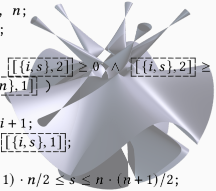
Algebraic Geometry for Loop Invariants and Program Synthesis

9th October 2025 | Pascaline Seminar

```
@real: i, s, n;
@pre: n ≥ 1;
i = 0; s = 0;
@invariant: [[{i,s},2]] ≥ 0  ∧  [[{i,s},2]] ≥ 0
while( [[{i,n},1]] )
{
        i = i + 1;
        s = [[{i,s},1]];
}
@post: (n − 1) · n/2 ≤ s ≤ n · (n + 1)/2;
```



Rémi Prébet
Joint works with E. Bayarmagnai (PhD), F. Mohammadi

Slides: rprebet.github.io/#talks

Program Verification and Synthesis

Verification

Test or Generate specification for a program

Synthesis

Generate a program from a given specification

Program Verification and Synthesis

Polynomial loop

$\mathtt{x} = (\mathtt{x}_1, \ldots, \mathtt{x}_n)$ and
$F \in \mathbb{Q}[\mathtt{x}]^n$ polynomial map

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

Verification

Test or Generate polynomial invariants

Synthesis

Generate a loop from polynomial invariant

Polynomial loop invariant

Ψ formula polynomial in $\mathtt{x}$ s.t.:

- $\Psi(a)$ is true
- $\Psi(F(a))$ is true
- $\Psi(F^{(2)}(a))$ is true

$\vdots \qquad \vdots$

Program Verification and Synthesis

Polynomial loop

$\mathtt{x} = (\mathtt{x}_1, \ldots, \mathtt{x}_n)$ and

$F \in \mathbb{Q}[\mathtt{x}]^n$ polynomial map

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

Verification

Test or Generate polynomial invariants

Synthesis

Generate a loop from polynomial invariant

Polynomial loop invariant

Ψ formula polynomial in $\mathtt{x}$ s.t.:

- $\Psi(a)$ is true
- $\Psi(F(a))$ is true
- $\Psi(F^{(2)}(a))$ is true
- $\vdots \qquad \vdots$

Polynomial Loop

```
(c, k, m, n) = (0, 1, 6, 0)
while n < N do
    c ← c + k
    k ← k + 6n + 6
    m ← m + 6
    n ← n + 1
end while
```

Program Verification and Synthesis

Polynomial loop

$\mathtt{x} = (\mathtt{x}_1, \ldots, \mathtt{x}_n)$ and

$F \in \mathbb{Q}[\mathtt{x}]^n$ polynomial map

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

Verification

Test or Generate polynomial invariants

Synthesis

Generate a loop from polynomial invariant

Polynomial loop invariant

Ψ formula polynomial in $\mathtt{x}$ s.t.:

- $\Psi(a)$ is true
- $\Psi(F(a))$ is true
- $\Psi(F^{(2)}(a))$ is true

$\vdots \qquad\qquad \vdots$

Polynomial Loop

```
(c, k, m, n) = (0, 1, 6, 0)
while n < N do
    c ← c + k
    k ← k + 6n + 6
    m ← m + 6
    n ← n + 1
end while
```

Polynomial Invariants

$$c = n^3 \;\wedge\; k = 3n^2 + 3n + 1 \;\wedge\; m = 6n + 6 \;\wedge\; n \leq N$$

Program Verification and Synthesis

Polynomial loop

$\mathtt{x} = (\mathtt{x}_1, \dots, \mathtt{x}_n)$ and

$F \in \mathbb{Q}[\mathtt{x}]^n$ polynomial map

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

Verification

Test or Generate polynomial invariants

Synthesis

Generate a loop from polynomial invariant

Polynomial loop invariant

Ψ formula polynomial in $\mathtt{x}$ s.t.:

- $\Psi(a)$ is true
- $\Psi(F(a))$ is true
- $\Psi(F^{(2)}(a))$ is true

$\vdots \qquad \vdots$

Polynomial Loop

```
(c, k, m, n) = (0, 1, 6, 0)
while n < N do
    c ← c + k
    k ← k + 6n + 6
    m ← m + 6
    n ← n + 1
end while
```

Polynomial Invariants

$$c = n^3 \wedge k = 3n^2 + 3n + 1 \wedge m = 6n + 6 \wedge n \leq N$$

Postcondition

$$c_{\text{final}} = N^3$$

Program Verification and Synthesis

Polynomial loop

$\mathtt{x} = (\mathtt{x}_1, \ldots, \mathtt{x}_n)$ and

$F \in \mathbb{Q}[\mathtt{x}]^n$ polynomial map

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

Verification

Test or Generate polynomial invariants

Synthesis

Generate a loop from polynomial invariant

Polynomial loop invariant

Ψ formula polynomial in $\mathtt{x}$ s.t.:

- $\Psi(a)$ is true
- $\Psi(F(a))$ is true
- $\Psi(F^{(2)}(a))$ is true
- $\vdots$ $\qquad\vdots$

Polynomial Loop

1: $(\mathtt{c}, \mathtt{k}, \mathtt{m}, \mathtt{n}) = (0, 1, 6, 0)$
2: **while** $\mathtt{n} < \mathtt{N}$ **do**
3: $\mathtt{c} \leftarrow \mathtt{c} + \mathtt{k}$
4: $\mathtt{k} \leftarrow \mathtt{k} + \mathtt{m}$
5: $\mathtt{m} \leftarrow \mathtt{m} + 6$
6: $\mathtt{n} \leftarrow \mathtt{n} + 1$
7: **end while**

Polynomial Invariants

$$c = n^3 \wedge k = 3n^2 + 3n + 1 \wedge m = 6n + 6 \wedge n \leq N$$

Postcondition

$$c_{\mathrm{final}} = N^3$$

Polynomial equations

A difficult problem

Invariant ideal $\mathcal{I}(\mathcal{L})$

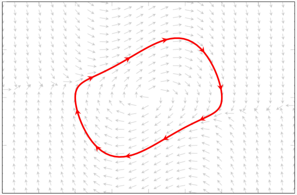
Polynomial invariants (equations) for a loop $\mathcal{L}$ form an ideal

Hilbert basis theorem $\longrightarrow$ Compute a *finite* basis

Discrete Van der Pol oscillator

1: $(\mathtt{x}, \mathtt{y}) = (x_0, y_0)$
2: **while** true **do**
3: $\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \end{bmatrix} \leftarrow \begin{bmatrix} \mathtt{x} + \Delta_t \mathtt{y} \\ \mathtt{y} + (\mathtt{y}(1 - \mathtt{x}^2) - \mathtt{x})\Delta_t \end{bmatrix}$
4: **end while**

Algebraic geometry $\longrightarrow$



A difficult problem

Invariant ideal $\mathcal{I}(\mathcal{L})$

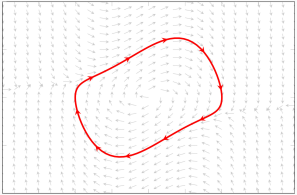
Polynomial invariants (equations) for a loop $\mathcal{L}$ form an ideal

$\xrightarrow{\text{Hilbert basis theorem}}$ Compute a *finite* basis

Discrete Van der Pol oscillator

$(\mathtt{x}, \mathtt{y}) = (x_0, y_0)$
while true **do**
$$\begin{bmatrix}\mathtt{x}\\ \mathtt{y}\end{bmatrix} \leftarrow \begin{bmatrix}\mathtt{x} + \Delta_t \mathtt{y}\\ \mathtt{y} + (\mathtt{y}(1-\mathtt{x}^2) - \mathtt{x})\Delta_t\end{bmatrix}$$
end while

$\xrightarrow{\text{Algebraic geometry}}$



Computability results [Müllner & Moosbrugger & Kovác 2024] ✓: decidable ✗: undecidable ?: unknown

Program model		Affine Inv	Poly. Inv
Unguarded	Affine	✓ [Karr 1976]	✓ [Kovác 2008]
	Poly.	✓ [Müller-Olm & Seidl 2004]	? SKOLEM-HARD [Müllner et al. 2024]
Guarded $(=, \leq)$	Affine	✗ (Halting Problem) [Hopcroft & Ullman 1969]	
	Poly.		

A difficult problem

Invariant ideal $\mathcal{I}(\mathcal{L})$

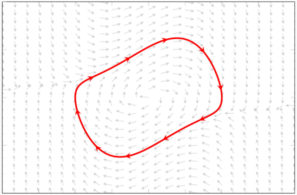
Polynomial invariants (equations) for a loop $\mathcal{L}$ form an ideal

$\xrightarrow{\text{Hilbert basis theorem}}$ Compute a *finite* basis

Discrete Van der Pol oscillator

1: $(\mathtt{x}, \mathtt{y}) = (x_0, y_0)$
2: **while** true **do**
3: $\begin{bmatrix}\mathtt{x}\\ \mathtt{y}\end{bmatrix} \leftarrow \begin{bmatrix}\mathtt{x} + \Delta_t \mathtt{y}\\ \mathtt{y} + (\mathtt{y}(1-\mathtt{x}^2) - \mathtt{x})\Delta_t\end{bmatrix}$
4: **end while**

$\xrightarrow{\text{Algebraic geometry}}$



Computability results [Müllner & Moosbrugger & Kovác 2024] ✓: decidable ✗: undecidable ?: unknown

Program model		Affine Inv	Poly. Inv
Unguarded	Affine	✓ [Karr 1976]	✓ [Kovác 2008]
	Poly.	✓ [Müller-Olm & Seidl 2004]	? SKOLEM-HARD [Müllner et al. 2024]
Guarded ($=, \leq$)	Affine	✗ (Halting Problem) [Hopcroft & Ullman 1969]	
	Poly.		

Truncated invariant ideal

$\mathcal{I}(\mathcal{L}) \cap \mathbb{C}[\mathtt{x}]_{\leq d}$ computable [Müller-Olm & Seidl 2004]

A difficult problem

Invariant ideal $\mathcal{I}(\mathcal{L})$

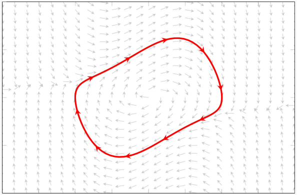
Polynomial invariants (equations) for a loop $\mathcal{L}$ form an ideal

Hilbert basis theorem $\longrightarrow$ Compute a *finite* basis

Discrete Van der Pol oscillator

1: $(\mathtt{x}, \mathtt{y}) = (x_0, y_0)$
2: **while** true **do**
3: $\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \end{bmatrix} \leftarrow \begin{bmatrix} \mathtt{x} + \Delta_t \mathtt{y} \\ \mathtt{y} + (\mathtt{y}(1 - \mathtt{x}^2) - \mathtt{x})\Delta_t \end{bmatrix}$
4: **end while**

Algebraic geometry $\longrightarrow$



Computability results [Müllner & Moosbrugger & Kovác 2024] ✓: decidable ✗: undecidable ?: unknown

Program model		Affine Inv	Poly. Inv
Unguarded	Affine	✓ [Karr 1976]	✓ [Kovác 2008]
	Poly.	✓ [Müller-Olm & Seidl 2004]	? SKOLEM-HARD [Müllner et al. 2024]
Guarded $(=, \leq)$	Affine	✗ (Halting Problem) [Hopcroft & Ullman 1969]	
	Poly.		

Truncated invariant ideal

$\mathcal{I}(\mathcal{L}) \cap \mathbb{C}[\mathtt{x}]_{\leq d}$ computable [Müller-Olm & Seidl 2004]

BUT

Degree of regularity [Eisenbud 2005]

Find d such that it generates $\mathcal{I}(\mathcal{L})$ is hard!

Reduction to parametric invariant test

Invariant test

$\mathtt{X} \leftarrow \boldsymbol{A}?$

while $\mathtt{true}$ **do**

Assert: $\sum \boldsymbol{\lambda_i} \cdot \mathtt{X}^{\alpha_i} = 0$

$\mathtt{X} \leftarrow \sum \boldsymbol{f_i} \cdot \mathtt{X}^{\beta_i}$

end while

Reduction to parametric invariant test

Invariant generation

$(\mathtt{x}, \mathtt{c}) \leftarrow (\boldsymbol{a}, \boldsymbol{\lambda})?$

while true do

Assert: $\sum_i 1 \cdot \mathtt{c}_i \mathtt{x}^{\alpha_i} = 0$

$(\mathtt{x}, \mathtt{c}) \leftarrow \left(\sum \boldsymbol{f_i} \cdot \mathtt{x}^{\beta_i}, \mathtt{c}\right)$

end while

$\downarrow$

Invariant test

$\mathtt{X} \leftarrow \boldsymbol{A}?$

while true do

Assert: $\sum \boldsymbol{\lambda_i} \cdot \mathtt{X}^{\alpha_i} = 0$

$\mathtt{X} \leftarrow \sum \boldsymbol{f_i} \cdot \mathtt{X}^{\beta_i}$

end while

Reduction to parametric invariant test

Invariant generation

$(\mathtt{x}, \mathtt{c}) \leftarrow (\boldsymbol{a}, \boldsymbol{\lambda})?$

while true do

Assert: $\sum_i 1 \cdot \mathtt{c}_i \mathtt{x}^{\alpha_i} = 0$

$(\mathtt{x}, \mathtt{c}) \leftarrow \left(\sum \boldsymbol{f_i} \cdot \mathtt{x}^{\beta_i}, \mathtt{c}\right)$

end while

Loop synthesis

$(\mathtt{x}, \mathtt{c}) \leftarrow (\boldsymbol{a}, \boldsymbol{f})?$

while true do

Assert: $\sum_i \boldsymbol{\lambda_i} \cdot \mathtt{x}^{\alpha_i} = 0$

$(\mathtt{x}, \mathtt{c}) \leftarrow \left(\sum 1 \cdot \mathtt{c}_i \mathtt{x}^{\beta_i}, \mathtt{c}\right)$

end while

Invariant test

$\mathtt{X} \leftarrow \boldsymbol{A}?$

while true do

Assert: $\sum \boldsymbol{\lambda_i} \cdot \mathtt{X}^{\alpha_i} = 0$

$\mathtt{X} \leftarrow \sum \boldsymbol{f_i} \cdot \mathtt{X}^{\beta_i}$

end while

Reduction to parametric invariant test

Invariant generation

$(\mathtt{x}, \mathtt{c}) \leftarrow (\boldsymbol{a}, \boldsymbol{\lambda})$?

while true do

Assert: $\sum_i 1 \cdot \mathtt{c}_i \mathtt{x}^{\alpha_i} = 0$

$(\mathtt{x}, \mathtt{c}) \leftarrow \left(\sum \boldsymbol{f_i} \cdot \mathtt{x}^{\beta_i}, \mathtt{c}\right)$

end while

Loop synthesis

$(\mathtt{x}, \mathtt{c}) \leftarrow (\boldsymbol{a}, \boldsymbol{f})$?

while true do

Assert: $\sum_i \boldsymbol{\lambda_i} \cdot \mathtt{x}^{\alpha_i} = 0$

$(\mathtt{x}, \mathtt{c}) \leftarrow \left(\sum 1 \cdot \mathtt{c}_i \mathtt{x}^{\beta_i}, \mathtt{c}\right)$

end while

Invariant test

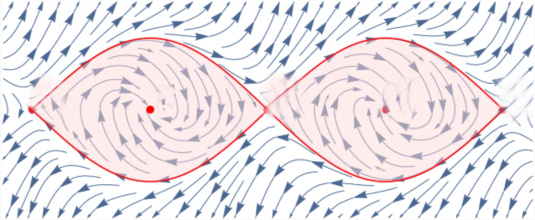
$\mathtt{X} \leftarrow \boldsymbol{A}$?

while true do

Assert: $\sum \boldsymbol{\lambda_i} \cdot \mathtt{X}^{\alpha_i} = 0$

$\mathtt{X} \leftarrow \sum \boldsymbol{f_i} \cdot \mathtt{X}^{\beta_i}$

end while



Invariant set

For which $\boldsymbol{A} \in \mathbb{C}^n$, $\boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{A}) = 0$ for all $m \geq 0$?

Invariant set

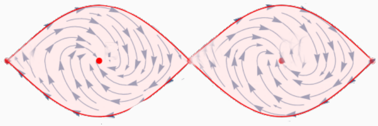
Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \{\boldsymbol{a} \in \mathbb{C}^n, \forall m \geq 0, \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) = 0\}$$

Stabilisation property

$X_m = \{\boldsymbol{h} = \boldsymbol{h} \circ \boldsymbol{F} = \cdots \boldsymbol{h} \circ \boldsymbol{F}^{(m)} = 0\}$



Invariant set

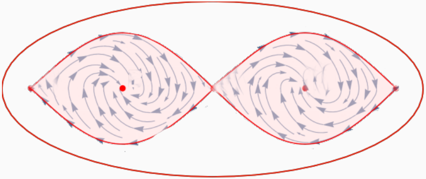
Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \{\boldsymbol{a} \in \mathbb{C}^n, \forall m \geq 0, \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) = 0\}$$

Stabilisation property

$X_m = \{\boldsymbol{h} = \boldsymbol{h} \circ \boldsymbol{F} = \cdots \boldsymbol{h} \circ \boldsymbol{F}^{(m)} = 0\}$
$S_{(\boldsymbol{F},\boldsymbol{h})} = X_0 \cap \dots$



Invariant set

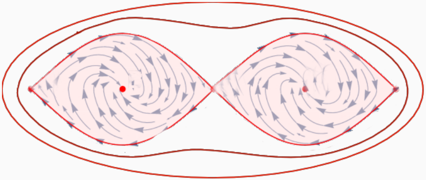
Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \{\boldsymbol{a} \in \mathbb{C}^n, \forall m \geq 0, \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) = 0\}$$

Stabilisation property

$$X_m = \{\boldsymbol{h} = \boldsymbol{h} \circ \boldsymbol{F} = \cdots \boldsymbol{h} \circ \boldsymbol{F}^{(m)} = 0\}$$
$$S_{(\boldsymbol{F},\boldsymbol{h})} = X_0 \cap X_1 \cap \ldots$$
$$\supset$$



Invariant set

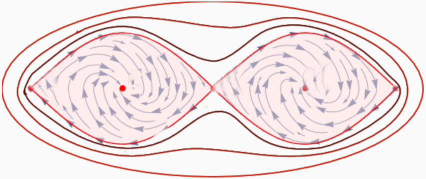
Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \{\boldsymbol{a} \in \mathbb{C}^n, \forall m \geq 0, \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) = 0\}$$

Stabilisation property

$$\begin{aligned} X_m &= \{\boldsymbol{h} = \boldsymbol{h} \circ \boldsymbol{F} = \cdots \boldsymbol{h} \circ \boldsymbol{F}^{(m)} = 0\} \\ S_{(\boldsymbol{F},\boldsymbol{h})} &= X_0 \cap X_1 \cap \ldots \cap X_m \ \cap \ldots \\ &\quad\ \supset \quad \supset \cdots \supset \quad\ \supset \ldots \end{aligned}$$



Invariant set

Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

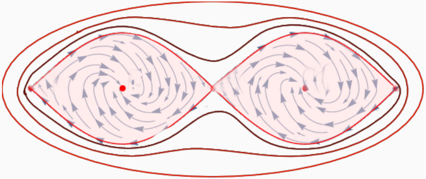
$$S_{(\boldsymbol{F},\boldsymbol{h})} = \{\boldsymbol{a} \in \mathbb{C}^n, \forall m \geq 0, \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) = 0\}$$

