Algebraic Tools for Computing Polynomial Loop Invariants

Fatemeh Mohammadi

Joint work with Erdenebayar Bayarmagnai and Rémi Prébet

Polynomial invariants for loops

Polynomial invariant

Polynomial equations/inequalities that hold before & after every iteration.

Polynomial invariants for loops

Polynomial invariant

Polynomial equations/inequalities that hold before & after every iteration.

$(\mathrm{x}, \mathrm{y}) = (0, 1)$
while true **do**

$$\begin{pmatrix} \mathrm{x} \\ \mathrm{y} \end{pmatrix} \longleftarrow \begin{pmatrix} \mathrm{x} + \mathrm{y} \\ \mathrm{x} \end{pmatrix}$$

end while

- Values of (x, y): $(1, 0)$, $(1, 1)$, $(2, 1)$, $(3, 2)$, $(5, 3)$, $8, 5)$

Polynomial invariants for loops

Polynomial invariant

Polynomial equations/inequalities that hold before & after every iteration.

$(\mathtt{x}, \mathtt{y}) = (0, 1)$
while true **do**

$$\begin{pmatrix} \mathtt{x} \\ \mathtt{y} \end{pmatrix} \longleftarrow \begin{pmatrix} \mathtt{x} + \mathtt{y} \\ \mathtt{x} \end{pmatrix}$$

end while

- Values of (x, y): $(1, 0)$, $(1, 1)$, $(2, 1)$, $(3, 2)$, $(5, 3)$, $8, 5)$
- Two consecutive numbers of Fibonacci sequence satisfy

$$x^4 + y^4 + 2x^3y - x^2y^2 - 2xy^3 - 1 = 0.$$

Polynomial invariants for loops

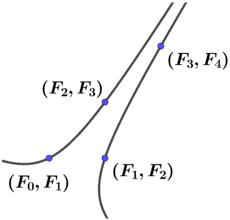
Polynomial invariant

Polynomial equations/inequalities that hold before & after every iteration.

$(\mathtt{x}, \mathtt{y}) = (0, 1)$
while true **do**

$$\begin{pmatrix} \mathtt{x} \\ \mathtt{y} \end{pmatrix} \longleftarrow \begin{pmatrix} \mathtt{x} + \mathtt{y} \\ \mathtt{x} \end{pmatrix}$$

end while



- Values of (x, y): $(1, 0)$, $(1, 1)$, $(2, 1)$, $(3, 2)$, $(5, 3)$, $8, 5)$
- Two consecutive numbers of Fibonacci sequence satisfy

$$x^4 + y^4 + 2x^3y - x^2y^2 - 2xy^3 - 1 = 0.$$

Prior Works

- **Special classes of loops:**
  - Affine loops (Hrushovski, Ouaknine, Pouly, Worrell; LICS ’18)
  - P-solvable loops Kovács; TACAS ’08
  - Solvable loops (Rodriguez-Carbonell, Kapur; Symb. Comput. ’07)

- **Degree-bounded polynomial invariants:**
  - Synthesis for solvable loops (Amrollahi, Bartocci, Kenison, Kovács, Moosbrugger, Stankovic; Formal Methods Syst. Des. ’24)
  - Ideal-based reasoning (Cyphert Kincaid; ACM ’24)
  - Invariants from symbolic initialization (Müller-Olm, Seidl; Inf. Process. Lett. ’04)

(Semi)-algebraic loop

$(x_1, x_2, \dots, x_n) = (a_1, a_2, \dots, a_n)$

while $g_1 = \cdots = g_k = 0$ and $h_1 > 0, \dots, h_s > 0$ **do**

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \overset{F}{\longleftarrow} \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{pmatrix}$$

end while

(Semi)-algebraic loop

$(x_1, x_2, \dots, x_n) = (a_1, a_2, \dots, a_n)$
while $g_1 = \cdots = g_k = 0$ and $h_1 > 0, \dots, h_s > 0$ **do**

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \xleftarrow{F} \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{pmatrix}$$

end while

$(x_1, \dots, x_n) = (a_1, \dots, a_n)$
while true **do**

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \xleftarrow{F} \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{pmatrix}$$

end while

Outline

- Symbolic Computations – Algorithms:
    - Compute all polynomial invariants up to a fixed degree.

Outline

- Symbolic Computations – Algorithms:
  - Compute all polynomial invariants up to a fixed degree.
    a) Valid for all possible initial values

Outline

- Symbolic Computations – Algorithms:
  - Compute all polynomial invariants up to a fixed degree.
    - *a*) Valid for all possible initial values
    - *b*) Specific to a given initial value

Outline

- Symbolic Computations – Algorithms:
  - Compute all polynomial invariants up to a fixed degree.
    - *a*) Valid for all possible initial values
    - *b*) Specific to a given initial value
  - Identify initial values for which a given polynomial is an invariant.

