SMT-based Bounded Model Checking for Weighted Interpreted Systems and for Weighted Epistemic ECTL

(Extended Abstract)

Agnieszka M. Zbrzezny* and Bożena Woźna-Szcześniak and Andrzej Zbrzezny
IMCS, Jan Długosz University in Częstochowa, Al. Armii Krajowej 13/15, 42-200 Częstochowa, Poland
{agnieszka.zbrzezny,b.wozna,a.zbrzezny}@ajd.czest.pl

ABSTRACT

We define the SMT-based bounded model checking (BMC) method for Weighted Interpreted Systems and for the existential fragment of the Weighted Epistemic Computation Tree Logic. We implemented the new BMC algorithm and compared it with the SAT-based BMC method for the same systems and the same property language on several benchmarks for multi-agent systems.

Categories and Subject Descriptors

D.2.4 [**Software/Program Verification**]: Model checking

Keywords

Bounded model checking; SMT; SAT; Weighted Interpreted Systems; Weighted Epistemic Computation Tree Logic

1. INTRODUCTION

Interpreted systems (ISs) [2] are the most generally considered models of multi-agent systems (MASs). An important limitation in these models is that there are no expenses connected with agents' actions. The models get to be more expressive when this confinement is dropped. For instance, the formalism of *weighted interpreted systems* (WISs) [6] extends ISs to make the reasoning possible about not only temporal and epistemic properties, but also about agents' quantitative properties. In the paper we harness this weighted formalism as the model of MASs.

To describe the prerequisites of MASs, different extensions of temporal logics [1] with epistemic [2], doxastic [3], and deontic [4] modalities have been proposed. In this paper, we consider the existential fragment of a weighted epistemic computation tree logic (WECTLK) interpreted over WISs.

The fundamental thought behind SMT-based bounded model checking (BMC) methods consists in translating the existential model checking problem for a modal logic and for a model to the satisfiability modulo theory problem (SMT-problem) of a quantifier-free first-order formula, and in taking advantage of the power of modern SMT-solvers.

*The study is co-funded by the European Union, European Social Fund. Project PO KL "Information technologies: Research and their interdisciplinary applications", Agreement UDA-POKL.04.01.01-00-051/10-00.

Appears in: *Proceedings of the 14th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2015), Bordini, Elkind, Weiss, Yolum (eds.), May 4–8, 2015, Istanbul, Turkey.*

In this paper we make the following contributions. Firstly, we define and implement an SMT-based BMC method for WECTLK and for WISs. Next, we report on the initial experimental evaluation of our SMT-based BMC methods. Finally, we compare our prototype implementation of the SMT-based BMC method against the SAT-based BMC engine of [5, 7], the only existing technique that is suitable with respect to the input formalism and checked properties.

2. PRELIMINARIES

WISs. Let $Ag = \{1, \dots, n\}$ denote the non-empty and finite set of agents, and $\mathcal{E}$ be a special agent that is used to model the environment in which the agents operate, and let $\mathcal{PV}$ be a set of propositional variables. The *weighted interpreted system* (WIS) [5, 6] is a tuple $(\{L_{\mathbf{c}}, \iota_{\mathbf{c}}, Act_{\mathbf{c}}, P_{\mathbf{c}}, t_{\mathbf{c}}, \mathcal{V}_{\mathbf{c}}, d_{\mathbf{c}}\}_{\mathbf{c}\in Ag\cup\{\mathcal{E}\}})$, where $L_{\mathbf{c}}$ is a non-empty set of *local states*, $\iota_{\mathbf{c}} \subseteq L_{\mathbf{c}}$ is a non-empty set of initial states, $Act_{\mathbf{c}}$ is a non-empty set of *possible actions*, $Act = Act_1 \times \dots \times Act_n \times Act_{\mathcal{E}}$ is a non-empty set of *joint actions*, $P_{\mathbf{c}} : L_{\mathbf{c}} \to 2^{Act_{\mathbf{c}}}$ is a *protocol function*, $t_{\mathbf{c}} : L_{\mathbf{c}} \times Act \to L_{\mathbf{c}}$ is a (partial) *evolution function*, $\mathcal{V}_{\mathbf{c}} : L_{\mathbf{c}} \to 2^{\mathcal{PV}}$ is a *valuation function*, and $d_{\mathbf{c}} : Act_{\mathbf{c}} \to \mathbb{N}$ is a *weight function*.