Stabilisation property

$$X_m = \{\boldsymbol{h} = \boldsymbol{h} \circ \boldsymbol{F} = \cdots \boldsymbol{h} \circ \boldsymbol{F}^{(m)} = 0\}$$

$$S_{(\boldsymbol{F},\boldsymbol{h})} = X_0 \cap X_1 \cap \ldots \cap X_N \cap X_{N+1}$$

$$\supset \qquad \supset \cdots \supset \qquad =$$



Invariant set

Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

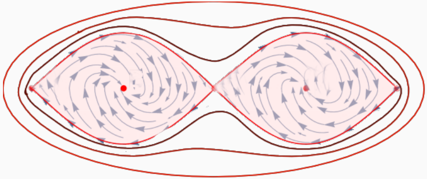
$$S_{(\boldsymbol{F},\boldsymbol{h})} = \{\boldsymbol{a} \in \mathbb{C}^n, \forall m \geq 0, \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) = 0\}$$

Stabilisation property

$$X_m = \{\boldsymbol{h} = \boldsymbol{h} \circ \boldsymbol{F} = \cdots \boldsymbol{h} \circ \boldsymbol{F}^{(m)} = 0\}$$

$$S_{(\boldsymbol{F},\boldsymbol{h})} = X_0 \cap X_1 \cap \ldots \cap X_N \cap X_{N+1}$$

$$\supsetneq \quad \supsetneq \cdots \supsetneq \quad =$$



Invariant set

Definition

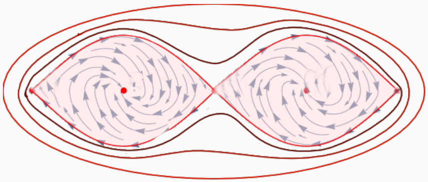
Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \{\boldsymbol{a} \in \mathbb{C}^n, \forall m \geq 0, \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) = 0\}$$

Stabilisation property

$$X_m = \{\boldsymbol{h} = \boldsymbol{h} \circ \boldsymbol{F} = \cdots \boldsymbol{h} \circ \boldsymbol{F}^{(m)} = 0\}$$

$$\begin{array}{ccccccccccc} S_{(\boldsymbol{F},\boldsymbol{h})} = & X_0 & \cap & X_1 & \cap \ldots \cap & X_N & \cap & X_{N+1} \\ & & \supsetneq & & \supsetneq \cdots \supsetneq & & = & \end{array}$$



Algorithm

Compute $\boldsymbol{h} \circ \boldsymbol{F}^{(m)}(x)$ until $X_N = X_{N+1}$

Radical membership test:

$$\boldsymbol{h} \circ \boldsymbol{F}^{(N+1)}(x) \in \sqrt{\langle \boldsymbol{h}, \ldots, \boldsymbol{h} \circ \boldsymbol{F}^{(N)} \rangle}$$

Invariant set

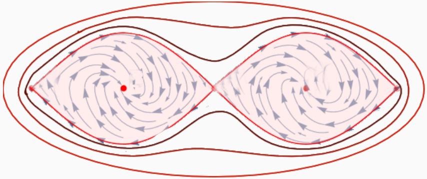
Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \{\boldsymbol{a} \in \mathbb{C}^n, \forall m \geq 0, \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) = 0\}$$

Stabilisation property

$$X_m = \{\boldsymbol{h} = \boldsymbol{h} \circ \boldsymbol{F} = \cdots \boldsymbol{h} \circ \boldsymbol{F}^{(m)} = 0\}$$
$$S_{(\boldsymbol{F},\boldsymbol{h})} = X_0 \cap X_1 \cap \ldots \cap X_N \cap X_{N+1}$$
$$\supsetneq \quad \supsetneq \cdots \supsetneq \quad =$$



Algorithm

Compute $\boldsymbol{h} \circ \boldsymbol{F}^{(m)}(x)$ until $X_N = X_{N+1}$

Radical membership test:

$$\boldsymbol{h} \circ \boldsymbol{F}^{(N+1)}(x) \in \sqrt{\langle \boldsymbol{h}, \ldots, \boldsymbol{h} \circ \boldsymbol{F}^{(N)} \rangle}$$

Complexity

- Radical membership: $\rightsquigarrow$ poly. in D^{Nn^2}
- N may be *Ackermann-large* (sharp)
- primitive recursive under assumptions on $\boldsymbol{F}$

[Seidenberg '72; Moreno-Socías '92; Novikov, Yakovenko '99; Benedikt, Duff, Sharad, Worrel 2017]

Testing polynomial invariant

Invariant test

$(\mathtt{x}, \mathtt{y}) \leftarrow (\boldsymbol{a}, \boldsymbol{b})$

while true **do**

Assert: $\boldsymbol{h} = \mathtt{x}^2 - \mathtt{x}\mathtt{y} + 9\mathtt{x}^3 - 24\mathtt{x}^2\mathtt{y} + 16\mathtt{x}\mathtt{y}^2 = 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \end{bmatrix} \leftarrow \boldsymbol{F}(\mathtt{x}, \mathtt{y}) = \begin{bmatrix} 10\mathtt{x} - 8\mathtt{y} \\ 6\mathtt{x} - 4\mathtt{y} \end{bmatrix}$$

end while

Testing polynomial invariant

Invariant test

$(x, y) \leftarrow (a, b)$

while true **do**

Assert: $h = x^2 - xy + 9x^3 - 24x^2y + 16xy^2 = 0$

$$\begin{bmatrix} x \\ y \end{bmatrix} \leftarrow F(x, y) = \begin{bmatrix} 10x - 8y \\ 6x - 4y \end{bmatrix}$$

end while

Program verification →

h invariant for $(0, 1)$?

Could h be an invariant (in $\mathbb{Q}$ or $\mathbb{R}$)?

h invariant for any ($\mathbb{Q}$ or $\mathbb{R}$) initial value?

Testing polynomial invariant

Invariant test

$(\mathtt{x}, \mathtt{y}) \leftarrow (\boldsymbol{a}, \boldsymbol{b})$

while true do

Assert: $h = \mathtt{x}^2 - \mathtt{xy} + 9\mathtt{x}^3 - 24\mathtt{x}^2\mathtt{y} + 16\mathtt{xy}^2 = 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \end{bmatrix} \leftarrow \boldsymbol{F}(\mathtt{x}, \mathtt{y}) = \begin{bmatrix} 10\mathtt{x} - 8\mathtt{y} \\ 6\mathtt{x} - 4\mathtt{y} \end{bmatrix}$$

end while

Invariant set $S_{(\boldsymbol{F}, \boldsymbol{h})}$

h is invariant for $(\boldsymbol{a}, \boldsymbol{b}) \in \mathbb{C}^2$ if and only if

$$h = \boldsymbol{a}^2 - \boldsymbol{ab} + 9\boldsymbol{a}^3 - 24\boldsymbol{a}^2\boldsymbol{b} + 16\boldsymbol{ab}^2 = 0$$

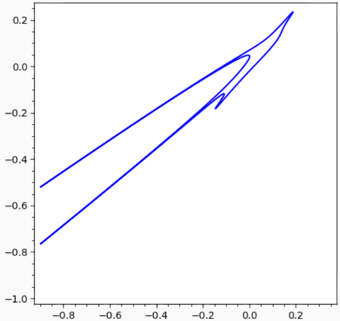
$$h \circ \boldsymbol{F} = 360\boldsymbol{a}^3 - 1248\boldsymbol{a}^2\boldsymbol{b} + 40\boldsymbol{a}^2 + 1408\boldsymbol{ab}^2 - 72\boldsymbol{ab} - 512\boldsymbol{b}^3 + 32\boldsymbol{b}^2 = 0$$

Program verification →

h invariant for $(0, 1)$?

Could h be an invariant (in $\mathbb{Q}$ or $\mathbb{R}$)?

h invariant for any ($\mathbb{Q}$ or $\mathbb{R}$) initial value?



Testing polynomial invariant

Invariant test

$(\mathtt{x}, \mathtt{y}) \leftarrow (\boldsymbol{a}, \boldsymbol{b})$

while true do

Assert: $h = \mathtt{x}^2 - \mathtt{xy} + 9\mathtt{x}^3 - 24\mathtt{x}^2\mathtt{y} + 16\mathtt{xy}^2 = 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \end{bmatrix} \leftarrow \boldsymbol{F}(\mathtt{x}, \mathtt{y}) = \begin{bmatrix} 10\mathtt{x} - 8\mathtt{y} \\ 6\mathtt{x} - 4\mathtt{y} \end{bmatrix}$$

end while

Invariant set $S_{(\boldsymbol{F}, \boldsymbol{h})}$

$\boldsymbol{h}$ is invariant for $(\boldsymbol{a}, \boldsymbol{b}) \in \mathbb{C}^2$ if and only if

$$\boldsymbol{h} = \boldsymbol{a}^2 - \boldsymbol{ab} + 9\boldsymbol{a}^3 - 24\boldsymbol{a}^2\boldsymbol{b} + 16\boldsymbol{ab}^2 = 0$$

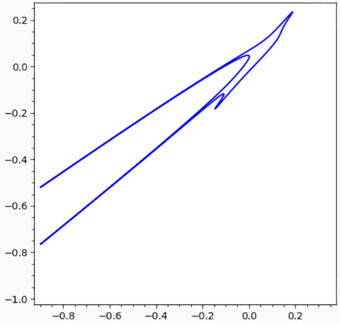
$$\boldsymbol{h} \circ \boldsymbol{F} = 360\boldsymbol{a}^3 - 1248\boldsymbol{a}^2\boldsymbol{b} + 40\boldsymbol{a}^2 + 1408\boldsymbol{ab}^2 - 72\boldsymbol{ab} - 512\boldsymbol{b}^3 + 32\boldsymbol{b}^2 = 0$$

Program verification → Algebraic geometry

$\boldsymbol{h}$ invariant for $(\mathbf{0}, \mathbf{1})$?

Could $\boldsymbol{h}$ be an invariant (in $\mathbb{Q}$ or $\mathbb{R}$)?

$\boldsymbol{h}$ invariant for any ($\mathbb{Q}$ or $\mathbb{R}$) initial value?



Testing polynomial invariant

Invariant test

$(\mathtt{x}, \mathtt{y}) \leftarrow (\boldsymbol{a}, \boldsymbol{b})$

while true do

Assert: $\boldsymbol{h} = \mathtt{x}^2 - \mathtt{xy} + 9\mathtt{x}^3 - 24\mathtt{x}^2\mathtt{y} + 16\mathtt{xy}^2 = 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \end{bmatrix} \leftarrow \boldsymbol{F}(\mathtt{x}, \mathtt{y}) = \begin{bmatrix} 10\mathtt{x} - 8\mathtt{y} \\ 6\mathtt{x} - 4\mathtt{y} \end{bmatrix}$$

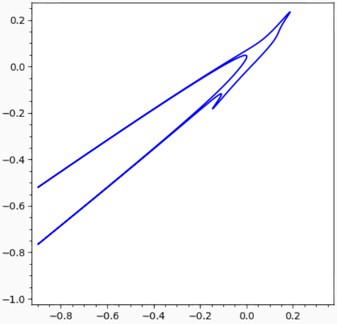
end while

Invariant set $S_{(\boldsymbol{F}, \boldsymbol{h})}$

$\boldsymbol{h}$ is invariant for $(\boldsymbol{a}, \boldsymbol{b}) \in \mathbb{C}^2$ if and only if

$$\boldsymbol{h} = \boldsymbol{a}^2 - \boldsymbol{ab} + 9\boldsymbol{a}^3 - 24\boldsymbol{a}^2\boldsymbol{b} + 16\boldsymbol{ab}^2 = 0$$

$$\boldsymbol{h} \circ \boldsymbol{F} = 360\boldsymbol{a}^3 - 1248\boldsymbol{a}^2\boldsymbol{b} + 40\boldsymbol{a}^2 + 1408\boldsymbol{ab}^2 - 72\boldsymbol{ab} - 512\boldsymbol{b}^3 + 32\boldsymbol{b}^2 = 0$$



Program verification → Algebraic geometry

$\boldsymbol{h}$ invariant for $(\mathbf{0}, \mathbf{1})$?

→ $\boldsymbol{h}(\mathbf{0}, \mathbf{1}) = \boldsymbol{h} \circ \boldsymbol{F}(\mathbf{0}, \mathbf{1}) = 0$?

→ No! $\boldsymbol{h}(\mathbf{0}, \mathbf{1}) = -480$.

Could $\boldsymbol{h}$ be an invariant (in $\mathbb{Q}$ or $\mathbb{R}$)?

$\boldsymbol{h}$ invariant for any ($\mathbb{Q}$ or $\mathbb{R}$) initial value?

Testing polynomial invariant

Invariant test

$(x, y) \leftarrow (a, b)$

while true do

Assert: $h = x^2 - xy + 9x^3 - 24x^2y + 16xy^2 = 0$

$$\begin{bmatrix} x \\ y \end{bmatrix} \leftarrow F(x, y) = \begin{bmatrix} 10x - 8y \\ 6x - 4y \end{bmatrix}$$

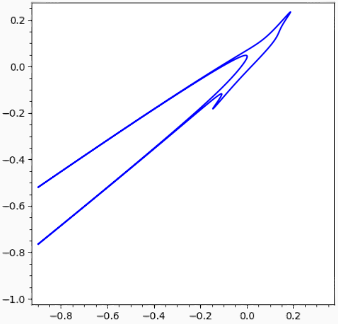
end while

Invariant set $S_{(F,h)}$

h is invariant for $(a, b) \in \mathbb{C}^2$ if and only if

$$h = a^2 - ab + 9a^3 - 24a^2b + 16ab^2 = 0$$

$$h \circ F = 360a^3 - 1248a^2b + 40a^2 + 1408ab^2 - 72ab - 512b^3 + 32b^2 = 0$$



Program verification → Algebraic geometry

h invariant for $(0, 1)$?

→ $h(0, 1) = h \circ F(0, 1) = 0$?

→ No! $h(0, 1) = -480$.

Could h be an invariant (in $\mathbb{Q}$ or $\mathbb{R}$)?

→ $S_{(F,h)} \cap \mathbb{Q}$ or $\mathbb{R} = \emptyset$?

→ Yes! Critical points: $(0, 0)$ and $(1/16, 5/64)$

h invariant for any ($\mathbb{Q}$ or $\mathbb{R}$) initial value?

Testing polynomial invariant

Invariant test

$(x, y) \leftarrow (a, b)$

while true do

Assert: $h = x^2 - xy + 9x^3 - 24x^2y + 16xy^2 = 0$

$$\begin{bmatrix} x \\ y \end{bmatrix} \leftarrow F(x, y) = \begin{bmatrix} 10x - 8y \\ 6x - 4y \end{bmatrix}$$

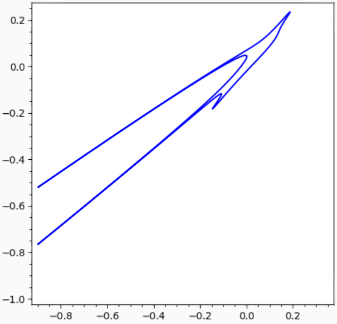
end while

Invariant set $S_{(F,h)}$

h is invariant for $(a, b) \in \mathbb{C}^2$ if and only if

$$h = a^2 - ab + 9a^3 - 24a^2b + 16ab^2 = 0$$

$$h \circ F = 360a^3 - 1248a^2b + 40a^2 + 1408ab^2 - 72ab - 512b^3 + 32b^2 = 0$$



Program verification → Algebraic geometry

h invariant for $(0, 1)$?
→ $h(0, 1) = h \circ F(0, 1) = 0$?
→ No! $h(0, 1) = -480$.

Could h be an invariant (in $\mathbb{Q}$ or $\mathbb{R}$)?
→ $S_{(F,h)} \cap \mathbb{Q}$ or $\mathbb{R} = \emptyset$?
→ Yes! Critical points: $(0, 0)$ and $(1/16, 5/64)$

h invariant for any ($\mathbb{Q}$ or $\mathbb{R}$) initial value?
→ $S_{(F,h)} = \mathbb{C}^2$?
→ No! $\langle h, h \circ F \rangle \neq \{0\}$

Generating polynomial invariant: any initial value

Invariant generation

$(\mathtt{x}, \mathtt{y}, \ ) \leftarrow (\boldsymbol{a}, \boldsymbol{b}, \ )$

while true **do**

Assert: $\boldsymbol{h} : \boldsymbol{\lambda_0} + \boldsymbol{\lambda_1}\mathtt{x} + \boldsymbol{\lambda_2}\mathtt{y} + \boldsymbol{\lambda_3}\mathtt{x}^2 + \boldsymbol{\lambda_4}\mathtt{xy} + \boldsymbol{\lambda_5}\mathtt{y}^2 = 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \end{bmatrix} \leftarrow \boldsymbol{F}(\mathtt{x}, \mathtt{y}) = \begin{bmatrix} 10\mathtt{x} - 8\mathtt{y} \\ 6\mathtt{x} - 4\mathtt{y} \end{bmatrix}$$

end while

Generating polynomial invariant: any initial value

Invariant generation

$(\mathtt{x}, \mathtt{y}, \mathtt{c}) \leftarrow (\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\lambda})$

while `true` **do**

Assert: $\boldsymbol{h}$: $\mathtt{c}_0 + \mathtt{c}_1\,\mathtt{x} + \mathtt{c}_2\,\boldsymbol{y} + \mathtt{c}_3\,\mathtt{x}^2 + \mathtt{c}_4\,\mathtt{xy} + \mathtt{c}_5\,\mathtt{y}^2 = 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{c} \end{bmatrix} \leftarrow \widetilde{\boldsymbol{F}}(\mathtt{x}, \mathtt{y}) = \begin{bmatrix} 10\mathtt{x} - 8\mathtt{y} \\ 6\mathtt{x} - 4\mathtt{y} \\ \mathtt{c} \end{bmatrix}$$

end while

Generating polynomial invariant: any initial value

Invariant generation

$(\mathtt{x}, \mathtt{y}, \mathtt{c}) \leftarrow (\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\lambda})$

while true do

Assert: $\boldsymbol{h} : \mathtt{c}_0 + \mathtt{c}_1\,\mathtt{x} + \mathtt{c}_2\,\boldsymbol{y} + \mathtt{c}_3\,\mathtt{x}^2 + \mathtt{c}_4\,\mathtt{xy} + \mathtt{c}_5\,\mathtt{y}^2 = 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{c} \end{bmatrix} \leftarrow \widetilde{\boldsymbol{F}}(\mathtt{x}, \mathtt{y}) = \begin{bmatrix} 10\mathtt{x} - 8\mathtt{y} \\ 6\mathtt{x} - 4\mathtt{y} \\ \mathtt{c} \end{bmatrix}$$

end while

Invariant generation → (Linear) Algebra

? Invariants for a given $(\boldsymbol{a}, \boldsymbol{b}) \in \mathbb{C}^2$?

? Invariants for generic $(\boldsymbol{a}, \boldsymbol{b}) \in \mathbb{C}^2$?

? Invariant for all $(\boldsymbol{a}, \boldsymbol{b}) \in \mathbb{C}^2$?

