

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
UNIVERSITY OF SOUTHERN DENMARK, ODENSE

COMPUTER SCIENCE COLLOQUIUM

Verification and Analysis of Probabilistic Systems

Petr Novotný
Institute of Science and Technology, Austria

Friday, 13 October, 2017 at 12:15

IMADA's Seminar Room

Abstract:

Formal methods have been successfully applied to verify correctness and safety of various computer systems, both hardware and software. The highly anticipated proliferation of intelligent agents, such as self-driving cars or care assistant robots, necessitates verification of a new type of programs: programs containing probabilistic code. This is because controlling software of these agents typically contains some statistical machine-learning code, as well as other probabilistic subroutines, such as stochastic gradient descent or Monte Carlo tree search. However, probabilistic methods are also useful in other application domains, including security, network analysis, or approximate computing, to name a few.

In this talk, I will present several results on formal analysis of probabilistic systems. First, I will focus on proving the fundamental liveness property of probabilistic programs: almost-sure termination. I will present our approach to this problem, which relies on the use of so-called martingales (a construct from probability theory) and which we studied in a series of POPL papers. I will introduce the concept of lexicographic ranking supermartingales and I will show how it can be used to automatically prove almost-sure termination of probabilistic programs of non-trivial control-flow structure. I will also show how to automatically apply martingale-based concentration bounds on probability measure to prove certain quantitative properties of probabilistic code. In the second part of the talk, I will focus on theoretical foundations of probabilistic verification and present our results on decidability and complexity of analysing probabilistic vector addition systems with states (pVASS, equivalent to discrete-time stochastic Petri nets). In this line of work, developed in a series of LICS papers, we discovered counter-examples disproving some classical results about stochastic Petri nets. On the positive note, for a certain class of low-dimensional pVASS, we developed algorithms computing a certain natural characterization of all possible long-run behaviours of a given model.

I will conclude the talk with a presentation of ideas for future research.