Polynomial invariants by linear algebra

Steven de Oliveira, Saddek Bensalem, Virgile Prevosto

https://arxiv.org/abs/1611.07726

Loop invariants

Parametrized loop: Given $n \in \mathbb{N}_{>0}$

$(x, y, v, w) := (n, 0, 1, 0)$
while $(x > 0)$ **do**
    $x := x - 1$
    $y := y + x$
    $v := v + 1$
    $w := w + v$

Parametrized loop: Given $n \in \mathbb{N}_{>0}$

$$
\begin{array}{l}
(x, y, v, w) := (n, 0, 1, 0) \\
\textbf{while } (x > 0) \textbf{ do} \\
\quad x := x - 1 \\
\quad y := y + x \\
\quad v := v + 1 \\
\quad w := w + v
\end{array}
$$

Orbit

$(n, 0, 1, 0) \rightarrow$
$(n-1, n, 2, 1) \rightarrow$
$(n-2, 2n-1, 3, 3) \rightarrow$
$(n-3, 3n-3, 4, 6) \rightarrow \dots$

Parametrized loop: Given $n \in \mathbb{N}_{>0}$

$$
\begin{aligned}
&(x, y, v, w) := (n, 0, 1, 0)\\
&\textbf{while } (x > 0) \textbf{ do}\\
&\quad x := x - 1\\
&\quad y := y + x\\
&\quad v := v + 1\\
&\quad w := w + v
\end{aligned}
$$

Question

Is there a polynomial $p \in \mathbb{Q}[n][x, y, v, w]$ such that $p(\vec{v}) = 0$ [a] for all $\vec{v} \in \mathit{Orbit}$?

[a] *Identify p as a mapping $p : \mathbb{Q}[n]^4 \to \mathbb{Q}[n]$, by $\vec{v} \mapsto p(\vec{v})$*

Orbit

$(n, 0, 1, 0) \to$
$(n - 1, n, 2, 1) \to$
$(n - 2, 2n - 1, 3, 3) \to$
$(n - 3, 3n - 3, 4, 6) \to \dots$

Parametrized loop: Given $n \in \mathbb{N}_{>0}$

$$
\begin{array}{l}
(x, y, v, w) := (n, 0, 1, 0) \\
\textbf{while } (x > 0) \textbf{ do} \\
\quad x := x - 1 \\
\quad y := y + x \\
\quad v := v + 1 \\
\quad w := w + v
\end{array}
$$

Orbit

$(n, 0, 1, 0) \rightarrow$
$(n-1, n, 2, 1) \rightarrow$
$(n-2, 2n-1, 3, 3) \rightarrow$
$(n-3, 3n-3, 4, 6) \rightarrow \ldots$

Question

Is there a polynomial $p \in \mathbb{Q}[n][x, y, v, w]$ such that $p(\vec{v}) = 0$ [a] for all $\vec{v} \in \mathit{Orbit}$?

[a] *Identify p as a mapping* $p : \mathbb{Q}[n]^4 \rightarrow \mathbb{Q}[n]$, *by* $\vec{v} \mapsto p(\vec{v})$

Answer: yes, some examples

- $p_1(x, y, v, w) = x + v - (n + 1)$
- $p_2(x, y, v, w) = (n + 1)x + y + w - n(n + 1)$
- $p_3(x, y, v, w) = x^2 + x + 2y - n(n + 1)$

Loop invariants

Parametrized loop: Given $n \in \mathbb{N}_{>0}$

$(x, y, v, w) := (n, 0, 1, 0)$
while $(x > 0)$ **do**
    $x := x - 1$
    $y := y + x$
    $v := v + 1$
    $w := w + v$

Orbit

$(n, 0, 1, 0) \to$
$(n-1, n, 2, 1) \to$
$(n-2, 2n-1, 3, 3) \to$
$(n-3, 3n-3, 4, 6) \to \dots$

Question

Is there a polynomial $p \in \mathbb{Q}[n][x, y, v, w]$ such that $p(\vec{v}) = 0$ [a] for all $\vec{v} \in \mathit{Orbit}$?

[a] *Identify p as a mapping* $p : \mathbb{Q}[n]^4 \to \mathbb{Q}[n]$, *by* $\vec{v} \mapsto p(\vec{v})$

Answer: yes, some examples

- $p_1(x, y, v, w) = x + v - (n+1)$
- $p_2(x, y, v, w) = (n+1)x + y + w - n(n+1)$
- $p_3(x, y, v, w) = x^2 + x + 2y - n(n+1)$

Quick check: $p_1(n-3, 3n-3, 4, 6) = (n-3) + 4 - (n+1) = 0$

Goal

Automatic generation of polynomial loop invariants.

Approach

Linear algebra

Goal

Automatic generation of polynomial loop invariants.

Approach

Linear algebra

$(x, y, v, w) := (n, 0, 1, 0)$

while $(x > 0)$ **do**

$x := x - 1$

$y := y + x$

$v := v + 1$

$w := w + v$

$\rightsquigarrow$

Recurrence relation

$\vec{v}_0 = (n, 0, 1, 0)$

$\vec{v}_{n+1} = f(\vec{v}_n)$

$$f(x, y, v, w) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ v \\ w \end{pmatrix} + \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

Invariant generation

Affine mapping

$$f(x,y,v,w) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ v \\ w \end{pmatrix} + \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

Linearization

$$f(x,y,v,w,\mathbb{1}) = \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & -1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \end{array}\right) \begin{pmatrix} x \\ y \\ v \\ w \\ \mathbb{1} \end{pmatrix}$$

General idea paper

Compute invariants, using a linearized version of f.

You might need to introduce more variables

Quadratic assignments

while $(*)$ **do**

$x := x + y^2$

$y := y + 1$

$\rightsquigarrow$

Linearization Let $y_2 = y^2$

while $(*)$ **do**

$x := x + y_2$

$y := y + 1$

$y_2 := y_2 + 2y + 1$

You might need to introduce more variables

Quadratic assignments

while $(*)$ **do**

$$x := x + y^2$$
$$y := y + 1$$

$\rightsquigarrow$

Linearization Let $y_2 = y^2$

while $(*)$ **do**

$$x := x + y_2$$
$$y := y + 1$$
$$y_2 := y_2 + 2y + 1$$

$\Longrightarrow$

$$f(x, y, y_2, \mathbb{1}) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 2 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ y_2 \\ \mathbb{1} \end{pmatrix}$$

Other methods for generating invariants

- Semantic unification
  https://inria.hal.science/hal-04143456/
- Gröbner basis
  https://dl.acm.org/doi/10.1145/1005285.1005324
  https://dl.acm.org/doi/10.1145/964001.964028
- Quantifier elimination in Presburger arithmetic
  https://link.springer.com/article/10.1007/s11424-006-0307-x
- Linear programming: Farkas Lemma
  https://link.springer.com/chapter/10.1007/978-3-540-27864-1_7
  https://link.springer.com/chapter/10.1007/978-3-031-13185-1_13