For a given WIS we define a *model* as a tuple $M = (Act, S, \iota, T, \mathcal{V}, d)$, where $Act = Act_1 \times \dots \times Act_n \times Act_{\mathcal{E}}$ is the set of all joint actions, $S = L_1 \times \dots \times L_n \times L_{\mathcal{E}}$ is the set of all *global states*, $\iota = \iota_1 \times \dots \times \iota_n \times \iota_{\mathcal{E}}$ is the set of all *initial* global states, $\mathcal{V} : S \to 2^{\mathcal{PV}}$ is the valuation function defined as $\mathcal{V}(s) = \bigcup_{\mathbf{c}\in Ag\cup\{\mathcal{E}\}} \mathcal{V}_{\mathbf{c}}(l_{\mathbf{c}}(s))$, $T \subseteq S \times Act \times S$ is the transition relation defined as follows: $(s, a, s') \in T$ (or $s \xrightarrow{a} s'$) iff $t_{\mathbf{c}}(l_{\mathbf{c}}(s), a) = l_{\mathbf{c}}(s')$ for all $\mathbf{c} \in Ag \cup \{\mathcal{E}\}$; we assume that the relation T is total. $d : Act \to \mathbb{N}$ is the "joint" weight function defined as follows: $d((a_1, \dots, a_n, a_{\mathcal{E}})) = d_1(a_1) + \dots + d_n(a_n) + d_{\mathcal{E}}(a_{\mathcal{E}})$.

WECTLK. WECTLK has been defined in [5] as the existential fragment of the weighted CTLK with cost constraints on *all* temporal modalities. In the syntax of WECTLK we assume the following: $p \in \mathcal{PV}$ is an atomic proposition, $\mathbf{c} \in Ag$, $\Gamma \subseteq Ag$, I is an interval in $\mathbb{N} = \{0, 1, 2, \dots\}$ of the form: $[a, \infty)$ and $[a, b)$, for $a, b \in \mathbb{N}$ and $a \neq b$. The WECTLK formulae are defined by the following grammar: $\varphi ::= \mathbf{true} \mid \mathbf{false} \mid p \mid \neg p \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \mathrm{EX}_I\varphi \mid \mathrm{E}(\varphi \mathrm{U}_I \varphi) \mid \mathrm{EG}_I\varphi \mid \overline{\mathrm{K}}_{\mathbf{c}}\varphi \mid \overline{\mathrm{D}}_\Gamma\varphi \mid \overline{\mathrm{E}}_\Gamma\varphi \mid \overline{\mathrm{C}}_\Gamma\varphi$. The modalities X_I, U_I and G_I are read as the *weighted next*, the *weighted until*, and the *weighted always*, respectively. The existential epistemic modalities are read as standard.

The satisfiability relation $\models$ which indicates truth of a WECTLK formula in the model M at some state s of M is defined as in [5]. A WECTLK formula φ is *true* in the model M (in symbols $M \models \varphi$) iff φ is true at some initial state of the model M. The bounded satisfiability relation $\models_k$ which indicates k-truth of a WECTLK formula in the model M at some state s of M is also defined as in

[5]. A WECTLK formula φ is *k-true* in the model M (in symbols $M \models_k \varphi$) iff φ is k-true at some initial state of the model M. The *model checking problem* asks whether $M \models \varphi$, but the *bounded model checking* problem asks whether there exists $k \in \mathbb{N}$ such that $M \models_k \varphi$.

3. SMT-BASED BMC

SMT encoding of the BMC problem for WECTLK and for WIS is based on the same bounded semantics as the SAT encoding presented in [5]. Namely, the main difference between SAT- and SMT-based BMC for WECTLK and for WIS is in the representation of symbolic states, symbolic actions, and symbolic weights. Thus, the main result is the generalization of the propositional encoding of [5] into the quantifier-free first-order encoding.

Let M be the abstract model, φ a WECTLK formula, and $k \geq 0$ a bound. The presented SMT encoding of the BMC problem for WECTLK and for WIS relies on defining the quantifier-free first-order formula $[M, \varphi]_k := [M^{\varphi,\iota}]_k \wedge [\varphi]_{M,k}$ that is satisfiable if and only if $M \models_k \varphi$ holds.

THEOREM 1. *Let M be a model, and φ a WECTLK formula. For every $k \in \mathbb{N}$, $M \models_k \varphi$ if, and only if, the the quantifier-free first-order formula $[M, \varphi]_k$ is satisfiable.*

4. EXPERIMENTAL RESULTS

First of all we conducted the experiments using two benchmarks: the *weighted generic pipeline paradigm* (WGPP) WIS model [5, 6] and the *weighted bits transmission problem* (WBTP) WIS model [6]. The size of the reachable state space of the WGPP system is $4 \cdot 3^n$, for $n \geq 1$. The size of the reachable state space of the WBTP system is $3 \cdot 2^n$ for $n \geq 1$. Next, our experimental results we computed on a computer equipped with I7-3770 processor, 32 GB of RAM, and the operating system Arch Linux with the kernel 3.15.3. We set the CPU time limit to 3600 seconds. Finally, we compared our SMT-based BMC with our SAT-based BMC [5, 7].

