Research Article

Bounded Model Checking of ETL Cooperating with Finite and Looping Automata Connectives

Rui Wang, Wanwei Liu, Tun Li, Xiaoguang Mao, and Ji Wang

College of Computer Science, National University of Defense Technology, Changsha, Hunan 410073, China

Correspondence should be addressed to Wanwei Liu; wwliu@nudt.edu.cn

Received 8 March 2013; Accepted 14 June 2013

Academic Editor: Xiaoyu Song

Copyright © 2013 Rui Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

As a complementary technique of the BDD-based approach, bounded model checking (BMC) has been successfully applied to LTL symbolic model checking. However, the expressiveness of LTL is rather limited, and some important properties cannot be captured by such logic. In this paper, we present a semantic BMC encoding approach to deal with the mixture of ETL, and ETL. Since such kind of temporal logic involves both finite and looping automata as connectives, all regular properties can be succinctly specified with it. The presented algorithm is integrated into the model checker ENuSMV, and the approach is evaluated via conducting a series of imperial experiments.

1. Introduction

A crucial bottleneck of model checking is the state-explosion problem, and the symbolic model checking technique has proven to be an applicable approach to alleviate it. In the early 1990s, McMillan presented the BDD [1] based model checking technique [2]. It is first applied to CTL model checking and is later adapted to deal with LTL. With the rapid evolvement of SAT solvers, an entirely new approach, namely, bounded model checking (BMC), is presented in [3]. It represents the problem “there is a path (with bounded length) violating the specification in the model” with a Boolean formula and then tests its satisfiability via a SAT solver. Usually, BMC is considered to be a complementary approach of the BDD-based approach: BMC is normally used for hunting bugs not for proving their absence. It performs better when handling a model having a large reachable state set but involving (relatively) shallow error runnings.

BMC has been successfully employed in LTL model checking. However, LTL has the drawback of limited expressiveness. Wolper was the first to complain about this by addressing the fact that some counting properties such as “p holds at every even moment” cannot be expressed by any LTL formula [4]. Indeed, LTL formulae are just as expressive as star-free \( \omega \)-expressions, that is, \( \omega \)-regular expressions disallowing arbitrary (in a star-free expression, Kleene-closure operators (\( \cdot^* \) and \( \cdot^{\omega} \)) can only be applied upon \( \Sigma \), which is the whole set of alphabet) use of Kleene-closure operators.

As pointed in [5, 6], it is of great importance for a specification language to have the power to express all \( \omega \)-regular properties—as an example, it is a necessary requirement to support modular model checking. Actually, such specification language like PSL [7] has been accepted as industrial standard.

For temporal logics within linear framework, there are several ways to pursue such an expressiveness.

(1) The first way is to add fixed-point operators or propositional quantifiers to the logic, such as linear \( \mu \)-calculus [8] and QLTL [9].

(2) An alternative choice is to add regular expressions to LTL-like logics, as done in RLTL [10], FTL [11, 12], and PSL [7].

(3) The third approach is to cooperate infinitely many temporal connectives with the logic, just like various of ETLs [4, 9, 13].

The first extension requires finitely many operators in defining formulae. Meanwhile, the use of fixed-point operators and higher-order quantifiers tends to rise difficulties in understanding. In contrast, using regular expressions or automata as syntactical ingredients is much more intuitive in
comprehension. To some extent, since nesting of automata connectives is allowed, the third approach generalizes the second one.

In [4], Wolper suggested using right linear grammars as connectives. Later, Wolper, Vardi, and Sistla consider taking various $\omega$-automata [9, 13]. Depending on the type of automata used as temporal connectives, we may obtain various ETLs. As a result, ETLs employing $\omega$-automata with looping, finite, and repeating (alternatively, Büchi [14]) acceptance are, respectively, named ETL$_{l+f}$, ETL$_{l}$, and ETL$_{r}$, and all of them are known to be as expressive as $\omega$-regular expressions [13].

We have presented a BDD-based model checking algorithm for ETL$_{l}$ in [15] and an algorithm for BDD-based model checking of an invariant of PSL in [16]. Jehle et al. present a bounded model checking algorithm for linear $\mu$-calculus in [17]. And in [18], a tester based symbolic model checking approach is proposed by Pnueli and Zacks to deal with PSL properties. Meanwhile, a modular symbolic Büchi automata construction is presented in [19] by Cimatti et al.

In this paper, we present a semantic BMC encoding for ETL employing both finite acceptance and looping acceptance automata connectives (we in the following refer to it as ETL$_{l+f}$). The reason that we study BMC algorithm for such kind of logic is for the following considerations.

(1) The BDD-based symbolic model checking technique for ETL$_{l}$ has been established in [15] by extending LTL construction [20]. Nevertheless, in a pure theoretical perspective, looping and finite acceptance, respectively, correspond to safety and liveness properties, and looping acceptance automata can be viewed as the counterparts of finite acceptance automata. Actually, both similarities and differences could be found in compiling the semantic models and translating Boolean representations when dealing with these two types of connectives. Since ETL$_{l+f}$ has a rich set of fragments, such as LTL, it is hopeful to develop a unified semantic BMC framework of such logics.

(2) Practically, things would usually be much more succinct when employing both types of automata connectives, in comparison to merely using finite or looping ones. As an example, there is no direct encoding for the temporal operator $\mathbf{G}$ just with finite acceptance automata—to do this with ETL$_{l}$, we need to use a two-state and two-letter connective to represent the operator $\mathbf{F}$ and then to dualize it. In contrast, with looping automata, we just need to define a one-state and one-letter connective. It would save much space overhead in building tableaux.

(3) Lastly, unlike syntactic BMC encodings (such kind of encodings give inductive Boolean translations with the formulae’s structure, cf. [21, 22] for a survey), the semantic fashion [22] yields a natural completeness threshold computation approach, and it describes the fair path finding problem over the product model with Boolean formulae. In this paper, we give a linear semantic encoding approach (opposing to the original quadratic semantic encoding) for ETL$_{l+f}$. Moreover, the technique can also be tailored to semantic LTL BMC.

We have implemented the presented algorithm with our model checker ENuSMV (Ver. 1.2), and this tool allows end users to customize temporal connectives by defining automata. We have also justified the algorithm by conducting a series of comparative experiments.

The paper is structured as follows: Section 2 briefly revisits its basic notions. Section 3 introduces semantic BMC encoding technique for ETL$_{l+f}$. In Section 4, experimental results of ETL$_{l+f}$ BMC are given. Finally, we conclude the whole paper with Section 5.

2. Preliminaries

An infinite word $w$ over the alphabet $\Sigma$ is a mapping from $\mathbb{N}$ to $\Sigma$; hence we may use $w(i)$ to denote the $i$th letter of $w$. For the sake of simplicity, we usually write $w$ as the sequence $w(0)w(1)\ldots$. A finite prefix of $w$ with length $n$ is a restriction of $w$ to the domain $[0,\ldots,n-1]$, denoted by $w[n]$.

A (nondeterministic) automaton is a tuple $\mathcal{A} = \langle \Sigma, Q, \delta, q_0, F \rangle$, where:

(i) $\Sigma$ is a finite alphabet,
(ii) $Q$ is a finite set of states,
(iii) $\delta : Q \times \Sigma \rightarrow 2^Q$ is a transition function,
(iv) $q \in Q$ is an initial state, and
(v) $F \subseteq Q$ is a set of accepting states.

An infinite run of $\mathcal{A} = \langle \Sigma, Q, \delta, q_0, F \rangle$ over an infinite word $w$ is an infinite sequence $\sigma = q_0q_1\cdots \in Q^\omega$, where $q_0 = q$ and $q_{i+1} \in \delta(q_i, w(i))$ for each $i$. In addition, we say that each prefix $q_0\cdots q_{n+1}$ is a finite run over $w[n]$.

In this paper, we are concerned with two acceptance types for $\omega$-automata.

**Looping.** An infinite word $w$ is accepted if it has an infinite run over $w$.

**Finite.** An infinite word $w$ is accepted if it has a finite prefix $w[n]$, over which there is a finite run $q_0\cdots q_{m+1}$, where $q_{m+1}$ is an accepting state (call such a prefix accepting prefix).

In both cases, we denote by $L(\mathcal{A})$ the set of infinite words accepted by $\mathcal{A}$.