Outline

- Symbolic Computations – Algorithms:
  - Compute all polynomial invariants up to a fixed degree.
    - *a*) Valid for all possible initial values
    - *b*) Specific to a given initial value
  - Identify initial values for which a given polynomial is an invariant.
  - Generate all polynomial invariants of a specified algebraic form.

Outline

- Symbolic Computations – Algorithms:
  - Compute all polynomial invariants up to a fixed degree.
    a) Valid for all possible initial values
    b) Specific to a given initial value
  - Identify initial values for which a given polynomial is an invariant.
  - Generate all polynomial invariants of a specified algebraic form.
  - Algebraic formulation

Polynomial ideals

- Consider the polynomial ring $R = \mathbb{C}[x_1, \ldots, x_n]$.
- A subset $I \subseteq R$ is called a **polynomial ideal** if:
  - If $f, g \in I$, then $f + g \in I$ (closed under addition)
  - If $f \in I$ and $h \in R$, then $hf \in I$ (closed under multiplication in R).

Polynomial ideals

- Consider the polynomial ring $R = \mathbb{C}[x_1, \ldots, x_n]$.
- A subset $I \subseteq R$ is called a **polynomial ideal** if:
  - If $f, g \in I$, then $f + g \in I$ (closed under addition)
  - If $f \in I$ and $h \in R$, then $hf \in I$ (closed under multiplication in R).

Hilbert Basis Theorem

Every ideal in the polynomial ring $\mathbb{C}[x_1, x_2, \ldots, x_n]$ is finitely generated.

Polynomial ideals

- Consider the polynomial ring $R = \mathbb{C}[x_1, \ldots, x_n]$.
- A subset $I \subseteq R$ is called a **polynomial ideal** if:
  - If $f, g \in I$, then $f + g \in I$ (closed under addition)
  - If $f \in I$ and $h \in R$, then $hf \in I$ (closed under multiplication in R).

Hilbert Basis Theorem

Every ideal in the polynomial ring $\mathbb{C}[x_1, x_2, \ldots, x_n]$ is finitely generated.

- For any ideal $I \subseteq R$, there exist polynomials $f_1, \ldots, f_r \in I$ such that

$$I = \langle f_1, \ldots, f_r \rangle.$$

- For any polynomial g in I there exists $h_1, \ldots, h_r$ in R such that

$$g = h_1 f_1 + \cdots + h_r f_r$$

Algebraic varieties

- Let $S = \{f_1, f_2, \ldots, f_s\} \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n]$. Define

$$V(S) = \{(a_1, \ldots, a_n) \in \mathbb{C}^n : f_i(a_1, \ldots, a_n) = 0 \text{ for all } 1 \leq i \leq s\}.$$

Algebraic varieties

- Let $S = \{f_1, f_2, \ldots, f_s\} \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n]$. Define

$$V(S) = \{(a_1, \ldots, a_n) \in \mathbb{C}^n : f_i(a_1, \ldots, a_n) = 0 \text{ for all } 1 \leq i \leq s\}.$$

- Let I be the smallest ideal containing S. Then: $V(S) = V(I)$.

Algebraic varieties

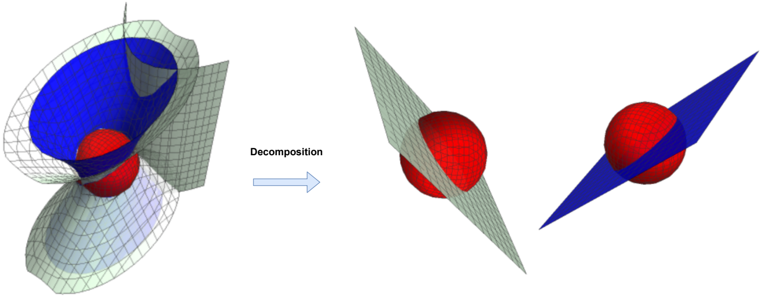
- Let $S = \{f_1, f_2, \ldots, f_s\} \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n]$. Define

$$V(S) = \{(a_1, \ldots, a_n) \in \mathbb{C}^n : f_i(a_1, \ldots, a_n) = 0 \text{ for all } 1 \leq i \leq s\}.$$

