Towards decidability of timed testing*

E. N. Bozhenkova

In the paper, we construct a formula that characterizes a timed event structure up to the timed must-preorder.

1. Introduction

An important component of every process theory is a notion of equivalence between processes. Typically, equivalences are used in the setting of specification and verification both to compare two distinct systems and to reduce the structure of a system. Over the past several years, a variety of equivalences have been proposed, and the relationship between them has been quite well-understood (see, for example, [9]).

Among the major equivalences are testing ones presented in [8]. Two processes are considered to be testing equivalent, if there is no test that can distinguish them. A test itself is usually a process applied to another process by computing them together in parallel. A particular computation is considered to be successful, if the test reaches a designated successful state, and the process passes the test if every computation is successful. This notion is intuitively appealing; it has led to a well-developed mathematical theory of processes that ties together the equivalences and preorders. However, no characterization of these equivalences has led to an algorithmic solution for finite-state processes. Therefore, testing decision procedures are based on reduction of testing to bisimulation [6]. These equivalences have been considered for formal system models without time delays [1, 6, 8, 10].

Recently, testing equivalences have been developed for models with time. One of the papers [13] devoted to this subject investigates different betting semantics of "must" win and "may" win, taken from the testing methodology, in the context of an event structure model with delayed actions. Papers [7] and [14] have treated timed testing for discrete and dense time transition models, respectively. The latter paper also tries to provide a testing decision procedure that uses the untimed bisimulation between deterministic graphs built from mutually refined timer region graphs that are a finite abstraction of the operational semantics of the model under consideration.

*Supported by the Russian Foundation for Basic Research under Grants 00-01-00898 and 01-01-06134, and by RAS Program "Projects of Young Scientists" under Grant 114.
In paper [4], a framework for testing preorders and equivalences in the setting of timed event structures has been developed. But as for the characterization and the decision procedure, it turns out that the results of [14] were not the case for some timed event structures. Since these timed event structures can be easily transformed to timed transition systems, it seems that the results of [14] are valid only for some subclass of timed transition systems. So, we try to give the alternative characterization of the timed testing relations. Moreover, we have found a subclass of structures in which we could reduce timed testing relations to the corresponding variants of symbolic bisimulations.

This paper is devoted to decidability of timed must-equivalences for timed event structures. We try to reduce this problem to the model-checking one. As a basic logic, we take the timed logic $L_v$. This logic has been defined in [12] and used for construction of a characteristic formula for a timed automaton up to the timed bisimilarity and, as a consequence, for reduction of the timed bisimilarity decidability problem to the model-checking one. It is known that the latter problem is decidable.

Here we construct a characteristic formula up to the timed must-preorder. We do it only for timed event structures without internal actions, but this approach can be used for those with internal actions, too.

The rest of the paper is organized as follows. In Section 2, we remind the basic notions concerned with timed event structures and timed testing. The timed modal logic $L_v$ is described in Section 3. In Section 4, we construct a formula which characterizes a timed event structure up to the timed must-preorder.

2. Timed event structures

In this section, we introduce a model of timed event structures that is a real time extension of Winkler’s model of prime event structures [15] by equipping events with time intervals.

We first recall a notion of an event structure. The main idea behind event structures is to view the distributed computations as action occurrences, called events, together with a notion of causal dependence between events (which are reasonably characterized via a partial order). Moreover, to model nondeterminism, there is a notion of conflicting (mutually incompatible) events. A labelling function determines which action corresponds to an event.

Let $Act$ be a finite set of visible actions and $\tau$ be an internal action. Then $Act_\tau = Act \cup \{\tau\}$.

**Definition 1.** A *(labelled) event structure over $Act_\tau$* is a 4-tuple $S=(E,\leq,\#,I)$, where
Towards decidability of timed testing

- $E$ is a countable set of events;
- $\leq \subseteq E \times E$ is a partial order (the \textit{causality relation}) satisfying the principle of finite causes: $\forall e \in E . \{ e' \in E \mid e' \leq e \}$ is finite;
- $\# \subseteq E \times E$ is a symmetric and irreflexive relation (the \textit{conflict relation}) satisfying the principle of conflict heredity: $\forall e, e', e'' \in E . e \neq e' \leq e'' \Rightarrow e \neq e''$;
- $l : E \to \text{Act}_r$ is a labelling function.

Let $C \subseteq E$. Then $C$ is left-closed iff $\forall e, e' \in E . e \in C \land e' \leq e \Rightarrow e' \in C$; $C$ is conflict-free iff $\forall e, e' \in C . \neg(e \neq e')$; $C$ is a configuration of $S$ iff $C$ is left-closed and conflict-free. Let $\text{Conf}(S)$ denote the set of all configurations of $S$. For $C \in \text{Conf}(S)$, we define the set of events enabled in $C$ $\text{En}(C) = \{ e \in E \mid C \cup \{ e \} \in \text{Conf}(S) \}$.

In the following, we will consider only finite event structures, i.e., the structures whose sets of events are finite.

Before introducing the concept of a timed event structure, we need to propose some auxiliary notations. Let $\mathbb{N}_0$ be the set of natural numbers with zero, $\mathbb{R}^+$ be the set of positive real numbers, and $\mathbb{R}_0^+$ be the set of nonnegative real numbers. For any $d \in \mathbb{R}_0^+$, $\{ d \}$ denotes its fractional part, $\lfloor d \rfloor$ and $\lceil d \rceil$ — its smallest and largest integer parts, respectively. Let us define the set $\text{Interv}(\mathbb{R}_0^+) = \{(d_1, d_2), (d_1, d_2), [d_1, d_2], [d_1, d_2] \subset \mathbb{R}_0^+ \mid d_1, d_2 \in \mathbb{N}_0 \}$.

