# ON THE EVENTUALITY OPERATOR IN TEMPORAL LOGIC

A. Prasad Sistla and Lenore D. Zuck

YALEU/DCS/TR 536
Revision of TR 503
March, 1987

# On the Eventuality Operator in Temporal Logic

A. Prasad Sistla
GTE Laboratories Inc., Waltham, Mass.

Lenore D. Zuck*
Department of Computer Science, Yale University

**Abstract**

We consider RTL, a linear time propositional temporal logic whose only modalities are the $\Diamond$ (*eventually*) operator and its dual—$\Box$ (*always*). Although less expressive than the full temporal logic, RTL is the fragment of temporal logic that is used most often and in many verification systems. Indeed, most properties of distributed systems discussed in the literature are RTL properties. Another advantage of RTL over the full temporal logic is in the decidability procedure; while deciding satisfiability of a formula in full temporal logic is a PSPACE complete procedure, doing that for an RTL formula is in co-NP. We characterize the class of $\omega$-regular languages that are definable in RTL and show simple translations between $\omega$-regular sets and RTL formulae that define them. We explore the applications of RTL in reasoning about communication systems and the relationship between RTL and several fragments of Interval Modal Logic.

## 1 Introduction

Propositional Linear Time Temporal Logic (TL) was introduced in [Pnu77] as a formal system for reasoning about concurrent programs. Recent trends in program verification (e.g., [Var85], [VW86], and [AS85]) suggest using

*Research of this author was partly supported by the National Science Foundation under grant DCR-8405478

automata-theoretic approaches in program verification, i.e., applying techniques developed in automata-theory in the temporal framework. The classical finite-state automata (see [RS59]) were used to define regular languages. Later works (see [Buc62,McN66]) showed how they can be used to define classes of infinite sequences. The resulting languages are termed *$\omega$-regular*. TL was shown to be (expressibility-wise) a strict subset of the class of $\omega$-regular languages. (This was first implied by a combination of several works, for example [GPSS80] or [Kam68] with [MP71] or [Tho81].)

The "strict subclass" of the $\omega$-regular languages which is equivalent to TL is the language definable by *$\omega$-star free* regular expressions, which, in turn, are equivalent to the *$\omega$-non-counting* languages. (Definitions and discussions of these $\omega$-regular languages appear in [Tho81,LPZ85,Zuc86].)

In most formal systems that allow temporal-like reasoning, the $\Diamond$ (eventually) operator is used as the main modal operator. It is therefore natural to consider a temporal logic that uses $\Diamond$ as the only temporal operator. We call the restricted temporal logic obtained RTL. At first glance RTL seems to be a very limited language. Yet, if we are concerned with properties of concurrent programs, there are convincing indications that the RTL language is adequate:

It was shown in [Sis85] that RTL is sufficient to define the set of *strong safety* properties. Chandy and Misra conjectured that there is essentially one class of interesting liveness properties of concurrent programs, namely, the class of *progress* properties ([CM86]). In their propositional version, progress properties are easily definable by RTL. Owicki and Lamport, when giving proof rules for liveness properties, considered only formulae of the form $\Box(p \rightarrow \Diamond q)$ ([OL82]), which provides another indication that RTL is an adequate temporal language.

Indeed, most temporal properties of distributed programs discussed in the literature are given in RTL. As shown in [SC85], the satisfiability problem for RTL formulae is NP complete, while the problem for general TL formulae is PSPACE complete. Hence, using RTL instead of TL provides a considerable advantage.

We characterize below the class of $\omega$-regular languages that are definable in RTL. In particular, we show that every RTL formula is equivalent to a finite union of some simply defined $\omega$-regular sets which we call *temporal sets*, and that every union of such temporal sets is definable by some RTL formula.

We then consider problems concerning theories of message buffers in RTL. For example, we show that the theory of unbounded fifo buffers in RTL is in co-NP; the corresponding theory in the full TL is $\Pi_1^1$-complete (cf.[SCFM84]).

Finally, we consider the relationships between several simple extensions of RTL and fragments of Interval Modal Logic (see [HS86]). For example, we show that RTL, when interpreted over points in the (continuous) interval $[0,1]$, is equivalent to the fragment of Interval Modal Logic that uses only the modality $\langle E \rangle$ . We show that the satisfiability problem for RTL that is interpreted over the continuous line $[0,1]$ is NP-complete.

# 2 Notations and Definitions

## 2.1 Restricted Regular Sets and Temporal Sets

Let $S$ be a finite set of *states*, $\Pi$ be a finite set of propositions, $\Sigma = 2^{\Pi}$ be an *alphabet*, and $I: S \rightarrow \Sigma$ be an *evaluation* mapping each state $s \in S$ to the set of propositions $I(s) \in \Sigma$ that are true in $s$. We assume that $I$ is an isomorphism. We hold $S$, $\Pi$, $\Sigma$, and $I$ fixed for the subsequent discussion.

We shall consider both finite and infinite sequences of states, i.e., sequences over $S$. Every sequence $\sigma$ over $S$ can be mapped into a *string* $I(\sigma)$ which is a sequence over $\Sigma$. Similarly, a string $\sigma$ over $\Sigma$ can be mapped to a set of sequences $I^{-1}(\sigma)$ over $S$. When there is no danger of confusion, we shall interchange strings and sequences over $S$.

Let $\sigma = s_0, \ldots, s_k$ be a *finite* sequence over $S$ and let $\sigma' = s'_0, \ldots$ be a (possibly infinite) sequence over $S$. The concatenation of $\sigma$ and $\sigma'$ is the (possibly infinite) sequence $\sigma;\sigma' = s_0, \ldots, s_k, s'_0, \ldots$.

Let $A$ be a subset of $S$. We define the following *restricted regular sets* over $S$:

- $A$ is a restricted regular set.
- $A^*$, the set of all (possibly empty) *finite* sequences over $A$, is a restricted regular set.
- $A^+$, the set of all *non-empty* finite sequences over $A$, is a restricted regular set.
- $A^\omega$, the set of all *infinite* sequences over $A$, is a restricted regular set.

- $A^\infty = A^* \cup A^\omega$, the set of all sequences over $A$, is a restricted regular set.
- Let $L_1$ and $L_2$ be restricted regular sets. We denote by $L_1 \circ L_2$ the *concatenation* of the two sets, defined by: $L_1 \circ L_2 = \{\sigma;\sigma' \mid \sigma \in L_1 \cap S^* \text{ and } \sigma' \in L_2\} \cup \{\sigma \mid \sigma \in L_1 \cap S^\omega\}$. The set $L_1 \circ L_2$ is a restricted regular set.

If a set $A$ is a singleton, e.g., $A = \{a\}$, we omit the braces and write, for example, $a^*$ instead of $\{a\}^*$.

Let $s \in S$ be an element of $S$. We denote by $\inf(s)$ the set of infinite sequences where $s$ appears infinitely many times. Similarly, for a subset $S' \subseteq S$, we denote

$$\inf(S') = \bigcap_{s \in S'} \inf(s)$$

Let $L \subseteq S^\omega$ be a restricted regular set over $S$ and assume $S' \subseteq S$. We define $L_{\inf(S')} = L \cap \inf(S')$, i.e., $L_{\inf(S')}$ is the set of (infinite) sequences of $L$ where every element of $S'$ occurs infinitely many times.

Note that the set of restricted regular sets defined above is a subset of the set of $\omega$-regular sets, i.e., the sets of infinite strings languages accepted by regular automata that accept infinite strings (for more elaborate definitions see, e.g., [McN66,Buc62,SVW85,Zuc86]).

A restricted regular set $L$ is called a $\Lambda$-*set* if

$$L = s_0 \circ S_1^* \circ s_1 \circ S_2^* \circ s_2 \circ \cdots \circ S_{m-1}^* \circ s_{m-1} \circ S_m^\omega$$

for some $S_1, \ldots, S_m \subseteq S$ and $s_1, \ldots, s_{m-1} \in S$ such that $s_0 \in S_1$ and for every $i$, $1 \leq i < m$, $s_i \in S_i - S_{i+1}$.

