

Semantics of temporal e over infinite sequences

David Van Campenhout
Verisity Design, Inc.
Confidential

February 14, 2001

Abstract

The semantics of temporal e has been defined for finite sequences, which suffices for simulation. To model check properties specified in temporal e , its semantics over infinite-length sequences need to be defined. In this paper, we extend the semantics of temporal e to the domain of infinite-length sequences.

1 Introduction

The temporal subset of the e language has an expressiveness comparable to that of linear temporal logic (LTL) augmented with regular events. [this point deserves more attention.] So far, temporal e has been used to express properties that are checked in a simulation environment. Simulation deals with *finite-length* sequences and for this context the semantics of temporal e has been described in [1]. We assume that the reader is familiar with the material of [1].

Model checkers reason about *infinite-length* sequences and this allows them to decide liveness properties in addition to safety properties¹. If we wish to model check properties described in temporal e , we first need to define the semantics of temporal e over infinite-length sequences. These semantics should constitute a natural extension of the semantics over finite sequences. Such an extension is the subject of this paper.

In the remainder of this section we present some notation, borrowing heavily from [1], and motivate the need for infinite-sequence semantics. Section 2 develops the infinite-sequence semantics.

¹Note that it is not the *number* of sequences but the *length* of the sequences that is the key to deciding liveness properties. Throughout this paper, the term *infinite sequence* should be read as short for infinite-length sequence.

1.1 Preliminaries

1.1.1 Domain

- Let P be a set of proposition symbols, and let $p \in P$ be a representative.
- Let E be a set of event names, and let $e, q \in E$ be a representative.
- Let $A = P \cup E$ be the set of atoms, and let $a \in A$ be a representative.

1.1.2 Interpretations

Temporal expressions (TEs) are interpreted over 1) finite sequences of states, or 2) infinite sequences of states.

- Let $\Sigma = 2^A$ (the alphabet), and $s \in \Sigma$ be a state.
- Let Σ^* be the set of all finite sequences over Σ , and let $\sigma \in \Sigma^*$ be a representative.
- Let Σ^ω be the set of all infinite sequences over Σ , and let $\sigma \in \Sigma^\omega$ be a representative.
- If σ is the finite sequence of states $\langle s_1, s_2, \dots, s_n \rangle$ then $|\sigma| = n \geq 0$ is the length of the sequence. The empty sequence is represented by ϵ .
- If σ_1 is a finite sequence and σ_2 is a sequence then $\sigma_1\sigma_2$ denotes the concatenation of these two sequences.

1.1.3 Models

Suppose t is a TE then the denotation of t over finite sequences is the set $\|t\|_* \subseteq \Sigma^*$. The sequence $\sigma \subseteq \Sigma^*$ satisfies, or is a model of, the expression t if and only if σ is in the denotation, i.e., $\sigma \models t$ iff $\sigma \in \|t\|_*$.

Similarly, the denotation of t over infinite sequences is the set $\|t\|_\omega \subseteq \Sigma^\omega$. The sequence $\sigma \subseteq \Sigma^\omega$ satisfies, or is a model of, the expression t if and only if σ is in the denotation, i.e., $\sigma \models t$ iff $\sigma \in \|t\|_\omega$.

1.2 The *-semantics is the alpha but not the omega

Consider the temporal expression $t = \text{any } U p$, which states that eventually p will happen. $\|t\|_*$ is the set of all finite sequences in which p holds in the last state of the sequence and p does not hold in any other state. $\|\text{fail } t\|_* = \emptyset$ since any finite sequence over which t has not yet succeeded, can be extended so that the new

sequence satisfies t . The set of sequences over which t has not yet been decided, $\Sigma^* \setminus (\|t\|_* \cup \|\mathbf{fail} t\|_*)$, is the set of all finite sequences in which p holds in none of its states. Note that the length of a sequence over which t has not yet been decided is not bounded. Intuitively, the infinite-length sequence in which p holds in none of its states violates t , however none of its finite-length prefixes violates nor satisfies t . So, the finite-sequence semantics, $\|t\|_*$ and $\|\mathbf{fail} t\|_*$, are simply insufficient to decide t . New semantics need to be defined that tell us how to interpret temporal expressions over infinite-length sequences. These semantics should be consistent with the finite sequence semantics in that infinite sequences which have a prefix over which t is decided in the $*$ -semantics should be decided identically in the ω semantics. An infinite sequence semantics that is consistent with the finite sequence semantics for the example is as follows: $\|t\|_\omega = \Sigma^\omega \setminus S_2$, $\|\mathbf{fail} t\|_\omega = S_2$, where $S_2 = \{\sigma \in \Sigma^\omega \mid \sigma = \langle s_1, s_2, \dots \rangle, \forall i : s_i \models \neg p\}$.

