

Real-time Property Preservation in Approximations of Timed Systems *

Jinfeng Huang, Jeroen Voeten and Marc Geilen
Eindhoven University of Technology
Faculty of Electrical Engineering
Eindhoven, 5600MB, The Netherlands
E-mail: {J.Huang, J.P.M.Voeten, M.C.W.Geilen}@tue.nl

Abstract

Formal techniques have been widely applied in the design of real-time systems and have significantly helped detect design errors by checking real-time properties of the model. However, a model is only an approximation of its realization in terms of the issuing time of events. Therefore, a real-time property verified in the model can not always be directly transferred to the realization. In this paper, both the model and the realization are viewed as sets of timed state sequences. In this context, we first investigate the real-time property preservation between two neighbouring timed state sequences (execution traces of timed systems), and then extend the results to two “neighbouring” timed systems. The study of real-time property preservation gives insight in building a formal link between real-time properties satisfied in the model and those in the realization.

1 Introduction

Over the past decades, we have witnessed a significant increase in the application of formal techniques to the design of real-time systems. Various studies have been carried out in the advance of real-time property verification techniques [2, 3, 11, 10] and their applications [9, 13]. These real-time properties are formal representations of timing requirements in a realization, whose behaviour is abstracted in the corresponding model. Typically, timed systems and metric interval temporal logic (MITL)[3] have been used to formalize behaviour and timing requirements respectively and have achieved success in yielded a wide range of real-time systems.

*This research is supported by PROGRESS, the embedded systems research program of the Dutch organisation for Scientific Research NWO, the Dutch Ministry of Economic Affairs, the Technology Foundation STW and the Netherlands Organisation for Applied Scientific Research TNO.

However, a model is generally only an approximation of its realization with respect to time (or vice versa). For example, it has been argued in [12] that a real-time formal model M often over-specifies its corresponding physical realizations. In model M , the issuing time of an event p is usually specified as some time instant t_M . However, it cannot be guaranteed that the issuing time t_M of p in M is identical to its counterpart t_R in R (a realization of M). There is a time difference δ_t between them ($\delta_t = t_M - t_R$).

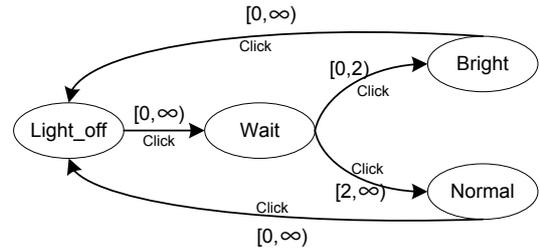


Figure 1. Model of the intelligent light controller

Example 1. Consider an intelligent lighting controller, which can adjust the light intensity according to different input sequences. If there is a click action at the *Light_off* state, the controller goes into the *Wait* state and a timer is activated. If there is a second click taking place within 2 seconds, the controller goes into the *Bright* state. Otherwise, it goes into the *Normal* state. The state transitions of the controller are illustrated in Figure 1.

Consider the following example of a timing requirement for the controller: *Bright* intensity light **only** occurs when the time interval between two clicks is less than 2. This is a real-time property clearly satisfied by the above model. However, in a realization of this model, the timer always has an error in the measurement of time. In case that the timer runs ϵ behind of than the physical time, *Bright* inten-

sity light may occur within $2 + \epsilon$ seconds after a click action at the *Light_off* state. Therefore, a second click taking place at $2 + \frac{1}{2}\epsilon$ will trigger a *Bright* state in the realization. Hence, the property checked in the model does not hold in the realization.

From the example above, we can see that the verification results obtained from the model can not be directly carried over to its realization. In this paper we study properties that can be preserved from a model to its realizations and under what conditions this preservation is guaranteed. Since in general the model and the realization can be both viewed as timed systems, in this paper we study the preservation of real-time properties between two timed systems.

A timed system defines a set of timed state sequences. We first examine real-time property preservation between timed state sequences, the results of which can be applied to the analysis of real-time properties of timed systems. We address the problem by defining two functions.

- A metric d_{sup} as a distance measure over timed state sequences.
- A weakening function R^μ ($\mu \in \mathbb{R}^{\geq 0}$) over real-time properties.

Based on these two functions, we derive two main conclusions for real-time property preservation.

1. *Relaxation property of R^μ* : For real-time property φ , $R^\mu(\varphi)$ is weaker than φ . Furthermore, the larger μ is, the weaker is the real-time property $R^\mu(\varphi)$.
2. *Real-time property preservation between timed state sequences*: Assume that the distance between two timed state sequences $\bar{\tau}$ and $\bar{\tau}'$ is less than or equal to ϵ , i.e. $d_{sup}(\bar{\tau}, \bar{\tau}') \leq \epsilon$. If $\bar{\tau}$ satisfies formula φ , the real-time property $R^{2\epsilon}(\varphi)$ is preserved from $\bar{\tau}$ to $\bar{\tau}'$. Note that by the relaxation property of R^μ , $R^{2\epsilon}(\varphi)$ is also satisfied by $\bar{\tau}$.

We can then extend the results for real-time property preservation between timed state sequences to timed systems. For example, given two timed systems S_1 and S_2 such that for any trace $\bar{\tau}_2$ of S_2 , there exists a trace $\bar{\tau}_1$ of S_1 whose distance from $\bar{\tau}_2$ is less than or equal to ϵ . Thus it can be verified that $S_1 \models \phi$ implies $S_2 \models R^{2\epsilon}(\phi)$. Now if we use S_1 to represent the model and S_2 to represent the realization, the real-time property of the realization can be derived from the real-time property of the model and the distance between their execution traces. The other way around, the satisfaction of a real-time property φ in a realization can also be checked by examining a stronger property φ' in its corresponding model.

The remainder of this paper is organized as follows. Section 2 introduces some mathematical preliminaries. In Section 3, the results of real-time property preservation are explained and proven. In Section 4 we will show how the results can help in solving the over-specification problem described in this section. Discussions and conclusions are presented in Section 5.

2 Preliminaries

In this section we introduce the mathematical structures employed in this paper.

