講演番号 252

文献番号 20225252

Blackbox Analysis of Automotive Systems by Logic and Optimization

Software Science Approaches to Efficiency and Deployability

Ichiro Hasuo[1,5] **Masaki Waga**[2,1] **Zhenya Zhang**[3] **Étienne André**[4] **Paolo Arcaini**[1]
Fuyuki Ishikawa[1] **Masaaki Konishi**[1] **James Haydon**[1]

1) National Institute of Informatics
Hitotsubashi 2-1-2, Tokyo 101-8430, Japan. (E-mail: {hasuo, arcaini, f-ishikawa, konishi, jhaydon}@nii.ac.jp)
2) Graduate School of Informatics, Kyoto University
Yoshida-Honmachi 36-1, Kyoto 606-8501, Japan. (E-mail: mwaga@fos.kuis.kyoto-u.ac.jp)
3) School of Computer Science and Engineering, Nanyang Technological University
50 Nanyang Avenue, Singapore 639798. (E-mail: zhenya.zhang@ntu.edu.sg)
4) LORIA, Université de Lorraine
54506 Vandœuvre-lés-Nancy, France. (E-mail: Etienne.Andre@loria.fr)
5) SOKENDAI (The Graduate University for Advanced Studies), Japan

KEY WORDS: Safety, intelligent vehicle, test/evaluation, safety assurance, software

We present latest results in the software science research towards safety analysis and performance tuning of automotive systems. Our focus is on blackbox analysis techniques that do not require whitebox modeling of target systems' internal working. We present 1) the benefit of combining formal logic and numeric optimization, 2) enhanced efficiency by logical division of problems, and 3) scientific results that enable flexibility and thus improve deployability of those blackbox techniques.

Use of techniques from software science in real-world automotive applications is sought by the authors and their colleagues, in the context of JST ERATO HASUO Metamathematics for Systems Design Project (ERATO MMSD, 2016–2025). An emphasis is on the collaboration of rigorous reasoning (as in formal verification) and statistical/numerical reasoning (as in testing and ML).

The approaches in this direction include *automata-based monitoring* [1], *gradual verification via model refinement* [2], *model learning* [3], [4], etc. These approaches have been explained in the *ERATO MMSD Seminar Series for Automotive Industry* towards industry practitioners. In this summarized paper, we focus on one example, namely optimization-based falsification.

Problem 1 (falsification):

- *Given:*
  - A black-box system model $\mathcal{M}$, typically given by a Simulink model. Being black-box means that its internal structure need not be observable—it is enough that the input and output correspondence is observable. See Fig. 1.
  - A specification φ (typically given by a logical formula in *signal temporal logic (STL)*)
- *Answer:* an input signal σ to the system, called a *falsifying input* or a *counterexample*, so that the corresponding output signal $\mathcal{M}(\sigma)$ violates the specification φ.

The falsification problem is therefore a testing problem: it does not aim at a guarantee of the *absence* of errors. In real-world design and safety assurance scenarios, however, a concrete counterexample discovered in falsification is very much appreciated—it reveals a concrete fault of the system and suggests a hint to fix it.

The key idea here is to change the truth values of logical formulas, from the conventional two-valued semantics ("true" vs. "false"), to real numbers. The latter is often amenable to efficient search by gradient descent. See Fig. 2.

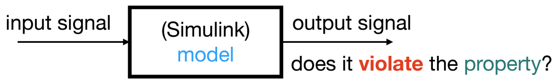

Fig. 1. the falsification problem

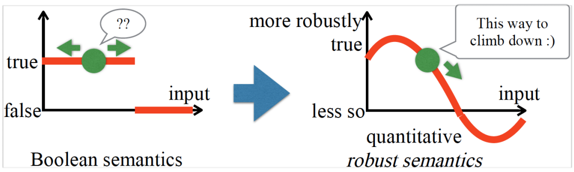

Fig. 2. quantitative robustness semantics

The technique of optimization falsification originated in [5], where the quantitative robustness for the logic STL is introduced together with the above falsification workflow. There are some mature tools available, including Breach[1] and S-Taliro[2]. Applications in industrial contexts have been reported by Toyota, Airbus, and Bosch.

References

[1] M. Waga, É. André, and I. Hasuo, "Symbolic monitoring against specifications parametric in time and data," in *CAV 2019.* https://doi.org/10.1007/978-3-030-25540-4_30

[2] T. Kobayashi and F. Ishikawa, "Analysis on strategies of superposition refinement of event-b specifications," in *ICFEM 2018.* https://doi.org/10.1007/978-3-030-02450-5_21

[3] M. Waga, "Falsification of cyber-physical systems with robustness-guided black-box checking," in *HSCC'20.* https://doi.org/10.1145/3365365.3382193

[4] T. Okudono, M. Waga, T. Sekiyama, and I. Hasuo, "Weighted automata extraction from recurrent neural networks via regression on state spaces," in *AAAI 2020.* http://arxiv.org/abs/1904.02931

[5] G. E. Fainekos and G. J. Pappas, "Robustness of temporal logic specifications for continuous-time signals," *Theor. Comput. Sci.*, vol. 410, no. 42, pp. 4262–4291, 2009. [Online]. Available: http://dx.doi.org/10.1016/j.tcs.2009.06.021

[1] `github.com/decyphir/breach`
[2] `sites.google.com/a/asu.edu/s-taliro/s-taliro`

2022 JSAE Annual Congress (Spring) - Summarized Paper
Issued on May 20, 2022