Program Monitoring with LTL in EAGLE

Howard Barringer*  Allen Goldberg, Klaus Havelund  Koushik Sen†
University of Manchester, England  Kestrel Technology, NASA Ames Research Center, USA  University of Illinois, Urbana Champaign, USA

Abstract

We briefly present a rule-based framework, called EAGLE, shown to be capable of defining and implementing finite trace monitoring logics, including future and past time temporal logic, extended regular expressions, real-time and metric temporal logics (MTL), interval logics, forms of quantified temporal logics, and so on. In this paper we focus on a linear temporal logic (LTL) specialisation of EAGLE. For an initial formula of size \( m \), we establish upper bounds of \( O(m^{2^m} \log m) \) and \( O(m^{2^m \log^2 m}) \) for the space and time complexity, respectively, of single step evaluation over an input trace. This bound is close to the lower bound \( O(2^{\sqrt{m}}) \) for future-time LTL presented in [18]. EAGLE has been successfully used, in both LTL and metric LTL forms, to test a real-time controller of an experimental NASA planetary rover.

1. Introduction

Linear temporal logic (LTL) [17] is now widely used for expressing properties of concurrent and reactive systems. Associated, production quality, verification tools have been developed, most notably based on model-checking technology, and have enjoyed much success when applied to relatively small-scale models. Tremendous advances have been made in combating the combinatoric state space explosion inherent with data and concurrency in model checking, however, there remain serious limitations for its application to full-scale models and to software. This has encouraged a shift in the way model checking techniques are being applied, from full state space coverage to bounded use for sophisticated testing, or debugging, and from static application to dynamic, or runtime, application. Our work on EAGLE concerns this latter direction.

*This author is most grateful to RIACS/USRA and to the UK’s EPSRC under grant GR/S40435/01 for the partial support provided to conduct this research.
†This author is grateful for the support received from RIACS to undertake this research while participating in the Summer Student Research Program at the NASA Ames Research Center.
The paper is structured as follows. Section 2 introduces our logic framework EAGLE and then specializes it to LTL. In section 3 we discuss the monitoring algorithm and calculus with an illustrative example. This underlies our implementation for the special case of LTL, which is briefly described in section 4 where complexity bounds for the implementation can also be found. Section 5 describes an experiment performed using EAGLE, and shows how cyclic deadlock potentials can be detected with EAGLE. Section 6 states conclusion and future work.

2 EAGLE and Linear Temporal Logic

EAGLE [5] offers a succinct but powerful set of primitives, essentially supporting recursive parameterized equations, with a minimal/maximal fix-point semantics together with three temporal operators: next-time, previous-time, and concatenation. The parametrization of rules supports reasoning about data values as well as the embedding of real-time, metric and statistical temporal logics. In Section 2.1 we motivate the fundamental concepts of EAGLE through some simple examples drawn from LTL before presenting its formal definition. Then, in Section 2.2 we present a full embedding of LTL in EAGLE and establish its correctness.

2.1 Introducing EAGLE

2.1.1 Fundamental Concepts

In most temporal logics, the formulas $\square F$ and $\Diamond F$ satisfy the following equivalences:

$$\square F \equiv F \land \Diamond (\square F) \quad \Diamond F \equiv F \lor \Diamond (\Diamond F)$$

One can show that $\square F$ is a solution to the recursive equation $X = F \land \Diamond X$; in fact it is the maximal solution. A fundamental idea in our logic, EAGLE, is to support this kind of recursive definition, and to enable users define their own temporal combinators in such a fashion. In the current framework one can write the following definitions for the two combinators Always and Sometime:

$$\begin{align*}
\text{max } \text{Always} & (\text{Form } F) = F \land \Diamond \text{Always} (\text{Form } F) \\
\text{min } \text{Sometime} & (\text{Form } F) = F \lor \Diamond \text{Sometime} (\text{Form } F)
\end{align*}$$

First note that these rules are parameterized by an EAGLE formula (of type Form). Thus, assuming an atomic formula, say $x < 0$, then, in the context of these two definitions, we will be able to write EAGLE formulas such as, Always$(x > 0)$, or Always$(\text{Sometime}(x > 0))$. Secondly, note that the Always operator is defined as maximal; when applied to a formula $F$ it denotes the maximal solution to the equation $X = F \land \Diamond X$. On the other hand, the Sometime operator is defined as a minimal, and Sometimes$(F)$ represents the minimal solution to the equation $X = F \lor \Diamond X$. In EAGLE, this difference only becomes important when evaluating formulas at the boundaries of a trace.