2.1 Behaviour of real-time systems

In this paper, a real-time system is formalized as a timed system consisting of a set of timed state sequences. Each sequence represents a possible execution path of the real-time system. The related concepts are introduced as follows:

- **Proposition set** $Prop$ is a (finite) set of atomic propositions. An observable state of a system can be interpreted by a subset of $Prop$ in which all true-valued propositions are included.
- A **state sequence** σ over proposition set $Prop$ is an infinite or finite sequence $\sigma_0\sigma_1\sigma_2\dots$, where $\sigma_i \in 2^{Prop}$, for $i \in \mathbb{N}$. We use $\bar{\sigma}(i)$ to denote σ_i in the sequence.
- A **time interval** I has one of the following forms: $[a, b)$ and $[a, \infty)$, where $a < b$ and $a, b \in \mathbb{R}^{\geq 0}$. The lower(upper) bound of the interval is represented by $l(I)$ ($r(I)$). $|I| = r(I) - l(I)$ denotes the length of time interval I . If the time interval I is unbounded, $|I|$ is infinite.
- A **time interval sequence** $\bar{I} = I_0I_1I_2\dots$ is an infinite or finite sequence of time intervals. The length (number of time intervals) of a sequence \bar{I} is represented by $N(\bar{I})$ which can be finite or countable infinite. \bar{I} is adjacent, i.e. $r(I_i) = l(I_{i+1})$ for every $i < N(\bar{I})$ and $i \in \mathbb{N}$. \bar{I} is diverging, i.e. for any $t \geq l(I_0)$, there exists some $i \in \mathbb{N}$, such that $t \in I_i$. Hence, a finite time interval sequence ends with an unbounded interval.
- A **metric** d on time interval sequences is given as follows¹.

$$d(\bar{I}, \bar{I}') = \begin{cases} \sup\{|l(I_i) - l(I'_i)| \mid i < N(\bar{I}) \wedge i \in \mathbb{N}\} & \text{if } N(\bar{I}) = N(\bar{I}'); \\ \infty & \text{otherwise.} \end{cases}$$

¹In \mathbb{R} , The supremum (sup) is only exists on bounded sets. In this definition, we define $\sup S = \infty$ when $S \subseteq \mathbb{R}^{\geq 0}$ and is unbounded.

If the lengths of two time interval sequences is equal, the distance between them is defined by the least upper bound of the absolute difference between the left-end points of the corresponding intervals. Otherwise, the distance between them is infinite.

- A **timed state sequence** $\bar{\tau}$ over $Prop$ is a sequence pair $(\bar{\sigma}, \bar{I})$, where $\bar{\sigma}$ is a state sequence over $Prop$ and \bar{I} is a time interval sequence in which $l(I_0) = 0$. The length of $\bar{\sigma}$ and \bar{I} is identical. $\bar{\tau}(t)$ stands for the state presented at the time t .

The untimed behaviour of a system is often abstracted as a set of states and a set of actions representing possible transitions between the states. There are two approaches commonly in use to formalize this behaviour, Kripke Structures (KSs) and Labelled Transitions Systems (LTSs). In KSs, a state is annotated with atomic propositions and a transition is given by a pair of states. In LTSs, a transition is labelled by a single action and states are not annotated. There are various ways to encode a KS to an LTS or vice versa. In this paper, we adopt the approach of KSs to represent the untimed behaviour of a system and a timed system can be interpreted as a set of timed state sequences, each of which represents an execution trace of the system.

2.2 Properties of real-time systems

Basically temporal logics can be classified into branch-time logics and linear-time logics [5]. The main difference between them is that they are interpreted over different structures of states. Branch-time logics are interpreted over tree structures of states such as in CTL [6, 7] and $TCTL$ [1]. Linear-time logics, on the other hand, are interpreted over trace semantics (linear structures of states) such as in $TPTL$ [4] and $MITL$ [3].

In this paper, we adopt $MITL_{\mathbb{R}}$ (an extension of real-time logic $MITL$) to formalize properties of real-time systems. $MITL_{\mathbb{R}}$ formulas are formed by the following structures.

$$\varphi ::= p \mid \neg p \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \mathbf{U}_I \varphi_2 \mid \varphi_1 \mathbf{V}_I \varphi_2$$

where I is a time-bound interval of nonnegative reals. It takes one of the following forms: $[a, b]$, $[a, b)$, $(a, b]$, (a, b) , $[a, \infty)$ and (a, ∞) , where $a \leq b$ for $a, b \in \mathbb{R}^{\geq 0}$. Now we define two scaling operators on time-bound interval. Let $\epsilon \in \mathbb{R}^{\geq 0}$. \oplus and \ominus are defined:

$$\begin{aligned} I \oplus \epsilon &= \{t \in \mathbb{R}^{\geq 0} \mid \exists t' \in I \wedge |t - t'| \leq \epsilon\} \\ I \ominus \epsilon &= \{t \in \mathbb{R}^{\geq 0} \mid \forall t' \in \mathbb{R}^{\geq 0} \wedge |t - t'| \leq \epsilon \rightarrow t' \in I\} \end{aligned}$$

Informally speaking, $I \oplus \epsilon$ represents the time interval which elongates the end points of I to $l(I) - \epsilon$ and $r(I) + \epsilon$ respectively in nonnegative reals. Similarly, $I \ominus \epsilon$ represents the

time interval which shrinks the end points of I to $l(I) + \epsilon$ and $r(I) - \epsilon$ respectively. Several examples are:

- if $I = [2\pi, 4\pi]$ then $I \oplus \pi = [\pi, 5\pi]$;
- if $I = (3, \infty)$ then $I \oplus 5 = [0, \infty)$;
- if $I = [1.1, 2)$ then $I \ominus 3 = \emptyset$.

$MITL_{\mathbb{R}}$ extends $MITL$ in the following aspects: In order to make model-checking feasible, there are two constraints on time-bound intervals in the $MITL$ formulas.

- Every time-bound interval I should be nonsingular and nonempty.
- The end-points of I are restricted to integer values²

Since we only use $MITL_{\mathbb{R}}$ to express real-time properties of a system, it is not necessary to employ the same constraints on the representation of time bound in $MITL_{\mathbb{R}}$ formulas.

The interpretation of $MITL_{\mathbb{R}}$ formulas over timed state sequences is standard and given in Definition 1.