Generating polynomial invariant: any initial value

Invariant generation

$(\mathtt{x},\mathtt{y},\mathtt{c}) \leftarrow (\boldsymbol{a},\boldsymbol{b},\boldsymbol{\lambda})$

while true do

Assert: $h : \mathtt{c}_0 + \mathtt{c}_1\,\mathtt{x} + \mathtt{c}_2\,\boldsymbol{y} + \mathtt{c}_3\,\mathtt{x}^2 + \mathtt{c}_4\,\mathtt{xy} + \mathtt{c}_5\,\mathtt{y}^2 = 0$

$$\begin{bmatrix}\mathtt{x}\\ \mathtt{y}\\ \mathtt{c}\end{bmatrix} \leftarrow \widetilde{F}(\mathtt{x},\mathtt{y}) = \begin{bmatrix}10\mathtt{x}-8\mathtt{y}\\ 6\mathtt{x}-4\mathtt{y}\\ \mathtt{c}\end{bmatrix}$$

end while

Invariant generation → (Linear) Algebra

- ? Invariants for a given $(\boldsymbol{a},\boldsymbol{b}) \in \mathbb{C}^2$?
- ? Invariants for generic $(\boldsymbol{a},\boldsymbol{b}) \in \mathbb{C}^2$?
- ? Invariant for all $(\boldsymbol{a},\boldsymbol{b}) \in \mathbb{C}^2$?

Invariant set $S_{\widetilde{F},h}$ - Parametric Linear System

$$\begin{bmatrix} h \\ h\circ\widetilde{F} \\ h\circ\widetilde{F}^2 \\ h\circ\widetilde{F}^3 \\ h\circ\widetilde{F}^4 \end{bmatrix} = \begin{bmatrix} a^2 & ab & b^2 & a & b & 1 \\ (10a-8b)^2 & (10a-8b)(6a-4b) & (6a-4b)^2 & 10a-8b & 6a-4b & 1 \\ (52a-48b)^2 & (52a-48b)(36a-32b) & (36a-32b)^2 & 52a-48b & 36a-32b & 1 \\ (232a-224b)^2 & (232a-224b)(168a-160b) & (168a-160b)^2 & 232a-224b & 168a-160b & 1 \\ (976a-960b)^2 & (976a-960b)(720a-704b) & (720a-704b)^2 & 976a-960b & 720a-704b & 1 \end{bmatrix} \cdot \begin{bmatrix} \lambda_5 \\ \lambda_4 \\ \lambda_3 \\ \lambda_2 \\ \lambda_1 \\ \lambda_0 \end{bmatrix} = 0$$

Generating polynomial invariant: any initial value

Invariant generation

$(\mathtt{x}, \mathtt{y}, \mathtt{c}) \leftarrow (\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\lambda})$

while true do

Assert: $h : \mathtt{c}_0 + \mathtt{c}_1\,\mathtt{x} + \mathtt{c}_2\,\boldsymbol{y} + \mathtt{c}_3\,\mathtt{x}^2 + \mathtt{c}_4\,\mathtt{xy} + \mathtt{c}_5\,\mathtt{y}^2 = 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{c} \end{bmatrix} \leftarrow \widetilde{F}(\mathtt{x}, \mathtt{y}) = \begin{bmatrix} 10\mathtt{x} - 8\mathtt{y} \\ 6\mathtt{x} - 4\mathtt{y} \\ \mathtt{c} \end{bmatrix}$$

end while

Invariant generation → (Linear) Algebra

- ? Invariants for a given $(\boldsymbol{a}, \boldsymbol{b}) \in \mathbb{C}^2$?
  → Row Echelon Form
- ? Invariants for generic $(\boldsymbol{a}, \boldsymbol{b}) \in \mathbb{C}^2$?
- ? Invariant for all $(\boldsymbol{a}, \boldsymbol{b}) \in \mathbb{C}^2$?

Invariant set $S_{\widetilde{F},h}$ - Parametric Linear System

$$\begin{bmatrix} h \\ h \circ \widetilde{F} \\ h \circ \widetilde{F}^2 \\ h \circ \widetilde{F}^3 \\ h \circ \widetilde{F}^4 \end{bmatrix} = \begin{bmatrix} a^2 & ab & b^2 & a & b & 1 \\ (10a-8b)^2 & (10a-8b)(6a-4b) & (6a-4b)^2 & 10a-8b & 6a-4b & 1 \\ (52a-48b)^2 & (52a-48b)(36a-32b) & (36a-32b)^2 & 52a-48b & 36a-32b & 1 \\ (232a-224b)^2 & (232a-224b)(168a-160b) & (168a-160b)^2 & 232a-224b & 168a-160b & 1 \\ (976a-960b)^2 & (976a-960b)(720a-704b) & (720a-704b)^2 & 976a-960b & 720a-704b & 1 \end{bmatrix} \cdot \begin{bmatrix} \lambda_5 \\ \lambda_4 \\ \lambda_3 \\ \lambda_2 \\ \lambda_1 \\ \lambda_0 \end{bmatrix} = 0$$

Generating polynomial invariant: any initial value

Invariant generation

$(\mathtt{x}, \mathtt{y}, \mathtt{c}) \leftarrow (a, b, \lambda)$

while true do

Assert: $h : c_0 + c_1\,\mathtt{x} + c_2\,\boldsymbol{y} + c_3\,\mathtt{x}^2 + c_4\,\mathtt{xy} + c_5\,\mathtt{y}^2 = 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{c} \end{bmatrix} \leftarrow \widetilde{F}(\mathtt{x}, \mathtt{y}) = \begin{bmatrix} 10\mathtt{x} - 8\mathtt{y} \\ 6\mathtt{x} - 4\mathtt{y} \\ \mathtt{c} \end{bmatrix}$$

end while

Invariant generation → (Linear) Algebra

? Invariants for a given $(a, b) \in \mathbb{C}^2$?
→ Row Echelon Form

? Invariants for generic $(a, b) \in \mathbb{C}^2$?
→ Eval./Interpolation of Row Echelon Form

? Invariant for all $(a, b) \in \mathbb{C}^2$?

Invariant set $S_{\widetilde{F},h}$ - Parametric Linear System

$$\begin{bmatrix} h \\ h \circ \widetilde{F} \\ h \circ \widetilde{F}^2 \\ h \circ \widetilde{F}^3 \\ h \circ \widetilde{F}^4 \end{bmatrix} = \begin{bmatrix} a^2 & ab & b^2 & a & b & 1 \\ (10a-8b)^2 & (10a-8b)(6a-4b) & (6a-4b)^2 & 10a-8b & 6a-4b & 1 \\ (52a-48b)^2 & (52a-48b)(36a-32b) & (36a-32b)^2 & 52a-48b & 36a-32b & 1 \\ (232a-224b)^2 & (232a-224b)(168a-160b) & (168a-160b)^2 & 232a-224b & 168a-160b & 1 \\ (976a-960b)^2 & (976a-960b)(720a-704b) & (720a-704b)^2 & 976a-960b & 720a-704b & 1 \end{bmatrix} \cdot \begin{bmatrix} \lambda_5 \\ \lambda_4 \\ \lambda_3 \\ \lambda_2 \\ \lambda_1 \\ \lambda_0 \end{bmatrix} = 0$$

Generating polynomial invariant: any initial value

Invariant generation

$(\mathtt{x},\mathtt{y},\mathtt{c}) \leftarrow (\boldsymbol{a},\boldsymbol{b},\boldsymbol{\lambda})$

while true do

Assert: $h : \mathtt{c}_0 + \mathtt{c}_1\,\mathtt{x} + \mathtt{c}_2\,\boldsymbol{y} + \mathtt{c}_3\,\mathtt{x}^2 + \mathtt{c}_4\,\mathtt{xy} + \mathtt{c}_5\,\mathtt{y}^2 = 0$

$$\begin{bmatrix}\mathtt{x}\\ \mathtt{y}\\ \mathtt{c}\end{bmatrix} \leftarrow \widetilde{\boldsymbol{F}}(\mathtt{x},\mathtt{y}) = \begin{bmatrix}10\mathtt{x}-8\mathtt{y}\\ 6\mathtt{x}-4\mathtt{y}\\ \mathtt{c}\end{bmatrix}$$

end while

Invariant generation → (Linear) Algebra

? Invariants for a given $(\boldsymbol{a},\boldsymbol{b}) \in \mathbb{C}^2$?
→ Row Echelon Form

? Invariants for generic $(\boldsymbol{a},\boldsymbol{b}) \in \mathbb{C}^2$?
→ Eval./Interpolation of Row Echelon Form

? Invariant for all $(\boldsymbol{a},\boldsymbol{b}) \in \mathbb{C}^2$?
→ Minor based stratification of $\mathbb{C}^2$

Invariant set $S_{\widetilde{\boldsymbol{F}},h}$ - Parametric Linear System

$$\begin{bmatrix} h\\ h\circ\widetilde{\boldsymbol{F}}\\ h\circ\widetilde{\boldsymbol{F}}^2\\ h\circ\widetilde{\boldsymbol{F}}^3\\ h\circ\widetilde{\boldsymbol{F}}^4\end{bmatrix} = \begin{bmatrix} \boldsymbol{a}^2 & \boldsymbol{ab} & \boldsymbol{b}^2 & \boldsymbol{a} & \boldsymbol{b} & 1\\ (10\boldsymbol{a}-8\boldsymbol{b})^2 & (10\boldsymbol{a}-8\boldsymbol{b})(6\boldsymbol{a}-4\boldsymbol{b}) & (6\boldsymbol{a}-4\boldsymbol{b})^2 & 10\boldsymbol{a}-8\boldsymbol{b} & 6\boldsymbol{a}-4\boldsymbol{b} & 1\\ (52\boldsymbol{a}-48\boldsymbol{b})^2 & (52\boldsymbol{a}-48\boldsymbol{b})(36\boldsymbol{a}-32\boldsymbol{b}) & (36\boldsymbol{a}-32\boldsymbol{b})^2 & 52\boldsymbol{a}-48\boldsymbol{b} & 36\boldsymbol{a}-32\boldsymbol{b} & 1\\ (232\boldsymbol{a}-224\boldsymbol{b})^2 & (232\boldsymbol{a}-224\boldsymbol{b})(168\boldsymbol{a}-160\boldsymbol{b}) & (168\boldsymbol{a}-160\boldsymbol{b})^2 & 232\boldsymbol{a}-224\boldsymbol{b} & 168\boldsymbol{a}-160\boldsymbol{b} & 1\\ (976\boldsymbol{a}-960\boldsymbol{b})^2 & (976\boldsymbol{a}-960\boldsymbol{b})(720\boldsymbol{a}-704\boldsymbol{b}) & (720\boldsymbol{a}-704\boldsymbol{b})^2 & 976\boldsymbol{a}-960\boldsymbol{b} & 720\boldsymbol{a}-704\boldsymbol{b} & 1 \end{bmatrix} \cdot \begin{bmatrix}\lambda_5\\ \lambda_4\\ \lambda_3\\ \lambda_2\\ \lambda_1\\ \lambda_0\end{bmatrix} = 0$$

Generating polynomial invariant: any initial value

Invariant generation

$(\mathtt{x}, \mathtt{y}, \mathtt{c}) \leftarrow (a, b, \lambda)$

while true do

Assert: $h : c_0 + c_1 x + c_2 y + c_3 x^2 + c_4 xy + c_5 y^2 = 0$

$$\begin{bmatrix} x \\ y \\ c \end{bmatrix} \leftarrow \widetilde{F}(x,y) = \begin{bmatrix} 10x - 8y \\ 6x - 4y \\ c \end{bmatrix}$$

end while

Invariant generation → (Linear) Algebra

- Invariants for a given $(a, b) \in \mathbb{C}^2$?
  → Row Echelon Form
- Invariants for generic $(a, b) \in \mathbb{C}^2$?
  → Eval./Interpolation of Row Echelon Form
- Invariant for all $(a, b) \in \mathbb{C}^2$?
  → Minor based stratification of $\mathbb{C}^2$

Invariant set $S_{\widetilde{F},h}$ - Parametric Linear System

$$\begin{bmatrix} h \\ h \circ \widetilde{F} \\ h \circ \widetilde{F}^2 \\ h \circ \widetilde{F}^3 \\ h \circ \widetilde{F}^4 \end{bmatrix} = \begin{bmatrix} a^2 & ab & b^2 & a & b & 1 \\ (10a-8b)^2 & (10a-8b)(6a-4b) & (6a-4b)^2 & 10a-8b & 6a-4b & 1 \\ (52a-48b)^2 & (52a-48b)(36a-32b) & (36a-32b)^2 & 52a-48b & 36a-32b & 1 \\ (232a-224b)^2 & (232a-224b)(168a-160b) & (168a-160b)^2 & 232a-224b & 168a-160b & 1 \\ (976a-960b)^2 & (976a-960b)(720a-704b) & (720a-704b)^2 & 976a-960b & 720a-704b & 1 \end{bmatrix} \cdot \begin{bmatrix} \lambda_5 \\ \lambda_4 \\ \lambda_3 \\ \lambda_2 \\ \lambda_1 \\ \lambda_0 \end{bmatrix} = 0$$

Invariant stratification [Sit 1992]

Initial values' stratum	Basis of $I_{2,\mathcal{L}}$	Dim
$a = b = 0$	$\{x, y, xy, x^2, y^2\}$	5
$a - b = 0$	$\{x - y, x^2 - xy, -xy + y^2\}$	3
$3a - 4b = 0$	$\{3x - 4y, -3x^2 + 16xy - 16y^2, -3xy + 4y^2\}$	3
$(3a - 4b)(a - b) \neq 0$	$\{(3a-4b)^2 x - (3a-4b)^2 y - 9(a-b)x^2 + 24(a-b)xy - 16(a-b)y^2\}$	1

Generating polynomial invariant: Fixed initial values

Invariant generation

$(\mathtt{x}, \mathtt{y}, \mathtt{c}) \leftarrow (\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\lambda})$

while true **do**

Assert: $\boldsymbol{h} : \mathtt{c}_0 + \mathtt{c}_1\,\mathtt{x} + \mathtt{c}_2\,\boldsymbol{y} + \mathtt{c}_3\,\mathtt{x}^2 + \mathtt{c}_4\,\mathtt{xy} + \mathtt{c}_5\,\mathtt{y}^2 = 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{c} \end{bmatrix} \leftarrow \widetilde{\boldsymbol{F}}(\mathtt{x}, \mathtt{y}) = \begin{bmatrix} 10\mathtt{x} - 8\mathtt{y} \\ 6\mathtt{x} - 4\mathtt{y} \\ \mathtt{c} \end{bmatrix}$$

end while

Invariant generation $S_{\widetilde{\boldsymbol{F}}, \boldsymbol{h}}$ - Parametric Linear System

$$\begin{bmatrix} \boldsymbol{h} \\ \boldsymbol{h} \circ \widetilde{\boldsymbol{F}} \\ \boldsymbol{h} \circ \widetilde{\boldsymbol{F}}^2 \\ \boldsymbol{h} \circ \widetilde{\boldsymbol{F}}^3 \\ \boldsymbol{h} \circ \widetilde{\boldsymbol{F}}^4 \end{bmatrix} = \begin{bmatrix} \boldsymbol{a}^2 & \boldsymbol{a}\boldsymbol{b} & \boldsymbol{b}^2 & \boldsymbol{a} & \boldsymbol{b} & 1 \\ (10\boldsymbol{a} - 8\boldsymbol{b})^2 & (10\boldsymbol{a} - 8\boldsymbol{b})(6\boldsymbol{a} - 4\boldsymbol{b}) & (6\boldsymbol{a} - 4\boldsymbol{b})^2 & 10\boldsymbol{a} - 8\boldsymbol{b} & 6\boldsymbol{a} - 4\boldsymbol{b} & 1 \\ (52\boldsymbol{a} - 48\boldsymbol{b})^2 & (52\boldsymbol{a} - 48\boldsymbol{b})(36\boldsymbol{a} - 32\boldsymbol{b}) & (36\boldsymbol{a} - 32\boldsymbol{b})^2 & 52\boldsymbol{a} - 48\boldsymbol{b} & 36\boldsymbol{a} - 32\boldsymbol{b} & 1 \\ (232\boldsymbol{a} - 224\boldsymbol{b})^2 & (232\boldsymbol{a} - 224\boldsymbol{b})(168\boldsymbol{a} - 160\boldsymbol{b}) & (168\boldsymbol{a} - 160\boldsymbol{b})^2 & 232\boldsymbol{a} - 224\boldsymbol{b} & 168\boldsymbol{a} - 160\boldsymbol{b} & 1 \\ (976\boldsymbol{a} - 960\boldsymbol{b})^2 & (976\boldsymbol{a} - 960\boldsymbol{b})(720\boldsymbol{a} - 704\boldsymbol{b}) & (720\boldsymbol{a} - 704\boldsymbol{b})^2 & 976\boldsymbol{a} - 960\boldsymbol{b} & 720\boldsymbol{a} - 704\boldsymbol{b} & 1 \end{bmatrix} \cdot \begin{bmatrix} \boldsymbol{\lambda}_5 \\ \boldsymbol{\lambda}_4 \\ \boldsymbol{\lambda}_3 \\ \boldsymbol{\lambda}_2 \\ \boldsymbol{\lambda}_1 \\ \boldsymbol{\lambda}_0 \end{bmatrix} = 0$$

Generating polynomial invariant: Fixed initial values

Invariant generation

$(\mathtt{x}, \mathtt{y}, \mathtt{c}) \leftarrow (\mathbf{4}, \mathbf{3}, \lambda)$

while true **do**

Assert: $h : \mathtt{c}_0 + \mathtt{c}_1\,\mathtt{x} + \mathtt{c}_2\,\boldsymbol{y} + \mathtt{c}_3\,\mathtt{x}^2 + \mathtt{c}_4\,\mathtt{xy} + \mathtt{c}_5\,\mathtt{y}^2 = 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{c} \end{bmatrix} \leftarrow \widetilde{F}(\mathtt{x}, \mathtt{y}) = \begin{bmatrix} 10\mathtt{x} - 8\mathtt{y} \\ 6\mathtt{x} - 4\mathtt{y} \\ \mathtt{c} \end{bmatrix}$$

end while

Invariant vector space $\mathcal{I}_{\leq 2}((\mathbf{4}, \mathbf{3}), \boldsymbol{F})$ - Linear System

$$\begin{bmatrix} h \\ h \circ \widetilde{F} \\ h \circ \widetilde{F}^2 \\ h \circ \widetilde{F}^3 \\ h \circ \widetilde{F}^4 \end{bmatrix} = \begin{bmatrix} 9 & 12 & 1 & 3 & 4 & 1 \\ 144 & 192 & 1 & 3 \cdot 2^2 & 4 \cdot 2^2 & 1 \\ 2304 & 3072 & 1 & 3 \cdot 2^4 & 4 \cdot 2^4 & 1 \\ 36864 & 49152 & 1 & 3 \cdot 2^6 & 4 \cdot 2^6 & 1 \\ 589824 & 786432 & 1 & 3 \cdot 2^8 & 4 \cdot 2^8 & 1 \end{bmatrix} \cdot \begin{bmatrix} \lambda_5 \\ \lambda_4 \\ \lambda_3 \\ \lambda_2 \\ \lambda_1 \\ \lambda_0 \end{bmatrix} = 0$$

Generating polynomial invariant: Fixed initial values

Invariant generation

$(\mathtt{x}, \mathtt{y}, \mathtt{c}) \leftarrow (\mathbf{4}, \mathbf{3}, \lambda)$

while true do

Assert: $h : \mathtt{c}_0 + \mathtt{c}_1\mathtt{x} + \mathtt{c}_2\boldsymbol{y} + \mathtt{c}_3\mathtt{x}^2 + \mathtt{c}_4\mathtt{xy} + \mathtt{c}_5\mathtt{y}^2 = 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{c} \end{bmatrix} \leftarrow \widetilde{F}(\mathtt{x}, \mathtt{y}) = \begin{bmatrix} 10\mathtt{x} - 8\mathtt{y} \\ 6\mathtt{x} - 4\mathtt{y} \\ \mathtt{c} \end{bmatrix}$$

