Theoretical Computer Science 546 (2014) 164–175

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Complete proof systems for weighted modal logic

Kim G. Larsen, Radu Mardare

Department of Computer Science, Aalborg University, Selma Lagerlöfs Vej 300, DK-9220 Aalborg, Denmark

ARTICLE INFO

Available online 6 March 2014

Keywords:
Weighted transition systems
Modal logic
Proof systems
Completeness

ABSTRACT

The weighted transition systems (WTS) considered in this paper are transition systems having both states and transitions labeled with real numbers: the state labels denote quantitative resources, while the transition labels denote costs of transitions in terms of resources. Weighted Modal Logic (WML) is a multi-modal logic that expresses qualitative and quantitative properties of WTSs. While WML has been studied in various contexts and for various application domains, no proof system has been developed for it. In this paper we solve this open problem and propose both weak-complete and strong-complete axiomatizations for WML against WTSs. We prove a series of metatheorems including the finite model property and the existence of canonical models. We show how the proof system can be used in the context of a process-algebra semantics for WML to convert a model-checking problem into a theorem-proving problem. This work emphasizes a series of similarities between WML and the probabilistic/stochastic modal logics for Markov processes and Harsanyi type spaces, such as the use of particular infinitary rules to guarantee the strong-completeness.

1. Introduction

Model-driven and component-based development (MDD) is finding its way into industrial practice, in particular within the area of embedded systems. Here a key challenge is how to handle the growing complexity of systems, while meeting requirements on correctness, predictability, performance and not least time- and cost-to-market. In this respect MDD is seen as a valuable and promising approach, as it allows early design-space exploration and verification and may be used as the basis for systematic and unambiguous testing of a final product. However, for embedded systems, verification should not only address functional properties but also a number of non-functional properties related to timing and resource constraints. Within the area of model checking, a number of state-machine based modeling formalisms have emerged, which allow for such quantitative aspects to be expressed. In particular the formalisms of timed automata [1], and the extensions to weighted timed automata [6,2] allow for such constraints to be modeled and efficiently analyzed.

In several ways, the work on process calculi – pioneered by Tony Hoare [15] and Robin Milner [24] – addresses and provides principal solutions to several of the issues that are now considered within the application area of embedded systems. The desire for component-based development requires semantically well-defined notions of compositions, which preserve suitable notions of behavioral equivalence – as found in the algebraic part of a process calculus. Also, the logical part of a process calculus provides an immediate link to an unambiguous treatment of requirements to systems.

A desirable property of a process calculus is that of *adequacy* in the sense that the behavioral equivalence is identical with that of the process equivalence induced by the logic. This notion was coined in the landmark paper [14] showing that

E-mail addresses: kgl@cs.aau.dk (K.G. Larsen), mardare@cs.aau.dk (R. Mardare).

http://dx.doi.org/10.1016/j.tcs.2014.03.007
0304-3975/© 2014 Published by Elsevier B.V.

bisimilarity agrees with logical equivalence with respect to Hennessy–Milner logic. Soon after, several researchers[1] were developing proof systems and algorithms for establishing that (the behavior of) a given process-algebraic term P satisfies a given logical property ϕ, i.e. $P \models \phi$. In particular, research was aiming at so-called *local* (or on-the-fly) methods [19,32,28,10] and *compositional* methods [4,31,30,18,3,22,20]. In this effort, the pioneering work by Glynn Winskel was especially influential.

The additional notion of *expressiveness*[2] of a process calculus was introduced slightly later than that of *adequacy*. Here a process calculus is *expressive* if for any process algebraic term P, there exists a logical formula f_P such that $Q \models f_P$ precisely when Q is behavioral equivalent to P. In this way, equivalence checking $P \sim Q$ may be translated in to a model checking problem $Q \models f_P$, where f_P often is referred to as the characteristic property of P. Several behavioral equivalences have been shown to possess characteristic properties, e.g., [27,9,26]. Moreover, model checking problems $P \models \phi$ may be translated into validity problems of type $\models f_P \to \phi$, thus making the search for complete axiomatizations of validity the most fundamental research question. Here the work on axiomatizing the modal mu-calculus by Dexter Kozen [16] and Igor Walukiewicz [29] is a landmark result.