A restricted regular set $L$ is called a *temporal set* if

$$L = \bigcup_{i=1}^{n} L^i_{\inf(S'_i)}$$

for some $\Lambda$-sets $L^1, \ldots, L^n$ and some $S'_1, \ldots, S'_n \subseteq S$.

## 2.2 Restricted Temporal Logic—RTL

A *model* for RTL is an infinite sequence of states $\sigma \in S^\omega$, i.e.,

$$\sigma : s_0, s_1, \ldots \qquad s_i \in S$$

Usually, a model is generated by an underlying program; however, in our discussions we shall not use this fact directly.

Given a model $\sigma$ and a position $i \geq 0$, we denote by $\sigma^{(i)}$ the suffix of $\sigma$ from the $i$'th position, i.e., $\sigma^{(i)} = s_i, s_{i+1}, \ldots$. Similarly, we denote by $\sigma_{\rightarrow i}$ the prefix of $\sigma$ until the $i$'th position, i.e., $\sigma_{\rightarrow i} = s_0, \ldots, s_i$. We introduce a temporal language over the propositional formulae in $\Pi$ using the boolean connectives $\neg$ and $\vee$, and the *temporal* operator $\Diamond$ (*eventually*).

Temporal formulae are constructed by the following:

- $T$ and $F$ are RTL formulae..
- Every proposition $Q \in \Pi$ is an RTL formula.
- If $\varphi$ is an RTL formula, then so are $\neg\varphi$ and $\Diamond\varphi$.
- If $\varphi_1$ and $\varphi_2$ are RTL formulae, then so is $\varphi_1 \vee \varphi_2$.

We define a satisfiability relation $\models$ between a model $\sigma$ and an RTL formula. The satisfiability relation is defined inductively as follows:

$\sigma \models T$ and $\sigma \not\models F$ for every $\sigma \in S^\omega$.

For a proposition $Q \in \Pi$, $\sigma \models Q$ *iff* $Q \in I(s_j)$.

$\sigma \models \neg\varphi$ *iff* $\sigma \not\models \varphi$.
$\sigma \models \varphi_1 \vee \varphi_2$ *iff* $\sigma \models \varphi_1$ **or** $\sigma \models \varphi_2$.
$\sigma \models \Diamond\varphi$ *iff* For some $i \geq 0$, $\sigma^{(i)} \models \varphi$.

Additional boolean connectives (such as $\wedge$, $\rightarrow$, $\equiv$) can be defined in the usual way. We define an additional temporal operator, $\Box$ (*always*), by:

$$\Box\varphi \equiv \neg\Diamond\neg\varphi$$

Let $\varphi$ be an RTL formula. If for some $\sigma \in S^\omega$, $\sigma \models \varphi$, we say that $\sigma$ ***satisfies*** $\varphi$. If there is a model $\sigma$ that satisfies $\varphi$, we say that $\varphi$ is ***satisfiable.*** If all $\sigma \in S^\omega$ satisfy $\varphi$, we say that $\varphi$ is ***valid.***

For a given RTL formula $\varphi$, we denote by $\mathcal{L}(\varphi)$ the set of models that satisfy $\varphi$, i.e.,

$$\mathcal{L}(\varphi) = \{\sigma \in S^\omega \mid \sigma \models \varphi\}.$$

## 3 From Temporal Sets to RTL

As mentioned above, for every TL formula there exists a regular set whose members are exactly those sequences satisfying the formula. As RTL formulae are special cases of TL formulae, it follows that for every RTL formula $\varphi$, $\mathcal{L}(\varphi)$ is a regular set. In this section we show that every temporal set is equivalent to $\mathcal{L}(\varphi)$ for some $\varphi \in$RTL, or, as we term it, every temporal set is *RTL-definable*.

We first show that every $\Lambda$-set is RTL-definable. Let $LS$ be a $\Lambda$-set defined by:

$$LS = s_0 \circ S_1^* \circ s_1 \circ S_2^* \circ s_2 \circ \cdots \circ S_{m-1}^* \circ s_{m-1} \circ S_m^\omega$$

for some $S_1, \ldots, S_m \subseteq S$ and $s_1, \ldots, s_{m-1} \in S$ such that $s_0 \in S_1$ and for every $i$, $1 \leq i < m$, $s_i \in S_i - S_{i+1}$.

We define the following RTL formulae inductively:

$$\psi_m = \Box S_m$$

and for every $i$, $1 \leq i < m$,

$$\psi_i = \Box (S_i \vee \psi_{i+1}).$$

Note that we use $S_i$ to denote $\bigvee_{s \in S_i} (\bigwedge_{Q \in I(s)} Q \wedge \bigwedge_{Q \in \Pi - I(s)} \neg Q)$.

We next define a sequence $\{E_i\}_{i=1}^{m-1}$ of restricted regular sets, and a sequence $\{\varphi_i\}_{i=1}^{m-1}$ of RTL formulae. The two sequences are defined inductively by:

$$\begin{aligned} E_{m-1} &= s_{m-1}^+ \circ S_m^\omega \\ \varphi_{m-1} &= s_{m-1} \wedge \Box (s_{m-1} \vee \Box S_m) \wedge \Diamond (\neg s_{m-1}) \end{aligned}$$

For every $i$, $1 \leq i < m-1$:

$$\begin{aligned} E_i &= s_i^+ \circ S_{i+1}^* \circ E_{i+1} \\ \varphi_i &= s_i \wedge \Box (s_i \vee \psi_{i+1}) \wedge \Diamond (\varphi_{i+1}). \end{aligned}$$

Our goal here is to show that for every $i = 1, \ldots, m-1$:

$$E_i = \mathcal{L}(\varphi_i) \tag{1}$$

from which we derive that $LS = \mathcal{L}(s_0 \wedge \psi_1 \wedge \Diamond \varphi_1)$, i.e., that the $\Lambda$-set $LS$ is equivalent to the set of sequences that satisfy $s_0 \wedge \psi_1 \wedge \Diamond \varphi_1$.

The following observations and claims are used to establish (1):

**Observation 3.1** *Let $p \in \Sigma$ and let $\chi$ be an RTL formula. Then the following holds:*

1. $\mathcal{L}(p) = p \circ S^\omega$.
2. $\mathcal{L}(\Diamond\chi) = S^* \circ \mathcal{L}(\chi)$.
3. *If $\chi = \Box\varphi$ for some RTL formula $\varphi$, then $\mathcal{L}(\Box(p \vee \chi)) = p^\infty \circ \mathcal{L}(\chi)$.*

**Proof** We prove only part (3) of the Observation. In one direction, assume $\sigma \in (\Box(p \vee \chi))$, i.e., $\sigma \models \Box(p \vee \chi)$. There are two cases to consider: The first case is when $\sigma \models \Box p$, and then $\sigma \in p^\omega$ and the claim is established. The second case is when $\sigma \models \Diamond\neg p$. Let $j \geq 0$ be the minimal such that $\sigma^{(j)} \models \neg p$, i.e., $\sigma^{(j)} \models \chi$. It follows that $\sigma = \sigma_1;\sigma_2$, where $\sigma_1$ (which consists of the first $j$ elements of $\sigma$) is in $p^*$ and $\sigma_2 \in \mathcal{L}(\Box\chi) = \mathcal{L}(\chi)$.

In the other directions assume that $\sigma \in p^\infty \circ \mathcal{L}(\chi)$. If $\sigma \in p^\omega$ then clearly $\sigma \models \Box p$. Otherwise, $\sigma \in p^* \circ \mathcal{L}(\chi)$. Let $i$ be the minimal such that $\sigma^{(i)} \in \mathcal{L}(\chi)$. It follows that for all $j$, $0 \leq j < i$, $\sigma^{(j)} \models p$. As $\sigma^{(i)} \models \chi$ and $\chi \rightarrow \Box\chi$, for all $j \geq i$, $\sigma^{(j)} \models \chi$. Hence, for all $i \geq 0$, $\sigma^{(i)} \models p \vee \chi$, and therefore $\sigma \models \Box(p \vee \chi)$. ⋈

**Claim 3.1** *For every $i$, $1 \leq i \leq m$,*

$$\mathcal{L}(\psi_i) \;=\; S_i^\infty \circ \cdots \circ S_{m-1}^\infty \circ S_m^\omega.$$

**Proof** The proof is by (decreasing) induction on $i$. The base case ($i = m$) is trivial as $S_m$ is a singleton and therefore $\mathcal{L}(\Box S_m)$ equals $S_m^\omega$.

