Quantitative Analysis of Randomized Distributed Systems and Probabilistic Automata

Christel Baier

Technische Universität Dresden,
Institute for Theoretical Computer Science, Germany

Abstract. The automata-based model checking approach for randomized distributed systems relies on an operational interleaving semantics of the system by means of a Markov decision process and a formalization of the desired event E by an ω-regular linear-time property, e.g., an LTL formula. The task is then to compute the greatest lower bound for the probability for E that can be guaranteed even in worst-case scenarios. Such bounds can be computed by a combination of polynomially time-bounded graph algorithm with methods for solving linear programs. In the classical approach, the "worst-case" is determined when ranging over all schedulers that decide which action to perform next. In particular, all possible interleavings and resolutions of other nondeterministic choices in the system model are taken into account.

As in the nonprobabilistic case, the commutativity of independent concurrent actions can be used to avoid redundancies in the system model and to increase the efficiency of the quantitative analysis. However, there are certain phenomena that are specific for the probabilistic case and require additional conditions for the reduced model to ensure that the worst-case probabilities are preserved. Related to this observation is also the fact that the worst-case analysis that ranges over all schedulers is often too pessimistic and leads to extreme probability values that can be achieved only by schedulers that are unrealistic for parallel systems. This motivates the switch to more realistic classes of schedulers that respect the fact that the individual processes only have partial information about the global system states. Such classes of partial-information schedulers yield more realistic worst-case probabilities, but computationally they are much harder since the semantic model of randomized systems with partial-information schedulers is closely related to probabilistic automata over words. Indeed, a wide range of verification problems that impose conditions on all partial-information schedulers turns out to be undecidable.