Given an automaton $\mathcal{A} = \langle \Sigma, Q, \delta, q_0, F \rangle$ and a state $r \in Q$, we denote by $\mathcal{A}'$ the automaton $\langle \Sigma, Q, \delta, r, F \rangle$. That is, $\mathcal{A}'$ is almost identical to $\mathcal{A}$, except for that its initial state is replaced by $r$. Hence, $\mathcal{A}$ and $\mathcal{A}'$ are the same.

Given a set of atomic propositions $AP$, the class of ETL$_{l,f}$ formulae can be inductively defined as follows.

(i) Both $\top$ and $\bot$ are ETL$_{l,f}$ formulae.
(ii) Each proposition $p \in AP$ is an ETL$_{l,f}$ formula.
(iii) If $\varphi$ is an ETL$_{l,f}$ formula, then $\neg \varphi$ and $\varphi \land \psi$ are ETL$_{l,f}$ formulae.
(iv) If $\varphi_1, \varphi_2$ are ETL$_{l+f}$ formulae, then both $\varphi_1 \land \varphi_2$ and $\varphi_1 \lor \varphi_2$ are ETL$_{l+f}$ formulae.

(v) If $\mathcal{A}$ is an automaton with the alphabet $\Sigma = \{a_1, \ldots, a_n\}$ and $\varphi_1, \ldots, \varphi_n$ are ETL$_{l+f}$ formulae, then $\mathcal{A}(\varphi_1, \ldots, \varphi_n)$ is also an ETL$_{l+f}$ formula.

Remark 1. In the original definition of various ETLs (say ETL$_b$, ETL$_{l+f}$, and ETL$_r$), the “next operator” ($\odot$) is not explicitly declared. However, this operator is extremely important in building the semantic BMC encodings for ETL$_{l+f}$. Hence, we explicitly use this operator in our definition, and it would not change the expressiveness of the logic.

Remark 2. Since we employ both finite and looping acceptance automata connectives, our logic is a mixture of ETL$_b$ and ETL$_r$. On the one hand, ETL$_{l+f}$ generalizes both of these two logics; on the other hand, it can be embedded into ETL$_b$; hence this logic is also as expressive as omega-regular expressions.

The satisfaction relation of an ETL$_{l+f}$ formula $\varphi$ with respect to an infinite word $\pi \in (2^AP)^\omega$ and a position $i \in \mathbb{N}$ is inductively given as follows.

(i) $\pi(i) \models \top$ and $\pi(i) \neq \emptyset$.

(ii) $\pi(i) \models p$ if and only if $p \in \pi(i)$.

(iii) $\pi(i) \models \neg p$ if and only if $\pi(i) \neq \emptyset$.

(iv) $\pi(i) \models \varphi \land \psi$ if and only if $\pi(i) \models \varphi$ and $\pi(i) \models \psi$.

(v) $\pi(i) \models \varphi \lor \psi$ if and only if $\pi(i) \models \varphi$ or $\pi(i) \models \psi$.

(vi) $\pi(i) \models \varphi_1 \lor \varphi_2$ if and only if $\pi(i) \models \varphi_1$ or $\pi(i) \models \varphi_2$.

(vii) $\delta(\mathcal{A})$ is a looping acceptance automaton with the alphabet $\{a_1, \ldots, a_n\}$, then $\pi(i) \models \delta(\mathcal{A}(\varphi_1, \ldots, \varphi_n))$ if and only if: there is an infinite word $w \in \mathcal{L}(\mathcal{A})$, and, for each $j \in \mathbb{N}, w(j) = a_k$ implies $\pi(i + j) \models \varphi_k$.

(viii) $\mathcal{A}$ is a finite acceptance automaton with the alphabet $\{a_1, \ldots, a_n\}$, then $\pi(i) \models \mathcal{A}(\varphi_1, \ldots, \varphi_n)$ if and only if: there is an infinite word $w \in \mathcal{L}(\mathcal{A})$ with an accepting prefix $w[n]$, such that, for each $j < n, w(j) = a_k$ implies $\pi(i + j) \models \varphi_k$.

As usual, we directly use $\pi \models \varphi$ in place of $\pi(0) \models \varphi$.

To make a better understanding of ETL$_{l+f}$ formulas, we here give some examples of the use of automata connectives.

(1) Considering the LTL formula $\varphi_1 \lor \varphi_2$, it can be described with an ETL$_{l+f}$ formula $\mathcal{A}_E(\varphi_1, \varphi_2)$, where $\mathcal{A}_E$ is the finite acceptance automaton $\{a_1, a_2\}, \{q_1, q_2\}, \delta, \{q_1\}, \{q_2\}$, and we let $\delta_1(q_1, a_1) = q_1$, $\delta(q_1, a_2) = q_2$, and $\delta(q_2, a_1) = \emptyset$.

(2) The LTL formula $\varphi$ is equivalent to ETL$_{l+f}$ formula $\mathcal{A}_L(\varphi)$, where $\mathcal{A}_L = \{a, \{q\}, \delta, \varnothing, \emptyset\}$ is a looping acceptance automaton and $\delta(q, a) = \{q\}$.

Remark 3. The order of letters is important in defining automata connectives. Hence, the alphabet should be considered as a vector, rather than a set.

We use $\text{sub}(\varphi)$ to denote the set of subformulae of $\varphi$. Formula $\varphi$ is in negation normal form (NNF) if all negations in $\varphi$ are adjacent to atomic propositions or automata connectives. One can achieve this by repeatedly using De Morgan’s law and the schemas of $\neg \varphi \equiv \neg \neg \varphi \equiv \neg \varphi$. In addition, we call a formula $\varphi$ being of the form $\mathcal{A}(\varphi_1, \ldots, \varphi_n)$ an automaton formula.

Given a formula $\varphi$ (in NNF), we use a two-letter-acronym to designate the type of an automaton subformula of $\varphi$: the first letter is either “P” or “N,” which means “positive” or “negative”; and the second letter can be “F” or “L,” which describes the acceptance type. For example, NL-subformulae stand for “negative automata formulae with looping automata connectives,” such as $\neg \mathcal{A}(\varphi_1, \varphi_2)$, where $\mathcal{A}$ is a two-letter looping automaton.

A model or interchangeably a labeled transition system (LTS) is a tuple $\mathcal{M} = \langle S, \rho, I, \pi, \mathcal{F} \rangle$, where:

(i) $S$ is a finite set of states,

(ii) $\rho \subseteq S \times S$ is a transition relation (usually, we require $\rho$ to be total; that is, for each $s \in S$, there is some $s' \in S$ having $(s, s') \in \rho$),

(iii) $I \subseteq S$ is the set of initial states,

(iv) $L : S \rightarrow 2^AP$ is the labeling function, and

(v) $\mathcal{F} \subseteq 2^S$ is a set of fairness constraints.

A path of $\mathcal{M}$ is an infinite sequence $\pi = s_0s_1 \cdots$ in $S^\omega$, where $s_0 \in I$ and $(s_i, s_{i+1}) \in \rho$ for each $i \in \mathbb{N}$. In addition, $\pi$ is a fair path if $\pi$ visits each $F \in \mathcal{F}$ infinitely often. Formally, $\pi$ is a fair path if $\inf(\pi) \cap F \neq \emptyset$ for each $F \in \mathcal{F}$, where $\inf(\pi)$ denotes the set of states occurring infinitely many times in $\pi$.

An infinite word $\pi = a_0a_1 \cdots$ is derived from a path $\sigma$ of $\mathcal{M}$ (denoted by $\pi = L(\sigma)$) if $a_i = L(s_i)$ for each $i \in \mathbb{N}$. We use $\mathcal{L}(\mathcal{M})$ to denote the set of infinite words derived from fair paths of $\mathcal{M}$.

Given an ETL$_{l+f}$ formula $\varphi$ and an LTS $\mathcal{M}$, we denote by $\mathcal{M} \models \varphi$ if $\pi \models \varphi$ for each $\pi \in \mathcal{L}(\mathcal{M})$. The model checking problem of ETL$_{l+f}$ is just to verify if $\mathcal{M} \models \varphi$ holds for the given LTS $\mathcal{M}$ and the given ETL$_{l+f}$ formula $\varphi$.

