Available online at www.sciencedirect.com
SCIENCE DIRECT®
Theoretical Computer Science 343 (2005) 305–331
Theoretical Computer Science
www.elsevier.com/locate/tcs

Behavioural specification for hierarchical object composition

Răzvan Diaconescu*

Institute of Mathematics "Simion Stoilow" of the Romanian Academy, P.O. Box 1-764, Bucharest 014700, Romania

Abstract

Behavioural specification based on hidden (sorted) algebra constitutes one of the most promising recently developed formal specification and verification paradigms for system development.

Here we formally introduce novel concepts of *behavioural object* and equivalence between behavioural objects within the hidden algebra framework. We formally define several object composition operators on behavioural objects corresponding to the hierarchical object composition methodology introduced by CafeOBJ. We study their basic semantical properties and show that our most general form of behavioural object composition with synchronisation has final semantics and a composability property of behavioural equivalence supporting a high reusability of verifications. We also show the commutativity and the associativity of parallel compositions without synchronisation.

Keywords: Algebraic specification; Behavioural specification; Hidden algebra; Object composition

1. Introduction

The current Internet/Intranet technologies have led to an explosive increase in the demand for the construction of reliable distributed systems. Among the new technologies proposed for meeting this new technological challenge, component-based software engineering is one of the most promising. If we have an adequate set of components and a good design pattern, a system development process may become easier and the quality of the product may be greatly improved. However, such a development process raises some serious problems. How

* Tel.: +40 744 153703; fax: +40 21 2125126.
E-mail address: Razvan.Diaconescu@imar.ro.

0304-3975/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2005.06.015

can we get an adequate set of components or how can we know the components we get are adequate for our systems?

A good solution seems to be given by formal specifications supporting the following characteristics:

- can specify the interface of components,
- can specify the behaviour of components,
- supports a precise semantics of composition, and
- be executable and/or have tools supporting testing and verification.

Here we adopt the behavioural algebraic specification framework [8,4,11,9]. Due to its simple logical foundations and its efficient specification and verification methodologies, behavioural algebraic specification provides a good framework for such formal specifications.

Work related to the CafeOBJ algebraic specification language [3,5] has proposed a hierarchical object composition methodology (see [3,13,6]) based on behavioural specification. The behavioural specification paradigm is reflected rather directly in the definition of CafeOBJ, this being maybe the most distinctive feature of this language among other modern algebraic specification languages such as CASL [1] or Maude [16].

Here we formally define the novel concept of *behavioural object* within hidden algebra, which is the logic of CafeOBJ behavioural specification. Informally, a behavioural object is just a special kind of behavioural specification which formally specifies the space of the states of the objects together with actions ('methods') changing the state of the object, and with observations ('attributes') to (ordinary) data types. This is the basis for a precise definition of several types of composition operators on behavioural objects, such as parallel composition (without synchronisation), dynamic composition (in which component objects get created and deleted dynamically), and composition with synchronisation generalising both the former operators. Informally, these composition operators are based on specifications of projections from the state space of the compound object to the state spaces of the components. Our definitions provide mathematical foundations for the corresponding methodological definitions of object composition in [3,12,6]. Our composition operators support hierarchical composition processes in the sense that the result of a composition is still a behavioural object which can be therefore used for another composition.

Our framework permits a clear formulation of semantical properties of the composition operators, such as associativity and commutativity, and final semantics (i.e. the existence of final composition models). We show that the basic parallel composition operator is associative and commutative modulo a meaningful equivalence relation between behavioural objects. Informally, two behavioural objects are *equivalent* when there is an isomorphism between the implementations modulo, the same state space, the same actions, and the same behavioural equivalence between the states. For the general composition with synchronisation operator we prove a compositionality result for the behavioural equivalence relation, a result which constitutes the foundation for automation of the verification process at the level of a compound object (see [3,12,6]), and the existence of final semantics.

The paper is structured as follows: the first section recalls briefly the basic mathematical notions necessary for this work. We first present general algebra notions, and then we give a very brief overview of hidden algebra. At the end of this section we introduce the novel concept of behavioural object. The next section introduces briefly the CafeOBJ notation for