Let Min denote the minimum cost incurred by Consumer to receive the data produced by Producer, and p denote the cost of producing data by Producer. Further, let $a \in \mathbb{N}$ and $b \in \mathbb{N}$ be the costs of sending, respectively, bits by Sender and an acknowledgement by Receiver. The specifications we consider for the WGPP and WBTP systems, respectively, are:

$\varphi_1 = \overline{\mathrm{K}}_P \mathrm{EF}_{[Min, Min+1)} ConsReady$

$\varphi_2 = \overline{\mathrm{K}}_P \mathrm{EF}(ProdSend \wedge \overline{\mathrm{K}}_C \overline{\mathrm{K}}_P \mathrm{EG}_{[0, Min-p)} ConsReady)$

$\phi_1 = \mathrm{EF}_{[a+b, a+b+1)}(\mathbf{recack} \wedge \overline{\mathrm{K}}_{\mathcal{S}}(\overline{\mathrm{K}}_{\mathcal{R}}(\bigwedge_{i=0}^{2^n-2}(\neg \mathbf{i}))))$

$\phi_2 = \mathrm{EF}_{[a+b, a+b+1)}(\overline{\mathrm{K}}_{\mathcal{S}}(\bigwedge_{i=0}^{2^n-1}(\overline{\mathrm{K}}_{\mathcal{R}}(\neg \mathbf{i}))))$

The number of the considered k-paths is equal to 2 for φ_1, 5 for φ_2, 3 for ϕ_1, and $2^n + 2$ for ϕ_2, respectively.

From Fig. 1 we can notice that for WGPP and both considered formulae the SMT-based BMC is able to verify more nodes and it is faster than the SAT-base BMC. However, the SAT-based BMC consumes less memory. For the WBTP system the SAT-based BMC performs much better in terms of the total time and the memory consumption. The reason of the higher efficiency of the SAT-based BMC for WBTP is, probably, that the lengths of the witnesses for both formulae is constant and very short, and that there is no nested temporal modalities in the scope of epistemic operators. For formulae like ϕ_1 and ϕ_2 the number of arithmetic operations is small, so the SMT-solvers cannot show its strength.

5. CONCLUSIONS

We proposed, implemented, and experimentally evaluated SMT-based BMC for WECTLK interpreted over WIS. We compared our method with the corresponding SAT-based technique. The experimental results show that the approaches are complementary, and that the SMT-based BMC approach appears to be superior for the WGPP system, while the SAT-based approach appears to be superior for the WBTP system. This is a novel and interesting result, which shows that the choice of the BMC method should depend on the considered system.

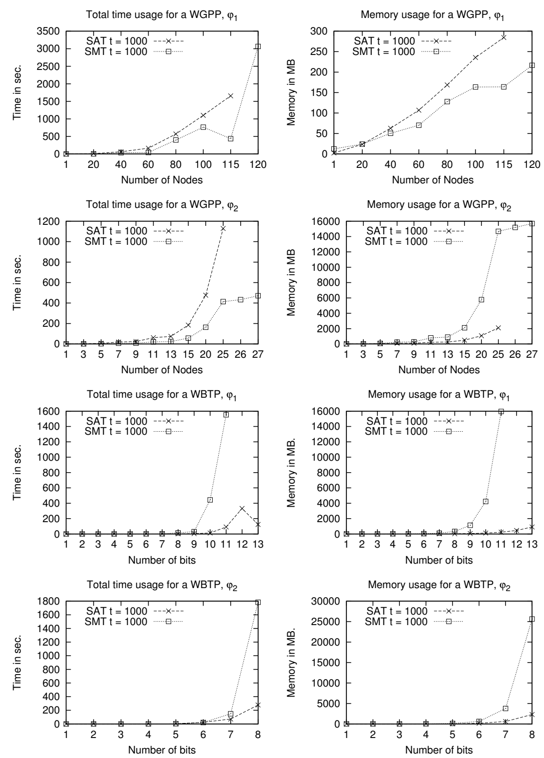

Figure 1: SAT- and SMT-based BMC: WGPP with n nodes and WBTP with n bits integer value.

REFERENCES

[1] E. A. Emerson. Temporal and modal logic. *Handbook of Theoretical Computer Science*, vol. B, chapter 16, pp. 996–1071. Elsevier Science Publishers, 1990.

[2] R. Fagin, J. Y. Halpern, Y. Moses, and M. Y. Vardi. *Reasoning about Knowledge*. MIT Press, 1995.

[3] H. Levesque. A logic of implicit and explicit belief. In *Proceedings of AAAI*, pp. 198–202. Morgan Kaufman, 1984.

[4] A. Lomuscio and M. Sergot. Deontic interpreted systems. *Studia Logica*, 75(1):63–92, 2003.

[5] B. Woźna-Szcześniak. SAT-based bounded model checking for weighted deontic interpreted systems. In *Proceedings of EPIA'2013*, vol. 8154 of *LNAI*, pp. 444–455. Springer, 2013.

[6] B. Woźna-Szcześniak, A. M. Zbrzezny, and A. Zbrzezny. SAT-based bounded model checking for weighted interpreted systems and weighted linear temporal logic. In *Proceedings of PRIMA 2013*, vol. 8291 of *LNAI*, pp. 355–371. Springer, 2013.

[7] B. Woźna-Szcześniak, I. Szcześniak, A. M. Zbrzezny, and A. Zbrzezny. Bounded model checking for weighted interpreted systems and for flat weighted epistemic computation tree logic. In *Proceedings of PRIMA'2014*, vol. 8861 of *LNAI*, pp. 107–115. Springer, 2014.