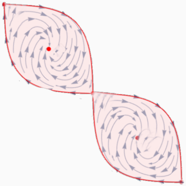
end while

Invariant vector space $\mathcal{I}_{\leq 2}((\mathbf{4}, \mathbf{3}), \boldsymbol{F})$ - Linear System

$$\begin{bmatrix} h \\ h \circ \widetilde{F} \\ h \circ \widetilde{F}^2 \\ h \circ \widetilde{F}^3 \\ h \circ \widetilde{F}^4 \end{bmatrix} = \begin{bmatrix} 9 & 12 & 1 & 3 & 4 & 1 \\ 144 & 192 & 1 & 3 \cdot 2^2 & 4 \cdot 2^2 & 1 \\ 2304 & 3072 & 1 & 3 \cdot 2^4 & 4 \cdot 2^4 & 1 \\ 36864 & 49152 & 1 & 3 \cdot 2^6 & 4 \cdot 2^6 & 1 \\ 589824 & 786432 & 1 & 3 \cdot 2^8 & 4 \cdot 2^8 & 1 \end{bmatrix} \cdot \begin{bmatrix} \lambda_5 \\ \lambda_4 \\ \lambda_3 \\ \lambda_2 \\ \lambda_1 \\ \lambda_0 \end{bmatrix} = 0$$

An observation

$$\mathcal{I}_{\leq 2}((\mathbf{4}, \mathbf{3}), \boldsymbol{F}) = \left\{ h \circ \widetilde{F}^0(\mathbf{4}, \mathbf{3}) = 0, \ldots, h \circ \widetilde{F}^{(?)}(\mathbf{4}, \mathbf{3}) = 0 \right\}$$



Generating polynomial invariant: Fixed initial values

Invariant generation

$(x, y, c) \leftarrow (\mathbf{4}, \mathbf{3}, \lambda)$

while true do

Assert: h : $c_0 + c_1 x + c_2 y + c_3 x^2 + c_4 xy + c_5 y^2 = 0$

$$\begin{bmatrix} x \\ y \\ c \end{bmatrix} \leftarrow \widetilde{F}(x, y) = \begin{bmatrix} 10x - 8y \\ 6x - 4y \\ c \end{bmatrix}$$

end while

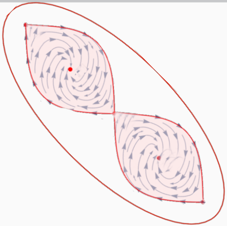
Invariant vector space $\mathcal{I}_{\leq 2}((\mathbf{4}, \mathbf{3}), F)$ - Linear System

$$\begin{bmatrix} h \\ h \circ \widetilde{F} \\ h \circ \widetilde{F}^2 \\ h \circ \widetilde{F}^3 \\ h \circ \widetilde{F}^4 \end{bmatrix} = \begin{bmatrix} 9 & 12 & 1 & 3 & 4 & 1 \\ 144 & 192 & 1 & 3 \cdot 2^2 & 4 \cdot 2^2 & 1 \\ 2304 & 3072 & 1 & 3 \cdot 2^4 & 4 \cdot 2^4 & 1 \\ 36864 & 49152 & 1 & 3 \cdot 2^6 & 4 \cdot 2^6 & 1 \\ 589824 & 786432 & 1 & 3 \cdot 2^8 & 4 \cdot 2^8 & 1 \end{bmatrix} \cdot \begin{bmatrix} \lambda_5 \\ \lambda_4 \\ \lambda_3 \\ \lambda_2 \\ \lambda_1 \\ \lambda_0 \end{bmatrix} = 0$$

An observation

$$\mathcal{I}_{\leq 2}((\mathbf{4}, \mathbf{3}), F) \subseteq \left\{ h \circ \widetilde{F}^0(\mathbf{4}, \mathbf{3}) = 0, \ldots, h \circ \widetilde{F}^{(k)}(\mathbf{4}, \mathbf{3}) = 0 \right\}$$

$$\mathcal{I}_{\leq 2}((\mathbf{4}, \mathbf{3}), F) =$$



Generating polynomial invariant: Fixed initial values

Invariant generation

$(\mathtt{x}, \mathtt{y}, \mathtt{c}) \leftarrow (4, 3, \lambda)$

while true do

Assert: $h : \mathtt{c}_0 + \mathtt{c}_1\,\mathtt{x} + \mathtt{c}_2\,\boldsymbol{y} + \mathtt{c}_3\,\mathtt{x}^2 + \mathtt{c}_4\,\mathtt{xy} + \mathtt{c}_5\,\mathtt{y}^2 = 0$

$$\begin{bmatrix}\mathtt{x}\\ \mathtt{y}\\ \mathtt{c}\end{bmatrix} \leftarrow \widetilde{F}(\mathtt{x},\mathtt{y}) = \begin{bmatrix}10\mathtt{x}-8\mathtt{y}\\ 6\mathtt{x}-4\mathtt{y}\\ \mathtt{c}\end{bmatrix}$$

end while

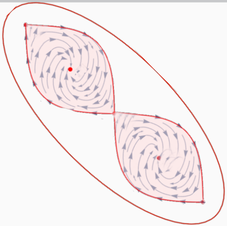
Invariant vector space $\mathcal{I}_{\leq 2}((4, 3), F)$ - Linear System

$$\begin{bmatrix} h \\ h\circ\widetilde{F} \\ h\circ\widetilde{F}^2 \\ h\circ\widetilde{F}^3 \\ h\circ\widetilde{F}^4 \end{bmatrix} = \begin{bmatrix} 9 & 12 & 1 & 3 & 4 & 1 \\ 144 & 192 & 1 & 3\cdot 2^2 & 4\cdot 2^2 & 1 \\ 2304 & 3072 & 1 & 3\cdot 2^4 & 4\cdot 2^4 & 1 \\ 36864 & 49152 & 1 & 3\cdot 2^6 & 4\cdot 2^6 & 1 \\ 589824 & 786432 & 1 & 3\cdot 2^8 & 4\cdot 2^8 & 1 \end{bmatrix} \cdot \begin{bmatrix} \lambda_5 \\ \lambda_4 \\ \lambda_3 \\ \lambda_2 \\ \lambda_1 \\ \lambda_0 \end{bmatrix} = 0$$

An observation

$$\mathcal{I}_{\leq 2}((4,3), F) \subseteq \left\{ h\circ\widetilde{F}^0(4,3) = 0, \ldots, h\circ\widetilde{F}^{(k)}(4,3) = 0 \right\} = \mathbb{C}h_0 + \mathbb{C}h_1 + \mathbb{C}g_0 + \mathbb{C}g_1$$

$$\mathcal{I}_{\leq 2}((4,3), F) =$$



Generating polynomial invariant: Fixed initial values

Invariant generation

$(\mathtt{x}, \mathtt{y}, \mathtt{c}) \leftarrow (\mathbf{4}, \mathbf{3}, \lambda)$

while true do

Assert: $h : \mathtt{c}_0 + \mathtt{c}_1\,\mathtt{x} + \mathtt{c}_2\,\boldsymbol{y} + \mathtt{c}_3\,\mathtt{x}^2 + \mathtt{c}_4\,\mathtt{xy} + \mathtt{c}_5\,\mathtt{y}^2 = 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{c} \end{bmatrix} \leftarrow \widetilde{F}(\mathtt{x}, \mathtt{y}) = \begin{bmatrix} 10\mathtt{x} - 8\mathtt{y} \\ 6\mathtt{x} - 4\mathtt{y} \\ \mathtt{c} \end{bmatrix}$$

end while

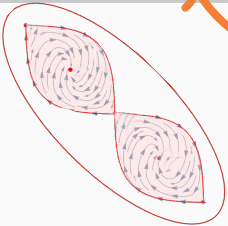
Invariant vector space $\mathcal{I}_{\leq 2}((\mathbf{4}, \mathbf{3}), \boldsymbol{F})$ - Linear System

$$\begin{bmatrix} h \\ h \circ \widetilde{F} \\ h \circ \widetilde{F}^2 \\ h \circ \widetilde{F}^3 \\ h \circ \widetilde{F}^4 \end{bmatrix} = \begin{bmatrix} 9 & 12 & 1 & 3 & 4 & 1 \\ 144 & 192 & 1 & 3 \cdot 2^2 & 4 \cdot 2^2 & 1 \\ 2304 & 3072 & 1 & 3 \cdot 2^4 & 4 \cdot 2^4 & 1 \\ 36864 & 49152 & 1 & 3 \cdot 2^6 & 4 \cdot 2^6 & 1 \\ 589824 & 786432 & 1 & 3 \cdot 2^8 & 4 \cdot 2^8 & 1 \end{bmatrix} \cdot \begin{bmatrix} \lambda_5 \\ \lambda_4 \\ \lambda_3 \\ \lambda_2 \\ \lambda_1 \\ \lambda_0 \end{bmatrix} = 0$$

An observation

$$\mathcal{I}_{\leq 2}((\mathbf{4}, \mathbf{3}), \boldsymbol{F}) \subseteq \left\{ h \circ \widetilde{F}^0(\mathbf{4}, \mathbf{3}) = 0, \ldots, h \circ \widetilde{F}^{(k)}(\mathbf{4}, \mathbf{3}) = 0 \right\} = \mathbb{C}h_0 + \mathbb{C}h_1 + \mathbb{C}g_0 + \mathbb{C}g_1$$

$$\mathcal{I}_{\leq 2}((\mathbf{4}, \mathbf{3}), \boldsymbol{F}) = \mathbb{C}h_0 + \mathbb{C}h_1 +$$



Generating polynomial invariant: Fixed initial values

Invariant generation

$(x, y, c) \leftarrow (4, 3, \lambda)$

while true do

Assert: $h : c_0 + c_1 x + c_2 y + c_3 x^2 + c_4 xy + c_5 y^2 = 0$

$$\begin{bmatrix} x \\ y \\ c \end{bmatrix} \leftarrow \widetilde{F}(x, y) = \begin{bmatrix} 10x - 8y \\ 6x - 4y \\ c \end{bmatrix}$$

end while

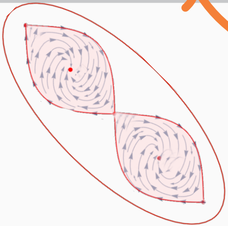
Invariant vector space $\mathcal{I}_{\leq 2}((4, 3), F)$ - Linear System

$$\begin{bmatrix} h \\ h \circ \widetilde{F} \\ h \circ \widetilde{F}^2 \\ h \circ \widetilde{F}^3 \\ h \circ \widetilde{F}^4 \end{bmatrix} = \begin{bmatrix} 9 & 12 & 1 & 3 & 4 & 1 \\ 144 & 192 & 1 & 3 \cdot 2^2 & 4 \cdot 2^2 & 1 \\ 2304 & 3072 & 1 & 3 \cdot 2^4 & 4 \cdot 2^4 & 1 \\ 36864 & 49152 & 1 & 3 \cdot 2^6 & 4 \cdot 2^6 & 1 \\ 589824 & 786432 & 1 & 3 \cdot 2^8 & 4 \cdot 2^8 & 1 \end{bmatrix} \cdot \begin{bmatrix} \lambda_5 \\ \lambda_4 \\ \lambda_3 \\ \lambda_2 \\ \lambda_1 \\ \lambda_0 \end{bmatrix} = 0$$

An observation

$$\mathcal{I}_{\leq 2}((4, 3), F) \subseteq \left\{ h \circ \widetilde{F}^0(4, 3) = 0, \ldots, h \circ \widetilde{F}^{(k)}(4, 3) = 0 \right\} = \mathbb{C}h_0 + \mathbb{C}h_1 + \mathbb{C}g_0 + \mathbb{C}g_1$$

$$\mathcal{I}_{\leq 2}((4, 3), F) = \mathbb{C}h_0 + \mathbb{C}h_1 +$$



Invariant test (fast & parallel)

$(x, y) \leftarrow (4, 3)$

while true do

Assert: $h_1 = 0 \wedge h_2 = 0$

$$\begin{bmatrix} x \\ y \end{bmatrix} \leftarrow F(x, y) = \begin{bmatrix} 10x - 8y \\ 6x - 4y \end{bmatrix}$$

end while

Generating polynomial invariant: Fixed initial values

Invariant generation

$(x, y, c) \leftarrow (4, 3, \lambda)$

while true do

Assert: h : $c_0 + c_1 x + c_2 y + c_3 x^2 + c_4 xy + c_5 y^2 = 0$

$$\begin{bmatrix} x \\ y \\ c \end{bmatrix} \leftarrow \widetilde{F}(x, y) = \begin{bmatrix} 10x - 8y \\ 6x - 4y \\ c \end{bmatrix}$$

end while

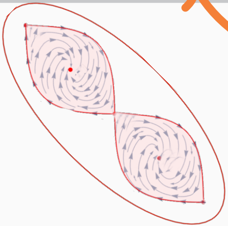
Invariant vector space $\mathcal{I}_{\leq 2}((4, 3), F)$ - Linear System

$$\begin{bmatrix} h \\ h \circ \widetilde{F} \\ h \circ \widetilde{F}^2 \\ h \circ \widetilde{F}^3 \\ h \circ \widetilde{F}^4 \end{bmatrix} = \begin{bmatrix} 9 & 12 & 1 & 3 & 4 & 1 \\ 144 & 192 & 1 & 3 \cdot 2^2 & 4 \cdot 2^2 & 1 \\ 2304 & 3072 & 1 & 3 \cdot 2^4 & 4 \cdot 2^4 & 1 \\ 36864 & 49152 & 1 & 3 \cdot 2^6 & 4 \cdot 2^6 & 1 \\ 589824 & 786432 & 1 & 3 \cdot 2^8 & 4 \cdot 2^8 & 1 \end{bmatrix} \cdot \begin{bmatrix} \lambda_5 \\ \lambda_4 \\ \lambda_3 \\ \lambda_2 \\ \lambda_1 \\ \lambda_0 \end{bmatrix} = 0$$

An observation

$$\mathcal{I}_{\leq 2}((4, 3), F) \subseteq \left\{ h \circ \widetilde{F}^0(4, 3) = 0, \ldots, h \circ \widetilde{F}^{(k)}(4, 3) = 0 \right\} = \mathbb{C}h_0 + \mathbb{C}h_1 + \mathbb{C}g_0 + \mathbb{C}g_1$$

$$\mathcal{I}_{\leq 2}((4, 3), F) = \mathbb{C}h_0 + \mathbb{C}h_1 + (\mathbb{C}g_0 + \mathbb{C}g_1) \cap \mathcal{I}_{\leq 2}((4, 3), F)$$



Invariant test (fast & parallel)

$(x, y) \leftarrow (4, 3)$

while true do

Assert: $h_1 = 0 \wedge h_2 = 0$

$$\begin{bmatrix} x \\ y \end{bmatrix} \leftarrow F(x, y) = \begin{bmatrix} 10x - 8y \\ 6x - 4y \end{bmatrix}$$

end while

Generating polynomial invariant: Fixed initial values

Invariant generation

$(\mathtt{x}, \mathtt{y}, \mathtt{c}) \leftarrow (4, 3, \lambda)$

while true do

Assert: $h : \mathtt{c}_0 + \mathtt{c}_1 \mathtt{x} + \mathtt{c}_2 \boldsymbol{y} + \mathtt{c}_3 \mathtt{x}^2 + \mathtt{c}_4 \mathtt{xy} + \mathtt{c}_5 \mathtt{y}^2 = 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{c} \end{bmatrix} \leftarrow \widetilde{F}(\mathtt{x}, \mathtt{y}) = \begin{bmatrix} 10\mathtt{x} - 8\mathtt{y} \\ 6\mathtt{x} - 4\mathtt{y} \\ \mathtt{c} \end{bmatrix}$$

end while

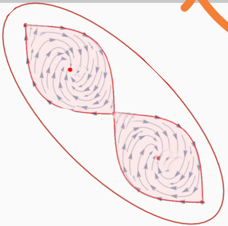
Invariant vector space $\mathcal{I}_{\leq 2}((4, 3), F)$ - Linear System

$$\begin{bmatrix} h \\ h \circ \widetilde{F} \\ h \circ \widetilde{F}^2 \\ h \circ \widetilde{F}^3 \\ h \circ \widetilde{F}^4 \end{bmatrix} = \begin{bmatrix} 9 & 12 & 1 & 3 & 4 & 1 \\ 144 & 192 & 1 & 3 \cdot 2^2 & 4 \cdot 2^2 & 1 \\ 2304 & 3072 & 1 & 3 \cdot 2^4 & 4 \cdot 2^4 & 1 \\ 36864 & 49152 & 1 & 3 \cdot 2^6 & 4 \cdot 2^6 & 1 \\ 589824 & 786432 & 1 & 3 \cdot 2^8 & 4 \cdot 2^8 & 1 \end{bmatrix} \cdot \begin{bmatrix} \lambda_5 \\ \lambda_4 \\ \lambda_3 \\ \lambda_2 \\ \lambda_1 \\ \lambda_0 \end{bmatrix} = 0$$

An observation

$$\mathcal{I}_{\leq 2}((4, 3), F) \subseteq \left\{ h \circ \widetilde{F}^0(4, 3) = 0, \ldots, h \circ \widetilde{F}^{(k)}(4, 3) = 0 \right\} = \mathbb{C}h_0 + \mathbb{C}h_1 + \mathbb{C}g_0 + \mathbb{C}g_1$$

$$\mathcal{I}_{\leq 2}((4, 3), F) = \mathbb{C}h_0 + \mathbb{C}h_1 + (\mathbb{C}g_0 + \mathbb{C}g_1) \cap \mathcal{I}_{\leq 2}((4, 3), F)$$



Invariant test (fast & parallel)

$(\mathtt{x}, \mathtt{y}) \leftarrow (4, 3)$

while true do

Assert: $h_1 = 0 \wedge h_2 = 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \end{bmatrix} \leftarrow F(\mathtt{x}, \mathtt{y}) = \begin{bmatrix} 10\mathtt{x} - 8\mathtt{y} \\ 6\mathtt{x} - 4\mathtt{y} \end{bmatrix}$$

end while

Invariant generation (reduced)

