Graz University of Technology

Faculty of Computer Science and Biomedical Engineering
IAIK

Prof Roderick Bloem
Inffeldgasse 16a
8010 Graz, AUSTRIA

Tel.: +43 316 873 5580
Fax: +43 316 873 105580

roderick.bloem@iaik.TUGraz.at

DVR: 008 1833 UID: ATU 574 77 929

Report on the Petr Novotný habilitation thesis

Dear Committee:

I have had the pleasure of reading Petr Novotný's habilitation thesis and examining his publication and citation record. Based on my evaluation, I am confident that he is well-deserving of a habilitation.

First, in regards to formal requirements, I was provided with a list of minimal criteria for a habilitation. I have included the research component of this list below and have expanded upon it to highlight Dr. Novotný's exceptional achievements.

	minimum	actual
original results in peer-reviewed international scientific forums	15	26 conference papers and 2 journal papers (according to DBLP)
- from which with IF or equivalent	5	23 (about 13 of which at A* conferences)
number of citations	40	484 (Google, scholar, including self-citations)

These numbers provide a first indication of Dr. Novotný's scientific prowess. He has maintained a consistently high output at top-rated conferences such as POPL, CAV, and LICS, and has developed an impressive body of work over the course of his academic career.

Let me now turn to the content of his scientific work and especially his habilitation thesis. The thesis comprises 9 closely interrelated papers, the majority of which were published in renowned conferences. This work represents a significant advancement in extending system analysis, which previously had been primarily focused on non-probabilistic systems, to probabilistic systems. Probabilistic systems provide a natural abstraction for systems in which some aspects are unknown or cannot be accurately modeled. Throwing dice is a stereotypical example, but the behavior of any multi-tasking or networked computer system can be approximated using probabilities. In addition, probabilities are utilized in specific algorithms to enhance security or achieve high performance. Probabilities make the analysis of systems much more complicated and give rise to entirely new questions that have no counterpart in the non-probabilistic setting.

The thesis is divided into two conceptual parts. The first part focuses on almost sure termination of programs using a mathematical construct called martingales. For non-probabilistic programs, the question of termination is straightforward: either the program terminates for all inputs, or it

does not. However, for probabilistic programs, more subtle questions about termination arise, and the first part of the thesis provides a thorough examination of these questions. It initially explores almost sure termination and termination in finite expected time, and extends existing results from a one-player setting to a two-player setting with "angelic" and "demonic" non-determinism. (The two-player version of the question asks if termination can be guaranteed by making the right choices at certain points in the program.) The thesis demonstrates that the existence of a specific type of martingale is sufficient to construct proofs for both almost-sure termination and finite expected termination time. It also establishes that constructing such martingales is an NP-hard problem

The thesis then addresses a more detailed version of the termination problem, which asks if we can provide a lower bound on the termination time. To solve this problem, the thesis introduces the new notion of a “stochastic invariant”. It then introduces lexicographic martingales, which are useful in proving termination of systems with constructs like nested loops. The thesis further extends the types of martingales that can be used and, as a result, the types of programs that can be analyzed. Finally, the thesis presents a convincing argument showing that similar techniques can be used to prove non-termination of systems. This part of the thesis offers a thorough investigation of the mathematics underlying the various notions of termination of probabilistic systems and how to compute proofs. The subtle aspects of these issues, when coming from a non-probabilistic perspective, mean that a careful and rigorous treatment of the topic is necessary, and the thesis indeed provides that. I was surprised by several statements on the relation between different notions of probabilistic termination, emphasizing the importance of the thesis's rigor.

The second part of the thesis focuses on a controller synthesis problem, specifically partially observable Markov decision processes (POMDPs), which are probabilistic systems with two players and incomplete information about the system's state. The partial observability adds another layer of complexity to the analysis. While the formalism of POMDPs is standard, the questions asked are novel and challenging. The first question the thesis addresses is how to optimize the expected quality of system runs, given a quality measure, subject to preventing disastrous behavior. The thesis proposes a two-step process of eliminating unwanted behavior and then optimizing the remaining system to solve this problem. The second question the thesis considers is how to make the disastrous behavior unlikely, given a bound on acceptable probability. The thesis shows that the previous solution cannot be easily adapted, and instead proposes a heuristic approach that works well in practice. Finally, the thesis investigates a restricted subset of the same problem that can be solved much more efficiently.

The thesis consists of a summary of the results followed by a reprint of published papers. As stated above, the 60 or so pages of introduction are a true pleasure to read. They give an easily accessible introduction to the field based, including an excellent historical treatise of its development and a gentle explanation of the most important results, without losing mathematical rigor. Considering the non-trivial mathematical nature of the results, the clarity and accessibility of the introduction is a testament to the applicant's didactic ability.

I am highly impressed by the level of mathematical rigor demonstrated in the thesis, which addresses challenging problems in a domain where intuitive reasoning is not always effective. The author's ability to prove intricate results is commendable, given the complexity of the problems addressed. Additionally, the author demonstrates a keen sense of selecting pertinent

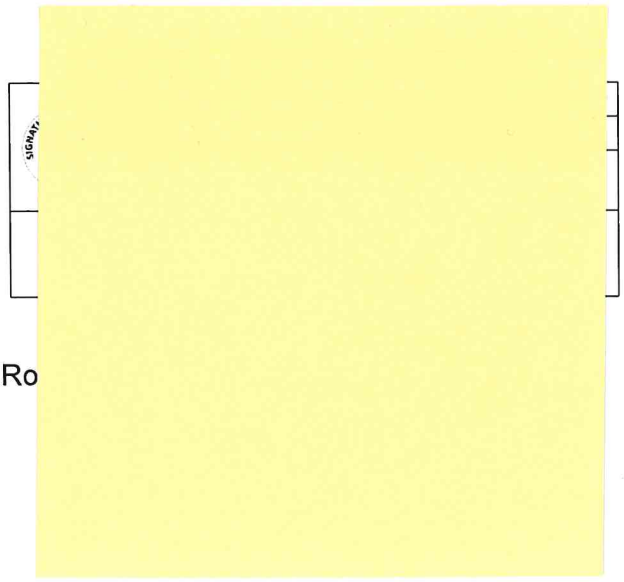
problems to solve. The motivation for most questions is derived from simple probabilistic programs with behaviors that are not satisfactorily captured by existing techniques, thus emphasizing the combination of theoretical depth and practical application. Furthermore, the inclusion of implementation and experimental evaluations for some of the results highlights the practical relevance of the research.

The thesis includes a statement of contribution for each of the nine papers that are included. While Krishnendu Chatterjee is listed as a co-author on all papers, the author's DBLP page shows a varied set of co-authors. It is customary in theoretical computer science for authors to be listed in alphabetical order. The statement of contribution clearly demonstrates that the applicant has been a central contributor to each paper, originating the main idea of five papers and contributing equally to the rest. This highlights the applicant's strong research capabilities and his ability to make significant contributions to collaborative research

In conclusion, I am extremely impressed by Petr Novotný's research. He has clearly demonstrated that he is an excellent researcher in theoretical computer science, who is able to develop novel ideas with relevant motivations and rigorous mathematical content, accompanied by implementations where applicable. His ability to communicate difficult ideas in a surprisingly accessible manner will serve him well in his research and teaching career. His habilitation thesis and his track record leave no doubt that he has the credentials to pursue an academic career and would be a very competitive candidate for a professorship at any university.

Thus, the habilitation thesis entitled “Code and Design Safety of Probabilistic Systems” by RNDr. Petr Novotný, Ph.D., **fulfills** the requirements expected of a habilitation thesis in the field of informatics.

Yours sincerely,



Ro