Title	Theorem Proving and Institutions
Author(s)	Gaina, Daniel
Citation	
Issue Date	2009-09
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/8365
Rights	
Description	Supervisor:Professor Kokichi Futatsugi, 情報科学研究科, 博士

Theorem Proving and Institutions

by

Daniel GAINA

submitted to
Japan Advanced Institute of Science and Technology
in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy

Supervisor: Professor Kokichi FUTATSUGI

School of Information Science
Japan Advanced Institute of Science and Technology

September 24, 2009

Abstract

We investigate proof rules in various logics used in the area of computer science and prove their soundness and completeness in the abstract framework of institutions. The soundness and completeness results have great significance for logics because they establish a correspondence between the semantic truth and (syntactic) provability. We also specify and verify the correctness of software systems showing how theoretical results may be used in concrete specification examples.

During the process of software specification, we often use different logical systems to capture particular aspects of software systems. Each part of a software system may be described by a distinct logical system that best fit considered problems. It is important to present a (abstract) formal concept of a logical system which covers the population explosion of logics used in computer science. Institution theory of Goguen and Burstall arouse out of this necessity, with the ambition of doing as much as possible at a level of abstraction, independent of any particular logic. We try to provide general ideas and results that can be easily applied to a multitude of logical systems and may be reused in different contexts.

This research is largely focused on foundational aspects but it also takes seriously the task of providing support for the specification and verification of software and hardware systems. We specify a mutual exclusion protocol and prove that it satisfies the desired requirements with the help of the tools provided by our general framework. Even though we use CafeOBJ for mechanical assistance for proofs, our goal is not to present CafeOBJ in detail, but rather its underlying logics.

We develop an abstract proof calculus for logics whose sentences are universal Horn sentences of the form $(\forall X)(\wedge H \Rightarrow C)$ and prove an institution generalization of Birkhoff completeness theorem. This result is applied to Horn clause logic, the "Horn fragment" of preorder algebra, order-sorted algebra and partial algebra and their infinitary variants.

The completeness of the infinitary logic $\mathcal{L}_{\omega_1,\omega}$ was proved by Carol Karp in 1964. We express and prove the completeness of infinitary first-order logics in the institution-independent setting by using forcing, a powerful method for constructing models. As a consequence of this abstraction, our results become available for the infinitary versions of many first-order logical systems. Although we emphasize the results for the infinitary logics our framework covers also the finitary cases.

Many computer science applications concern properties which are true of a restricted class of models, in most of the cases reachable models with constructor-generated elements. We introduce the concept of reachable model in the institution model theory. We present a couple of constructor-based institutions defined on top of the Horn and first-order institutions, basically by restricting the class of models to the reachable models. We define the proof rules for these logics, and lift the completeness results previously obtained to the constructor-based logics using institution-independent techniques.