Basic Research in Computer Science

Timed Bisimulation and Open Maps

Mogens Nielsen
Thomas S. Hune

BRICS Report Series **RS-98-4**

ISSN 0909-0878 **February 1998**

See back inner page for a list of recent BRICS Report Series publications. Copies may be obtained by contacting:

BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK–8000 Aarhus C
Denmark
Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@brics.dk

BRICS publications are in general accessible through the World Wide Web and anonymous FTP through these URLs:

`http://www.brics.dk`
`ftp://ftp.brics.dk`
This document in subdirectory `RS/98/4/`

Timed Bisimulation and Open Maps

Thomas Hune and Mogens Nielsen

BRICS*Department of Computer Science, University of Aarhus, Denmark, {baris,mn}@brics.dk

Abstract

Formal models for real-time systems have been studied intensively over the past decade. Much of the theory of untimed systems have been lifted to real-time settings. One example is the notion of bisimulation applied to timed transition systems, which is studied here within the general categorical framework of open maps. We define a category of timed transition systems, and show how to characterize standard timed bisimulation in terms of spans of open maps with a natural choice of a path category. This allows us to apply general results from the theory of open maps, e.g. the existence of canonical models and characteristic logics. Also, we obtain here an alternative proof of decidability of bisimulation for finite transition systems, and illustrate the use of open maps in finite presentations of bisimulations

1 Introduction

When specifying and reasoning about a computing system, it is often sufficient to view its behavior from a classical point of view in terms of computations defined as sequences of atomic discrete actions of the system. For some systems, however, it is essential to include more detailed information. In the specification of a controller of a railway crossing it is not sufficient to state that the gate is closed when the train is at the crossing. It is equally important to specify timing constraints on the actions of gate closing and

*Basic Research in Computer Science,
Centre of the Danish National Research Foundation.

train crossing. Formal models for such so-called real-time systems have been studied intensively over the past decade, e.g. the timed automata [AD90], timed process algebras [Wan90], timed nets [LPY95], and timed Petri Nets [MBC+95].

Much of the theory of untimed systems has been lifted successfully to these models of real-time behavior of systems. As examples, many results from automata theory apply also to timed automata, [AD90, AD94, ACM97], and a number of timed versions of classical specification logics have been studied, [AH91, LLW95].

In this paper we focus on the classical notion of bisimulation [Mil89] which has already been introduced and studied for real-time models by many researchers, e.g. in [Wan90, AKLN95, NSY93, AM94]. A large part of the elegant theory of bisimulation for transition systems and reactive languages has been lifted to the real-time setting. As an example, bisimulation was shown decidable for finite timed transition systems by Čerāns [Čer92], and efficient algorithms checking for bisimilarity have been discovered [LLW95, WL97] and implemented in tools for automatic verification [KN94] .

Our aim here is to apply the general categorical framework of open maps [JNW96] to timed transition systems. The open map approach provides a general concept of bisimulation for any categorical model of computation, i.e. models consisting of objects (systems) and morphisms (to be thought of as simulations between two systems). The general definition is in terms of spans of so-called open maps, which are those morphisms which, roughly speaking, reflect as well as preserve behavior. Formally, the definition of open maps is parameterized not just on a categorical presentation of a model (i.e. on the choice of morphisms), but also on a notion of computation path and what it means to extend a computation path by another.

For the standard model of transition systems, computation paths are naturally chosen as sequences of consecutive transitions, formally picked out by a morphisms from strings of actions, extended by standard composition of strings. With this choice, it was shown in [JNW96] that the open map bisimulation simply specializes to Milner's notion of bisimulation. However, many other behavioral equivalences are captured by the open morphism approach, e.g. Hoare's trace equivalence and Milner's weak bisimulation, both of which may be obtained by slightly changing the notion of path extension from the one indicated above [CN96]. Also, the open morphism approach has been applied successfully to different categories of models, e.g. probabilistic [CN96], higher-order models [CFW98], and models with independence [JNW96].

Rather than having bisimulations defined in terms of two parameters, a model and a path category, it was suggested in [JNW96] to study presheaves as models derived directly from path categories. Intuitively, a presheaf represents the effect of gluing together a set of computation paths to form a nondeterministic computation, and hence can be looked upon as labelled transition systems, in which the labels are morphisms of path extension. Following [WN96] this yields logical and game-theoretic characterizations of open morphisms and their bisimulations on presheaves. Furthermore, models and their notion of bisimulation can be understood in a uniform way via their representation as presheaves, and via this representation, the characterizations can be specialized to concrete models. The characteristic logics take the form of Hennessy-Milner like modal logics, with modalities indexed by path morphisms (path extensions, future modalities) and their inverses (path projections, past modalities).

Here we define a category of timed transition systems, where the morphisms are to be thought of as simulations, with computation paths which are equivalent to the standard notion of runs of timed words. We show the derived notion of bisimulation in terms of open maps to coincide with the standard timed bisimulation from e.g. [Čer92]. Hence, we may apply the general results from [JNW96], e.g. obtaining canonical models and characteristic games and logics.

Furthermore, we show within the framework of open maps that bisimilarity is decidable for finite timed transition systems. As for many existing results for timed models, including results concerning verification of real-time systems, our proof relies heavily on the idea behind the regional construction of [AD90, AD94], which essentially provides a finite description of the uncountable behavior of a finite real-time system.

One of the main advantages of Milners notion of bisimulation for untimed transition systems, is the fact that for two transition systems, the property of being bisimilar may be expressed in terms of presenting an explicit bisimulation between the two systems, i.e. a relation on the states of the two systems. Unfortunately, this property does not generalize to the setting of timed transition systems, where bisimulations are defined in terms of the uncountable unfolded version of given timed transition systems, and where the decision procedures from e.g. [Čer92] produce relations over nontrivial regional constructions. Here, we obtain as a corollary, a way of presenting bisimilarity between two finite timed transition systems in terms of a span with a finite vertex.

In Section 2 we define formally our category of timed transition systems and computation paths, and the set-up is shown to have a number of useful properties following the approach of [JNW96]. Next, in Section 3 the resulting notion of bisimulation is studied, and it is shown to coincide with the standard notion of timed bisimulation. A new proof of the decidability of timed bisimulation is provided in Section 4, and the use of open maps to express bisimulations is illustrated. We briefly address the issue of robustness of our approach in Section 5 by extending our results to models with state time-invariants. Section 6 contains some conclusions and ideas for future work.

This paper is an extended version of [HN98] appearing in the proceedings of MFCS'98.

2 A Category of Timed Transition Systems

In the following we define the categorical set-up for our use of the open map approach.

The objects of our model category will be timed transition systems, i.e. timed automata in the sense of Alur and Dill [AD94] without accepting states and acceptance conditions (called timed transition tables in [AD94]).

Definition 1 (Timed Transition Systems) *A timed transition system is a quintuple* $(S, \Sigma, s^{in}, X, T)$ *where*

- S *is a set of states and* s^{in} *is the initial state.*
- Σ *is a finite alphabet of actions.*
- X *is a set of clock variables.*
- T *is the set of transitions such that* $T \subseteq S \times \Sigma \times \Delta \times 2^X \times S$ *where* Δ *is a clock constraint generated by the grammar* $\Delta ::= c \sharp x \,|\, x + c \sharp y \,|\, \Delta \wedge \Delta$ *in which* $\sharp \in \{\leq, <, \geq, >\}$, c *is a real valued constant and* x, y *are clock variables. A transition* $(s, \sigma, \delta, \lambda, s')$ *is written* $s \xrightarrow[\delta,\lambda]{\sigma} s'$.

Timed transition systems are to be thought of as generalizations of standard transition systems, having runs over timed words as obvious generalizations of words over an alphabet.

Definition 2 (Timed Words) *A timed word over an alphabet Σ is a finite sequence of pairs $\alpha = (\sigma_1, \tau_1)(\sigma_2, \tau_2)(\sigma_3, \tau_3) \cdots (\sigma_n, \tau_n)$, where for all $1 \leq i \leq n$, $\sigma_i \in \Sigma, \tau_i \in \mathbf{R}_+$ and furthermore $\tau_i < \tau_{i+1}$.*

A pair (σ, τ) represents an occurrence of action σ at time τ relative to the starting time (0) of the execution.

Example 1 *The timed transition system in Figure 1 has two clocks x and y, and three actions* a,b,c. *The state s_0 is the initial state.*

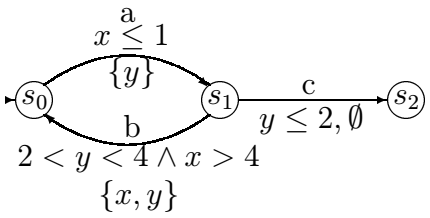


Figure 1: A timed transition system .

Before introducing formally computations of timed transition systems, we need the notion of a clock evaluation.

Definition 3 (Clock Evaluation) *A clock evaluation ν is a function $\nu : X \to \mathbf{R}_+$ which assigns times to the clock variables of a system. We define $(\nu + c)(x) := \nu(x) + c$ for all clock variables x. If λ is a set of clock variables then $\nu[\lambda \mapsto 0](x) := 0$ if $x \in \lambda$, and $\nu(x)$ otherwise.*

A constraint δ is satisfied by clock evaluation ν iff the expression $\delta[\nu(x)/x]$[1] evaluates to true. A constraint δ defines a subset of $\mathbf{R}^n$ where n is the number of clocks in X. We will speak of this subset as the meaning of δ and write it $[\![\delta]\!]_X$. As an example the meaning of the constraint on the transition from s_0 to s_1 in Figure 1 is the hatched area in Figure 2. A clock evaluation defines a point in $\mathbf{R}^n$ which we shall denote by $[\![\nu]\!]_X$, so the constraint δ is satisfied for the clock evaluation ν if and only if $[\![\nu]\!]_X \in [\![\delta]\!]_X$.

