

# Parametrization of Symbolic Control Envelopes of Cyber-Physical Systems

Sam Sami<sup>[0009-0002-1099-1701]</sup> and Stefan Mitsch<sup>[0000-0002-3194-9759]</sup>

School of Computing, DePaul University, Chicago, IL, USA  
msami4@depaul.edu smitsch@depaul.edu

**Keywords:** Cyber-Physical Systems, Runtime Verification

## Abstract

The KeYmaera X theorem prover [1] is an automated and interactive theorem prover for cyber-physical systems. Its underlying logic systems, differential dynamic logic, differential game logic, and dynamic logic for communicating hybrid programs, enables modeling distributed computing systems, in which agents interact, communicate, and compete in a shared physical space. For generality of the formal analysis, the models are fully symbolic to enable analysis of all possible executions and to obtain fully symbolic control envelopes that can be adjusted to many different concrete systems. For example, a car model is typically phrased with a symbolic bound  $A \geq 0$  for maximum acceleration, and another symbolic bound  $B < 0$  for maximum deceleration. While beneficial for system analysis and theorem proving, this makes models difficult to apply in simulation or on a true platform where concrete numbers are needed to fit the symbolic model parameters to the actual system parameters.

The gap between a formal model (models an infinite number of executions without concrete numbers) and a simulation (some number of specific executions with concrete numbers) can be partially filled using the ModelPlex runtime verification technique [2]: we interpret a formal model as a symbolic input-output relation between system states and propose a data-driven approach to fill in the symbolic parameters of the input-output relation from simulation traces. Starting from an initial assignment of the model parameters (obtained with a satisfiability solver directly from the symbolic input-output relation), the optimization goal is to find parameters that allow aggressive executions when safe and raise alarms when unsafe situations are encountered. To this end, we propose to collect simulation traces from driving scenarios (both safe and unsafe) and use optimization and machine learning to tune the model parameters.

## References

1. Fulton, N., Mitsch, S., Quesel, J., Völpl, M., Platzer, A.: KeYmaera X: an axiomatic tactical theorem prover for hybrid systems. In: Felty, A.P., Middeldorp, A. (eds.) Automated Deduction - CADE-25 - 25th International Conference on Automated

- Deduction, Berlin, Germany, August 1-7, 2015, Proceedings. Lecture Notes in Computer Science, vol. 9195, pp. 527–538. Springer (2015). [https://doi.org/10.1007/978-3-319-21401-6\\_36](https://doi.org/10.1007/978-3-319-21401-6_36)
2. Mitsch, S., Platzer, A.: Modelplex: verified runtime validation of verified cyber-physical system models. *Formal Methods Syst. Des.* **49**(1-2), 33–74 (2016). <https://doi.org/10.1007/S10703-016-0241-Z>