$: $\tilde{O}(n(L_h + L_g + n^2) \max(C\, E, D\, J))$

$$q_h(T) = 0, \quad Q(U,T) = 0, \quad \begin{cases} x_1 & = W_1(U,T) \\ & \vdots \\ x_n & = W_n(U,T) \end{cases}$$

$\rightsquigarrow$ bivariate representation of $\boldsymbol{F} = 0$: $\tilde{O}(n(L_h + L_g + n^2) \max(C\,E, D\,J))$

$$q_h(T) = 0, \quad Q(U,T) = 0, \quad \begin{cases} x_1 & = W_1(U,T) \\ & \vdots \\ x_n & = W_n(U,T) \end{cases}$$

$\rightsquigarrow$ find a univariate representation $\big(\Gamma(S), \gamma_1(S), \dots, \gamma_n(S)\big)$ of $\boldsymbol{F} = 0$?

$\rightsquigarrow$ bivariate representation of $\boldsymbol{F} = 0$: $\tilde{O}(n(L_h + L_g + n^2)\max(C\,E, D\,J))$

$$q_h(T) = 0, \quad Q(U,T) = 0, \quad \begin{cases} x_1 & = W_1(U,T) \\ & \vdots \\ x_n & = W_n(U,T) \end{cases}$$

$\rightsquigarrow$ find a univariate representation $(\Gamma(S), \gamma_1(S), \dots, \gamma_n(S))$ of $\boldsymbol{F} = 0$? $\tilde{O}(CD)$

- compute a univ. repr. $(\Gamma(S), \xi(S), \tau(S))$ of $q_h(T) = Q(U,T) = 0$, i.e.,

$$\Gamma(S) = 0, \begin{cases} U & = \xi(S) \\ T & = \tau(S) \end{cases}$$

- $\gamma_1(S) = W_1(\xi(S), \tau(S)), \dots, \gamma_n(S) = W_n(\xi(S), \tau(S))$

An example $f_1 = h_1(g_1, g_2)$ and $f_2 = h_2(g_1, g_2)$

Solve $F = H \circ G$:

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

System H:

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

System G:

$$\begin{cases} g_1 & = x_1 + x_2 - 1 \\ g_2 & = x_1 x_2 \end{cases}$$

An example $f_1 = h_1(g_1, g_2)$ and $f_2 = h_2(g_1, g_2)$

Solve $F = H \circ G$:

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

System H:

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

System G:

$$\begin{cases} g_1 & = x_1 + x_2 - 1 \\ g_2 & = x_1 x_2 \end{cases}$$

- a univariate repr. 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 $f_1 = h_1(g_1, g_2)$ and $f_2 = h_2(g_1, g_2)$

Solve $F = H \circ G$:

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

System H:

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

System G:

$$\begin{cases} g_1 &= x_1 + x_2 - 1 \\ g_2 &= x_1x_2 \end{cases}$$

- a univariate repr. of $h_1 = h_2 = 0$:

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

- a bivariate repr. of $g_1(x_1, x_2) - v_1(T) = g_2(x_1, x_2) - v_2(T) = 0$:

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

$$W_1(U, T) = \tfrac{3}{2} - \tfrac{U}{2} + \tfrac{3T}{2}, \text{ and } \quad W_2(U, T) = -\tfrac{1}{2} + \tfrac{U}{2} - \tfrac{T}{2}$$

An example $f_1 = h_1(g_1, g_2)$ and $f_2 = h_2(g_1, g_2)$

Solve $F = H \circ G$:

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

System H:

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

System G:

$$\begin{cases} g_1 &= x_1 + x_2 - 1 \\ g_2 &= x_1 x_2 \end{cases}$$

- a univariate repr. of $h_1 = h_2 = 0$:

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

- a bivariate repr. of $g_1(x_1, x_2) - v_1(T) = g_2(x_1, x_2) - v_2(T) = 0$:

