Title: SIMPAL: A Compositional Reasoning Framework for Imperative Programs

Abstract:

The Static IMPerative AnaLyzer (SIMPAL) is a tool for performing compositional reasoning over software programs that utilize preexisting software components. SIMPAL features a specification language, called Limp, for modeling programs that utilize preexisting components. Limp is an extension of the Lustre synchronous data flow language. Limp extends Lustre by introducing control flow elements, global variables, and syntax specifying preconditions, postconditions, and global variable interactions of preexisting components.

SIMPAL translates Limp programs to an equivalent Lustre representation which can be passed to the JKind model checking tool to perform assume-guarantee reasoning, reachability, and viability analyses. The feedback from these analyses can be used to refine the program to ensure the software functions as intended.