An interesting consequence is that the infinite sequence semantics are actually required to obtain the natural $*$ -semantics of the **fail** operator. Consider again the same example. There are no finite sequences that violate t : $\|\mathbf{fail} t\|_* = \emptyset$, but does this imply that **fail fail** t is always immediately satisfied, i.e., $\|\mathbf{fail fail} t\|_* = \{\varepsilon\}$? If we were to consider the finite sequence semantics only, the logical answer to the question appears to be yes. However, that answer would also be counter intuitive. Intuitively, one would expect $\|\mathbf{fail fail} t\|_* = \|t\|_*$, but within the finite sequence semantics this simply does not work out. The key to resolving this dilemma is to take the infinite sequence semantics into account in defining the finite semantics of the fail operator. Finite sequences 1) over which **fail** t has not yet succeeded, and 2) which are not prefixes of **fail** t , and 3) are the shortest such sequences, should satisfy **fail fail** t . Since $\|\mathbf{fail} t\|_* = \emptyset$, we might be inclined to think that therefore the empty sequence ε is the only sequence that can satisfy **fail fail** t . However, when computing these prefixes we should also consider those infinite sequences that are not already implied by the finite sequence semantics. For the example, all sequences in $\|\mathbf{fail} t\|_\omega = S_2$ need to be considered since none of them is implied by $\|\mathbf{fail} t\|_* = \emptyset$. Therefore finite sequences that are not prefixes of the \mathcal{S} should also satisfy **fail fail** t . With the new insight we conclude for this example that $\|\mathbf{fail fail} t\|_* = \|t\|_*$.

It should be said that for the negation-free language, the $*$ -semantics do not need to consider the ω -semantics.

2 Interpreting temporal expressions over infinite sequences

The denotational semantics of a temporal expression interpreted over finite sequences is defined in [1]. These semantics define $\|t\|_*$ inductively over the syntac-

tic structure of t . For each basic operator $op(\cdot, \cdot)$, the semantics define $\|op(t_1, t_2)\|_*$ in terms of $\|t_1\|_*$, $\|t_2\|_*$, and special elements of Σ^* such as ϵ .

The subject of our work are the denotational semantics of a temporal expression interpreted over infinite sequences. These semantics should be consistent with the finite sequence semantics.

In this section, we first present the requirements for an ω -semantics to be consistent with the $*$ -semantics. We then introduce an adjustment to the $*$ -semantics. Next, we present a condition that guarantees fulfillment of these requirements. Finally, we propose a concrete ω -semantics based on that condition.

2.1 Requirements for consistency

The requirements for an ω -semantics to be consistent with the $*$ -semantics are as follows:

Requirement 1 *Cross-consistency: Given a temporal expression t and an infinite sequence that has a finite prefix over which t holds, then t should also hold over that infinite sequence:*

$$\sigma_1 \in \|t\|_* \Rightarrow \forall \sigma_2 \in \Sigma^\omega : \sigma_1 \sigma_2 \in \|t\|_\omega$$

Requirement 2 *Self-consistency: For any temporal expression t , there should not be any infinite sequence for which both t and also **fail** t hold:*

$$\|t\|_\omega \cap \|\mathbf{fail} t\|_\omega = \emptyset$$

A desirable, but not necessary, property is:

Requirement 3 *Completeness: For any temporal expression t and any infinite sequence, either t or **fail** t should hold:*

$$\|t\|_\omega \cup \|\mathbf{fail} t\|_\omega = \Sigma^\omega$$

The motivation for these requirements is to ensure that an infinite-sequence analysis of a system, e.g., model checking, does not contradict a finite-sequence analysis, e.g., simulation. This can be seen as follows:

