Available online at www.sciencedirect.com

ScienceDirect

Fuzzy Sets and Systems 262 (2015) 44–59

FUZZY sets and systems

www.elsevier.com/locate/fss

Computation tree logic model checking based on possibility measures ☆

Yongming Li *, Yali Li, Zhanyou Ma

College of Computer Science, Shaanxi Normal University, Xi'an, 710062, China

Received 19 February 2013; received in revised form 2 March 2014; accepted 6 March 2014

Available online 27 March 2014

Abstract

In order to deal with the systematic verification with uncertain information in possibility theory, Li and Li (2013) introduced model checking of linear-time properties in which the uncertainty is modeled by possibility measures. Xue, Lei and Li (2011) defined computation tree logic (CTL) based on possibility measures, which is called possibilistic CTL (PoCTL). This paper is a continuation of the above work. First, we study the expressiveness of PoCTL. Unlike probabilistic CTL, it is shown that PoCTL (in particular, qualitative PoCTL) is more powerful than CTL with respect to their expressiveness. The equivalent expressions of basic CTL formulae using qualitative PoCTL formulae are presented in detail. Some PoCTL formulae that cannot be expressed by any CTL formulae are presented. In particular, some qualitative properties of repeated reachability and persistence are expressed using PoCTL formulae. Next, adapting CTL model-checking algorithm, a method to solve the PoCTL model-checking problem and its time complexity are discussed in detail. Finally, an example is given to illustrate the PoCTL model-checking method.

Keywords: Computation tree logic; Possibilistic Kripke structure; Possibility measure; Qualitative property; Quantitative property

1. Introduction

Model checking [15] is a formal verification technique which allows for desired behavioral properties of a given system to be verified on the basis of a suitable model of the system through systematic inspection of all states of the model. It is widely used in the design and analysis of computer systems [6,7]. Although it has been rapidly gaining in importance in recent years, classical model checking cannot deal with verification of systems (e.g., concurrent systems) coping with uncertainty information. Such as, the development of most large and complex systems is inevitably involved with lots of uncertainty and inconsistency information.

☆ This work was partially supported by National Science Foundation of China (Grant Nos: 11271237, 61228305) and the Higher School Doctoral Subject Foundation of Ministry of Education of China (Grant No: 20130202110001).

* Corresponding author.
E-mail address: liyongm@snnu.edu.cn (Y. Li).

http://dx.doi.org/10.1016/j.fss.2014.03.009
0165-0114/

In order to handle the systematic verification with probability information, Hart and Sharir [18] in 1986 applied probability theory to model checking in which the uncertainty is modeled by probability measures. Baier and Katoen [2] systematically introduced the principle and method of model checking based on probability measures and related applications with Markov chain models for probabilistic systems. For the past few years, there were even more applications on probability model checking in verifying properties of systems with uncertain information (see e.g. [3]).

On the other hand, possibility theory [12,29] is an uncertain theory devoted to the handling of incomplete information. As said in [14], possibility theory is comparable to probability theory because it is based on set-functions. It differs from the later by the use of a pair of dual set-functions (possibility and necessity measures) instead of only one. Besides, possibility theory is not additive and makes sense on ordinal structures. The specificity of possibility theory is to deal with incomplete information in a gradual way. Fuzzy sets [28], coming from linguistic information are one important source for possibility measures. For the motivation and applications of possibility theory, we refer to the survey papers [1,9,14]. In order to cope with the systematic verification on non-deterministic systems with uncertain information in possibility theory, Li and Li [22] introduced model checking of linear-time properties in which the uncertainty is modeled by possibility measures and initiated the model checking based on possibility measures. Xue, Lei and Li [27] defined computation tree logic based on possibility measures, which is called possibilistic computation tree logic (PoCTL, in short).

Although we have studied the quantitative and qualitative properties of PoCTL in [27], there are many important issues that still have not been addressed. The first important problem is the expressiveness of PoCTL: whether any CTL formulae can be expressed by PoCTL or vise versa. As we know, probabilistic CTL and CTL are not comparable with each other [2]. This allows probabilistic CTL to be used to do model checking of real-world problems, which cannot be tackled by classical CTL model checking. The surprising result of this paper is that CTL is a proper subclass of PoCTL. The second problem is looking for the method to solve PoCTL model-checking problems. As we know, there are effective algorithms and automated tools to solve CTL model-checking problems. As we just mentioned, CTL is a proper subclass of PoCTL, it is nontrivial to study whether there are effective algorithms to solve the PoCTL model-checking problems. We shall give complete study to the above two problems in this paper.

The content of this paper is arranged as follows. In Section 2 we recall the notion of possibilistic Kripke structures, the related possibility measures induced by the possibilistic Kripke structures, and the main notions of PoCTL introduced in [27]. In Section 3, the equivalence of PoCTL formulae and CTL formulae is investigated, and the differences between PoCTL formulae and CTL formulae are discussed. An important result, CTL is a proper subclass of PoCTL, is obtained. Section 3 also presents qualitative properties of repeated reachability and persistence. The PoCTL model checking approach is presented in Section 4, and an illustrative example is given in Section 5. The paper ends with conclusion section.

2. Preliminaries

Transition systems or Kripke structures are key representations for model checking. Corresponding to possibilistic model checking, we have the notion of possibilistic Kripke structures, which is defined as follows.

Definition 2.1. (See [22].) A possibilistic Kripke structure is a tuple $M = (S, P, I, AP, L)$, where

(1) S is a countable, nonempty set of states;

(2) $P : S \times S \longrightarrow [0, 1]$ is the transition possibility distribution such that for all states s, $\bigvee_{s' \in S} P(s, s') = 1$;

(3) $I : S \longrightarrow [0, 1]$ is the initial distribution, such that $\bigvee_{s \in S} I(s) = 1$;

(4) AP is a set of atomic propositions;

(5) $L : S \longrightarrow 2^{AP}$ is a labeling function that labels a state s with those atomic propositions in AP that are supposed to hold in s.

Furthermore, if the set S and AP are finite sets, then $M = (S, P, I, AP, L)$ is called a finite possibilistic Kripke structure.

Remark 1. (1) In Definition 2.1, we require the transition possibility distribution and initial distribution are normal, i.e., $\bigvee_{s' \in S} P(s, s') = 1$ and $\bigvee_{s \in S} I(s) = 1$, where we use $\bigvee X$ or $\bigwedge X$ to represent the least upper bound (or