- Let I be the smallest ideal containing S. Then: $V(S) = V(I)$.
- If $\{f_1, \ldots, f_s\}$ and $\{g_1, \ldots, g_t\}$ generate the same ideal I, then:

$$V(f_1, \ldots, f_s) = V(g_1, \ldots, g_t)$$

- Equivalent polynomial systems



$\{x^2+y^2+z^2=1,\ 3x^2y^2-6x^2z+9x^2+y^4-y^2z^2-2y^2z+2y^2+2z^3-3z^2+2z-3=0,\ 5x^2-z^2+2y^2=2\}$ is decomposed to $\{x^2+y^2+z^2=1,\ x-z=0\}$ and $\{x^2+y^2+z^2=1,\ x+z=0\}$

Radical of ideals

Given an ideal $I \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n]$, the **radical** of I is:

$$\text{rad}(I) = \{f \in \mathbb{C}[x_1, x_2, \ldots, x_n] : f^n \in I \text{ for some } n \in \mathbb{N}_{>0}\}.$$

Radical of ideals

Given an ideal $I \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n]$, the **radical** of I is:

$$\mathrm{rad}(I) = \{f \in \mathbb{C}[x_1, x_2, \ldots, x_n] : f^n \in I \text{ for some } n \in \mathbb{N}_{>0}\}.$$

$$I = (x_1^5x_5^5 + 5x_1^5x_5^4 - 10x_1^4x_3x_5^4 + 5x_1^4x_4x_5^4 + 10x_1^5x_5^3 - 40x_1^4x_3x_5^3 + 40x_1^3x_3^2x_5^3 + 20x_1^4x_4x_5^3 - 40x_1^3x_3x_4x_5^3 + 10x_1^3x_4^2x_5^3 + 10x_1^5x_5^2 - 60x_1^4x_3x_5^2 + 120x_1^3x_3^2x_5^2 - 80x_1^2x_3^3x_5^2 + 30x_1^4x_4x_5^2 - 120x_1^3x_3x_4x_5^2 + 120x_1^2x_3^2x_4x_5^2 + 30x_1^3x_4^2x_5^2 - 60x_1^2x_3x_4^2x_5^2 + 10x_1^2x_4^3x_5^2 + 5x_1^5x_5 - 40x_1^4x_3x_5 + 120x_1^3x_3^2x_5 - 160x_1^2x_3^3x_5 + 80x_1x_3^4x_5 + 20x_1^4x_4x_5 - 120x_1^3x_3x_4x_5 + 240x_1^2x_3^2x_4x_5 - 160x_1x_3^3x_4x_5 + 30x_1^3x_4^2x_5 - 120x_1^2x_3x_4^2x_5 + 120x_1x_3^2x_4^2x_5 + 20x_1^2x_4^3x_5 - 40x_1x_3x_4^3x_5 + 5x_1x_4^4x_5 + x_1^5 - 10x_1^4x_3 + 40x_1^3x_3^2 - 80x_1^2x_3^3 + 80x_1x_3^4 - 32x_3^5 + 5x_1^4x_4 - 40x_1^3x_3x_4 + 120x_1^2x_3^2x_4 - 160x_1x_3^3x_4 + 80x_3^4x_4 + 10x_1^3x_4^2 - 60x_1^2x_3x_4^2 + 120x_1x_3^2x_4^2 - 80x_3^3x_4^2 + 10x_1^2x_4^3 - 40x_1x_3x_4^3 + 40x_3^2x_4^3 + 5x_1x_4^4 - 10x_3x_4^4 + x_4^5,\ x_1^5 - 2x_3,\ x_3^3x_4^6 + 3x_1x_3^2x_4^4 + 3x_1^2x_3x_4^2 + x_1^3)$$

Radical of ideals

Given an ideal $I \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n]$, the **radical** of I is:

$$\text{rad}(I) = \{f \in \mathbb{C}[x_1, x_2, \ldots, x_n] : f^n \in I \text{ for some } n \in \mathbb{N}_{>0}\}.$$