Assume that the claim is true for $i = k+1 \leq m$, i.e., assume:

$$\mathcal{L}(\psi_{k+1}) = S_{k+1}^\infty \circ \cdots \circ S_{m-1}^\infty \circ S_m^\omega.$$

By definition, $\psi_k = \Box(S_k \vee \psi_{k+1})$, hence, by Observation 3.1 (as $\psi_k = \Box\chi$ for some $\chi$ and $S_k$ is a singleton),

$$\mathcal{L}(\Box(S_k \vee \psi_{k+1})) \;=\; S_k^\infty \circ \mathcal{L}(\psi_{k+1})$$

From the induction hypothesis it follows that:

$$\mathcal{L}(\psi_k) \;=\; S_k^\infty \circ \cdots \circ S_{m-1}^\infty \circ S_m^\omega.$$

⋈

**Observation 3.2** *For every $i$, $1 \leq i < m$ the following holds:*

1. $\varphi_i \rightarrow \psi_i$.
2. $\varphi_i \rightarrow \neg\psi_{i+1}$.
3. $\psi_{i+1} \rightarrow \neg\Diamond\varphi_i$.

**Proof**

1. By definition, for every $i$, $1 \leq i < m$, $\varphi_i$ implies $\Box(s_i \vee \psi_{i+1})$. As $s_i \in S_i$ (i.e., $s_i \rightarrow S_i$) and as $\psi_i = \Box(S_i \vee \psi_{i+1})$, the claim follows.
2. The proof is by (decreasing) induction on $i$:

   **Base case ($i = m-1$):** By definition, $\varphi_{m-1} \rightarrow s_{m-1}$ and $s_{m-1} \rightarrow \neg S_m$, hence $\varphi_{m-1} \rightarrow \neg\Box S_m$. As $\psi_m = \Box S_m$, it follows that

   $$\varphi_{m-1} \rightarrow \neg\psi_m.$$

   **Inductive step:** Assume that for some $k$, $1 \leq k < m-1$, $\varphi_{k+1} \rightarrow \neg\psi_{k+2}$. Assume to the contrary that there exists a model $\sigma \in S^\omega$ such that $\sigma \models \varphi_k \wedge \psi_{k+1}$. As $\varphi_k \rightarrow s_k$ $s_k \notin S_{k+1}$, $\psi_{k+1} \rightarrow \Box(S_{k+1} \vee \psi_{k+2})$, and $\psi_{k+2}$ is a $\Box$-formula it follows that $\sigma \models \Box\psi_{k+2}$. By definition, $\varphi_k \rightarrow \Diamond\varphi_{k+1}$, hence $\sigma \models \Diamond(\varphi_{k+1} \wedge \psi_{k+2})$, which contradicts the induction hypothesis. Hence there exists no model $\sigma$ such that $\sigma \models \varphi_k \wedge \psi_{k+1}$. We can therefore conclude that:

   $$\varphi_k \rightarrow \neg\psi_{k+1}.$$

3. Assume to the contrary that for some $k$, $1 \leq k < m$, there exists a model $\sigma \in S^\omega$ such that $\sigma \models \psi_{k+1} \wedge \Diamond\varphi_k$. As $\psi_{k+1}$ is a $\Box$-formula, it follows that for some $i \geq 0$, $\sigma^{(i)} \models \psi_{k+1} \wedge \varphi_k$, contradicting part (2) of the claim. ⋈

**Claim 3.2** *For every $i = 1, \ldots, m-1$, $\mathcal{L}(\varphi_i) \subseteq E_i$.*

**Proof** The proof is by (decreasing) induction on $i$.

**Base case ($i = m-1$):** Assume that $\sigma \in \varphi_{m-1}$. Recall that:

$$\varphi_{m-1} \;=\; s_{m-1} \wedge \Box(s_{m-1} \vee \Box S_m) \wedge \Diamond(\neg s_{m-1})$$

By Observation 3.1, it follows that:

(a) $\sigma \in s_{m-1} \circ S^{\omega}$.

(b) $\sigma \in s_{m-1}^{\infty} \circ S_m^{\omega}$.

(c) $\sigma \in S^* \circ (\neg s_{m-1}) \circ S^{\omega}$.

(c) implies that $\sigma \notin s_{m-1}^{\omega}$, and together with (a) and (b) it follows that $\sigma \in s_{m-1}^{+} \circ S_m^{\omega}$. Hence $\sigma \in E_{m-1}$.

**Inductive step:** Assume that the claim is true for $i = k+1 < m$, i.e., assume:

$$\mathcal{L}(\varphi_{k+1}) \subseteq E_{k+1}$$

Let $\sigma$ be a sequence such that $\sigma \models \varphi_k$, i.e.,

$$\sigma \models s_k \wedge \Box(s_k \vee \psi_{k+1}) \wedge \Diamond(\varphi_{k+1}).$$

By definition, $\varphi_{k+1} \rightarrow s_{k+1}$. As $s_{k+1} \neq s_k$ (since $s_k \notin S_{k+1}$ and $s_{k+1} \in S_{k+1}$) it follows that $\sigma \in S^+ \circ \mathcal{L}(\varphi_{k+1})$. Using similar reasoning to the base case, we derive that:

(a) $\sigma \in s_k^{+} \circ \mathcal{L}(\psi_{k+1})$.

(b) $\sigma \in s_k^{+} \circ S^* \circ \mathcal{L}(\varphi_{k+1})$.

The induction hypothesis implies that $\mathcal{L}(\varphi_{k+1}) \subseteq E_{k+1}$. Claim 3.1 implies that $\mathcal{L}(\psi_{k+1}) = S_{k+1}^{\infty} \circ \mathcal{L}(\psi_{k+2})$. Putting it all together, we derive that:

(a) $\sigma \in s_k^{+} \circ S_{k+1}^{\infty} \circ \mathcal{L}(\psi_{k+2})$.

(b) $\sigma \in s_k^{+} \circ S^* \circ E_{k+1}$.

We can distinguish between the following two cases:

**case 1:** $\sigma \in s_k^{+} \circ S_{k+1}^{*} \circ E_{k+1}$. Then trivially $\sigma \in E_k$.

**case 2:** $\sigma = \sigma_1;\sigma_2$, where $\sigma_1 \in s_k^{+} \circ S_{k+1}^{*}$ and $\sigma_2 \in \mathcal{L}(\psi_{k+2}) \cap S^* \circ E_{k+1}$.
By Observation 3.1, this implies that

$$\sigma_2 \models \psi_{k+2} \wedge \Diamond \varphi_{k+1},$$

which contradicts Observation 3.2 (part 3).

We may therefore conclude that $\sigma \in E_k$. ⋈

**Claim 3.3** *For every* $i = 1, \ldots, m-1$, $E_i \subseteq \mathcal{L}(\varphi_i)$.

**Proof** The proof is by (decreasing) induction on $i$.

**Base case** ($i = m-1$): Let $\sigma$ be a model such that $\sigma \in E_{m-1}$, i.e., $\sigma \in s^+_{m-1} \circ S^\omega_m$. Observe that:

1. $\sigma \in s_{m-1} \circ S^\omega$ and hence, by Observation 3.1 (part 1), $\sigma \models s_{m-1}$.
2. $\sigma \in S^* \circ S_m \circ S^\omega$, and since $s_{m-1} \notin S_m$, Observation 3.1 (parts 1 and 2) implies that $\sigma \models \Diamond(\neg s_m)$.
3. $\sigma \in s^\infty_{m-1} \circ S^\omega_m$ and hence, by Observation 3.1 (part 3), $\sigma \models \Box(s_{m-1} \vee \Box S_m)$.