EAGLE has been designed specifically as a general purpose kernel temporal logic for run-time monitoring. So to complete this very brief introduction to EAGLE suppose one wished to monitor the following property of a Java program state containing two variables $x$ and $y$: \textit{"whenever we reach a state where } x = k \text{ for some value } k \text{, then eventually we will reach a state at which } y = k \text{"}. In a linear temporal logic augmented with first order quantification, we would write: $\text{C}(x > 0 \rightarrow \exists k (k = x \land \forall y = k))$. The parametrization mechanism of EAGLE allows data as well as formulas as parameters and are able to encode the above as:

$$\begin{align*}
\text{max } R(\text{int } k) & = \text{Sometime} (y = k) \\
\text{mon } M & = \text{Always} (x > 0 \rightarrow R(x))
\end{align*}$$

The definition starting with keyword mon specifies the EAGLE formula to be monitored. The rule $R$ is parameterized with an integer $k$; it is instantiated in the monitor $M$ when $x > 0$ and hence captures the value of $x$ at that moment. Rule $R$ replaces the existential quantifier. EAGLE also provides a previous-time operator, which allows us to define past time operators, and a concatenation operator, which allows users to define interval based logics, and more. Data parametrization works uniformly for rules over past as well as future; this is non-trivial to achieve as the implementation doesn’t store the trace, see [5].

2.1.2 EAGLE Syntax

A specification $S$ comprises a declaration part $D$ and an observer part $O$. $D$ comprises zero or more rule definitions $R$, and $O$ comprises zero or more monon definitions $M$, which specify what is to be monitored. Rules and monitors are named $(N)$.

$$\begin{align*}
S & ::= DO \\
D & ::= R* \\
O & ::= M* \\
R & ::= \{ \text{max } | \text{min } \} N(T_1, x_1, \ldots , T_n, x_n) = F \\
M & ::= \text{mon } N = F \\
T & ::= \text{Form } | \text{primitive type} \\
F & ::= \text{exp } | \text{true } | \text{false } | \neg F | F_1 \land F_2 | F_1 \lor F_2 | F_1 \rightarrow F_2 | \Diamond F | \Diamond F | F_1 \cdot F_2 | N(F_1, \ldots , F_n) | x_i
\end{align*}$$

A rule definition $R$ is preceded by a keyword indicating whether the interpretation is maximal or minimal. Parameters are typed, and can either be a formula of type Form, or of a primitive type, such as int, long, float, etc.. The body of a rule/monitor is a boolean-valued formula of the syntactic category Form. However, a monitor cannot have a recursive definition, that is, a monitor defined as mon $N = F$ cannot use $N$ in $F$. For rules we do not place such restrictions. The propositions of this logic are boolean expressions over an observer state. Formulas are composed using standard propositional connectives together with a next-state operator ($\Diamond F$), a previous-state operator ($\Diamond F$), and a concatenation-operator ($F_1 \cdot F_2$). Finally, rules can be applied and their parameters must be type correct; formula arguments can be any formula, with the restriction that if an argument is an expression, it must be of boolean type.
2.1.3 EAGLE Semantics

The semantics of the logic is defined in terms of a satisfaction relation, $\models$, between execution traces and specifications. We assume that an execution trace $\sigma$ is a finite sequence of program states $\sigma = s_1 s_2 \ldots s_n$, where $|\sigma| = n$ is the length of the trace. The $i$th state $s_i$ of a trace $\sigma$ is denoted by $\sigma(i)$. The term $\sigma[i{:}\{j\}]$ denotes the sub-trace of $\sigma$ from position $i$ to position $j$, both positions included. Given a trace $\sigma$ and a specification $D \sigma$, we define:

$$\sigma \models D \sigma \text{ if and only if } \forall \text{mon } N = F \in D . \sigma_{\text{mon}} \models D F$$

That is, a trace satisfies a specification if the trace, observed from position 1 (the first state), satisfies each monitored formula. The definition of the satisfaction relation $\models D \subseteq (\text{Trace} \times \text{Nat}) \times \text{Form}$, for a set of rule definitions $D$, is presented below, where $0 \leq i \leq n + 1$ for some trace $\sigma = s_1 s_2 \ldots s_n$. Note that the position of a trace can become 0 (before the first state) when going backwards, and can become $n + 1$ (after the last state) when going forwards, both cases causing rule applications to evaluate to either true if maximal or false if minimal, without considering the body of the rules at that point.