We are now ready to introduce the concept of timed event structures.

\textbf{Definition 2.} A (labelled) timed event structure over $\text{Act}_r$ is a pair $TS = (S, D)$, where

- $S = (E, \leq, \#, l)$ is a (labelled) event structure over $\text{Act}_r$;
- $D : E \to \text{Interv}(\mathbb{R}_0^+)$ is a timing function such that $D(e)$ is a closed interval from $\text{Interv}(\mathbb{R}_0^+)$ for all $e \in E$ with $l(e) \in \text{Act}$.

In a graphic representation of a timed event structure, the corresponding action labels and time intervals are drawn close to events. If no confusion arises, we will often use action labels instead of the event identifiers to denote events. The $\prec$-relations are depicted by arcs (omitting those derivable by transitivity), and conflicts are depicted by “$\#$” (omitting those derivable by the conflict heredity). Following these conventions, a trivial example of a labelled timed event structure is shown in Figure 1.

Let $\mathcal{E}_r$ denote the set of all labelled timed event structures over $\text{Act}_r$. For convenience, we fix timed event structures $TS = (S = (E, \leq, \#, l), D), TS' = (S' = (E', \leq', \#, l'), D')$ from the class $\mathcal{E}_r$ and work with them further.
A state of \( TS \) is a pair \( M = (C, \delta) \), where \( C \in \text{Conf}(S) \) and \( \delta : E \rightarrow \mathbb{R}^+_0 \). The initial state of \( TS \) is \( M_{TS} = (C_0, \delta_0) = (\emptyset, 0) \). A state \( M = (C, \delta) \) is said to be terminated, if \( \text{En}(C) = \emptyset \). Let \( ST(TS) \) denote the set of all states of \( TS \).

A timed event structure progresses through a sequence of states in one of two ways given below.

Let \( M_1 = (C_1, \delta_1), M_2 = (C_2, \delta_2) \in ST(TS) \) such that \( M_1 \) is a non-terminated state. An event \( e \in \text{En}(C_1) \) may occur in \( M_1 \) (denoted \( M_1 \xrightarrow{e} ) \) if \( \delta_1(e) \in D(e) \) and \( \forall e' \in \text{En}(C_1) \exists d \in \mathbb{R}^+_0 . \ \delta_1(e') + d \in D(e) \). We write \( M_1 \xrightarrow{e} M_2 \) if \( M_1 \xrightarrow{e} \) and \( l(e) = a \). The occurrence of \( e \) in \( M_1 \) leads to \( M_2 \) (denoted \( M_1 \xrightarrow{e} M_2 \)), if \( M_1 \xrightarrow{e} \), \( C_2 = C_1 \cup \{e\} \) and
\[
\delta_2(e') = \begin{cases} 
0, & \text{if } e' \in \text{En}(C_2) \setminus \text{En}(C_1), \\
\delta_1(e'), & \text{otherwise.}
\end{cases}
\]

We write \( M_1 \xrightarrow{d} M_2 \), if \( M_1 \xrightarrow{e} M_2 \) and \( l(e) = a \).

A time \( d \in \mathbb{R}^+ \) may pass in \( M_1 \) (denoted \( M_1 \xrightarrow{d} ) \), if \( \forall e \in \text{En}(C_1) \exists d' \in \mathbb{R}^+_0 (d' \geq d) . \ \delta_1(e) + d' \in D(e) \). The passage \( d \) in \( M_1 \) leads to \( M_2 \) (denoted \( M_1 \xrightarrow{d} M_2 \)), if \( C_2 = C_1 \) and \( \delta_2(e) = \delta_1(e) + d \) for all \( e \in E \).

The weak leading relation \( \Rightarrow \) on states of \( TS \) is the largest relation defined by:
\[
\xrightarrow{s} \iff \xrightarrow{s}*, \quad \xrightarrow{d} \iff \xrightarrow{d}_s \xrightarrow{s}_r,
\]
where \( \xrightarrow{s} \) is the reflexive and transitive closure of \( \xrightarrow{s} \) and \( x \in \text{Act} \cup \mathbb{R}^+ \). We consider the relation \( \xrightarrow{d} \) as possessing the time continuity property: \( M \xrightarrow{d_1, d_2} \iff M \xrightarrow{d_3} \) for some \( d_1, d_2, d_3 \in \mathbb{R}^+ \).