It follows that $\sigma \models s_{m-1} \wedge \Box(s_{m-1} \vee \Box S_m) \wedge \Diamond(\neg s_{m-1})$, i.e., $\sigma \models \varphi_{m-1}$. We may therefore conclude that:

$$E_{m-1} \subseteq \mathcal{L}(\varphi_{m-1}).$$

**Inductive step** Assume that for all $i$, $k+1 \leq i < m$, $E_i \subseteq \mathcal{L}(\varphi_i)$. Let $\sigma$ be such that $\sigma \in E_k$, i.e., $\sigma \in s^+_k \circ S^*_{k+1} \circ E_{k+1}$. Similar reasoning to that of the base case establishes that:

1. $\sigma \models s_k$.
2. $\sigma \models \Diamond(\neg s_k)$.
3. By the induction hypothesis, $\sigma \in s^+_k \circ S^*_{k+1} \circ \mathcal{L}(\varphi_{k+1})$. From Observation 3.2 it follows that $\sigma \in s^+_k \circ S^*_{k+1} \circ \mathcal{L}(\psi_{k+1})$. From Claim 3.1 it follows that

$$S^*_{k+1} \circ \mathcal{L}(\psi_{k+1}) \subseteq \mathcal{L}(\psi_{k+1}),$$

and therefore $\sigma \in s^+_k \circ \mathcal{L}(\psi_{k+1})$. Since $\psi_{k+1}$ is a $\Box$-formula, we can apply Observation 3.1 and derive that $\sigma \models \Box(s_k \vee \psi_{k+1})$.

Putting it all together, it follows that $\sigma \in \varphi_k$, hence:

$$E_k \subseteq \mathcal{L}(\varphi_k).$$

$\bowtie$

The above two claims establish:

**Corollary 3.1** *For every* $i = 1, \ldots, m-1$, $E_i = \mathcal{L}(\varphi_i)$.

The following lemma establishes that $LS$ is RTL-definable:

**Lemma 3.1**

$$LS = \mathcal{L}(s_0 \wedge \psi_1 \wedge \Diamond\varphi_1)$$

**Proof** In one direction, let $\sigma$ be such that $\sigma \in LS$, i.e., $\sigma \in s_0 \circ S_1^* \circ E_1$. From Claim 3.1 it follows that $\sigma \models s_0 \wedge \psi_1$. From Corollary 3.1 and Observation 3.1 it follows that $\sigma \models \Diamond\varphi_1$, hence $\sigma \in \mathcal{L}(s_0 \wedge \psi_1 \wedge \Diamond\varphi_1)$.

In the other direction, let $\sigma$ be such that $\sigma \models (s_0 \wedge \psi_1 \wedge \Diamond\varphi_1)$. From Corollary 3.1 and Observation 3.1, it follows that we can distinguish between the following two cases:

**case:** $\sigma \in s_0 \circ S_1^* \circ E_1$. Obviously, $\sigma \in LS$.
**case:** $\sigma = \sigma_1;\sigma_2$ where $\sigma_1 \in s_0 \circ S_1^*$, $\sigma_2 \in \mathcal{L}(\psi_2)$, and $\sigma_2 \in S^* \circ E_1$. It follows that $\sigma_2 \models \psi_2 \wedge \Diamond\varphi_1$, contradicting Claim 3.2 which established that $\psi_2 \rightarrow \neg\Diamond\varphi_1$.

We may therefore conclude that $\sigma \in s_0 \circ S_1^* \circ E_1$ and hence $\sigma \in LS$. ⋈

The following theorem establishes that every temporal set is RTL-definable:

**Theorem 3.1** *Let $L$ be a temporal set, i.e., let*

$$L = \bigcup_{i=1}^{n} L^i_{\mathrm{inf}(S_i)}$$

*such that for every $i = 1,\ldots,n$, $L^i$ is a $\Lambda$-set and $S_i \subseteq S$. Then $L$ is RTL-definable.*

**Proof** It suffices to prove the theorem for the case $n = 1$. Let $L$ be defined by $L = LS_{\mathrm{inf}(S')}$ where $LS$ is a $\Lambda$-set and $S' \subseteq S$. Let $\chi$ be the RTL-formula defining $LS$ (whose construction is described above). Let $\theta$ be the RTL-formula defined by:

$$\theta = \chi \wedge \bigwedge_{s \in S'} \Box\Diamond s.$$

Obviously, $L = \mathcal{L}(\theta)$. Thus $L$ is RTL-definable. ⋈

# 4 From RTL to Temporal Sets

Let $\varphi$ be an RTL formula. Following Fischer and Ladner ([FL79]), we define the ***closure*** of $\varphi$, $CL(\varphi)$, to be the smallest set of formulae containing $\varphi$ and satisfying:

$$
\begin{array}{lcl}
T, F \in CL(\varphi) & & \\
\neg\psi \in CL(\varphi) & \Leftrightarrow & \psi \in CL(\varphi) \text{ (we identify } \neg\neg\psi \text{ with } \psi) \\
\psi_1 \vee \psi_2 \in CL(\varphi) & \Rightarrow & \psi_1, \psi_2 \in CL(\varphi) \\
\Diamond\psi \in CL(\varphi) & \Rightarrow & \psi \in CL(\varphi)
\end{array}
$$

An ***atom*** is a set of formulae $A \subseteq CL(\varphi)$ such that:

- $T \in A$.
- For every $\psi \in CL(\varphi)$, $\psi \in A \Leftrightarrow \neg\psi \notin A$.
- For every $\psi_1 \vee \psi_2 \in CL(\varphi)$, $\psi_1 \vee \psi_2 \in A \Leftrightarrow (\psi_1 \in A$ **or** $\psi_2 \in A)$.
- For every $\Diamond\psi \in CL(\varphi)$, $\psi \in A \Rightarrow \Diamond\psi \in A$.

The set of all atoms is denoted by $At$. An atom $A$ that contains $\varphi$ is called ***initial***. The procedure for checking satisfiability attempts to construct a structure of atoms, interpreted as states, which contains a path satisfying $\varphi$. When interpreting atoms as states we take the natural evaluation $I$ defined by $I(A) = A \cap \Pi$, i.e., the propositions taken to be true in $A$ are all the propositions contained in $A$. Similarly, for a subset $At' \subseteq At$ of atoms, we denote $I(At') = \cup_{A \in At'}\{I(A)\}$. We assume that the set of propositional variables in $\varphi$ is exactly $\Pi$.

We construct a structure $\mathcal{A} = (At, R)$ which is a graph whose nodes are all the atoms and whose edges are defined by the relation $R$:

$$
\begin{array}{c}
(A, B) \in R \\
\text{iff} \\
\text{For every } \Diamond\psi \in CL(\varphi), \\
\Diamond\psi \in A \Leftrightarrow \psi \in A \text{ or } \Diamond\psi \in B.
\end{array}
$$

The following claims establish properties of paths and (maximal) strongly connected components (SCC's) in the structure $\mathcal{A}$. These claims shall be used when we describe how to construct the temporal set that equals to $\mathcal{L}(\varphi)$.

**Observation 4.1** *Let $\pi = A_0, \ldots$ be a (possibly infinite) path in $\mathcal{A}$ and assume $\Diamond\psi \in CL(\varphi)$. Then:*

1. *If* $\Diamond\psi \notin A_0$ *then for every* $i \geq 0$, $\Diamond\psi \notin A_i$.
2. *If for some* $i \geq 0$, $\Diamond\psi \in A_i$, *then for all* $j$, $0 \leq j \leq i$, $\Diamond\psi \in A_j$.

**Proof**

1. By definition, for every $i \geq 0$, $\Diamond\psi \notin A_i$ and $(A_i, A_{i+1}) \in R$ imply that $\Diamond\psi \notin A_{i+1}$. The claim trivially follows.
2. Follows immediately from (1). ⋈

The following corollary establishes that all the atoms in a SCC of $\mathcal{A}$ have the same future subformulae.

**Corollary 4.1** *Let* $C$ *be a SCC of* $\mathcal{A}$, *and let* $A$ *and* $B$ *be atoms in* $C$. *Then for every* $\Diamond\psi \in CL(\varphi)$:

$$\Diamond\psi \in A \iff \Diamond\psi \in B.$$

**Proof** Follows immediately from Observation 4.1 as $A, B \in C$ imply that there exists a path from $A$ to $B$ and a path from $B$ to $A$. ⋈

The following corollary establishes that every SCC is a clique.