Definition 4 *Let $\mathcal{T}$ be a timed transition system. A configuration is a pair $\langle s, \nu \rangle$, where s is a state and ν is a clock evaluation. A run of $\mathcal{T}$ is a sequence $\langle s_0, \nu_0 \rangle \xrightarrow{\sigma_1}_{\tau_1} \langle s_1, \nu_1 \rangle \xrightarrow{\sigma_2}_{\tau_2} \cdots \xrightarrow{\sigma_n}_{\tau_n} \langle s_n, \nu_n \rangle$ such that for all $i > 0$ there is a transition $s_{i-1} \xrightarrow{\sigma_i}_{\delta_i, \lambda_i} s_i$ such that $[\![\nu_{i-1} + (\tau_i - \tau_{i-1})]\!]_X \in [\![\delta_i]\!]_X$ and*

[1] $\delta[y/x]$ is syntactic substitution of y for x in δ.

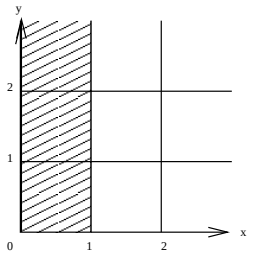


Figure 2: Interpretation of constraint $[\![x \leq 1]\!]_{\{x,y\}}$.

$\nu_i = (\nu_{i-1} + (\tau_i - \tau_{i-1}))[\lambda_i \mapsto 0]$. *The state* s_0 *is the initial state of* $\mathcal{T}$, ν_0 *is the constant 0 function, and* τ_0 *is defined to be 0. A run as above is said to generate the timed word* $(\sigma_1, \tau_1)\,(\sigma_2, \tau_2)\,(\sigma_3, \tau_3) \cdots (\sigma_n, \tau_n)$.

Example 2 *A run in the timed transition system in Figure 1 generating the timed word* $(a, 0.9)(c, 2.3)$ *is*

$$\langle s_0, [0,0]\rangle \xrightarrow[0.9]{a} \langle s_1, [0.9,0]\rangle \xrightarrow[2.3]{c} \langle s_2, [2.3,1.4]\rangle$$

where $[2.3, 1.4]$ *denotes the clock assignment assigning* 2.3 *to the clock variable* x *and* 1.4 *to* y.

Another run in the timed transition system could be

$$\langle s_0, [0,0]\rangle \xrightarrow[0.7]{a} \langle s_1, [0.7,0]\rangle \xrightarrow[4.2]{b} \langle s_0, [0,0]\rangle \xrightarrow[4.4]{a} \langle s_1, [0.2,0]\rangle \xrightarrow[8.3]{b} \langle s_0, [0,0]\rangle$$

which generates the timed word $(a, 0.7)(b, 4.2)(a, 4.4)(a, 8.3)$.

The morphisms of our model category will be simulation morphisms following the approach of [JNW96]. This leads to the following definition of a morphism, consisting of two functions, one mapping states of the simulated system to simulating states of the other, and one mapping clocks of the simulating system to simulated clocks of the other.

Definition 5 *A morphism* (m, η) *between timed transition systems* $\mathcal{T}_1$ *and* $\mathcal{T}_2$ *consists of two components; a map* $m : S_1 \to S_2$ *between the states and a map* $\eta : X_2 \to X_1$ *between the clocks. These maps must satisfy that* $m(s_1^{in}) = s_2^{in}$ *and whenever there is a transition in* $\mathcal{T}_1$ *of the form* $s_1 \xrightarrow[\delta_1, \lambda_1]{\sigma} s_1'$ *then there is a transition* $m(s_1) \xrightarrow[\delta_2, \lambda_2]{\sigma} m(s_1')$ *in* $\mathcal{T}_2$ *satisfying the following two constraints:*

- $\lambda_2 = \eta^{-1}(\lambda_1)$ *where* $\eta^{-1}(\lambda_1) = \{x \in X_2 \mid \eta(x) \in \lambda_1\}$
- $[\![\delta_1]\!]_{X_1} \subseteq [\![\delta_2[\eta(x)/x]]\!]_{X_1}$

Example 3 *Consider the map m from the states of the timed transition system in Figure 3 to the states of the one in Figure 1, mapping states with index i to s_i, paired with the map η sending the clock variable* x *to* z *and* y *to* u. *We leave it to the reader to check to check that m, η constitute a morphism .*

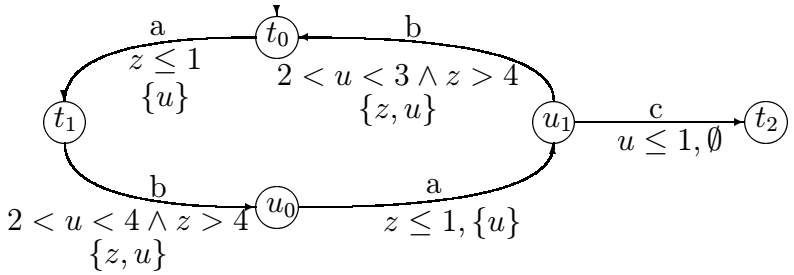


Figure 3: A timed transition system.

Definition 6 *For a function $\eta : X' \to X$ and a clock evaluation $\nu : X \to \mathbf{R}_+$ we define $\eta^{-1}(\nu) : X' \to \mathbf{R}_+$, the inverse image of ν under η, as*

$$\eta^{-1}(\nu)(x) := \nu(\eta(x))$$

Theorem 1 *Given two timed transition systems $\mathcal{T}$ and $\mathcal{T}'$ and a morphism (m, η) from $\mathcal{T}$ to $\mathcal{T}'$. If $\langle s_0, \nu_0\rangle \xrightarrow[\tau_1]{\sigma_1} \langle s_1, \nu_1\rangle \xrightarrow[\tau_2]{\sigma_2} \cdots \xrightarrow[\tau_n]{\sigma_n} \langle s_n, \nu_n\rangle$ is a run of $\mathcal{T}$ generating the timed word $(\sigma_1, \tau_1)(\sigma_2, \tau_2)(\sigma_3, \tau_3)\cdots(\sigma_n, \tau_n)$, then $\langle m(s_0), \eta^{-1}(\nu_0)\rangle \xrightarrow[\tau_1]{\sigma_1} \langle m(s_1), \eta^{-1}(\nu_1)\rangle \xrightarrow[\tau_2]{\sigma_2} \cdots \xrightarrow[\tau_n]{\sigma_n} \langle m(s_n), \eta^{-1}(\nu_n)\rangle$ is a run of $\mathcal{T}'$ generating the same timed word.*

Proof We will prove this by induction on the length of the run.

As base case, we have the empty run with just one configuration. Since the initial state of $\mathcal{T}$ is mapped to the initial state of $\mathcal{T}'$ and all clock values initially are set to 0, we also have $\forall x' \in X' : \eta^{-1}(\nu_0)(x') = 0$ which is the initial clock evaluation for a run in $\mathcal{T}'$.

For the induction step, assume $\mathcal{T}$ is in the configuration $\langle s_i, \nu_i\rangle$, $\mathcal{T}'$ is in the configuration $\langle m(s_i), \eta^{-1}(\nu_i)\rangle$, and $\mathcal{T}$ can extend its run by

$$\langle s_i, \nu_i\rangle \xrightarrow[\tau_{i+1}]{\sigma_{i+1}} \langle s_{i+1}, \nu_{i+1}\rangle$$

extending the generated timed word with the element $(\sigma_{i+1}, \tau_{i+1})$.

The extension uses some transition

$$s_i \xrightarrow[\delta_{i+1},\lambda_{i+1}]{\sigma_{i+1}} s_{i+1}$$

in $\mathcal{T}$ satisfying $[\![\nu_i+(\tau_{i+1}-\tau_i)]\!]_X \in [\![\delta_{i+1}]\!]_X$. From the definition of a morphism we must have some transition

$$m(s_i) \xrightarrow[\delta'_{i+1},\lambda'_{i+1}]{\sigma_{i+1}} m(s_{i+1})$$

in $\mathcal{T}'$ such that $\lambda'_{i+1} = \eta^{-1}(\lambda_{i+1})$ and $[\![\delta_{i+1}]\!]_X \subseteq [\![\delta'_{i+1}[\eta(x)/x]]\!]_X$. From the latter property we get that $[\![\eta^{-1}(\nu_i)+(\tau_{i+1}-\tau_i)]\!]_{X'} \in [\![\delta'_{i+1}]\!]_{X'}$ so the transition can be used to extend the run in $\mathcal{T}'$, obtaining

$$(m(s_i), \eta^{-1}(\nu_i)) \xrightarrow[\tau_{i+1}]{\sigma_{i+1}} (m(s_{i+1}), \nu'_{i+1})$$

where

$$\begin{aligned}
\nu'_{i+1} &= (\eta^{-1}(\nu_i) + (\tau_{i+1} - \tau_i))[\lambda'_{i+1} \mapsto 0] \\
&= (\eta^{-1}(\nu_i) + (\tau_{i+1} - \tau_i))[\eta^{-1}(\lambda_{i+1}) \mapsto 0] \\
&= (\eta^{-1}(\nu_i + (\tau_{i+1} - \tau_i)))[\eta^{-1}(\lambda_{i+1}) \mapsto 0] \\
&= \eta^{-1}((\nu_i + (\tau_{i+1} - \tau_i))[\lambda_{i+1} \mapsto 0]) \\
&= \eta^{-1}(\nu_{i+1})
\end{aligned}$$

□

Example 4 *Using the morphism from Example 3 the run*

$$\langle t_0, [0,0]\rangle \xrightarrow[0.7]{a} \langle t_1, [0.7,0]\rangle \xrightarrow[4.2]{b} \langle t_2, [0,0]\rangle \xrightarrow[4.4]{a} \langle t_3, [0.2,0]\rangle \xrightarrow[8.3]{b} \langle t_0, [0,0]\rangle$$

in the timed transition system in Figure 3 is simulated by the second run in Example 2. Here $[0.7, 0]$ *is notation for* ν *assigning the value* 0.7 *to the clock* z *and the value* 0 *to* u.

