Review for Dissertation „Behavior Protocols Extensions“, by Mr Jan Kofron

Summary

The proposed PhD thesis presents an extension of the Behavioral Protocols (BP) approach of contract checking of component-based based on finite state machines. The presented language Extended BP (EBP) does not only lift the abstraction level of the BP specifications, but speeds up efficiency and memory consumption by a translation to the SPIN model checker.

Problem

Contracts with finite state machines are decidable, i.e., are of uttermost importance to component-based software engineering, as can be seen by their recent industrial exploitation in the Microsoft SLAM device driver checker. Since raw automata or CSP specifications are a bit messy to specify, language abstractions are needed that simplify the specifications of contracts and improve the acceptance of the method in practice. That is also the goal of the thesis, to improve the usability of the BP method, by adding abstractions to it.

Outline of Thesis

Chapter 1 gives a clear introduction to the topic and specifies problems and goals explicitly. It also mentions several publications of the author.

Chapter 2 considers all relevant component models, among which are SOFA, Fractal, BP, CCS. Also modeling languages such as Promela or Tracta are handled. This chapter alone is a very nice overview that deserves publication elsewhere.

Chapter 3 presents the extensions of BP, which are local variables, method parameters, multisynchronization (synchronization barriers between several automata) and control flow constructs (while, switch). Section 3.4 gives an informal semantics by mapping the extended constructs to BP or, as is the case for the consent operator of EBP, to NFAA.
Chapter 4 presents the translation to Promela, the input language of SPIN. From the EBP specification, first a NFAA is generated, then a DFAA, then Promela. Communication between automata is not modeled with Promela channels but shared variables, so that the deadlock checker can detect communication errors. Method parameters are mapped to global data. Multisynchronization events are modeled with shard variables. An example concludes the chapter.

Chapter 5 first evaluates the EBP language and verification approach in comparison with the BP system, then compares it with competing approaches. As an example, an architectural specification of the CoCoME project is used. The EBP specifications are slightly shorter and more expressive (which was to be expected). More interesting is the time for verification, where the translation approach verifies the problem in half the time (plus translation time). Also some more properties of the specification can be checked by SPIN.

Chapter 6 wraps up the work.

Scientific Merits

The proposed PhD thesis contains the following scientific merits:

1. Definition of language extensions to a specification language for behavioral protocols (method parameters, simple data structures, multisynchronization events).
2. Mapping of this language to Promela/SPIN.
3. Evaluation of the mapping in terms of verification speed.
4. The comparison with related work shows that with EBP and the EBP translator, an excellent approach for a real expressive, verifiable contract checking language has been engineered.

The work also has some weaknesses:

1. The mapping (translational semantics) of the compilation process to Promela is not formally specified, e.g., with a denotational or natural semantics.
2. The evaluation benchmark is rather small, and does not really reveal the improved expressivity of the EBP language.
3. I would have expected more plans for the future, how the EBP translator will cope with the disadvantage of additional translation time. The argument may be irrelevant for large specifications, but since the translation is probably not linear, there should have been some complexity or efficiency considerations.
4. Although the comparison with the related work discusses the advantages of the method, the progress is not very well highlighted elsewhere in the work.

The work is easy to read, well-structured, and contains sufficient examples. I did not find many typing errors.

Evaluation

Because of the scientific progress, I suggest to accept Mr Kofron's PhD thesis proposal. Despite the weaknesses, the work does contain important improvements for the specification of behavioral protocols and, as a whole, is a well-written overview for this research area. Hence, I grade the work still as 5 (excellent).