**Corollary 4.2** *Let* $C$ *be a SCC of* $\mathcal{A}$, *and let* $A$ *and* $B$ *be atoms in* $C$. *Then* $(A, B) \in R$.

**Proof** By Corollary 4.1, for every $\Diamond\psi \in CL(\varphi)$, $\Diamond\psi \in A$ iff $\Diamond\psi \in B$. From the definition of $R$ it follows that $\Diamond\psi \in A \equiv \Diamond\psi \in B$ implies that $(A, B) \in R$. ⋈

The following corollary establishes if an atom is $R$-connected to an atom in a SCC, then it is $R$-connected to all the atoms in the SCC.

**Corollary 4.3** *Let* $C$ *be a SCC of* $\mathcal{A}$, *let* $A_1$ *and* $A_2$ *be atoms in* $C$, *and let* $B$ *be an atom in* $At$. *Then*

$$(B, A_1) \in R \iff (B, A_2) \in R.$$

**Proof** As (by Corollary 4.1) $A_1$ and $A_2$ contain the same future formulae, the claim follows immediately from the definition of $R$. ⋈

The following observation establishes that if an edge connects two disjoint atoms then these atoms differ in some propositional formula.

**Observation 4.2** *Let $A$ and $B$ be two atoms such that $(A, B) \in R$. Then:*

$$A \neq B \quad \Longrightarrow \quad I(A) \neq I(B).$$

**Proof** Let $A, B \in At$ be such that $(A, B) \in R$ and $A \neq B$. Hence, there exists a formula $\psi \in CL(\varphi)$ such that $\psi \in A$ and $\psi \notin B$. Let $\chi$ be such a formula whose length is minimal. We distinguish between the following cases:

**case:** $\chi$ **is propositional.** Then $I(A) \neq I(B)$ follows.

**case:** $\chi = \theta_1 \vee \theta_2$. Then either $\theta_1 \in A$ or $\theta_2 \in A$ and $\theta_1, \theta_2 \notin B$. Hence at least one of $\theta_1$ and $\theta_2$ is both shorter than $\chi$ and distinguishes between $A$ and $B$, contradicting the minimality of $|\chi|$.

**case:** $\chi = \neg\theta$ **where** $\chi$ **is not propositional.** We distinguish between the following subcases:

**subcase:** $\theta = \theta_1 \vee \theta_2$. This subcase is symmetric to the previous case (i.e., $\chi = \theta_1 \vee \theta_2$) and hence contradicts the minimality of $|\chi|$.

**subcase:** $\theta = \Diamond\theta_1$. Then $\neg\Diamond\theta_1 \in A$ and $\Diamond\theta_1 \in B$. This contradicts Observation 4.1.

**case:** $\chi = \Diamond\theta$. i.e., $\Diamond\theta \in A$ and $\Diamond\theta \notin B$. From the definition of $R$ it follows that $\theta \in A$. From the definition of atoms, it follows that $\theta \notin B$. Hence at $\theta$ is both shorter than $\chi$ and distinguishes between $A$ and $B$, contradicting the minimality of $|\chi|$.

It follows that $\psi$ is propositional and therefore $I(A) \neq I(B)$. ⋈

**Corollary 4.4** *Let $C$ be a SCC of $\mathcal{A}$, and let $A$ and $B$ be such that $(A, B) \in R$, $A \notin C$ and $B \in C$. Then for every $B' \in C$, $I(A) \neq I(B')$.*

**Proof** Follows immediately from Corollary 4.3 and Observation 4.2. ⋈

Let $C$ be a set of atoms. $C$ defined to be *self-fulfilling* if for every formula $\Diamond\psi \in A \in C$ there exists an atom $B \in C$ such that $\psi \in B$.

Let $C$ be a self-fulfilling set of atoms. We define $\mathcal{F}(C)$ to be the set of $C$'s subsets such that for every $F \in \mathcal{F}(C)$, $F$ is self-fulfilling and no proper subset $F' \subset F$ is self-fulfilling.

**Observation 4.3** *Let $C \in \mathcal{A}$ be a self-fulfulling SCC. Then for every $F \in \mathcal{F}(C)$, $|F| = O(|\varphi|)$.*

**Proof** Let $F$ be an element of $\mathcal{F}(C)$. Then for every $A \in F$ there exists some $\Diamond\psi \in CL(\varphi)$ such that $\psi \in A$ and for every $A' \in F - \{A\}$, $\psi \notin A'$. The claim immediately follows. ⋈

The following observation establishes that every self-fulfilling SCC $C \in \mathcal{A}$ can be uniquely identified by its set of propositions.

**Observation 4.4** *Let $C_1, C_2 \in \mathcal{A}$ be self-fulfilling SCC's. Then:*

$$I(C_1) = I(C_2) \implies C_1 = C_2.$$

**Proof** Assume to the contrary that $I(C_1) = I(C_2)$ and that $C_1 \neq C_2$. Let $A_1, \ldots, A_n \in At$ and $B_1, \ldots, B_n \in At$ be $C_1$'s and $C_2$'s atoms respectively. As $I(C_1) = I(C_2)$, we can choose the $A_i$'s and $B_i$'s such that for every $i$, $1 \leq i \leq n$, $I(A_i) = I(B_i)$. As $C_1 \neq C_2$, there exists some $j$, $1 \leq j \leq n$, such that $A_j \neq B_j$. For each such $j$, let $\psi_j \in CL(\varphi)$ be the minimal length formula such that $\psi_j \in A_j$ and $\psi_j \notin B_j$. Let $\psi = \psi_l$ be the shortest among the $\psi_j$ formulae. As $I(A_l) = I(B_l)$, $\psi$ is not propositional. It is obvious that $\psi$ is not a disjunction. Therefore, we can assume that $\psi = \Diamond\chi$ for some $\chi \in CL(\varphi)$. As $C_1$ is self-fulfilling and $\Diamond\chi \in A_l \in C_1$, it follows that for some $A_k \in C_1$, $\chi \in A_k$. As $C_2$ is a SCC, it follows (from Corollary 4.1) that $\chi \notin B_k$. Hence $\chi \in CL(\varphi)$ is a formula which both distinguishes between $A_k$ and $B_k$ and is shorter than $\psi$, contradicting the minimality of $\psi$. ⋈

Let $\pi = A_0, A_1, \ldots$ be an infinite path in $\mathcal{A}$, i.e., for every $i \geq 0$, $(A_i, A_{i+1}) \in R$. Denote by $\inf(\pi)$ the set of atoms which appear in $\pi$ infinitely many times. Note that the set $\inf(\pi)$ defines a SCC $C \in \mathcal{A}$.

The following proposition establishes the relation between $\mathcal{L}(\varphi)$ and paths in $\mathcal{A}$. It is a collection of results that were originally established in [SC85] and extended in [VW86] and in [Zuc86].

**Proposition 4.1** *For every model $\sigma = s_0, \ldots$, $\sigma \models \varphi$ iff there exists a path $\pi = A_0, \ldots$ in $\mathcal{A}$ such that the following holds:*

1. *$A_0$ is an intial atom.*
2. *$\inf(\pi)$ is self-fulfilling.*

3. $I(\pi) = \sigma$, *i.e., for every* $i \geq 0$, $I(A_i) = I(s_i)$.

Let $\{C_i\}_{0=1}^{m-1}$ and $\{\mathcal{C}_i\}_{i=1}^{m}$ be sequences of atoms and of SCC's respectively. We say that $\mathbf{C} = \langle \{C_i\}_{i=0}^{m-1}, \{\mathcal{C}_i\}_{i=1}^{m} \rangle$ is a $\Lambda$-*structure* if the following holds:

1. $C_0 \in \mathcal{C}_1$ is an initial atom.
2. $\mathcal{C}_m$ is self-fulfilling.
3. For every $i$, $1 \leq i < m$, $C_i \in \mathcal{C}_i - \mathcal{C}_{i+1}$ and $C_i$ is $R$-connected to some node $A \in \mathcal{C}_{i+1}$.

