
Zbl 1255.68097

Siegel, Stephen F.

Transparent partial order reduction. (English)

Form. Methods Syst. Des. 40, No. 1, 1-19 (2012). ISSN 0925-9856; ISSN 1572-8102/e

<http://dx.doi.org/10.1007/s10703-011-0126-0>

<http://link.springer.com/journal/volumesAndIssues/10703>

Partial order reduction is a technique used to tackle the state space explosion problem incurring in the verification of multi-component systems. In the interleaving semantics of parallel composition, the parallel execution of two actions from different components yields two different orders of executions in the combined system. In general, the number of different executions is exponential in the number of components.

Partial order reduction identifies combinations of actions from different components that are independent of each other in the sense that considering only one particular order of execution between them does not violate the underlying correctness property. The success of partial order reductions hinges on how effective the process of deciding which actions are independent of each other is. Research in partial order reduction therefore has to provide methods that guarantee non-violence of correctness properties for particular classes of such properties, for instance those that can be defined by stutter-free LTL formulas.

The paper at hand relaxes a well-known so-called invisibility condition which requires the value of no atomic proposition to be changed in transitions whose actions can be considered for partial order reductions. It shows that it is sufficient to require the values of atomic propositions never to change from positive to negative in such transitions for as long as the proposition is only used negatively in the correctness property (and vice-versa). The paper presents the theoretical foundations of this approach and reports some experimental data which show that using the weaker condition can result in stronger partial order reductions.

Martin Lange (Kassel)

Keywords : formal verification; state space explosion; model checking

Classification :

*68Q60 Specification and verification of programs

68Q85 Models and methods for concurrent and distributed computing