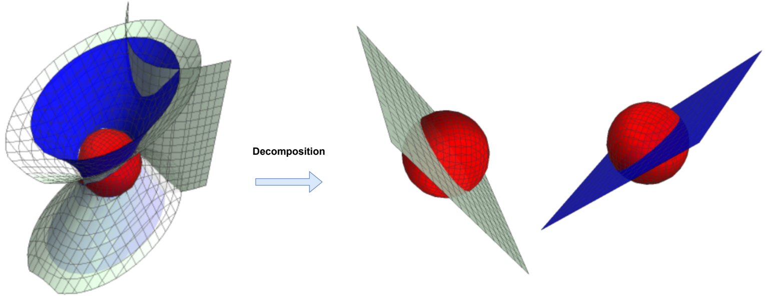
$$I = (x_1^5x_5^5 + 5x_1^5x_5^4 - 10x_1^4x_3x_5^4 + 5x_1^4x_4x_5^4 + 10x_1^5x_5^3 - 40x_1^4x_3x_5^3 + 40x_1^3x_3^2x_5^3 + 20x_1^4x_4x_5^3 - 40x_1^3x_3x_4x_5^3 + 10x_1^3x_4^2x_5^3 + 10x_1^5x_5^2 - 60x_1^4x_3x_5^2 + 120x_1^3x_3^2x_5^2 - 80x_1^2x_3^3x_5^2 + 30x_1^4x_4x_5^2 - 120x_1^3x_3x_4x_5^2 + 120x_1^2x_3^2x_4x_5^2 + 30x_1^3x_4^2x_5^2 - 60x_1^2x_3x_4^2x_5^2 + 10x_1^2x_4^3x_5^2 + 5x_1^5x_5 - 40x_1^4x_3x_5 + 120x_1^3x_3^2x_5 - 160x_1^2x_3^3x_5 + 80x_1x_3^4x_5 + 20x_1^4x_4x_5 - 120x_1^3x_3x_4x_5 + 240x_1^2x_3^2x_4x_5 - 160x_1x_3^3x_4x_5 + 30x_1^3x_4^2x_5 - 120x_1^2x_3x_4^2x_5 + 120x_1x_3^2x_4^2x_5 + 20x_1^2x_4^3x_5 - 40x_1x_3x_4^3x_5 + 5x_1x_4^4x_5 + x_1^5 - 10x_1^4x_3 + 40x_1^3x_3^2 - 80x_1^2x_3^3 + 80x_1x_3^4 - 32x_3^5 + 5x_1^4x_4 - 40x_1^3x_3x_4 + 120x_1^2x_3^2x_4 - 160x_1x_3^3x_4 + 80x_3^4x_4 + 10x_1^3x_4^2 - 60x_1^2x_3x_4^2 + 120x_1x_3^2x_4^2 - 80x_3^3x_4^2 + 10x_1^2x_4^3 - 40x_1x_3x_4^3 + 40x_3^2x_4^3 + 5x_1x_4^4 - 10x_3x_4^4 + x_4^5,\ x_1^5 - 2x_3,\ x_3^3x_4^6 + 3x_1x_3^2x_4^4 + 3x_1^2x_3x_4^2 + x_1^3)$$

$$\text{rad}(I) = (x_1x_5 + x_1 - 2x_3 + x_4,\ x_1^5 - 2x_3,\ x_3x_4^2 + x_1)$$

- $V(I) = V(\text{rad}(I))$
- $I \subseteq \text{rad}(I)$

Description of polynomial invariant ideals

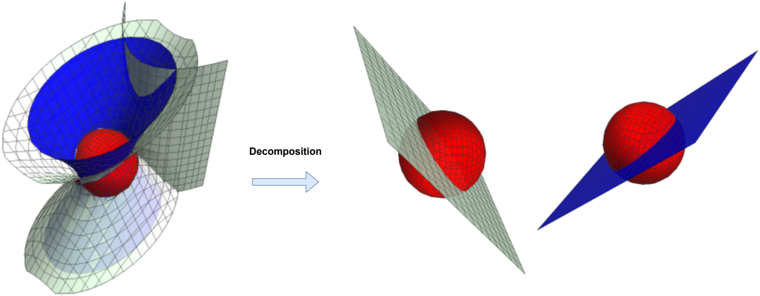
- Polynomial systems with the same solution set.



$\{x^2+y^2+z^2=1,\ 3x^2y^2-6x^2z+9x^2+y^4-y^2z^2-2y^2z+2y^2+2z^3-3z^2+2z-3=0,\ 5x^2-z^2+2y^2=2\}$ is decomposed to $\{x^2+y^2+z^2=1,\ x-z=0\}$ and $\{x^2+y^2+z^2=1,\ x+z=0\}$

Description of polynomial invariant ideals

- Polynomial systems with the same solution set.

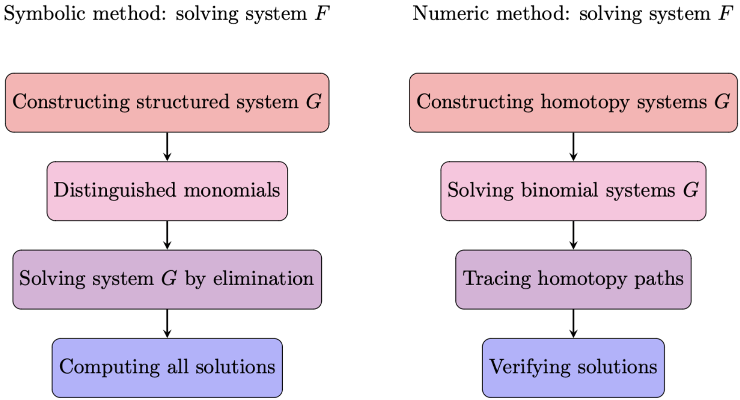


$\{x^2+y^2+z^2=1,\ 3x^2y^2-6x^2z+9x^2+y^4-y^2z^2-2y^2z+2y^2+2z^3-3z^2+2z-3=0,\ 5x^2-z^2+2y^2=2\}$ is decomposed to $\{x^2+y^2+z^2=1,\ x-z=0\}$ and $\{x^2+y^2+z^2=1,\ x+z=0\}$

