Computing polynomial invariants for loops

Erdenebayar Bayarmagnai, Rémi Prebet, Fatemeh Mohammadi

SAMSA 2026

Polynomial invariants

Polynomial invariant for loops (P.I.)

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

Polynomial invariants

Polynomial invariant for loops (P.I.)

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

Example

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

$$\begin{pmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \end{pmatrix} \longleftarrow \begin{pmatrix} \mathtt{z}^2 \\ \mathtt{z}^3 \\ \mathtt{x} + \mathtt{y} \end{pmatrix}$$

end while

A polynomial invariant (P.I.) for this loop is $y^2 - x^3 = 0$.

Polynomial invariants

Polynomial invariant for loops (P.I.)

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

Example

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

$$\begin{pmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \end{pmatrix} \longleftarrow \begin{pmatrix} \mathtt{z}^2 \\ \mathtt{z}^3 \\ \mathtt{x} + \mathtt{y} \end{pmatrix}$$

end while

$(\mathtt{x}_0, \mathtt{y}_0, \mathtt{z}_0) = (1, 1, 1) \qquad 1^2 - 1^3 = 0$

A polynomial invariant (P.I.) for this loop is $y^2 - x^3 = 0$.

Polynomial invariants

Polynomial invariant for loops (P.I.)

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

Example

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

$$\begin{pmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \end{pmatrix} \longleftarrow \begin{pmatrix} \mathtt{z}^2 \\ \mathtt{z}^3 \\ \mathtt{x} + \mathtt{y} \end{pmatrix}$$

end while

$(\mathtt{x}_0, \mathtt{y}_0, \mathtt{z}_0) = (1, 1, 1) \qquad 1^2 - 1^3 = 0$

$(\mathtt{x}_1, \mathtt{y}_1, \mathtt{z}_1) = (1, 1, 2) \qquad 1^2 - 1^3 = 0$

A polynomial invariant (P.I.) for this loop is $y^2 - x^3 = 0$.

Polynomial invariants

Polynomial invariant for loops (P.I.)

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

Example

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

$$\begin{pmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \end{pmatrix} \longleftarrow \begin{pmatrix} \mathtt{z}^2 \\ \mathtt{z}^3 \\ \mathtt{x} + \mathtt{y} \end{pmatrix}$$

end while

$$\begin{array}{ll} (\mathtt{x}_0, \mathtt{y}_0, \mathtt{z}_0) = (1, 1, 1) & 1^2 - 1^3 = 0 \\ (\mathtt{x}_1, \mathtt{y}_1, \mathtt{z}_1) = (1, 1, 2) & 1^2 - 1^3 = 0 \\ (\mathtt{x}_2, \mathtt{y}_2, \mathtt{z}_2) = (4, 8, 2) & 8^2 - 4^3 = 0 \\ \vdots & \vdots \end{array}$$

A polynomial invariant (P.I.) for this loop is $y^2 - x^3 = 0$.

State of the art/Main result

[1][*Hrushovski, Ouaknine, Pouly, Worrell; LICS'18*], [2][*Rodríguez-Carbonell, Kapur; JSC'07*]
[3][*Amrollahi, Bartocci, Kenison et al.; FMSD'24*], [4][*Cyphert, Kincaid; POPL'24*]
[5][*Müller-Olm, Seidl; IPL'04*]

Works	LICS'18[1], JSC'07[2]	FMSD'24[3], POPL'24[4]	IPL'04[5], Our work
Assignments	Affine, Solvable	Polynomial	Polynomial
Invariants	Polynomial	Polynomial$\leq d$	Polynomial$\leq d$
Complete	✓	×	✓

State of the art/Main result

[1] [*Hrushovski, Ouaknine, Pouly, Worrell; LICS'18*], [2] [*Rodríguez-Carbonell, Kapur; JSC'07*]
[3] [*Amrollahi, Bartocci, Kenison et al.; FMSD'24*], [4] [*Cyphert, Kincaid; POPL'24*]
[5] [*Müller-Olm, Seidl; IPL'04*]