Suppose that σ_1 is the sequence of states over which we have simulated the system. Suppose that simulation concluded that t holds on σ_1 , i.e., $\sigma_1 \in \|t\|_*$ then, due to Requirement 1, t also holds over any infinite sequence $\sigma = \sigma_1 \sigma_2$. Suppose that simulation concluded that t fails over a prefix of σ_1 , i.e., $\exists \sigma_p \in \mathbf{prefix} \sigma_1 : \sigma_p \in \|\mathbf{fail} t\|_*$, again due to Requirement 1, t will also fail over an infinite sequence $\sigma = \sigma_1 \sigma_2 : \sigma \in \|\mathbf{fail} t\|_\omega$. For those finite sequences σ_1 for which simulation is inconclusive, i.e., $\sigma_1 \notin \|t\|_*$ and $\sigma_1 \notin \|\mathbf{fail} t\|_*$, analysis over an infinite sequence $\sigma = \sigma_1 \sigma_2$ may yield resolution, but due to Requirement 2, it will never result in a contradiction: $\|t\|_\omega \cap \|\mathbf{fail} t\|_\omega = \emptyset$. If we impose Requirement 3, resolution is obtained for any ω -word.

2.2 Adjustment to the *-semantics of fail

The *-semantics of the **fail** operator is defined in [1] as follows:

$$\|\mathbf{fail} t\|_* = \Sigma^* \setminus (\|\{t; [1..]any\}\|_* \cup \|\mathbf{prefix} t\|_* \cup \|\{\neg\mathbf{prefix} t; [1..]any\}\|_*) \quad (1)$$

$$\|\mathbf{prefix} t\|_* = \{\sigma : \exists \sigma', |\sigma'| \geq 0, \sigma\sigma' \in \|t\|_*\} \quad (2)$$

We modify the semantics of **fail** by redefining the semantics of **prefix** (**fail** is the only operator defined in terms of **prefix**):

$$\|\mathbf{prefix} t\|_* = \|\mathbf{prefix} t\|_{*1} \cup \|\mathbf{prefix} t\|_{*2} \quad (3)$$

$$\|\mathbf{prefix} t\|_{*1} = \{\sigma | \exists \sigma' \in \Sigma^*, \sigma\sigma' \in \|t\|_*\} \quad (4)$$

$$\|\mathbf{prefix} t\|_{*2} = \{\sigma | \exists \sigma' \in \Sigma^\omega, \sigma\sigma' \in \|t\|_{\omega2}\} \quad (5)$$

Note that $\|\mathbf{prefix} t\|_{*1}$ corresponds to the old definition. $\|\mathbf{prefix} t\|_{*2}$ adds to $\|\mathbf{prefix} t\|_*$ sequences that are finite prefixes of sequences in $\|t\|_{\omega2}$. For safety properties $\|t\|_{\omega2}$ is empty and hence $\|\mathbf{prefix} t\|_*$ reduces to $\|\mathbf{prefix} t\|_{*1}$.

(The effect of the redefinition of **prefix** on the construction of **fail** is that instead of removing all paths to \emptyset , it suffices to remove all *fair* paths to \emptyset .)

2.3 Sufficient condition for consistency

We now formulate a condition for an ω -semantics that will be shown to guarantee satisfaction of the consistency requirements.

$$\|t\|_\omega = \|t\|_{\omega1} \cup \|t\|_{\omega2} \quad (6)$$

$$\|t\|_{\omega1} = \{\sigma = \sigma_1\sigma_2 | \sigma_1 \in \|t\|_* \text{ and } \sigma_2 \in \Sigma^\omega\} \quad (7)$$

$$\|t\|_{\omega2} \subseteq \Sigma^\omega \setminus (\|t\|_{\omega1} \cup \|\mathbf{fail} t\|_\omega) \quad (8)$$

$$\|\mathbf{fail} t\|_{\omega2} \subseteq \Sigma^\omega \setminus (\|\mathbf{fail} t\|_{\omega1} \cup \|t\|_\omega) \quad (9)$$

We also define:

$$\begin{aligned} \|t\|_{\omega0} &= \Sigma^\omega \setminus \{\sigma = \sigma_1\sigma_2 | \sigma_1 \in \|t\|_* \cup \|\mathbf{fail} t\|_* \text{ and } \sigma_2 \in \Sigma^\omega\} \\ & (= \Sigma^\omega \setminus (\|t\|_{\omega1} \cup \|\mathbf{fail} t\|_{\omega1})) \end{aligned} \quad (10)$$

The condition dictates that those ω -sequences that have a finite prefix that can be decided over the *-semantics, i.e., sequences in $\|t\|_{\omega1} \cup \|\mathbf{fail} t\|_{\omega1}$, have to be decided identically over the ω semantics (see (7)). For those ω -sequences for which

all of their prefixes are undecided in the *-semantics, i.e., sequences in $\|t\|_{\omega 0}$, the condition leaves us freedom to define the semantics of t or even to leave it undefined, as long as the definition is not contradictory (see (8), (9)), i.e., $\|t\|_{\omega 2} \subseteq \|t\|_{\omega 0}$, $\|\mathbf{fail} t\|_{\omega 2} \subseteq \|t\|_{\omega 0}$, and $\|\mathbf{fail} t\|_{\omega 2} = \emptyset$.

