A Temporal Approach to Algebraic Specifications*

Yulin Feng†    Junbo Liu

FB3 Mathematik und Informatik
Universität Bremen
Postfach 330 440, D-2800 Bremen 33
F.R. Germany

Usenet: {feng,liu} %informatik.Uni-Bremen.de

Abstract. This paper is contributed to make connections between models for algebraic and temporal specifications. It brings a different viewpoint for classical algebras and algebraic specifications. Every algebra we concern here is finitely generated and associated with an implicit transition structure. The operators in the algebra may be partially defined. The class of algebras could be used as Kripke semantic models to interpret the temporals, so that we can do temporal reasoning about system behaviours such as safety and liveness properties. The unification of notions in algebraic and temporal specifications has many advantages for system developments. We may use a formal temporal deduction system to verify some dynamic properties from premises of algebraic specifications; or a temporal requirement specification may be used to develop systems in the style of top-down refinements. The notion of C-algebras has been crucial all along this work. In this paper we present the concepts, definitions and some basic theorems on C-algebras. Moreover, there exists a minimally defined algebra which is the initial one for each partially defined specification. The example of a lift controller is finally used to illustrate how to reason about the temporal behaviours of an algebraic specification.

1. Introduction

Every approach to algebraic specifications is based on some logical systems to make descriptions really precise and to allow computers to perform interpretations. The classical approach to algebraic specifications is based on equational logic, which has been proved very successful for specifying systems in abstraction. However, a major drawback of this approach has been its limited capacity to deal with systems involving concurrence. A large number of approaches (cf. [1,2,4,11,13,16-18]) has been taken so far to extend traditional algebraic framework to cope with this problem. The value of temporal logic for specifying concurrent systems is also well appreciated (cf. [5,8,15,19]). In order to reason about dynamic behaviours of systems, it seems useful to combine techniques from both algebraic and temporal approaches.

* This work is partly supported by the Commission of the European Communities under the ESPRIT Programme, Contract #390, PROSPECTRA Project.
† On leave from University of Science & Technology of China, Hefei, Anhui 230026, China.
It is essential that the temporal and algebraic specifications are based on different semantic models. To combine classical algebraic specifications with techniques in temporal logic, it must be clarified how these models can be unified. Our purpose in this paper is try to answer the question and to integrate algebraic specifications into a temporal framework, so that we can do temporal reasoning about their behaviour both with respect to safety and liveness properties.

Some aspects characterizing our approach are listed below.

- We take a different view of algebraic specifications. Each object in an algebra is considered as a temporal entity that evolves by some update operators.
- We consider hierarchically defined specifications. Each signature can only define one new sort, while other sorts involved are considered to be predefined.
- As the notion of partial operators is of practical importance for system specifications, we consider a class of partial algebras as the semantics of concerning specifications with a set of positive conditional equations. A definition of existential equality is used to interpret equality for partially defined terms.
- Algebraic specifications are integrated into a temporal framework. The logic used here is first order branching time temporal logic. The Kripke semantics of the logic is defined with respect to a transition structure. The class of algebras we concern here is called C-algebras. For a partially defined specification, there exists a unique (up to isomorphism) C-algebra which is initial in the class of all of C-algebras satisfying equations in the specification.
- Emphasis is put on the abstract data type of which the system evolves. It is essential that the specification is property-oriented, only to define the necessary properties on system states, while to leave rooms for different implementations. It may be implemented in a system either in a sequential, or in a concurrent system. From a methodological viewpoint, the unification of algebraic and temporal specifications may bring the advantages for system development in two aspects. We may use a formal temporal deduction system to verify some dynamic conclusions from premises of algebraic specifications; on the other side, a temporal requirement specification may be used to develop systems in the style of top-down refinements.

The authors consider the paper as a first approach to combine the different approaches (algebraic and temporal) for system specification. The layout of the paper is as follows. Section 2 is a brief introduction to temporal logic. Section 3 is the main part of the paper. It is devoted to the concepts, definitions and some theorems on C-algebras. To illustrate the temporal reasoning from an algebraic specification, we give the lift example in section 4. We in the last section conclude with some remarks and indicate some problems and the further research directions.

2. Temporal Logic

Temporal logic was originally developed by philosophers for reasoning about the ordering