3. Semantic BMC Encoding for ETL$_{l+f}$

In this section, we will give a detailed description of the semantic BMC encoding for ETL$_{l+f}$. Firstly, we show how to extend the tableau construction of LTL [20] to that of ETL$_{l+f}$, and hence a product model can also be constructed. Subsequently, we interpret the fairness path finding problem (upon the product model) into SAT, and the size blow-up of this encoding is linear with the bound.

For the sake of convenience, in this section, we always assume that the given ETL$_{l+f}$ formulae have been normalized into NNF.

3.1. The Tableaux of ETL$_{l+f}$ Formulae. Given an ETL$_{l+f}$ formula $\varphi$, we first inductively define its elementary formula set $\text{el}(\varphi)$ as follows.

(i) $\text{el}(\top) = \text{el}(\bot) = \emptyset$.

(ii) $\text{el}(p) = \text{el}(\neg p) = \{p\}$ for each $p \in AP$. 
(iii) \( \text{el}(\varphi_1 \land \varphi_2) = \text{el}(\varphi_1) \cup \text{el}(\varphi_2) \).

(iv) \( \text{el}(\varphi) = \text{el}(\varphi) \setminus \{ \varphi \} \).

(v) If \( \varphi = \mathcal{A}^f(\varphi_1, \ldots, \varphi_n) \) or \( \varphi = \neg \mathcal{A}^f(\varphi_1, \ldots, \varphi_n) \) and the states set of \( \mathcal{A}^f \) is \( Q \), then

\[
\text{el}(\varphi) = \bigcup_{1 \leq k \leq n} \text{el}(\varphi_k) \cup \left\{ \text{el}(\varphi_1, \ldots, \varphi_n) \mid q' \in Q \right\}.
\] (1)

Hence, if \( \psi \in \text{el}(\varphi) \), then \( \psi \) is either an atomic proposition or a formula rooted at the next operator.

Subsequently, we define the function \( \text{sat} \), which maps each subformula \( \varphi \) of \( \varphi \) to a set of members in \( 2^\text{el}(\varphi) \). Inductively the following hold.

(i) \( \text{sat}(\tau) = 2^\text{el}(\varphi) \), \( \text{sat}(\bot) = \emptyset \).

(ii) \( \text{sat}(\varphi) = \{ [\Gamma \subseteq \text{el}(\varphi) \mid p \in \Gamma] \} = \{ [\Gamma \subseteq \text{el}(\varphi) \mid p \notin \Gamma] \} \).

(iii) \( \text{sat}(\neg\varphi) = \{ [\Gamma \subseteq \text{el}(\varphi) \mid \psi \in \Gamma] \} \).

(iv) \( \text{sat}(\varphi_1 \land \varphi_2) = \text{sat}(\varphi_1) \cap \text{sat}(\varphi_2) \).

(v) Suppose that \( \mathcal{A} = \langle \{a_1, \ldots, a_n\}, Q, \delta, q_0, F \rangle \).

(1) If \( \mathcal{A} \) is a looping acceptance automaton or a finite acceptance automaton and \( q \notin F \), then

\[
\text{sat}(\mathcal{A}^f(\varphi_1, \ldots, \varphi_n)) = \bigcup_{1 \leq k \leq n} \left( \text{sat}(\varphi_k) \cap \bigcup_{q' \in \delta(q, a_k)} \text{sat}(\mathcal{A}^f(\varphi_1, \ldots, \varphi_n)) \right).
\] (2)

(2) If \( \mathcal{A} \) is a finite acceptance automaton and \( q \in F \), then

\[
\text{sat}(\neg\mathcal{A}^f(\varphi_1, \ldots, \varphi_n)) = 2^\text{el}(\varphi) \setminus \text{sat}(\mathcal{A}^f(\varphi_1, \ldots, \varphi_n)).
\]

Recall the tableau construction for LTL [20], an “until subformula” would generate a fairness constraint to the tableau. Indeed, such a subformula corresponds to a “least-fixpoint subformula” if we translate the specification into a logic employing higher-order quantifiers, such as \( \mu \)-calculus. Similarly, for ETL, the PF- and NL-subformulae also impose fairness constraints. For this, we need to define the following two auxiliary relations before giving the tableau construction.

For a PF-subformula \( \psi = \mathcal{A}^f(\varphi_1, \ldots, \varphi_n) \) of \( \varphi \), where \( \mathcal{A} = \langle \{a_1, \ldots, a_n\}, Q, \delta, q_0, F \rangle \), we define a relation \( \Delta_\psi^f \subseteq (2^{\text{el}(\varphi)} \times 2^Q) \times (2^{\text{el}(\varphi)} \times 2^Q) \) as follows: suppose that \( \Gamma, \Gamma' \subseteq \text{el}(\varphi) \) and \( P, P' \subseteq Q \); then (\( (\Gamma, P), (\Gamma', P') \)) \( \in \Delta_\psi^f \) if and only if the following hold.

(i) When \( P \neq \emptyset \), then, for each \( q \in P \setminus F \), there exists some \( 1 \leq k \leq n \) such that \( \Gamma \subseteq \text{sat}(\varphi_k) \) and \( P' \cap \delta(q, a_k) = \emptyset \).

(ii) When \( P = \emptyset \), then \( q \in P' \) if and only if \( \Gamma' \subseteq \text{sat}(\mathcal{A}^f(\varphi_1, \ldots, \varphi_n)) \) for each \( q \in Q \).

Likewise, for each NL-subformula \( \psi = \neg\mathcal{A}^f(\varphi_1, \ldots, \varphi_n) \) of \( \varphi \), we also define a relation \( \Delta_\psi^f \subseteq (2^{\text{el}(\varphi)} \times 2^Q) \times (2^{\text{el}(\varphi)} \times 2^Q) \). In detail, for any \( \Gamma, \Gamma' \subseteq \text{el}(\varphi) \) and \( P, P' \subseteq Q \), we have

\[
(\Gamma, P), (\Gamma', P') \in \Delta_\psi^f
\]

whenever the following hold.

(i) When \( P \neq \emptyset \), then, for each \( q \in P \) and \( 1 \leq k \leq n \), we have

\[
\Gamma \subseteq \text{sat}(\varphi_k), \quad P' \cap \delta(q, a_k) = \emptyset.
\]

(ii) When \( P = \emptyset \), then \( q \in P' \) if and only if \( \Gamma' \notin \text{sat}(\mathcal{A}^f(\varphi_1, \ldots, \varphi_n)) \) for each \( q \in Q \).

The below two theorems (Theorems 4 and 5) reveal the language property of ETL_{\infty,f} tableaux. To remove the lengthiness, we here just provide the proof sketches, and rigorous proofs of them are postponed to the appendices.

**Theorem 4.** For each \( \pi \in (2^A)^\omega \), if \( \pi \in \mathcal{L}(\mathcal{F}_\psi) \), then \( \pi \equiv \varphi \).

**Proof (sketch).** Just assume that \( \sigma = s_0s_1 \cdots \in S_\psi^\omega \) is the corresponding fair path of \( \mathcal{F}_\psi \) such that \( \pi = L_\psi(\sigma) \), where \( s_i = (\Gamma_i; P_{i1}, \ldots, P_{imj}; R_{ij1}, \ldots, R_{inn}) \). We may inductively prove the following claim.

"For each \( \psi \in \text{sub}(\varphi) \cup \text{el}(\varphi) \), we have: \( \Gamma_i \subseteq \text{sat}(\psi) \) implies \( \pi, i \equiv \psi" \).

Because we require that \( L_0 \in \text{sat}(\psi) \), hence we have \( \pi, 0 \equiv \varphi \).

**Theorem 5.** For each \( \pi \in (2^A)^\omega \), if \( \pi \equiv \varphi \), then \( \pi \in \mathcal{L}(\mathcal{F}_\psi) \).

**Proof (sketch).** Suppose that \( \pi \equiv \varphi \); to show \( \pi \in \mathcal{L}(\mathcal{F}_\psi) \), we need to first construct an infinite state sequence \( \sigma = s_0s_1 \cdots \in S_\psi^\omega \) guided by \( \pi \) (the detailed construction is given in Section A.2), and then we will subsequently show that \( \sigma \) is a fair path of \( \mathcal{F}_\psi \) and \( \pi = L_\psi(\sigma) \).
The following theorem is immediate from Theorems 4 and 5.