Definition 1. Let $\bar{\tau}$ be a timed state sequence and let $t \in \mathbb{R}^{\geq 0}$. For any $MITL_{\mathbb{R}}$ formula φ , the interpretation of φ over $(\bar{\tau}, t)$ is given as follows:

- $(\bar{\tau}, t) \models p$ iff $p \in \bar{\tau}(t)$;
- $(\bar{\tau}, t) \models \neg p$ iff $p \notin \bar{\tau}(t)$;
- $(\bar{\tau}, t) \models \varphi_1 \vee \varphi_2$ iff $(\bar{\tau}, t) \models \varphi_1$ or $(\bar{\tau}, t) \models \varphi_2$;
- $(\bar{\tau}, t) \models \varphi_1 \wedge \varphi_2$ iff $(\bar{\tau}, t) \models \varphi_1$ and $(\bar{\tau}, t) \models \varphi_2$;
- $(\bar{\tau}, t) \models \varphi_1 \mathbf{U}_I \varphi_2$ iff there is some $t_2 \in I$, such that $(\bar{\tau}, t + t_2) \models \varphi_2$ and for all $0 \leq t_1 < t_2$, $(\bar{\tau}, t + t_1) \models \varphi_1$;
- $(\bar{\tau}, t) \models \varphi_1 \mathbf{V}_I \varphi_2$ iff for all $t_2 \in I$, $(\bar{\tau}, t + t_2) \models \varphi_2$ or there is some $0 \leq t_1 < t_2$, $(\bar{\tau}, t + t_1) \models \varphi_1$.

In case that I is empty, $(\bar{\tau}, t) \models \varphi_1 \mathbf{U}_I \varphi_2$ is always false and $(\bar{\tau}, t) \models \varphi_1 \mathbf{V}_I \varphi_2$ always holds. we use $(\bar{\tau}, 0) \models \varphi$ ($\bar{\tau} \models \varphi$, in short) to denote that a timed state sequence $\bar{\tau}$ satisfies $MITL_{\mathbb{R}}$ formula φ . We extend the interpretation of $MITL_{\mathbb{R}}$ to sets of timed state sequences as follows.

Definition 2. Let φ be an $MITL_{\mathbb{R}}$ formula, and let T be a set of timed state sequences. $T \models \varphi$ iff for each timed state sequence $\bar{\tau} \in T$, $\bar{\tau} \models \varphi$.

Now we introduce two additional operators: $\diamond_I \varphi$ (time-bounded eventually) and $\square_I \varphi$ (time-bounded always) abbreviate $true \mathbf{U}_I \varphi$ and $false \mathbf{V}_I \varphi$ respectively.

²The $MITL$ logic employs the nonnegative real-valued time domain, but it constrains the endpoints of I as integers.

2.3 Normalization of timed state sequences

A timed state sequence $\bar{\tau} = (\bar{\sigma}, \bar{I})$ can be viewed as a function from a time domain $\mathbb{R}^{\geq 0}$ to a state space 2^{Prop} [3]. Through this function, every time instant t along the time line is assigned a state $\bar{\tau}(t)$. From this point of view, some timed state sequences with different state sequences and time interval sequences may represent the same function and can not be discriminated by $MITL_{\mathbb{R}}$.

Example 2. Define two timed state sequences $\bar{\tau}$ and $\bar{\tau}'$ as follows. $\bar{\tau} = (\bar{\sigma}, \bar{I})$ where for all $i \in \mathbb{N}$, $\bar{\sigma}(i) = \delta_i$ and $\bar{I}(i) = [2i, 2i + 2)$. $\bar{\tau}' = (\bar{\sigma}', \bar{I}')$ where for all $i \in \mathbb{N}$, $\bar{\sigma}'(2i) = \bar{\sigma}'(2i+1) = \delta_i$ and $\bar{I}'(i) = [i, i+1)$. It is not hard to see that for any $t \in \mathbb{R}^{\geq 0}$, $\bar{\tau}(t) = \bar{\tau}'(t)$. Therefore, the timed state sequences $\bar{\tau}$ and $\bar{\tau}'$ represent the same function from time domain $\mathbb{R}^{\geq 0}$ to state set $\{\delta_i \mid i \in \mathbb{N}\}$.

Definition 3. Two timed state sequences $\bar{\tau} = (\bar{\sigma}, \bar{I})$ and $\bar{\tau}' = (\bar{\sigma}', \bar{I}')$ are equivalent (\equiv) iff for all $t \in \mathbb{R}^{\geq 0}$, $\bar{\tau}(t) = \bar{\tau}'(t)$.

Any timed state sequence $\bar{\tau}$ can be normalized to a timed state sequence $\bar{\tau}^*$, which is the normal form of $\bar{\tau}$, by performing the following operations. Along the state sequence of $\bar{\tau}$, successive identical states are replaced by one single state, and their corresponding time intervals are also merged into one single time interval. It can be shown that $\bar{\tau} \equiv \bar{\tau}^*$ iff they have the same normal form. In Example 2, if no two sequential states δ_i and δ_{i+1} ($i \in \mathbb{N}$) are identical, we can conclude that $\bar{\tau}$ is the normal form of $\bar{\tau}'$.

Recall the interpretation of $MITL_{\mathbb{R}}$ formulas over timed state sequences in Definition 1. Notice that the satisfaction relation $\bar{\tau} \models \varphi$ depends on the mapping from the time domain to its state set only, so it is independent of various choices of time interval sequences.

Proposition 1. Let φ be an $MITL_{\mathbb{R}}$ formula. If two timed state sequences $\bar{\tau}$ and $\bar{\tau}'$ are equivalent, then $\bar{\tau} \models \varphi$ iff $\bar{\tau}' \models \varphi$.

Since $MITL_{\mathbb{R}}$ formulas cannot distinguish equivalent timed state sequences, we assume in the sequel that timed state sequences are in normal form if not explicitly stated otherwise.

2.4 Measuring timed state sequences

Let set S_{Prop} consist of all timed state sequences in normal form over a proposition set $Prop$. We define another equivalence relation (\equiv_s) that divides S_{Prop} into groups sharing the same state sequence $\bar{\sigma}$.

Definition 4. An equivalence relation (\equiv_s) on set S_{Prop} is defined as follows. For any two timed state sequences

$\bar{\tau}, \bar{\tau}' \in S_{Prop}$, if $\bar{\tau} = (\bar{\sigma}, \bar{I})$ and $\bar{\tau}' = (\bar{\sigma}', \bar{I}')$, then $\bar{\tau} \equiv_s \bar{\tau}'$ iff $\bar{\sigma} = \bar{\sigma}'$.

In order to evaluate the distance between two timed state sequences in S_{Prop} , we adopt a metric d_{sup} . For two timed sequences in the same partition of S_{Prop} , d_{sup} is defined as the *least upper bound* of the absolute difference between time-stamps of corresponding state transitions in two state sequences. For example, Figure 2 shows two timed state sequences which have the same state sequence. There are four state transitions in each timed state sequence. $d_{sup}(\bar{\tau}_1, \bar{\tau}_2)$ is computed as $\sup\{|0 - 0|, |1.1 - 1.2|, |2.3 - 2.2|, |3.3 - 3.4|, |4.4 - 4.2|\} = 0.2$.