$$\begin{align*}
\sigma, i &\models D \text{ exp} \quad \text{if } 1 \leq i \leq |\sigma| \text{ and } \text{eval}(\text{exp})(\sigma(i)) \\
\sigma, i &\models D \text{ true} \\
\sigma, i &\not\models D \text{ false} \\
\sigma, i &\not\models D \neg F \quad \text{if } \sigma, i \not\models F \\
\sigma, i &\models D F_1 \land F_2 \quad \text{if } \sigma, i \models D F_1 \text{ and } \sigma, i \models D F_2 \\
\sigma, i &\models D F_1 \lor F_2 \quad \text{if } \sigma, i \models D F_1 \text{ or } \sigma, i \models D F_2 \\
\sigma, i &\models D F_1 \rightarrow F_2 \quad \text{if } \sigma, i \models D F_1 \text{ implies } \sigma, i \models D F_2 \\
\sigma, i &\models D \bigcirc F \quad \text{if } i \leq |\sigma| \text{ and } \sigma, i + 1 \models D F \\
\sigma, i &\models D \bigtriangledown F \quad \text{if } 1 \leq i \text{ and } \sigma, i - 1 \models D F \\
\sigma, i &\models D F_1 \cdot F_2 \quad \text{if } \exists j \text{ such that } i \leq j \leq |\sigma| + 1 \text{ and } \\
& \quad \sigma[0:j-1], i \models D F_1 \text{ and } \sigma[j, \infty), 1 \models D F_2 \\
\sigma, i &\models D (F_1, \ldots, F_m) \quad \text{if } 1 \leq i \leq |\sigma| \text{ then:} \\
& \quad \text{where } (N(F_1, x_1, \ldots, x_m) = F) \in D \text{ otherwise, if } i = 0 \text{ or } i = |\sigma| + 1 \text{ then:} \\
& \quad \text{rule } N \text{ is defined as max in } D
\end{align*}$$

An atomic formula (exp) is evaluated in the current state, $i$, in case the position $i$ is within the trace ($1 \leq i \leq n$); for the boundary cases ($i = 0$ and $i = n + 1$) it evaluates to false. Propositional connectives have their usual semantics in all positions. A next-time formula $\bigcirc F$ evaluates to true if the current position is not beyond the last state and $F$ holds in the next position. Dually for the previous-time formula. The concatenation formula $F_1 \cdot F_2$ is true if the trace $\sigma$ can be split into two sub-traces $\sigma = \sigma_1 \sigma_2$, such that $F_1$ is true on $\sigma_1$, observed from the current position $i$, and $F_2$ is true on $\sigma_2$ (ignoring $\sigma_1$, and thereby limiting the scope of past time operators). Applying a rule within the trace (positions $1 \ldots n$) consists of replacing the call with the right-hand-side of the definition, substituting arguments for formal parameters. At the boundaries ($0$ and $n + 1$) a rule application evaluates to true if and only if it is maximal.

2.2 Linear Temporal Logic in EAGLE

We have briefly seen how in EAGLE one can define rules for the $\bigcirc$ and $\bigtriangledown$ temporal operators for LTL. Here we complete an embedding of propositional LTL in EAGLE and prove its semantic correspondence. Figure 1 gives the semantic definition of the since and until LTL temporal operators over finite traces; the definitions of $\bigcirc$ and $\bigtriangledown$, and the propositional connectives, are as for EAGLE. We assume the usual collection of future and past linear-time temporal operators.

$$\begin{align*}
\sigma, i &\models F_1 \bigcirc F_2 \quad \text{if } \\
1 \leq i \leq |\sigma| \text{ and } \exists j : i \leq j \leq |\sigma| \text{ and } \sigma, i \models F_1 \text{ and } \\
& \forall k : i < j \text{ implies } \sigma, k \models F_1 \\
\sigma, i &\models F_1 \bigtriangledown F_2 \quad \text{if } \\
1 \leq i \leq |\sigma| \text{ and } \exists j : i \leq j \leq |\sigma| \text{ and } \\
& \forall k : i < j \leq i \text{ implies } \sigma, k \models F_1
\end{align*}$$

with definitions

$$\begin{align*}
\bigcirc F &= \text{true} \quad \bigtriangledown F = \text{true} \quad F
\bigcirc F &= \neg \bigcirc \neg F \\
F \bigcirc = \neg F \quad F \bigtriangledown = \bigcirc F \\
F_1 \bigcirc F_2 &= F_1 \bigcirc F_2 \\
F_1 \bigtriangledown F_2 &= F_1 \bigtriangledown F_2
\end{align*}$$

Figure 1. Semantic definitions for LTL

For each temporal operator, future and past, we define a corresponding EAGLE rule. The embedding is straightforward and requires little explanation. The future time operators give rise to the following set of rules:

$$\begin{align*}
\min \text{Next}(\text{Form } F) &= \bigcirc F \\
\max \text{Always}(\text{Form } F) &= F \land \text{Always}(F) \\
\min \text{Sometime}(\text{Form } F) &= F \lor \text{Sometime}(F) \\
\max \text{Until}(\text{Form } F, \text{Form } F_2) &= F_1 \lor (F_1 \land \text{Until}(F_1, F_2)) \\
\max \text{Unless}(\text{Form } F, \text{Form } F_2) &= F_1 \lor (F_1 \land \text{Unless}(F_1, F_2))
\end{align*}$$