From now on, we shall use the following notions and notations. Let \( \text{Act}(\mathbb{R}^+_0) = \{a(d) \mid a \in \text{Act} \land d \in \mathbb{R}^+_0\} \) be the set of timed actions of \( \text{Act} \) over \( \mathbb{R}^+_0 \). Then \( (\text{Act}(\mathbb{R}^+_0))^* \) is the set of finite timed words over \( \text{Act}(\mathbb{R}^+_0) \). The function \( \Delta : (\text{Act}(\mathbb{R}^+_0))^* \rightarrow \mathbb{R}^+_0 \) measuring the duration of a timed word is defined by: \( \Delta(\epsilon) = 0 \), \( \Delta(w \cdot a(d)) = \Delta(w) + d \). The domain for real-time languages is denoted by \( \text{Dom}(\text{Act}, \mathbb{R}^+_0) = \{\langle w, d \rangle \mid w \in (\text{Act}(\mathbb{R}^+_0))^*, d \in \mathbb{R}^+_0, d \geq \Delta(w)\} \). The weak leading relation \( \Rightarrow \) is extended to timed words from \( (\text{Act}(\mathbb{R}^+_0))^* \) and \( \text{Dom}(\text{Act}, \mathbb{R}^+_0) \) as follows. Let \( d \in \mathbb{R}^+_0 \), \( d' \in \mathbb{R}^+ \), \( a \in \text{Act} \) and \( w \in (\text{Act}(\mathbb{R}^+_0))^* \). Then
\[
\begin{align*}
\text{if } M \xrightarrow{a(0)} M', & \text{ then } M \xrightarrow{a(0)} M'; & \text{if } M \xrightarrow{d} M', & \text{ then } M \xrightarrow{d} M'; \\
\text{if } M \xrightarrow{w \cdot a(d)} M', & \text{ then } M \xrightarrow{w \cdot a(d)} M'; & \text{if } M \xrightarrow{w \cdot \Delta(w)} M', & \text{ then } M \xrightarrow{w \cdot \Delta(w)} M'; \\
\text{if } M \xrightarrow{(w, d')}, & \text{ then } M \xrightarrow{(w, d')} M', & \text{if } M \xrightarrow{(w, d')}, & \text{ then } M \xrightarrow{(w, d')} M'.
\end{align*}
\]
The set $L(TS) = \{ \langle w, d \rangle \in \text{Dom}(\text{Act}, \mathbb{R}_0^+) \mid M_{TS}^{(w,d)} \}$ is the language of $TS$. For instance, for the timed event structure $TS_1$ (see Figure 1) we have $L(TS_1) = \{ \langle e, d_1 \rangle, \langle e, 1 \rangle, \langle a(d_1), d_1 + d_2 \rangle, \langle a(1), 1 \rangle, \langle a(d_1)b(d_2), d_1 + d_2 \rangle \mid d_1 + d_2 < 1 \}$.

The timed testing relations may be defined in terms of the responses of timed event structures to a collection of tests. We shall, however, use an alternative characterization that relies on the following definitions. Let $M \in ST(TS)$ and $\langle w, d \rangle \in \text{Dom}(\text{Act}, \mathbb{R}_0^+)$. Then $S(M) = \{ x \in \text{Act}, \cup \mathbb{R}^+ \mid M \stackrel{x}{\rightarrow} \}$ and $\text{Acc}(TS, \langle w, d \rangle) = \{ S(M') \mid M_{TS}^{(w,d)} \rightarrow M', M' \not\rightarrow \} \text{ (timed acceptance set).}$ Let $N, N' \subset 2^{\text{Act} \cup \mathbb{R}^+}$. Then $N \subset N' \iff \forall S \in N \exists S' \in N'. \left[ (S' \mid _{\text{Act} \subseteq S} \mid _{\text{Act}}) \land (S \mid _{\mathbb{R}^+ = \emptyset} \Rightarrow S' \mid _{\mathbb{R}^+ = \emptyset}) \right]; N \equiv N' \iff N \subset N' \land N' \subset N$.

**Definition 3.**

- $TS \leq_{\text{must}} TS' \iff \forall \langle w, d \rangle \in \text{Dom}(\text{Act}, \mathbb{R}_0^+) \cdot \text{Acc}(TS', \langle w, d \rangle) \subset \text{Acc}(TS, \langle w, d \rangle)$;

- $TS \approx_{\text{must}} TS' \iff TS \leq_{\text{must}} TS'$ and $TS' \leq_{\text{must}} TS$.

An example of timed must-equivalent structures is shown in Figure 2(a). The timed event structures $TS_3$ and $TS'_3$ shown in Figure 2(b) are not timed must-equivalent. Let us consider the timed word $\langle w, d \rangle = \langle a(0.5), 1.5 \rangle \in L(TS_3) \cap L(TS'_3)$. We have $\text{Acc}(TS_3, \langle w, d \rangle) = \{ \{ b, c \} \cup (0, 1], \{ c \} \}, \text{ i.e., } \neg(\text{Acc}(TS'_3, \langle w, d \rangle) \subset \text{Acc}(TS_3, \langle w, d \rangle))$.

(a) $TS_2$

<table>
<thead>
<tr>
<th>[1, 1]</th>
<th>[1, 1]</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>$a$</td>
</tr>
<tr>
<td>$#$</td>
<td>$#$</td>
</tr>
<tr>
<td>$\tau$</td>
<td>$\tau$</td>
</tr>
<tr>
<td>[0, 1]</td>
<td>[0, 1]</td>
</tr>
</tbody>
</table>

$TS'_2$

<table>
<thead>
<tr>
<th>[1, 1]</th>
<th>[1, 1]</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>$a$</td>
</tr>
<tr>
<td>$#$</td>
<td>$#$</td>
</tr>
<tr>
<td>$\tau$</td>
<td>$\tau$</td>
</tr>
<tr>
<td>[0, 1]</td>
<td>[0, 1]</td>
</tr>
</tbody>
</table>

(b) $TS_3$

$[0, 1]a \quad \text{arrow} \quad b$ $[2, 3]$

$[0, 1]a \quad \# \quad c$ $[0, 2]$

$TS'_3$

$[0, 1]a \quad \text{arrow} \quad b$ $[2, 3]$

$[0, 1]a \quad \# \quad c$ $[0, 2]$

$[0, 1]a \quad \text{arrow} \quad c$ $[0, 1]$

Figure 2
3. Timed modal logic

In [12], a dense-timed logic $L_\nu$ was considered. Here we shall recall it and modify a satisfiability relation for timed event structures.

**Definition 4.** Let $K$ be a finite set of clocks, $Id$ be a set of identifiers and $k$ be an integer. The set of formulas of $L_\nu$ over $K$, $Id$ and $k$ is generated by the abstract syntax with $\phi$ and $\psi$ ranging over $L_\nu$:

$$\phi := \top | ff | \phi \land \psi | \phi \lor \psi | \exists \phi | \forall \phi | \langle a \rangle \phi | \langle x \rangle | x \text{ in } \phi | x + n \equiv y + m | x \equiv m | Z,$$

where $a \in Act$, $x, y \in K$, $n, m \in \{0, 1, \ldots, k\}$, $\equiv \in \{=, \leq, >, \geq\}$ and $Z \in Id$.

