Formal Characterization and Verification of Loop Invariant Based on Finite Difference

Mengjun Li

School of Computer Science, National University of Defense Technology, Changsha, China

Loop invariants play a major role in software verification. Dynamic approach provides ways to discover likely invariants rapidly. Since the likely loop invariant may not be real, the validity of the likely loop invariants need to be verified. In this paper, we present a formal characterization and a verification approach for equality loop invariants based on finite difference.

The following theorem gives a formal characterization of loop invariants, where $\overline{x} = (x_1, \cdots, x_n)$.

Theorem 1. *$E(\overline{x}) = 0$ is a loop invariant if and only if, for each transition $\tau_i (1 \leq i \leq m)$, $\Delta_{\tau_i} E(\overline{x})$ is 0 or $\Delta_{\tau_i} E(\overline{x}) = 0$ is also a loop invariant.*

Definition 1. *The finite difference tree (FDT) of a likely loop invariant $E(\overline{x}) = 0$ with respect to transitions $\mathcal{T} = \{\tau_1, \cdots, \tau_m\}$ is defined as follows:*

(1)The root is $E(\overline{x})$ and the leaves are values 0;

(2)If the tree contains a non-leaf node $F(\overline{x})$, then $F(\overline{x})$ has m child nodes $\Delta_{\tau_1} F(\overline{x}), \cdots, \Delta_{\tau_m} F(\overline{x})$.

If the FDTs are infinite, theorem 1 can not be used to verify the validity of likely loop invariants. In the following, we presents a practical verification approach for loop invariants.

Definition 2. *Let T be a finite difference tree of a likely loop invariant $E(\overline{x}) = 0$ with respect to transitions $\mathcal{T} = \{\tau_1, \cdots, \tau_m\}$, a node $F(\overline{x})$ in T is called a zero node if $F(\overline{x}) = \sum_{j=0}^{k} p_j(\overline{x}) F_j(\overline{x})$, where $F_j(\overline{x})(j = 0, \cdots, k))$ is the ancestor node of $F(\overline{x})$ and each $F_j(\overline{x})$ satisfies that $F_j(\overline{x_0}) = 0 (j = 0, \cdots, k)$, where $\overline{x_0}$ expresses the initial value of $\overline{x}$, and each $p_j(\overline{x})(j = 0, \cdots, k)$ is an arbitrary function over variables $x_1, \cdots, x_n$.*

Definition 3. *The decidable finite difference tree(DFDT) of a likely loop invariant $E(\overline{x}) = 0$ with respect to transitions $\mathcal{T} = \{\tau_1, \cdots, \tau_m\}$ is the finite difference tree of $E(\overline{x}) = 0$ with respect to transitions $\mathcal{T} = \{\tau_1, \cdots, \tau_m\}$ with zero nodes as leaves.*

Theorem 2. *If there exists a finite DFDT T of $E(\overline{x}) = 0$ with respect to transitions $\mathcal{T} = \{\tau_1, \cdots, \tau_m\}$ and $E(\overline{x_0}) = 0$, then $E(\overline{x}) = 0$ is a loop invariant.*

The effectiveness of our verification approach have been demonstrated on those examples occurring in Laura Kovács's Ph.D.Thesis. We even can prove $f - n! = 0$ is a loop invariant of the program computing the greatest factorial less than or equal to a given N. Note that $f - n! = 0$ is not a polynomial loop invariant, to the best of our knowledge, our work is the first on verifing the validity of non-polynomial loop invariants.