The past time operators of LTL give rise to the following rules:

$$\begin{align*}
\min \text{Previous}(\text{Form } F) &= \bigtriangledown F \\
\max \text{AlwaysPast}(\text{Form } F) &= F \land \text{AlwaysPast}(F) \\
\min \text{SometimePast}(\text{Form } F) &= F \lor \text{SometimePast}(F) \\
\max \text{Since}(\text{Form } F, \text{Form } F_2) &= F_1 \lor (F_1 \land \text{Since}(F_1, F_2)) \\
\max \text{Max}(\text{Form } F, \text{Form } F_2) &= F_1 \lor (F_1 \land \text{Max}(F_1, F_2))
\end{align*}$$

An EAGLE context containing all of the above rules then enables any propositional LTL monitoring formula to be expressed as a monitoring formula in EAGLE by mapping the LTL operators to the EAGLE counterparts. Note that through simply combining the definitions for the future and past time LTLs defined above, we obtain a temporal logic over the future, present and past, in which one can freely intermix the future and past time modalities.

Correctness of Embedding:

To justify the above EAGLE definitions of LTL temporal operators, we can define an embedding function $\text{Embed}$.
Consider the **Future Time Operators**

A formula of the form $\Diamond F$, $\Box F$ to $\always(\Embed(F))$, etc., and then formally establish that $\sigma, i \models F$ if and only if $\sigma, i+1 \models \Embed(F)$ for all traces $\sigma$ and indices $i$. The proof follows by induction over the structure of the formula $F$; insufficient space allows for its inclusion, but see [4].

### 3 Algorithm

In this section, we now outline the computation mechanism used to determine whether a monitoring formula given in LTL holds for some given input sequence of events. The evaluation of a formula $F$ on a state $s = \sigma(i)$ in a trace $\sigma$ results in another formula $eval(F,s)$ with the property that $\sigma, i \models F$ if and only if $\sigma, i+1 \models eval(F,s)$. The definition of the function $eval : \text{Form} \times \text{State} \to \text{Form}$ uses another auxiliary function $update : \text{Form} \times \text{State} \to \text{Form}$. The role of the function $update$ is to pre-evaluate a formula if it is guarded by a previous operator. Formally, $update$ has the property that $\sigma, i \models \Box F$ if $\sigma, i+1 \models update(F,s)$. Had there been no past time modality in EAGLE we could have ignored $update$ and simply written $\sigma, i \models \Box F$ if $\sigma, i+1 \models F$. The value of a formula $F$ at the end of a trace is given by $value(F)$. The function $value : Form \to \{true, false\}$ when applied on $F$ returns $true$ if $F$ is satisfied at the end of the trace or in other words iff $\sigma, |\sigma|+1 \models F$ and returns $false$ otherwise. Thus given a sequence of states $s_1, s_2, \ldots, s_n$, an LTL formula $F$ written in EAGLE is said to be satisfied by the sequence of states if and only if $value(eval_F(s_1), s_2, \ldots, s_n)$ is true. The definition of the functions $eval, update$ and $value$ forms the calculus of the LTL subset of EAGLE.

#### 3.1 Calculus

The $eval$, $update$ and $value$ functions are defined a priori for all operators, which is not possible for fully general EAGLE [5]. We do not define the functions on the previous operator $\Box$, since this operator is eliminated in the calculus. The definition of $eval$, $update$ and $value$ on the different primitive EAGLE operators is given in Figure 2. In the given definitions, $op$ can be $\land, \lor, \to$. Note that $eval$ of a formula of the form $\Box F$ on a state $s$ reduces to the $update$ of $F$ on state $s$. This ensures that if $F$ contains any past time operators then $update$ of $F$ updates them properly. Moreover, $value(\Box F)$ is false as the operator $\Box$ has a strong interpretation in EAGLE. The value of a $\max$ rule is true and that of a $\min$ rule is false.

\[
\begin{align*}
value(\Box F) = true & \text{ if } F \text{ is } \max \\
value(\Box F) = false & \text{ if } F \text{ is } \min
\end{align*}
\]

**Future Time Operators**

Consider the $\always$ operator:

$$\always(F) = \Box F$$

For this rule $eval$ and $update$ are defined as follows.

$$eval(\always(F),s) = eval(F \land \always(F),s)$$
$$update(\always(F),s) = \always(update(F,s))$$

Similarly we can give the calculus for the other future time LTL operators as follows:

$$eval(\next(F),s) = eval(\Box F, s)$$
$$update(\next(F),s) = update(\Box F, s)$$

**Past Time Operators**

The past time LTL operators are defined in the form of rules containing a $\Box$ operator. In general, if a rule contains a formula $F$ guarded by a previous operator on its right hand side then we evaluate $F$ at every event and use the result of this evaluation in the next state. Thus, the result of evaluating $F$ must be stored in some temporary placeholder so that it can be used in the next state. To allocate a placeholder, we introduce, for every formula guarded by a previous operator, an argument in the rule and use these arguments in the definition of $eval$ and $update$ for this rule. Let us illustrate this as follows.