**Theorem 6.** The model $\mathcal{M}$ violates the ETL$_{\ell, f}$ property $\varphi$ if and only if $\mathcal{L}(\mathcal{M}) \cap \mathcal{L}(\mathcal{F}_{\varphi}) \neq \emptyset$, equivalently; there exists some fair path in $\mathcal{M} \times \mathcal{F}_{\varphi}$. 

**Theorem 7.** For an ETL$_{\ell, f}$ formula $\varphi$, its tableau $\mathcal{T}_\varphi$ has at most $4^{|\text{el}(\varphi)|}$ states.

**Proof.** Observe that a state should be of the form $(\Gamma; P_1, \ldots, P_m; R_1, \ldots, R_n)$. For $\Gamma$, there are $2^{|\text{el}(\varphi)|}$ possible choices. Suppose that $\varphi_j = \mathcal{A}_j(\varphi_1, \ldots, \varphi_k)$ (resp., $\neg \varphi_j = \neg \mathcal{A}_j(\varphi_1^1, \ldots, \varphi_1^l)$) and the state set of $\mathcal{A}_j$ is $Q_j$ (resp., $\neg \mathcal{A}_j$ with $Q'_j$). According to the construction, each $q \in Q_j$ (resp., $q \in Q'_j$) corresponds to a unique elementary formula $\mathcal{A}_j[\varphi_1, \ldots, \varphi_k]$ (resp., $\neg \mathcal{A}_j[\varphi_1^1, \ldots, \varphi_1^l]$), and such a mapping is an injection. Hence we have

$$
\left(\sum_{1 \leq j \leq m} |Q_j| + \sum_{1 \leq j \leq n} |Q'_j|\right) \leq |\text{el}(\varphi)|. 
$$
(4)

Note that $P_j \subseteq Q_j$ (resp., $R_j \subseteq Q'_j$), and hence we have $|S_p| \leq (2^{|\text{el}(\varphi)|})^2 = 4^{|\text{el}(\varphi)|}$. 

### 3.2. The Linear Semantic Encoding

Practically, a model’s state space is determined by the evaluation of a set of variables. Further, we may assume that each of them is a “Boolean variable” (which corresponds to a proposition belonging to $AP$), because every variable over finite domain could be encoded with several Boolean variables.

Let $\mathcal{C} = \langle S, \rho, I, L, \mathcal{F} \rangle$ be an arbitrary LTS, and we also assume that the corresponding variable set is $S = \{p_1, \ldots, p_m\}$; then each state $s \in S$ uniquely corresponds to an assignment of such $p_i$s.

If we use $s(p)\psi$ to denote the value of $p_i$ at $s$, then each subset $Z \subseteq S$ can be represented by a Boolean formula $\Phi_Z$ over $V$. In detail, it fulfills

$$s \in S \iff s \models \Phi_Z,$$
(5)

where $s \models \Phi_Z$ means that $\Phi_Z$ is evaluated to be true if we assign each $p_i$ with the value $s(p_i)$. Let $V' = \{p_1', \ldots, p_m'\}$, and each binary relation $\lambda \subseteq S \times S$ also has a Boolean representation $\Phi_\lambda$ over the variable set $V \cup V'$. That is,

$$(s_1, s_2) \in \lambda \iff (s_1, s_2) \models \Phi_\lambda,$$
(6)

where $(s_1, s_2) \models \Phi_\lambda$ means that $\Phi_\lambda$ is evaluated to be true if we assign each $p_i$ with $s_i(p)$, and each $p'_j$ with $s_j(p)$.

Hence, all components of $\mathcal{M}$ can be encoded: $I$ and $p$ can be represented by two Boolean formulae $\Phi_I$ and $\Phi_p$, respectively; we subsequently create a Boolean formula $\Phi_F$ for each $F \in \mathcal{F}$; note that the labeling function $L$ is not concerned any longer, because the states labeled with $p$ can be captured by the Boolean formula $p$.

For example, from Theorem 7, we have that the symbolic representation of $\mathcal{F}_p$ requires $2 \times |\text{el}(\varphi)| \setminus AP$ new Boolean variables—because variables in $\text{el}(\varphi) \setminus AP$ can be shared with the encoding of the original model.

A canonical Boolean encoding of fair path existence detection upon LTSs is presented in [22]: given a model $\mathcal{C} = \langle S, \rho, I, L, \mathcal{F} \rangle$ and a bound $k \in \mathbb{N}$, one may use the formula

$$
\Phi^{(0)}_I \land \bigvee_{0 \leq i < k} \Phi^{(i+1)}_\rho \land \bigvee_{0 \leq \ell < k} \left( \Phi^{(k; \ell)}_p \land \bigvee_{F \in \mathcal{F}} \bigvee_{0 \leq i < k} \Phi^{(i)}_F \right),
$$
(7)

where $\Phi^{(0)}_I$ and $\Phi^{(i)}_F$ are, respectively, the Boolean formulae obtained from $\Phi_I$ and $\Phi_F$ by replacing each variable $p$ with a new copy $p^{(i)}$, and $\Phi^{(k; \ell)}_p$ is obtained from $\Phi_p$ by replacing each $p$ with $p^{(i)}$ and replacing each $p'$ with $p^{(j)}$.

It can be seen that this formula is satisfiable if and only if $\mathcal{C}$ involves a fair path of the form $s_0, s_1, \ldots, s_{k-1}(s_k \ldots s_k)$ (call it is of the lasso shape). Since $\mathcal{L}(\mathcal{C}) \neq \emptyset$ if and only if $\mathcal{C}$ contains some lasso fair path (note that from each fair path we may derive another fair path of lasso shape), hence we may convert the fair path detection into the satisfiability problem of the above Boolean formula.

However, a closer look shows that the size of such encoding is quadratic with the bound. To reduce the blow-up in size, we need to introduce the following new variables (the linearization can also be done with the syntactic fashion presented in [23, 24]. We would draw a comparison of these two approaches in Section 4.).

1. For each $0 \leq \ell \leq k$, we introduce a new variable $r_\ell$. Intuitively, $r_\ell$ indicates that $s_\ell$ is a successor of $s_k$.

2. For each fairness constraint $F \in \mathcal{F}$ and each $0 \leq \ell \leq k$, we introduce a variable $f^{(\ell)}_F$, and this variable is evaluated to be true only if there is some $\Phi^{(\ell)}_F$ which is evaluated to true, where $\ell \leq j \leq k$.

And the new encoding (with the bound $k \in \mathbb{N}$) can be formulated as

$$
\Phi^{(0)}_I \land \bigvee_{0 \leq i < k} \Phi^{(i+1)}_\rho \land \bigvee_{0 \leq \ell < k} r_\ell,
$$
$$
\psi^{(k)}_\mathcal{C} = \bigwedge_{0 \leq \ell < k} \left( r_\ell \rightarrow \left( \Phi^{(k; \ell)}_p \land \bigvee_{F \in \mathcal{F}} f^{(\ell)}_F \right) \right)
$$
(8)

$$
\land \bigwedge_{F \in \mathcal{F}} \left( f^{(j)}_F \rightarrow \left( f^{(j+1)}_F \lor \Phi^{(j)}_F \right) \right)
$$

Hence, both the number of variables and the size of this encoding are linear with $k$. Moreover, the following theorem guarantees the correctness of such encoding.

**Theorem 8.** $\mathcal{L}(\mathcal{C}) \neq \emptyset$ if and only if $\psi^{(k)}_\mathcal{C}$ is satisfiable for some $k$. 

Proof. We begin with the “if” direction: suppose that the variable set is \( \{p_1, \ldots, p_m\} \); if there is some \( k \) such that \( \Psi_{\rho}^{(k)} \) is evaluated to \( 1 \) (i.e., true) under the assignment \( e \), then we denote \( s_i = (e(p_{i1}^{(0)}), \ldots, e(p_{im}^{(0)})) \) for each \( 1 \leq i \leq m \). Hence, each \( s_i \) is a state of \( \mathcal{C} \).

(i) Since the truth value of \( \Phi_{\rho}^{(0)} \) is \( 1 \) under \( e \), then we have \( s_0 \vdash \Phi_{\rho}^{(0)} \); this implies that \( s_0 \in I \).

(ii) For each \( 0 \leq i < k \), we have \( (s_i, s_{i+1}) \vdash \Phi_{\rho}^{(i+1)} \), and thus \( (s_i, s_{i+1}) \in \rho \).