So, in the formal sense of Theorem 1 we have shown that the morphisms from Definition 5 do represent a notion of simulation. Our category of timed transition systems is defined as follows.

Definition 7 *The category* CTTS_Σ *has timed transition systems with alphabet* Σ *as objects, and the morphisms from Definition 5 as arrows. For morphisms* $\mathcal{T} \xrightarrow{(m,\eta)} \mathcal{T}'$ *and* $\mathcal{T}' \xrightarrow{(m',\eta')} \mathcal{T}''$ *composition is defined as* $(m',\eta') \circ (m,\eta) := (m' \circ m, \eta \circ \eta')$*. The identity morphism is the morphism where both* m *and* η *are the identity function.*

Proposition 1 CTTS_Σ *is a category.*

Proof The only non-trivial part of the proof is to see that composition is well-defined. Assume we have morphisms $\mathcal{T} \xrightarrow{(m,\eta)} \mathcal{T}'$ and $\mathcal{T}' \xrightarrow{(m',\eta')} \mathcal{T}''$. A transition $s_1 \xrightarrow[\delta,\lambda]{\sigma} s_2$ in $\mathcal{T}$ implies the existence of a transition $m(s_1) \xrightarrow[\delta',\lambda']{\sigma} m(s_2)$ in $\mathcal{T}'$ where $\lambda' = \eta^{-1}(\lambda)$ and $[\![\delta]\!]_X \subseteq [\![\delta'[\eta(x)/x]]\!]_X$. This transition implies the existence of a transition $m'(m(s_1)) \xrightarrow[\delta'',\lambda'']{\sigma} m'(m(s_2))$ in $\mathcal{T}''$ where $\lambda'' = \eta'^{-1}(\lambda') = \eta'^{-1}(\eta^{-1}(\lambda))$ and $[\![\delta']\!]_X \subseteq [\![\delta''[\eta'(x)/x]]\!]_X$. Combining these facts we get $[\![\delta]\!]_X \subseteq [\![\delta''[(\eta \circ \eta')(x)/x]]\!]_X$ from which we conclude that composition is well-defined.

□

CTTS_Σ has a number of useful properties. For our purpose here we only need the following.

Theorem 2 CTTS_Σ *has (binary) products.*

Proof Given two timed transition systems $\mathcal{T}_1 = (S_1, \Sigma, s_1^{in}, X_1, T_1)$ and $\mathcal{T}_2 = (S_2, \Sigma, s_2^{in}, X_2, T_2)$, we define the product of the two systems as $\mathcal{T}_1 \times \mathcal{T}_2 = (S_1 \times S_2, \Sigma, (s_1^{in}, s_2^{in}), X_1 \uplus X_2, \mathcal{T})$, where $X_1 \uplus X_2$ denotes the disjoint union of X_1 and X_2, and the set of transitions $\mathcal{T}$ consists of all transitions of the form $(s_1, s_2) \xrightarrow[\delta_1 \wedge \delta_2, \lambda_1 \cup \lambda_2]{\sigma} (s_1', s_2')$ such that $s_i \xrightarrow[\delta_i,\lambda_i]{\sigma} s_i'$ belongs to $\mathcal{T}_i$ for $i = 1, 2$.

The projections $(m_i, \eta_i) : \mathcal{T}_1 \times \mathcal{T}_2 \to \mathcal{T}_i$ for $i = 1, 2$ are defined as expected, with m_i as the projection on states and η_i is the embedding of X_i into $X_1 \uplus X_2$. It follows easily that this defines products in CTTS_Σ.

□

Theorem 3 CTTS_Σ *has pullbacks.*

Proof Given two morphisms $(m_1, \eta_1) : \mathcal{T}_1 \to \mathcal{T}$ and $(m_2, \eta_2) : \mathcal{T}_2 \to \mathcal{T}$, we construct $\mathcal{T}_1 \times_{\mathcal{T}} \mathcal{T}_2$ and two morphisms $(m_i', \eta_i') : \mathcal{T}_1 \times_{\mathcal{T}} \mathcal{T}_2 \to \mathcal{T}_i$ such that

$$(m_1, \eta_1) \circ (m_1', \eta_1') = (m_2, \eta_2) \circ (m_2', \eta_2') \tag{1}$$

The construction of m_i' and the states of $\mathcal{T}_1 \times_{\mathcal{T}} \mathcal{T}_2$ is based on pullbacks in the category of sets with functions. Similarly the construction of η_i' and the clocks of $\mathcal{T}_1 \times_{\mathcal{T}} \mathcal{T}_2$ is based on pushouts in the category of sets with functions, i.e. the clocks of $\mathcal{T}_1 \times_{\mathcal{T}} \mathcal{T}_2$ are the equivalence classes of the equivalence relation $\mathcal{R}$ over $X_1 \uplus X_2$ generated by $\mathcal{R}_0$ where

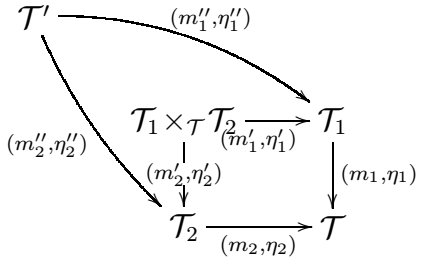
$$\mathcal{R}_0 = \{(x_1, x_2) \mid \exists x \in X. \eta_1(x) = x_1 \text{ and } \eta_2(x) = x_2\},$$

and η_i' sends a clock variable of $\mathcal{T}_i$ to the equivalence class to which it belongs. More specifically we define $\mathcal{T}_1 \times_{\mathcal{T}} \mathcal{T}_2$ as follows.

- $\mathrm{S}\times_{\mathcal{T}} : \{(s_1, s_2) \in S_1 \times S_2 \mid m_1(s_1) = m_2(s_2)\}$
- $\mathrm{s^{in}}\times_{\mathcal{T}} : (s_1^{in}, s_2^{in})$
- $\mathrm{X}\times_{\mathcal{T}}$: the equivalence classes of $\mathcal{R}$ defined above
- $\mathrm{T}\times_{\mathcal{T}} : (s_1, s_2) \xrightarrow[\delta_1[\eta_1'(x)/x] \wedge \delta_2[\eta_2'(x)/x], \eta_1'(\lambda_1) \cup \eta_2'(\lambda_2)]{\sigma} (s_1', s_2')$, whenever $s_i \xrightarrow[\delta_i, \lambda_i]{\sigma} s_i'$ and $(s_1, s_2), (s_1', s_2')$ belongs to $\mathrm{S}\times_{\mathcal{T}}$.

With $m_i'(s_1, s_2) = s_i$ we leave it for the reader to check that (m_i', η_i') is indeed a morphism, and it follows immediately from the underlying conditions from the category of sets with functions that the required commutativity of (1) is satisfied.

Now consider $\mathcal{T}'$ with morphisms $(m_i'', \eta_i'') : \mathcal{T}' \to \mathcal{T}_i$ for $i = 1, 2$, such that the following diagram commutes.



The required morphism (m, η) from $\mathcal{T}'$ to $\mathcal{T}_1 \times_{\mathcal{T}} \mathcal{T}_2$ is defined as expected, i.e. $m(s') = (m_1''(s'), m_2''(s'))$ and $\eta(x) = \eta_1''(x) \cup \eta_2''(x)$. We leave it for the reader

to check that (m, η) indeed is a morphism. Finally, from the underlying constructions in the category of sets with functions we get that the required commutativities $(m_i'', \eta_i'') = (m_i', \eta_i') \circ (m, \eta)$ hold for $i = 1, 2$.

□

2.1 A Path Category

Following the standards of timed transition systems and [JNW96], we would like to choose timed words over Σ with word extension as our category of computation paths. However, it is not immediately clear how to see formally this choice as a subcategory of CTTS_Σ, as required in the approach of [JNW96].

Definition 8 *Given a timed word $\alpha = (\sigma_1, \tau_1)\,(\sigma_2, \tau_2)\,(\sigma_3, \tau_3) \cdots (\sigma_n, \tau_n)$, we define a timed transition system $\mathcal{T}_\alpha$: $0 \xrightarrow[\delta_1, \lambda_1]{\sigma_1} 1 \xrightarrow[\delta_2, \lambda_2]{\sigma_2} \cdots \xrightarrow[\delta_n, \lambda_n]{\sigma_n} n$ as follows. The states are the integers $0..n$, with 0 as the initial state, and the set of clock variables, X, consists of the 2^n subsets of states $\{1, 2, \ldots, n\}$. We define λ_i and δ_i as*

$$\lambda_i = \{x |\ i \in x\} \text{ and } \delta_i = \bigwedge_{x \in X} (x = \tau_i - \tau_{I(i,x)})$$

where $I(i, x) := \max\{k \in x \cup \{0\} \mid k < i\}$, and $\tau_0 := 0$. The index returned by $I(i, x)$ is the index of the last state at which x was reset. We write $\mathcal{T}_\alpha$ for the transition system in CTTS_Σ representing α.

The only purpose of this seemingly ad hoc construction is that it allows us to represent the category of timed words with extension inside CTTS_Σ, and to identify runs of α in $\mathcal{T}$ with morphisms from $\mathcal{T}_\alpha$ to $\mathcal{T}$, as expressed formally in the following two results.