Works	LICS'18[1], JSC'07[2]	FMSD'24[3], POPL'24[4]	IPL'04[5], Our work
Assignments	Affine, Solvable	Polynomial	Polynomial
Invariants	Polynomial	Polynomial$\leq d$	Polynomial$\leq d$
Complete	✓	×	✓

State of the art/Main result

[1][*Hrushovski, Ouaknine, Pouly, Worrell; LICS'18*], [2][*Rodríguez-Carbonell, Kapur; JSC'07*]
[3][*Amrollahi, Bartocci, Kenison et al.; FMSD'24*], [4][*Cyphert, Kincaid; POPL'24*]
[5][*Müller-Olm, Seidl; IPL'04*]

Works	LICS'18[1], JSC'07[2]	FMSD'24[3], POPL'24[4]	IPL'04[5], Our work
Assignments	Affine, Solvable	Polynomial	Polynomial
Invariants	Polynomial	Polynomial$\leq d$	Polynomial$\leq d$
Complete	✓	×	✓

Our contributions

1. Compute the set of initial values s.t. given polynomials are P.I
2. Classify all polynomial invariants of degree $\leq d$ with respect to initial values
3. More efficient algorithm for a given fixed initial value
4. Compute all polynomial invariants of a particular form

State of the art/Main result

[1][*Hrushovski, Ouaknine, Pouly, Worrell; LICS'18*], [2][*Rodríguez-Carbonell, Kapur; JSC'07*]
[3][*Amrollahi, Bartocci, Kenison et al.; FMSD'24*], [4][*Cyphert, Kincaid; POPL'24*]
[5][*Müller-Olm, Seidl; IPL'04*]

Works	LICS'18[1], JSC'07[2]	FMSD'24[3], POPL'24[4]	IPL'04[5], Our work
Assignments	Affine, Solvable	Polynomial	Polynomial
Invariants	Polynomial	Polynomial$\leq d$	Polynomial$\leq d$
Complete	✓	×	✓

Our contributions

1. Compute the set of initial values s.t. given polynomials are P.I
2. Classify all polynomial invariants of degree $\leq d$ with respect to initial values
3. More efficient algorithm for a given fixed initial value
4. Compute all polynomial invariants of a particular form

Hardness of invariant generation

- Undecidable for branching loops [*Hrushovski, Ouaknine, Pouly, Worrell; J.ACM, '23*]
- Simple loops: Skolem-hard [*Müllner, Moosbrugger, Kovács; PACMPL, '24*]

Algebraic geometry formulation

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

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

Algebraic geometry formulation

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

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

$\Longleftrightarrow$

$g(a) = 0$

Algebraic geometry formulation

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

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

$\Longleftrightarrow$

$g(a) = 0$
$g \circ F(a) = 0$

Algebraic geometry formulation

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

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

$\Longleftrightarrow$

$g(a) = 0$
$g \circ F(a) = 0$
$g \circ F^{(2)}(a) = 0$

Algebraic geometry formulation

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

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

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

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

Let $F : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ be a polynomial map and g in $\mathbb{C}[x_1, \ldots, x_n]$. Define the invariant set of (F, g) to be:

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

Invariant sets are algebraic varieties.

Algebraic geometry formulation

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

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

Let $F : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ be a polynomial map and g in $\mathbb{C}[x_1, \ldots, x_n]$. Define the invariant set of (F, g) to be:

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

Invariant sets are algebraic varieties.