(iii) Because we have the conjunct \( \bigvee_{0 \leq \ell \leq k} \), then there is some \( 0 \leq \ell \leq k \) such that \( e(r_{\ell}) = 1 \). In the following, we fix this specific value \( \ell \) for the discussion.

(iv) According to the constraint \( r_{\ell} \rightarrow (\Phi_{\rho}^{(k, \ell)} \land \bigwedge_{F \in \mathcal{F}} f_{F}^{(\ell)}(k)) \), we have the following.

\[
\begin{align*}
(1) & \quad e(\Phi_{\rho}^{(k, \ell)}) = 1, \text{ which indicates that } (s_{k}, s_{k}) \in \rho. \\
(2) & \quad \text{For each } F \in \mathcal{F}, \text{ we have } e(f_{F}^{(\ell)}) = 1.
\end{align*}
\]

(v) For each fairness constraint \( F \in \mathcal{F} \) and \( 0 \leq i \leq k \), we now inductively show that \( e(f_{F}^{(i)}) = 1 \) implies \( e(\Phi_{\rho}^{(i)}) = 1 \) (alternatively, \( s_i \in F \) for some \( i \leq j \leq k \)."

First of all, it holds in the case of \( k = 1 \), because we have the constraint \( f_{F}^{(i)} \rightarrow \Phi_{\rho}^{(i)} \). In addition, the fact of “when \( i = c \), it holds” can be immediately inferred from the hypothesis “when \( i = c + 1 \), it holds,” according to the conjunct \( f_{F}^{(i)} \rightarrow (f_{F}^{(i+1)} \lor \Phi_{F}^{(i)}) \). Since we have shown that \( e(f_{F}^{(i)}) = 1 \), we can conclude that there exists some \( \ell \leq j \leq k \) such that \( s_j \in F \).

The above shows that \( s_0 s_1 \cdots s_{j-1} s_j \cdots s_k \) is a fair path of \( \mathcal{C} \), and hence \( \mathcal{L}(\mathcal{C}) \neq \emptyset \).

Conversely, for the "only if" direction, it suffices to find some \( k \) and some assignment \( e \) evaluating \( \Psi_{\rho}^{(k)} \) to be true. Since \( \mathcal{L}(\mathcal{C}) \neq \emptyset \), there must exist some fair path of lasso shape in \( \mathcal{C} \). Without loss of generality, assume that \( \sigma = s_0 s_1 \cdots s_{j-1} s_j \cdots s_k \) is such a path; just let \( k \) be this value, and we now illustrate how the assignment \( e \) is constructed.

(i) For each variable \( p_i \) and each \( i \leq k \), let \( e(p_i^{(0)}) = s_i(p_i) \). Since \( s_0 \) is an initial state, according to the definition, we have \( e(\Phi_{\rho}^{(0)}) = 1 \). Meanwhile, because each \( (s_i, s_{i+1}) \in \rho \), we have that the conjunction \( \bigwedge_{0 \leq j \leq k}(\Phi_{\rho}^{(i+j+1)}) \) is satisfied under \( e \).

(ii) For each \( 0 \leq i \leq k \), we let

\[
e(r_{\ell}) = \begin{cases} 
1, & i = \ell, \\
0, & i \neq \ell.
\end{cases}
\]

Then it can be seen that \( e(\bigvee_{0 \leq \ell \leq k} r_{\ell}) = 1 \).

(iii) For each \( F \in \mathcal{F} \) and each \( 0 \leq i \leq k \), we let

\[
e(f_{F}^{(i)}) = \begin{cases} 
1, & \text{if there is some } j \geq i \text{ such that } s_j \in F, \\
0, & \text{otherwise}.
\end{cases}
\]

Then it can be directly checked that the conjunct

\[
\bigwedge_{F \in \mathcal{F}} \left( \bigwedge_{0 \leq i \leq k} \left( f_{F}^{(i)} \rightarrow \left( f_{F}^{(i+1)} \lor \Phi_{F}^{(i)} \right) \right) \land \left( f_{F}^{(k)} \rightarrow \Phi_{F}^{(k)} \right) \right)
\]

is evaluated to be true under \( e \).

(iv) Since \( (s_k, s_{k}) \in \rho \), we have \( e(\Phi_{\rho}^{(k, \ell)}) = 1 \). Also note that \( \sigma \) is a fair path; then for each \( F \in \mathcal{F} \) there is some \( s_j \in F \), where \( \ell \leq j \leq k \). According to the previous definition, we can infer that \( e(\bigwedge_{F \in \mathcal{F}} f_{F}^{(\ell)}) = 1 \). Thus the conjunct

\[
\bigwedge_{0 \leq i \leq k} \left( r_{\ell} \rightarrow \left( \Phi_{\rho}^{(k, \ell)} \land \bigwedge_{F \in \mathcal{F}} f_{F}^{(\ell)} \right) \right)
\]

is also satisfied under \( e \) (recall that we have assigned \( e(r_i) = 0 \) in the case of \( i \neq \ell \).)

Thus, the formula \( \Psi_{\rho}^{(k)} \) is satisfiable.

For bounded model checking, an important issue is the completeness threshold, which is the specific value \( k \) such that we may declare \( \mathcal{L}(\mathcal{C}) = \emptyset \) in the case that \( \Psi_{\rho}^{(k)} \) is not satisfiable, and we denote it by \( CT(\mathcal{C}) \) in this paper.

Since we need only to concern about fair paths of the form \( \sigma_1(\sigma_2)^{w}, \) as pointed in [22], a possible candidate for the completeness threshold \( CT(\mathcal{C}) \) is

\[
D^I(\mathcal{C}) + |\mathcal{F}| \times D(\mathcal{C}),
\]

where \( D \) and \( D^I \) are, respectively, the diameter and the initial diameter (cf. [22]). Since [22] just considers LTSs having only one fairness constraint, we here add the factor \( |\mathcal{F}| \).

Observe that the part \( \sigma_1 \) must be enclosed in some SCC (i.e., strongly connected component) of \( \mathcal{C} \), and we may replace \( D(\mathcal{C}) \) with \( D(\mathcal{F}) \), where \( \mathcal{F} \) is the largest SCC that intersects all fairness constraints. Therefore, we may get a more compact upper bound of the completeness threshold.

Then, for a given LTS \( \mathcal{M} \) and the given ETL formula \( \varphi \), since we have shown that \( \mathcal{M} \models \varphi \) if and only if \( \mathcal{M} \times \mathcal{T}_{\varphi} \) involves some fair path, we now just need to test if there is some \( k \) making \( \Psi_{\rho}^{(k)} \) satisfiable, where \( k \leq CT(\mathcal{M} \times \mathcal{T}_{\varphi}) \).

Remark 9. In the case that \( \mathcal{C} = C_1 \times C_2 \), where \( \mathcal{C} = \langle S, \rho, I, L, \mathcal{F} \rangle \) and \( \mathcal{C}_1 = \langle S_1, \rho_1, I_1, L_1, \mathcal{F}_1 \rangle \) for \( i = 1, 2 \), we have \( \Phi_{\mathcal{C}} = \Phi_{\mathcal{C}_1} \land \Phi_{\mathcal{C}_2} \), \( \Phi_{\rho} = \Phi_{\rho_1} \land \Phi_{\rho_2} \), and \( \Phi_{\mathcal{F}} = \Phi_{\mathcal{F}_1} \cup \Phi_{\mathcal{F}_2} \), and in addition, the variable set of \( \mathcal{C} \) is just the union of the variable sets of \( \mathcal{C}_1 \) and \( \mathcal{C}_2 \).

Remark 10. Actually, for an ETL formula \( \varphi \), the symbolic representation of \( \mathcal{T}_{\varphi} \) can be directly given without the detour of explicit construction of the LTS. Because, the relation sat could be inductively constructed if we introduce corresponding new variables in \( e(\varphi) \). Subsequently, encodings of \( \Phi_{\Delta_1} \) or \( \Phi_{\Delta_2} \) could be naturally obtained from the underlying Boolean variables corresponding to states of automata connectives. Hence, the Boolean representation of \( \Phi_{\rho_\Delta} \) is obtained. And, encodings of other components are as routine.
4. Experimental Results

To justify our idea, we have integrated (the tool is available at https://sourceforge.net/projects/enusmv12/) the ETL\(_{l+f}\) BMC algorithm into ENuSMV (Ver. 1.2). This tool is completely compatible with NuSMV [25], and it allows end-users to customize new temporal connectives by defining automata.