$(\mathtt{x}, \mathtt{y}, \mathtt{c}) \leftarrow (4, 3, \lambda)$

while true do

Assert: $\mathtt{c}_0 g_0 + \mathtt{c}_1 g_1 = 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{c} \end{bmatrix} \leftarrow \widetilde{F}(\mathtt{x}, \mathtt{y}) = \begin{bmatrix} 10\mathtt{x} - 8\mathtt{y} \\ 6\mathtt{x} - 4\mathtt{y} \\ \mathtt{c} \end{bmatrix}$$

end while

Synthesizing polynomial loops

Loop synthesis

$(\mathtt{x}, \mathtt{y}, \mathtt{z}, \quad) \leftarrow (\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \quad)$

while true **do**

Assert: $\left[\boldsymbol{h_1} : \mathtt{y}^2 - \mathtt{x} = 0 \wedge \boldsymbol{h_2} : \mathtt{z}^3 + 2\mathtt{y} - \mathtt{x} = 0\right]$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \end{bmatrix} \leftarrow \boldsymbol{F}(\mathtt{x}, \mathtt{y}, \mathtt{z}) = \begin{bmatrix} \boldsymbol{f_1}\mathtt{x}^3 + \boldsymbol{f_2}\mathtt{y}^2 \\ \boldsymbol{f_3}\mathtt{x} - \boldsymbol{f_4}\mathtt{y}^2 \\ \boldsymbol{f_5}\mathtt{x} \end{bmatrix}$$

end while

Synthesizing polynomial loops

Loop synthesis

$(\mathtt{x}, \mathtt{y}, \mathtt{z}, \mathtt{c}) \leftarrow (\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{f})$

while true **do**

Assert: $\left[\boldsymbol{h_1} : \mathtt{y}^2 - \mathtt{x} = 0 \wedge \boldsymbol{h_2} : \mathtt{z}^3 + 2\mathtt{y} - \mathtt{x} = 0\right]$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{c} \end{bmatrix} \leftarrow \widetilde{\boldsymbol{F}}(\mathtt{x}, \mathtt{y}, \mathtt{z}) = \begin{bmatrix} \mathtt{c}_1 \mathtt{x}^3 + \mathtt{c}_2 \mathtt{y}^2 \\ \mathtt{c}_3 \mathtt{x} - \mathtt{c}_4 \mathtt{y}^2 \\ \mathtt{c}_5 \mathtt{x} \\ \mathtt{c} \end{bmatrix}$$

end while

Synthesizing polynomial loops

Loop synthesis

$(\mathtt{x},\mathtt{y},\mathtt{z},\mathtt{c}) \leftarrow (\boldsymbol{a},\boldsymbol{b},\boldsymbol{c},\boldsymbol{f})$

while true do

Assert: $\left[\boldsymbol{h_1} : \mathtt{y}^2 - \mathtt{x} = 0 \wedge \boldsymbol{h_2} : \mathtt{z}^3 + 2\mathtt{y} - \mathtt{x} = 0\right]$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{c} \end{bmatrix} \leftarrow \widetilde{\boldsymbol{F}}(\mathtt{x},\mathtt{y},\mathtt{z}) = \begin{bmatrix} \mathtt{c}_1\mathtt{x}^3 + \mathtt{c}_2\mathtt{y}^2 \\ \mathtt{c}_3\mathtt{x} - \mathtt{c}_4\mathtt{y}^2 \\ \mathtt{c}_5\mathtt{x} \\ \mathtt{c} \end{bmatrix}$$

end while

Invariant set $S_{(\boldsymbol{F},\boldsymbol{h})}$

$\boldsymbol{h}$ is invariant for $(\boldsymbol{a},\boldsymbol{b},\boldsymbol{c},\boldsymbol{f}) \in \mathbb{C}^4$ if and only if

$$\boldsymbol{h_1} = \boldsymbol{b}^4\boldsymbol{f_4}^2 - 2\boldsymbol{a}\boldsymbol{b}^2\boldsymbol{f_3}\boldsymbol{f_4} - \boldsymbol{a}^3\boldsymbol{f_1} + \boldsymbol{a}^2\boldsymbol{f_3}^2 + \boldsymbol{b}^2\boldsymbol{f_2}$$

$$\boldsymbol{h_2} = \boldsymbol{a}^3\boldsymbol{f_5}^3 - \boldsymbol{a}^3\boldsymbol{f_1} + \boldsymbol{b}^2\boldsymbol{f_2} - 2\boldsymbol{b}^2\boldsymbol{f_4} + 2\boldsymbol{a}\boldsymbol{f_3}$$

$$(\boldsymbol{h_1},\boldsymbol{h_2}) \circ \widetilde{\boldsymbol{F}} = 0 \qquad (\boldsymbol{h_1},\boldsymbol{h_2}) \circ \widetilde{\boldsymbol{F}}^2 = 0$$

Synthesizing polynomial loops

Loop synthesis

$(\mathtt{x}, \mathtt{y}, \mathtt{z}, \mathtt{c}) \leftarrow (\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{f})$

while true **do**

Assert: $[\boldsymbol{h_1} : \mathtt{y}^2 - \mathtt{x} = 0 \wedge \boldsymbol{h_2} : \mathtt{z}^3 + 2\mathtt{y} - \mathtt{x} = 0]$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{c} \end{bmatrix} \leftarrow \widetilde{\boldsymbol{F}}(\mathtt{x}, \mathtt{y}, \mathtt{z}) = \begin{bmatrix} \mathtt{c}_1 \mathtt{x}^3 + \mathtt{c}_2 \mathtt{y}^2 \\ \mathtt{c}_3 \mathtt{x} - \mathtt{c}_4 \mathtt{y}^2 \\ \mathtt{c}_5 \mathtt{x} \\ \mathtt{c} \end{bmatrix}$$

end while

Invariant set $S_{(\boldsymbol{F}, \boldsymbol{h})}$

$\boldsymbol{h}$ is invariant for $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{f}) \in \mathbb{C}^4$ if and only if

$$\boldsymbol{h_1} = \boldsymbol{b}^4 \boldsymbol{f_4}^2 - 2\boldsymbol{a}\boldsymbol{b}^2 \boldsymbol{f_3}\boldsymbol{f_4} - \boldsymbol{a}^3 \boldsymbol{f_1} + \boldsymbol{a}^2 \boldsymbol{f_3}^2 + \boldsymbol{b}^2 \boldsymbol{f_2}$$

$$\boldsymbol{h_2} = \boldsymbol{a}^3 \boldsymbol{f_5}^3 - \boldsymbol{a}^3 \boldsymbol{f_1} + \boldsymbol{b}^2 \boldsymbol{f_2} - 2\boldsymbol{b}^2 \boldsymbol{f_4} + 2\boldsymbol{a} \boldsymbol{f_3}$$

$$(\boldsymbol{h_1}, \boldsymbol{h_2}) \circ \widetilde{\boldsymbol{F}} = 0 \qquad (\boldsymbol{h_1}, \boldsymbol{h_2}) \circ \widetilde{\boldsymbol{F}}^2 = 0$$

Final step

Find solutions to a polynomial sys. with entries:

- in $\mathbb{Z} \rightsquigarrow$ undecidable (Hilbert's 10th pb.)
- in $\mathbb{Q} \rightsquigarrow$ major open problem

Synthesizing polynomial loops

Loop synthesis

$(\mathtt{x},\mathtt{y},\mathtt{z},\mathtt{c}) \leftarrow (\boldsymbol{a},\boldsymbol{b},\boldsymbol{c},\boldsymbol{f})$

while true do

Assert: $[h_1 : \mathtt{y}^2 - \mathtt{x} = 0 \wedge h_2 : \mathtt{z}^3 + 2\mathtt{y} - \mathtt{x} = 0]$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{c} \end{bmatrix} \leftarrow \widetilde{F}(\mathtt{x},\mathtt{y},\mathtt{z}) = \begin{bmatrix} \mathtt{c}_1\mathtt{x}^3 + \mathtt{c}_2\mathtt{y}^2 \\ \mathtt{c}_3\mathtt{x} - \mathtt{c}_4\mathtt{y}^2 \\ \mathtt{c}_5\mathtt{x} \\ \mathtt{c} \end{bmatrix}$$

end while

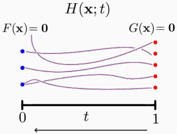
Finitely many sols

Numerical guesses

⇝ HomotopyContinuation.jl

⇝ Continued frac. exp.

⇝ Truncation



Symbolic methods

⇝ AlgebraicSolving.jl

⇝ factor in $\mathbb{Q}[t]$

$$\begin{cases} \omega(\boldsymbol{f_1}) = 0 & \omega \in \mathbb{Q}[t] \\ \boldsymbol{f_i} = \dfrac{\mu_i(\boldsymbol{f_1})}{\omega'(\boldsymbol{f_1})} & \mu_i \in \mathbb{Q}[t] \end{cases}$$

Invariant set $S_{(\boldsymbol{F},\boldsymbol{h})}$

$\boldsymbol{h}$ is invariant for $(\boldsymbol{a},\boldsymbol{b},\boldsymbol{c},\boldsymbol{f}) \in \mathbb{C}^4$ if and only if

$$\boldsymbol{h_1} = \boldsymbol{b}^4\boldsymbol{f_4}^2 - 2\boldsymbol{a}\boldsymbol{b}^2\boldsymbol{f_3}\boldsymbol{f_4} - \boldsymbol{a}^3\boldsymbol{f_1} + \boldsymbol{a}^2\boldsymbol{f_3}^2 + \boldsymbol{b}^2\boldsymbol{f_2}$$

$$\boldsymbol{h_2} = \boldsymbol{a}^3\boldsymbol{f_5}^3 - \boldsymbol{a}^3\boldsymbol{f_1} + \boldsymbol{b}^2\boldsymbol{f_2} - 2\boldsymbol{b}^2\boldsymbol{f_4} + 2\boldsymbol{a}\boldsymbol{f_3}$$

$$(\boldsymbol{h_1},\boldsymbol{h_2}) \circ \widetilde{\boldsymbol{F}} = 0 \qquad (\boldsymbol{h_1},\boldsymbol{h_2}) \circ \widetilde{\boldsymbol{F}}^2 = 0$$

Final step

Find solutions to a polynomial sys. with entries:

- in $\mathbb{Z}$ ⇝ undecidable (Hilbert's 10th pb.)
- in $\mathbb{Q}$ ⇝ major open problem

Synthesizing polynomial loops

Loop synthesis

$(\mathtt{x}, \mathtt{y}, \mathtt{z}, \mathtt{c}) \leftarrow (\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{f})$

while true do

Assert: $[\boldsymbol{h_1} : \mathtt{y}^2 - \mathtt{x} = 0 \wedge \boldsymbol{h_2} : \mathtt{z}^3 + 2\mathtt{y} - \mathtt{x} = 0]$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{c} \end{bmatrix} \leftarrow \widetilde{\boldsymbol{F}}(\mathtt{x}, \mathtt{y}, \mathtt{z}) = \begin{bmatrix} \mathtt{c}_1 \mathtt{x}^3 + \mathtt{c}_2 \mathtt{y}^2 \\ \mathtt{c}_3 \mathtt{x} - \mathtt{c}_4 \mathtt{y}^2 \\ \mathtt{c}_5 \mathtt{x} \\ \mathtt{c} \end{bmatrix}$$

end while

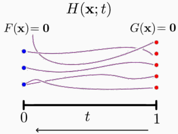
Finitely many sols

Numerical guesses

$\rightsquigarrow$ HomotopyContinuation.jl

$\rightsquigarrow$ Continued frac. exp.

$\rightsquigarrow$ Truncation



Symbolic methods

$\rightsquigarrow$ AlgebraicSolving.jl

$\rightsquigarrow$ factor in $\mathbb{Q}[t]$

$$\begin{cases} \omega(\boldsymbol{f_1}) = 0 & \omega \in \mathbb{Q}[t] \\ \boldsymbol{f_i} = \dfrac{\mu_i(\boldsymbol{f_1})}{\omega'(\boldsymbol{f_1})} & \mu_i \in \mathbb{Q}[t] \end{cases}$$

Invariant set $S_{(\boldsymbol{F},\boldsymbol{h})}$

$\boldsymbol{h}$ is invariant for $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{f}) \in \mathbb{C}^4$ if and only if

$$\boldsymbol{h_1} = \boldsymbol{b}^4 \boldsymbol{f_4}^2 - 2\boldsymbol{a}\boldsymbol{b}^2 \boldsymbol{f_3} \boldsymbol{f_4} - \boldsymbol{a}^3 \boldsymbol{f_1} + \boldsymbol{a}^2 \boldsymbol{f_3}^2 + \boldsymbol{b}^2 \boldsymbol{f_2}$$

$$\boldsymbol{h_2} = \boldsymbol{a}^3 \boldsymbol{f_5}^3 - \boldsymbol{a}^3 \boldsymbol{f_1} + \boldsymbol{b}^2 \boldsymbol{f_2} - 2\boldsymbol{b}^2 \boldsymbol{f_4} + 2\boldsymbol{a} \boldsymbol{f_3}$$

$$(\boldsymbol{h_1}, \boldsymbol{h_2}) \circ \widetilde{\boldsymbol{F}} = 0 \qquad (\boldsymbol{h_1}, \boldsymbol{h_2}) \circ \widetilde{\boldsymbol{F}}^2 = 0$$

Final step

Find solutions to a polynomial sys. with entries:

- in $\mathbb{Z} \rightsquigarrow$ undecidable (Hilbert's 10th pb.)
- in $\mathbb{Q} \rightsquigarrow$ major open problem

Exploit structure

Decompose into "simpler" subsystems

1. $\{\mathtt{c}_5 = \mathtt{c}_3 + \mathtt{c}_4 = \mathtt{c}_1 + \mathtt{c}_2 = 0\}$
2. $\{\mathtt{c}_5 + 1 = \mathtt{c}_3 + \mathtt{c}_4 \pm 1 = \mathtt{c}_1 + \mathtt{c}_2 - 1 = 0\}$
3. $\{\mathtt{c}_3 + \mathtt{c}_4 \pm 1 = \mathtt{c}_1 + \mathtt{c}_2 - 1 = \mathtt{c}_5^2 - \mathtt{c}_5 + 1 = 0\}$

   where $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}) = (1, 1, -1)$

Synthesizing polynomial loops

Loop synthesis

$(x, y, z, c) \leftarrow (a, b, c, f)$

while true do

Assert: $[h_1 : y^2 - x = 0 \wedge h_2 : z^3 + 2y - x = 0]$

$$\begin{bmatrix} x \\ y \\ z \\ c \end{bmatrix} \leftarrow \widetilde{F}(x, y, z) = \begin{bmatrix} c_1 x^3 + c_2 y^2 \\ c_3 x - c_4 y^2 \\ c_5 x \\ c \end{bmatrix}$$

end while

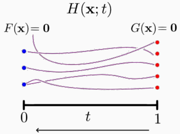
Finitely many sols

Numerical guesses

⇝ HomotopyContinuation.jl

⇝ Continued frac. exp.

⇝ Truncation



Symbolic methods

⇝ AlgebraicSolving.jl

⇝ factor in $\mathbb{Q}[t]$

$$\begin{cases} \omega(f_1) = 0 & \omega \in \mathbb{Q}[t] \\ f_i = \dfrac{\mu_i(f_1)}{\omega'(f_1)} & \mu_i \in \mathbb{Q}[t] \end{cases}$$

Invariant set $S_{(F,h)}$

h is invariant for $(a, b, c, f) \in \mathbb{C}^4$ if and only if

$$h_1 = b^4 f_4{}^2 - 2ab^2 f_3 f_4 - a^3 f_1 + a^2 f_3{}^2 + b^2 f_2$$

$$h_2 = a^3 f_5{}^3 - a^3 f_1 + b^2 f_2 - 2b^2 f_4 + 2a f_3$$

$$(h_1, h_2) \circ \widetilde{F} = 0 \qquad (h_1, h_2) \circ \widetilde{F}^2 = 0$$

Final step

Find solutions to a polynomial sys. with entries:

- in $\mathbb{Z}$ ⇝ undecidable (Hilbert's 10th pb.)
- in $\mathbb{Q}$ ⇝ major open problem

Exploit structure

Decompose into "simpler" subsystems

1. $\{c_5 = c_3 + c_4 = c_1 + c_2 = 0\}$
2. $\{c_5 + 1 = c_3 + c_4 \pm 1 = c_1 + c_2 - 1 = 0\}$
3. $\{c_3 + c_4 \pm 1 = c_1 + c_2 - 1 = c_5^2 - c_5 + 1 = 0\}$

   where $(a, b, c) = (1, 1, -1)$

SMT solvers (Z3)

Satisfiability of logical formulas mathematical theories

State of the art - Main results

Loop Invariants

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	✓	×	✓

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

Some of our contributions from [arXiv:2412.14043]

For loops of any degree we can:

1. test polynomial invariant
2. template-based polynomial invariant generation
3. optimization when fixed initial value

State of the art - Main results

Loop Invariants

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	✓	✗	✓

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

Loop synthesis

Works	ISSAC'23[1]	STACS'24[2]	Form. Asp. Comput'22[3]	Our work
Assignments	Linear	Linear	Linear	Polynomial
Invariants	Binomial	Quadratic	Polynomial	Polynomial
Complete	✓	✓	✗	✗
Non-trivial	✓	✓	✗	✗

[1] [Kenison, Kovács, Varonka; ISSAC'23] , [2] [Hitarth, Kenison, Kovács, Varonka; STACS'24]
[3] [Humenberger, Amrollahi, Bjørner, Kovács; Form. Asp. Comput'22]

Some of our contributions from [arXiv:2412.14043] [arXiv:2509.25114]

For loops of any degree we can:

1. test polynomial invariant
2. template-based polynomial invariant generation
3. optimization when fixed initial value
4. reduce loop synthesis to polynomial invariant

Polynomial inequalities
(Work In Progress)

What changes?

Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{ \boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) \ > \ 0 \right\}$$

What changes?

Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{\boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) > 0\right\}$$

No stabilisation 😱

Let $S_m = \{h > 0, \cdots, h \circ F^{(m)} > 0\}$

$S_{(F,h)} = S_0 \cap S_1 \cap \cdots \cap S_m \cap \cdots$

$\rightsquigarrow S_{(F,h)}$ can generally **not** be defined using *finitely many* $=$, $>$, $\wedge$ and $\neg$

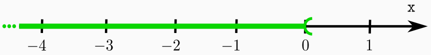
What changes?

Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{ \boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) > 0 \right\}$$

$(S_m)_{m \geq 0}$ does not stabilize



No stabilisation 😱

Let $S_m = \{h > 0, \cdots, h \circ F^{(m)} > 0\}$

$S_{(F,h)} = S_0 \cap S_1 \cap \cdots \cap S_m \cap \cdots$

$\rightsquigarrow S_{(F,h)}$ can generally **not** be defined using *finitely many* $=$, $>$, $\wedge$ and $\neg$

Example

```
x ← a
while true do
    Assert: x < 0
    x ← x + 1
end while
```

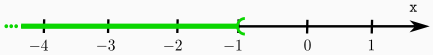
What changes?

Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{\boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) > 0\right\}$$

$(S_m)_{m \geq 0}$ does not stabilize



No stabilisation 😱

Let $S_m = \{h > 0, \cdots, h \circ F^{(m)} > 0\}$

$S_{(F,h)} = S_0 \cap S_1 \cap \cdots \cap S_m \cap \cdots$

$\rightsquigarrow$ $S_{(F,h)}$ can generally **not** be defined using *finitely many* $=, >, \wedge$ and $\neg$

Example

```
x ← a
while true do
    Assert: x < 0
    x ← x + 1
end while
```

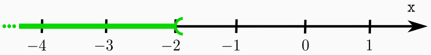
What changes?

Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{ \boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) > 0 \right\}$$

$(S_m)_{m \geq 0}$ does not stabilize



No stabilisation 😱

Let $S_m = \{h > 0, \cdots, h \circ F^{(m)} > 0\}$

$S_{(F,h)} = S_0 \cap S_1 \cap \cdots \cap S_m \cap \cdots$

$\rightsquigarrow S_{(F,h)}$ can generally **not** be defined using *finitely many* $=, >, \wedge$ and $\neg$

Example

```
x ← a
while true do
    Assert: x < 0
    x ← x + 1
end while
```

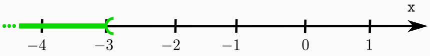
What changes?

Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{\boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) > 0\right\}$$

$(S_m)_{m\geq 0}$ does not stabilize



No stabilisation 😱

Let $S_m = \{h > 0, \cdots, h \circ F^{(m)} > 0\}$

$S_{(F,h)} = S_0 \cap S_1 \cap \cdots \cap S_m \cap \cdots$

$\rightsquigarrow S_{(F,h)}$ can generally **not** be defined using *finitely many* $=$, $>$, $\wedge$ and $\neg$

Example

```
x ← a
while true do
    Assert: x < 0
    x ← x + 1
end while
```

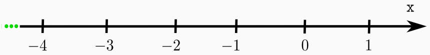
What changes?

Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{ \boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) > 0 \right\}$$

$(S_m)_{m \geq 0}$ does not stabilize



No stabilisation 😱

Let $S_m = \{h > 0, \cdots, h \circ F^{(m)} > 0\}$

$S_{(F,h)} = S_0 \cap S_1 \cap \cdots \cap S_m \cap \cdots$

$\rightsquigarrow$ $S_{(F,h)}$ can generally **not** be defined using *finitely many* $=$, $>$, $\wedge$ and $\neg$

Example

```
x ← a
while true do
    Assert: x < 0
    x ← x + 1
end while
```

What changes?

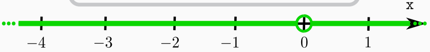
Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{\boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) > 0\right\}$$

$(S_m)_{m\geq 0}$ does not stabilize

$S_{\boldsymbol{F},\boldsymbol{h}} = \mathbb{R} - \mathbb{Z}_{\leq 0}$ not semi-algebraic



No stabilisation 😱

Let $S_m = \{h > 0, \cdots, h \circ F^{(m)} > 0\}$

$S_{(F,h)} = S_0 \cap S_1 \cap \cdots \cap S_m \cap \cdots$

$\rightsquigarrow$ $S_{(F,h)}$ can generally **not** be defined using *finitely many* $=$, $>$, $\wedge$ and $\neg$

Example

```
x ← a
while true do
    Assert: x ≠ 0
    x ← x + 1
end while
```

What changes?

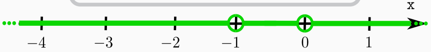
Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{\boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) > 0\right\}$$

$(S_m)_{m\geq 0}$ does not stabilize

$S_{\boldsymbol{F},\boldsymbol{h}} = \mathbb{R} - \mathbb{Z}_{\leq 0}$ not semi-algebraic



No stabilisation

Let $S_m = \{h > 0, \cdots, h \circ F^{(m)} > 0\}$

$S_{(F,h)} = S_0 \cap S_1 \cap \cdots \cap S_m \cap \cdots$

$\rightsquigarrow$ $S_{(F,h)}$ can generally **not** be defined using *finitely many* $=$, $>$, $\wedge$ and $\neg$

Example

```
x ← a
while true do
    Assert: x ≠ 0
    x ← x + 1
end while
```

What changes?

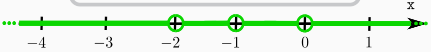
Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{ \boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) > 0 \right\}$$

$(S_m)_{m \geq 0}$ does not stabilize

$S_{\boldsymbol{F},\boldsymbol{h}} = \mathbb{R} - \mathbb{Z}_{\leq 0}$ not semi-algebraic



No stabilisation

Let $S_m = \{h > 0, \cdots, h \circ F^{(m)} > 0\}$

$S_{(F,h)} = S_0 \cap S_1 \cap \cdots \cap S_m \cap \cdots$

$\rightsquigarrow$ $S_{(F,h)}$ can generally **not** be defined using *finitely many* $=$, $>$, $\wedge$ and $\neg$

Example

```
x ← a
while true do
    Assert: x ≠ 0
    x ← x + 1
end while
```

What changes?

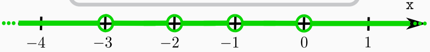
Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{\boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) > 0\right\}$$

$(S_m)_{m\geq 0}$ does not stabilize

$S_{\boldsymbol{F},\boldsymbol{h}} = \mathbb{R} - \mathbb{Z}_{\leq 0}$ not semi-algebraic



No stabilisation 😱

Let $S_m = \{h > 0, \cdots, h \circ F^{(m)} > 0\}$

$S_{(F,h)} = S_0 \cap S_1 \cap \cdots \cap S_m \cap \cdots$

$\rightsquigarrow S_{(F,h)}$ can generally **not** be defined using *finitely many* $=$, $>$, $\wedge$ and $\neg$

Example

```
x ← a
while true do
    Assert: x ≠ 0
    x ← x + 1
end while
```

What changes?

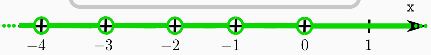
Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{ \boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) > 0 \right\}$$

$(S_m)_{m\geq 0}$ does not stabilize

$S_{\boldsymbol{F},\boldsymbol{h}} = \mathbb{R} - \mathbb{Z}_{\leq 0}$ not semi-algebraic



No stabilisation 😱

Let $S_m = \{h > 0, \cdots, h \circ F^{(m)} > 0\}$

$S_{(F,h)} = S_0 \cap S_1 \cap \cdots \cap S_m \cap \cdots$

$\rightsquigarrow$ $S_{(F,h)}$ can generally **not** be defined using *finitely many* $=$, $>$, $\wedge$ and $\neg$

Example

```
x ← a
while true do
    Assert: x ≠ 0
    x ← x + 1
end while
```

What changes?

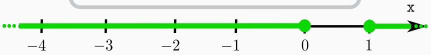
Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{\boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) > 0\right\}$$

$(S_m)_{m \geq 0}$ does not stabilize

$S_{\boldsymbol{F},\boldsymbol{h}} = \mathbb{Z}_{\leq 0} \cup \,]0, +\infty[$ not semi-algebraic



No stabilisation 😱

Let $S_m = \{h > 0, \cdots, h \circ F^{(m)} > 0\}$

$S_{(F,h)} = S_0 \cap S_1 \cap \cdots \cap S_m \cap \cdots$

$\rightsquigarrow S_{(F,h)}$ can generally **not** be defined using *finitely many* $=, >, \wedge$ and $\neg$

Example

```
x ← a
while true do
    Assert: 0 ≤ x ≤ 1
    x ← x + 1
end while
```

What changes?

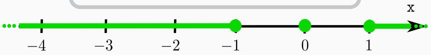
Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{\boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) > 0\right\}$$

$(S_m)_{m\geq 0}$ does not stabilize

$S_{\boldsymbol{F},\boldsymbol{h}} = \mathbb{Z}_{\leq 0} \cup \,]0, +\infty[$ not semi-algebraic



No stabilisation 😱

Let $S_m = \{h > 0, \cdots, h \circ F^{(m)} > 0\}$

$S_{(F,h)} = S_0 \cap S_1 \cap \cdots \cap S_m \cap \cdots$

$\rightsquigarrow$ $S_{(F,h)}$ can generally **not** be defined using *finitely many* $=$, $>$, $\wedge$ and $\neg$

Example

while true **do**

```
x ← a
while true do
    Assert: 0 ≤ x ≤ 1
    x ← x + 1
end while
```

What changes?

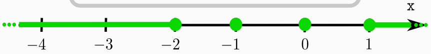
Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{\boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) > 0\right\}$$

$(S_m)_{m\geq 0}$ does not stabilize

$S_{\boldsymbol{F},\boldsymbol{h}} = \mathbb{Z}_{\leq 0} \cup \,]0, +\infty[$ not semi-algebraic



No stabilisation 😱

Let $S_m = \{h > 0, \cdots, h \circ F^{(m)} > 0\}$

$S_{(F,h)} = S_0 \cap S_1 \cap \cdots \cap S_m \cap \cdots$

$\rightsquigarrow$ $S_{(F,h)}$ can generally **not** be defined using *finitely many* $=$, $>$, $\wedge$ and $\neg$

Example

```
x ← a
while true do
    Assert: 0 ≤ x ≤ 1
    x ← x + 1
end while
```

What changes?

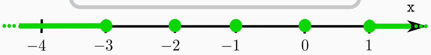
Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{\boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) > 0\right\}$$

$(S_m)_{m\geq 0}$ does not stabilize

$S_{\boldsymbol{F},\boldsymbol{h}} = \mathbb{Z}_{\leq 0} \cup]0, +\infty[$ not semi-algebraic



No stabilisation 😱

Let $S_m = \{h > 0, \cdots, h \circ F^{(m)} > 0\}$

$S_{(F,h)} = S_0 \cap S_1 \cap \cdots \cap S_m \cap \cdots$

$\rightsquigarrow$ $S_{(F,h)}$ can generally **not** be defined using *finitely many* $=$, $>$, $\wedge$ and $\neg$

Example

```
x ← a
while true do
    Assert: 0 ≤ x ≤ 1
    x ← x + 1
end while
```

What changes?

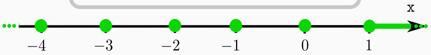
Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{ \boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) > 0 \right\}$$

$(S_m)_{m \geq 0}$ does not stabilize

$S_{\boldsymbol{F},\boldsymbol{h}} = \mathbb{Z}_{\leq 0} \cup]0, +\infty[$ not semi-algebraic



No stabilisation 😱

Let $S_m = \{h > 0, \cdots, h \circ F^{(m)} > 0\}$

$S_{(F,h)} = S_0 \cap S_1 \cap \cdots \cap S_m \cap \cdots$

$\rightsquigarrow S_{(F,h)}$ can generally **not** be defined using *finitely many* $=$, $>$, $\wedge$ and $\neg$

Example

```
x ← a
while true do
    Assert: 0 ≤ x ≤ 1
    x ← x + 1
end while
```

What changes?

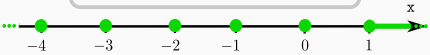
Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{ \boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) > 0 \right\}$$

$(S_m)_{m\geq 0}$ does not stabilize

$S_{\boldsymbol{F},\boldsymbol{h}} = \mathbb{Z}_{\leq 0} \cup \,]0, +\infty[$ not semi-algebraic



No stabilisation 😱

Let $S_m = \{h > 0, \cdots, h \circ F^{(m)} > 0\}$

$S_{(F,h)} = S_0 \cap S_1 \cap \cdots \cap S_m \cap \cdots$

$\rightsquigarrow$ $S_{(F,h)}$ can generally **not** be defined using *finitely many* $=$, $>$, $\wedge$ and $\neg$

Example

```
x ← a
while true do
    Assert: 0 ≤ x ≤ 1
    x ← x + 1
end while
```

Positivity test

$$\begin{cases} \boldsymbol{u_0}, \ldots, \boldsymbol{u_{k-1}} \in \mathbb{Q} \\ \boldsymbol{a_0}, \ldots, \boldsymbol{a_{k-1}} \in \mathbb{Q} \\ u_{n+k} + \boldsymbol{a_{k-1}} u_{n+k-1} + \cdots + \boldsymbol{a_0} u_n = 0 \end{cases}$$

Are all $u_n \geq 0$?

Open problem for $k \geq 6$
(diophantine approx. [Ouaknine & Worrell '10])

Invariant test

$(\mathtt{x}_0, \ldots, \mathtt{x}_{k-1}) \leftarrow (\boldsymbol{u_0}, \ldots, \boldsymbol{u_{k-1}})$
while true do
Assert: $\mathtt{x}_0 \geq 0, \ldots, \mathtt{x}_{k-1} \geq 0$

$$\begin{bmatrix} \mathtt{x}_0 \\ \vdots \\ \mathtt{x}_{k-2} \\ \mathtt{x}_{k-1} \end{bmatrix} = \begin{bmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ & & 0 & 1 \\ \boldsymbol{a_0} & \cdots & \boldsymbol{a_{k-2}} & \boldsymbol{a_{k-1}} \end{bmatrix} \cdot \begin{bmatrix} \mathtt{x}_0 \\ \vdots \\ \mathtt{x}_{k-2} \\ \mathtt{x}_{k-1} \end{bmatrix}$$

end while

What changes?

Definition

Invariant set of $(\boldsymbol{F}, \boldsymbol{h})$:

$$S_{(\boldsymbol{F},\boldsymbol{h})} = \left\{ \boldsymbol{a} \in \mathbb{C}^n,\ \forall m \geq 0,\ \boldsymbol{h} \circ \boldsymbol{F}^{(m)}(\boldsymbol{a}) > 0 \right\}$$

No stabilisation 😱

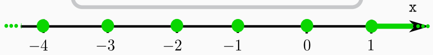
Let $S_m = \{h > 0, \cdots, h \circ F^{(m)} > 0\}$

$S_{(F,h)} = S_0 \cap S_1 \cap \cdots \cap S_m \cap \cdots$

$\rightsquigarrow$ $S_{(F,h)}$ can generally **not** be defined using *finitely many* $=$, $>$, $\wedge$ and $\neg$

$(S_m)_{m \geq 0}$ does not stabilize

$S_{\boldsymbol{F},\boldsymbol{h}} = \mathbb{Z}_{\leq 0} \cup \,]0, +\infty[$ not semi-algebraic



Example

```
x ← a
while true do
    Assert: 0 ≤ x ≤ 1
    x ← x + 1
end while
```

Positivity test

$$\begin{cases} \boldsymbol{u_0}, \ldots, \boldsymbol{u_{k-1}} \in \mathbb{Q} \\ \boldsymbol{a_0}(n), \ldots, \boldsymbol{a_{k-1}}(n) \in \mathbb{Q}[n] \\ u_{n+k} + \boldsymbol{a_{k-1}}(n) u_{n+k-1} + \cdots + \boldsymbol{a_0}(n) u_n = 0 \end{cases}$$

Are all $u_n \geq 0$?

Assumptions on eigenvalue and initial values [Ibrahim & Salvy '25]

Invariant test

$(\mathtt{x}_0, \ldots, \mathtt{x}_{k-1}, \mathtt{n}) \leftarrow (\boldsymbol{u_0}, \ldots, \boldsymbol{u_{k-1}}, 0)$
while true do
  Assert: $\mathtt{x}_0 \geq 0, \ldots, \mathtt{x}_{k-1} \geq 0$

$$\begin{bmatrix} \mathtt{x}_0 \\ \vdots \\ \mathtt{x}_{k-2} \\ \mathtt{x}_{k-1} \\ \mathtt{n} \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ & & 0 & 1 \\ \boldsymbol{a_0}(\mathtt{n}) & \cdots & \cdots & \boldsymbol{a_{k-1}}(\mathtt{n}) \end{bmatrix} \cdot \begin{bmatrix} \mathtt{x}_0 \\ \vdots \\ \mathtt{x}_{k-1} \end{bmatrix} \\ \mathtt{n} + 1 \end{bmatrix}$$

end while

Inductive invariants

Polynomial loop

```
x ← a
while true do
    Assert: h(x) > 0
    x ← F(x)
end while
```

Inductive invariant

$$h(a) > 0 \text{ and } \forall x,\ h(x) > 0 \Longrightarrow h \circ F(x) > 0$$

Inductive invariants

Polynomial loop

$x \leftarrow a$
while true **do**
  Assert: $h(x) > 0$
  $x \leftarrow F(x)$
end while

Inductive invariant

$$h(a) > 0 \text{ and } \forall x,\ h(x) > 0 \Longrightarrow h \circ F(x) > 0$$

Example

$x \leftarrow (2, 1)$
while true **do**
  $$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 \cdot x \\ -\frac{3}{2} \cdot y \end{bmatrix}$$
end while

Inductive invariants

Polynomial loop

$\mathtt{x} \leftarrow \boldsymbol{a}$
while true **do**
  Assert: $\boldsymbol{h}(\mathtt{x}) > 0$
  $\mathtt{x} \leftarrow \boldsymbol{F}(\mathtt{x})$
end while

Inductive invariant

$$\boldsymbol{h}(\boldsymbol{a}) > 0 \text{ and } \forall x,\ \boldsymbol{h}(x) > 0 \Longrightarrow \boldsymbol{h} \circ \boldsymbol{F}(x) > 0$$

Example

$\mathtt{x} \leftarrow (\mathbf{2}, \mathbf{1})$
while true **do**
  $\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \end{bmatrix} = \begin{bmatrix} 2 \cdot \mathtt{x} \\ -\frac{3}{2} \cdot \mathtt{y} \end{bmatrix}$
end while

$\boldsymbol{h} = x - 1 > 0$ **Order 0**

$\boldsymbol{h}(\mathbf{2}, \mathbf{1}) > 0$ and $\boldsymbol{h} \circ F = 2\boldsymbol{h} + 1$

Inductive invariants

Polynomial loop

```
x ← a
while true do
    Assert: h(x) > 0
    x ← F(x)
end while
```

Inductive invariant

$$h(a) > 0 \text{ and } \forall x,\ h(x) > 0 \Longrightarrow h \circ F(x) > 0$$

Order-k Inductive invariant [Gerhold & Kauers '05, Falke & Kapur '15]

$$h(a) > 0, \ldots, h \circ F^{(k)}(a) > 0 \text{ and}$$

$$\forall x,\ h(x) > 0, \ldots, h \circ F^{(k)}(x) > 0 \Rightarrow h \circ F^{(k+1)}(x) > 0$$

Example

1: $\mathtt{x} \leftarrow (2, 1)$

2: **while true do**

3: $\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \end{bmatrix} = \begin{bmatrix} 2 \cdot \mathtt{x} \\ -\frac{3}{2} \cdot \mathtt{y} \end{bmatrix}$

4: **end while**

$h = x - 1 > 0$ **Order 0**

$h(2, 1) > 0$ and $h \circ F = 2h + 1$

Inductive invariants

Polynomial loop

```
x ← a
while true do
    Assert: h(x) > 0
    x ← F(x)
end while
```

Inductive invariant

$$h(a) > 0 \text{ and } \forall x,\ h(x) > 0 \Longrightarrow h \circ F(x) > 0$$

Order-k Inductive invariant [Gerhold & Kauers '05, Falke & Kapur '15]

$$h(a) > 0, \dots, h \circ F^{(k)}(a) > 0 \text{ and}$$

$$\forall x,\ h(x) > 0, \dots, h \circ F^{(k)}(x) > 0 \Rightarrow h \circ F^{(k+1)}(x) > 0$$

Example

```
x ← (2, 1)
while true do
    [x; y] = [2 · x; −(3/2) · y]
end while
```

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 \cdot x \\ -\frac{3}{2} \cdot y \end{bmatrix}$$

$h = x - 1 > 0$ **Order 0**

$h(2, 1) > 0$ and $h \circ F = 2h + 1$

$h = 3x - 4y - 1 > 0$ **Order 1**

Not order 0 $\rightsquigarrow \begin{cases} h(0, -1) > 0 \\ h \circ F(0, -1) < 0 \end{cases}$

But order 1: $h(2, 1) > 0$ and

$$2 \cdot h \circ F^2 = h \circ F + 6h + 5$$

Inductive invariants

Polynomial loop

```
x ← a
while true do
    Assert: h(x) > 0
    x ← F(x)
end while
```

Inductive invariant

$$h(a) > 0 \text{ and } \forall x,\ h(x) > 0 \Longrightarrow h \circ F(x) > 0$$

Order-k Inductive invariant [Gerhold & Kauers '05, Falke & Kapur '15]

$$h(a) > 0, \ldots, h \circ F^{(k)}(a) > 0 \text{ and}$$

$$\forall x,\ h(x) > 0, \ldots, h \circ F^{(k)}(x) > 0 \Rightarrow h \circ F^{(k+1)}(x) > 0$$

Example

```
x ← (2, 1)
while true do
    [x; y] = [2 · x; −3/2 · y]
end while
```

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 \cdot x \\ -\frac{3}{2} \cdot y \end{bmatrix}$$

This is the max. order here

$h = x - 1 > 0$ **Order 0**

$h(2, 1) > 0$ and $h \circ F = 2h + 1$

$h = 3x - 4y - 1 > 0$ **Order 1**

Not order 0 $\rightsquigarrow \begin{cases} h(0, -1) > 0 \\ h \circ F(0, -1) < 0 \end{cases}$