Proposition

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

Compute invariant sets

Polynomial map $F : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ and a polynomial g

Proposition

$S_{(F,g)} \stackrel{?}{=}$

Algorithm Invariant set computation

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

Compute invariant sets

Polynomial map $F : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ and a polynomial g

Proposition

$S_{(F,g)} \subset V(g)$

Algorithm Invariant set computation

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

1: $S \leftarrow \{g\}$;

Compute invariant sets

Polynomial map $F : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ and a polynomial g

Proposition

$S_{(F,g)} \subset V(g) \cap V(g \circ F)$

Algorithm Invariant set computation

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

1: $S \leftarrow \{g\}$;
2: $\widetilde{g} \leftarrow g \circ F$;

4: $S \leftarrow S \cup \{\widetilde{g}\}$;

Compute invariant sets

Polynomial map $F : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ and a polynomial g

Proposition

$S_{(F,g)} = V(g) \cap V(g \circ F) \cap V(g \circ F^{(2)}) \cap \ldots$

Algorithm Invariant set computation

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

1: $S \leftarrow \{g\}$;
2: $\widetilde{g} \leftarrow g \circ F$;
3: **while** **do**
4: $\quad S \leftarrow S \cup \{\widetilde{g}\}$;
5: $\quad \widetilde{g} \leftarrow \widetilde{g} \circ F$;
6: **end while**

Compute invariant sets

Polynomial map $F : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ and a polynomial g

Proposition

$S_{(F,g)} = V(g) \cap V(g \circ F) \cap V(g \circ F^{(2)}) \cap \ldots \cap V(g \circ F^{(N)})$ for some $N \in \mathbb{N}$.

Algorithm Invariant set computation

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

1: $S \leftarrow \{g\}$;
2: $\widetilde{g} \leftarrow g \circ F$;
3: **while** $V(S) \neq V(S, \widetilde{g})$ **do**
4: $\quad S \leftarrow S \cup \{\widetilde{g}\}$;
5: $\quad \widetilde{g} \leftarrow \widetilde{g} \circ F$;
6: **end while**

Compute invariant sets

Polynomial map $F : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ and a polynomial g

Proposition

$S_{(F,g)} = V(g) \cap V(g \circ F) \cap V(g \circ F^{(2)}) \cap \ldots \cap V(g \circ F^{(N)})$ for some $N \in \mathbb{N}$.

Algorithm Invariant set computation

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

1: $S \leftarrow \{g\}$;
2: $\widetilde{g} \leftarrow g \circ F$;
3: **while** $V(S) \neq V(S, \widetilde{g})$ **do**
4: $\quad S \leftarrow S \cup \{\widetilde{g}\}$;
5: $\quad \widetilde{g} \leftarrow \widetilde{g} \circ F$;
6: **end while**
7: **return** S;

Example

Let us compute all initial values s.t.

g is a P.I.of $\mathcal{L}((a_1, a_2), F)$:

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

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

Example

Let us compute all initial values s.t.

g is a P.I.of $\mathcal{L}((a_1, a_2), F)$:

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

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

- $g \circ F(x_1, x_2) =$
$$360x_1^3 - 1248x_1^2 x_2 + 40x_1^2 + 1408x_1 x_2^2 - 72x_1 x_2 - 512x_2^3 + 32x_2^2$$

Example

Let us compute all initial values s.t.

g is a P.I.of $\mathcal{L}((a_1, a_2), F)$:

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

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

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

Example

Let us compute all initial values s.t.

g is a P.I.of $\mathcal{L}((a_1, a_2), F)$:

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

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

- $g \circ F(x_1, x_2) =$
  $$360x_1^3 - 1248x_1^2 x_2 + 40x_1^2 + 1408x_1 x_2^2 - 72x_1 x_2 - 512x_2^3 + 32x_2^2$$
- By Gröbner basis computation, $V(g) \neq V(g, g \circ F)$
- $g \circ F^{(2)}(x_1, x_2) =$
  $$7488x_1^3 - 26880x_1^2 x_2 + 832x_1^2 + 31744x_1 x_2^2 - 1600x_1 x_2 - 12288x_2^3 + 768x_2^2$$

  This time, $V(g, g \circ F) = V(g, g \circ F, g \circ F^{(2)})$.