- Goals:
  - Find a **minimal** generating set for the ideal of polynomial invariants.
  - Decompose the associated variety into smaller ones
  - Generate equivalent generating sets which are easier to represent

Symbolic-numerical algebraic computation

- Approach: Degenerating a given system F to a more-structured system



- Main idea: Gröbner degenerations.

Algebraic formulation

g is a P.I. of $\mathcal{L}(a, F)$:

```
x ← a
while true do
    x ← F(x)
end while
```

$\Longleftrightarrow$

$g(a) = 0$
$g \circ F(a) = 0$
$g \circ F^{(2)}(a) = 0$
$\dots$
$g \circ F^{(k)}(a) = 0$ for all $k \in \mathbb{N}$

Algebraic formulation

g is a P.I. of $\mathcal{L}(a, F)$:

```
x ← a
while true do
    x ← F(x)
end while
```

$\iff$

$g(a) = 0$
$g \circ F(a) = 0$
$g \circ F^{(2)}(a) = 0$
$\dots$
$g \circ F^{(k)}(a) = 0$ for all $k \in \mathbb{N}$

Definition

The invariant set of (F, g) is

$$S_{(F,g)} = \{x \in \mathbb{C}^n \mid \forall m \in \mathbb{Z}_{\geq 0} : g \circ F^{(m)}(x) = 0\}.$$

Invariant sets are algebraic varieties.

Algebraic formulation

g is a P.I. of $\mathcal{L}(a, F)$:

```
x ← a
while true do
    x ← F(x)
end while
```

$\Longleftrightarrow$

$g(a) = 0$
$g \circ F(a) = 0$
$g \circ F^{(2)}(a) = 0$
$\ldots$
$g \circ F^{(k)}(a) = 0$ for all $k \in \mathbb{N}$

Definition

The invariant set of (F, g) is

$$S_{(F,g)} = \{x \in \mathbb{C}^n \mid \forall m \in \mathbb{Z}_{\geq 0} : g \circ F^{(m)}(x) = 0\}.$$

Invariant sets are algebraic varieties.

Proposition

Let $a \in \mathbb{C}^n$. Then, g is a P.I. of $\mathcal{L}(a, F)$ if and only if $a \in S_{(F,g)}$.

Computing Invariant Sets

Theorem

Given a polynomial map $F : \mathbb{C}^n \to \mathbb{C}^n$ and a polynomial g, there exists an integer $N \in \mathbb{N}$ such that:

$$S_{(F,g)} = V(g) \cap V(g \circ F) \cap \cdots \cap V(g \circ F^{(N)}).$$

INVARIANTSETCOMPUTATION

Input: g and $F = (f_1, \ldots, f_n)$ in $\mathbb{Q}[x_1, \ldots, x_n]$
Output: A finite set of polynomials whose common zero set is $S_{(F,g)}$

$S \leftarrow \{g\}$
$\widetilde{g} \leftarrow g \circ F$
while $V(S) \neq V(S \cup \{\widetilde{g}\})$ **do**
    $S \leftarrow S \cup \{\widetilde{g}\}$
    $\widetilde{g} \leftarrow \widetilde{g} \circ F$
end while
return S

Example

$(\mathtt{x}_1, \mathtt{x}_2) \leftarrow (a_1, a_2)$
while true **do**
$$\begin{pmatrix} \mathtt{x}_1 \\ \mathtt{x}_2 \end{pmatrix} \leftarrow \begin{pmatrix} 10 & -8 \\ 6 & -4 \end{pmatrix} \begin{pmatrix} \mathtt{x}_1 \\ \mathtt{x}_2 \end{pmatrix}$$
end while

