Formal Methods in Computer-Aided Design 2021

Reactive Synthesis Beyond Realizability

Rayna Dimitrova
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany
dimitrova@cispa.de

***Abstract*—The automatic synthesis of reactive systems from high-level specifications is a highly attractive and increasingly viable alternative to manual system design, with applications in a number of domains such as robotic motion planning, control of autonomous systems, and development of communication protocols. The idea of asking the system designer to describe what the system should do instead of how exactly it does it, holds a great promise. However, providing the right formal specification of the desired behaviour of a system is a challenging task in itself. In practice it often happens that the system designer provides a specification that is unrealizable, that is, there is no implementation that satisfies it. Such situations typically arise because the desired behavior represents a trade-off between multiple conflicting requirements, or because crucial assumptions about the environment in which the system will execute are missing. Addressing such scenarios necessitates a shift towards synthesis algorithms that utilize quantitative measures of system correctness. In this tutorial I will discuss two recent advances in this research direction.**

First, I will talk about the maximum realizability problem, where the input to the synthesis algorithm consists of a hard specification which must be satisfied by the synthesized system, and soft specifications which describe other desired, possibly prioritized properties, whose violation is acceptable. I will present a synthesis algorithm that maximizes a quantitative value associated with the soft specifications, while guaranteeing the satisfaction of the hard specification. In the second half of the tutorial I will present algorithms for synthesis in bounded environments, where a bound is associated with the sequences of input values produced by the environment. More concretely, these sequences consists of an initial prefix followed by a finite sequence repeated infinitely often, and satisfy the constraint that the sum of the lengths of the initial prefix and the loop does not exceed a given bound. I will also discuss the synthesis of approximate implementations from unrealizable specifications, which are guaranteed to satisfy the specification on at least a specified portion of the bounded-size input sequences. I will conclude by outlining some of the open avenues and challenges in quantitative synthesis from temporal logic specifications.

This tutorial is based on joint work with Mahsa Ghasemi and Ufuk Topcu published in [1], [2], and with Bernd Finkbeiner and Hazem Torfah published in [3].

References

[1] R. Dimitrova, M. Ghasemi, and U. Topcu, “Reactive synthesis with maximum realizability of linear temporal logic specifications,” *Acta Informatica*, vol. 57, no. 1-2, pp. 107–135, 2020.

[2] ——, “Maximum realizability for linear temporal logic specifications,” in *Automated Technology for Verification and Analysis - 16th International Symposium, ATVA 2018, Los Angeles, CA, USA, October 7-10, 2018, Proceedings*, ser. Lecture Notes in Computer Science, S. K. Lahiri and C. Wang, Eds., vol. 11138. Springer, 2018, pp. 458–475.

[3] R. Dimitrova, B. Finkbeiner, and H. Torfah, “Synthesizing approximate implementations for unrealizable specifications,” in *Computer Aided Verification - 31st International Conference, CAV 2019, New York City, NY, USA, July 15-18, 2019, Proceedings, Part I*, ser. Lecture Notes in Computer Science, I. Dillig and S. Tasiran, Eds., vol. 11561. Springer, 2019, pp. 241–258.

https://doi.org/10.34727/2021/isbn.978-3-85448-046-4_1