Example

Let us compute all initial values s.t.

g is a P.I.of $\mathcal{L}((a_1, a_2), F)$:

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

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

- $g \circ F(x_1, x_2) =$
  $360x_1^3 - 1248x_1^2 x_2 + 40x_1^2 + 1408x_1 x_2^2 - 72x_1 x_2 - 512x_2^3 + 32x_2^2$
- By Gröbner basis computation, $V(g) \neq V(g, g \circ F)$
- $g \circ F^{(2)}(x_1, x_2) =$
  $7488x_1^3 - 26880x_1^2 x_2 + 832x_1^2 + 31744x_1 x_2^2 - 1600x_1 x_2 - 12288x_2^3 + 768x_2^2$

  This time, $V(g, g \circ F) = V(g, g \circ F, g \circ F^{(2)})$.

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

2. Invariant sets and polynomial invariants

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

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

2. Invariant sets and polynomial invariants

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

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

$\Longleftrightarrow$

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

2. Invariant sets and polynomial invariants

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

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

$\Longleftrightarrow$

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

Theorem

$$S_{(G,h)} = \left\{ (a, b) : \sum_{|\alpha_i| \leq d} b_i x^{\alpha_i} \text{ is a polynomial invariant of } \mathcal{L}(a, F) \right\}$$

2. Invariant sets and polynomial invariants

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

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

$\Longleftrightarrow$

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

Theorem

$$S_{(G,h)} = \left\{ (a, b) : \sum_{|\alpha_i| \leq d} b_i x^{\alpha_i} \text{ is a polynomial invariant of } \mathcal{L}(a, F) \right\}$$

$$S_{(G,h)} = \begin{cases} h(F^{(0)}(x), y) = 0 \\ \vdots \\ h(F^{(N)}(x), y) = 0 \end{cases}$$

2. Invariant sets and polynomial invariants

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

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

$\Longleftrightarrow$

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

Theorem

$$S_{(G,h)} = \left\{ (a, b) : \sum_{|\alpha_i| \leq d} b_i x^{\alpha_i} \text{ is a polynomial invariant of } \mathcal{L}(a, F) \right\}$$

$$S_{(G,h)} = \begin{cases} h(F^{(0)}(x), y) = 0 \\ \vdots \\ h(F^{(N)}(x), y) = 0 \end{cases} = \begin{cases} \sum y_i (F^{(0)}(x))^{\alpha_i} = 0 \\ \vdots \\ \sum y_i (F^{(N)}(x))^{\alpha_i} = 0 \end{cases}$$

Example

Let us compute all polynomial invariants up to degree 2.

$g = \sum_{|\alpha_i| \leq 2} b_i x^{\alpha_i}$ is a P.I.:

$(\mathrm{x}_1, \mathrm{x}_2) \leftarrow (a_1, a_2)$
while true **do**
  $(\mathrm{x}_1, \mathrm{x}_2) \xleftarrow{\mathbf{F}} (10\mathrm{x}_1 - 8\mathrm{x}_2, 6\mathrm{x}_1 - 4\mathrm{x}_2)$
end while

We first run our Algorithm on input $G = (10x_1 - 8x_2, 6x_1 - 4x_2, y_1, \ldots, y_6)$, and $h = y_1 + y_2x_1 + y_3x_2 + y_4x_1^2 + y_5x_1x_2 + y_6x_2^2$. The output is polynomials $h_1, \ldots, h_5$ in $\mathbb{Q}[x_1, x_2, y_1, \ldots, y_6]$ whose common zero set is $S_{(G,h)} \subset \mathbb{C}^8$.

Example

Let us compute all polynomial invariants up to degree 2.