The meaning of the identifiers from $Id$ is specified by a declaration $D$ that assigns a formula of $L_\nu$ to each identifier. When $D$ is clear, we write $Z := \phi$ for $D(Z) = \phi$. The $K$ clocks are called formula clocks and a formula $\phi$ is said to be closed if every formula clock $x$ occurs in $\phi$ in the scope of an “$x$ in . . .” operator. Given a timed event structure $TS$, we interpret the formulas from $L_\nu$ over an extended state $(C, \delta u)$, where $(C, \delta)$ is a state of $TS$ and $u$ is a time assignment for $K$. Transitions between extended states are defined by: $(C, \delta u) \overset{e}{\rightarrow} (C, (\delta + e)(u + e))$ and $(C, \delta u) \overset{\delta}{\rightarrow} (C', \delta' u')$ iff $(C, \delta) \overset{\delta}{\rightarrow} (C', \delta')$ and $u = u'$. Formally, the satisfaction relation between extended states and formulas is defined as follows:

**Definition 5.** Let $TS$ be a timed event structure and $D$ be a declaration. The satisfaction relation $\models_D$ is the largest one that satisfies the following implications:

$$
\begin{align*}
(C, \delta u) \models_D \top & \Rightarrow true; \\
(C, \delta u) \models_D ff & \Rightarrow false; \\
(C, \delta u) \models_D \phi \land \psi & \Rightarrow (C, \delta u) \models_D \phi \text{ and } (C, \delta u) \models_D \psi; \\
(C, \delta u) \models_D \forall \phi & \Rightarrow \forall \phi \in R. (C, \delta + du + d) \models_D \phi; \\
(C, \delta u) \models_D \langle a \rangle \phi & \Rightarrow \exists (C', \delta') \in ST(TS) \cdot (C, \delta) \overset{\delta}{\rightarrow} (C', \delta') \\
& \quad \text{and } (C', \delta' u) \models_D \phi; \\
(C, \delta u) \models_D x + m \approx y + n & \Rightarrow u(x) + m \approx u(y) + n; \\
(C, \delta u) \models_D x \text{ in } \phi & \Rightarrow (C, \delta u') \models_D \phi, \text{ where } u' = [\{x\} \rightarrow 0] u; \\
(C, \delta u) \models_D Z & \Rightarrow (C, \delta u) \models_D D(Z).
\end{align*}
$$

Any relation that satisfies the above implications is called a satisfiability relation. We say that $TS$ satisfies a closed formula $\phi$ from $L_\nu$ and write $TS \models_D \phi$ when $(C_0, \delta_0 u) \models_D \phi$ for any $u$. Note that if $\phi$ is closed, then $(C, \delta u) \models_D \phi$ iff $(C, \delta u') \models_D \phi$ for any $u, u' \in \mathbb{R}_0^+K$.

\(^1\)For the complete definition, see [12].
4. Formula construction

Further we restrict our model to timed event structures labelled only over Act.

Since a timed event structure is defined over a dense time domain, the number of its states is infinite. In order to get a discrete representation of the state-space of a timed event structure, we use the concept of regions (equivalence classes of states) [2]. But we do not construct regions over states of ST(TS) for the following reasons.

One of the problems we meet when trying to develop an algorithm of decidability of timed testing [4] is existence of several regions which contain states reachable by the same timed word. So, we construct a region over states that unite all states of TS which we get by passing some time word. By doing so, we want to exclude nondeterminism when progressing in a timed event structure from state to state. For this purpose we define the notion of common states of TS.

The other problem is to synchronize actions being executed in two timed event structures. Here we decide it by including counters into regions of one timed event structure in order to restrict states of the second one for which a region formula has to be checked.

Some subset of ST(TS) is called a common state of TS, i.e., $\mu \subseteq ST(TS)$ is a common state of TS. We shall sometimes denote $\mu$ as $[C_1, \ldots, C_n, \delta_1, \ldots, \delta_n]$, where $(C_i, \delta_i) \in \mu$ $(1 \leq i \leq n)$ and $En(\mu) = \bigcup \{En(C) \mid C \in \mu\}$. The initial common state of TS is $\mu_0 = \{M_{TS}\}$. The relation $\rightarrow$ is modified on common states as follows: $\mu \rightarrow \mu' = \{(C', \delta') \mid \exists (C, \delta) \in \mu . (C, \delta) \rightarrow (C', \delta')\}$, where $z \in Act \cup R^*$. Let STC(TS) denote the set of all common states reachable from $\mu_0$. The leading relation on common states of STC(TS) is extended to timed words from $Dom(Act, R^n)$ just as on the states of ST(TS).

