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 imple-
mented 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 they become
more structured and the more careful about not only temporal and epistemic properties, but also about agents’ quantitative properties.
In the paper we harness this expressive power of ISs as the model of MASs.

To describe the pre-emptive MGs, different extensions of
temporal logics [1] with modal modal logics [1] have been proposed. In this paper, we consider the ex-

satisfied 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 satisfi-
ability 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.


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 $Ag = \{1, \ldots, n\}$ denote the non-empty and finite set
of agents, and $E$ be a special agent that is used to model the
environment in which the agents operate, and let $PV$ be a set of
propositional variables. The weighted interpreted system (WIS) [5, 6] is a tuple $\langle \{L_e, l_e, Act_e, \Phi_e, \delta_e\}_{e \in Ag(e)} \rangle$, where
$\Phi_e$ is a non-empty set of local states, $l_e \subseteq L_e$ is a non-empty
set of initial states, $Act_e$ is a non-empty set of possible actions,
$Act = Act_1 \times \ldots \times Act_n \times Act_E$ is a non-empty set of joint actions, $\Phi : L_e \rightarrow 2^{Act_e}$ is a protocol function, $l_e : L_e \rightarrow L_e$ is a
is the valuation function defined as
$V(s) = \bigcup_{e \in Ag(e)} V_e(l_e(s))$. $T \subseteq S \times Act \times S$ is the transition relation
defined as follows: $(s, a, s') \in T$ (or $s \xrightarrow{a} s'$) if $l_e(l_e(s), a) = l_e(s')$ for a e in $Ag$ and $\{e\}$; we assume that the relation $T$ is total. $d : Act \rightarrow \mathbb{N}$ is the “joint” weight function defined as follows:
d$a_{\{a_1, \ldots, a_n, a_E\}} = d_1(a_1) + \ldots + d_n(a_n) + d_e(a_E)$. WECTLK. WECTLK has been defined in [5] as the existential
fragment of the weighted CTLK with cost constraints on all tempo-
ral modalities. In the syntax of WECTLK we assume the following:

\[
\begin{align*}
\phi &::= \text{true} \mid \text{false} \mid p \mid \neg \phi \mid \phi \lor \phi \mid EX_\Gamma \phi \mid EG_\Gamma \phi \mid FE_\Gamma \phi \mid \Gamma E_\phi \mid \Gamma \forall \phi \mid \Gamma \exists \phi. \\
\end{align*}
\]

The modalities $X_\Gamma$, $U_\Gamma$ and $G_\Gamma$ 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 $|=\cdot$ indicates truth of a WECTLK
formula in the model $M$ at some state $s$ of $M$ is defined as in [5]. A
WECTLK formula $\phi$ is true in the model $M$ (in symbols $M|=\phi$
$iff \phi$ is true at some initial state of the model $M$. The bounded
satisfiability relation $|=_{k}$, which indicates $k$-truth of a WECTLK
formula in the model $M$ at some state $s$ of $M$ is also defined as in

\[
\begin{align*}
\phi &::= \text{true} \mid \text{false} \mid p \mid \neg \phi \mid \phi \lor \phi \mid EX_\Gamma \phi \mid EG_\Gamma \phi \mid FE_\Gamma \phi \mid \Gamma E_\phi \mid \Gamma \forall \phi \mid \Gamma \exists \phi. \\
\end{align*}
\]
[5]. A WECTLK formula \( \varphi \) is \( k \)-true in the model \( M \) (in symbols \( M \models_k \varphi \)) if \( \varphi \) 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, \( \varphi \) 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 \( [M, \varphi]_k := [M^0\varphi]_k \land [\varphi]_{M,k} \) that is satisfiable if and only if \( M \models_k \varphi \) holds.

**Theorem 1.** Let \( M \) be a model, and \( \varphi \) 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:

\[
\begin{align*}
\varphi_1 &= \overline{K_p}E_\phi (Min, Min + 1) ConsReady \\
\varphi_2 &= K_p E_\phi (ProdSend) \land K_p E_{\phi \Delta 0, Min - p} ConsReady \\
\phi_1 &= E_\phi (\overline{recack} \land \overline{K_S}(\sum_{i=0}^{n-2} (-i))) \\
\phi_2 &= E_{\phi \Delta 0, a+b+1} (K_S (\sum_{i=0}^{n-1} (-1))) \\
\end{align*}
\]

The number of the considered \( k \)-paths is equal to 2 for \( \varphi_1 \), 5 for \( \varphi_2 \), 3 for \( \phi_1 \), and \( 2^n + 2 \) for \( \phi_2 \), 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-based 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 \( \phi_1 \) and \( \phi_2 \) 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.

REFERENCES