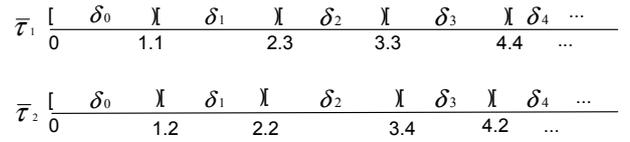


Figure 2. Two finite timed state sequences

Definition 5. The metric d_{sup} on S_{Prop} is formally defined as follows. For $\bar{\tau}, \bar{\tau}' \in S_{Prop}$,

$$d_{sup}(\bar{\tau}, \bar{\tau}') = \begin{cases} d(\bar{I}, \bar{I}') & \text{if } \bar{\tau} \equiv_s \bar{\tau}'; \\ \infty & \text{otherwise} \end{cases}$$

where $d(\bar{I}, \bar{I}')$, which is defined in Section 2.1, denotes the distance between two time interval sequences.

Gupta et al. proposed several metrics over finite timed state sequences in [12]. We only adopt d_{sup} (similar to the metric d_{max} in [12]) as a measure over S_{Prop} including both infinite and finite timed state sequences.

Definition 6. For $\bar{\tau} = (\bar{\sigma}, \bar{I})$ and $\epsilon \in \mathbb{R}^{\geq 0}$ we define an ϵ -close set $T_{\epsilon}^{\bar{\tau}} = \{\bar{\tau}' \in S_{Prop} \mid d_{sup}(\bar{\tau}, \bar{\tau}') \leq \epsilon\}$.

Set $T_{\epsilon}^{\bar{\tau}}$ includes all timed state sequences whose distance from $\bar{\tau}$ is less than or equal to ϵ in set S_{Prop} .

3 Real-time property preservation

Real-time property preservation between timed state sequences is based on their distance in S_{Prop} . Given a real-time property of one timed state sequence and (an upper bound of) its distance to another timed state sequence, a related property of the latter one is guaranteed without additional computation.

In this section, the results of real-time property preservation are presented in the following order.

1. The introduction of the ϵ -neighbouring function ($\epsilon \in \mathbb{R}^{\geq 0}$) and the proof of its existence for two timed interval sequences whose distance is less than or equal

to ϵ based on metric d_{sup} (see Section 3.1). In fact, ϵ -neighbouring function between two timed interval sequences provide another representation of the distance between them.

2. The definition of a weakening function R^μ (parameterized with $\mu \in \mathbb{R}^{\geq 0}$) over the set of $MITL_{\mathbb{R}}$ formulas in which $R^\mu(\varphi)$ is called the μ -weakened formula of φ (see Section 3.2).
3. The results of real-time property preservation are explained and proven (see Sections 3.3 and 3.4).

3.1 ϵ -neighbouring function

Recall that metric d_{sup} defines the distance between two timed state sequences in set S_{Prop} by calculating the least upper bound of the absolute time difference of their corresponding state transitions. In other words, the distance between two timed state sequences which share the same state sequence is equal to the distance between their timed interval sequences.

Given two time interval sequences \bar{I} and \bar{I}' , an ϵ -neighbouring function establishes a one-to-one mapping from a time instant t in \bar{I} to a time instant t' in \bar{I}' . The definition of the ϵ -neighbouring function is given in Definition 7.

Definition 7. Let $\epsilon \in \mathbb{R}^{\geq 0}$. A function $F : \mathbb{R}^{\geq l(I_0)} \rightarrow \mathbb{R}^{\geq l(I'_0)}$ is called an ϵ -neighbouring function from time interval sequence \bar{I} to \bar{I}' , if and only if it has all of the following properties³.

- **Interval consistency:** For every $t \in \mathbb{R}^{\geq l(I_0)}$, $t \in I_k$ implies $F(t) \in I'_k$ where $k < N(\bar{I})$ and $k \in \mathbb{N}$.
- **One to one mapping:** For all $t_1, t_2 \in \mathbb{R}^{\geq l(I_0)}$, $t_1 \neq t_2$ implies $F(t_1) \neq F(t_2)$. Furthermore, for every $t' \in \mathbb{R}^{\geq l(I'_0)}$, there exists a $t \in \mathbb{R}^{\geq l(I_0)}$, such that $t' = F(t)$.
- **Monotone increasing mapping:** For any $t_1, t_2 \in \mathbb{R}^{\geq l(I_0)}$, $t_1 > t_2$ implies $F(t_1) > F(t_2)$.
- **ϵ -bound:** For every $t \in \mathbb{R}^{\geq l(I_0)}$, $|F(t) - t| \leq \epsilon$.

If there exists an ϵ -neighbouring function F from \bar{I} to \bar{I}' , timed interval sequences \bar{I} and \bar{I}' are called ϵ -neighbouring.

Lemma 1. If F is an ϵ -neighbouring function from \bar{I} to \bar{I}' , then F^{-1} is an ϵ -neighbouring function from \bar{I}' to \bar{I} .

³ $\mathbb{R}^{\geq l(I_0)}$ represents the interval $[l(I_0), \infty)$

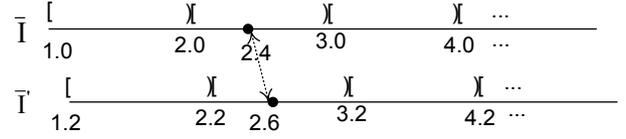


Figure 3. Two time interval sequences

Proof. The lemma follows straightforwardly from the definition of ϵ -neighbouring function. \square

Example 3. Given two time interval sequences $\bar{I} = I_1 I_2 I_3 \dots$ (where $I_k = [k, k + 1)$) and $\bar{I}' = I'_1 I'_2 I'_3 \dots$ (where $I'_k = [k + 0.2, k + 1.2)$) as in Figure 3. $F(t) = t + 0.2$ ($t \in \mathbb{R}^{\geq 1.0}$) is a mapping from \bar{I} to \bar{I}' . It is not hard to check that F is a 0.2-neighbouring function from \bar{I} to \bar{I}' . $F^{-1}(t) = t - 0.2$ ($t \in \mathbb{R}^{\geq 1.2}$) is a 0.2-neighbouring function from \bar{I}' to \bar{I} .

It should be noticed that for any two time interval sequences and any ϵ ($\epsilon \in \mathbb{R}^{\geq 0}$), the ϵ -neighbouring function does not always exist. For example, there is no 0.1-neighbouring function from \bar{I} to \bar{I}' defined in Example 3. The following theorem establishes the necessary and sufficient condition for the existence of an ϵ -neighbouring function over two time interval sequences.