2.3.1 Main theorem

Theorem 1 *A definition of an infinite-sequence semantics for temporal expressions that satisfies the conditions expressed by (6), (7), (8), and (9) also satisfies the consistency requirements 1 and 2. If furthermore $\|t\|_{\omega 2} \cup \|\mathbf{fail} t\|_{\omega 2} = \|t\|_{\omega 0}$ then requirement 3 is also satisfied.*

2.4 ω -Semantics

Theorem 1 shows that any definition of the infinite-sequence semantics that satisfies the condition given by (6), (7), (8), and (9) constitutes a sound extension of the finite-sequence semantics. The condition expressed by (6), (7), (8), and (9) provides us with a form for constructing $\|t\|_{\omega}$, but it is not a complete definition. What remains to be refined is how to partition $\|t\|_{\omega 0}$ into $\{\|t\|_{\omega 2}, \|\mathbf{fail} t\|_{\omega 2}\}$.

In this section we give inductive definitions for the ω semantics of each primary operator of temporal e . The terms appearing on the right hand side either follow directly from the *-semantics:

$$\|t\|_* = \text{see [1]} \quad (11)$$

$$\|t\|_{\omega 1} = \{\sigma \mid \exists \sigma_1 \in \|t\|_* \text{ and } \exists \sigma_2 \in \Sigma^\omega : \sigma = \sigma_1 \sigma_2\} \quad (12)$$

$$\|t\|_{\omega 4} = \{\sigma \in \Sigma^\omega \mid \forall i > 0, \exists j \geq 0, \sigma_1 \in \|t\|_*, \sigma_2 \in \Sigma^\omega : \sigma = \sigma_1 \sigma_2 \text{ and } |\sigma_1| = i + j\} \quad (13)$$

or they follow from the ω semantics of subexpressions:

$$\|t\|_{\omega 2} = \|t\|_{\omega} \setminus \|t\|_{\omega 1} \quad (14)$$

For each of the inductive definitions we can prove that it satisfies the sufficient condition given by (6), (7), (8), and (9). As we have defined the ω semantics directly in terms of $\|t\|_{\omega}$ rather than $\|t\|_{\omega 2}$ the proof obligations are (8), (9), and:

$$\|t\|_{\omega 1} \subseteq \|t\|_{\omega} \quad (15)$$

But given our definition of the ω semantics of **fail** (see (28)), (8), and (9) are fulfilled trivially. By the main theorem we then know that the proposed ω -semantics form a sound extension of the *-semantics.

The astute reader may suspect circularity via the definition of **prefix** in (3). To illustrate that this is not the case, consider the semantics of **fail**. The dependencies among the relevant definitions are shown in Figure 1.