- Consider $g = x_1^2 - x_1 x_2 + 9x_1^3 - 24x_1^2 x_2 + 16x_1 x_2^2$

Example

$$(\mathtt{x}_1, \mathtt{x}_2) \leftarrow (a_1, a_2)$$

while true **do**

$$\begin{pmatrix} \mathtt{x}_1 \\ \mathtt{x}_2 \end{pmatrix} \leftarrow \begin{pmatrix} 10 & -8 \\ 6 & -4 \end{pmatrix} \begin{pmatrix} \mathtt{x}_1 \\ \mathtt{x}_2 \end{pmatrix}$$

end while

- Consider $g = x_1^2 - x_1 x_2 + 9x_1^3 - 24x_1^2 x_2 + 16x_1 x_2^2$
- $g \circ F = 360x_1^3 - 1248x_1^2 x_2 + 40x_1^2 + 1408x_1 x_2^2 - 72x_1 x_2 - 512x_2^3 + 32x_2^2$

Example

$(\mathtt{x}_1, \mathtt{x}_2) \leftarrow (a_1, a_2)$
while true **do**
$$\begin{pmatrix} \mathtt{x}_1 \\ \mathtt{x}_2 \end{pmatrix} \leftarrow \begin{pmatrix} 10 & -8 \\ 6 & -4 \end{pmatrix} \begin{pmatrix} \mathtt{x}_1 \\ \mathtt{x}_2 \end{pmatrix}$$
end while

- Consider $g = x_1^2 - x_1 x_2 + 9x_1^3 - 24x_1^2 x_2 + 16x_1 x_2^2$
- $g \circ F = 360x_1^3 - 1248x_1^2 x_2 + 40x_1^2 + 1408x_1 x_2^2 - 72x_1 x_2 - 512x_2^3 + 32x_2^2$
- Gröbner basis computation shows $V(g) \neq V(g, g \circ F)$.

Example

$(\mathtt{x}_1, \mathtt{x}_2) \leftarrow (a_1, a_2)$
while true **do**
$$\begin{pmatrix} \mathtt{x}_1 \\ \mathtt{x}_2 \end{pmatrix} \leftarrow \begin{pmatrix} 10 & -8 \\ 6 & -4 \end{pmatrix} \begin{pmatrix} \mathtt{x}_1 \\ \mathtt{x}_2 \end{pmatrix}$$
end while

- Consider $g = x_1^2 - x_1 x_2 + 9x_1^3 - 24x_1^2 x_2 + 16x_1 x_2^2$
- $g \circ F = 360x_1^3 - 1248x_1^2 x_2 + 40x_1^2 + 1408x_1 x_2^2 - 72x_1 x_2 - 512x_2^3 + 32x_2^2$
- Gröbner basis computation shows $V(g) \neq V(g, g \circ F)$.
- $g \circ F^2 = 7488x_1^3 - 26880x_1^2 x_2 + 832x_1^2 + 31744x_1 x_2^2 - 1600x_1 x_2 - 12288x_2^3 + 768x_2^2$
- This time, $V(g, g \circ F) = V(g, g \circ F, g \circ F^2)$.

Example

$(\mathtt{x}_1, \mathtt{x}_2) \leftarrow (a_1, a_2)$
while true **do**
$$\begin{pmatrix} \mathtt{x}_1 \\ \mathtt{x}_2 \end{pmatrix} \leftarrow \begin{pmatrix} 10 & -8 \\ 6 & -4 \end{pmatrix} \begin{pmatrix} \mathtt{x}_1 \\ \mathtt{x}_2 \end{pmatrix}$$
end while

- Consider $g = x_1^2 - x_1 x_2 + 9x_1^3 - 24x_1^2 x_2 + 16x_1 x_2^2$
- $g \circ F = 360x_1^3 - 1248x_1^2 x_2 + 40x_1^2 + 1408x_1 x_2^2 - 72x_1 x_2 - 512x_2^3 + 32x_2^2$
- Gröbner basis computation shows $V(g) \neq V(g, g \circ F)$.
- $g \circ F^2 = 7488x_1^3 - 26880x_1^2 x_2 + 832x_1^2 + 31744x_1 x_2^2 - 1600x_1 x_2 - 12288x_2^3 + 768x_2^2$
- This time, $V(g, g \circ F) = V(g, g \circ F, g \circ F^2)$.

Conclusion: g is a P.I. for $\mathcal{L}((a_1, a_2), F)$ if and only if $(a_1, a_2) \in V(g, g \circ F)$.

Polynomial invariants of degree d

$g = \sum_{|\alpha_i| \leq d} b_i x^{\alpha_i} \in \mathbb{C}[x]$ is a P.I.

$\mathtt{x} \leftarrow a$
while true **do**
    $\mathtt{x} \leftarrow F(\mathtt{x})$
end while

Polynomial invariants of degree d

$g = \sum_{|\alpha_i| \leq d} b_i x^{\alpha_i} \in \mathbb{C}[x]$ is a P.I.

$\mathtt{x} \leftarrow a$
while true **do**
  $\mathtt{x} \leftarrow F(\mathtt{x})$
end while

$h = \sum_{|\alpha_i| \leq d} y_i x^{\alpha_i} \in \mathbb{C}[x, y]$ is a P.I.

