Affeldt, Reynald; Kobayashi, Naoki
A Coq library for verification of concurrent programs. (English) Zbl 1278.68152

Summary: Thanks to recent advances, modern proof assistants now enable verification of realistic sequential programs. However, regarding the concurrency paradigm, previous work essentially focused on formalization of abstract systems, such as pure concurrent calculi, which are too minimal to be realistic. In this paper, we propose a library that enables verification of realistic concurrent programs in the Coq proof assistant. Our approach is based on an extension of the π-calculus whose encoding enables such programs to be modeled conveniently. This encoding is coupled with a specification language akin to spatial logics, including in particular a notion of fairness, which is important to write satisfactory specifications for realistic concurrent programs. In order to facilitate formal proof, we propose a collection of lemmas that can be reused in the context of different verifications. Among these lemmas, the most effective for simplifying the proof task take advantage of confluence properties. In order to evaluate feasibility of verification of concurrent programs using this library, we perform verification for a non-trivial application.

For the entire collection see [Zbl 1276.68030].

MSC:
68Q60 Specification and verification (program logics, model checking, etc.)
68Q85 Models and methods for concurrent and distributed computing (process algebras, bisimulation, transition nets, etc.)
68T15 Theorem proving (deduction, resolution, etc.) (MSC2010)

Keywords:
proof assistant; Coq; concurrent programs; pi-calculus

Software:
Isabelle/HOL; Why3; HOL; Pict; Coq

Full Text: DOI

References:
[2] Affeldt, Reynald; Kobayashi, Naoki, Formalization and verification of a mail server in coq, (), 217-233 · Zbl 1033.68502
[3] Affeldt, Reynald; Kobayashi, Naoki, A coq library for verification of concurrent programs, Coq scripts · Zbl 1278.68152