Lemma 2. If F is an ϵ -neighbouring function from \bar{I} to \bar{I}' then $F(l(I_i)) = l(I'_i)$, for all $i < N(\bar{I})$ and $i \in \mathbb{N}$.

Proof. Suppose $F(l(I_i)) = t$ and $t \neq l(I'_i)$. By the interval consistency property of F , it is easy to see that $t > l(I'_i)$. For any $l(I'_i) < t' < t$, there exists t'' and $F(t'') = t'$. By the monotone increasing mapping property of F , it is easy to see that $t'' < l(I_i)$, which contradicts the interval consistency property of F . \square

Theorem 1. Let \bar{I} and \bar{I}' be two time interval sequences. \bar{I} and \bar{I}' are ϵ -neighbouring, iff $d(\bar{I}, \bar{I}') \leq \epsilon$.

Proof. (\Rightarrow) It is not hard to prove by Lemma 2 and the ϵ -bound property of the ϵ -function.

(\Leftarrow) Construct a function $G : \mathbb{R}^{\geq l(I_0)} \rightarrow \mathbb{R}^{\geq l(I'_0)}$ as follows.

$$G(t) = (t - l(I_k)) \frac{|I'_k|}{|I_k|} + l(I'_k) \quad t \in I_k, k < N(\bar{I}) \text{ and } k \in \mathbb{N}$$

In case that both $|I_k|$ and $|I'_k|$ are infinite, we define $\frac{|I'_k|}{|I_k|} = 1$.

As shown in Figure 4(b), the function G is a monotone increasing linear function on every time interval. It is not hard to show that G satisfies the first three properties of the ϵ -neighbouring function.

Next we show that G also satisfies the ϵ -bound property.

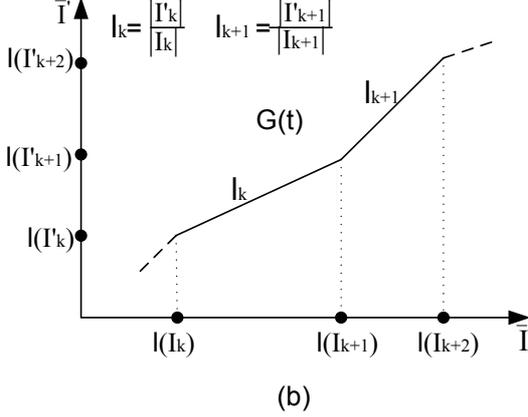
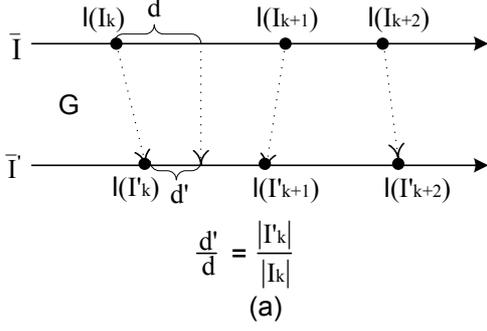


Figure 4. ϵ -neighbouring function G

(a) Function G from \bar{I} to \bar{I}' along the time line
(b) Visualization of function G

For any $t \in \mathbb{R}^{\geq l(I_0)}$, there exists a time interval I_k , $k \in \mathbb{N}$ such that $t \in I_k$. Construct a function $diff(t) = G(t) - t$. Since $diff(t)$ is a linear function within interval I_k , $|diff(t)| \leq \text{Max}\{|diff(l(I_k))|, \lim_{t \rightarrow r(I_k)} |diff(t)|\}$. By the continuity of $diff(t)$ and the adjacent property of time interval sequence \bar{I} , it is not hard to see that $|diff(t)| \leq \text{Max}\{|diff(l(I_k))|, |diff(l(I_{k+1}))|\}$. By the definition of G , It is easy to prove that $diff(l(I_k)) = l(I'_k) - l(I_k)$. Since $d_{sup}(\bar{I}, \bar{I}') \leq \epsilon$, by the definition of d_{sup} , we can see $|diff(t)| \leq \epsilon$. Hence, G satisfies the ϵ -bound property.

We have shown that G is an ϵ -neighbouring function from \bar{I} to \bar{I}' and hence, \bar{I} and \bar{I}' are ϵ -neighbouring. \square

From Theorem 1, we can see that the existence of ϵ -neighbouring functions between two time interval sequences give another characterization of the distance between them.

3.2 Weakening functions R^μ over formulas

$MITL_{\mathbb{R}}$ incorporates quantitative timing constraints in its operators which enables $MITL_{\mathbb{R}}$ formulas to express quantitative timing properties. At the same time, these

quantitative timing constraints in the formulas can also be used to show weakening or strengthening relation between formulas. For example, in $MITL_{\mathbb{R}}$, $pU_{[0,\mu]}q$ specifies a real-time property that q happens within μ time after p . For different values of μ , formulas have different quantitative timing constraints. Formula $pU_{[0,2]}q$ has stronger requirement on the issuing time of q than formula $pU_{[0,2.5]}q$, because the satisfaction of the former formula always implies the satisfaction of the latter one. In Definition 8, function R^μ defines such a weakening function on formulas. It offers a quantitative way to weaken timing requirements of $MITL_{\mathbb{R}}$ formulas.

Definition 8. Let $\mu \in \mathbb{R}^{\geq 0}$. The weakening function $R^\mu : MITL_{\mathbb{R}} \rightarrow MITL_{\mathbb{R}}$ is defined as follows:

$$\begin{aligned} R^\mu(p) &= p; \\ R^\mu(\neg p) &= \neg p; \\ R^\mu(\varphi_1 \vee \varphi_2) &= R^\mu(\varphi_1) \vee R^\mu(\varphi_2); \\ R^\mu(\varphi_1 \wedge \varphi_2) &= R^\mu(\varphi_1) \wedge R^\mu(\varphi_2); \\ R^\mu(\varphi_1 U_I \varphi_2) &= R^\mu(\varphi_1) U_{I \oplus \mu} R^\mu(\varphi_2); \\ R^\mu(\varphi_1 V_I \varphi_2) &= R^\mu(\varphi_1) V_{I \ominus \mu} R^\mu(\varphi_2); \end{aligned}$$

For every $\mu \in \mathbb{R}^{\geq 0}$, R^μ defines a function over $MITL_{\mathbb{R}}$. $R^\mu(\varphi)$ relaxes the quantitative timing constraints in formula φ and is called the μ -weakened formula of φ . Next, we will prove that formula $R^\mu(\varphi)$ is indeed weaker than formula φ .

