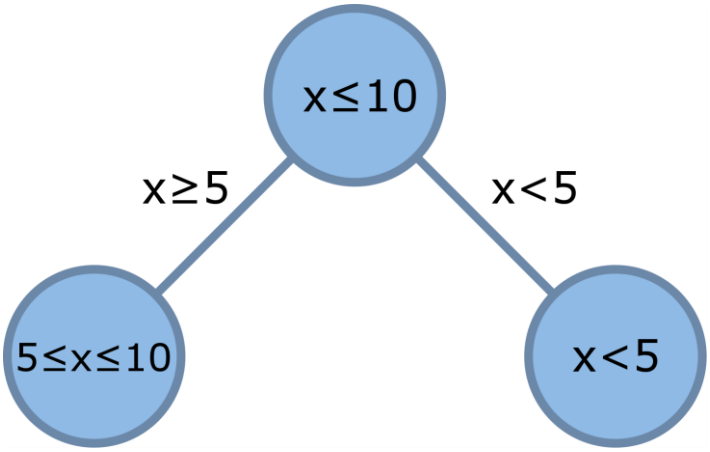
Master's Thesis

Finding Policies for Advanced Control Flow Conditionals

Problem Statement

An important program analysis is the static analysis, which determines, among other information, value sets of variables at program locations without explicitly running the program. An important part of static analysis is handling conditionals (e.g. if (x < 5)) correctly, so that each of the branches of an if, for instance, only receives values that can actually be present during program execution.



Because classical static analysis oftentimes takes a lot of steps, a technique called *policy iteration*[2] was developed, which generates a set of simpler programs with similar behaviour to the original program and uses analysis results from these programs to calculate the result for the actual program.

Task

ARCADE, a program analysis tool for industrial control software developed at i11, already contains a rudimentary implementation for policy iteration on intervals. However, it only works for simple control flow conditionals (e.g. x < 5), but cannot be used for more complex conditionals (e.g. x*y < z+x). Goal of this thesis is to extend the policy iteration in order for it to be able to handle more classes of conditionals on the domain of intervals.

A first approach to this may be linearisation, i.e. replacing the conditionals with linear inequalities that overapproximate them. More advanced approaches may call for a different way of generating the set of simpler programs.

Qualifications

Knowledge of formal methods, especially in the context of static analysis, is greatly appreciated. Since the policy iteration has been implemented in the C++-Version of ARCADE, applicants should be well-versed in programming C++.

Advisor

Marcus Völker, M. Sc. RWTH
voelker@embedded.rwth-aachen.de

[1] Costan, A.; Gaubert, S.; Goubault, E.; Martel, M. & Putot, S. (2005), A Policy Iteration Algorithm for Computing Fixed Points in Static Analysis of Programs., in Kousha Etessami & Sriram K. Rajamani, ed., 'CAV' , Springer, pp. 462-475 .