$g = \sum_{|\alpha_i| \leq 2} b_i x^{\alpha_i}$ is a P.I.:

$(\mathrm{x}_1, \mathrm{x}_2) \leftarrow (a_1, a_2)$
while true **do**
$(\mathrm{x}_1, \mathrm{x}_2) \overset{\mathbf{F}}{\leftarrow} (10\mathrm{x}_1 - 8\mathrm{x}_2, 6\mathrm{x}_1 - 4\mathrm{x}_2)$
end while

We first run our Algorithm on input $G = (10x_1 - 8x_2, 6x_1 - 4x_2, y_1, \ldots, y_6)$, and $h = y_1 + y_2x_1 + y_3x_2 + y_4x_1^2 + y_5x_1x_2 + y_6x_2^2$. The output is polynomials $h_1, \ldots, h_5$ in $\mathbb{Q}[x_1, x_2, y_1, \ldots, y_6]$ whose common zero set is $S_{(G,h)} \subset \mathbb{C}^8$.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3x_1 - 4x_2 & 3x_1 - 4x_2 & 0 & 0 & 0 \\ 0 & 64x_2 & 112x_2 - 48x_1 & 48x_2^2 & 84x_2^2 - 36x_1x_2 & 27x_1^2 - 126x_1x_2 + 147x_2^2 \\ 0 & 32x_2 & 56x_2 - 24x_1 & 24x_1x_2 & -9x_1^2 + 21x_1x_2 + 12x_2^2 & -18x_1x_2 + 42x_2^2 \\ 0 & 4x_2 & 7x_2 - 3x_1 & 3x_1^2 & 3x_1x_2 & 3x_2^2 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \end{bmatrix} = 0$$

g is a P.I of $\mathcal{L}((a_1, a_2), F) \iff (a_1, a_2, b_1, \ldots, b_6) \in V(h_1, \ldots, h_5)$.

Example

Let us compute all polynomial invariants up to degree 2.

$g = \sum_{|\alpha_i| \leq 2} b_i x^{\alpha_i}$ is a P.I.:

$(\mathrm{x}_1, \mathrm{x}_2) \leftarrow (a_1, a_2)$
while true **do**
  $(\mathrm{x}_1, \mathrm{x}_2) \overset{\mathbf{F}}{\leftarrow} (10\mathrm{x}_1 - 8\mathrm{x}_2, 6\mathrm{x}_1 - 4\mathrm{x}_2)$
end while

We first run our Algorithm on input $G = (10x_1 - 8x_2, 6x_1 - 4x_2, y_1, \ldots, y_6)$, and $h = y_1 + y_2x_1 + y_3x_2 + y_4x_1^2 + y_5x_1x_2 + y_6x_2^2$. The output is polynomials $h_1, \ldots, h_5$ in $\mathbb{Q}[x_1, x_2, y_1, \ldots, y_6]$ whose common zero set is $S_{(G,h)} \subset \mathbb{C}^8$.

Initial values	Basis of $I_{2,\mathcal{L}}$
$S_1 = \{(0,0)\}$	$T_1 = \{x_1, x_2, x_1x_2, x_1^2, x_2^2\}$
$S_2 = \{(a,a) \mid a \in \mathbb{C}^*\}$	$T_2 = \{x_1 - x_2, x_1^2 - x_1x_2, -x_1x_2 + x_2^2\}$
$S_3 = \left\{\left(\frac{4}{3}a, a\right) \mid a \in \mathbb{C}^*\right\}$	$T_3 = \{3x_1 - 4x_2, -3x_1^2 + 16x_1x_2 - 16x_2^2, -3x_1x_2 + 4x_2^2\}$
$S_4 = \{(a_1,a_2) \in \mathbb{C}^2 \mid a_1 \neq \frac{4}{3}a_2, a_1 \neq a_2\}$	$T_4 = \{(3a_1 - 4a_2)^2x_1 - (3a_1 - 4a_2)^2x_2 - 9(a_1 - a_2)x_1^2$ $+24(a_1 - a_2)x_1x_2 - 16(a_1 - a_2)x_2^2\}$

3. Loops with given initial values

$$S_{(G,h)} = \begin{cases} \sum y_i (F^{(0)}(x))^{\alpha_i} = 0 \\ \vdots \\ \sum y_i (F^{(N)}(x))^{\alpha_i} = 0 \end{cases}$$

3. Loops with given initial values

$$\{\text{coefficients of P.I. of } \mathcal{L}(a, F)\} = \begin{cases} \sum y_i (F^{(0)}(a))^{\alpha_i} = 0 \\ \vdots \\ \sum y_i (F^{(N)}(a))^{\alpha_i} = 0 \end{cases}$$

