Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 319 (2015) 315–331

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Sound and Complete Equational Reasoning over Comodels

Dirk Pattinson[1]

The Australian National University

Lutz Schröder [2,3]

Friedrich-Alexander-Universität Erlangen-Nürnberg

Abstract

Comodels of Lawvere theories, i.e. models in Set^{op}, model state spaces with algebraic access operations. Standard equational reasoning is known to be sound but incomplete for comodels. We give two sound and complete calculi for equational reasoning over comodels: an inductive calculus for equality-on-the-nose, and a coinductive/inductive calculus for equality modulo bisimulation which captures bisimulations syntactically through non-wellfounded proofs.

Keywords: Equational Logic, Comodels, Completeness, Bisimulation

1 Introduction

Comodels are an algebraic abstraction of the notion of global state, often used in the operational semantics of programming languages [13,15,11]. The most prominent example is the modelling of global state in imperative programs, where the explicit modelling of a store as a function that maps locations to values is replaced by algebraic operations that read and manipulate the values of global variables. Equations, in the standard universal-algebraic sense, ensure the intended semantics of these operations. Comodels are attractive for two reasons: first, they abstract implementation of state from the operational semantics, as state is not modelled explicitly, but only manipulated using operations. Second, the operations integrate seamlessly with programming language syntax. Some progress has been made towards the development of congruence formats in these settings [2]. While this builds

[1] dirk.pattinson@anu.edu.au

[2] lutz.schroeder@fau.de

[3] Work supported by the DFG under project COAX (SCHR 1118/12-1)

http://dx.doi.org/10.1016/j.entcs.2015.12.019

1571-0661/

the link between operational and denotational semantics, the link with axiomatic semantics is much less understood. Comodels are essentially an algebraic concept, defined in terms of function symbols and equations, but the interpretation of function symbols takes place in the category Set^{op}, the opposite category of the category Set of sets and maps. While a unary function symbol, say wr_v for writing a value v, is still interpreted as a unary function $(\!|\mathsf{wr}_v|\!) : C \to C$ on a set (of comodel states), general n-ary function symbols are interpreted as functions $(\!|f|\!) : C \to n{\cdot}C = C + \cdots + C$ (n times) and so are not understood as constructors, but as a combination of observation and state change. For example, a binary function symbol rd (that we think of as reading a binary value from a memory cell) receives the interpretation $(\!|\mathsf{rd}|\!) : C \to C + C$ and so indicates the value of the cell being read (by choosing one of the alternatives in $C + C$) on top of a new state. As a consequence, the standard tools of universal algebra for proving completeness of equational logic, including the construction of free algebras from terms modulo equations, are not available in the setting of comodels. Moreover, it is easy to see that equational reasoning is sound but incomplete over comodels. The easiest example is that of a theory comprising a nullary operation n and no equations: a comodel for this theory interprets n as a function $(\!|n|\!) : C \to 0{\cdot}C = \varnothing$ and therefore is empty, hence validates all equations; but clearly not all equations are derivable from the empty set of equations by standard equational reasoning. Excluding nullary operations does not improve this situation: we give an example below, due to Power, that shows that the same effect happens for a commutative binary operation.

This situation is remedied in the present paper, where we provide sound and complete calculi for equational reasoning over comodels. The overall flavour of comodels is coalgebraic, with a very simple type functor but with added complexity creeping in via the algebraic equations, which, for instance, may relate terms of different lookahead. The semantics of equations over comodels therefore naturally comes in two variants: satisfaction on-the-nose, and satisfaction up to bisimilarity, inducing correspondingly different notions of logical consequence. For reasoning on-the-nose, we give a standard, purely inductive calculus. We formalize this calculus in the style of a labelled sequent system. Key rules of the system express that terms with disjoint sets of free variables can never be equal in the comodel interpretation, and that terms with n free variables are essentially n-fold case statements allowing for a corresponding case distinction. For reasoning modulo bisimilarity, we then extend this inductive calculus by a single coinductive rule that allows us to conclude that two comodel terms are equal if they have the same output and their successors are equal. This rule may be applied in non-wellfounded proofs, resulting in a mixed inductive/coinductive calculus.

Related Work. We have already mentioned [14] where the theory of arrays is developed in terms of comodels, and the use of comodels in the semantics of programming languages [12,15,2]. None of these papers is concerned with axiomatic semantics, i.e. the equational logic of comodels. The model/comodel duality is investigated in [9,8] on the basis of clones and establishes, in our terminology, a dual equivalence between categories of comodels and certain topological spaces, but does not inves-