For example, Figure 1 illustrates how to declare a finite acceptance automata connective (to define a looping acceptance automata connective, just replace the keyword FIN with LOOP), namely, A. Since it has three states q1, q2, and q3 (where q1 is the initial state and q3 is an accepting state), then A[q1], A[q2], and A[q3] are also connectives—for example, A[q2] just replaces the initial state with q2. Subsequently, one may define ETL\(_{l+f}\) specifications; for example,

\[
\text{ETLSPEC } A(p, A[q2] (q,p))
\]

is a proper declaration.

In this redistribution, both BDD-based and bounded model checkings for ETL\(_{l+f}\) are supported. To perform (semantic encoding based) BMC, we need to use the command option bmc.tab. We have conducted some experiments to test the correctness and efficiency of our algorithm. In this paper, we are especially concerned with the following issues.

(1) The comparison of BDD-based symbolic model checking and bounded model checking.

(2) The overhead contrast in verifications of ETL\(_{l}\) and ETL\(_{l+f}\) upon both star-free and nonstar-free properties.

(3) The comparison of performances with syntactic/semantic BMC of LTL and semantic BMC of ETL\(_{l+f}\).

To compare the efficiencies between BDD-based MC and BMC, we chose the (distributed mutual exclusion) DME circuit as the model (which involves a buggy design), as described in [3]. It consists of \(n\) cells for \(n\) users that want to have exclusive access to a shared resource. We conducted the experiment by describing the liveness property that “a request for using the resource will eventually be acknowledged” (with ETL\(_{l+f}\) formula). The max bound are set to 100, and the comparative results are shown in Table 1, where “C.L.” stands for the length of counterexample.

As a previous work, we have implemented the symbolic model checking algorithm for ETL\(_{l}\) in ENuSMV 1.0. To justify that in general ETL\(_{l+f}\) could be more effectively checked, we would make a comparison of BMC for ETL\(_{l}\) and ETL\(_{l+f}\).

To draw the comparison upon non-start-free regular properties, we use a “mod 2\(^{n}\)” counter as the model. The model consists of \(n\) “cells” bit\(_0\), ..., bit\(_{n-1}\). Each cell is a (mod 2) counter having an input carry.in and an output signal carry.out. These cells are connected in a serial manner; that is, bit\(_0\)’s carry.in is set to 1, and bit\(_i\)’s carry.in is connected to bit\(_{i-1}\)’s carry.out as described in Figure 2.
We, respectively, describe the periodicity property that “bit_0 carries out at every even (except for 0) moment” with \( \text{ETL}_f \) and \( \text{ETL}_{l,f} \). We set the time bound to 1 hour, and Table 2 provides the max bounds (together with related information) which can be handled by the SAT solver within the time bound. From it, we can see that a deeper search could be done when specifications are described with \( \text{ETL}_{l,f} \).

To compare the overhead of \( \text{ETL}_f \) and \( \text{ETL}_{l,f} \) upon star-free properties, we would first use the DME model to check the safety property: “no two cells will be simultaneously acknowledged.” The results are shown in Table 3, and the time bound is also set to 1 hour.

At the same time, we can also compare the verification performances of the DME model upon the aforementioned liveness property that “each request will be acknowledged in the further.” Note that for this property, the verification could be accomplished within the given time bound, and a counterexample could be detected at the bound \( k = 39 \). The comparative results are given in Table 4.

The last group of experiments aims at comparing the efficiencies of (syntactic/semantic) LTL BMC and \( \text{ETL}_{l,f} \). First of all, for LTL BMC, we are also concerned with two types of encoding approaches.

1. The Syntactic Approach. We here adopt the linear incremental syntactic encoding proposed in [26]—to the best of our knowledge, this is the most effective syntactic encoding for full LTL.

2. The Semantic Approach. ENuSMV 1.2 also supports semantic encoding for LTL—which is tailored from our linear encoding presented in Section 3.2.

We still use the DME circuit as the model and the liveness property as specification; Table 5 provides the experimental results on LTL BMC based on syntactic and semantic encodings. From that, we can see that, with semantic encoding, it tends to generate less clauses and tends to terminate earlier than that with the syntactic encoding, whereas the latter requires fewer variables.

Meanwhile, we can also make a comparison between Tables 4 and 5; we may find that the variable numbers of semantic ETB BMC and LTL BMC are almost at a fixed ratio—for this experiment, the ratio is 1.09 (approximately).

### 5. Concluding Remarks

The logic \( \text{ETL}_{l,f} \) is a variant of extended temporal logic, it employs both finite and looping acceptance automata connectives, and it can be considered a mixture of \( \text{ETL}_f \) and \( \text{ETL}_l \). Thus, any omega-regular properties can be succinctly described with this kind of logic, particularly for safety and liveness properties.

We have presented the semantic bounded model checking algorithm for \( \text{ETL}_{l,f} \). The central part of this approach is the tableau construction. Meanwhile, we also illustrate how to give a linear BMC encoding for it. To justify it, we have implemented the presented algorithm (in ENuSMV 1.2). Experimental results show that \( \text{ETL}_{l,f} \) could be more efficiently verified via BMC (in comparison to our previous implementation for \( \text{ETL}_{l,f} \)).

In this paper, verification of \( \text{ETL}_r \), namely, extended temporal logic using Büchi (alternatively, repeating) automata as connectives, has not been studied. This is partly because of the inherited difficulties of Büchi complementation [27]. Indeed, we may mimic the ranking complementing technique of Büchi automata [28–30]. However, this would cause an asymptotically quadratic blow-up of variable number in building the tableaux. Hence, a further work is about to study the semantic BMC encodings of \( \text{ETL}_r \).

### Appendix

#### A. Omitted Proofs

**A.1. Proof of Theorem 4.** Just assume that \( \sigma = s_0 s_1 \cdots \in S^\omega_p \) is the corresponding fair path of \( \omega \) having \( \pi = L_p(\sigma) \), where \( s_i = (\Gamma_0 ; R_{i,1} \cdots , R_{i,1} , \ldots , R_{i,m}) \). We now inductively prove the following claim.

“For each \( \psi \in \text{sub}(\varphi) \cup \text{el}(\varphi) \), we have: \( \Gamma_i \in \text{sat}(\psi) \) implies \( \pi, i \models \psi \).”

(i) The basic cases are trivial.

(a) \( \varphi = \top \), or \( \varphi = \bot \). Since \( \pi, i \models \top \) holds trivially, the case \( \Gamma_i \in \text{sat}(\bot) \) never happens.
(b) \( \psi = p \) or \( \psi = \neg p \), where \( p \in AP \). Because \( \Gamma_i \in sat(p) \) if and only if \( p \in \Gamma_i \), if and only if \( p \in \pi(i) \) if and only if \( \pi, i \models p \). Similar to show it when \( \psi = \neg p \).

(ii) The following inductions are as routine.

(a) For the case \( \psi = \psi_1 \land \psi_2 \), or \( \psi_1 \lor \psi_2 \). For the first case, we have \( \Gamma_i \in sat(\psi_1) \) if and only if \( \Gamma_i \in sat(\psi_2) \); by induction, we have \( \pi, i \models \psi_1 \) and \( \pi, i \models \psi_2 \); hence \( \pi, i \models \psi \); similar to the case of \( \psi = \psi_1 \lor \psi_2 \).

(b) In the case of \( \psi = \sigma^j \psi \), we have \( \Gamma_i \in sat(\psi) \) if and only if \( \Gamma_i \in sat(\psi_i) \), according to the definition of \( \Delta_\psi \) (note that in this case \( \psi \) is an elementary formula of \( \Phi \)). By induction, we have \( \pi, i \models \psi \); hence \( \pi, i \models \psi \).

(iii) If \( \psi = \sigma^j(\psi_1, \ldots, \psi_k) \) is a PF-subformula, without loss of generality, assume \( \psi = \psi_i \) (i.e., the \( j \)th PF-subformula of \( \Phi \)), where \( 1 \leq j \leq m \) and \( \sigma^j \phi = \{a_1, \ldots, a_k \}, Q, \delta, q, F \), then the proof is given as follows.

