Title	項書換えを用いた安全性検証の組織化
Author(s)	清野，貴博
Citation	
Issue Date	2003-03
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/938
Rights	
Description	Supervisor:二木 厚吉，情報科学研究科，博士

Organizing case analysis for verifying safety properties with term rewriting

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

January 9, 2003

Abstract

In software engineering, state machines are important computational models. In the design of safety critical systems, we formally specify the systems and verify that systems have some desired properties based on the formal specifications. This approach is effective to ensure their reliability. State machines are roughly classified between finite state machines and infinite state machines. Models of state machines which has inductive definition are the latter one. In these models, safety properties can be proved by induction, but there is a disadvantage. Success of a verification depends upon human's knowledge and experience since it is impossible to verify the properties automatically.

There are many tools which perform verification by induction in semi-automatic way. CafeOBJ is one of them. CafeOBJ is an algebraic specification language. We can describe specifications of state machines in CafeOBJ. The interpreter regards a specification as a term rewriting system, and performs equational reasoning by reduction. To verify properties by induction, case analysis is indispensable. However it is not realistic that persons manage enormous cases. For this reason, it is important to support case analysis.

In this paper, a case is a set of states. Firstly, we propose a method to represent a case by a term. This allows us to operate case analysis by reduction. I propose two techniques to support case analysis by CafeOBJ interpreter. The first one is a technique of organizing cases by a matrix. This matrix consists of the axis derived from the specification of the state machine, and the axis derived from a assertion (or induction hypothesis). This matrix can be reuse each asseation because the latter axis is a parameter. It is easy to add more precisely case analysis if the analysis is not enough to prove a assertion. The second one is used when it cannot verify well using the first one. This technique generates cases mechanically to find candidate cases which can be used for verification or missing lemma. These techniques are implemented in CafeOBJ.

In this paper, we show effectiveness of these techniques by applying ones to some practical examples which are some railroad signaling systems.

Key Words: algebraic specification, state machine, safety property, case analysis, term rewriting