Then the notion of region is defined analogously to Alur’s one. Let $\mu = (C_1, \ldots, C_n, \delta_1, \ldots, \delta_n) \neq \mu' = (C'_1, \ldots, C'_n, \delta'_1, \ldots, \delta'_n)$. Then $\mu \approx \mu'$ iff there exists renaming $\pi(n) : l \rightarrow \pi(n)(l)$, where $l = 1, \ldots, n$, such that $(C_1, \ldots, C_n) = (C'_1, \ldots, C'_n)$ and

\[(i) \ \forall 1 \leq i \leq m . \ [\delta_1] \ldots [\delta_n(\bar{i})] = [\delta'_1(\pi(n)(1))] \ldots [\delta'_n(\pi(n)(n))(\bar{i})], \]

\[(ii) \ \forall 1 \leq i, j \leq m . \]

\[- \{\delta_1 \ldots \delta_n(i)\} \subseteq \{\delta_1 \ldots \delta_n(j)\} \iff \{\delta'_1(\pi(n)(1))] \ldots [\delta'_n(\pi(n)(n))(i)\} \leq \{\delta'_1(\pi(n)(1))] \ldots [\delta'_n(\pi(n)(n))(j)\}, \]

\[- \{\delta_1 \ldots \delta_n(i)\} = 0 \iff \{\delta'_1(\pi(n)(1))] \ldots [\delta'_n(\pi(n)(n))(i)\} = 0, \]
where \( \delta_1 \ldots \delta_n \) is the concatenation of vectors \( \delta_i \) \((1 \leq i \leq n)\) and \( m = \sum_{1 \leq i \leq n} |C_i| \).

A set \( R = [\mu] = \{ \mu' \mid \mu \simeq \mu' \} \) is called a region of \( TS \). We define \( R_0 = [\mu_0] \). Let \( R \) and \( R' \) be regions of \( TS \). Then the leading relation on regions is defined as follows: \( R \overset{a}{\longrightarrow} R' \) if \( \exists \mu \in R, \mu' \in R' : \mu \overset{a}{\longrightarrow} \mu' (a \in Act); \)
\( R \overset{d}{\longrightarrow} R' \) if \( \exists \mu \in R, \mu' \in R', \exists d \in \mathbb{R}^+ : \mu \overset{d}{\longrightarrow} \mu' \land \forall 0 < d' < d : \mu \overset{d'}{\longrightarrow} \mu' \in R \cup R' \).

The leading relation on regions is extended to timed words from \( Dom(Act, R_0^+) \) just as on the states of \( ST(TS) \).

We shall call a partition of \( STC(TS) \) into regions stable if the following holds: if \( R \overset{a}{\longrightarrow} R' \), then \( \forall \mu \in R : \mu \overset{a}{\longrightarrow} \mu' \) for some \( \mu' \in R' (a \in Act); \) if \( R \overset{d}{\longrightarrow} R' \), then \( \forall \mu \in R : \exists d' \in \mathbb{R}^+ : \mu \overset{d'}{\longrightarrow} \mu' \) for some \( \mu' \in R' \) and \( \mu \overset{d}{\longrightarrow} \mu' \in R \cup R' \) for all \( 0 < d' \leq d \). So, we can define the notion of region graph of \( TS \) \( RG(TS) = (V_{RG}, E_{RG}, l_{RG}) \). The set of vertices \( V_{RG} \) is a stable partition of \( STC(TS) \), the set of edges \( E_{RG} \) is the leading relation on regions of \( V_{RG} \), the labelling function \( l_{RG} : E_{RG} \rightarrow Act \cup \{ \chi \} \) is defined as: \( l((R, R')) = z \iff R \overset{z}{\longrightarrow} R' \).

For correctness of our formula construction we need to introduce the following notion.

**Definition 6.** Let \( \langle w, d \rangle \in L(TS) \) and \( RG(TS) = (V_{RG}, E_{RG}, l_{RG}) \). Let \( p = R_0 \ldots R \) be a path in \( RG(TS) \). Then \( \mu \in STC(TS) \) is reachable by \( \langle w, d \rangle \) consistent with \( p \) iff \( \mu \in R \) and either

- \( p = R_0 \) and \( \langle w, d \rangle = \langle e, 0 \rangle \),

or

- \( p = p' \overset{a}{\longrightarrow} R \) and there exists \( \mu' \in STC(TS) \) reachable by \( \langle w', d' \rangle \) consistent with \( p' \) and either

  - \( z = a \in Act, \mu' \overset{a}{\longrightarrow} \mu \) and \( \langle w, d \rangle = \langle w' a(d' - \Delta(w')), d' + d'' \rangle \) for some \( d'' \in R_0^+ \),

  or

  - \( z = \chi, \mu' \overset{d''}{\longrightarrow} \mu \) and \( \langle w, d \rangle = \langle w', d' + d'' \rangle \) for some \( d'' \in \mathbb{R}^+ \).

Note that \( \mu_0 \overset{\langle w, d \rangle}{\longrightarrow} \mu \iff \forall (C, \delta) \in \mu \ (C_0, \delta_0) \overset{\langle w, d \rangle}{\longrightarrow} (C, \delta) \). Moreover, for any \( \langle w, d \rangle \) there exists only one \( \mu \in STC(TS) \) such that \( \mu_0 \overset{\langle w, d \rangle}{\longrightarrow} \mu \). Consequently, \( R \) and path \( p \) from \( R_0 \) to \( R \) such that \( \mu \) is reachable by \( \langle w, d \rangle \) consistent with \( p \), are unique.

**Lemma 1.** Let \( \langle w, d \rangle \in L(TS) \) and \( \mu_0 \overset{\langle w, d \rangle}{\longrightarrow} \mu \). Then there exists only one path \( p \) in \( RG(TS) \) such that \( \mu \) is reachable by \( \langle w, d \rangle \) consistent with \( p \).
Lemma 2. Let \( R \in V_{RG} \). Then \( \forall \mu, \mu' \in R \ \forall (C, \delta) \in \mu \ \exists (C', \delta') \in \mu' \cdot C = C' \land S((C, \delta)) \cup_{Act} S((C', \delta')) \cup_{Act} S((C, \delta)) \mid R^+ = \emptyset \iff S((C', \delta')) \mid R^+ = \emptyset \).