Since \( \sigma \) is a fair path, there exists \( i_2 > i_1 > i \), such that \( P_{j,i_1} = P_{j,i_2} = 0 \) and \( P_{jx} \neq 0 \) for each \( i_1 < c < i_2 \).

(a) First, let \( q_0 = q_i \); then we have \( \Gamma_i \in sat(\sigma^j(\psi_1, \ldots, \psi_k)) \).

(b) For each \( t \leq i_1 - i \), if \( q_i \notin F \) and \( \Gamma_{i,t} \in sat(\sigma^j(\psi_1, \ldots, \psi_k)) \), then, according to the definition of \( sat \), there is some \( 1 \leq k_i \leq k \) and a \( q' \) such that \( \Gamma_{i,t} \in sat(q_{k_i}) \), \( q' \equiv q_i \), \( q_i \in \sigma^j(\psi_1, \ldots, \psi_k) \), and \( \Gamma_{i,t} \in sat(\sigma^j(\psi_1, \ldots, \psi_k)) \) (equivalently, \( \Gamma_{i,t+1} \in sat(\sigma^j(\psi_1, \ldots, \psi_k)) \), as discussed above). Now, we let \( q_{i+1} = q' \).

Till now, if there is some \( t \) having \( q_t \in F \), we stop the processing. Otherwise, we go on with the following procedure.

(a) When \( t = i_1 - i + 1 \), we have \( \Gamma_i \in sat(\sigma^j(\psi_1, \ldots, \psi_k)) \).

Since \( P_{j,i_1} = 0 \), according to the definition of \( \Delta_\psi \), we have \( q_t \in P_{j,i_1+1} = P_{j,i_2+1} \).

(b) For each \( i_1 < t < i_2 - i \), if \( q_i \notin F \), according to \( \Delta_\psi \), there is some \( 1 \leq k_i \leq k \), such that \( \Gamma_{i,t} \in sat(q_{k_i}) \), and there is some \( q' \in P_{j,i+1} \cap \delta(q_{k_i}) \). Now, we let \( q_{i+1} = q' \).

Notice that \( P_{j,i_2} = 0 \), and we have the inductive assertion that \( q_i \notin F \) implies \( q_i \in P_{j,i_1} \); hence there must exist some \( b_q \in F \). Thus, \( \sigma^j \Phi \) have some accepting prefix \( a_1 a_2 \cdots a_k \) of some infinite word. On the other hand, by induction, \( \Gamma_{i,t} \in sat(q_{k_i}) \) implies \( \pi, i + t = \sigma^j(F) \). Hence, we have \( \pi, i \models \psi \) by definition.

(iv) If \( \psi = \neg \sigma^j(\psi_1, \ldots, \psi_k) \) is an NF-subformula of \( \Phi \) and assume that \( \sigma^j \phi = \{a_1, \ldots, a_k \}, Q, \delta, q, F \), then the proof is given as below.

Assume by contradiction it is not the case; then \( \pi, i \models \sigma^j(F(q_0, \ldots, q_k)) \) holds. Therefore, there exist some accepting prefix \( a_1 a_2 \cdots a_k \) of some infinite word and a state sequence \( q_0 q_1 \cdots q_{i-1} q_i \) such that

(a) \( q_0 = q_i \), \( q_{i+1} \in F \) and each \( q_{i+1} \in \delta(q_t, a_k) \),

(b) for each \( t > \ell \), we have \( \pi, i + t = \sigma^j(F) \).

Then, we have the following facts.

(a) \( \Gamma_{i,t+1} \in sat(\sigma^j(\psi_1, \ldots, \psi_k)) = \sigma^j(\psi_1) \), because \( q_{i+1} \in F \).

(b) Assume that \( \Gamma_{i,t+1} \in sat(\sigma^j(\psi_1, \ldots, \psi_k)) \), where \( t > \ell \); then \( \Gamma_{i,t+1} \in sat(\sigma^j(\psi_1, \ldots, \psi_k)) \). In addition, \( \pi, i + t = q_{i+1} \) implies that \( \Gamma_{i,t} \in sat(q_{i+1}) \); otherwise (it is not hard to show that if there is an infinite path in \( \Phi \) starting from \( s_j \), then, for each \( q \), either \( \Gamma_{i,t} \in sat(q) \) or \( \Gamma_{i,t} \in sat(\neg q) \) holds), \( \Gamma_{i+1} \in sat(\neg q_k) \); then we have \( \pi, i + t = \neg q_k \) by induction contracts. Hence, by the definition of \( sat \), we have \( \Gamma_{i,t} \in sat(\sigma^j(\psi_1, \ldots, \psi_k)) \).

Then, we have \( \Gamma_{i+1} \in sat(\sigma^j(\psi_1, \ldots, \psi_k)) \) when \( t = 0 \). However, it contradicts the premise \( \Gamma_i \in sat(\neg \sigma^j(q_1, \ldots, q_k)) \), because \( q_0 = q_i \). Therefore, the assumption \( \pi, i \models \sigma^j(\psi_1, \ldots, \psi_k) \) is a falsity, and this implies that \( \pi, i \models \psi \) holds.

(v) If \( \psi = \sigma^j(q_1, \ldots, q_k) \) is a PL-subformula of \( \Phi \), where \( \sigma^j \phi = \{a_1, \ldots, a_k \}, Q, \delta, q, F \), then we have the following proof in the case that \( \Gamma_i \in sat(\psi) \).

(a) Let \( q_0 \in F \), and \( \Gamma_i \in sat(\sigma^j(\psi_1, \ldots, \psi_k)) \).

(b) For each \( t \geq 0 \), assume that \( \Gamma_{i,t} \in sat(\sigma^j(\psi_1, \ldots, \psi_k)) \); then by the definition of \( sat \), there is some \( 1 \leq k_i \leq k \), such that \( \Gamma_{i,t} \in sat(q_{k_i}) \), and there is
Table 5: Comparison of syntactic/semantic LTL BMC with liveness properties.

<table>
<thead>
<tr>
<th>Cells</th>
<th>Time (s)</th>
<th>Syntactic LTL BMC encoding</th>
<th>Semantic LTL BMC encoding</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>9.34</td>
<td>2052 5474 32.66</td>
<td>8.59 2128 4291 24.79</td>
</tr>
<tr>
<td>4</td>
<td>16.71</td>
<td>2736 6806 35.74</td>
<td>10.87 2812 5623 28.44</td>
</tr>
<tr>
<td>5</td>
<td>24.06</td>
<td>3420 8138 37.02</td>
<td>15.90 3469 6955 32.28</td>
</tr>
</tbody>
</table>

For each $i \geq 0$, we let $\Gamma_i = \{\psi \in \text{el}(\varphi) | \pi, i \vdash \psi\}$. We will now show the following claim.

“For each $\psi \in \text{sub}(\varphi) \cup \text{el}(\varphi)$, we have $\Gamma_i \in \text{sat}(\psi)$ if and only if $\pi, i \vdash \psi$.”

By induction of the structure of $\psi$ the following hold.

(a) Cases are trivial when $\psi = \bot$ or $\psi = \top$.

(b) If $\psi = p \in AP$, then $\psi \in \text{el}(\varphi)$. Thus, $\Gamma_i \in \text{sat}(p)$ if and only if $\Gamma_i \in \text{sat}(\psi)$.

(c) Another basic case is $\psi = \psi' \lor \psi''$: note that in this case we also have $\psi \in \text{el}(\varphi)$; hence $\Gamma_i \in \text{sat}(\psi'')$ if and only if $\Gamma_i \in \text{sat}(\psi' \lor \psi'')$. By induction, we have $\pi, i \vdash \psi'$ and $\pi, i \vdash \psi''$ if and only if $\pi, i \vdash \psi$. Similar to show the case of $\psi = \psi' \land \psi''$.

(d) If $\psi = \psi_1 \land \psi_2$, then $\Gamma_i \in \text{sat}(\psi)$ if and only if $\Gamma_i \in \text{sat}(\psi_1)$ and $\Gamma_i \in \text{sat}(\psi_2)$. By induction, we have $\pi, i \vdash \psi_1$ and $\pi, i \vdash \psi_2$ if and only if $\pi, i \vdash \psi$. Similar to show the case of $\psi = \psi_1 \lor \psi_2$.

