Baxter, James; Cavalcanti, Ana

Algebraic compilation of safety-critical Java bytecode. (English) Zbl 1498.68064


Summary: Safety-Critical Java (SCJ) is a version of Java that facilitates the development of certifiable programs, and requires a specialised virtual machine (SCJVM). In spite of the nature of the applications for which SCJ is designed, none of the SCJVMs are verified. In this paper, we contribute a formal specification of a bytecode interpreter for SCJ and an algebraic compilation strategy from Java bytecode to C. For the target C code, we adopt the compilation approach for icecap, the only SCJVM that is open source and up-to-date with the SCJ standard. Our work enables either prototyping of a verified compiler, or full verification of icecap or any other SCJVM.

For the entire collection see Zbl 1371.68014.

MSC:

68N19 Other programming paradigms (object-oriented, sequential, concurrent, automatic, etc.)
68N20 Theory of compilers and interpreters

Full Text: DOI