Faster Computation for Predicate Abstraction of Hybrid Systems

Yusuke Tanaka (710045)

School of School of Information Science,
Japan Advanced Institute of Science and Technology

February 5, 2009

Keywords: Hybrid system, safety verification, predicate abstract, BDD, reachability problem.

Hybrid systems consist of continuous dynamical systems such as differential/difference equations and discrete dynamical systems such as if-then rules and finite automata. As is well known, hybrid systems are widely used as mathematical models for many practical applications such as automated highway systems, air-traffic management system, manufacturing systems, chemical processes, robotics, real-time communication networks, and real-time circuits. In the last years, there have been a lot of studies contributed to analysis and control of hybrid systems from both control theory community and theoretical computer science community. In particular, the safety verification problem is one of the significant topics in the analysis problem of hybrid systems. The safety verification problem is the problem that determines whether the state reaches the unsafe state set or not. If the state reaches the unsafe state set, then a given system is unsafe. However, it is shown that the safety verification problem of hybrid systems is in general undecidable. So it will be important to approximately solve the safety verification problem of hybrid systems. As one of methods for approximately solving the safety verification problem, the predicate abstraction technique is well known. The predicate abstraction has emerged to be a powerful technique for extracting finite state models from infinite state systems. The predicate abstraction, which has a track

record in verification of a source code, divides the continuous state space into the abstract state space by using given predicates of variables. By applying the predicate abstraction, we can consider transitions from some region to other region. Although the safety of a given hybrid system is guaranteed in the original continuous state space, the abstract state may reach the unsafe abstract state set, since a abstract state is an upper approximation of the continuous state. In order to exactly search abstract state sequences, the counterexample-guided refinement of abstractions has been proposed. A Counterexample is an abstract states sequence such that the terminal abstract state is included in the unsafe state set. If there do not exist such counterexamples, then we determine that the given system is safe. If there exist counterexamples, then we do not determine whether the given system is unsafe. This is because the abstract states sequence is an upper approximation of the original state sequence. So it is necessary to exactly check counterexamples. Then in the original state space, it is checked whether counterexamples are spurious, or not. If a counterexample is spurious, then a predicate is added, and counterexamples are searched. By using added predicates, it is achieved that transition computations on the abstract state space becomes more precisely. Thus the predicate abstraction technique is effective in the analysis problem of hybrid systems. However, this technique has one serious weakness, that is, the number of abstract states increases exponentially for increasing the number of predicates in the predicate abstraction. As a result, the number of transition computations from each abstract state increases exponentially. Furthermore, there is also the technical problem that one transition computation is not so easy. So it means if the number of transition computations from each abstract state increases, the computations time of safety verification problem in the predicate abstraction increases. In practical applications, since the number of predicates is huge, it is important to overcome these problems toward applying the predicate abstraction to many practical systems.

In this paper, we propose a faster computation technique for predicate abstraction of hybrid systems. In order to overcome the problem that the number of transition computations from each abstract state increases exponentially, the concept of the extended abstract state is proposed. Each

extended abstract state is given as the union of some abstract states. Since an upper approximation of the transition from some abstract state is given by the set product of some extended abstract states, it is not necessary to compute the transition computation from each abstract state. Furthermore, the number of extended abstract state increases in polynomial-time for increasing the number of predicates. Therefore, the reduction of the number of transition computations is achieved. In order to overcome the second problem that that one transition computation is not so easy, we implement one transition computation by using the BDD (Binary Decision Diagram). The BDD is one of data structures that is used to represent a Boolean function. On a more abstract level, the BDD can be considered as a compressed representation of sets or relations. Unlike other compressed representations, operations are performed directly on the compressed representation, i.e. without decompression. The transition computation of the abstract state can be computed on Boolean operations. So it will be suitable to use the BDD.

Also, in this paper, discrete-time piecewise linear systems are used, because discrete-time piecewise linear systems are one of simple models in hybrid systems. Note here that even if discrete-time piecewise linear systems are used, the problems considered in this paper are appeared. For simplicity of discussion, predicates are limited to linear predicates with one variable. In other words, the abstract state space is given as a lattice structure. By using a lattice structure, selecting extended abstract states is relatively easy, and we can analytically derive the number of transition computations, i.e., the number of extended abstract states. So we can easily compare between the proposed and the conventional methods. Furthermore, by using a numerical example on a discrete-time linear system, we show that the computation time to solve the transition from each abstract state is dramatically reduced. Therefore, the proposed method is effective for overcoming the problems in the predication abstraction of hybrid systems.