From Observation 4.1 and Corollary 4.1 it follows that if $\mathbf{C} = \langle \{C_i\}_{i=0}^{m-1}, \{\mathcal{C}_i\}_{i=1}^{m} \rangle$ is a $\Lambda$-structure, then for every $i = 1, \ldots, m-1$, the set of $\Diamond$-formulae in $\mathcal{C}_i$ (i.e., $\{\psi \mid \Diamond\psi \in CL(\varphi)$ and $\Diamond\psi \in A \in \mathcal{C}_i\}$) is a strict superset of the set of $\Diamond$-formulae in $\mathcal{C}_{i+1}$. As the number of $\Diamond$-formulae is linear in $\varphi$, we conclude:

**Observation 4.5** *Let* $\mathbf{C} = \langle \{C_i\}_{i=0}^{m-1}, \{\mathcal{C}_i\}_{i=1}^{m} \rangle$ *be a* $\Lambda$*-structure. Then* $m = O(|\varphi|)$.

Let $\mathbf{C}$ be a $\Lambda$-structure as above. We associate with $\mathbf{C}$ a restricted regular set $L(\mathbf{C})$ defined by:

$$L(\mathbf{C}) \;=\; I(C_0) \circ I(C_1)^* \circ I(C_1) \circ \cdots \circ I(C_{m-1}) \circ I(\mathcal{C}_m)^\omega.$$

**Observation 4.6** *Let* $\mathbf{C}$ *and* $L(\mathbf{C})$ *be defined as above. Then* $L(\mathbf{C})$ *is a* $\Lambda$*-set.*

**Proof** It suffices to show that for every $i$, $1 \leq i < m$, $I(C_i) \notin I(\mathcal{C}_{i+1})$, i.e., that for every $A \in \mathcal{C}_{i+1}$, $I(C_i) \neq I(A)$. By definition, $C_i$ is $R$-connected to $\mathcal{C}_{i+1}$. As $C_i \notin \mathcal{C}_{i+1}$, the claim follows immediately from Corollary 4.4. $\bowtie$

Let $\mathbf{C}$ be a $\Lambda$-structure as above. We define

$$L_{\mathbf{C}} = \bigcup_{F \in \mathcal{F}(\mathcal{C}_m)} L(\mathbf{C})_{\inf(I(F))}.$$

From Observation 4.6 it follows that $L_{\mathbf{C}}$ is a temporal set. As $\mathcal{A}$ is a finite structure, there are finitely many disjoint $\Lambda$-structures that $\mathcal{A}$ defines. Let $\mathbf{C}(\mathcal{A})$ denote the set of all these $\Lambda$-structures. We show below that $\mathcal{L}(\varphi)$ equals to the union of the temporal sets defined by $\mathbf{C}(\mathcal{A})$'s elements. From this we derive that $\mathcal{L}(\varphi)$ is a temporal set.

**Theorem 4.1**

$$\mathcal{L}(\varphi) = \bigcup_{\mathbf{C} \in \mathbf{C}(\mathcal{A})} L_{\mathbf{C}}$$

**Proof** In one direction, let $\sigma$ be such that $\sigma \models \varphi$. From Proposition 4.1 it follows that there exists a path $\pi = A_0, \ldots$ in $\mathcal{A}$ such that $A_0$ is an initial atom, $\inf(\pi)$ is self-fulfilling, and $I(\pi) = \sigma$. The path $\pi$ can be partitioned into fragments $\pi_1, \ldots, \pi_m$ such that $\pi = \pi_1; \ldots; \pi_m$ and for some SCC's $\mathcal{A}_1, \ldots, \mathcal{A}_m$ the following holds:

1. For every $i$, $1 \leq i < m$, $\mathcal{A}_i \neq \mathcal{A}_{i+1}$.
2. For every $i$, $1 \leq i < m$, $\pi_i$ includes only atoms from $\mathcal{A}_i$, and ends in an atom $A^i \in \mathcal{A}_i - \mathcal{A}_{i+1}$.
3. $\inf(\pi)$ defines a self-fulfilling SCC $\mathcal{A}_m \in \mathcal{A}$.

Define $A^0 = A_0$. The structure $\mathbf{C} = \langle \{A^i\}_{i=0}^{m-1}, \{\mathcal{A}_i\}_{i=1}^{m} \rangle$ is a obviously a $\Lambda$-structure which is in $\mathbf{C}(\mathcal{A})$. By construction, $I(\pi) \in L(\mathbf{C})$. Moreover, since $\mathcal{A}_m \supseteq \inf(\pi)$, it follows that $I(\pi) \in L_{\mathbf{C}}$. As $I(\pi) = \sigma$, the claim follows.

In the other direction, assume that $\mathbf{C} = \langle \{C_i\}_{i=0}^{m-1}, \{\mathcal{C}_i\}_{i=1}^{m} \rangle \in \mathbf{C}(\mathcal{A})$. Let $\sigma = s_0, \ldots$ be a sequence such that $\sigma \in L_{\mathbf{C}}$. From Corollaries 4.2 and 4.3, and Observations 4.2 and 4.4, it follows that $\sigma$ identifies a unique path $\pi = A_0, \ldots$ in $\mathcal{A}$ such that $I(\pi) = \sigma$ and $A_0$ is an initial atom. Moreover, from the definition of $\sigma$ it follows that $\inf(\pi)$ is self-fulfilling. Consequently, by Proposition 4.1, $\sigma \models \varphi$. ⋈

The corollary below will play a major role in the section discussing message buffers:

**Corollary 4.5** *Let $\sigma$ be such that $\sigma \models \varphi$. Then there exists a $\Lambda$-set $LS$ defined by:*

$$L = s_0 \circ S_1^* \circ s_1 \circ S_2^* \circ s_2 \circ \cdots \circ S_{m-1}^* \circ s_{m-1} \circ S_m^\omega$$

*such that for some $S' \subseteq S$, $\sigma \in LS_{\inf(S')}$ and $m, |S'| = O(|\varphi|)$*

**Proof** Follows immediately from Observations 4.3 and 4.5, and Theorem 4.1.

# 5 Fairness in RTL

A concurrent (or distributed) program is usually associated with a set of *fairness properties*. This set corresponds to the properties which every computation of the program is assumed to satisfy. Verifying that all executions of a program $P$ satisfy a property $\varphi$ usually means verifying that all *fair* executions of $P$ satisfy $\varphi$. Fairness properties play a major role in verification of liveness properties, where very often the property would not hold over computations which are not fair. An example of a fairness property is *impartiality* which asserts that every process which is permanently enabled is eventually activated. Impartiality thus requires that every process which has not terminated eventually perform some action. In this section we present a normal-form for fairness properties that are RTL-definable.

A set $L \subseteq S^\omega$ is defined to be a *Fairness-set* (or simply *F-set*) if for every $\sigma \in L$ the following holds:

1. For every $i \geq 0$, $\sigma^{(i)} \in L$, i.e., every suffix of $\sigma$ is also in $L$.
2. For every $\sigma' \in S^*$, $\sigma'; \sigma \in L$, i.e., the string obtained by attaching any finite string as a prefix to $\sigma$ is also in $L$.

**Claim 5.1** *Let $L$ be an F-set which is definable by $LS_{\inf(S')}$ for some $\Lambda$-set $LS$ and $S' \subseteq S$. Then there exists $p_1, \ldots, p_n, q_1, \ldots, q_n \in \Sigma$ such that:*

$$L = \mathcal{L}(\bigwedge_{i=1}^{n} (\Diamond\Box p_i \wedge \Box\Diamond q_i)).$$

**Proof** As $LS$ is a $\Lambda$-set it is definable by

$$L = s_0 \circ S_1^* \circ s_1 \circ S_2^* \circ s_2 \circ \cdots \circ S_{m-1}^* \circ s_{m-1} \circ S_m^\omega$$

for some $S_1, \ldots, S_m \subseteq S$ and $s_0, \ldots, s_{m-1} \in S$.

Let $\varphi_L$ be the RTL formula defined by:

$$\varphi_L = \Diamond\Box I(S_m) \wedge \bigwedge_{s \in S'} \Box\Diamond I(s).$$

We establish the claim by showing that $\mathcal{L}(\varphi_L) = L$. In one direction, if $\sigma \in L$ then obviously $\sigma \models \varphi_L$. In the other direction, assume that $\sigma \models \varphi_L$.

