Carnegie Mellon University
Computer Science Department

Speaking Skills Talk

CoasterX: A Case Study in Component-Driven Hybrid Systems Proof Automation

Brandon Bohrer

Friday, March 2, 2018
12:00 pm
GHC 6501

Safety-critical cyber-physical systems (CPSs), such as automotive, rail, and aviation systems, combine discrete cyber control with continuous physical dynamics. Formal methods such as deductive proof in differential dynamic logic (dL) provide strong safety guarantees for CPSs. Verification in dL has achieved safety results in automotive, rail, and aviation domains, however (a) as with other CPS verification techniques, scaling dL proofs beyond a few dozen variables has proven difficult, and (b) modeling and verification in dL have a steep learning curve for non-experts.

We introduce component-driven proof automation, an approach to overcome these problems for CPSs built from small libraries of reusable components. First, an end-user builds a high-level component-based design in a graphical design tool, then automation exploits the component structure of the high-level model to derive a formal safety specification and proof in dL. Formal methods expertise is only required once, in the implementation of the specification generator and automated prover: the resulting design and verification toolchain can be used with no formal methods knowledge. Example applications include flight plans for unmanned drones as well as road and rail network designs.

We present the CoasterX toolchain for design and verification of roller coaster track designs as a case study in component-driven proof automation. Roller coasters are a safety-critical class of trains, characterized by gravity propulsion and closed-loop tracks with complex changes in track grade. We show how the velocity and acceleration bounds proved by CoasterX can (a) assure compliance with international safety standards and (b) explain safety violations and their resolution in real coasters, such as the Steel Phantom and its successor Phantom's Revenge, both at the Kennywood Amusement Park in Pittsburgh. We significantly advance the scalability of dL verification according to multiple metrics, achieving near order-of-magnitude improvement in the numbers of variables and component instances verified.

Joint work with AndrPlatzer, Adriel Luo, and Xuean Chuang (CMU).

Presented in Partial Fulfillment of the CSD Speaking Skills Requirement.