But order 1: $h(2, 1) > 0$ and

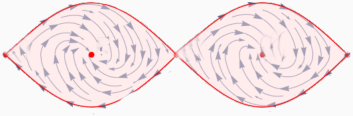
$$2 \cdot h \circ F^2 = h \circ F + 6h + 5$$

On the set of inductive invariants

Definition

Inductive polynomials $f \in \mathrm{Ind}_r(\boldsymbol{F}) \cap \mathbb{R}_{\leq \boldsymbol{d}}[\boldsymbol{x}] = \mathrm{Ind}_{r,\boldsymbol{d}}$:

$$\text{for all } \boldsymbol{x} \in \mathbb{R}^n, \quad \boldsymbol{h}(\boldsymbol{x}) > 0, \ldots, \boldsymbol{h} \circ \boldsymbol{F}^r(\boldsymbol{x}) > 0 \Longrightarrow \boldsymbol{h} \circ \boldsymbol{F}^{r+1}(\boldsymbol{x}) > 0$$



Properties

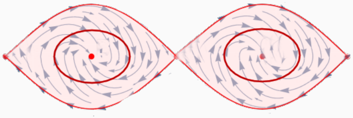
✓ 1

On the set of inductive invariants

Definition

Inductive polynomials $f \in \mathrm{Ind}_r(\boldsymbol{F}) \cap \mathbb{R}_{\leq \boldsymbol{d}}[\boldsymbol{x}] = \mathrm{Ind}_{r,\boldsymbol{d}}$:

$$\text{for all } \boldsymbol{x} \in \mathbb{R}^n, \quad \boldsymbol{h}(\boldsymbol{x}) > 0, \ldots, \boldsymbol{h} \circ \boldsymbol{F}^r(\boldsymbol{x}) > 0 \Longrightarrow \boldsymbol{h} \circ \boldsymbol{F}^{r+1}(\boldsymbol{x}) > 0$$



Properties

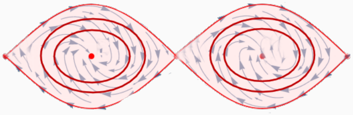
✓ $1 \subsetneq \mathrm{Ind}_{0,\boldsymbol{d}}$

On the set of inductive invariants

Definition

Inductive polynomials $f \in \mathrm{Ind}_r(\boldsymbol{F}) \cap \mathbb{R}_{\leq \boldsymbol{d}}[\boldsymbol{x}] = \mathrm{Ind}_{r,\boldsymbol{d}}$:

$$\text{for all } \boldsymbol{x} \in \mathbb{R}^n, \quad \boldsymbol{h}(\boldsymbol{x}) > 0, \dots, \boldsymbol{h} \circ \boldsymbol{F}^r(\boldsymbol{x}) > 0 \Longrightarrow \boldsymbol{h} \circ \boldsymbol{F}^{r+1}(\boldsymbol{x}) > 0$$



Properties

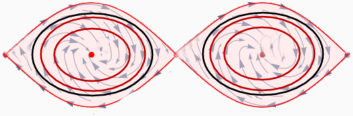
✓ $1 \subsetneq \mathrm{Ind}_{0,\boldsymbol{d}} \subsetneq \cdots \subsetneq \mathrm{Ind}_{r,\boldsymbol{d}}$

On the set of inductive invariants

Definition

Inductive polynomials $f \in \mathrm{Ind}_r(\boldsymbol{F}) \cap \mathbb{R}_{\leq \boldsymbol{d}}[\boldsymbol{x}] = \mathrm{Ind}_{r,\boldsymbol{d}}$:

$$\text{for all } \boldsymbol{x} \in \mathbb{R}^n, \quad \boldsymbol{h}(\boldsymbol{x}) > 0, \ldots, \boldsymbol{h} \circ \boldsymbol{F}^r(\boldsymbol{x}) > 0 \Longrightarrow \boldsymbol{h} \circ \boldsymbol{F}^{r+1}(\boldsymbol{x}) > 0$$



Properties

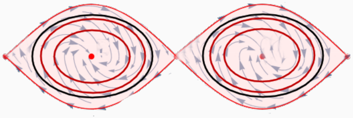
✓ $1 \subsetneq \mathrm{Ind}_{0,\boldsymbol{d}} \subsetneq \cdots \subsetneq \mathrm{Ind}_{r,\boldsymbol{d}} \stackrel{?}{=} \mathrm{Ind}_{r+1,\boldsymbol{d}} = \cdots$

On the set of inductive invariants

Definition

Inductive polynomials $f \in \mathrm{Ind}_r(\boldsymbol{F}) \cap \mathbb{R}_{\leq \boldsymbol{d}}[\boldsymbol{x}] = \mathrm{Ind}_{r,\boldsymbol{d}}$:

$$\text{for all } \boldsymbol{x} \in \mathbb{R}^n, \quad \boldsymbol{h}(\boldsymbol{x}) > 0, \ldots, \boldsymbol{h} \circ \boldsymbol{F}^r(\boldsymbol{x}) > 0 \Longrightarrow \boldsymbol{h} \circ \boldsymbol{F}^{r+1}(\boldsymbol{x}) > 0$$



Properties

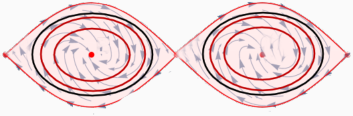
- ✓ $1 \subsetneq \mathrm{Ind}_{0,\boldsymbol{d}} \subsetneq \cdots \subsetneq \mathrm{Ind}_{r,\boldsymbol{d}} \stackrel{?}{=} \mathrm{Ind}_{r+1,\boldsymbol{d}} = \cdots$
- × No guarantee to stabilize

On the set of inductive invariants

Definition

Inductive polynomials $f \in \mathrm{Ind}_r(\boldsymbol{F}) \cap \mathbb{R}_{\leq \boldsymbol{d}}[\boldsymbol{x}] = \mathrm{Ind}_{r,\boldsymbol{d}}$:

$$\text{for all } \boldsymbol{x} \in \mathbb{R}^n, \quad \boldsymbol{h}(\boldsymbol{x}) > 0, \ldots, \boldsymbol{h} \circ \boldsymbol{F}^r(\boldsymbol{x}) > 0 \Longrightarrow \boldsymbol{h} \circ \boldsymbol{F}^{r+1}(\boldsymbol{x}) > 0$$



Properties

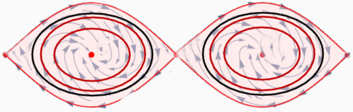
- ✓ $1 \subsetneq \mathrm{Ind}_{0,\boldsymbol{d}} \subsetneq \cdots \subsetneq \mathrm{Ind}_{r,\boldsymbol{d}} \stackrel{?}{=} \mathrm{Ind}_{r+1,\boldsymbol{d}} = \cdots$
- × No guarantee to stabilize
- ✓ Soundness: $\mathrm{Ind}_{r,\boldsymbol{d}} \subset \left\{\text{All invariants}\right\}$

On the set of inductive invariants

Definition

Inductive polynomials $f \in \mathrm{Ind}_r(\boldsymbol{F}) \cap \mathbb{R}_{\leq \boldsymbol{d}}[\boldsymbol{x}] = \mathrm{Ind}_{r,\boldsymbol{d}}$:

$$\text{for all } \boldsymbol{x} \in \mathbb{R}^n, \quad \boldsymbol{h}(\boldsymbol{x}) > 0, \ldots, \boldsymbol{h} \circ \boldsymbol{F}^r(\boldsymbol{x}) > 0 \Longrightarrow \boldsymbol{h} \circ \boldsymbol{F}^{r+1}(\boldsymbol{x}) > 0$$



Properties

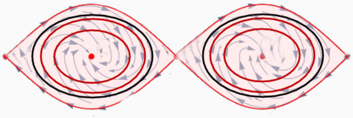
- ✓ $1 \subsetneq \mathrm{Ind}_{0,\boldsymbol{d}} \subsetneq \cdots \subsetneq \mathrm{Ind}_{r,\boldsymbol{d}} \overset{?}{=} \mathrm{Ind}_{r+1,\boldsymbol{d}} = \cdots$
- × No guarantee to stabilize
- ✓ Soundness: $\mathrm{Ind}_{r,\boldsymbol{d}} \subset \left\{ \text{All invariants} \right\}$
- × In general $\bigcup_r \mathrm{Ind}_r \subsetneq \left\{ \text{All invariants} \right\}$

On the set of inductive invariants

Definition

Inductive polynomials $f \in \mathrm{Ind}_r(\boldsymbol{F}) \cap \mathbb{R}_{\leq \boldsymbol{d}}[\boldsymbol{x}] = \mathrm{Ind}_{r,\boldsymbol{d}}$:

$$\text{for all } \boldsymbol{x} \in \mathbb{R}^n, \quad \boldsymbol{h}(\boldsymbol{x}) > 0, \ldots, \boldsymbol{h} \circ \boldsymbol{F}^r(\boldsymbol{x}) > 0 \Longrightarrow \boldsymbol{h} \circ \boldsymbol{F}^{r+1}(\boldsymbol{x}) > 0$$



Properties

- ✓ $1 \subsetneq \mathrm{Ind}_{0,\boldsymbol{d}} \subsetneq \cdots \subsetneq \mathrm{Ind}_{r,\boldsymbol{d}} \overset{?}{=} \mathrm{Ind}_{r+1,\boldsymbol{d}} = \cdots$
- × No guarantee to stabilize
- ✓ Soundness: $\mathrm{Ind}_{r,\boldsymbol{d}} \subset \left\{\text{All invariants}\right\}$
- × In general $\bigcup_r \mathrm{Ind}_r \subsetneq \left\{\text{All invariants}\right\}$

Computability

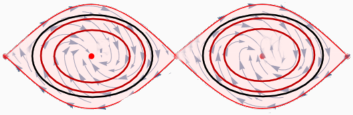
$\mathrm{Ind}_{r,\boldsymbol{d}}(\boldsymbol{F})$ can be written with finitely many *quantifier-free* equation+inequalities $\rightsquigarrow$ semi-algebraic set

On the set of inductive invariants

Definition

Inductive polynomials $f \in \mathrm{Ind}_r(\boldsymbol{F}) \cap \mathbb{R}_{\leq \boldsymbol{d}}[\boldsymbol{x}] = \mathrm{Ind}_{r,\boldsymbol{d}}$:

$$\text{for all } \boldsymbol{x} \in \mathbb{R}^n, \quad \boldsymbol{h}(\boldsymbol{x}) > 0, \ldots, \boldsymbol{h} \circ \boldsymbol{F}^r(\boldsymbol{x}) > 0 \Longrightarrow \boldsymbol{h} \circ \boldsymbol{F}^{r+1}(\boldsymbol{x}) > 0$$



Properties

✓ $1 \subsetneq \mathrm{Ind}_{0,\boldsymbol{d}} \subsetneq \cdots \subsetneq \mathrm{Ind}_{r,\boldsymbol{d}} \stackrel{?}{=} \mathrm{Ind}_{r+1,\boldsymbol{d}} = \cdots$

× No guarantee to stabilize

✓ Soundness: $\mathrm{Ind}_{r,\boldsymbol{d}} \subset \left\{\text{All invariants}\right\}$

× In general $\bigcup_r \mathrm{Ind}_r \subsetneq \left\{\text{All invariants}\right\}$

Symbolic Quantifier Elimination

Presburger (e.g.Fourier-Motzkin) $(\boldsymbol{d} = 1, \deg(\boldsymbol{F}) = 1)$

Cylindrical Algebraic Decomposition [Collins, '75]

Computability

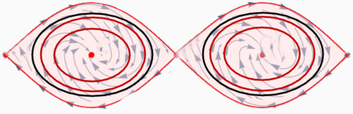
$\mathrm{Ind}_{r,\boldsymbol{d}}(\boldsymbol{F})$ can be written with finitely many *quantifier-free* equation+inequalities $\rightsquigarrow$ semi-algebraic set

On the set of inductive invariants

Definition

Inductive polynomials $f \in \mathrm{Ind}_r(\boldsymbol{F}) \cap \mathbb{R}_{\leq \boldsymbol{d}}[\boldsymbol{x}] = \mathrm{Ind}_{r,\boldsymbol{d}}$:

$$\text{for all } \boldsymbol{x} \in \mathbb{R}^n, \quad \boldsymbol{h}(\boldsymbol{x}) > 0, \ldots, \boldsymbol{h} \circ \boldsymbol{F}^r(\boldsymbol{x}) > 0 \Longrightarrow \boldsymbol{h} \circ \boldsymbol{F}^{r+1}(\boldsymbol{x}) > 0$$



Properties

- ✓ $1 \subsetneq \mathrm{Ind}_{0,\boldsymbol{d}} \subsetneq \cdots \subsetneq \mathrm{Ind}_{r,\boldsymbol{d}} \overset{?}{=} \mathrm{Ind}_{r+1,\boldsymbol{d}} = \cdots$
- × No guarantee to stabilize
- ✓ Soundness: $\mathrm{Ind}_{r,\boldsymbol{d}} \subset \left\{\text{All invariants}\right\}$
- × In general $\bigcup_r \mathrm{Ind}_r \subsetneq \left\{\text{All invariants}\right\}$

Symbolic Quantifier Elimination

Presburger (e.g.Fourier-Motzkin) $(\boldsymbol{d} = 1, \deg(\boldsymbol{F}) = 1)$
Cylindrical Algebraic Decomposition [Collins, '75]

Computability

$\mathrm{Ind}_{r,\boldsymbol{d}}(\boldsymbol{F})$ can be written with finitely many *quantifier-free* equation+inequalities $\rightsquigarrow$ semi-algebraic set

Numerical Quantifier Elimination

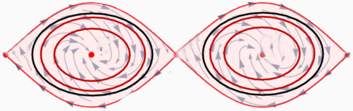
Semidefinite programming [Lasserre '15]

On the set of inductive invariants

Definition

Inductive polynomials $f \in \mathrm{Ind}_r(\boldsymbol{F}) \cap \mathbb{R}_{\leq \boldsymbol{d}}[\boldsymbol{x}] = \mathrm{Ind}_{r,\boldsymbol{d}}$:

$$\text{for all } \boldsymbol{x} \in \mathbb{R}^n, \quad \boldsymbol{h}(\boldsymbol{x}) > 0, \ldots, \boldsymbol{h} \circ \boldsymbol{F}^r(\boldsymbol{x}) > 0 \Longrightarrow \boldsymbol{h} \circ \boldsymbol{F}^{r+1}(\boldsymbol{x}) > 0$$



Properties

- ✓ $1 \subsetneq \mathrm{Ind}_{0,\boldsymbol{d}} \subsetneq \cdots \subsetneq \mathrm{Ind}_{r,\boldsymbol{d}} \stackrel{?}{=} \mathrm{Ind}_{r+1,\boldsymbol{d}} = \cdots$
- × No guarantee to stabilize
- ✓ Soundness: $\mathrm{Ind}_{r,\boldsymbol{d}} \subset \left\{\text{All invariants}\right\}$
- × In general $\bigcup_r \mathrm{Ind}_r \subsetneq \left\{\text{All invariants}\right\}$

Symbolic Quantifier Elimination

Presburger (e.g.Fourier-Motzkin) ($\boldsymbol{d} = 1, \deg(\boldsymbol{F}) = 1$)
Cylindrical Algebraic Decomposition [Collins, '75]

Exploit structure

Farkas' lemma ($\boldsymbol{d} = 1, \deg(\boldsymbol{F}) = 1$)
Putinar's Positivstellensatz

Computability

$\mathrm{Ind}_{r,\boldsymbol{d}}(\boldsymbol{F})$ can be written with finitely many *quantifier-free* equation+inequalities $\rightsquigarrow$ semi-algebraic set

Numerical Quantifier Elimination

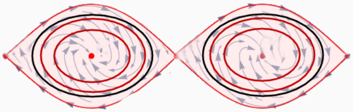
Semidefinite programming [Lasserre '15]

On the set of inductive invariants

Definition

Inductive polynomials $f \in \mathrm{Ind}_r(\boldsymbol{F}) \cap \mathbb{R}_{\leq \boldsymbol{d}}[\boldsymbol{x}] = \mathrm{Ind}_{r,\boldsymbol{d}}$:

$$\text{for all } \boldsymbol{x} \in \mathbb{R}^n, \quad h(\boldsymbol{x}) > 0, \ldots, h \circ \boldsymbol{F}^r(\boldsymbol{x}) > 0 \Longrightarrow h \circ \boldsymbol{F}^{r+1}(\boldsymbol{x}) > 0$$



Properties

- ✓ $1 \subsetneq \mathrm{Ind}_{0,\boldsymbol{d}} \subsetneq \cdots \subsetneq \mathrm{Ind}_{r,\boldsymbol{d}} \stackrel{?}{=} \mathrm{Ind}_{r+1,\boldsymbol{d}} = \cdots$
- × No guarantee to stabilize
- ✓ Soundness: $\mathrm{Ind}_{r,\boldsymbol{d}} \subset \{\text{All invariants}\}$
- × In general $\bigcup_r \mathrm{Ind}_r \subsetneq \{\text{All invariants}\}$

Symbolic Quantifier Elimination

Presburger (e.g.Fourier-Motzkin) $(\boldsymbol{d} = 1, \deg(\boldsymbol{F}) = 1)$

Cylindrical Algebraic Decomposition [Collins, '75]

Exploit structure

In the following

Farkas' lemma $(\boldsymbol{d} = 1, \deg(\boldsymbol{F}) = 1)$

Putinar's Positivstellensatz

Computability

$\mathrm{Ind}_{r,\boldsymbol{d}}(\boldsymbol{F})$ can be written with finitely many *quantifier-free* equation+inequalities $\rightsquigarrow$ semi-algebraic set

Numerical Quantifier Elimination

Semidefinite programming [Lasserre '15]

Adapted Farkas lemma

Affine loop

$\mathtt{x} \leftarrow \boldsymbol{a}$

while true **do**

Assert: $\boldsymbol{h}$: $c_1\mathtt{x} + c_2\mathtt{y} + c_3\mathtt{z} + c_4\mathtt{t} > 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{t} \end{bmatrix} \leftarrow \left[\begin{array}{cc|cc} 1 & 1 & & \\ 0 & 1 & & \\ \hline & & 0 & -1 \\ & & 1 & 0 \end{array}\right] \begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{t} \end{bmatrix}$$

end while

Adapted Farkas lemma

Affine loop

$\mathtt{x} \leftarrow \boldsymbol{a}$

while true **do**

Assert: $\boldsymbol{h}$: $c_1\mathtt{x} + c_2\mathtt{y} + c_3\mathtt{z} + c_4\mathtt{t} > 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{t} \end{bmatrix} \leftarrow \left[\begin{array}{cc|cc} 1 & 1 & & \\ 0 & 1 & & \\ \hline & & 0 & -1 \\ & & 1 & 0 \end{array}\right] \begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{t} \end{bmatrix}$$

end while

Farkas' Lemma **(friendly version)**

Let $\Phi : \begin{cases} a_1\mathtt{x} + a_2\mathtt{y} + a_2\mathtt{z} + a_4\mathtt{t} \geq 0 \\ b_1\mathtt{x} + b_2\mathtt{y} + b_2\mathtt{z} + b_4\mathtt{t} \geq 0 \end{cases}$