3. Loops with given initial values

$$\{\text{coefficients of P.I. of } \mathcal{L}(a, F)\}\ ? \begin{cases} \sum y_i (F^{(0)}(a))^{\alpha_i} = 0 \\ \vdots \\ \sum y_i (F^{(\mathbf{k})}(a))^{\alpha_i} = 0 \end{cases}$$

3. Loops with given initial values

$$\{\text{coefficients of P.I. of } \mathcal{L}(a, F)\} \subseteq \begin{cases} \sum y_i (F^{(0)}(a))^{\alpha_i} = 0 \\ \vdots \\ \sum y_i (F^{(k)}(a))^{\alpha_i} = 0 \end{cases}$$

3. Loops with given initial values

$$\{\text{coefficients of P.I. of } \mathcal{L}(a, F)\} \subseteq \begin{cases} \sum y_i (F^{(0)}(a))^{\alpha_i} = 0 \\ \vdots \\ \sum y_i (F^{(k)}(a))^{\alpha_i} = 0 \end{cases} \cong Span(g_1(x), \ldots, g_s(x))$$

3. Loops with given initial values

$$\{\text{coefficients of P.I. of } \mathcal{L}(a,F)\} \subseteq \begin{cases} \sum y_i (F^{(0)}(a))^{\alpha_i} = 0 \\ \vdots \\ \sum y_i (F^{(k)}(a))^{\alpha_i} = 0 \end{cases} \cong Span(g_1(x), \ldots, g_s(x))$$

Proposition

For every P.I. g of $\mathcal{L}(a,F)$, g is a linear combination of $g_1(x), \ldots, g_s(x)$.

3. Loops with given initial values

$$\{\text{coefficients of P.I. of } \mathcal{L}(a,F)\} \subseteq \begin{cases} \sum y_i (F^{(0)}(a))^{\alpha_i} = 0 \\ \vdots \\ \sum y_i (F^{(k)}(a))^{\alpha_i} = 0 \end{cases} \cong Span(g_1(x), \ldots, g_s(x))$$

Proposition

For every P.I. g of $\mathcal{L}(a,F)$, g is a linear combination of $g_1(x), \ldots, g_s(x)$.

$g = \sum_{|\alpha_i| \leq d} b_i x^{\alpha_i}$ is a P.I.

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

$\binom{n+d}{d}$ = nb of monomials x^{α_i}

3. Loops with given initial values

$$\{\text{coefficients of P.I. of } \mathcal{L}(a,F)\} \subseteq \begin{cases} \sum y_i (F^{(0)}(a))^{\alpha_i} = 0 \\ \vdots \\ \sum y_i (F^{(k)}(a))^{\alpha_i} = 0 \end{cases} \cong Span(g_1(x), \ldots, g_s(x))$$

Proposition

For every P.I. g of $\mathcal{L}(a,F)$, g is a linear combination of $g_1(x), \ldots, g_s(x)$.

$g = \sum_{|\alpha_i| \leq d} b_i x^{\alpha_i}$ is a P.I.

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

$\iff$

$g = \sum_{i=1}^{s} \lambda_i g_i(x)$ is a P.I.

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

$\binom{n+d}{d} = \text{nb of monomials } x^{\alpha_i} \quad \geq \quad s = \text{number of } g_i(x)$

4. General polynomial invariants

Polynomial invariants of a form $g(x) - c(a) = 0$ for all initial values a

4. General polynomial invariants

Polynomial invariants of a form $g(x) - g(a) = 0$ for all initial values a

4. General polynomial invariants

Polynomial invariants of a form $g(x) - g(a) = 0$ for all initial values a

Proposition

For all a, $g(x) - g(a)$ P.I. for $\mathcal{L}(a, F)$ if and only if $g \circ F(x) = g(x)$

4. General polynomial invariants

Polynomial invariants of a form $g(x) - g(a) = 0$ for all initial values a

Proposition

For all a, $g(x) - g(a)$ P.I. for $\mathcal{L}(a, F)$ if and only if $g \circ F(x) = g(x)$

Consider $g = \sum_{|\alpha_i| \leq d} y_i x^{\alpha_i}$. Assume that $g(x) - g(a)$ is P.I for $\mathcal{L}(a, F)$ for all a.

