Formal Methods in Computer-Aided Design 2020

From Correctness to High Quality

Orna Kupferman
School of Computer Science and Engineering
The Hebrew University
Jerusalem, Israel

Abstract

In the synthesis problem, we are given a specification ψ over input and output signals, and we synthesize a system that realizes ψ: with every sequence of input signals, the system associates a sequence of output signals so that the generated computation satisfies ψ. The above classical formulation of the problem is Boolean. The talk surveys recent efforts to automatically synthesize reactive systems that are not only correct, but also of high quality. Indeed, designers would be willing to give up manual design only after being convinced that the automatic procedure that replaces it generates systems of comparable quality.

We distinguish between *behavioral quality*, which refers to the way the specification is satisfied, and *costs*, which refer to resources that the system consumes. For the first, we focus on the temporal logics $\mathrm{LTL}[\mathcal{F}]$ and $\mathrm{LTL}[\mathcal{D}]$, which extend LTL by quality operators [1]. The satisfaction value of $\mathrm{LTL}[\mathcal{F}]$ and $\mathrm{LTL}[\mathcal{D}]$ formulas is a real value in $[0, 1]$, where the higher the value is, the higher is the quality in which the computation satisfies the specification. Essentially, $\mathrm{LTL}[\mathcal{F}]$ contains *propositional quality operators*, like weighted-average, and $\mathrm{LTL}[\mathcal{D}]$ contains *discounted eventuality operators*. Using $\mathrm{LTL}[\mathcal{F}]$ and $\mathrm{LTL}[\mathcal{D}]$, a designer can prioritize different ways to satisfy the specification and formally weight parameters such as security, maintainability, runtime, delays, and more.

For the second, we distinguish between four classes of costs, induced by the following two characteristics: (1) *construction* vs. *activaty* costs, and (2) *physical* vs. *monetary* costs. For example, the sensing cost of a system is physical, and we distinguish between the number of sensors in the system (construction cost) and the sensing required during its operation (activity cost) [2], [3].

Index Terms

Synthesis, Temporal Logic, Sensing

References

[1] S. Almagor, U. Boker, and O. Kupferman. Formalizing and reasoning about quality. *Journal of the ACM*, 63(3), 2016.
[2] S. Almagor, D. Kuperberg, and O. Kupferman. Sensing as a complexity measure. *Int. J. Found. Comput. Sci.*, 30(6-7):831–873, 2019.
[3] K. Chatterjee, R. Majumdar, and T. A. Henzinger. Controller synthesis with budget constraints. In *Proc 11th International Workshop on Hybrid Systems: Computation and Control*, volume 4981 of *Lecture Notes in Computer Science*, pages 72–86. Springer, 2008.

Supported in part by the Israel Science Foundation, grant No. 2357/19.

https://doi.org/10.34727/2020/isbn.978-3-85448-042-6_5

This article is licensed under a Creative Commons Attribution 4.0 International License