$\sigma$ has a suffix $\sigma''$ such that $\sigma'' \models \Box I(S_m) \wedge \bigwedge_{s \in S'} \Diamond I(s)$. Hence, there exists some finite sequence $\sigma' \in S^*$ such that $\sigma'; \sigma'' \in L$. As $L$ is an F-set, every suffix of $\sigma'; \sigma''$ is in $L$, in particular, $\sigma'' \in L$. Similarly, since $L$ is an F-set, any finite string attached as a prefix to $\sigma''$ is also in $L$; in particular, it follows that $\sigma \in L$, which establishes the claim. $\bowtie$

The equivalence between temporal sets and RTL-definability together with the above claim yield:

**Corollary 5.1** *Let $\varphi$ be an RTL formula such that $\mathcal{L}(\varphi)$ is an F-set. Then $\varphi$ is equivalent to some RTL formula of the form:*

$$\bigvee_{i=1}^{n} \Big( \bigwedge_{j=1}^{n_i} (\Diamond \Box p_i^j \wedge \Box \Diamond q_i^j) \Big)$$

*for some $p_i^j, q_i^j \in \Sigma$ $(i = 1, \ldots n,\ j = 1, \ldots, n_i)$.*

# 6 Reasoning about message buffers in RTL

In this section we consider the problem of axiomatizing different message buffers in RTL. Message buffers model communication between processes through message passing and are of special importance to distributed computing. The problem of characterizing message buffers in TL was studied in [SCFM84]. It is shown there that the theory of bounded buffers is axiomatizable in TL, while the theory of unbounded fifo buffers is $\Pi_1^1$-complete (and hence not axiomatizable). We consider the theory of unbounded message buffers in RTL and show that for both the fifo and the unordered case these theories are in co-NP (and hence axiomatizable in RTL). This is of practical significance as fifo buffers is the most widely used model of communication. The results in this section provide more evidence that reasoning in RTL is both easier and more plausible than reasoning in the full TL.

A message buffer is characterized by the set of *read/write* operations allowed on it. A *write* operation writes a message onto the buffer. A *read* operation reads a message and deletes it from the buffer. Reading from an empty buffer is not allowed. We consider both unbounded *fifo* buffers where a read operation reads the last message written, and unbounded *unordered* buffers where a read operation can read any message that was written (and is still in the buffer).

Let $\Delta = \{0,1\}$ be the message alphabet. We extend $\Pi$ to include the set $\Pi_\Delta = \{R_0, W_0, R_1, W_1\}$. We similarly extend the evaluation such that for every $s \in S$ there exists exactly one operation $P \in \Pi_\Delta$ such that $P \in I(s)$, i.e., with each $s \in S$ we associate one read/write operation.

Let $\sigma = s_0, s_1, \ldots$ be a (possibly finite) sequence of states. We define $W(\sigma)$ to be the sequence of messages written in $\sigma$ and $R(\sigma)$ to be the sequence message read in $\sigma$. For every $\delta \in \Delta$ and $X \in \{R, W\}$, let $\sharp X_\delta(\sigma)$ denote the number of $X_\delta$ operations in $\sigma$.

Let *FIFO* denote the set of sequences over $S$ that consist of valid operations in a fifo buffer, and *UNOR* denote those that consist of valid operations in an unordered buffer. Formally:

$$\text{FIFO} = \{\sigma \in S^\omega \mid \text{For every } i \geq 0,\ R(\sigma_{\rightarrow i}) \preceq W(\sigma_{\rightarrow i})\}$$

and

$$\text{UNOR} = \{\sigma \in S^\omega \mid \text{For every } i \geq 0 \text{ and } \delta \in \Delta,\ \sharp R_\delta(\sigma_{\rightarrow i}) \leq \sharp W_\delta(\sigma_{\rightarrow i})\}$$

The *theory of fifo buffers in RTL*, $\mathcal{T}$(fifo), is the set of all RTL formulae $\varphi$ such that for every model $\sigma \in$FIFO, $\sigma \models \varphi$. Similarly, the *theory of unordered buffers in RTL*, $\mathcal{T}$(unor), is the set of all RTL formulae $\varphi$ such that for every model $\sigma \in$UNOR, $\sigma \models \varphi$.

Let $\overline{\mathcal{T}}$ be the complement of $\mathcal{T}$(fifo), i.e.,

$$\overline{\mathcal{T}} = \{\varphi \in RTL \mid \text{For some } \sigma \in \text{FIFO},\ \sigma \not\models \varphi\}.$$

The following claim enables us to show that the $\overline{\mathcal{T}}$ is in NP.

**Claim 6.1** *Let $\varphi \in \overline{\mathcal{T}}$ be such that $|\varphi| = n - 1$ for some $n > 1$. Then there exists a sequence $\sigma \in$FIFO such that $\sigma = \sigma_1; \sigma_2^\omega$ where $|\sigma_1|, |\sigma_2| = O(n)$ and $\sigma \models \neg\varphi$.*

**Proof** As $\varphi \in \overline{\mathcal{T}}$, there exists a sequence $\alpha = s^0, s^1, \ldots \in$FIFO such that $\alpha \models \neg\varphi$. From Corollary 4.5, it follows that there exists a $\Lambda$-set $LS$ defined by:

$$LS = s_0 \circ S_1^* \circ s_1 \circ S_2^* \circ s_2 \circ \cdots \circ S_{m-1}^* \circ s_{m-1} \circ S_m^\omega$$

such that $\alpha \in LS_{\text{inf}(S')}$ for some $S' \subseteq S$ where $m, |S'| = O(n)$.

Let $0 = i_0 < i_1 < \ldots < i_{m-1}$ be such that for every $j$, $0 \leq j < m$, $s^{i_j} = s_j$ and for every $j$, $0 \leq j < m-1$, for every $k$, $i_j < k < i_{j+1}$, $s^k \in S_j$.

(As $\alpha \in LS$, the existence of such $i_j$'s is guaranteed.) The sequence $\sigma_1$ is constructed by taking the sequence $s^{i_0}, \ldots, s^{i_{m-1}}$, and adding states to it such that the resulting sequence preserves the fifo properties and is a prefix of some model that satisfies $\neg\varphi$. The states are added as follows:

For every $j$, $0 \leq j < m$, if for some $x \in \{0,1\}$, $R_x \in I(s^{i_j})$ then, as $\alpha \in$ FIFO, there exists some $k < i_j$ such that $W_x \in I(s^k)$ and $R(\alpha_{\rightarrow i_j}) = W(\alpha_{\rightarrow k})$. Moreover, since $\alpha \in LS$, there exists some $l < j$ such that $i_l \leq k < i_{l+1}$. If $k \neq i_l$, then we add the state $s^k$ to the sequence and place it arbitrarily between $s^{i_l}$ and $s^{i_{l+1}}$.

Similarly, for every $j$, $0 \leq j < m$, if for some $x \in \{0,1\}$, $W_x \in I(s^{i_j})$ and there exsits a $k > i_j$, $k \neq i_{j+1}, \ldots, i_{m-1}$, such that $R_x \in I(s^k)$ and $R(\alpha_{\rightarrow k}) = W(\alpha_{\rightarrow i_j})$, we add the state $s^k$ to the sequence and place in the appropriate location.

