Abstract

論 文 の 内 容 の 要 旨

論文題目　Reachability Analysis of Hybrid Systems
via Predicate and Relational Abstraction
（述語と関係を用いた抽象化による
ハイブリッドシステムの到達可能性解析）

氏　　名　　木戸　肩吾

Cars, robots, drones, medical equipment and other embedded systems are ubiquitous these days. In such systems, the embedded computer (controller) and the controlled physical object (plant) interact with each other via sensors and actuators. The combined system of the controller software and the physical plant is called a cyber-physical system (CPS).

Since the plant in a CPS behaves in the physical environment, a malfunction of the system has physical effects. Therefore safety assurance of CPSs is an important topic. There are mainly two approaches for safety assurance of CPSs: one is simulation/testing, and the other is formal methods. Currently, the dominant approach for safety assurance of CPSs in industry is simulation and testing, in which the behavior of the system is checked by giving some concrete inputs to the system. However, testing may miss a malfunction because for complex systems we cannot check all the possible inputs. Thus taking advantage of formal methods, which are mathematically valid techniques to analyze the behavior of systems, is recognized as an important direction of safety assurance.

The main topic of this thesis is formal methods for CPSs. More concretely, among a lot of techniques in formal methods, we focus on overapproximation in this thesis. Compared to software that works in desktop computers, CPSs have special characteristics. Among those characteristics of CPSs, we focus on its real-time property and hybrid dynamics.

First, we consider the real-time property. One of the common ways a CPS works is that the sensing occurs periodically, and the controller determines the next input to the plant based on the sensed data. In an ideal system, the input to the plant is changed periodically, at the same moment as the data is sensed. However, in practice, computation and data transfer cause delays

from the sensing of the data to the change of the input. The Usage of networked control—digital control of physical systems via computer networks—makes analyzing the effect of delays more important. In networked control, plants and controllers are separated physically. This physical distance leads to inevitable communication delays. What is worse, the use of cloud control makes both physical and logical distances between system components even bigger and unpredictable. In such settings, precise estimation of communication delays is often hard, and the delays have effects on the behavior of the system that cannot be ignored.

Then, we consider the hybrid dynamics of CPSs. A CPS consists of a plant and a controller, and it exhibits the hybrid behavior of continuous behavior in the physical environment and discrete behavior of the controller software. In that sense, a CPS is called a hybrid system.

Taking the above two characteristics into consideration, we consider a hybrid system with bounded time-delays as a model of a CPS. In this thesis, we introduce a methodology to calculate an overapproximation of its reachable set in two steps: the overapproximation of the errors due to time-delays, and the overapproximation of the reachable set of the delay-free model. This separation of concern enables us to replace the methodology used in each step with another existing methodology. In particular, for the second step where we do reachability analysis of delay-free hybrid systems, there is a lot of existing work and we can choose a suitable technique depending on the system under consideration.

The first step is to approximate a CPS with time-delays with the ideal model without time-delays. Given a Lyapunov function that certifies incremental stability, our proposed methodology gives an upper bound of the error between the system with bounded delays and the system without delays. In order to do this, we construct a transition system whose state is a triple consisting of a memory state, time and a mode. We define a premetric on these extended states, and give an upper bound of the premetric by constructing an approximate bisimulation relation on the transition system. As the first example, we show that our method can successfully analyze the effect of the delays of the boost DC-DC converter that is used in hybrid and electric vehicles. The dynamics of this example is characterized by linear ODEs, but we also show that our method can be applied to nonlinear ODEs using nonlinear water tank example.

In the above methodology to approximate a delayed system with its delay-free model, we computed an upper bound of the error of the two states at the same time instant. We extend this methodology by changing the definition of the premetric so that it can give a more precise upper bound of the Skorokhod distance between the trajectories of the two systems. The Skorokhod distance allows some wiggle in time. The resulting overapproximation of Skorokhod distance can be used, for example, for reachability analysis.

Then, we compute an overapproximation of the reachable set in the second step. For this purpose, we extend Cousot and Cousot's abstract interpretation framework to hybrid systems, using Robinson's nonstandard analysis (NSA). The approach of using NSA for verification of hybrid systems has been introduced by Suenaga and Hasuo. They model hybrid systems as programs with an infinitesimal constant, by regarding continuous behavior as infinitely many infinitesimal discrete jumps. This approach enables us to extend usual formal methods for discrete systems to hybrid systems almost as they are, thanks to the transfer principle in NSA. As a result, our extended abstract interpretation framework enables us a sound approximation of the reachable sets of hybrid systems. Using the domain of convex polyhedra, we can analyze linear water tank example with fixed time-delays, and nonlinear water tank without delays.

As mentioned above, the proposed methodologies for both of the two steps are applicable to nonlinear dynamics. Thus, by combining the two analysis, we successfully analyze the nonlinear water tank with bounded delays, and verify that the water level stays within a certain region. We also illustrate an advantage of the two-step analysis—the methodologies proposed in this thesis for each step can be replaced with another existing methodology—using the example of boost DC-DC converter. For this example, we can even synthesize a controller using the existing work by Girard instead of the extension of abstract interpretation.