Successive Approximation Method for Verifying Invariants on Statechart

Takaaki Tateishi
Japan Advanced Institute Science and Technology, HOKURIKU

January 9, 2003

Abstract

Statechart is widely used for modeling behavior of a system and distributed objects. Behavior of a statechart depends on others when these statecharts communicate with each other. In such case, we need to consider how it depends on others for the verification. The direct method for verifying a property of the statechart is to make a composite statechart of all the statecharts. This method often brings state explosion problem. So, we have proposed a method for solving this problem. The essence of this method is to approximate the behavior of the statechart taking the effect from other component statecharts and use this approximated behavior in verifying its property.

Though a statechart receives events from all the other statecharts and its behavior is determined by them, the idea of the approximation is to receive events from a specific other statechart at a time instead of considering all the others, and repeating this process until the verification succeeds. The approximation technique is very generally introduced so that it could be applied to several communication protocols used for event sending and receiving.

Analysis of statechart is used to verify two classes of property: liveness and safety. Our purpose is to propose a technique for verifying an invariant of an attribute which classified into safety property. We have shown that if a property is proved for the approximated behavior, it also holds in the multiple statechart system.

For the above verification, we represent a statechart using a regular expression called a TSE (transition sequence expression) for the verification. An algorithm for obtaining the TSE from the statechart is same as one for obtaining a regular expression from a finite automaton. In a verification for a single statechart, we first put assertions before and after the TSE, which is called a A-TSE (asserted transition sequence expression). We then prove the A-TSE using a deductive system, which is similar to Hoare's one. We have proved the fact that this system is sound and relatively complete.

Also, this technique could be applicable to test of statecharts, though we have introduced it for the case of verifying an invariants.

Keywords: **statechart, state explosion problem, distributed objects, verification, invariant**