A Logic for Parameterized Octagonal Constraints with $\pm\infty$ [⋆]

Deepak Kapur

Dept. of Computer Science
University of New Mexico
Albuquerque, NM, USA
and
Institue of Software
Chinese Academy of Sciences
Beijing, China
kapur@cs.unm.edu

Abstract

A logic for parameterized octagonal formulas is proposed in which for any pair of distinct variables, atomic formulae are of the form $l_1 \leq \pm x, l_2 \leq \pm x + \pm y$, where l_1, l_2 can be linear expressions in parameters which range over $\mathbb{Z} \cup \{-\infty, \infty\}$ and x, y range over $\mathbb{Z}$. The special constant ∞ ($-\infty$) stands for an octagonal expression not having any upper bound (no lower bound, respectively). Such formulae arise in our recent work on automatically generating octagonal invariants of imperative programs using geometric and local quantifier elimination heuristics. Program invariants are hypothesized as parameterized octagonal formule to mean that octagonal expressions such as $\pm x$ and $\pm x \pm y$ on program variables x, y have parameterized lower (upper) bounds. Of particular importance is the fact that the ordering relation $\leq$ in this logic is not transitive since it allows an octagonal expression such as $u - l$ to have an integer c as the lower bound and another integer d as the upper bound but $d < c$; the above parametric constraints can be satisfied with assignments of ∞ and $-\infty$ for u, v, respectively. All relations including $=$ are translated using $\leq$. A model theoretic semantics as well as an axiomatization for the logic are presented. Satisfiability and validity of the formulas in the logic are defined. An algorithm for computing a satisfying assignment of a satisfiable formula is given. A quantifier elimination method to eliminate program variables from a parameterized octagonal formula universally quantified over program variables is presented. The application of the logic for automatic generation of invariants of imperative programs is discussed.

[⋆] Supported in part by NSF awards CCF-1248069, and DMS-1217054.