$$\max \alwayspast(F) = F \land \alwayspast(F)$$
For this rule we introduce another auxiliary rule AlwaysPast' that contains an extra argument corresponding to the formula \( \circ \text{AlwaysPast}(F) \). In any LTL formula, we use this primed version of the rule instead of the original rule.

\[
\text{AlwaysPast}(F) = \text{AlwaysPast}'(F, \text{true})
\]

\[
eval(\text{AlwaysPast}'(F, \text{past}_1), s) = \eval(F \land \text{past}_1, s)
\]

\[
\text{update}(\text{AlwaysPast}'(F, \text{past}_1), s) = \text{AlwaysPast}'(\text{update}(F, s), \eval(\text{AlwaysPast}'(F, \text{past}_1), s))
\]

Here, in \( \eval \), the subformula \( \circ \text{AlwaysPast}(F) \) guarded by the previous operator is replaced by the argument \( \text{past}_1 \) that contains the evaluation of the subformula in the previous state. In \( \text{update} \) we not only update the argument \( F \) but also evaluate the subformula \( \text{AlwaysPast}'(F, \text{past}_1) \) and pass it as second argument of \( \text{AlwaysPast}' \). Thus in the next state \( \text{past}_1 \) is bound to \( \circ \text{AlwaysPast}'(F, \text{past}_1) \).

Note that in the definition of \( \text{AlwaysPast}' \) we pass true as the second argument. This is because, \( \text{AlwaysPast} \) being defined a maximal operator, its previous value at the beginning of the trace is true. Similarly, we can give the calculus for the other past time LTL operators as follows:

\[
\text{Previous}(F) = \text{Previous}'(F, \text{false})
\]

\[
eval(\text{Previous}'(F, \text{past}_1), s) = \eval(\text{past}_1, s)
\]

\[
\text{update}(\text{Previous}'(F, \text{past}_1), s) = \text{Previous}'(\text{update}(F, s), \eval(\text{Previous}'(F, \text{past}_1), s))
\]

\[
\text{SometimesPast}(F) = \text{SometimesPast}'(F, \text{false})
\]

\[
eval(\text{SometimesPast}'(F, \text{past}_1), s) = \eval(F \lor \text{past}_1, s)
\]

\[
\text{update}(\text{SometimesPast}'(F, \text{past}_1), s) = \text{SometimesPast}'(\text{update}(F, s), \eval(\text{SometimesPast}'(F, \text{past}_1), s))
\]

\[
\text{Since}(F_1, F_2) = \text{Since}'(F_1, F_2, \text{false})
\]

\[
eval(\text{Since}'(F_1, F_2, \text{past}_1), s) = \eval(F_2 \lor (F_1 \land \text{past}_1), s)
\]

\[
\text{update}(\text{Since}'(F_1, F_2, \text{past}_1), s) = \text{Since}'(\text{update}(F_1, s), \text{update}(\text{Since}'(F_1, F_2, \text{past}_1), s))
\]

\[
\text{Since}(F_1, F_2) = \text{Since}'(F_1, F_2, \text{true})
\]

\[
eval(\text{Since}'(F_1, F_2, \text{past}_1), s) = \eval(F_2 \lor (F_1 \land \text{past}_1), s)
\]

\[
\text{update}(\text{Since}'(F_1, F_2, \text{past}_1), s) = \text{Since}'(\text{update}(F_1, s), \text{update}(\text{Since}'(F_1, F_2, \text{past}_1), s))
\]

For the sake of completeness of the calculus we explicitly define \( \text{value} \) on the above LTL operators as follows:

\[
\text{value}(\text{AlwaysPast}(F)) = \text{value}(\text{AlwaysPast}'(F, \text{past}_1))
\]

\[
\text{value}(\text{Previous}(F)) = \text{value}(\text{Previous}'(F, \text{false}))
\]

\[
\text{value}(\text{AlwaysPast}'(F, \text{past}_1)) = \text{value}(\text{AlwaysPast}'(F, \text{past}_1))
\]

\[
\text{value}(\text{SometimesPast}(F)) = \text{value}(\text{SometimesPast}'(F, \text{past}_1))
\]

\[
\text{value}(\text{Since}(F_1, F_2)) = \text{value}(\text{Since}'(F_1, F_2, \text{false}))
\]

\[
\text{value}(\text{Since}'(F_1, F_2, \text{false})) = \text{value}(\text{Since}'(F_1, F_2, \text{false}))
\]

Note that in the above calculus we have eliminated the previous operator by introducing an auxiliary argument or placeholder for every formula guarded by the \( \circ \) operator. So, we can't use the operator \( \circ \) when writing an LTL formula; instead we use the rule Previous as defined above.

**Correctness of Evaluation**

Given a set of definitions of \( \eval, \text{update} \) and \( \text{value} \) functions for the different operators of LTL, as detailed above, we claim that for a given sequence \( \sigma = s_1s_2\ldots s_n \) and an EAGLE-embedded LTL formula \( F \):

\[
\sigma, 1 \models \text{EAGLE} F \iff \text{value}(\ldots \text{eval}(\ldots \text{eval}(F, s_1), s_2)\ldots s_n))
\]

Insufficient space prohibits inclusion of the proof.