Lemma 3. For any $\mu \in \mathbb{R}^{\geq 0}$, $t \in \mathbb{R}^{\geq 0}$, $\varphi \in MITL_{\mathbb{R}}$ and $\bar{\tau} \in S_{Prop}$, if $(\bar{\tau}, t) \models \varphi$, then $(\bar{\tau}, t) \models R^\mu(\varphi)$.

Proof. Suppose $(\bar{\tau}, t) \models \varphi$. We will show that $(\bar{\tau}, t) \models R^\mu(\varphi)$ by induction on the structure of formula φ .

Case 1: $\varphi = p$.

By definition of function R^μ , $R^\mu(\varphi) = p$. Hence, $(\bar{\tau}, t) \models R^\mu(\varphi)$.

Case 2: $\varphi = \neg p$.

The proof is similar to the pervious case.

Case 3: $\varphi = \varphi_1 \vee \varphi_2$.

By the interpretation of $MITL_{\mathbb{R}}$ over timed state sequences, $(\bar{\tau}, t) \models \varphi_1$ or $(\bar{\tau}, t) \models \varphi_2$. By induction we thus have $(\bar{\tau}, t) \models R^\mu(\varphi_1)$ or $(\bar{\tau}, t) \models R^\mu(\varphi_2)$. Hence, $(\bar{\tau}, t) \models R^\mu(\varphi_1) \vee R^\mu(\varphi_2) = R^\mu(\varphi)$.

Case 4: $\varphi = \varphi_1 \wedge \varphi_2$.

The proof of this case is similar to the previous case.

Case 5: $\varphi = \varphi_1 U_I \varphi_2$.

There is some $t_2 \in I$, such that $(\bar{\tau}, t + t_2) \models \varphi_2$ and for all $0 \leq t_1 < t_2$, $(\bar{\tau}, t + t_1) \models \varphi_1$. It is obvious that $t_2 \in I \oplus \mu$. By induction we have $(\bar{\tau}, t + t_2) \models R^\mu(\varphi_2)$ and for all $0 \leq t_1 < t_2$, $(\bar{\tau}, t + t_1) \models R^\mu(\varphi_1)$. Hence, $(\bar{\tau}, t) \models R^\mu(\varphi_1) U_{I \oplus \mu} R^\mu(\varphi_2) = R^\mu(\varphi_1 U_I \varphi_2) = R^\mu(\varphi)$.

Case 6: $\varphi = \varphi_1 V_I \varphi_2$.

For all $t_2 \in I$, $(\bar{\tau}, t + t_2) \models \varphi_2$ or there is some $0 \leq t_1 < t_2$, $(\bar{\tau}, t + t_1) \models \varphi_1$. By induction we thus have for all $t_2 \in I \ominus \mu$, $(\bar{\tau}, t + t_2) \models R^\mu(\varphi_2)$ or there is some

$0 \leq t_1 < t_2$, $(\bar{\tau}, t + t_1) \models R^\mu(\varphi_1)$. Hence, $(\bar{\tau}, t) \models R^\mu(\varphi_1) \vee_{I \oplus \mu} R^\mu(\varphi_2) = R^\mu(\varphi)$.

This completes our inductive proof of Lemma 3. \square

Theorem 2. (Relaxation property of R^μ) For any $\mu \in \mathbb{R}^{\geq 0}$, $\varphi \in MITL_{\mathbb{R}}$ and $\bar{\tau} \in S_{Prop}$, if $\bar{\tau} \models \varphi$, then $\bar{\tau} \models R^\mu(\varphi)$.

Proof. Follows directly from Lemma 3. \square

In general, the larger the value of μ is, the weaker is formula $R^\mu(\varphi)$.

3.3 Real-time property preservation between timed state sequences

In the previous sections, the ϵ -neighbouring function is used to characterize the distance between two neighbouring timed state sequences in set S_{Prop} . Then we introduced the weakening functions R^μ to quantitatively weaken $MITL_{\mathbb{R}}$ formulas. In this section, we investigate the properties that are preserved between neighbouring sequences in S_{Prop} by employing the above two functions.

Lemma 4. Let $\epsilon \in \mathbb{R}^{\geq 0}$, $t \in \mathbb{R}^{\geq 0}$ and $\varphi \in MITL_{\mathbb{R}}$. Further let $\bar{\tau}$ and $\bar{\tau}'$ be two ϵ -neighbouring timed state sequences⁴ and let G be an ϵ -neighbouring function from the time interval sequence of $\bar{\tau}$ to that of $\bar{\tau}'$. Then $(\bar{\tau}, t) \models \varphi$ implies $(\bar{\tau}', G(t)) \models R^{2\epsilon}(\varphi)$.

Proof. We show that $(\bar{\tau}', G(t)) \models R^{2\epsilon}(\varphi)$ by induction on the structure of formula φ .

Case 1: $\varphi = p$.

By definition of function $R^{2\epsilon}$, $R^{2\epsilon}(\varphi) = p$. By the interpretation of $MITL_{\mathbb{R}}$ formulas over timed state sequences, $p \in \bar{\tau}(t)$. Since G is an ϵ -neighbouring function from the time interval sequence of $\bar{\tau}$ to that of $\bar{\tau}'$ and since $\bar{\tau}$ and $\bar{\tau}'$ share the same state sequence, we know that $\bar{\tau}(t) = \bar{\tau}'(G(t))$ by the interval consistency property of G . Hence, $p \in \bar{\tau}'(G(t))$. But then, $(\bar{\tau}', G(t)) \models R^{2\epsilon}(\varphi)$.

Case 2: $\varphi = \neg p$.

The proof is similar to the previous case.

Case 3: $\varphi = \varphi_1 \vee \varphi_2$.

$(\bar{\tau}, t) \models \varphi_1$ or $(\bar{\tau}, t) \models \varphi_2$. By induction we have $(\bar{\tau}', G(t)) \models R^{2\epsilon}(\varphi_1)$ or $(\bar{\tau}', G(t)) \models R^{2\epsilon}(\varphi_2)$. But then $(\bar{\tau}', G(t)) \models R^{2\epsilon}(\varphi_1) \vee R^{2\epsilon}(\varphi_2) = R^{2\epsilon}(\varphi)$.

Case 4: $\varphi = \varphi_1 \wedge \varphi_2$.

The proof is similar to the previous case.

Case 5: $\varphi = \varphi_1 \cup_I \varphi_2$.