Suppose Φ satisfiable, then

$$\forall(\mathtt{x}, \mathtt{y}, \mathtt{z}, \mathtt{t}),\ \Phi \implies c_1\mathtt{x} + c_2\mathtt{y} + c_2\mathtt{z} + c_4\mathtt{t} \geq 0$$

iff there exists $\lambda_1, \lambda_2, \lambda_3 \geq 0$ such that

$$c_i = \lambda_1 a_i + \lambda_2 b_i \quad \text{for } i \in \{1, 2, 3\}$$

Adapted Farkas lemma

Affine loop

$\mathtt{x} \leftarrow \boldsymbol{a}$

while true **do**

Assert: $\boldsymbol{h}$: $c_1\mathtt{x} + c_2\mathtt{y} + c_3\mathtt{z} + c_4\mathtt{t} > 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{t} \end{bmatrix} \leftarrow \left[\begin{array}{cc|cc} 1 & 1 & & \\ 0 & 1 & & \\ \hline & & 0 & -1 \\ & & 1 & 0 \end{array}\right] \begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{t} \end{bmatrix}$$

end while

Farkas' Lemma **(friendly version)**

Let $\Phi : \begin{cases} a_1\mathtt{x} + a_2\mathtt{y} + a_2\mathtt{z} + a_4\mathtt{t} \geq 0 \\ b_1\mathtt{x} + b_2\mathtt{y} + b_2\mathtt{z} + b_4\mathtt{t} \geq 0 \end{cases}$

Suppose Φ satisfiable, then

$$\forall(\mathtt{x},\mathtt{y},\mathtt{z},\mathtt{t}),\ \Phi \implies c_1\mathtt{x} + c_2\mathtt{y} + c_2\mathtt{z} + c_4\mathtt{t} \geq 0$$

iff there exists $\lambda_1, \lambda_2, \lambda_3 \geq 0$ such that

$$c_i = \lambda_1 a_i + \lambda_2 b_i \quad \text{for } i \in \{1, 2, 3\}$$

$\times$ $=$

All blocks

$\{(\boldsymbol{c}', \boldsymbol{c}'')\} \subset \mathbb{R}^4$

Adapted Farkas lemma

Affine loop

$\mathtt{x} \leftarrow \boldsymbol{a}$

while true **do**

Assert: h : $c_1\mathtt{x} + c_2\mathtt{y} + c_3\mathtt{z} + c_4\mathtt{t} > 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{t} \end{bmatrix} \leftarrow \left[\begin{array}{cc|cc} 1 & 1 & & \\ 0 & 1 & & \\ \hline & & 0 & -1 \\ & & 1 & 0 \end{array}\right] \begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{t} \end{bmatrix}$$

end while

Farkas' Lemma **(friendly version)**

Let $\Phi : \begin{cases} a_1\mathtt{x} + a_2\mathtt{y} + a_2\mathtt{z} + a_4\mathtt{t} \geq 0 \\ b_1\mathtt{x} + b_2\mathtt{y} + b_2\mathtt{z} + b_4\mathtt{t} \geq 0 \end{cases}$

Suppose Φ satisfiable, then

$$\forall(\mathtt{x}, \mathtt{y}, \mathtt{z}, \mathtt{t}),\ \Phi \implies c_1\mathtt{x} + c_2\mathtt{y} + c_2\mathtt{z} + c_4\mathtt{t} \geq 0$$

iff there exists $\lambda_1, \lambda_2, \lambda_3 \geq 0$ such that

$$c_i = \lambda_1 a_i + \lambda_2 b_i \quad \text{for } i \in \{1, 2, 3\}$$

Real Jordan blocks

$\{\boldsymbol{c}' \in \mathbb{R}^2 \mid \exists \boldsymbol{\lambda} \in \mathbb{R}^r_{\geq 0}, \boldsymbol{\ell}'(\boldsymbol{\lambda}, \boldsymbol{c}') = 0\}$

$\times$

$=$

All blocks

$\{(\boldsymbol{c}', \boldsymbol{c}'')\} \subset \mathbb{R}^4$

Adapted Farkas lemma

Affine loop

$\mathtt{x} \leftarrow \boldsymbol{a}$

while true **do**

Assert: $\boldsymbol{h}$: $c_1\mathtt{x} + c_2\mathtt{y} + c_3\mathtt{z} + c_4\mathtt{t} > 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{t} \end{bmatrix} \leftarrow \left[\begin{array}{cc|cc} 1 & 1 & & \\ 0 & 1 & & \\ \hline & & 0 & -1 \\ & & 1 & 0 \end{array}\right] \begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{t} \end{bmatrix}$$

end while

Farkas' Lemma (friendly version)

Let $\Phi : \begin{cases} a_1\mathtt{x} + a_2\mathtt{y} + a_2\mathtt{z} + a_4\mathtt{t} \geq 0 \\ b_1\mathtt{x} + b_2\mathtt{y} + b_2\mathtt{z} + b_4\mathtt{t} \geq 0 \end{cases}$

Suppose Φ satisfiable, then

$$\forall(\mathtt{x}, \mathtt{y}, \mathtt{z}, \mathtt{t}),\ \Phi \implies c_1\mathtt{x} + c_2\mathtt{y} + c_2\mathtt{z} + c_4\mathtt{t} \geq 0$$

iff there exists $\lambda_1, \lambda_2, \lambda_3 \geq 0$ such that

$$c_i = \lambda_1 a_i + \lambda_2 b_i \quad \text{for } i \in \{1, 2, 3\}$$

Real Jordan blocks

$\{\boldsymbol{c}' \in \mathbb{R}^2 \mid \exists \boldsymbol{\lambda} \in \mathbb{R}^r_{\geq 0}, \boldsymbol{\ell}'(\boldsymbol{\lambda}, \boldsymbol{c}') = 0\}$

$\times$

Complex Jordan blocks

$\{\boldsymbol{c}'' \in \mathbb{R}^3 \mid \exists \boldsymbol{\lambda} \in \mathbb{R}^r_{\geq 0}, \boldsymbol{\ell}''(\boldsymbol{\lambda}, \boldsymbol{c}'') = 0\}$

$=$

All blocks

$\{(\boldsymbol{c}', \boldsymbol{c}'')\} \subset \mathbb{R}^4$

Adapted Farkas lemma

Affine loop

$\mathtt{x} \leftarrow \boldsymbol{a}$

while true do

Assert: h : $c_1\mathtt{x} + c_2\mathtt{y} + c_3\mathtt{z} + c_4\mathtt{t} > 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{t} \end{bmatrix} \leftarrow \left[\begin{array}{cc|cc} 1 & 1 & & \\ 0 & 1 & & \\ \hline & & 0 & -1 \\ & & 1 & 0 \end{array}\right] \begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{t} \end{bmatrix}$$

end while

Farkas' Lemma (friendly version)

Let $\Phi : \begin{cases} a_1\mathtt{x} + a_2\mathtt{y} + a_2\mathtt{z} + a_4\mathtt{t} \geq 0 \\ b_1\mathtt{x} + b_2\mathtt{y} + b_2\mathtt{z} + b_4\mathtt{t} \geq 0 \end{cases}$

Suppose Φ satisfiable, then

$$\forall(\mathtt{x},\mathtt{y},\mathtt{z},\mathtt{t}),\ \Phi \implies c_1\mathtt{x} + c_2\mathtt{y} + c_2\mathtt{z} + c_4\mathtt{t} \geq 0$$

iff there exists $\lambda_1, \lambda_2, \lambda_3 \geq 0$ such that

$$c_i = \lambda_1 a_i + \lambda_2 b_i \quad \text{for } i \in \{1,2,3\}$$

Real Jordan blocks

$\{\boldsymbol{c}' \in \mathbb{R}^2 \mid \exists \boldsymbol{\lambda} \in \mathbb{R}^r_{\geq 0}, \boldsymbol{\ell}'(\boldsymbol{\lambda}, \boldsymbol{c}') = 0\}$

$\times$

Complex Jordan blocks

$\{\boldsymbol{c}'' \in \mathbb{R}^2 \mid c''_1 = 0 \wedge c''_2 = 0\}$

$=$

All blocks

$\{(\boldsymbol{c}', \boldsymbol{c}'')\} \subset \mathbb{R}^4$

Adapted Farkas lemma

Affine loop

$\mathtt{x} \leftarrow \boldsymbol{a}$

while true do

Assert: $h : c_1\mathtt{x} + c_2\mathtt{y} + c_3\mathtt{z} + c_4\mathtt{t} > 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{t} \end{bmatrix} \leftarrow \left[\begin{array}{cc|cc} 1 & 1 & & \\ 0 & 1 & & \\ \hline & & 0 & -1 \\ & & 1 & 0 \end{array}\right] \begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{t} \end{bmatrix}$$

end while

Farkas' Lemma **(friendly version)**

Let $\Phi : \begin{cases} a_1\mathtt{x} + a_2\mathtt{y} + a_2\mathtt{z} + a_4\mathtt{t} \geq 0 \\ b_1\mathtt{x} + b_2\mathtt{y} + b_2\mathtt{z} + b_4\mathtt{t} \geq 0 \end{cases}$

Suppose Φ satisfiable, then

$$\forall(\mathtt{x},\mathtt{y},\mathtt{z},\mathtt{t}),\ \Phi \implies c_1\mathtt{x} + c_2\mathtt{y} + c_2\mathtt{z} + c_4\mathtt{t} \geq 0$$

iff there exists $\lambda_1, \lambda_2, \lambda_3 \geq 0$ such that

$$c_i = \lambda_1 a_i + \lambda_2 b_i \quad \text{for } i \in \{1,2,3\}$$

Real Jordan blocks

$\{\boldsymbol{c}' \in \mathbb{R}^2 \mid \exists \boldsymbol{\lambda} \in \mathbb{R}^r_{\geq 0}, \boldsymbol{\ell}'(\boldsymbol{\lambda}, \boldsymbol{c}') = 0\}$

$\times$

Complex Jordan blocks

$\{\boldsymbol{c}'' \in \mathbb{R}^2 \mid c''_1 = 0 \wedge c''_2 = 0\}$

$=$

All blocks

$\{(\boldsymbol{c}', \boldsymbol{c}'')\} \subset \mathbb{R}^4$

Lemma: uniform regions

$(\neq 0\,,\ \cdot\ ) \in Ind_r \Leftrightarrow (1,0) \in Ind_r$

$(=0\,,\ \neq 0) \in Ind_r \Leftrightarrow (0,1) \in Ind_r$

E.g. for the region $(\neq 0\,,\ \cdot\ )$ only check:

$$\exists \boldsymbol{\lambda} \in \mathbb{R}^r_{\geq 0}, \boldsymbol{\ell}'(\boldsymbol{\lambda}, (1,0)) = 0$$

Adapted Farkas lemma

Affine loop

$\mathtt{x} \leftarrow \boldsymbol{a}$

while true do

Assert: h : $c_1\mathtt{x} + c_2\mathtt{y} + c_3\mathtt{z} + c_4\mathtt{t} > 0$

$$\begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{t} \end{bmatrix} \leftarrow \left[\begin{array}{cc|cc} 1 & 1 & & \\ 0 & 1 & & \\ \hline & & 0 & -1 \\ & & 1 & 0 \end{array}\right] \begin{bmatrix} \mathtt{x} \\ \mathtt{y} \\ \mathtt{z} \\ \mathtt{t} \end{bmatrix}$$

end while

Farkas' Lemma (friendly version)

Let $\Phi : \begin{cases} a_1\mathtt{x} + a_2\mathtt{y} + a_2\mathtt{z} + a_4\mathtt{t} \geq 0 \\ b_1\mathtt{x} + b_2\mathtt{y} + b_2\mathtt{z} + b_4\mathtt{t} \geq 0 \end{cases}$

Suppose Φ satisfiable, then

$$\forall(\mathtt{x},\mathtt{y},\mathtt{z},\mathtt{t}),\ \Phi \implies c_1\mathtt{x} + c_2\mathtt{y} + c_2\mathtt{z} + c_4\mathtt{t} \geq 0$$

iff there exists $\lambda_1, \lambda_2, \lambda_3 \geq 0$ such that

$$c_i = \lambda_1 a_i + \lambda_2 b_i \quad \text{for } i \in \{1,2,3\}$$

Real Jordan blocks

$\{\boldsymbol{c}' \in \mathbb{R}^2 \mid \exists \boldsymbol{\lambda} \in \mathbb{R}^r_{\geq 0}, \boldsymbol{\ell}'(\boldsymbol{\lambda}, \boldsymbol{c}') = 0\}$

$\times$

Complex Jordan blocks

$\{\boldsymbol{c}'' \in \mathbb{R}^2 \mid c''_1 = 0 \wedge c''_2 = 0\}$

$=$

All blocks

$\{(\boldsymbol{c}', \boldsymbol{c}'')\} \subset \mathbb{R}^4$

Lemma: uniform regions

$(\neq 0\,,\ \cdot\ ) \in Ind_r \Leftrightarrow (1,0) \in Ind_r$

$(=0\,,\ \neq 0) \in Ind_r \Leftrightarrow (0,1) \in Ind_r$

E.g. for the region $(\neq 0\,,\ \cdot\ )$ only check:

$$\exists \boldsymbol{\lambda} \in \mathbb{R}^r_{\geq 0}, \boldsymbol{\ell}'(\boldsymbol{\lambda}, (1,0)) = 0$$

Theorem

- The difference $\mathrm{Ind}_{r+1} \setminus \mathrm{Ind}_r$ consists of *uniform new regions*.
- There are at most n such regions.

$\Rightarrow$ The sequence $(\mathrm{Ind}_r)_r$ stabilizes after at most n iterations.

Limitations

Outputs of the algorithm

1. $c_1 = 0 \wedge c_2 = 0 \wedge c_3 = 0$
2. $c_1 \neq 0 \wedge c_2 = 0 \wedge c_3 = 0$
3. $c_1 = 0 \wedge c_2 = 0 \wedge c_3 \neq 0$

Limitations

Outputs of the algorithm

$$J = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -\sqrt{\mathbf{2}} & 0 \\ 0 & 0 & \sqrt{\mathbf{2}} \end{pmatrix}$$

1. $c_1 = 0 \wedge c_2 = 0 \wedge c_3 = 0$
2. $c_1 \neq 0 \wedge c_2 = 0 \wedge c_3 = 0$
3. $c_1 = 0 \wedge c_2 = 0 \wedge c_3 \neq 0$

$\boxed{\mathrm{Ind}_0(J)}$

Limitations

Outputs of the algorithm

$$J = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -\sqrt{2} & 0 \\ 0 & 0 & \sqrt{2} \end{pmatrix} \qquad M = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix}$$

1. $c_1 = 0 \wedge c_2 = 0 \wedge c_3 = 0 \implies c_1 = 0 \wedge c_3 - \sqrt{2}c_2 = 0 \wedge c_3 + \sqrt{2}c_2 = 0$
2. $c_1 \neq 0 \wedge c_2 = 0 \wedge c_3 = 0 \implies c_1 \neq 0 \wedge c_3 - \sqrt{2}c_2 = 0 \wedge c_3 + \sqrt{2}c_2 = 0$
3. $c_1 = 0 \wedge c_2 = 0 \wedge c_3 \neq 0 \implies c_1 = 0 \wedge c_3 - \sqrt{2}c_2 = 0 \wedge c_3 + \sqrt{2}c_2 \neq 0$

$\mathrm{Ind}_0(J)$ $\qquad$ $\mathrm{Ind}_0(M)$

Limitations

Outputs of the algorithm

$$J = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -\sqrt{2} & 0 \\ 0 & 0 & \sqrt{2} \end{pmatrix} \qquad M = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix}$$

1. $c_1 = 0 \wedge c_2 = 0 \wedge c_3 = 0 \implies c_1 = 0 \wedge c_3 - \sqrt{2}c_2 = 0 \wedge c_3 + \sqrt{2}c_2 = 0$
2. $c_1 \neq 0 \wedge c_2 = 0 \wedge c_3 = 0 \implies c_1 \neq 0 \wedge c_3 - \sqrt{2}c_2 = 0 \wedge c_3 + \sqrt{2}c_2 = 0$
3. $c_1 = 0 \wedge c_2 = 0 \wedge c_3 \neq 0 \implies c_1 = 0 \wedge c_3 - \sqrt{2}c_2 = 0 \wedge c_3 + \sqrt{2}c_2 \neq 0$

$\mathrm{Ind}_0(J)$ $\qquad$ $\mathrm{Ind}_0(M)$

Remarks

- the coefficients of the relations can be **irrationals**
- we look for rational solutions

Limitations

Outputs of the algorithm

$$J = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -\sqrt{2} & 0 \\ 0 & 0 & \sqrt{2} \end{pmatrix} \qquad M = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix}$$

1. $c_1 = 0 \wedge c_2 = 0 \wedge c_3 = 0 \implies c_1 = 0 \wedge c_3 - \sqrt{2}c_2 = 0 \wedge c_3 + \sqrt{2}c_2 = 0$
2. $c_1 \neq 0 \wedge c_2 = 0 \wedge c_3 = 0 \implies c_1 \neq 0 \wedge c_3 - \sqrt{2}c_2 = 0 \wedge c_3 + \sqrt{2}c_2 = 0$
3. $c_1 = 0 \wedge c_2 = 0 \wedge c_3 \neq 0 \implies c_1 = 0 \wedge c_3 - \sqrt{2}c_2 = 0 \wedge c_3 + \sqrt{2}c_2 \neq 0$

$\boxed{\mathrm{Ind}_0(J)}$ $\qquad$ $\boxed{\mathrm{Ind}_0(M)}$

Remarks

- the coefficients of the relations can be **irrationals**
- we look for rational solutions

The relevant subset — **Blue Pill**

Given an affine system of (in)equations $(l_0, \ldots, l_m) \in \mathbb{R}_{\leq 1}[c_1, \ldots, c_m]$

- decide on the existence of rational solutions
- compute a representation of these solutions

Limitations

Outputs of the algorithm

$$J = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -\sqrt{2} & 0 \\ 0 & 0 & \sqrt{2} \end{pmatrix} \qquad M = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix}$$

1. $c_1 = 0 \wedge c_2 = 0 \wedge c_3 = 0 \implies c_1 = 0 \wedge c_3 - \sqrt{2}c_2 = 0 \wedge c_3 + \sqrt{2}c_2 = 0$
2. $c_1 \neq 0 \wedge c_2 = 0 \wedge c_3 = 0 \implies c_1 \neq 0 \wedge c_3 - \sqrt{2}c_2 = 0 \wedge c_3 + \sqrt{2}c_2 = 0$
3. $c_1 = 0 \wedge c_2 = 0 \wedge c_3 \neq 0 \implies c_1 = 0 \wedge c_3 - \sqrt{2}c_2 = 0 \wedge c_3 + \sqrt{2}c_2 \neq 0$

$\mathrm{Ind}_0(J)$ $\qquad$ $\mathrm{Ind}_0(M)$

Remarks

- the coefficients of the relations can be **irrationals**
- we look for rational solutions

The relevant subset **Blue Pill**

Given an affine system of (in)equations $(l_0, \ldots, l_m) \in \mathbb{R}_{\leq 1}[c_1, \ldots, c_m]$

- decide on the existence of rational solutions
- compute a representation of these solutions

The dual problem **Red Pill**

Compute a (numerical) approximation of the *smallest reachable set:*

$$\{\boldsymbol{a} \in \mathbb{R}^n, f(\boldsymbol{a}) > 0 \text{ for every ind. invariant}\}$$

Conclusion

Equalities

- New methods for computing polynomial invariant up to given degree
- Reduction of general polynomial loop synthesis to system solving NEW!
- Many optimizations remains on ideal computations

Inequalities (Work in Progress)

- More general kind of inductive invariants NEW!
- Several computational methods to compute invariants
- Affine case almost completely solved NEW!