**4 Implementation and Complexity**

We have implemented in Java the EAGLE monitoring framework. In order to make the implementation efficient we use the decision procedure of Hsiang [13]. The procedure reduces a tautological formula to the constant true, a false formula to the constant false, and all other formulas to canonical forms, each as an exclusive disjunction (\( \oplus \)) of conjunctions. The procedure is given below using equations that are shown to be Church-Rosser and terminating modulo associativity and commutativity.

\[
\text{Simplify:}
\]

\[
\text{true} \land \phi = \phi \quad \text{false} \land \phi = \text{false}
\]

\[
\phi \land \phi = \phi \quad \phi_1 \lor \phi_2 = (\phi_1 \lor \phi_2) \oplus \phi_1 \oplus \phi_2
\]

\[
\phi \oplus \phi = \phi \quad \phi_1 \rightarrow \phi_2 = \text{true} \oplus \phi_1 \oplus (\phi_1 \oplus \phi_2)
\]

\[
\phi \oplus \text{false} = \text{false} \quad \phi_1 \equiv \phi_2 = \text{true} \oplus \phi_1 \oplus \phi_2
\]

\[
\neg \phi = \text{true} \oplus \phi \quad \phi_1 \land (\phi_2 \oplus \phi_3) = (\phi_1 \land \phi_2) \oplus (\phi_1 \land \phi_3)
\]

In particular the equations \( \phi \land \phi = \phi \) and \( \phi \oplus \phi = \phi \) is false ensures that, at the time of monitoring, we do not expand the formula beyond bound. The bound is given by the following theorem:

**Theorem 1** The size of the formula at any stage of monitoring is bounded by \( O(m^2 2^m \log m) \), where \( m \) is the size of the initial LTL formula \( \phi \) for which we started monitoring.

**Proof** The above set of equations, when regarded as simplification rules, keeps any LTL formula in a canonical form, which is an exclusive disjunction of conjunctions, where the conjuncts are either propositions or subformulas having temporal operators at top. Moreover, after a series of applications of \( \eval \) on the states \( s_1, s_2, \ldots, s_n \), the conjuncts in the normal formula \( \eval(\ldots \eval(\eval(\phi, s_1), s_2)\ldots s_n) \) are propositions or subformulas of the initial formula \( \phi \), each having a temporal operator at its top. Since there are at most \( m \) such subformulas, it follows that there are at most \( 2^m \) possibilities to combine them in a conjunction. The space requirement for a conjunction is \( O(m \log m) \), assuming that in the conjunction, instead of keeping the actual conjuncts, we keep a pointer to the conjuncts and assuming that each pointer takes \( O(\log m) \) bits.\(^1\) Therefore, one

---

\(^1\)Every unique subformula having a temporal operator at the top in the original formula can give rise to several copies in the process of monitoring. For example, if we consider \( F_1 = \Box Q \) after some steps, it may get converted to \( F_2 = Q \land \Box Q \). In \( F_2 \) the two subformulas \( Q \) are essentially copies of \( Q \) in \( F_1 \). It is easy to see all such copies at any stage of monitoring will be same. So we can keep a single copy of them and in the formula we use a pointer to point to that copy.
needs space $O(m^{2m\log m})$ to store the structure of any exclusive disjunction of such conjunctions. Now, we need to consider the storage requirements for each of the conjunctions that appear in the conjunction. Note that, if a conjunction contains a nested past time operator, the past$_1$ argument of that operator can be a formula. However, instead of storing the actual formula at the argument past$_1$ we can have a pointer to the formula. Thus, each conjunction can take space up to $O(m^2\log m)$. Hence space required by all the conjunctions is $O(m^2\log m)$. Now for each past operator we have a formula that is pointed to by the past$_1$ argument and all those formulas by the above reasoning can take up space $O(m^2m\log m)$. Hence the total space requirement is $O(m^2\log m^2 + m^2\log m + m^2m\log m)$, which is $O(m^22^m\log m)$.

The implementation contains a strategy for the application of these equations that ensures that the time complexity of each step in monitoring is bounded. We next describe the strategy briefly. Since, our LTL formulas are exclusive disjunction of conjunctions we can treat them as a tree of depth two: the root node at depth 0 representing the $\oplus$ operator, the children of the root at depth 1 representing the $\land$ operators, and the leaf nodes at depth 2 representing propositions and subformulas having temporal operators at the top. The application of the eval function on a formula is done in depth-first fashion on this tree and we build up the resultant formula in a bottom-up fashion. At the leaves the application of eval results either in the evaluation of a proposition or the evaluation of a rule. The evaluation of a proposition returns either true or false. We assume that this evaluation takes unit time. On the other-hand, the evaluation of a rule may result in another formula in canonical form. The formula at any internal node (i.e. a $\land$ node or an $\oplus$ node) is then evaluated by taking the conjunction (or exclusive disjunction) of the formulas of the children nodes as they get evaluated and then simplifying them using the set of equations simplify. Note that the application of simplify on the conjunction of two formulas requires the application of the distributive equation $\phi_1 \land (\phi_2 \oplus \phi_3) = (\phi_1 \land \phi_2) \oplus (\phi_1 \land \phi_3)$ and possibly other equations.

