Summary: We consider the broad problem of analyzing safety properties of asynchronous concurrent programs under arbitrary thread interleavings. Delay-bounded deterministic scheduling, introduced in prior work, is an efficient bug-finding technique to curb the large cost associated with full scheduling nondeterminism. In this paper we first present a technique to lift the delay bound for the case of finite-domain variable programs, thus adding to the efficiency of bug detection the ability to prove safety of programs under arbitrary thread interleavings. Second, we demonstrate how, combined with predicate abstraction, our technique can both refute and verify safety properties of programs with unbounded variable domains, even for unbounded thread counts. Previous work has established that, for non-trivial concurrency routines, predicate abstraction induces a highly complex abstract program semantics. Our technique, however, never statically constructs an abstract parametric program; it only requires some abstract-states set to be closed under certain actions, thus eliminating the dependence on the existence of verification algorithms for abstract programs. We demonstrate the efficiency of our technique on many examples used in prior work, and showcase its simplicity compared to earlier approaches on the unbounded-thread Ticket Lock protocol.

For the entire collection see [Zbl 1489.68029].

MSC:

68N30 Mathematical aspects of software engineering (specification, verification, metrics, requirements, etc.)
68N19 Other programming paradigms (object-oriented, sequential, concurrent, automatic, etc.)
68Q85 Models and methods for concurrent and distributed computing (process algebras, bisimulation, transition nets, etc.)

Software:

ACL2s; monabs; veriSoft

Full Text: DOI arXiv

References:


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.