Let \( RG(TS) \) be the region graph and \( X \) be a countable set of counters. Before we shall start to construct the formula, we need to add some additional information into common states and regions. Let all regions of \( RG(TS) \) get a unique number, then with each region \( R_i \) we shall associate its own counter \( x_{R_i} \). For simplicity, sometimes we shall denote \( x_{R_i} \) by \( x_i \). Moreover, with each region \( R \) we shall associate the additional set of counters \( RC(R) \), the region representative \( \mu_R = (C_1, \ldots, C_{n_R}, \delta_1, \ldots, \delta_{n_R}) \in R \) and the function \( \sigma_R : RC(R) \rightarrow 2^n \) which associates the set of configurations from \( \mu_R \) with each counter of \( RC(R) \). At first, we suppose \( RC(R_0) = \{ x_0 \} \) and take \( \mu_0 \) as a representative of \( R_0 \), \( \sigma_{R_0}(x_0) = \{ C_0 \} \). For others \( R \in RG(TS) \) we suppose \( RC(R) = \emptyset \) and take an arbitrary \( \mu \in R \) as its representative, \( \sigma_R \equiv \emptyset \). Then the leading relation on regions is modified so that we add \( x_R \) into \( RC(R) \), if after execution of some action we get \( \mu \in R \) and some event becomes enabled in \( C \in \mu \). Then the configuration \( C \) is associated with \( x_R \). Additionally, we delete from \( RC(R) \) the counters for which there are no configurations associated with them. More formally:

- \((R, RC(R)) \xrightarrow{a} (R', RC(R')) \ (a \in Act) \) iff \( R \xrightarrow{a} R' \) (suppose \( \mu_R \xrightarrow{a} \tilde{\mu} \) for some \( \tilde{\mu} \in R' \) ) and the set \( RC(R') \) is modified in two steps:

1. \( RC(R') = RC(R') \cup (R' \setminus OLD(R, a)) \), where \( OLD(R, a) = \{ x_i \mid \forall j \in \sigma_R(x_i) \cdot (C_j, \delta_j) \not\xrightarrow{a} \} \);
2. \( RC(R') = RC(R') \cup \{ x_R \} \) if \( \exists e \in En(\tilde{\mu}) \setminus En(\mu_R) \land \forall (C, \delta) \in \mu_R \forall e \in C \cup En(C) \delta(e) \neq 0 \)

and \( \sigma_{R'} \) is modified as follows:

1. for all \( x \in RC(R') \cap RC(R) \)

\[
\sigma_{R'}(x) = \sigma_R(x) \cup \{ j \mid \exists i \in \sigma_R(x) \exists (\tilde{C}_k, \tilde{\delta}_k) \in \tilde{\mu} \cdot (C_i, \delta_i) \xrightarrow{a} (\tilde{C}_k, \tilde{\delta}_k) \land \exists \pi(n_{R'}), (C'_j, \delta'_j) = (\tilde{C}_k(\pi(n_{R'})), \tilde{\delta}_k(\pi(n_{R'}))) \in \mu_{R'} \};
\]
2. if \( x_R \in RC(R') \) then \( \sigma_{R'}(x_R) = \{ i \mid (C_i, \delta_i) \in \mu_{R'} \land \exists e \in En(C_i) \delta_i(e) = 0 \} \);

- \((R, RC(R)) \xrightarrow{d} (R', RC(R')) \) iff \( R \xrightarrow{d} R' \) (suppose \( \mu_R \xrightarrow{d} \tilde{\mu} \) for some \( d \in R^+ \) and \( \tilde{\mu} \in R' \) ) and

\[
RC(R') = RC(R') \cup (R' \setminus OLD(R, \chi)) \), where \( OLD(R, \chi) = \{ x_i \mid \forall j \in \sigma_R(x_i)(\exists \tilde{C}, \tilde{\delta}) \in \tilde{\mu} \cdot (C_j, \delta_j) \xrightarrow{d} (\tilde{C}, \tilde{\delta}) \};
\]
− for all \( x \in \text{RC}(R') \cap \text{RC}(R) \)
\[
\sigma_R(x) = \sigma_R(x) \cup \{ j \mid \exists i \in \sigma_R(x) \exists (C_k, \delta_k) \in \bar{\mu} \cdot (C_i, \delta_i) \xrightarrow{d} (C_k, \delta_k) \land \exists \pi(n_{R'}) \cdot (C'_i, \delta'_i) = (C_{\pi(n_{R'})(k)}, \sigma_{\pi(n_{R'})(k)}) \in \mu_{R'} \},
\]

We also need a time assignment of our counters, so, into all common states \( \mu \in R \), we include \( RI_\mu = \text{RC}(R) \) and the time assignment \( \Delta_\mu : RI_\mu \to \mathbb{R}_+^+ \).

At first, suppose \( \Delta_\mu \equiv 0 \). We shall omit subscription \( \mu \) if it will be clear.

The leading relation on common states is modified as follows:

- \((\mu, RI, \Delta) \xrightarrow{d} (\mu', RI', \Delta') \) (\( d \in \mathbb{R}^+ \)) \iff \( \mu \xrightarrow{d} \mu' \) and \( \Delta' \mid_{RI} = \Delta \mid_{RI} + d; \)
- \((\mu, RI, \Delta) \xrightarrow{a} (\mu', RI', \Delta') \) (\( a \in \text{Act} \)) \iff \( \mu \xrightarrow{a} \mu' \).

It is clear that additional pieces of information have no influence on leading relations on common states and regions. In the following, we shall use a simple notation \( R \) and \( \mu \) instead of \((\bar{R}, \text{RC}(R))\) and \((\mu, \; RI, \; \Delta)\).