Proposition 2 *The construction of $\mathcal{T}_\alpha$ from α above, extends to a full and faithful functor from the category of timed words (as objects) and word extension (as morphisms) into CTTS_Σ*

Proof The main observation is that for all timed words α, α', there is at most one morphism between $\mathcal{T}_\alpha$ and $\mathcal{T}_{\alpha'}$.

□

Theorem 4 *Given a timed transition system $\mathcal{T}$ and a timed word $\alpha = (\sigma_1, \tau_1)(\sigma_2, \tau_2)\ldots(\sigma_n, \tau_n)$. For each run of α in $\mathcal{T}$,*

$$\langle s_0, \nu_0\rangle \xrightarrow[\tau_1]{\sigma_1} \langle s_1, \nu_1\rangle \xrightarrow[\tau_2]{\sigma_2} \ldots \xrightarrow[\tau_n]{\sigma_n} \langle s_n, \nu_n\rangle \tag{2}$$

we may associate a morphism $(m, \eta) : \mathcal{T}_\alpha \to \mathcal{T}$ where:

$m(i) = s_i$

$\eta(x) = \{i \mid 1 \leq i \leq n \text{ and } \nu_i(x) = 0\}$

Furthermore, this association is a bijection between the runs of α in $\mathcal{T}$ and the morphisms $\mathcal{T}_\alpha \xrightarrow{(m,\eta)} \mathcal{T}$.

Proof It follows from the definition of runs and the definition of $\mathcal{T}_\alpha$ that (m, η) as defined is indeed a morphism.

Now, let (m, η) be a morphism from $\mathcal{T}_\alpha$ to $\mathcal{T}$. With (m, η) we associate the run of the form (2) where

$s_i = m(i)$

$$\nu_i(x) = \begin{cases} 0 & \text{if } i = 0 \text{ or } i \in \eta(x) \\ \nu_{i-1}(x) + (\tau_i - \tau_{i-1}) & \text{otherwise} \end{cases}$$

Again, it follows from the definition of morphisms that this indeed defines a run of α in $\mathcal{T}$.

It is easily shown that the correspondence given above is one to one.

□

3 Timed Bisimulation

Given our categories of timed transition systems and paths, we can now apply the general framework from [JNW96], defining notions of open maps and bisimulation.

Definition 9 (Open Map [JNW96]) *A morphism $\mathcal{T} \xrightarrow{(m,\eta)} \mathcal{T}'$ in CTTS_Σ is $\mathcal{TW}$-open iff for all timed words α and α', and morphisms such that the following diagram commutes:*

$$\begin{array}{ccc} \mathcal{T}_\alpha & \xrightarrow{(p,\eta_p)} & \mathcal{T} \\ {\scriptstyle (f,\eta_f)}\downarrow & & \downarrow{\scriptstyle (m,\eta)} \\ \mathcal{T}_{\alpha'} & \xrightarrow{(q,\eta_q)} & \mathcal{T}' \end{array}$$

there exists a morphism $(p', \eta_{p'}) : \mathcal{T}_{\alpha'} \to \mathcal{T}$ *such that the in the diagram*

$$\begin{array}{ccc} \mathcal{T}_\alpha & \xrightarrow{(p,\eta_p)} & \mathcal{T} \\ {\scriptstyle (f,\eta_f)}\downarrow & \nearrow{\scriptstyle (p',\eta_{p'})} & \downarrow{\scriptstyle (m,\eta)} \\ \mathcal{T}_{\alpha'} & \xrightarrow{(q,\eta_q)} & \mathcal{T}' \end{array}$$

the two triangles commute.

Definition 10 *Two timed transition systems* $\mathcal{T}_1$ *and* $\mathcal{T}_2$ *are* $\mathcal{TW}$*-bisimilar iff there exists a span* $\mathcal{T}_1 \xleftarrow{(m,\eta)} \mathcal{T} \xrightarrow{(m',\eta')} \mathcal{T}_2$ *with vertex* $\mathcal{T}$ *of* $\mathcal{TW}$*-open morphisms.*

Example 5 *In Figure 4 the (only) two morphisms from* $\mathcal{T}$ *to* $\mathcal{T}'$ *are open. We leave it for the reader to check that this is indeed the case.*

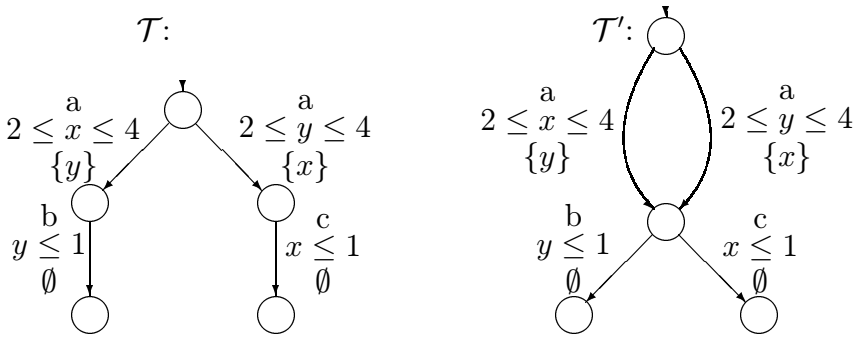


Figure 4: Two bisimilar timed transition systems.

Notice that it follows from [JNW96] and Theorem 3 that $\mathcal{TW}$-bisimulation is exactly the equivalence generated by $\mathcal{TW}$-open maps. Our next aim is to characterize $\mathcal{TW}$-open morphisms.

Definition 11 *Given a timed transition system* $\mathcal{T}$*, a configuration* $\langle s, \nu \rangle$ *of* $\mathcal{T}$ *is reachable iff* $\mathcal{T}$ *has a run with an occurrence of* $\langle s, \nu \rangle$*.*

Theorem 5 *A morphism $\mathcal{T}_1 \xrightarrow{(m,\eta)} \mathcal{T}_2$ is open iff for all reachable configurations $\langle s_1, \nu\rangle$ in $\mathcal{T}_1$, and for all $\nu' = \nu + \tau$ whenever there is a transition $m(s_1) \xrightarrow[\delta_2,\lambda_2]{\sigma} s_2'$ such that $[\![\eta^{-1}(\nu')]\!]_{X_2} \in [\![\delta_2]\!]_{X_2}$, then there exists a transition $s_1 \xrightarrow[\delta_1,\lambda_1]{\sigma} s_1'$ such that $m(s_1') = s_2'$, $[\![\nu']\!]_{X_1} \in [\![\delta_1]\!]_{X_1}$, and $\lambda_2 = \eta^{-1}(\lambda_1)$.*

Proof

Assume $\mathcal{T}_1 \xrightarrow{(m,\eta)} \mathcal{T}_2$ is open, and that the configuration $\langle s_1, \nu\rangle$ is reachable in $\mathcal{T}_1$, i.e. we have a run of some timed word α ending in $\langle s_1, \nu\rangle$. From the assumptions of the theorem the (m,η)-image of this run in $\mathcal{T}_2$ may be extended by some σ-timed transition $\langle m(s_1), \eta^{-1}(\nu)\rangle \xrightarrow[\tau']{\sigma} \langle s_2', \eta^{-1}[\lambda_2 \mapsto 0]\rangle$. Hence we have a commuting diagram with $\alpha' = \alpha(\sigma, \tau')$

$$\begin{array}{ccc} \mathcal{T}_\alpha & \xrightarrow{(q,\eta_q)} & \mathcal{T}_1 \\ \downarrow & & \downarrow{\scriptstyle (m,\eta)} \\ \mathcal{T}_{\alpha'} & \xrightarrow{(q',\eta_{q'})} & \mathcal{T}_2 \end{array}$$

¿From the definition of openness we get a mediating morphism

$$\begin{array}{ccc} \mathcal{T}_\alpha & \xrightarrow{(q,\eta_q)} & \mathcal{T}_1 \\ \downarrow & \nearrow{\scriptstyle (p,\eta_p)} & \downarrow{\scriptstyle (m,\eta)} \\ \mathcal{T}_{\alpha'} & \xrightarrow[(q',\eta_{q'})]{} & \mathcal{T}_2 \end{array}$$

¿From this diagram, it follows from Theorem 1 and Theorem 4 that there exists a transition $s_1 \xrightarrow[\delta_1,\lambda_1]{\sigma} s_1'$ such that $m(s_1') = s_2'$, $[\![\nu']\!]_{X_1} \in [\![\delta_1]\!]_{X_1}$, and $\lambda_2 = \eta^{-1}(\lambda_1)$.

For the if part of the theorem, assume the we have a commuting square

$$\begin{array}{ccc} \mathcal{T}_\alpha & \xrightarrow{(q,\eta_q)} & \mathcal{T}_1 \\ \downarrow & & \downarrow{\scriptstyle (m,\eta)} \\ \mathcal{T}_{\alpha'} & \xrightarrow{(q',\eta_{q'})} & \mathcal{T}_2 \end{array}$$

In the following we assume that $\alpha' = \alpha(\sigma, \tau')$, i.e. that α' is an extension of of α by a single timed action. The general case follows from repeated applications of the arguments in the following.