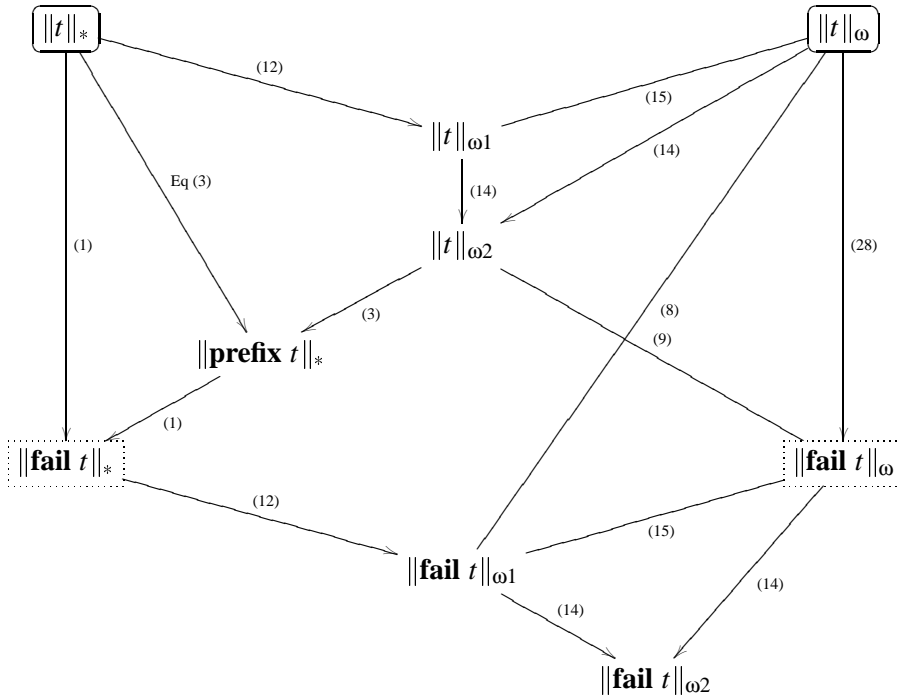


Figure 1: How it all fits together.

2.4.1 Empty sequence

$$\|\varepsilon\|_{\omega} = \Sigma^{\omega} \quad (16)$$

2.4.2 Cycle

$$\|\text{any}\|_{\omega} = \Sigma^{\omega} \quad (17)$$

2.4.3 Atom

$$\|a\|_{\omega} = \|a\|_{\omega 1} \quad (18)$$

2.4.4 Disjunction

$$\|\vee_i t_i\|_{\omega} = \cup_i \|t_i\|_{\omega} \quad (19)$$

2.4.5 Conjunction

$$\begin{aligned} \|\wedge_i t_i\|_{\omega} &= \|\wedge_i t_i\|_{\omega 1} \cup \\ &\cup_i (\|t_i\|_{\omega 2} \cap (\cap_{j \neq i} (\|t_j\|_{\omega 2} \cup \|t_j\|_{\omega 4}))) \end{aligned} \quad (20)$$

,where

$$\begin{aligned} \|t\|_{\omega 4} &= \{\sigma \in \Sigma^{\omega} \mid \forall i > 0, \exists j \geq 0, \sigma_1 \in \|t\|_{*}, \sigma_2 \in \Sigma^{\omega} : \\ &\sigma = \sigma_1 \sigma_2 \text{ and } |\sigma_1| = i + j\} \end{aligned} \quad (21)$$

2.4.6 Sequence

$$\begin{aligned} \|\{t_1; t_2; \dots; t_n\}\|_{\omega} &= \\ &\|\{t_1; t_2; \dots; t_n\}\|_{\omega 1} \cup \\ &\{\sigma \mid \exists \sigma_1 \in \|t_1\|_{*}, \exists \sigma_2 \in \|\{t_2; \dots; t_n\}\|_{\omega} : \sigma = \sigma_1 \sigma_2\} \cup \\ &\{\sigma \mid \sigma \in \|t_1\|_{\omega}, \varepsilon \in \|\{t_2; \dots; t_n\}\|_{*}\} \end{aligned} \quad (22)$$

2.4.7 Unbounded true match repeat

$$\|[\dots]t\|_{\omega} = \Sigma^{\omega} \quad (23)$$

2.4.8 First match

$$\|\mathbf{fm} t\|_{\omega} = \|t\|_{\omega} \quad (24)$$

2.4.9 Sample

$$\|e@q\|_{\omega} = \|e@q\|_{\omega_1} \quad (25)$$

$$\|p@q\|_{\omega} = \|p@q\|_{\omega_1} \quad (26)$$

$$\|t@q\|_{\omega} = \|t@q\|_{\omega_1} \cup (\|t\|_{\omega_2} \cap \|\{[.];q\}\|_{\omega_4}) \quad (27)$$

2.4.10 Fail

$$\|\mathbf{fail}t\|_{\omega} = \Sigma^{\omega} \setminus \|t\|_{\omega} \quad (28)$$