(e) If $\psi = \varphi^l(\varphi_1, \ldots, \varphi_k)$, where $\varphi^l = \langle \{a_1, \ldots, a_k\}, Q, \delta, q, F \rangle$ and $\varphi$ is a looping acceptance automaton or a finite acceptance automaton, but $q \notin F$, it is not difficult to show that

$$\varphi^l(\varphi_1, \ldots, \varphi_k) \iff \bigwedge_{1 \leq t \leq k} \left( \varphi_t \land \bigvee_{q' \in \delta(q,a_t)} \varphi^l_t(\varphi_1, \ldots, \varphi_k) \right).$$

Then by induction and according to the scheme

$$\text{sat}(\psi'') = \text{sat}(\psi' \lor \psi'') \land \text{sat}(\psi') \land \text{sat}(\psi'') = \text{sat}(\psi) \land \text{sat}(\psi') \land \text{sat}(\psi'')$$

and

$$\Gamma_i \in \text{sat}(\psi_1 \land \psi_2)$$

we have $\pi, i \vdash \psi$ if and only if

$$\Gamma_i \in \bigcup_{1 \leq t \leq k} \left( \text{sat}(\varphi_t) \land \bigcup_{q' \in \delta(q,a_t)} \text{sat}(\varphi^l_t(\varphi_1, \ldots, \varphi_k)) \right) = \text{sat}(\varphi^l(\varphi_1, \ldots, \varphi_k)).$$

Otherwise, if $\varphi$ is a finite acceptance automaton and $q \in F$, then

$$\varphi^l(\varphi_1, \ldots, \varphi_k) \iff \top.$$
Now, we have the following properties.

(1) Since \( \pi, 0 \models \varphi \), we have \( \Gamma_0 \in \text{sat}(\varphi) \), and hence \( s_0 \in I_\varphi \).
(2) For each \( i \) and each \( \psi \in \text{el}(\varphi) \), we have \( \Gamma_i \in \text{sat}(\psi) \) if and only if \( \pi, i \models \psi \) if and only if \( \pi, i + 1 \models \psi \) if and only if \( \Gamma_{i+1} \in \text{sat}(\psi) \).
(3) For each \( p \in AP \) and each \( i \), we have \( p \in \pi(i) \) if and only if \( \pi, i \models p \) if and only if \( p \in \Gamma_i \). Hence, \( \pi(i) = \Gamma_i \cap AP \).

(ii) The construction of \( P_{j,i} \), for \( 1 \leq j \leq m \) is as follows.
Assume that the \( j \)-th PF-subformula \( \psi_j = \sigma^j(\varphi_1, \ldots, \varphi_k) \) and the automata connective \( \sigma^j = (\{a_1, \ldots, a_k\}, Q, \delta, q, F) \); then the construction is as follows.

(a) We will find a series of “key positions" \( \epsilon_0, \epsilon_1, \ldots \), having \( P_{j,i}, \epsilon_0 = \emptyset \) for each \( \epsilon_i \). First, let \( \epsilon_0 = 0 \), and, for each \( t \geq 0 \) once \( \epsilon_t \) has been determined, we use the following two steps to determine \( \epsilon_{t+1} \) and each \( P_{j,i}, \epsilon_t < c < \epsilon_{t+1} \).

(b) Let \( P_{j,i}, \epsilon_t = 0 \), and let \( P_{j,i}, \epsilon_{t+1} = \{q' \mid \pi, \epsilon_t + 1 \models \sigma^j(\varphi_1, \ldots, \varphi_k)\} \). For each \( q' \in P_{j,i}, \epsilon_{t+1} \), there must exit a finite word \( w_{q'} = a_{k+1} \cdots a_k \), and a finite state sequence \( x_{q'} = q_0 q_1 \cdots q_{s-1} q_s \), such that \( q_0 = q' \), \( q_s \in F \), and, for each \( s \leq s \leq s \), we have \( q_{s+1} \in \delta(q_s, a_k) \) and \( \pi, \epsilon_t + c + 1 \models \sigma^j(q_0, \ldots, q_s) \) (equivalently, \( \Gamma_{j,i+1} \in \text{sat}(\sigma^j) \)).

(c) Now, let \( \epsilon_{t+1} = \epsilon_t + \max\{||x_{q'}| \mid q' \in P_{j,i}, \epsilon_{t+1} \} \) + 1. And we let

\[
P_{j,i} = \{x_{q'} (c - \epsilon_t - 1) > |x_{q'}| > c - \epsilon_t - 1 \}
\]

for each \( \epsilon_t + 1 < c < \epsilon_{t+1} \), where \( \chi_{x_{q'}}(s) \) is the \( s \)-ith element of \( x_{q'} \).

Now, it is not hard to check that \( (\Gamma, P_{j,i}, (\pi(i+1), P_{j-1})) \in \Delta^+_{\psi_j} \) for each \( i \). Moreover, for each \( t \), we have \( P_{j,i}, \epsilon_t = \emptyset \).

(iii) The construction of \( R_{j,i} \) for each \( 1 \leq j \leq n \) is as follows.
Assume that the \( j \)-th NL-subformula \( \eta_j = \neg \sigma^j(\varphi_1, \ldots, \varphi_k) \) and the automata connective \( \sigma^j = (\{a_1, \ldots, a_k\}, Q, \delta, q, F) \); then the construction is as follows.

(a) First, let \( \epsilon_0 = 0 \), and, for each \( t \geq 0 \), once \( \epsilon_t \) is decided, we use the following steps to determine \( \epsilon_{t+1} \) and each set \( R_{j,i} \) for \( \epsilon_t < c < \epsilon_{t+1} \).

(b) Let \( R_{j,i}, \epsilon_t = 0 \), and let \( R_{j,i}, \epsilon_{t+1} = \{q' \mid \Gamma_{i+1} \in \text{sat}(\neg \sigma^j(\varphi_1, \ldots, \varphi_k))\} \). For each \( c \geq \epsilon_t + 1 \), let

\[
R_{j,i+1} = \bigcup_{q' \in R_{j,i}} \{\delta q' a_k | 1 \leq s \leq k, \Gamma_c \in \text{sat}(\varphi_s)\}.
\]

(c) Since we have shown that \( \Gamma, i \models \psi \) if and only if \( \pi, i \models \psi \) for every \( \psi \in \text{sub}(\varphi) \cup \text{el}(\varphi) \), it is not hard to show that if \( R_{j,i}, \epsilon_t \neq \emptyset \), then there is some \( c > \epsilon_t + 1 \) such that \( R_{j,i} = \emptyset \)—otherwise (because, if \( R_{j,i} \neq \emptyset \) for each \( t > \epsilon_t \) using König’s lemma, we may find a run of \( \sigma^j \) over some infinite word), we can show

\[
\pi, \epsilon_t + 1 \models \sigma^j(\varphi_1, \ldots, \varphi_k) \text{ for some } q' \in R_{j,i+1},
\]

and this implies that \( \Gamma_{i+1} \in \text{sat}(\sigma^j(\varphi_1, \ldots, \varphi_k)) \), which is contradiction!

If \( R_{j,i}, \epsilon_t = \emptyset \), let \( \epsilon_{t+1} = \epsilon_t + 1 \); otherwise, let \( \epsilon_{t+1} = c \).

According to the construction, it can be examined that \( (\Gamma, R_{j,i}, (\Gamma_{i+1}, R_{j-1})) \in \Delta^+_{\psi_j} \) for each \( i \). In addition, we have \( R_{j,i} = \emptyset \) for each \( t \geq 0 \).

Taking all the above into account, by definition, we may conclude that \( (s_i, s_{i+1}) \in \rho \) for every \( i \geq 0 \); hence \( \sigma \) is a fair path of \( \mathcal{F} \). According to the construction of \( \Gamma \), we have that \( \pi = L^j(\sigma) \); hence \( \pi \in \mathcal{L}(\mathcal{F}_\psi) \).

Acknowledgments

The authors thank the anonymous reviewers for their helpful comments on a previous version of this paper. This work is supported by the NSFC in China under grant number 6103012, 61272335, 61133007, 91118007, 612106006, the 863 Program 2011AA010106, 2012AA011201, and the Program for New Century Excellent Talents in University.

References


Submit your manuscripts at http://www.hindawi.com