¿From Theorem 4, the morphism (q, η_q) defines a run of α in $\mathcal{T}_1$ ending in some configuration $\langle s_1, \nu\rangle$, mapped by (m,η) to $\langle m(s_1), \eta^{-1}(\nu)\rangle$. Now, $(q', \eta_{\ q'})$ implies that there is some transition $m(s_1) \xrightarrow[\delta_2,\lambda_2]{\sigma} s_2'$ in $\mathcal{T}_2$, such that $[\![\eta^{-1}(\nu')]\!]_{X_2} \in [\![\delta_2]\!]_{X_2}$, where $\nu' = \nu + \tau$ for some τ determined by α'. From the assumptions of the theorem, we now get that there exists a transition

$s_1 \xrightarrow[\delta_1,\lambda_1]{\sigma} s_1'$, such that $m(s_1') = s_2'$, $[\![\nu']\!]_{X_1} \in [\![\delta_1]\!]_{X_1}$, and $\lambda_2 = \eta^{-1}(\lambda_1)$. Using Theorem 4 this implies the existence of a morphism from $\mathcal{T}_{\alpha'}$ to $\mathcal{T}_1$, for which the commutativity properties required by openness follows by the properties listed above.

□

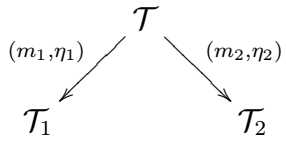
The standard notion of timed bisimulation is defined in terms of configurations as follows.

Definition 12 (Timed Bisimulation [Čer92, AM94]) *Two timed transition systems are bisimilar iff there exists a relation R over configurations $(\langle s, \nu_s\rangle, \langle t, \nu_t\rangle)$ of the two systems satisfying $(\langle s^{in}, \nu_s^0\rangle, \langle t^{in}, \nu_t^0\rangle) \in R$ and for all $(\langle s, \nu_s\rangle, \langle t, \nu_t\rangle) \in R$*

- *whenever $\langle s, \nu_s\rangle \xrightarrow[\tau]{\sigma} \langle s', \nu_s'\rangle$ then $\langle t, \nu_t\rangle \xrightarrow[\tau]{\sigma} \langle t', \nu_t'\rangle$ with $(\langle s', \nu_s'\rangle, \langle t', \nu_t'\rangle) \in R$ for some $\langle t', \nu_t'\rangle$.*
- *whenever $\langle t, \nu_t\rangle \xrightarrow[\tau]{\sigma} \langle t', \nu_t'\rangle$ then $\langle s, \nu_s\rangle \xrightarrow[\tau]{\sigma} \langle s', \nu_s'\rangle$ with $(\langle s', \nu_s'\rangle, \langle t', \nu_t'\rangle) \in R$ for some $\langle s', \nu_s'\rangle$.*

Theorem 6 *Two timed transition systems $\mathcal{T}_1$ and $\mathcal{T}_2$ are $\mathcal{TW}$-bisimilar iff they are bisimilar according to Definition 12.*

Proof Assume $\mathcal{T}_1$ and $\mathcal{T}_2$ to be $\mathcal{TW}$-bisimilar with span of open maps



Define $\mathcal{R}$ to be the following relation of configurations of $\mathcal{T}_1$ and $\mathcal{T}_2$:

> $\langle s_1, \nu_1\rangle \mathcal{R} \langle s_2, \nu_2\rangle$ iff
> there exists a reachable configuration $\langle s, \nu\rangle$ of $\mathcal{T}$ such that $s_i = m_i(s)$ and $\nu_i = \eta_i^{-1}(\nu)$ for $i = 1, 2$.

It follows easily from Theorem 5 that $\mathcal{R}$ satisfies the required properties of Definition 12.

Assume $\mathcal{T}_1$ and $\mathcal{T}_2$ to be bisimilar with relation $\mathcal{R}$ as defined in Definition 12. We construct a span of open maps with vertex $\mathcal{T}$ defined as follows.

The states of $\mathcal{T}$ will be pairs of "$\mathcal{R}$-related runs" of $\mathcal{T}_1$ and $\mathcal{T}_2$ - formally defined as follows.

Two runs of a timed word $\alpha = (\sigma_1, \tau_1)(\sigma_2, \tau_2)\ldots(\sigma_n, \tau_n), n \geq 0$ in $\mathcal{T}_1$ and $\mathcal{T}_2$ respectively

$$\langle s_i^0, \nu_i^0\rangle \xrightarrow[\tau_1]{\sigma_1} \langle s_i^1, \nu_i^1\rangle \xrightarrow[\tau_2]{\sigma_2} \ldots \xrightarrow[\tau_n]{\sigma_n} \langle s_i^n, \nu_i^n\rangle, i = 1, 2 \qquad (3)$$

are said to be $\mathcal{R}$-related iff

$$\langle s_1^j, \nu_1^j\rangle \mathcal{R} \langle s_2^j, \nu_2^j\rangle \text{for } 0 \leq j \leq n$$

The initial state of $\mathcal{T}$ is the pair of initial configurations of $\mathcal{T}_1$ and $\mathcal{T}_2$.

The clock variables of $\mathcal{T}$ will be the disjoint union of the clock variables of $\mathcal{T}_1$ and $\mathcal{T}_2$, $X_1 \uplus X_2$.

Finally for each pair of $\mathcal{R}$-related runs of the form (3), there will be an incoming transition in $\mathcal{T}$ from the pair of $\mathcal{R}$-related runs of ending in $(\langle s_1^{n-1}, \nu_1^{n-1}\rangle, \langle s_2^{n-1}, \nu_2^{n-1}\rangle)$ of the form $\xrightarrow[\delta,\lambda]{\sigma_n}$, where

$$\delta = \bigwedge_{x \in X_i, i=1,2} (x = \nu_i^{n-1}(x) + (\tau_n - \tau_{n-1}))$$

$$\lambda = \{x_i \in X_i \mid i = 1, 2 \text{ and } \nu_i^n(x_i) = 0\}$$

The open morphisms from $\mathcal{T}$ to $\mathcal{T}_i$ is $(m_i, \eta_i) : \mathcal{T} \to \mathcal{T}_i,\ i = 1, 2$ where the m_i-value on a pair of $\mathcal{R}$-related runs as in (3) is taken to be s_i^n, and η_i is the injection function from X_i to $X_1 \uplus X_2$. It follows from the construction that (m_i, η_i) are morphisms, and openness follows from Theorem 5.

□

Example 6 *Concider the timed transition systems in Figure 5. It is easy to see that there is exactly one morphism from $\mathcal{T}$ to $\mathcal{T}_i$, for $i = 1, 2$, and that this morphism is open. Hence, we have a span of open maps between $\mathcal{T}_1$ and $\mathcal{T}_2$ (with $\mathcal{T}$ as vertex), and bisimilarity between $\mathcal{T}_1$ and $\mathcal{T}_2$ follows from Theorem 6.*

Notice that there are simple arguments following Theorem 5 for openness of the morphisms in the example above. Hence we suggest spans of open maps as a convenient framework for presentations of bisimilarity of finite timed transition systems. In the next section this will be supported by two decidability results: openness of morphisms and bisimilarity for finite timed transition systems.

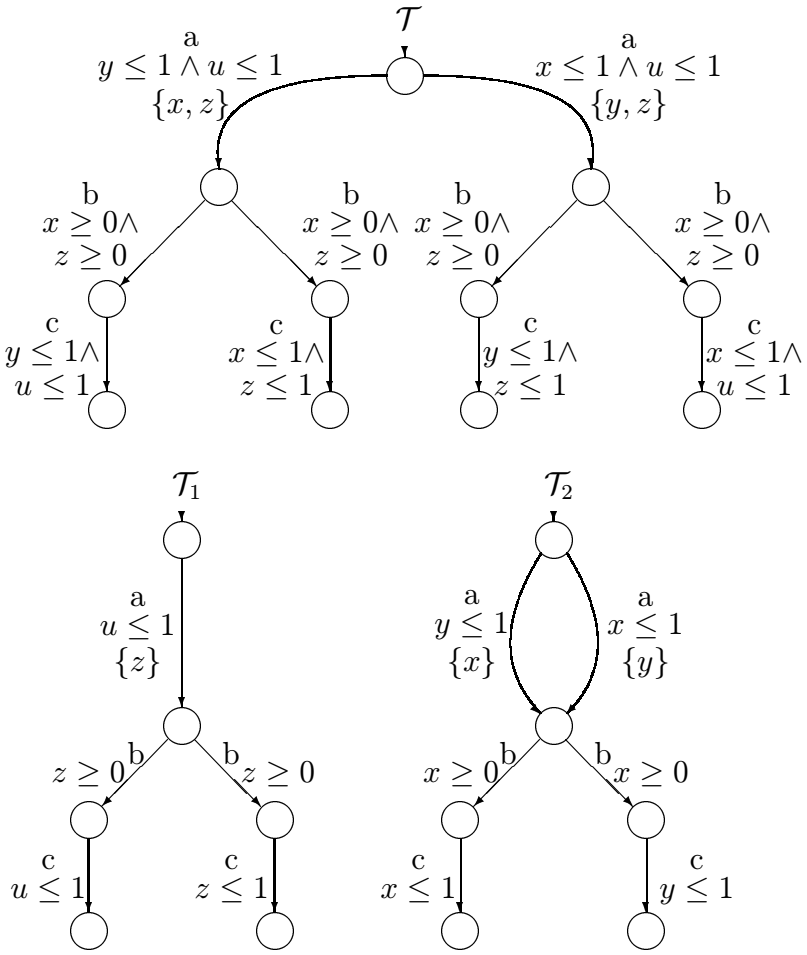


Figure 5: Three systems with a span.

4 Decidability

In this section we restrict ourselves to finite timed transition systems, i.e. systems with a finite number of states, clocks and transitions, and for which all constants referred to in constraints have rational values. By scaling the rational constants we assume without loss of generality in the following that all constants are integer valued [AD94].

To get a decidable characterization of openness we introduce the notion of regions, [AD94].

