Affine Encodings for Optimal Monitoring of Temporal Properties under Uncertain Observation

Martin Fränzle[1]

Carl von Ossietzky Universität Oldenburg
Dpt. of CS, Foundations and Applications of Systems of Cyber-Physical Systems
26111 Oldenburg, Germany
martin.fraenzle@uol.de

Keywords: Temporal logic; Online monitoring; Uncertain information; Partial observation; Affine encodings

Introduction

State estimation in a dynamic system subject to uncertain state observation, where uncertainties can be both aleatoric due to noisy measurements and epistemic due to partial observation, is a classical problem. Optimal state estimation algorithms [6] can provide as precise as possible verdicts on state conditions, answering questions like whether the current position of a drone violates a geo-fencing condition. Many interesting safety properties of interacting cyber-physical agents are, however, more complex than state conditions, calling for specification as a durational property in an adequate temporal logic [5, 4]. This provokes the quest for optimal, in the sense of as precise as possible, monitoring algorithms evaluating properties expressed in temporal logic based on noisy and incomplete, i.e. uncertain sensory information.

[1]joint work with Bernd Finkbeiner (CISPA Helmholtz Center for Information Security; Stuhlsatzenhaus 5, 66123 Saarbrücken, Germany), Florian Kohn (CISPA Helmholtz Center for Information Security), and Paul Kröger (Carl von Ossietzky Universität Oldenburg, Foundations and Applications of Systems of Cyber-Physical Systems,)

Results

In this talk, we will demonstrate that contrary to common belief, optimal monitoring under uncertainty cannot be achieved by first applying optimal state estimation and then evaluating the temporal logic property in question upon this sequence of as precise as possible state estimates. Based on the indicative example of Signal Temporal Logic (STL) [4], a linear-time temporal logic specifically designed for classifying the time-dependent signals originating from continuous-state or hybrid-state dynamical systems according to formal specifications, we demonstrate that more precise statements can be computed based on affine-arithmetic encodings of STL semantics. For this, we first define the pertinent notion of precision, namely that verdicts provided by a monitor ought be sound (yield 'true' or 'false' only if *all* ground-truth trajectories consistent with the uncertain measurements satisfy, or violate, resp., the property of interest) and informative (monitoring yields 'inconclusive' only if some ground-truth trajectories consistent with the uncertain measurements satisfy and other consistent ones violate the property of interest).

In a setting where measurements are subject to both an interval-bounded per-sample error and an unknown, yet fixed offset, sequential execution of optimal state estimation and STL evaluation yields a sound, yet not an informative monitoring algorithm. That means that this combination sometimes fails to provide conclusive verdicts though these would be adequate. For the model-free as well as for the linear model-based case of dynamic system monitoring, we then provide precise, i.e. sound and informative, evaluation algorithms based on affine arithmetic [2] and SAT modulo theory solving over linear arithmetic [7, 1]. We prove preciseness of these algorithms in the cases of interval-bounded measurement noise and, when a linear system model is provided, partial observation.

For full constructions and proofs, we refer the reader to [3].

References

[1] A. Cimatti, A. Griggio, B. Schaafsma, and R. Sebastiani. The MathSAT5 SMT Solver. In N. Piterman and S. Smolka, editors, *TACAS 2013*, volume 7795 of *Lecture Notes in Computer Science*. Springer, 2013.

[2] L. H. de Figueiredo and J. Stolfi. Affine arithmetic: Concepts and applications. *Numerical Algorithms*, 37(1-4):147–158, 2004.

[3] B. Finkbeiner, M. Fränzle, F. Kohn, and P. Kröger. A truly robust signal temporal logic: Monitoring safety properties of interacting cyber-physical systems under uncertain observation. *Algorithms*, 15(4):126, 2022.

[4] O. Maler and D. Nickovic. Monitoring temporal properties of continuous signals. In Y. Lakhnech and S. Yovine, editors, *FORMATS and FTRTFT 2004*, volume 3253 of *Lecture Notes in Computer Science*. Springer, 2004.

[5] Z. Manna and A. Pnueli. *The temporal logic of reactive and concurrent systems - specification*. Springer, 1992.

[6] P. S. Maybeck. *Stochastic models, estimation, and control*, volume 141 of *Mathematics in Science and Engineering*. 1979.

[7] S. A. Wolfman and D. S. Weld. The lpsat engine & its application to resource planning. In *IJCAI'99 - Volume 1*, page 310–316. Morgan Kaufmann Publishers Inc., 1999.