Available online at www.sciencedirect.com
SCIENCE DIRECT
Electronic Notes in Theoretical Computer Science
ELSEVIER Electronic Notes in Theoretical Computer Science 118 (2005) 111–128
www.elsevier.com/locate/entcs

Compositional Properties of Sequential Processes

Naijun Zhan

Lehrstuhl für Praktische Informatik II
Facultät für Mathematik und Informatik
Mannheim Universität
D7,27, 68163 Mannheim, Deutschland
Email: {zhan}@pi2.informatik.uni-mannheim.de

Abstract

It is widely agreed that the modular method is one of the most effective methods to specify and verify complex systems in order to avoid combinatorial explosion. FLC (Fixpoint Logic with Chop) is an important modal logic because of its expressivity and logic properties, e.g., it is strictly more expressive than the μ-calculus. In this paper, we study the compositionality of FLC, namely, to investigate the connection between the connectives of the logic and the constructors of programs. To this end, we first extend FLC with a nondeterministic operator "+" (FLC$^+$ for the extension) and then establish a correspondence between the logic and the basic process algebra with deadlock and termination (abbreviated by BPA$^\epsilon_\delta$). Finally, we show that as a by-product of the correspondence characteristic formulae for processes of BPA$^\epsilon_\delta$ up to strong (observational) bisimulation can be constructed compositionally directly from the syntax of processes.

Keywords: chop operator, modal logic, compositionality, verification, bisimulation, characteristic formula, process algebra

1 Introduction

There is a growing need for reliable methods in designing correct reactive systems [9] such as computer operating systems and air traffic control systems. These systems are characterized by ongoing, typically nonterminating and highly nondeterministic behavior. Such systems are often used to model "*safety critical systems*" like, e.g., air traffic control systems, nuclear reaction control systems and so on. As any faulty behavior of such systems might imply catastrophical consequences, proving the correctness of such systems with

1571-0661/$ – see front matter
doi:10.1016/j.entcs.2004.12.018

respect to the expected behavior is inevitable. There is a common agreement that formal methods, such as modal and temporal logics [17,24] and process algebra [3,10,19], are effective and reliable methods to design these systems.

Because the complexity of large systems is normally uncontrollable, it is necessary that a method for developing such systems is compositional (vertically or horizontally) in order to avoid combinatorial explosion in specifying and verifying them, e.g. [10,19,3,2,16,4,5,15]. The compositional method allows one to build up a large system by composing existing systems with the defined constructors and reduce the problem of correctness for a complex system to similar and simpler correctness problems for the subsystems.

FLC [18] is an extension of the μ-calculus [12] with the sequential composition operator — "chop" (denoted by ";"). [18] pointed out that FLC is strictly more expressive than the μ-calculus because [6,11] proved that only "regular" properties can be defined in the μ-calculus, but characteristic formulae of context-free processes can be defined in FLC. [13,14] investigated the issue of FLC model checking.

The compositionality was stated in [8] as one important requirement that should also be satisfied by specification logic used in a process algebraic setting, that is, any program constructor cons corresponds to an operator **cons** of the logic such that

(a) $P_i \models \phi_i$ for $i = 1, \ldots, n$ implies $cons(P_1, \ldots, P_n) \models \mathbf{cons}(\phi_1, \ldots, \phi_n)$;

(b) $cons(P_1, \ldots, P_n) \models \mathbf{cons}(\phi_1, \ldots, \phi_n)$ is the strongest assertion which can be deduced from $P_i \models \phi_i$ for $i = 1, \ldots, n$.

It is clear that FLC does not meet the above conditions since P meets ϕ and Q satisfies ψ, but we can not get any property that holds in the combined system $P + Q$ according to ϕ and ψ in FLC. In order to guarantee that a specification logic satisfies the above conditions, we have two alternatives: one is to show that for each constructor in process algebra, a corresponding connective can be defined in the logic. To our knowledge, until so far it is still an open problem if a suitable "+" is definable in classical modal logics; the other is directly to introduce a connective, which exactly corresponds to the constructor in process algebra, into the logic like, e.g., in [8,15] a nondeterministic choice "+" is introduced explicitly.

Besides, it is worth investigating the connection between the sequential composition of process algebra and the 'chop' operator of FLC, but it seems no people to do such a job up to now.

In this paper, we first extend FLC with a non-deterministic operator "+" (denoted by FLC$^+$). Intuitively, $P \models \phi + \psi$ means that P consists of two parts P_1 and P_2, which are executed nondeterministically such that $P_1 \models \phi$