Motivated by the needs from embedded systems, we consider in this paper Weighted Modal Logic (WML) for weighted transition systems (WTS), allowing to specify and reason about not only the discrete behavior of a system but also its consumption of resources. However, rather than focusing on language theoretic issues, our aim is to investigate the fundamental question of axiomatization of the proposed weighted logic.

Our notion of weighted transition systems is not just a simple instance of a weighted automata [11], but we also study infinite and infinitely branching systems. We identify, however, the subclass of WTSs that can be generated by finite terms of a simple Weighted Process Algebra (WPA) with only prefix and choice operations.

Weighted Modal Logic is a multi-modal logic defined for a semantics based on WTSs. It is endowed with modal operators that predicate about the values of both state and transition labels. While in a WTS we can have real labels, the modalities only encode rational values and often we are in the situation of characterizing a state or a transition using an infinite convergent sequences of rationals. Since in practice we often work with finite WTSs, we also developed a WPA-semantics for WML and we prove that WPA-processes can be in fact characterized by a WML formula. As mentioned before, this is important in applications since it can turn any model-checking problem into a validity-checking one.

In this paper we prove a series of metaproperties of WML. Firstly, we propose a weak-complete axiomatization for this logic guaranteeing that a logical formula is valid if and only if it is provable in our axiomatic system. In order to prove this result we demonstrate that WML enjoys the *finite model property* meaning that any consistent property has a finite model (WTS) and the cardinality of this model is bounded by parameters that depend on the syntactical structure of the property. In the context of a complete axiomatization, the logical characterization of WPA processes can be used to transform a model-checking problem of type $P \models \phi$ not only into a validity problem of type $\models f_P \to \phi$, but also into a theorem-proving problem of type $\vdash f_P \to \phi$ that has to be derived within the axiomatic system.

A second major achievement of this paper is providing a strong-complete extension of the aforementioned axiomatic system, which means that we can prove any consistent theory, possibly involving an infinite set of formulas. To get the strong completeness we had to consider, in addition to the infinitary version of Modus Ponens, one infinitary rule and to assume the Lindenbaum lemma[3] as a meta-axiom. These assumptions are in line with the assumptions one needs to do to get strong completeness for other modal logics with quantitative modalities, such as the probabilistic logics defined for semantics on Markov processes or Harsanyi type spaces [33] and stochastic logics [8,23]. In fact our infinitary rule is similar to the rule known in literature as the countable additivity rule used by Goldblatt to prove the strong completeness of logics for measurable polynomial functors on the category of measurable spaces [12].

2. Weighted transition systems and weighted process algebra

In this section we introduce the concept of Weighted Transition System (WTS), which is a transition system that has both the nodes and the transitions labeled with real numbers such that if the transition from m to n is indexed by x, then the label of n is the sum of x and the label of m. One can interpret the label of a state as the resource available for possible transitions and the label of a transition as the resource consumed/produced for the transition to take place (the cost of the transition). Our intention is to remain as general as possible and for this reason we impose no restriction on the labels: they can be any real number, possibly negative.

Definition 2.1 *(Weighted transition system).* A *weighted transition system* is a tuple $\mathcal{W} = (M, \theta, l)$ where M is an arbitrary set of *states*, $\theta \subseteq M \times \mathbb{R} \times M$ is the *transition function* and $l : M \to \mathbb{R}$ is a labeling function such that whenever $(m, x, m') \in \theta$,

$$l(m') = l(m) + x.$$

[1] Including Glynn Winskel and the first author of the present paper.

[2] Supposedly introduced by Amir Pnueli.

[3] Lindenbaum lemma states that any consistent set of formulas can be extended to a maximally-consistent one.