At any stage of this algorithm there are three formulas that are active: the original formula $F$ on which eval is applied, the formula $F'$, and the result of the evaluation of the subformula $F_{sub}$. So, by theorem 1 we can say that the space complexity of this algorithm is $O(m^2\log m)$. Moreover, as the algorithm traverses the formula once at each node it can possibly spend $O(m^2\log m)$ time to do the conjunction and exclusive disjunction. Hence the time complexity of the algorithm is $O(m^22^m\log m) \cdot O(m^2\log m)$ or $O(m^22^m\log^2 m)$. These two bounds are given as the following theorem.

**Theorem 2** At any stage of monitoring the space and time complexity of the evaluation of the monitored LTL formula on the current state is $O(m^22^m\log m)$ and $O(m^22^m\log^2 m)$ respectively.

5. **Examples and Experiments**

This section illustrates the use of Eagle on two concurrency-related applications – detection of deadlock potentials and testing of a real-time concurrent system.

5.1. **Using Eagle for Deadlock Detection**

We present an example that illustrates the use of EAGLE to detect a simple class of cyclic deadlocks. Specifically EAGLE monitors an event stream of lock acquisitions and releases, and reports any cyclic lock dependencies. If there are two threads $t_1$ and $t_2$ such that $t_1$ takes lock $l_1$, and then prior to releasing $l_1$, takes lock $l_2$, and furthermore if $t_2$ takes lock $l_2$, and then prior to releasing $l_2$, takes lock $l_1$, then there is a cyclic lock dependency that indicates the possibility of deadlock. This is a simplification of the general dining philosopher problem, restricted to cycles of length two.

We present two implementations. One illustrates how EAGLE integrates with Java, allowing one to intermix algorithms written in a general programming language with EAGLE monitors. The other is a "pure" solution that just uses EAGLE rules. Each solution utilizes the ability of EAGLE to parameterize rules with data values as well as formulas.

For both implementations the state observed by EAGLE contains three integer variables that get updated each time a new lock or release event is sent to the observer. Let $s$ be the object representing the observer state. The variable $s$.type is set to 1 if the event is a lock event and 2 if it is a release event. $s$.thread is an integer which uniquely identifies the thread and $s$.lock uniquely identifies the lock. For clarity we define predicates $s$.lock($l$) and $s$.release($l$) to test whether $s$.type is set to 1 or 2, respectively. We first present the pure solution.

```latex
\begin{align*}
\min \text{Conflict}(\text{int } t, \text{int } l_1, \text{int } l_2) = \text{Until}(- (s\text{.release()} \land s\text{.thread} = t \land s\text{.lock} = l_2), \\
& s\text{.lock()} \land s\text{.thread} = t \land s\text{.lock} = l_1) \\
\min \text{ConflictLock}(\text{int } t, \text{int } l_1, \text{int } l_2) = s\text{.lock()} \land s\text{.thread} \neq t \land s\text{.lock} = l_2 \land \text{Conflict}(s\text{.thread}, l_1, l_2) \\
\min \text{NestedLock}(\text{int } t, \text{int } l) = \text{Until}(- (s\text{.release()} \land s\text{.thread} = t \land s\text{.lock} = l), \\
& s\text{.lock()} \land s\text{.thread} = t \land s\text{.lock} \neq t \land \\
& (\text{Sometime}(\text{ConflictLock}(t, l_1, s\text{.lock}))) \\
& \lor \text{SometimeFast}(\text{ConflictLock}(t, l, s\text{.lock}))) \\
\min M = -\text{Sometime}(s\text{.lock()} \land s\text{.thread} = t) \\
& \land \text{NestedLock}(s\text{.thread}, s\text{.lock})
\end{align*}
```
The intuition is that the Sometime in monitor $M$ is satisfied in a state where a lock is taken that is the “first” of the four locks in the pattern described above. The thread and the lock value of that lock are passed as data parameters to NestedLock which “searches” for a subsequent lock taken by that thread prior to the release of the first lock. If such a second lock is found, it binds the data value of the second lock to a data parameter and searches both forward and backward through the trace with ConflictLock for a second thread that takes the two locks in reverse order.

