Compositional coordinator synthesis for discrete event systems

Compositional coordinator synthesis for discrete event systems

M.A. Goorden
Eindhoven University of Technology
The Netherlands
Email: m.a.goorden@tue.nl

M. Fabian
Chalmers University of Technology
Sweden

M.A. Reniers
TU/e
The Netherlands

J.M. van de Mortel-Fronczak
TU/e
The Netherlands

W.J. Fokkink
Vrije Universiteit
The Netherlands

J.E. Rooda
TU/e
The Netherlands

1 Introduction

The development complexity of high-tech systems has increased due to increasing market demand for verified safety, shorter time-to-market, and better performance. Model-based systems engineering approaches provide advantages for supervisory controller design. We consider discrete-event systems modeled by extended finite automata (EFAs) for which supervisory controllers need to be developed. The supervisory control theory of Ramadge-Wonham provides an approach to synthesize supervisors such that the controlled behavior of the system is restricted to specified behavior [1].

One of the major drawbacks of synthesizing supervisory controllers is the state-space explosion problem. There exist multiple attempts to overcome the computational difficulties. Among them, several divide-and-conquer strategies can be found, such as modular, hierarchical, decentralized, and multilevel supervisor architectures.

A set of supervisors, for example obtained with modular supervisory control synthesis, may be conflicting, which gives rise to global blocking of the system. Therefore, a nonblocking verification should be performed on the set of supervisors. In case a conflict is identified, a so-called coordinator needs to be synthesized. The current approach in the literature still suffers from the state-space explosion problem [2].

2 Result

Figure 1 shows our approach to efficiently synthesize a coordinator. It utilizes compositional nonblocking verification of [3]. The key idea of our compositional approach is to reduce the state space to the essence of the blocking issue.

The approach works as follows: first a sequence of abstractions is deployed to rewrite and simplify the EFA-based system models into a single one while maintaining the nonblocking property, then a coordinator is synthesized for the single automaton model, and finally this coordinator is refined to let it control the original system. The approach ensures that the closed-loop behavior of the refined coordinator and the original system is the same as the closed-loop behavior of a coordinator obtained with monolithic synthesis.

We have proven for ten different abstractions (in combination with their refinements) that they are coordinator equivalent, allowing them to be used in this compositional approach. Examples of these abstractions are partial composition, variable unfolding, and event merging.

Acknowledgement

This work is supported by Rijkswaterstaat, part of the Ministry of Infrastructure and Water Management of the Government of The Netherlands.

References

[1] P.J.G. Ramadge and W.M. Wonham, "Supervisory Control of a Class of Discrete Event Processes," SIAM Journal on Control and Optimization, Vol. 25, 1, 206–230, 1987.

[2] R. Su and J.H. van Schuppen and J.E. Rooda, "Synthesize nonblocking distributed supervisors with coordinators," 17th Mediterranean Conference on Control and Automation, 1108–1113, 2009.

[3] S. Mohajerani and R. Malik and M. Fabian, "A framework for compositional nonblocking verification of extended finite-state machines," Discrete Event Dynamic Systems, Vol. 26, 1, 33–84, 2016.

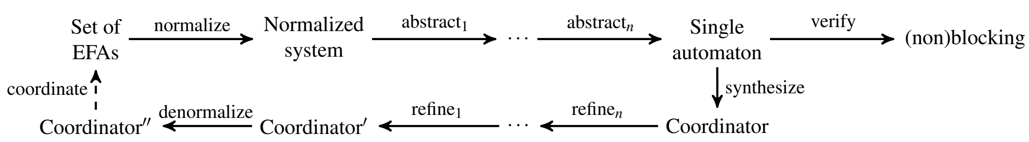

Figure 1: The top row represents the compositional nonblocking verification of [3]. In this work, we propose the addition of the bottom row: synthesize a coordinator based on the single, simplified automaton and then refine this coordinator back to the original system.