Definition 13 (Region[AD94]) *Given a finite set of clock variables X and an integer constant c, a region is an equivalence class of the equivalence relation $\cong$ over clock valuations, where $\nu \cong \nu'$ iff*

- *For each $x \in X$: $\lfloor \nu(x) \rfloor = \lfloor \nu'(x) \rfloor$[2] or both $\nu(x) > c$ and $\nu'(x) > c$.*
- *For every pair of clock variables $x, y \in X$ where both $\nu(x) \leq c$ and $\nu(y) \leq c$ we have that $fract(\nu(x)) \leq fract(\nu(y))$ iff $fract(\nu'(x)) \leq fract(\nu'(y))$.*
- *For every clock variable $x \in X$ where $\nu(x) \leq c$ we have $fract(\nu(x)) = 0$ iff $fract(\nu'(x)) = 0$.*

For a clock valuation ν, let $[\nu]$ denote the region to which it belongs. Let $\mathcal{R}_{X,c}$ denote the (finite) set of regions associated with X and c. Given regions $reg, reg' \in \mathcal{R}_{X,c}$, $reg' \in \text{Reach}(reg)$ iff there exists $\nu \in reg$ and $\tau \in \mathbf{R}_+$ such that $\nu + \tau \in reg'$. Finally, for a finite timed transition system $\mathcal{T}$ an extended state is defined as any pair $\langle s, reg \rangle$, where s is a state of $\mathcal{T}$ and reg is a region over the set of clock variables of $\mathcal{T}$.

Proposition 3 *Consider finite timed transition systems $\mathcal{T}$ and $\mathcal{T}'$ with clock variables X and X' respectively, and let c be an integer constant greater than or equal to the largest constant referred to in transition constraint expressions in $\mathcal{T}$ and $\mathcal{T}'$.*

For any $\mathcal{T}$-constraint expression δ and any region $reg \in \mathcal{R}_{X,c}$, $[\![reg]\!]_X \subseteq [\![\delta]\!]_X$ iff $[\![reg]\!]_X \cap [\![\delta]\!]_X \neq \emptyset$. For any $reg' \in \mathcal{R}_{X,c}$, and any $\nu, \nu' \in reg$, reg' is reachable from ν iff it is reachable from ν'.

Consider a morphism (m, η) from $\mathcal{T}$ to $\mathcal{T}'$ with $reg, reg' \in \mathcal{R}_{X,c}$, then

[2] We use $\lfloor x \rfloor$ for the largest integer smaller than or equal to x and $fract(x) := x - \lfloor x \rfloor$.

- $\eta^{-1}(reg) \in \mathcal{R}_{X',c}$
- *if* $reg' \in \mathrm{Reach}(reg)$ *then* $\eta^{-1}(reg') \in Reach(\eta^{-1}(reg))$

Proof First two properties follow from e.g. [AD94]. The regional properties of morphisms follow by simple calculation.

□

Our operations on clock evaluations can be extended to regions which will be used below. We can now give a characterization of open maps in terms of extended states.

Theorem 7 *Consider finite timed transition systems* $\mathcal{T}_1$ *and* $\mathcal{T}_2$ *with clock variables* X_1 *and* X_2 *respectively, and associated regions defined with respect to some integer constant greater than or equal to the largest constant referred to in transition constraint expressions in* $\mathcal{T}_1$ *and* $\mathcal{T}_2$*. A morphism* $(m, \eta) : \mathcal{T}_1 \to \mathcal{T}_2$ *is open iff for all reachable extended states* $\langle s_1, reg \rangle$ *in* $\mathcal{T}_1$*, and for all* $reg' \in Reach(reg)$*, whenever there is a transition* $m(s_1) \xrightarrow[\delta_2,\lambda_2]{\sigma} s_2'$ *such that* $[\![\eta^{-1}(reg')]\!]_{X_2} \subseteq [\![\delta_2]\!]_{X_2}$*, then there exists a transition* $s_1 \xrightarrow[\delta_1,\lambda_1]{\sigma} s_1'$ *such that* $m(s_1') = s_2'$*,* $\lambda_2 = \eta^{-1}(\lambda_1)$ *and* $[\![reg']\!]_{X_1} \subseteq [\![\delta_1]\!]_{X_1}$*.*

Proof Follows from Theorem 5 and Proposition 3.

□

Notice that Theorem 7 implies the following decidability result of openness of a morphism between two finite timed transition systems.

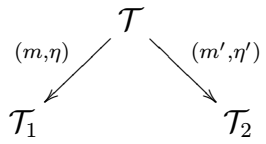
Theorem 8 *Given two finite timed transition systems* $\mathcal{T}_1$ *and* $\mathcal{T}_2$ *and a morphism* $(m, \eta) : \mathcal{T}_1 \to \mathcal{T}_2$ *, openness of* (m, η) *is decidable.*

Proof Follows immediately form Theorem 7 and Proposition 3.

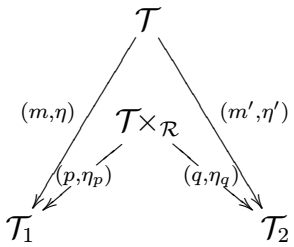
□

For untimed transition systems, decidability of bisimulation follows e.g. from the fact that a span of open maps between two finite transition systems imply a span with a vertex being a subsystem of their product, see [JNW96]. Unfortunately, this result does not generalize completely to our setting here. However, we still have the following.

Theorem 9 *Given two finite timed transition systems $\mathcal{T}_1$ and $\mathcal{T}_2$, if there exists a span of open maps*



then there is a finite vertex $\mathcal{T}\times_{\mathcal{R}}$ of size bounded by the size of $\mathcal{T}_1$ and $\mathcal{T}_2$ and with open morphisms



Proof Assume without loss of generality that the clock variables of $\mathcal{T}_1$ and $\mathcal{T}_2$ are disjoint. If ν and ν' are clock evaluations for $\mathcal{T}_1$ and $\mathcal{T}_2$ respectively we shall write $\nu \uplus \nu'$ for the combined clock evaluation over the disjoint union of the clock variables of $\mathcal{T}_1$ and $\mathcal{T}_2$, satisfying $(\nu \uplus \nu') := \nu(x)$ if $x \in X_1$ and $(\nu \uplus \nu') := \nu'(x)$ if $x \in X_2$. Let c be an integer constant greater than or equal to the largest constant mentioned in transition constraint expressions in $\mathcal{T}_1$ and $\mathcal{T}_2$, and let all regions in the following be defined with respect to c. The timed transition system $\mathcal{T}\times_{\mathcal{R}}$ is defined in the following way.

- $\mathrm{S}\times_{\mathcal{R}}$ is the set of pairs $\langle s_1, s_2\rangle$ for which there exists a reachable configuration $\langle s, \nu\rangle$ in $\mathcal{T}$ such that $m(s) = s_1$ and $m'(s) = s_2$.
- The initial state $\mathrm{s}^{\mathrm{in}}\times_{\mathcal{R}}$ is $\langle s_1^{in}, s_2^{in}\rangle$ where s_1^{in} is the initial state of $\mathcal{T}_1$ and s_2^{in} the initial state of $\mathcal{T}_2$.
- $\mathrm{X}\times_{\mathcal{R}} = X_1 \uplus X_2$.
- The transitions of $\mathcal{T}\times_{\mathcal{R}}$ are defined as follows. For all runs in $\mathcal{T}$

$$\langle s^{in}, \nu_0\rangle \xrightarrow[\tau_1]{\sigma_1} \langle s_1, \nu_1\rangle \xrightarrow[\tau_2]{\sigma_2} \ldots \xrightarrow[\tau_n]{\sigma_n} \langle s, \nu\rangle$$

  with an extended run of the form

$$\langle s^{in}, \nu_0\rangle \xrightarrow[\tau_1]{\sigma_1} \langle s_1, \nu_1\rangle \xrightarrow[\tau_2]{\sigma_2} \ldots \xrightarrow[\tau_n]{\sigma_n} \langle s, \nu\rangle \xrightarrow[\tau]{\sigma} \langle s', \nu'\rangle$$

we introduce a transition

$$\langle m(s), m'(s)\rangle \xrightarrow[\hat{\delta},\hat{\lambda}]{\sigma} \langle m(s'), m'(s')\rangle$$

in $\mathcal{T}\times_{\mathcal{R}}$, where $\hat{\lambda}$ consists of all clock variables x from $\mathcal{T}_1$ and x' from $\mathcal{T}_2$, for which $\nu^{'-1}(\eta(x))) = 0$ or $\nu^{'-1}(\eta'(x'))) = 0$, and $\hat{\delta}$ is the logical expression defining the region to which $\eta^{-1}(\nu+(\tau-\tau_n)) \uplus \eta^{'-1}(\nu+(\tau-\tau_n))$ belongs.

This completes the definition of $\mathcal{T}\times_{\mathcal{R}}$. Obviously, the size is bounded by the size of $\mathcal{T}_1$ and $\mathcal{T}_2$. The number of states is bounded by $|S_1| * |S_2|$. The number of regions over the disjoint union of X_1 and X_2 with constant c, is $|X|! * 2^{|X|} * (2c+2)^{|X|}$ where $|X| = |X_1| + |X_2|$, so there are at most $|\Sigma| * (|X|! * 2^{|X|} * (2c+2)^{|X|}) * 2^{|X|}$ transitions between any two states.

The morphisms from $\mathcal{T}\times_{\mathcal{R}}$ to $\mathcal{T}_1$ and $\mathcal{T}_2$ are the projections (p, η_p) and (q, η_q) respectively, where $p(\langle s_1, s_2\rangle) = s_1$ and similarly for q. The function η_p is the identity function on the clock variables of $\mathcal{T}_1$ and η_q is the identity function on the clock variables of $\mathcal{T}_2$. We need to verify that these are morphisms and that they are open. The proof for (p, η_p) will be shown here, and the arguments for (q, η_q) are symmetric.