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

$$W_1(U, T) = \tfrac{3}{2} - \tfrac{U}{2} + \tfrac{3T}{2}, \text{ and } \quad W_2(U, T) = -\tfrac{1}{2} + \tfrac{U}{2} - \tfrac{T}{2}$$

- $(Q(U, T), W_1(U, T), W_2(U, T))$ is a bivariate repr. of $\boldsymbol{F} = 0$

An example $f_1 = h_1(g_1, g_2)$ and $f_2 = h_2(g_1, g_2)$

Solve $F = H \circ G$:

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

System H:

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

System G:

$$\begin{cases} g_1 &= x_1 + x_2 - 1 \\ g_2 &= x_1 x_2 \end{cases}$$

- a univariate repr. of $h_1 = h_2 = 0$:

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

- a bivariate repr. of $g_1(x_1, x_2) - v_1(T) = g_2(x_1, x_2) - v_2(T) = 0$:

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

$$W_1(U, T) = \tfrac{3}{2} - \tfrac{U}{2} + \tfrac{3T}{2}, \text{ and } \quad W_2(U, T) = -\tfrac{1}{2} + \tfrac{U}{2} - \tfrac{T}{2}$$

- $(Q(U, T), W_1(U, T), W_2(U, T))$ is a bivariate repr. of $\boldsymbol{F} = 0$

- a univariate repr. of $Q(U, T) = q_h(T) = 0$:

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

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

An example $f_1 = h_1(g_1, g_2)$ and $f_2 = h_2(g_1, g_2)$

Solve $F = H \circ G$:

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

System H:

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

System G:

$$\begin{cases} g_1 &= x_1 + x_2 - 1 \\ g_2 &= x_1 x_2 \end{cases}$$

- a univariate repr. of $h_1 = h_2 = 0$:

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

- a bivariate repr. of $g_1(x_1, x_2) - v_1(T) = g_2(x_1, x_2) - v_2(T) = 0$:

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

$$W_1(U,T) = \tfrac{3}{2} - \tfrac{U}{2} + \tfrac{3T}{2}, \text{ and } \quad W_2(U,T) = -\tfrac{1}{2} + \tfrac{U}{2} - \tfrac{T}{2}$$

- $(Q(U,T), W_1(U,T), W_2(U,T))$ is a bivariate repr. of $\boldsymbol{F} = 0$

- a univariate repr. of $Q(U,T) = q_h(T) = 0$:

$$\mathit{\Gamma}(S) = S^4 - 4S^3 - S^2 + 16S - 12$$

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

- a univariate repr. of $f_1 = f_2 = 0$:

$$\mathit{\Gamma}(S) = S^4 - 4S^3 - S^2 + 16S - 12, \gamma_1(S) = W_1(\xi(S), \tau(S)) = \tfrac{2}{5}S^3 - \tfrac{9}{10}S^2 - \tfrac{21}{10}S + \tfrac{18}{5}, \text{ and}$$

$$\gamma_2(S) = W_2(\xi(S), \tau(S)) = -\tfrac{2}{15}S^3 + \tfrac{3}{10}S^2 + \tfrac{31}{30}S - \tfrac{6}{5}$$

Summary and Todo List

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

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

Summary and Todo List

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:

- exploiting the sparsity

Summary and Todo List

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:

- exploiting the sparsity
- real solutions (emptiness, connectivity of real algebraic sets, ...)

Summary and Todo List

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:

- exploiting the sparsity
- real solutions (emptiness, connectivity of real algebraic sets, ...)
- functional decomposition of polynomials
  - [Giesbrecht et al, ISSAC 2026] for univariate sparse polynomials (Mark's talk this afternoon)

Summary and Todo List

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:

- exploiting the sparsity
- real solutions (emptiness, connectivity of real algebraic sets, ...)
- functional decomposition of polynomials
  - [Giesbrecht et al, ISSAC 2026] for univariate sparse polynomials (Mark's talk this afternoon)
- implementations
  - use Straight-Line Programs (a recent developed library by [van der Hoeven and Lecerf, 2026])