Control for Composition: A Correct-by-construction synthesis approach for connected vehicles

Necmiye Ozay
Electrical Engineering and Computer Science
University of Michigan

16 December 2013

Safety and dependability are paramount concerns for transportation cyber-physical systems. Advanced control, communication and information processing systems and technologies are being developed to reduce accidents and to create a safer, smarter and interconnected transportation infrastructure. However, as the vehicles are equipped with these more advanced technologies, it becomes harder to analyze complex interactions between subsystems, systems, vehicles, operators and infrastructure and to reason about the correctness of the interconnected system. One way to address these challenges is to use high-level supervisory control protocols to *shape the behavior* of subsystems so that individual systems can be put together (i.e., composed temporally or spatially) to form more capable, complex systems that inherit correctness guarantees from their building blocks and interfaces thereof. In this framework, *control* is used as a *gluing mechanism to facilitate composition* in addition to its traditional use for guaranteeing that the closed-loop system meets the design objectives.

In recent years, a variety of tools and techniques have been developed for specification, design and verification of embedded control systems. Traditionally, control protocols are manually designed and "verified" against the specification either via model-checking or via Monte Carlo simulations. The former approach is complete but limited to simple systems; the latter approach may fail to find important bugs. Instead we advocate a different approach: automatic synthesis of control protocols that are "correct-by-construction" and auto-generation of the corresponding control software. We believe that there are substantial opportunities for further development of the mathematical framework for correct-by-construction control synthesis as well as applications of this framework to model-based design of connected and (semi)automated transportation systems. In particular, advances in the following directions are necessary:

- Novel representations, which abstract the behavior of interacting cyber and/or physical modules/systems in a unified way, to serve as reusable interface specifications for compositional synthesis.

- Scalable techniques for synthesizing decentralized, not necessarily sequential, asynchronous control protocols.

- Extensible and flexible control architectures that can handle dynamic changes in the underlying interconnection networks (e.g., as new vehicles move in and out of each others communication range) and that are robust against latencies and uncertainties in communication.

- Control protocols that can manage cooperating as well as adversarial agents (and possible changes in agent roles).