4. General polynomial invariants

Polynomial invariants of a form $g(x) - g(a) = 0$ for all initial values a

Proposition

For all a, $g(x) - g(a)$ P.I. for $\mathcal{L}(a, F)$ if and only if $g \circ F(x) = g(x)$

Consider $g = \sum_{|\alpha_i| \leq d} y_i x^{\alpha_i}$. Assume that $g(x) - g(a)$ is P.I for $\mathcal{L}(a, F)$ for all a.

$$\sum_{|\alpha_i| \leq d} y_i x^{\alpha_i} = \sum_{|\alpha_i| \leq d} y_i (F(x))^{\alpha_i}$$

4. General polynomial invariants

Polynomial invariants of a form $g(x) - g(a) = 0$ for all initial values a

Proposition

For all a, $g(x) - g(a)$ P.I. for $\mathcal{L}(a, F)$ if and only if $g \circ F(x) = g(x)$

Consider $g = \sum_{|\alpha_i| \leq d} y_i x^{\alpha_i}$. Assume that $g(x) - g(a)$ is P.I for $\mathcal{L}(a, F)$ for all a.

$$\sum_{|\alpha_i| \leq d} y_i x^{\alpha_i} = \sum_{|\alpha_i| \leq d} y_i (F(x))^{\alpha_i} \iff \begin{cases} \sum c_{1,i} y_i = 0 \\ \vdots \\ \sum c_{k,i} y_i = 0 \end{cases}$$

Example: Fibonacci trace map

Let us compute all polynomial invariants of the form $g(x) - g(a)$ up to degree 4 for the following loop.

$(\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3) = (a_1, a_2, a_3)$
while true **do**

$$\begin{pmatrix} \mathrm{x}_1 \\ \mathrm{x}_2 \\ \mathrm{x}_3 \end{pmatrix} \xleftarrow{\mathbf{F}} \begin{pmatrix} \mathrm{x}_2 \\ \mathrm{x}_3 \\ 2\mathrm{x}_2\mathrm{x}_3 - \mathrm{x}_1 \end{pmatrix}$$

end while

Example: Fibonacci trace map

Let us compute all polynomial invariants of the form $g(x) - g(a)$ up to degree 4 for the following loop.

$(\mathtt{x}_1, \mathtt{x}_2, \mathtt{x}_3) = (a_1, a_2, a_3)$
while true **do**
$$\begin{pmatrix} \mathtt{x}_1 \\ \mathtt{x}_2 \\ \mathtt{x}_3 \end{pmatrix} \xleftarrow{\mathbf{F}} \begin{pmatrix} \mathtt{x}_2 \\ \mathtt{x}_3 \\ 2\mathtt{x}_2\mathtt{x}_3 - \mathtt{x}_1 \end{pmatrix}$$
end while

Define $g = y_1 + y_2 x_3 + y_3 x_2 + y_4 x_1 + \ldots + y_{35} x_1^4$.

Example: Fibonacci trace map

Let us compute all polynomial invariants of the form $g(x) - g(a)$ up to degree 4 for the following loop.