To verify that the projection (p, η_p) is a morphism, consider a transition $\langle m(s), m'(s)\rangle \xrightarrow[\hat{\delta},\hat{\lambda}]{\sigma} \langle m(s'), m'(s')\rangle$ in $\mathcal{T}\times_{\mathcal{R}}$ as defined above. From definition and Theorem 1 this implies the existence in $\mathcal{T}_1$ of some transition $m(s) \xrightarrow[\delta_1,\lambda_1]{\sigma} m(s')$ realizing $\langle m(s), \eta^{-1}(\nu)\rangle \xrightarrow[\tau]{\sigma} \langle m(s'), \eta^{-1}(\nu')\rangle$, i.e. such that $[\![\eta^{-1}(\nu) + (\tau - \tau_n)]\!]_{X_1} \in [\![\delta_1]\!]_{X_1}$ and $\lambda_1 = \{x_1 \in X_1 \mid \eta^{-1}(\nu')(x_1) = 0\}$. This implies $[\![\eta_p^{-1}(\hat{\delta})]\!]_{X_1} \subseteq [\![\delta_1]\!]_{X_1}$, and hence $[\![\hat{\delta}]\!]_{X_\times} \subseteq [\![\eta^{-1}(\hat{\delta})[\eta_p(x)/x]]\!]_{X_\times} \subseteq [\![\delta_1[\eta_p(x)/x]]\!]_{X_\times}$, and $\lambda_1 = \eta_p^{-1}(\hat{\lambda})$.

To show that (p, η_p) is open, we show that it has the property from Theorem 7. Notice first that from construction, for any reachable extended state in $\mathcal{T}\times_{\mathcal{R}}$ of the form $(\langle s_1, s_2\rangle, reg)$ there exists a reachable configuration $\langle s, \nu\rangle$ in $\mathcal{T}$ such that $m(s) = s_1$, $m'(s) = s_2$, and $\eta^{-1}(\nu) \cup \eta^{'-1}(\nu) \in reg$.

Assume the extended state $\langle s_1, s_2, reg\rangle$ is reachable in $\mathcal{T}\times_{\mathcal{R}}$. Consider $reg' \in Reach(reg)$ and a transition $s_1 \xrightarrow[\delta_1,\lambda_1]{\sigma} s_1'$ in $\mathcal{T}_1$ for which $[\![\eta_p^{-1}(reg')]\!]_{X_1} \subseteq [\![\delta_1]\!]_{X_1}$. We must show the existence of a transition in $\mathcal{T}\times_{\mathcal{R}}$ of the form $\langle s_1, s_2\rangle \xrightarrow[\hat{\delta},\hat{\lambda}]{\sigma} \langle s_1', s_2'\rangle$, such that $[\![reg']\!]_{X_\times} \subseteq [\![\hat{\delta}]\!]_{X_\times}$ and $\lambda_1 = \eta_p^{-1}(\hat{\lambda})$.

Since $\langle s_1, s_2, reg\rangle$ is reachable we have a reachable configuration $\langle s, \nu\rangle$ in $\mathcal{T}$ such that $m(s) = s_1, m'(s) = s_2$, and $\eta^{-1}(\nu) \uplus \eta^{'-1}(\nu) \in reg$. Let τ be such that $\eta^{-1}(\nu+\tau) \uplus \eta^{'-1}(\nu+\tau) \in reg'$, and hence $[\![\eta^{-1}(\nu+\tau)]\!]_{X_1} \in [\![\eta_p^{-1}(reg')]\!]_{X_1} \subseteq$

$[\![\delta_1]\!]_{X_1}$. We obtain from Theorem 5 the existence in $\mathcal{T}$ of a transition $s \xrightarrow[\delta,\lambda]{\sigma} s'$ such that $m(s') = s'_1$, $[\![\nu + \tau]\!]_X \in [\![\delta]\!]_X$ and $\lambda_1 = \eta^{-1}(\lambda)$. Hence from construction we have $\langle s_1, s_2\rangle \xrightarrow[\hat{\delta},\hat{\lambda}]{\sigma} \langle m(s'), m'(s')\rangle$, where $[\![\hat{\delta}]\!]_{X_\times} = [\![reg']\!]_{X_\times}$ and $\lambda_1 = \eta^{-1}(\lambda) = \eta_p^{-1}(\hat{\lambda})$.

□

¿From the proof of Theorem 9, we have the following corollary.

Corollary 1 *Given two finite timed transition systems, timed bisimulation is decidable.*

5 Extension with invariants

In this section we will extend the timed transition systems with invariants [LPY97] on the states and argue that the results from the preceding sections can be generalized to the extended model without problems. We will state the results for the new model and hints to some of the proofs, all of which are simple extensions of the proofs for the model without invariants on states.

Definition 14 (Timed Transition Systems with invariants) *A timed transition system with invariants is six tuple $(S, \Sigma, s_0, X, T, I)$ where the first five components are as in Definition 1 and* I *assigns to each state an invariant. Invariants are given by the same syntax as constraints, so the invariant for state* s*, ι_s, can be generated by the grammar Δ from Definition 1.*

The meaning of a invariant ι_s, $[\![\iota_s]\!]_X$, is defined in the same way as the meaning of a constraint. In the definition of runs over a timed transition system with invariants, the invariant of a state must be satisfied when the state is entered and until the next state is entered. More formally, in the definition of a run

$$\langle s_0, \nu_0\rangle \xrightarrow[\tau_1]{\sigma_1} \langle s_1, \nu_1\rangle \xrightarrow[\tau_2]{\sigma_2} \cdots \xrightarrow[\tau_n]{\sigma_n} \langle s_n, \nu_n\rangle$$

we require $\forall i \in \{0, 1, \ldots, n-1\}, \forall \tau \in [0, \tau_i - \tau_{i-1}) : [\![\nu_i + \tau]\!]_X \in [\![\iota_{s_i}]\!]_X$ where $\tau_0 = 0$, and for the last state $[\![\nu_n]\!]_X \in [\![\iota_{s_n}]\!]_X$. We define a new kind of morphism which is going to be an extension of the ones from Definition 5 taking invariants into account.

Definition 15 *A morphism (m, η) between two timed transition systems with invariants $\mathcal{T}$ and $\mathcal{T}'$ consists of the same components as the morphisms in Definition 5 with one extra constraint:*

- *If a state* s *in $\mathcal{T}$ is mapped by m to a state $m(s)$ in $\mathcal{T}'$ then $[\![\iota_s]\!]_X \subseteq [\![\iota_{m(s)}[\eta(x)/x]]\!]_X$.*

This definition ensures that if an invariant is satisfied in some configuration in $\mathcal{T}$ the invariant of the simulating configuration is also satisfied. This implies that we still have morphisms as simulations as stated in Theorem 1.

With this notion of morphisms we have a category as in Definition 7, which we denote $\mathrm{CTTS}^{\iota}_{\Sigma}$.

Proposition 4 $\mathrm{CTTS}^{\iota}_{\Sigma}$ *has products and pullbacks.*

The construction of $\mathcal{T}_1 \times_{\mathcal{T}} \mathcal{T}_2$ follows the one in the proof of Theorem 3 where the invariant of the state $\langle s_1, s_2 \rangle$ is defined such that $[\![\iota_{\langle s_1, s_2 \rangle}]\!]_{X_\times} = [\![\iota_{s_1}]\!]_{X_\times} \cap [\![\iota_{s_2}]\!]_{X_\times}$. The invariants on the states in the product is defined in the same way.

As our category of computations we would again like to choose timed words over Σ with word extensions. Like for timed transition systems we choose a representation of these in terms of our models following the approach of [JNW96]. This is going to look very much like the representation we defined for timed transition systems, we just need to add invariants to all the states.

Definition 16 *Given a timed word $\alpha = (\sigma_1, \tau_1)\,(\sigma_2, \tau_2)\,(\sigma_3, \tau_3) \cdots (\sigma_n, \tau_n)$ we define a timed transition system $\mathcal{T}^{\iota}_{\alpha}$ $0 \xrightarrow[\delta_1, \lambda_1]{\sigma_1} 1 \xrightarrow[\delta_2, \lambda_2]{\sigma_2} \cdots \xrightarrow[\delta_n, \lambda_n]{\sigma_n} n$, as in Definition 8, where the invariants are defined inductively to be of the form $\bigwedge_{x \in X}(c_x \leq x < c'_x)$. The initial the invariant is*

$$\bigwedge_{x \in X} (0 \leq x < \tau_1)$$

Assume the invariant on the state i-1 is $\bigwedge_{x \in X}(c^{i-1}_x \leq x < \tilde{c}^{i-1}_x)$, then the invariant for state i is

$$\bigwedge_{x \in X} (\mathit{if}\ x \in \lambda_i\ \mathit{then}\ (0 \leq x < \tilde{\tau}_i)\ \mathit{else}\ (\tilde{c}^{i-1}_x \leq x < \tilde{c}^{i-1}_x + \tilde{\tau}_i))$$

where $\tilde{\tau}_i = \tau_i - \tau_{i-1}$. *The constraint on the final state is*

$$\bigwedge_{x \in X} (if\ x \in \lambda_i\ then\ (x = 0)\ else\ (x = \tilde{c}_x^{i-1}))$$

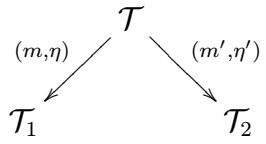
Using this construction we still get an embedding of the category of timed words with extensions into $\mathrm{CTTS}^{\iota}_{\Sigma}$, with properties as in Theorem 4.