2.5 Discussion

- Sequences in $\|t\|_{\omega_1}$ have finite prefixes over which t can be decided in the *-semantics. The outcome t over such a sequence (in Σ^{ω}) is implied by the outcome of t over one of its finite prefixes: $\sigma \in \|t\|_{\omega_1}$ iff $\exists \sigma_1, \sigma_2 : \sigma = \sigma_1\sigma_2$ and $\sigma_1 \in \|t\|_*$.
- Sequences in $\|t\|_{\omega_2} \cup \|\mathbf{fail}t\|_{\omega_2}$, which we will informally call ω_2 words, are sequences whose finite prefixes are undecided in the finite semantics (they are neither in $\|t\|_*$ nor in $\|\mathbf{fail}t\|_*$).
- The *only* constructs that *generate* ω_2 words are 1) true match until, 2) first match until, and 3) sampling. (These are the only constructs that introduce loops other than self loops on success states in the automata.)
- Operators may propagate or block ω_2 words from its operands upwards. For instance, consider $\{t_1; t_2\}$. If there are any ω_2 words in t_2 then they are propagated upwards: $\sigma \in \|t_2\|_{\omega_2} \Rightarrow \sigma_1\sigma \in \|\{t_1; t_2\}\|_{\omega_2}$, where $\sigma_1 \in \|t_1\|_*$. However, unless $\varepsilon \in \|t_2\|_*$, ω_2 words of t_1 do not propagate upwards to $\|\{t_1; t_2\}\|_{\omega_2}$. The intuition is that ω_2 words have an infinite cyclic tail, hence one cannot append something to such a sequence.

2.6 Examples

Example 1

$$t = \text{any } Up \quad (29)$$

$$\|t\|_* = \{\sigma \in \Sigma^* \mid \sigma = \langle s_1, s_2, \dots, s_i \rangle, s_i \models p \text{ and} \\ \forall 1 \leq j < i : s_j \not\models p\} \quad (30)$$

$$= \langle \bar{p}^*, p \rangle \quad (31)$$

$$S_1 = \{\sigma \in \Sigma^* \mid \sigma = \langle s_1, s_2, \dots, s_i \rangle, \forall 1 \leq j \leq i : s_j \not\models p\} \quad (32)$$

$$= \langle \bar{p}^* \rangle \quad (33)$$

$$\|t\|_* = \Sigma^* \setminus S_1 \quad (34)$$

$$\|\mathbf{fail } t\|_* = \emptyset \quad (35)$$

$$S_2 = \{\sigma \in \Sigma^\omega \mid \sigma = \langle s_1, s_2, \dots \rangle, \forall i \geq 1 : s_i \not\models p\} \quad (36)$$

$$\|t\|_\omega = \Sigma^\omega \setminus S_2 \quad (37)$$

$$\|\mathbf{fail } t\|_{\omega 1} = \emptyset \quad (38)$$

$$\|\mathbf{fail } t\|_{\omega 2} = S_2 \quad (39)$$

$$\|\mathbf{fail } t\|_\omega = S_2 \quad (40)$$

$$\|\mathbf{fail fail } t\|_* = \Sigma^* \setminus S_1 = \|\mathbf{fm } t\|_* \quad (41)$$

$$\|\mathbf{fail fail } t\|_{\omega 1} = \Sigma^\omega \setminus S_2 \quad (42)$$

$$\|\mathbf{fail fail } t\|_{\omega 2} = \emptyset \quad (43)$$

$$\|\mathbf{fail fail } t\|_\omega = \Sigma^\omega \setminus S_2 = \|t\|_\omega \quad (44)$$

Example 2

$$t = (p \Rightarrow \mathbf{fail} (\text{any } U \bar{p})) \wedge \{[.]; q\} \quad (45)$$

$$\|t\|_* = \langle \bar{p}q \rangle \cup \langle \bar{p}\bar{q}, q^*, q \rangle \quad (46)$$

$$\|t\|_{\omega 1} = \langle \bar{p}q, \mathbf{true}^\omega \rangle \cup \langle \bar{p}\bar{q}, q^*, q, \mathbf{true}^\omega \rangle \quad (47)$$

$$\|\{[.]; q\}\|_{\omega 1} = \{\sigma \in \Sigma^\omega \mid \exists i > 0 : s_i \models q\} \quad (48)$$

$$\|\{[.]; q\}\|_{\omega 2} = \emptyset \quad (49)$$

$$\|\{[.]; q\}\|_{\omega 4} = \{\sigma \in \Sigma^\omega \mid \forall i > 0, \exists j \geq i : s_j \models q\} \quad (50)$$

$$\|p \Rightarrow \mathbf{fail} (\text{any } U \bar{p})\|_{\omega 2} = \langle p^\omega \rangle \quad (51)$$

$$\|t\|_{\omega 2} = \langle p^\omega \rangle \cap \|\{[.]; q\}\|_{\omega 4} \quad (52)$$

References

- [1] M. Morley, "Semantics of temporal e," Tech. Rep., Verisity Ltd., March 2000.