We define $\sigma_1$ to be the resulting sequence. Clearly, $|\sigma_1| \leq 2 \cdot m$. We construct $\sigma_2$ as follows: We first construct as set $S'' \subseteq S$ such that $|S''| \leq 4$ by choosing one representative for each operation that is performed by some state that is in $\inf(\alpha)$. Note that if both writes (i.e., $W_0$ and $W_1$) are represented in $S''$ then either none or both of the reads are represented. We construct a sequence $\sigma_2$ such that:

- If $S''$ has no read states (i.e., states representing read operations), we take $\sigma_2$ to be any sequence that contains one occurrence of each of $S'$'s elements.
- If $S''$ has one read state, then we take $\sigma_2$ to be a concatenation of two sequences, $\sigma_2^1$ and $\sigma_2^2$, such that $\sigma_2^1$ contains one or more occurrence of each write state that is in $S' \cup S''$, and $\sigma_2^2$ contains all the read states that are in $s \in S' \cup S''$. Note that $|\sigma_2^1| \geq |\sigma_2^2|$.
- If $S''$ contains both read operations, then we take $\sigma_2$ to be a concatenation of two sequences, $\sigma_2^1$ and $\sigma_2^2$, such that $\sigma_2^1$ contains one or more occurrence of each write state that is in $S' \cup S''$, $\sigma_2^2$ contains one or more occurrence of each read state that is in $s \in S' \cup S''$, and if $\sigma_2^1 = W_{x_1}, \ldots, W_{x_m}$ then $\sigma_2^2 = R_{x_1}, \ldots, R_{x_m}$.

Note that $|\sigma_2| = O(n)$ and that $\sigma_2^\omega$ is a fifo sequence.

Let $\sigma = \sigma_1; \sigma_2^\omega$. Obviously, $|\sigma_1|, \sigma_2| = O(n)$. From the construction it follows that $\sigma \in$ FIFO and that $\sigma \in LS_{\inf(S')}$. Consequently, $\sigma \not\models \neg\varphi$. $\bowtie$

From Claim 6.1 we establish:

**Theorem 6.1** *$\mathcal{T}$(fifo) is in co-NP.*

**Proof** It suffices to show that there exists a procedure in NP that decides whether a given formula $\varphi \in$RTL where $|\varphi| = n$ is in $\mathcal{T}$(fifo). The procedure guesses two sequences of states $\sigma_1$ and $\sigma_2$ such that $|\sigma_1|, |\sigma_2| = O(n)$, checks whether $\sigma_1;\sigma_2^\omega$ is in FIFO, and checks whether $\sigma \models \neg\varphi$. The latter can be done in time which is polynomial in $n$. (This is established in [SC85].) $\bowtie$

Similar arguments establish:

**Theorem 6.2** *$\mathcal{T}$(unor) is in co-NP.*

# 7 Relationship between IML and RTL

Propositional Modal Logic of Intervals, or, Interval Modal Logic (IML) was introduced in [HS86], where it has been proposed to reason about the behavior of dynamic systems over intervals of time. While satisfiability of TL formulae is defined over discrete time models, satisfiability of IML formulae is defined over *time intervals*. In this section we define several Continuous-time RTL's and show how each corresponds to some subset of IML.

## 7.1 IML

The work in [HS86] considered different time structures that have "linear intervals". We, however, consider only the time structure $T = ([0,1], \leq)$ where $[0,1]$ is the closed interval included between the points 0 and 1 on the real line, and $\leq$ is the usual total ordering relation on these points. A *model* $M$ for IML is a pair $(J, I)$ where $J$ is the set of all closed intervals in $[0,1]$ (i.e., $J = \{[t_1, t_2] \mid 0 \leq t_1 \leq t_2 \leq 1\}$), and $I: J \rightarrow 2^\Pi$ is an evaluation that associates with each interval $j \in J$ the set of atomic propositions that are true in it.

We introduce an IML language over the propositional formulae in $\Pi$ using the boolean connectives $\neg$ and $\vee$, and the IML operators $\langle B\rangle$, $\langle E\rangle$, $\langle \overline{B}\rangle$, and $\langle \overline{E}\rangle$. IML formulae are constructed by the following:

- Every proposition $Q \in \Pi$ is an IML formula.
- If $\varphi$ is an IML formula, then so are $\neg\varphi$, $\langle B\rangle\varphi$, $\langle E\rangle\varphi$, $\langle \overline{B}\rangle\varphi$, and $\langle \overline{E}\rangle\varphi$.

- If $\varphi_1$ and $\varphi_2$ are IML formulae, then so is $\varphi_1 \vee \varphi_2$.

We define a satisfiability relation $\models_i$ between a model $M$, an interval $j = [t_1, t_2] \in J$ and an IML formlua. We omit the model $M$ whenever it is understood from the context. The satisfiability relation is defined as follows:

For a proposition $Q \in \Pi$,
$[t_1, t_2] \models_i Q$ *iff* $Q \in I([t_1, t_2])$.
$[t_1, t_2] \models_i \neg\varphi$ *iff* $[t_1, t_2] \not\models_i \varphi$.
$[t_1, t_2] \models_i \varphi_1 \vee \varphi_2$ *iff* $[t_1, t_2] \models_i \varphi_1$ **or** $[t_1, t_2] \models_i \varphi_2$.
$[t_1, t_2] \models_i \langle B \rangle \varphi$ *iff* For some $t_3$, $t_1 \leq t_3 \leq t_2$, $[t_1, t_3] \models_i \varphi$.
$[t_1, t_2] \models_i \langle \overline{B} \rangle \varphi$ *iff* For some $t_3 \geq t_2$, $[t_1, t_3] \models_i \varphi$.
$[t_1, t_2] \models_i \langle E \rangle \varphi$ *iff* For some $t_3$, $t_1 \leq t_3 \leq t_2$, $[t_3, t_2] \models_i \varphi$.
$[t_1, t_2] \models_i \langle \overline{E} \rangle \varphi$ *iff* For some $t_3 \leq t_1$, $[t_3, t_2] \models_i \varphi$.

Note that the semantics above does not coincide with that of [HS86].

For $X \subseteq \{\langle E \rangle, \langle B \rangle, \langle \overline{E} \rangle, \langle \overline{B} \rangle\}$ let $IML(X)$ denote the fragment of IML that uses only the modal operators that are in $X$.

## 7.2 Continuous Time RTL

Cosider a Continuous-time RTL (CRTL) which is similar to RTL. CRTL formulae are interpreted over points in time structure $T = ([0,1], \leq)$, where we assume an evaluation $I' : [0,1] \rightarrow 2^{\Pi}$ that maps each point $t \in [0,1]$ to $I'(t)$, the set of propositions true in it. The satisfiability relation between a point $t \in [0,1]$ and an CRTL formula is denoted by $\models_c$ and defined in the obvious way.

Assume $\varphi \in IML(\langle E \rangle)$, and let $R_\varphi$ be the RTL formula obtained by replacing every occurrence of $\langle E \rangle$ in $\varphi$ by $\Diamond$. Let $M$ be a model of IML such that for every $t \in [0,1]$, $I([t,1]) = I'(t)$.

**Lemma 7.1** *For every* $t \in [0,1]$, $[t,1] \models_i \varphi$ *iff* $t \models_c R_\varphi$.

**Proof** The proof is by induction on the structure of $\varphi$. The base case is when $\varphi$ is propositional, and then, as $I([t,1]) = I'(t)$, the claim is trivially true. Assume the claim is true for $\varphi'$ such that $|\varphi'| < |\varphi|$. We distinguish between the following cases:

**case:** $\varphi = \neg\varphi'$, i.e., $R_\varphi = \neg R_{\varphi'}$. This case is trivial.

*mation and Control*, **63**:1/2, pp. 88–112, 1984.

[Sis85] A. P. Sistla. On characterization of safety and liveness properties in Temporal Logic. In *Proc. 4th ACM Symp. on Principles of Distributed Computing*, pp. 39–48, 1985.

[SVW85] A. P. Sistla, M. Y. Vardi, and P. Wolper. The complementation problem for Büchi automata with applications to Temporal Logic. In *Proc. 12th International Colloq. on Automata, Languages, and Programming*, pp. 465–474, LNCS, Springer Verlag, 1985.

[Tho81] W. Thomas. A combinatorial approach to the theory of $\omega$-automata. *Information and Control*, **48**, pp. 261–283, 1981.

[Var85] M. Y. Vardi. Automatic verification of concurrent probabilistic finite state programs. In *Proc. 26th IEEE Symp. on Foundation of Computer Science*, pp. 327–338, 1985.

[VW86] M. Y. Vardi and P. Wolper. An automata-theoretic approach to automatic program verification (preliminary report). In *Proc. 1st IEEE Symp. on Logics in Computer Science*, 1986.

[Zuc86] L. Zuck. *Past Temporal Logic.* PhD thesis, The Weizmann Institute of Science, 1986.