$(\mathtt{x}, \mathtt{y}) \leftarrow (a, b)$
while true **do**
  $(\mathtt{x}, \mathtt{y}) \leftarrow G(\mathtt{x}, \mathtt{y}) = (F(\mathtt{x}), \mathtt{y})$
end while

- Let $I_{d,\mathcal{L}}$ denote the set of all polynomial invariants of degree $\leq d$.
- It forms a finite-dimensional vector space and can thus be uniquely characterized by a system of linear equations.

Polynomial invariants of degree d

$g = \sum_{\lvert\alpha_i\rvert \leq d} b_i x^{\alpha_i} \in \mathbb{C}[x]$ is a P.I.	$h = \sum_{\lvert\alpha_i\rvert \leq d} y_i x^{\alpha_i} \in \mathbb{C}[x, y]$ is a P.I.

$\mathtt{x} \leftarrow a$
while true **do**
    $\mathtt{x} \leftarrow F(\mathtt{x})$
end while
	$(\mathtt{x}, \mathtt{y}) \leftarrow (a, b)$
	while true **do**
	    $(\mathtt{x}, \mathtt{y}) \leftarrow G(\mathtt{x}, \mathtt{y}) = (F(\mathtt{x}), \mathtt{y})$
	end while

- Let $I_{d,\mathcal{L}}$ denote the set of all polynomial invariants of degree $\leq d$.
- It forms a finite-dimensional vector space and can thus be uniquely characterized by a system of linear equations.

Theorem (ISSAC 2024)

Let $F = (f_1, \ldots, f_n)$ be a sequence of polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$ and let $d \geq 1$. Then, there is an algorithm that computes a polynomial matrix A, s.t.

$$I_{d,\mathcal{L}} = \{ \sum_{\lvert\alpha_i\rvert \leq d} b_i x^{\alpha_i} \mid (b_1, \ldots, b_m) \in \ker A(\mathbf{a}) \}.$$

Example

$(\mathtt{x}_1, \mathtt{x}_2) \leftarrow (a_1, a_2)$
while true **do**
$$\begin{pmatrix} \mathtt{x}_1 \\ \mathtt{x}_2 \end{pmatrix} \leftarrow \begin{pmatrix} 10 & -8 \\ 6 & -4 \end{pmatrix} \begin{pmatrix} \mathtt{x}_1 \\ \mathtt{x}_2 \end{pmatrix}$$
end while

- **Goal:** Compute all polynomial invariants of degree ≤ 2.
- Consider $F = (10x_1 - 8x_2, \quad 6x_1 - 4x_2, \quad y_1, \ldots, y_6)$
- The general polynomial: $g = y_1 + y_2x_1 + y_3x_2 + y_4x_1^2 + y_5x_1x_2 + y_6x_2^2$
- The algorithm returns a matrix $M(x_1, x_2)$ such that

$$M(x_1, x_2) \cdot (y_1 \ y_2 \ \cdots \ y_6)^T = 0$$

encodes the polynomial invariants.

Output matrix and basis cases

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3x_1 - 4x_2 & 3x_1 - 4x_2 & 0 & 0 & 0 \\ 0 & 64x_2 & 112x_2 - 48x_1 & 48x_2^2 & 84x_2^2 - 36x_1x_2 & 27x_1^2 - 126x_1x_2 + 147x_2^2 \\ 0 & 32x_2 & 56x_2 - 24x_1 & 24x_1x_2 & -9x_1^2 + 21x_1x_2 + 12x_2^2 & -18x_1x_2 + 42x_2^2 \\ 0 & 4x_2 & 7x_2 - 3x_1 & 3x_1^2 & 3x_1x_2 & 3x_2^2 \end{bmatrix}$$

Output matrix and basis cases

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3x_1 - 4x_2 & 3x_1 - 4x_2 & 0 & 0 & 0 \\ 0 & 64x_2 & 112x_2 - 48x_1 & 48x_2^2 & 84x_2^2 - 36x_1x_2 & 27x_1^2 - 126x_1x_2 + 147x_2^2 \\ 0 & 32x_2 & 56x_2 - 24x_1 & 24x_1x_2 & -9x_1^2 + 21x_1x_2 + 12x_2^2 & -18x_1x_2 + 42x_2^2 \\ 0 & 4x_2 & 7x_2 - 3x_1 & 3x_1^2 & 3x_1x_2 & 3x_2^2 \end{bmatrix}$$

- We compute an explicit basis for the vector space $I_{2,\mathcal{L}}$ by computing the kernel of the above matrix, depending on the initial values (a_1, a_2).