The characterization of open maps is a little more complicated to state with the invariants. The proof though is again just a simple extension of the proof of Theorem 5 using the constraint for the invariants and the condition for runs.

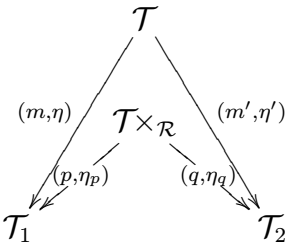
Proposition 5 *A morphism* $(m, \eta) : \mathcal{T}_1 \to \mathcal{T}_2$ *is open iff for all reachable configurations* $\langle s_1, \nu \rangle$ *for all* $\nu' = \nu + \tau$ *such that* $\forall \tau' : \tau' < \tau \Rightarrow [\![\eta^{-1}(\nu + \tau')]\!]_{X_2} \in [\![\iota_{m(s_1)}]\!]_{X_2}$ *whenever there is a transition* $m(s_1) \xrightarrow[\delta_2, \lambda_2]{\sigma} s_2'$ *if* $[\![\overline{\nu}]\!]_{X_2} \in [\![\delta_2]\!]_{X_2}$ *and* $[\![\overline{\nu}]\!]_{X_2} \in [\![\iota_{s_2'}]\!]_{X_2}$ *for* $\overline{\nu} = \eta^{-1}(\nu')$ *then there exists a transition* $s_1 \xrightarrow[\delta_1, \lambda_1]{\sigma} s_1'$ *such that* $m(s_1') = s_2'$, $[\![\nu']\!]_{X_1} \in [\![\delta_1]\!]_{X_1}$, $\lambda_2 = \eta^{-1}(\lambda_1)$, *and* $\forall \tau' < \tau : [\![\nu + \tau']\!]_{X_1} \in [\![\iota_{s_1}]\!]_{X_1}$, $[\![\nu']\!]_{X_1} \in [\![\iota_{s_2}]\!]_{X_1}$.

We also have a characterization in terms of extended states equivalent to Theorem 7, using the property that if one clock evaluation in a region satisfies an invariant then all the clock evaluations of that region satisfy the invariant. Given this, the proof of the theorem for extended states follows directly from the proof of Theorem 7. With the characterization of the open maps in terms of extended states, we again have the decidability of openness for morphisms between finite timed transition systems with invariants, and we can construct the finite vertex if such one exists.

Theorem 10 *Given to finite timed transition systems with invariants* $\mathcal{T}_1$ *and* $\mathcal{T}_2$ *if there exists a span of open maps*



then there is a finite $\mathcal{T}\times_{\mathcal{R}}$ giving a span of open maps



The construction of $\mathcal{T}\times_{\mathcal{R}}$ is almost the same as in the proof of Theorem 10. The meaning of the invariant of the state $\langle s_1, s_2\rangle$ is the intersection $[\![\iota_{s_1}]\!]_{X_\times} \cap [\![\iota_{s_2}]\!]_{X_\times}$ as in the construction used for the pullback.

Again the decidability of the bisimulation follows directly from the construction of the vertex and the decidability of openness.

6 Conclusion

We have illustrated how to apply the general framework of open maps to the setting of timed systems, providing a way of expressing a bisimulation purely within the framework of timed transition systems. Furthermore, a decision procedure for bisimulation was presented within this framework.

We propose the span of open maps idea as a useful way of expressing timed bisimulations for finite systems. On the other hand, we do not claim that our alternative decision procedure as presented here is more efficient than existing ones, e.g. [LLW95, WL97].

The categorical formulations in terms of open maps suggest applying general results from the categorical setting to concrete timed bisimulations, like the one studied here. One particularly interesting example is the characteristic path logic obtained from [JNW96]. It would be interesting to study this logic and its relation to existing timed logics from the literature.

References

[ACM97] E. Asarin, P. Caspi, and O. Maler. A Kleene theorem for timed automata. *Proc. of LICS'97*, 1997.

[AD90] R. Alur and D.L. Dill. Automata for modeling real-time systems. *Proc. of ICALP'90*, LNCS 433:pages 322–335, 1990.

[AD94] R. Alur and D.L. Dill. A theory of timed automata. *Theoretical Computer Science*, 126, 1994.

[AH91] R. Alur and T.A. Henzinger. Logics and models for real time: A survey. *Real-Time:Theory in Practice*, LNCS 600:pages 74–106, 1991.

[AKLN95] J.H. Andersen, K.J. Kristoffersen, K.G. Larsen, and J. Niedermann. Automatic synthesis of real time systems. *Proc. of ICALP'95*, LNCS 944:pages 535–546, 1995.

[AM94] H. H. Andersen and M. Mendler. An asynchronous process algebra with multiple clocks. In *Proceedings of ESOP'94*, volume LNCS 788, 1994.

[Čer92] K. Čerāns. Decidability of bisimulation equivalence for parallel timer processes. *Proc. of CAV'92*, LNCS 663, 1992.

[CFW98] G.L. Cattani, M. Fiore, and G. Winskel. A theory of recursive domains with applications to concurrency. In *Proceedings of LICS'98*, 1998.

[CN96] A. Cheng and M. Nielsen. Open maps (at) work. *Proc. of FST&TCS '95*, LNCS 1026, 1996.

[HN98] T. Hune and M. Nielsen. Timed bisimulation and open maps. *Proc. of MFCS'98*, LNCS 1450:pages 378–387, 1998.

[JNW96] A. Joyal, M. Nielsen, and G. Winskel. Bisimulation from open maps. *Information and Computation*, 127,2:pages 164–185, 1996.

[KN94] K.J. Kristoffersen and J. Niedermann. User's manual for Epsilon. Available via anonymous ftp at cs.auc.dk, December 1994.

[LLW95] F. Laroussinie, K. G. Larsen, and C. Weise. From timed automata to logic – and back. *Proc. of MFCS'95*, LNCS 969:pages 529–539, 1995.

[LPY95] K. G. Larsen, P. Pettersson, and W. Yi. Model-checking for real-time systems. *In Proceedings of the 10th International Conference on Fundamentals of Computation Theory*, LNCS 965:pages 62–88, 1995.

[LPY97] K. G. Larsen, P. Pettersson, and W. Yi. UPPAAL in a nutshell. *In Springer International Journal of Software Tools for Technology Transfer*, 1(1+2), 1997.

[MBC+95] M. A. Marsan, G. Balbo, G. Conte, S. Donatelli, and G. Franceschinis. *Modelling with generalized stochastic petri nets.* Wiley series in parallel computing. John Wiley & Sons, 1995.

[Mil89] R. Milner. *Communication and Concurrency.* Prentice Hall International Series in Computer Science, 1989.

[NSY93] X. Nicollin, J. Sifakis, and S. Yovine. From ATP to timed graphs and hybrid systems. *Acta Informatica*, 30:pages 181–202, 1993.

[Wan90] Y. Wang. Real-time behaviour of asynchronous agents. *Proc. of CONCUR'90*, LNCS 458, 1990.

[WL97] C. Weise and D. Lenzkes. Efficient scaling-invariant checking of timed bisimulation. *Proc. of STACS'97*, LNCS 1200:pages 177–188, 1997.

[WN96] G. Winskel and M. Nielsen. Presheaves as transition systems. In *Partial order methods in verification*, DIMACS, pages pages:129–140. 1996.

Recent BRICS Report Series Publications

RS-98-4 **Mogens Nielsen and Thomas S. Hune.** ***Timed Bisimulation and Open Maps*****. February 1998. 27 pp.**

RS-98-3 **Christian N. S. Pedersen, Rune B. Lyngsø, and Jotun Hein.** ***Comparison of Coding DNA*****. January 1998. 20 pp. To appear in** ***Combinatorial Pattern Matching: 9th Annual Symposium*****, CPM '98 Proceedings, LNCS, 1998.**

RS-98-2 **Olivier Danvy.** ***An Extensional Characterization of Lambda-Lifting and Lambda-Dropping*****. January 1998.**

RS-98-1 **Olivier Danvy.** ***A Simple Solution to Type Specialization (Extended Abstract)*****. January 1998. 7 pp.**

RS-97-53 **Olivier Danvy.** ***Online Type-Directed Partial Evaluation*****. December 1997. 31 pp. Extended version of an article to appear in** ***Third Fuji International Symposium on Functional and Logic Programming*****, FLOPS '98 Proceedings (Kyoto, Japan, April 2–4, 1998), pages 271–295, World Scientific, 1998.**

RS-97-52 **Paola Quaglia.** ***On the Finitary Characterization of π-Congruences*****. December 1997. 59 pp.**

RS-97-51 **James McKinna and Robert Pollack.** ***Some Lambda Calculus and Type Theory Formalized*****. December 1997. 43 pp.**

RS-97-50 **Ivan B. Damgård and Birgit Pfitzmann.** ***Sequential Iteration of Interactive Arguments and an Efficient Zero-Knowledge Argument for NP*****. December 1997. 19 pp. To appear in** ***25th International Colloquium on Automata, Languages, and Programming*****, ICALP '98 Proceedings, LNCS, 1998.**

RS-97-49 **Peter D. Mosses.** ***CASL for ASF+SDF Users*****. December 1997. 22 pp. Appears in Sellink, Editor,** ***2nd International Workshop on the Theory and Practice of Algebraic Specifications, Electronic Workshops in Computing*****, ASF+SDF '97 Proceedings, Springer-Verlag, 1997.**

RS-97-48 **Peter D. Mosses.** ***CoFI: The Common Framework Initiative for Algebraic Specification and Development*****. December 1997. 24 pp. Appears in Bidoit and Dauchet, editors,** ***Theory and Practice of Software Development: 7th International Joint Conference CAAP/FASE*****, TAPSOFT '97 Proceedings, LNCS 1214, 1997, pages 115–137.**