Theoretical Computer Science 564 (2015) 1–29

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Bounded semantics ☆

Wenhui Zhang

State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing, China

ARTICLE INFO

Article history:
Received 30 May 2012
Received in revised form 26 September 2014
Accepted 18 October 2014
Available online 24 October 2014
Communicated by D. Sannella

Keywords:
Formal methods
Formal semantics
Temporal logics
Model checking
Program correctness

ABSTRACT

Although there have been many works on bounded semantics, a characterization of a good definition for a bounded semantics has not been given, and this has led to definitions of bounded semantics of temporal logics that may not be appropriate with respect to the potential usefulness as a basis for developing bounded model checking approaches. On the other side, the research effort on bounded semantics has mainly focused on existentially interpreted fragments of temporal logics, due to the intricacy of defining appropriate bounded semantics for universally interpreted fragments, or for temporal logics with path quantifiers that are closed under negation. This work addresses these two problems, by defining the characteristics of bounded semantics for clarifying the concept of bounded semantics, and presenting a bounded semantics for the full set of CTL, a logic closed under negation, including possibility for specifying both existential and universal properties.

1. Introduction

Bounded semantics of LTL with existential interpretation has been studied and used as the theoretical basis for SAT-based bounded model checking [7,16]. The basic idea of the LTL bounded semantics is to consider bounded paths (possibly with loops) instead of all of the infinite ones. In a Kripke structure, there is an infinite path (starting from an initial state) that satisfies an LTL formula iff there is a bounded path (starting from the same initial state) that does the same, and it can be inferred that a bounded path satisfies an LTL formula according to the LTL bounded semantics iff the corresponding infinite path does the same according to the standard semantics [7]. The successfulness of model checking based on bounded semantics has led to extensive research on bounded semantics for various (fragments of) temporal logics [34,3,42,29,40,26,35]. This kind of model checking is considered complementary to BDD-based model checking [12,11,28,14] for combating the state explosion problem [13,9], esp. for efficient error detection [39]. However, there are two problems with this kind of research, one is that a characterization of a good definition for a bounded semantics has not been given; the other is that the research effort on bounded semantics has mainly focused on existentially interpreted fragments of temporal logics. The first problem may lead to definitions of bounded semantics of temporal logics (or fragments of such logics) that are not appropriate with respect to the potential usefulness as a basis for developing bounded model checking approaches, for instance, the one defined in [40]. The second problem makes it difficult to use bounded semantics as a basis for verification of universally specified properties. For verification purposes, one needs to reach a completeness threshold or some termination criteria [25,17,22,18,1,31] in order to show the non-existence of a counter-example. Ideally, the principle of bounded model checking for verification (called bounded verification for short) should be similar to bounded error detection, such that we

☆ This work merges and extends parts of the preliminary works presented at ICFEM 2007 and ICFEM 2009 [45,47]. This work was supported by the National Natural Science Foundation of China under Grant No. 61272135 and the National Key Basic Research Program (973 Program) of China under Grant No. 2014CB340701.

http://dx.doi.org/10.1016/j.tcs.2014.10.026
0304-3975/

start with a small bounded model, if this is not sufficient to make a conclusion, we increase the bound, until we have a conclusion or we run out of resources. This work addresses these two problems, by defining the characteristics of bounded semantics for clarifying the concept of bounded semantics, and presenting a bounded semantics for the full set of CTL, a logic closed under negation, including possibility for specifying both existential and universal properties. A QBF-encoding of CTL formulas based on the bounded semantics and an algorithm for QBF-based bounded correctness checking of CTL properties are also provided.

The rest of this paper is organized as follows. In Section 2, relevant concepts and the definition of CTL* are provided. In Section 3, a characterization of well-constructed bounded semantics is proposed, and different types of potential applications of bounded semantics are formulated. In Section 4, a bounded semantics of CTL is presented, and a QBF-based bounded correctness checking approach for CTL properties based on the bounded semantics is developed. In Section 5, related works are discussed and the difficulty of developing well-constructed bounded semantics for CTL* is analyzed. In Section 6, concluding remarks and open problems are presented.

2. Preliminaries

Given a set of models $\mathcal{M}$ and a set $\mathcal{L}$ of formulas interpreted on $\mathcal{M}$. A semantic relation R of $\mathcal{L}$ over $\mathcal{M}$ is a subset of $\mathcal{M} \times \mathcal{L}$. We assume that the temporal logics under consideration are interpreted over Kripke structures [19], which are also called transition systems in [23].

2.1. Models and semantics

Definition 2.1 *(Models).* Let AP be a set of propositions. A Kripke structure over AP is a quadruple $M = \langle S, T, I, L\rangle$ where S is a set of states, $T \subseteq S \times S$ is a transition relation which is total, $I \subseteq S$ is a non-empty set of initial states, and $L : S \to 2^{AP}$ is a labeling function that maps each state to a subset of propositions of AP. A Kripke structure is also called a model.

Paths and computations. An infinite path of M is an infinite sequence $s_0 s_1 \cdots$ such that $(s_i, s_{i+1}) \in T$ for $i \geq 0$. A computation of M is an infinite path $s_0 s_1 \cdots$ of M such that $s_0 \in I$.

Definition 2.2 *(Semantic relations).* Let $\mathcal{M}$ be a set of models, and $\mathcal{L}$ be the set of formulas of some temporal logic interpreted on $\mathcal{M}$. A semantic relation $\models$ of $\mathcal{L}$ over $\mathcal{M}$ is a subset of $\mathcal{M} \times \mathcal{L}$. $M \models \varphi$ denotes that M satisfies φ.

Definition 2.3 *(Indistinguishability).* Let $\models$ be a semantic relation of $\mathcal{L}$ over $\mathcal{M}$. Let $\varphi \in \mathcal{L}$. Two models M and M' are indistinguishable by $(\models, \varphi)$, if $M \models \varphi$ iff $M' \models \varphi$. Two models M and M' are indistinguishable by $(\models, \mathcal{L})$, if for all $\varphi \in \mathcal{L}$, they are indistinguishable by $(\models, \varphi)$.

Let a mutation of a model M be the model M' obtained by replacing a state s of M with a new state s' such that s' inherits all properties of s (i.e., the transitions to and from s, the membership in the set of the initial states, and the label on s).

Definition 2.4 *(Logical semantic relations).* A logical semantic relation $\models$ of $\mathcal{L}$ over $\mathcal{M}$ is a relation such that if M' is a mutation of M, then $M \models \varphi$ implies $M' \models \varphi$ for all $\varphi \in \mathcal{L}$.

In logical semantic relations, the name of a state is considered irrelevant, and the focus is on the structure of models and the information on the structure.

Definition 2.5 *(Structural equivalence).* Let $M_1 = \langle S_1, T_1, I_1, L_1\rangle$ and $M_2 = \langle S_2, T_2, I_2, L_2\rangle$ be two models. M_1 and M_2 are structurally equivalent, if there is a bijective map $f : S_1 \to S_2$ such that

$$\begin{array}{lcl} (x, y) \in T_1 & \leftrightarrow & (f(x), f(y)) \in T_2 \\ x \in I_1 & \leftrightarrow & f(x) \in I_2 \\ L_1(x) & = & L_2(f(x)) \end{array}$$

If two models are structurally equivalent, then one can be obtained from the other by a sequence of mutations. Therefore the following holds.

Proposition 2.1. *Structurally equivalent models are indistinguishable by logical semantic relations.*