Output matrix and basis cases

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3x_1-4x_2 & 3x_1-4x_2 & 0 & 0 & 0 \\ 0 & 64x_2 & 112x_2-48x_1 & 48x_2^2 & 84x_2^2-36x_1x_2 & 27x_1^2-126x_1x_2+147x_2^2 \\ 0 & 32x_2 & 56x_2-24x_1 & 24x_1x_2 & -9x_1^2+21x_1x_2+12x_2^2 & -18x_1x_2+42x_2^2 \\ 0 & 4x_2 & 7x_2-3x_1 & 3x_1^2 & 3x_1x_2 & 3x_2^2 \end{bmatrix}$$

- We compute an explicit basis for the vector space $I_{2,\mathcal{L}}$ by computing the kernel of the above matrix, depending on the initial values (a_1, a_2).
- Performing Gaussian elimination on M leads to four cases:

Initial values	Basis of $I_{2,\mathcal{L}}$
$a_1 = a_2 = 0$	$\{x_1, x_2, x_1x_2, x_1^2, x_2^2\}$
$a_1 = a_2 \neq 0$	$\{x_1 - x_2, x_1^2 - x_1x_2, -x_1x_2 + x_2^2\}$
$a_1 = \frac{4}{3}a_2 \neq 0$	$\{3x_1 - 4x_2, -3x_1^2 + 16x_1x_2 - 16x_2^2, -3x_1x_2 + 4x_2^2\}$
$a_1 \neq \frac{4}{3}a_2$, $a_1 \neq a_2$	$\{(3a_1-4a_2)^2x_1 - (3a_1-4a_2)^2x_2 - 9(a_1-a_2)x_1^2 + 24(a_1-a_2)x_1x_2 - 16(a_1-a_2)x_2^2\}$

Experiments (comparison with Polar)

- Polar: Moosbrugger, Stankovic, Bartocci, Kovács OOPSLA2, 2022
- Polar can handle **probabilistic loops**, whereas ours is limited to **deterministic** ones.
- We compute **all** possible polynomial invariants up to a specified degree,
- Ours are **minimal** generating polynomials of degree 1 to 4. TL = Timeout (360 seconds).

Degree	1		2		3		4	
Benchmark	Ours	Polar	Ours	Polar	Ours	Polar	Ours	Polar
Fib1	0.014	0.2	0.046	0.32	0.17	0.68	1.31	1.58
Fib2	0.017	0.23	0.056	0.46	6.3	1.18	TL	3.69
Fib3	0.013	0.21	0.056	0.4	0.137	1.26	0.61	3.82
Nagata	0.026	0.25	0.07	0.55	0.15	1.21	0.35	2.84
Yagzhev9	0.12	0.43	TL	5.2	TL	131.5	TL	TL
Yagzhev11	0.095	0.45	2.7	6.83	241	359	TL	TL
Ex 9	0.016	0.28	0.06	0.64	0.19	2.38	0.55	11.5
Ex 10	0.02	0.51	0.07	1.7	0.16	16.21	0.75	TL
Squares	0.02	0.5	0.06	0.67	0.15	1.15	0.38	2.25

Degree	1		2		3		4	
Benchmark	d	Polar	d	Polar	d	Polar	d	Polar
Fib1	0	0	0	0	1	1	**4**	1
Fib2	0	0	0	0	1	1	TL	**1**
Fib3	0	0	0	0	1	1	**4**	1
Nagata	**1**	0	**5**	1	**13**	1	**26**	2
Yagzhev9	**3**	0	TL	**3**	TL	**3**	TL	TL
Yagzhev11	0	0	0	0	TL	**1**	TL	TL
Ex 9	0	0	0	0	**3**	1	**11**	1
Ex 10	0	0	**2**	0	**8**	0	**19**	0
Squares	**1**	0	**5**	0	**13**	0	**26**	0

Summary

Summary

- Compute the set of initial values for which given polynomials are P.I.
- Compute all polynomial invariants up to a given degree:
  - For each possible initial value
  - For a fixed initial value
- Compute all polynomial invariants of a given form (fixed terms).
- Exploit the structure of polynomial systems for efficiency.
- Extend methods to loops with inequality guards (ISSAC 2024).

Summary

Summary

- Compute the set of initial values for which given polynomials are P.I.
- Compute all polynomial invariants up to a given degree:
  - For each possible initial value
  - For a fixed initial value
- Compute all polynomial invariants of a given form (fixed terms).
- Exploit the structure of polynomial systems for efficiency.
- Extend methods to loops with inequality guards (ISSAC 2024).

- Bayarmagnai, Mohammadi, Prébet. ISSAC 2024

Thank you for your attention!