$(\mathtt{x}_1, \mathtt{x}_2, \mathtt{x}_3) = (a_1, a_2, a_3)$
while true **do**
$$\begin{pmatrix} \mathtt{x}_1 \\ \mathtt{x}_2 \\ \mathtt{x}_3 \end{pmatrix} \xleftarrow{\mathbf{F}} \begin{pmatrix} \mathtt{x}_2 \\ \mathtt{x}_3 \\ 2\mathtt{x}_2\mathtt{x}_3 - \mathtt{x}_1 \end{pmatrix}$$
end while

Define $g = y_1 + y_2 x_3 + y_3 x_2 + y_4 x_1 + \ldots + y_{35} x_1^4$.

$$y_1 + y_2 x_1 + y_3 x_2 + y_4 x_3 + \ldots + y_{35} x_3^4 = y_1 + y_2(2x_2 x_3 - x_1) + y_3 x_3 + y_4 x_2 + \ldots + y_{35} x_2^4$$

Example: Fibonacci trace map

Let us compute all polynomial invariants of the form $g(x) - g(a)$ up to degree 4 for the following loop.

$(\mathtt{x}_1, \mathtt{x}_2, \mathtt{x}_3) = (a_1, a_2, a_3)$
while true **do**
$$\begin{pmatrix} \mathtt{x}_1 \\ \mathtt{x}_2 \\ \mathtt{x}_3 \end{pmatrix} \xleftarrow{\mathbf{F}} \begin{pmatrix} \mathtt{x}_2 \\ \mathtt{x}_3 \\ 2\mathtt{x}_2\mathtt{x}_3 - \mathtt{x}_1 \end{pmatrix}$$
end while

Define $g = y_1 + y_2 x_3 + y_3 x_2 + y_4 x_1 + \ldots + y_{35} x_1^4$.

$$y_1 + y_2 x_1 + y_3 x_2 + y_4 x_3 + \ldots + y_{35} x_3^4 = y_1 + y_2(2x_2 x_3 - x_1) + y_3 x_3 + y_4 x_2 + \ldots + y_{35} x_2^4$$

54 linear equations are obtained from the equation above such as

$$y_2 - y_3, y_4 - y_3, 16y_{11}, \text{ and } y_{10} - y_8$$

Example: Fibonacci trace map

Let us compute all polynomial invariants of the form $g(x) - g(a)$ up to degree 4 for the following loop.

$(\mathtt{x}_1, \mathtt{x}_2, \mathtt{x}_3) = (a_1, a_2, a_3)$
while true **do**
$$\begin{pmatrix} \mathtt{x}_1 \\ \mathtt{x}_2 \\ \mathtt{x}_3 \end{pmatrix} \xleftarrow{\mathbf{F}} \begin{pmatrix} \mathtt{x}_2 \\ \mathtt{x}_3 \\ 2\mathtt{x}_2\mathtt{x}_3 - \mathtt{x}_1 \end{pmatrix}$$
end while

Define $g = y_1 + y_2 x_3 + y_3 x_2 + y_4 x_1 + \ldots + y_{35} x_1^4$.

$$y_1 + y_2 x_1 + y_3 x_2 + y_4 x_3 + \ldots + y_{35} x_3^4 = y_1 + y_2(2x_2 x_3 - x_1) + y_3 x_3 + y_4 x_2 + \ldots + y_{35} x_2^4$$

54 linear equations are obtained from the equation above such as

$$y_2 - y_3, y_4 - y_3, 16y_{11}, \text{ and } y_{10} - y_8$$

The following is the only one P.I. for $\mathcal{L}(a, F)$ for all $(a_1, a_2, a_3) \in \mathbb{C}^3$.

$$x_1^2 + x_2^2 + x_3^2 - 2x_1 x_2 x_3 - (a_1^2 + a_2^2 + a_3^2 - 2a_1 a_2 a_3) = 0$$

Conclusion

Summary

1. Compute the set of initial values s.t. given polynomials are P.I.
2. Classify all polynomial invariants of degree $\leq d$ w.r.t initial values
3. More efficient algorithm for a given fixed initial value
4. Compute all polynomial invariants of the form $g(x) - g(a) = 0$

Conclusion

Summary

1. Compute the set of initial values s.t. given polynomials are P.I.
2. Classify all polynomial invariants of degree $\leq d$ w.r.t initial values
3. More efficient algorithm for a given fixed initial value
4. Compute all polynomial invariants of the form $g(x) - g(a) = 0$

Thank you for your attention!