There is some $t_2 \in I$, such that $(\bar{\tau}, t + t_2) \models \varphi_2$ and

⁴We call two timed state sequences ϵ -neighbouring iff they are \equiv_s -equivalent and their time interval sequences are ϵ -neighbouring. In other words, the distance between ϵ -neighbouring timed state sequences is less than or equal to ϵ

for all $0 \leq t_1 < t_2$, $(\bar{\tau}, t + t_1) \models \varphi_1$. By induction we have $(\bar{\tau}', G(t + t_2)) \models R^{2\epsilon}(\varphi_2)$. For any $0 \leq t'_1 < G(t + t_2) - G(t)$, by the one to one mapping and monotone increasing mapping properties of G , there is a $0 \leq t''_1 < t_2$, such that $G(t + t''_1) = G(t) + t'_1$. By induction we have $(\bar{\tau}', G(t + t''_1)) \models R^{2\epsilon}(\varphi_1)$. Hence $(\bar{\tau}', G(t) + t'_1) \models R^{2\epsilon}(\varphi_1)$.

Now, we will show that $G(t + t_2) - G(t) \in I \oplus 2\epsilon$. By the Triangle Inequality and the ϵ -bound property of G ,

$$\begin{aligned} & G(t + t_2) - G(t) \\ &= G(t + t_2) - (t + t_2) - (G(t) - t) + t_2 \\ &\leq |G(t + t_2) - (t + t_2)| + |(G(t) - t)| + t_2 \\ &\leq \epsilon + \epsilon + t_2 \\ &= t_2 + 2\epsilon \end{aligned}$$

Similarly, It is easy to prove that $G(t + t_2) - G(t) \geq t_2 - 2\epsilon$. By the monotone increasing mapping property of G , we know $G(t + t_2) - G(t) \geq 0$. Therefore, $\max\{t_2 - 2\epsilon, 0\} \leq G(t + t_2) - G(t) \leq t_2 + 2\epsilon$. Since $t_2 \in I$, it is not hard to check that $G(t + t_2) - G(t) \in I \oplus 2\epsilon$.

Hence, $(\bar{\tau}', G(t)) \models R^{2\epsilon}(\varphi_1) \cup_{I \oplus 2\epsilon} R^{2\epsilon}(\varphi_2) = R^{2\epsilon}(\varphi)$.

Case 6: $\varphi = \varphi_1 \vee_I \varphi_2$.

The proof is similar to the previous case. A brief proof is given as follows.

For all $t'_2 \in I \ominus 2\epsilon$, it is not hard to prove that there exist $t_2 \in I$ such that $G(t_2 + t) = t'_2 + G(t)$. There are two possibilities:

- $(\bar{\tau}, t + t_2) \models \varphi_2$. By induction we have $(\bar{\tau}', G(t + t_2)) \models R^{2\epsilon}(\varphi_2)$, that is, $(\bar{\tau}', G(t) + t'_2) \models R^{2\epsilon}(\varphi_2)$.
- There is some $0 \leq t_1 < t_2$, such that $(\bar{\tau}, t + t_1) \models \varphi_1$. Let $t'_1 = G(t + t_1) - G(t)$ and it is not hard to prove that $0 \leq t'_1 < t'_2$. By induction we have $(\bar{\tau}', G(t) + t'_1) \models R^{2\epsilon}(\varphi_1)$.

Hence, $(\bar{\tau}, G(t)) \models R^{2\epsilon}(\varphi_1) \vee_{I \oplus 2\epsilon} R^{2\epsilon}(\varphi_2) = R^{2\epsilon}(\varphi)$.

This completes our inductive proof of Lemma 4. \square

Theorem 3. Let $\epsilon \in \mathbb{R}^{\geq 0}$, $t \in \mathbb{R}^{\geq l(I_0)}$ and $\varphi \in MITL_{\mathbb{R}}$. Further let $\bar{\tau}$ and $\bar{\tau}'$ be two ϵ -neighbouring timed state sequences then $\bar{\tau} \models \varphi$ implies $\bar{\tau}' \models R^{2\epsilon}(\varphi)$.

Proof. It is not hard to prove by Lemma 4 and Lemma 2. \square

Recall Definition 2 and Definition 6, for any timed state sequence $\bar{\tau} \in S_{Prop}$, $T_\epsilon^{\bar{\tau}}$ is set which contains all timed state sequences whose distance from $(\bar{\tau}, t)$ is less than or equal to ϵ . We can extend the real-time preservation between two timed state sequences to sets of timed state sequences. This extension is given in Corollary 1.

Corollary 1. For any $\epsilon \in \mathbb{R}^{\geq 0}$, $\varphi \in MITL_{\mathbb{R}}$, $\bar{\tau} \in S_{Prop}$, if $\bar{\tau} \models \varphi$ then $T_\epsilon^{\bar{\tau}} \models R^{2\epsilon}(\varphi)$.

Proof. It is not hard to prove by Theorem 3 and interpretation of $MITL_{\mathbb{R}}$ formulas over the set of timed state sequences. \square

3.4 Real-time property preservation between timed systems

In the previous part of this paper, we concentrated on real-time property preservation between timed state sequences. However, in practice we often need to analyse real-time properties of a timed system instead of those of a single timed state sequence. Since a timed system consists of a set of timed state sequences, the problem of examining the satisfaction of a formula φ in a timed system S is equivalent to examining its satisfaction in all of the timed state sequences in S . Real-time property preservation between timed state sequences can also be extended to analyse real-time properties between timed systems. The following theorems give these extensions.

Theorem 4. *Let S be a set of timed state sequences and let φ be an $MITL_{\mathbb{R}}$ formula. For any $\epsilon \in \mathbb{R}^{\geq 0}$, if $S \models \varphi$, then $S \models R^\epsilon(\varphi)$.*

Proof. Follows from Definition 2 and Theorem 2. \square

Theorem 5. *Let S_1, S_2 be two sets of timed state sequences and let φ be an $MITL_{\mathbb{R}}$ formula. Assume there is some $\epsilon \in \mathbb{R}^{\geq 0}$, such that for any timed state sequence $\bar{\tau}$ in S_2 there exists a sequence $\bar{\tau}'$ in S_1 such that $\bar{\tau}$ and $\bar{\tau}'$ are ϵ -neighbouring. Then $S_1 \models \varphi$ implies $S_2 \models R^{2\epsilon}(\varphi)$.*

Proof. The theorem follows from Definition 2 and Theorem 3. \square

4 Problem revisited

As described in Section 1, the over-specification problem often leads to the failure of transferring of verification results from a model to its realization. The issuing time of event p in the realization may have a δ time shift from the time specified in the model M . Time shifts can be different for each event in the realization. Although it is often impossible to know the exact value of time shift δ for each pair of corresponding events in the model M and its physical realization R , the upper bound of all δ can be more easily estimated. Then for any execution trace \bar{t}_r in R , we can find an ϵ -neighbouring execution trace \bar{t}_m in M . In that case, we can establish properties of S based on the verification results of M .