The second implementation uses a set data structure within the observer state that holds triples of values of the form $[t_1, l_1, l_2]$ recording that thread $t_1$ took nested locks $l_1$ and then $l_2$. The predicate addTriple inserts such a triple into the set and evaluates to true if there is no conflicting triple in the set. A conflicting triple is one of the form $[t_2, l_2, l_1]$ for $t_2 \neq t$.

\[
\begin{align*}
\text{max} & \text{ DiffLock}(t_1, int l) = s.lock() \land s.thread = t \land s.lock \neq l \\
\text{max} & \text{ CheckLock}(t_1, int l) = s.lock() \land s.thread = t \\
& \land s.lock \neq l \land s.addTriple(t_1, l, s.lock) \\
\text{max} & \text{ Release}(t_1, int l) = s.release() \land s.thread = t \\
& \land s.lock = l \\
\text{min} & \text{ NestedDiffLock}(t_1, int l) = \\
\text{min} & \text{ NestedCheckLock}(t_1, int l) = \\
& \text{Until}(\neg \text{Release}(t, l), \text{DiffLock}(t, l)) \\
& \text{Until}(\neg \text{Release}(t, l), \text{CheckLock}(t, l)) \\
\text{mon} & \text{Always}((s.lock() \land \neg \text{NestedDiffLock}(s.thread, s.lock)) \\
& \rightarrow \text{NestedCheckLock}(s.thread, s.lock)
\end{align*}
\]

The monitor identifies a first lock and the rule NestedDiffLock returns true if a second, nested, lock is taken. If so, NestedCheckLock adds the triple to the set and returns false if a conflict exists.

5.2 Testing a Planetary Rover

The EAGLE logic has been applied in the testing of a planetary rover controller, as part of an ongoing collaborative effort with other colleagues (see [2]) to create a fully automated test-case generation and execution environment for this application. The controller consists of 35,000 lines of C++ code and is implemented as a multi-threaded system, where synchronization between threads is performed through shared variables, mutexes and condition variables. The controller operates a rover, named K9, which essentially is a small car/robot on wheels. K9 itself is a prototype, and serves to form the basis of experiments with rover missions on Mars. The controller executes plans given as input. A plan is a tree-like structure of actions and sub-actions. The leaf-actions control the rover hardware components. Each action is optionally associated with time constraints indicating when it should start and when it should terminate. Figure 3 presents an example input plan. The plan is named $P$ and consists of two sub-tasks $T_1$ and $T_2$, which are supposed to be executed sequentially in the given order. The plan specifies that $T_1$ should start 1-5 seconds after $P$ starts and should end 1-30 seconds after $T_1$ starts. Task $T_2$ should start 10-20 seconds after $T_1$ ends. The controller has been hand-instrumented in a few places to generate an execution trace when executed. An example execution trace of the plan in Figure 3 is presented below:

\[
\begin{align*}
\text{start} & \text{ P 397} \\
\text{start} & \text{ T1 1407} \\
\text{success} & \text{ T1 2440} \\
\text{start} & \text{ T2 14070} \\
\text{success} & \text{ T2 15200} \\
\text{success} & \text{ P 15360}
\end{align*}
\]

In addition to information about start and (successful or failing) termination, each event in the trace is associated with a time-stamp in milliseconds since the start if the application. The testing environment, named X9 (explorer of K9), contains a test-case generator, that automatically generates input plans for the controller from a grammar describing the structure of plans. A model checker extended with symbolic execution is used to generate the plans [14]. Additionally, for each input plan a set of temporal formulas is generated, that the execution trace obtained by executing that plan should satisfy. The controller is executed on each generated plan, and the implementation of EAGLE is used to monitor that the generated execution trace satisfies the formulas generated for that particular plan. The properties generated for the plan in Figure 3 are presented in Figure 4, and should be self-explainable.

X9 was evaluated by seeding errors in the rover controller. One error had to do with the closeness in time between termination of one task and the start of the successor. If a task $T_1$ ended in a particular time range (after the start time of the successor $T_2$), then task $T_2$ would wrongly fail rather than execute. Running X9 detected this problem immediately. Note that the property violated was binary/propositional in nature: a task failed that should have succeeded.
Future Work includes: optimizing the current implementation and investigating other efficient subsets of EAGLE.

6 Conclusion and Future Work

We have presented a representation of linear temporal logic with both past and future temporal operators in EAGLE. We have shown how the generalized monitoring algorithm for EAGLE becomes simple and elegant for this particular case. We have bounded the space and time complexity of this specialized algorithm and thus showed that general LTL monitoring is space efficient if we use the EAGLE framework. Initial experiments have been successful. Future work includes: optimizing the current implementation and investigating other efficient subsets of EAGLE.

References


Figure 4. Generated properties

EAGLE allows for the formulation of real-time properties that take the timestamp into account. Such an experiment is mentioned in [5]. In that experiment a real unknown bug was located. It was discovered that the application did not check lower bounds on durations, whereas it should. That is, if a task finished before it was supposed to, the task should fail, but it wrongly succeeded. The bug was not immediately corrected, and later showed up during a field test of the rover.