MASARYKOVA UNIVERZITA

Annex No. 11 to the MU Directive on Habilitation Procedures and Professor Appointment Procedures

# Habilitation Thesis Reviewer's Report

| | |
|---|---|
| **Masaryk University** | |
| **Faculty** | Faculty of Informatics |
| **Procedure field** | Informatics |
| **Applicant** | RNDr. Vojtěch Řehák, Ph.D. |
| **Applicant's home unit, institution** | Faculty informatics, Masaryk University |
| **Habilitation thesis** | Stochastic Real-Time Systems: Parameter Synthesis and Games |
| **Reviewer** | Prof. **Marta Zofia Kwiatkowska** |
| **Reviewer's home unit, institution** | Department of Computer Science, University of Oxford, UK |

The candidate's habilitation thesis is focused on rigorous modelling and correctness of stochastic real-time systems, which underpin the design of a wide variety of software and hardware systems, including computer networks with unreliable communication channels, security protocols, and air traffic control systems. Two important problems are studied, firstly whether the system model satisfies a given specification, and secondly whether one can automatically synthesise near-optimal values for system parameters (for example time delays) so that a given objective is satisfied. The modelling scenario adopted for the habilitation considers model variants which combine stochastically distributed time delays with fixed time delays, both for continuous time and discrete distributions, and non-deterministic choice that corresponds to decisions as to which action to take. Such a scenario is particularly challenging in view of the intricate interaction between different types of time delays and non-determinism.

Formally, the model variants are subclasses of the classical model of Generalised Semi-Markov Processes (GSMPs), formed by placing certain restrictions that may limit their expressive power but enhance tractability of the corresponding analysis. The Preliminaries chapter explains the model classes and their relationship in a concise and accessible manner. Following this, the research contributions are presented as five thematic blocks, based on eleven published papers, co-authored by Dr Rehak's students and colleagues, as well as international collaborators.

Block1 focuses on analysing the long-run behaviour of general GSMPs, which allow both stochastic variable-delay events, as well as fixed-delay events, in terms of state visit and time frequency. Such models were already studied in 1990s in the form of stochastic timed automata, and algorithms were proposed for their verification based on analysis of the underlying region graph. Remarkably, Dr Rehak was able to show that these algorithms contained a fundamental error, since a combination of variable- and fixed-delay events can lead to instability, and fix the problem by restricting the model class. This is a highly novel and important contribution, which also applies to other model classes, for example stochastic Petri nets.

Block 2 introduces a novel generalisation of GSMPs to two-player Generalised Semi-Markov Games (GSMGs), which are important in applications such as security (attacker versus defence). The specification formalism employed in this case is a deterministic time automaton (TA) which monitors the timing constraints. An exponential-time algorithm is presented for deciding and, if it exists, constructing a strategy that meets the TA specification.

Block 3 is concerned with Interactive Markov Chains (IMC), a model that permits non-determinism as well as continuous distributions, and develops an open IMC model in which two kinds of non-determinism (decision) are allowed, internal and external. Dr Rehak reduces the problem of synthesising optimal control for time-bounded reachability to a two-player game, and proposes an approximate algorithm to synthesise an $\varepsilon$-optimal controller by employing discretisation, for an arbitrarily small $\varepsilon$. This is a non-trivial and important algorithm that enables compositional analysis, which has already been applied in fault-tree analysis.

Block 4 deals with parametric CTMC models that may contain one fixed delay, and then synthesising $\varepsilon$-optimal parameter values for time delays given as objectives expected cumulative rewards. An exponential-time algorithm is proposed and implemented as an extension of the PRISM model checker; the algorithm is then significantly improved by reducing the search space based on computing symbolic derivatives of the objective function using Maple. An extension of the framework is also proposed for long-run average reward objectives. This work has been demonstrated to have high relevance in practice.

The final 5$^{th}$ block presents a novel problem formulation, that of resilience for MDPs, and studies the complexity of the corresponding decision problems.

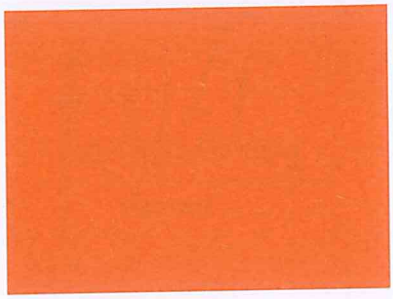
The research contributions are presented in leading conferences (notably CONCUR, HSCC, ATVA and QEST). In computer science, conferences are the main dissemination medium and are often more competitive than journals. The results contain a blend of foundational research, notably novel problem formulations, together with algorithmic contributions and their complexity analysis, and finally also software tool implementation. The results are highly original and non-trivial, and are of major importance for the rigorous specification and design of computerised systems. Importantly, they have already been taken up and/or significantly influenced the field of study, as indicated by citations and mention in survey and handbook chapters, and have opened up a number of new avenues for future work.

**Reviewer's questions for the habilitation thesis defence** (number of questions up to the reviewer)

1. Comment on the feasibility of the method of article P3 in practice, given that it is based on the region graph which is exponential. Would a zone-based approach, which is typically employed in real-time verification tools, be applicable in order to improve efficiency of the algorithm?
2. Can one employ Metric Temporal Logic instead of timed automata as specifications in the method introduced in article P1?
3. Can GSMGs be generalised to multi-player games? What issues would arise, if any?
4. It would be interesting to study equilibria for GSMGs.

**Conclusion**

The habilitation thesis entitled "*Stochastic Real-Time Systems: Parameter Synthesis and Games*" by Vojtěch Řehák ***fulfils*** requirements expected of a habilitation thesis in the field of Informatics.



In Oxford on 11th March 2019