Reconsider the example given in Section 1. Assume p, q and r are three atomic propositions as follows:

- p : The controller is in the *Wait* state.

- q : The controller is in the *Bright* state.

- r : The controller is in the *Normal* state.

A real-time property $\varphi = \Box(p \rightarrow (\Diamond_{[0,2]}q \vee \Diamond_{[2,\infty)}r))$ can be described as follows: when a click happens at the *Light_off* state, it either goes into *Bright* state within 2 seconds or goes into *Normal* state after 2 seconds. It is not hard to check that this property holds in the model.

Suppose that an upper bound of the timer error in the realization is 0.01 second. It is not hard to check that for any execution trace $\bar{\tau}$ of such a realization, we can always find an execution trace $\bar{\tau}'$ whose distance from $\bar{\tau}$ is less or equal to 0.01. Therefore, real-time property $R^{0.02}(\varphi) = \Box(p \rightarrow (\Diamond_{[0,2.02]}q \vee \Diamond_{[1.98,\infty)}r))$ is satisfied in this realization. Notice that the result also can be applied the other way around. If our objective is to check the satisfaction of the real-time property $R^{0.02}(\varphi) = \Box(p \rightarrow (\Diamond_{[0,2.02]}q \vee \Diamond_{[1.98,\infty)}r))$ in the realization, we can check a stronger property $\Box(p \rightarrow (\Diamond_{[0,2.02-2\epsilon]}q \vee \Diamond_{[1.98+2\epsilon,\infty)}r))$ in the model, where ϵ is used to measure the time difference between the model and the realization.

5 Discussion and Conclusion

In this paper, we have investigated the preservation of real-time properties between timed systems. For some special cases, a better property preservation result might be achieved. This can be illustrated in the following example. Let $\bar{\tau}_1$ and $\bar{\tau}_2$ be two ϵ -neighbouring timed state sequences. The issuing time of any state transition in $\bar{\tau}_1$ is always no later (or no earlier) than the corresponding issuing time in $\bar{\tau}_2$. Then $\bar{\tau}_1 \models \varphi$ implies that $\bar{\tau}_2 \models R^\epsilon(\varphi)$, in which $R^\epsilon(\varphi)$ is a stronger formula than $R^{2\epsilon}(\varphi)$. The proof of this is similar to the proof of Theorem 3.

Since interleaving semantics is not supported in this paper, which sequentialize concurrent actions as a sequence of actions occurring at the same time instant, we are investigating the real-time property preservation with interleaving semantics for concurrent systems.

Another application of real-time property preservation is real-time software synthesis as suggested in [8]. In the model, actions(events) are formalized as instantaneous events instead of events that have some time duration in the realization. If the synthesis method can guarantee that the absolute difference of the issuing time of the corresponding events in both the realization and the model is always less than or equal to a constant, we can obtain the real-time properties of the realization based on those of the model. We are extending and exploring this application and aim at a systematic approach to develop reliable real-time systems.

References

- [1] R. Alur, C. Courcoubetis, and D. Dill. Model checking for real-time systems. In *In Proceedings of the Fifth Annual Symposium on Logic in Computer Science*, pages 414–425. IEEE Computer Society Press, 1990.
- [2] R. Alur and D.L. Dill. A theory of timed automata. *Theoretical Computer Science*, 126:183–235, 1994.
- [3] R. Alur, T. Feder, and T.A. Henzinger. The benefits of relaxing punctuality. *Journal of the ACM*, 43(1):116–146, 1996.
- [4] R. Alur and T.A. Henzinger. A really temporal logic. In *In Proceedings of the 30th Annual Symposium on Foundations of Computer Science*, pages 162–169. IEEE Computer Society Press, 1989.
- [5] R. Alur and T.A. Henzinger. Logics and models of real time: A survey. In J. W. de Bakker, C. Huizing, W. P. de Roever, and G. Rozenberg, editors, *Proceedings of the REX Workshop 1991, Real-Time: Theory in Practice*, pages 74–106. Mook, The Netherlands, Jun 1991. Springer Verlag, LNCS 600.
- [6] E.A. Emerson and E.M. Clarke. Using branching-time temporal logic to synthesis synchronization skeletons. *Science of Computer Programming*, 2(3):241–266, 1982.
- [7] E.M. Clarke, E.A. Emerson, and A.P. Sistla. Automatic verification of finite-state concurrent systems using temporal-logic specifications. *ACM Transactions on Programming Languages and Systems*, 8(2):244–263, 1986.
- [8] L.J. van Bokhoven, J.P.M. Voeten, and M.C.W. Geilen. Software synthesis for system level design using process execution trees. In *Proceedings 25th Euromicro Conference*, pages 463–467, Milan, Italy, 1999. IEEE Computer Society Press, Los Alamitos, California.
- [9] M.C.W. Geilen. *Formal Techniques for Verification of Complex Real-time Systems*. PhD thesis, Eindhoven University of Technology, The Netherlands, 2002.
- [10] M.C.W. Geilen and D.R. Dams. An on-the-fly tableau construction for a real-time temporal logic. volume 1926 of *Lecture Notes in Computer Science*, pages 276–290, Pune, India, September 2000. Springer.
- [11] M.C.W. Geilen, J.P.M. Voeten, P.H.A. van der Putten, L.J. van Bokhoven, and M.P.J. Stevens. Object-oriented modelling and specification using she. *Journal of Computer Languages, special issue for VFM'99*, April-October 2001.
- [12] V. Gupta, T.A. Henzinger, and R. Jagadeesan. Robust timed automata. In O. Maler, editor, *Hybrid and Real-Time Systems, Proceedings of International Workshop HART'97*, pages 331–345, Grenoble, France, 1997. Springer Verlag, LNCS 1201.
- [13] W.Damm and E.-R. Olderog, editors. *Formal Techniques in Real-Time and Fault-Tolerant Systems, 7th International Symposium, FTRTFT 2002, Co-sponsored by IFIP WG 2.2, Oldenburg, Germany, September 9-12, 2002, Proceedings*, volume 2469 of *Lecture Notes in Computer Science*. Springer, 2002.