Now we can construct a formula for each region \( R = [\mu, R] \). In the formula, we shall use the following notations: \( R \xrightarrow{a} R_a \) and \( R \xrightarrow{d} R_X \) and write its optional parts in \( \langle \rangle \).

\[
F_R = \langle \langle \psi_R \rangle \rangle \quad \psi_R = \langle \langle \psi_R' \rangle \rangle \land \bigwedge_{\forall \overline{\alpha} \in \bar{\alpha}} \bigwedge_{\forall \bar{\beta} \in \bar{\beta}} \bigwedge_{\forall \bar{\gamma} \in \bar{\gamma}} \bigwedge_{\forall \bar{\delta} \in \bar{\delta}} [a]ff \land \bigwedge_{\forall \bar{\epsilon} \in \bar{\epsilon}} [a](\langle \langle X_{\bar{\epsilon}} \rangle \rangle) F_{R_{\bar{\epsilon}}} \land \text{ACC}(R);
\]

\[
\hat{F}_{R_a} = \begin{cases} 
F_R, & \text{if } \exists \mu \in R \exists d \in \mathbb{R}_+^+ \cdot \mu_R \xrightarrow{d} \mu, \\
\psi_R, & \text{otherwise}.
\end{cases}
\]

Here conditions \( \beta(R) \) that hold for the time assignment of states only from \( R \) are constructed in the following way:

1. \( \beta(R) = \emptyset; \)
2. for all \( x_i, x_j(x_i \neq x_j) \in \text{RC}(R) \) let \( \lfloor \Delta_{\mu_R}(x_i) \rfloor = a, \lfloor \Delta_{\mu_R}(x_j) \rfloor = b \), then

\[
\beta(R) = \beta(R) \land \begin{cases} 
x_i = a, & \text{if } \Delta_{\mu_R}(x_i) = \lfloor \Delta_{\mu_R}(x_i) \rfloor, \\
ar < x_i < a + 1, & \text{otherwise};
\end{cases}
\]

3. for all \( x_i, x_j(x_i \neq x_j) \in \text{RC}(R) \) let \( \lfloor \Delta_{\mu_R}(x_i) \rfloor = a, \lfloor \Delta_{\mu_R}(x_j) \rfloor = b \), then

\[
\beta(R) = \beta(R) \land \begin{cases} 
x_i + b = x_j + a, & \text{if } \{ \Delta_{\mu_R}(x_i) \} = \{ \Delta_{\mu_R}(x_j) \}, \\
x_i + b < x_j + a, & \text{if } \{ \Delta_{\mu_R}(x_i) \} < \{ \Delta_{\mu_R}(x_j) \}, \\
x_i + b > x_j + a, & \text{if } \{ \Delta_{\mu_R}(x_j) \} < \{ \Delta_{\mu_R}(x_i) \}.
\end{cases}
\]
The conditions $\beta^\geq(R)$ which mean that the values of counters are larger than appropriate time assignments in the states from $R$ are constructed as follows:

$$\beta^\geq(R) = \begin{cases} 
\beta(R) \lor \bigvee_{x_i \in RC(R)} x_i \geq [\Delta_{\mu_R}(x_i)], & \text{if all } (C, \delta) \in \mu_R \\
\bigvee_{x_i \in RC(R)} [\Delta_{\mu_R}(x_i)] - 0 \lor x_i > [\Delta_{\mu_R}(x_i)], & \text{otherwise}
\end{cases}$$

Below we give subformulas of $\psi_R$ and conditions of including them into $\psi_R$:

- $X_n = \{x \mid x \in RC(R_n) \setminus RC(R)\}$ is added if it is non-empty;
- $\psi^\geq(R) \Rightarrow F_{n_R}$ is added into $\psi_R$ if there is no region $R_X$;
- $ACC(R) = \bigvee_{(C, \delta) \in \mu} (\bigwedge_{a \in S((C, \delta))} (a) \#) \land \langle X(C, \delta) \land F_{R_n} \rangle \land \langle F_{n_R} \rangle);$
- $F_{n_R} = \bigwedge_{a \in \text{Act}} [a] f$ is added into $ACC(R)$ for all $(C, \delta) \in \mu_R$ such that $S((C, \delta)) \mid aR = \emptyset$;
- $X(C, \delta) = \begin{cases} 
\exists \beta(R_X) \Rightarrow (\bigwedge_{a \in S((C, \delta))} (a) \#), & \text{if } S(C, \delta) \mid aR \neq \emptyset, \\
\exists \beta^+(R_X) \Rightarrow (\bigwedge_{a \in \text{Act}} (a) \#), & \text{otherwise;}
\end{cases}$
- $X(C, \delta) \land F_{R_n}$ is added into $ACC(R)$ for all $(C, \delta) \in \mu_R$ such that $S((C, \delta)) \mid R^+ \neq \emptyset$.

Note that we use the symbol of implication ($\Rightarrow$) for simplicity. But it is easy to transform our formula into a correct formula from $L_\nu$, because negation of $\beta(R)$ and $\beta^\geq(R)$ can be expressed in $L_\nu$. Also, $X_n$ in $F$ means $(x_1 \in (x_2 \in \ldots (x_n \in F)))$ for $X_n = \{x_1, x_2, \ldots, x_n\}$. The formula $\psi_R$ contains three obligatory groups. The first group of conjunctions contains an $[a]$-formula for any action that can not be executed in $R$. The second group of conjunctions contains an $[a]$-formula for any action that can be executed in $R$. The third group is a group of disjunctions over all states in $\mu_R$ and each disjunction part contains conjunctions of $\langle a \rangle$-formulas for each action that can be executed in some state, and an optional part which characterizes the possibility of some amount of time to pass in this state. The optional group of $\psi_R$ is included into the formula, if there is no region $R_X$.

For a timed event structure $TS$, a characteristic formula is defined as $F_{TS} = x_0$ in $F_{R_0}$. We have the following theorem

**Theorem 1.** $TS \leq_{must} TS' \iff TS' \models_D F_{TS}$, where $D$ corresponds to the previous definition of $F_{R'}$ for each $R$ from $V_{RG(TS)}$.

To prove the theorem, we need

**Lemma 3.** Let $(C'_0, \delta'_0, u) \models_D F_{TS'}$, where $(C'_0, \delta'_0) = M_{TS'}$, $u \equiv 0$. For all $\langle w, d \rangle \in L(TS) \cap L(TS')$ and $(C'_0, \delta'_0) \models_D (C', \delta')$ it holds that $(C', \delta' \mid u') \models_D \psi_{R'}$ where $R$ and $u'$ are such that there exists $\mu$ which is reachable by $\langle w, d \rangle$ consistent with a path from $R_0$ to $R$, and $u' \mid R_{u'} = \Delta_{\mu}$. 


Proof (Theorem 1).

($\Leftarrow$) Take an arbitrary $\langle w, d \rangle \in L(TS')$ and $(C', \delta')$ such that $(C_0', \delta_0') \xrightarrow{\langle w, d \rangle} (C', \delta')$. According to Definition 3, we shall show that there exists $(C, \delta) \in ST(TS)$ such that $(C_0, \delta_0) \xrightarrow{\langle w, d \rangle} (C, \delta)$ and $S((C, \delta)) |_{\lambda \mu} \subseteq S((C', \delta')) |_{\lambda \mu}$, $S((C', \delta')) |_{R^+} = \emptyset \Rightarrow S((C, \delta)) |_{R^+} = \emptyset$.

Assume $\langle w, d \rangle \not\in L(TS)$. Let $\langle w, d \rangle = \langle a_1, \ldots, a_n, d_n \rangle$, $\sum_{1 \leq i \leq n+1} d_i$. We can find the maximal $0 \leq k \leq n$ and $0 \leq d' \leq d_{k+1}$ for which $\langle w, d \rangle = \langle a_1, \ldots, a_k, d_k, \sum_{1 \leq i \leq k} d_i + d' \rangle \in L(TS)$. Let $\mu_0 \xrightarrow{\langle w, d \rangle} \mu \in STC(TS)$ and $\langle C_0, \delta_0 \rangle \xrightarrow{\langle w, d \rangle} \langle C, \delta \rangle \xrightarrow{\langle w, d \rangle} \langle C', \delta' \rangle$ for some $(C', \delta') \in ST(TS')$ and $\langle w, d \rangle \in Dom(\lambda \mu, R^0_{\mu})$. By Lemma 1, there exists a path $\overline{p}$ in the region graph $RG(TS)$ such that $\overline{p}$ is reachable by $\langle w, d \rangle$ consistent with $\overline{p}$. Then, by Lemma 3, $\langle C', \delta' \rangle \xrightarrow{\langle w, d \rangle} \langle C, \delta \rangle \xrightarrow{\langle w, d \rangle} \langle C', \delta' \rangle$. By Lemma 1, there exists a path $\overline{p}$ in the region graph $RG(TS)$ such that $\overline{p}$ is reachable by $\langle w, d \rangle$ consistent with $\overline{p}$. Then, by Lemma 3, $\langle C', \delta' \rangle \xrightarrow{\langle w, d \rangle} \langle C, \delta \rangle \xrightarrow{\langle w, d \rangle} \langle C', \delta' \rangle$.

Let us consider $\psi_R$. If $d' < d_{k+1}$, then $\forall (C, \delta) \in R_\lambda |_{R_{\mu}} = \emptyset$, i.e., there is no region $R_\lambda$. So, by construction of the formula, $\psi_R$ includes $\forall \beta > \psi_R \Rightarrow F_{nil}$ as a conjunctive part. It is obvious that $\langle C', \delta' \rangle \not\xrightarrow{\langle w, d \rangle} \langle C, \delta \rangle \nexists \beta > \psi_R \Rightarrow F_{nil}$. We have got a contradiction with the assumption of Theorem 1. Similarly, we can get a contradiction if $d' = d_{k+1}$.

So, $\langle w, d \rangle \in L(TS)$.

Let $\mu_0 \xrightarrow{\langle w, d \rangle} \mu \in STC(TS)$. By Lemma 1 and Lemma 3, we can find $R$ and $u'$ such that $p$ is a path from $R_0$ to $R$, $u' |_{R_{\mu}} = \Delta_\mu$ and $(C', \delta', u') \xrightarrow{\langle w, d \rangle} \psi_R$. By construction of the formula $\psi_R$ and Lemma 2, there exists $(C, \delta) \in \mu$ for which $S((C, \delta)) |_{\lambda \mu} \subseteq S((C', \delta')) |_{\lambda \mu} \land S((C', \delta')) |_{R^+} \Rightarrow S((C, \delta)) |_{R^+}$.

($\Rightarrow$) Follows from construction of the formula $F_{TS}$.

\[ \square \]

5. Conclusion

In this paper, we have used as a formal model a timed generalization of Winskel’s prime event structures [4] which seems more appropriate for investigation of timed testing than the ones from [11, 5] because of the possibility to give notions of states and leading relation. This article is concentrated on constructing a characteristic formula. This formula allows us to decide the problem of recognizing timed must-equivalences by reducing it to the model-checking one. The formula obtained is only a first step towards the decision procedure for timed testing. The results may be extended onto a model with internal actions. Also, the way of construction of the characteristic formula may be applied to other timed testing equivalences.
Towards decidability of timed testing

References


