

# Automatic Synthesis of Real Time Systems <sup>★</sup>

Jørgen H. Andersen

Kåre J. Kristoffersen

Kim G. Larsen

Jesper Niedermann

**BRICS** <sup>\*\*</sup>

Department of Math. & Comp. Sc., Aalborg University

## Introduction

During the last few years the area of real time systems has received a lot of attention from the research community. In particular, a variety of specification formalisms has emerged allowing real time properties to be expressed explicitly. These specification formalisms may roughly be divided into two groups, namely: real time logics (e.g. [AH89, HNSY92]) and real time process algebras (e.g. [Yi90, NRJV90]).

Central to the ongoing research has been the construction of *model-checking* algorithms; i.e. algorithms for deciding whether a given real time system satisfies a given specification. A number of model-checking algorithms exists for real timed logical specifications [ACD90] and more recently algorithms for model-checking <sup>3</sup> timed process algebraic specifications have been given [Cer92, LY93].

In this work, we deal with the more ambitious goal of *model-construction*: i.e. given a real time specification (logical or process algebraic) we want to automatically synthesize a real time system satisfying the specification (if such a system exists). Moreover, we consider the model-construction problem in the setting of *implicit specifications*, i.e.:

$$(A_1 \mid \dots \mid A_n \mid X) \text{ sat } S \tag{1}$$

The requirement of (1) represents a certain stage in a top-down development of a network satisfying a given overall specification  $S$ : namely, the stage where some components  $A_1 \dots A_n$  have already been constructed, but for the completion of the development one component  $X$  remains to be constructed. We call  $S$  an implicit specification of  $X$  as it specifies the behaviour of  $X$  in a certain context.

In this paper we present a method for automatically constructing the component  $X$  (if possible) such that (1) is met. Our method is applicable to logical as well as process algebraic specifications and proceeds in two steps: First, the implicit specification  $S$  is (effectively) transformed into a *direct* specification  $S'$

---

<sup>\*</sup> This work has been partially supported by the European Communities under CONCUR2, BRA 7166.

<sup>\*\*</sup> Basic Research in Computer Science, Centre of the Danish National Research Foundation

<sup>3</sup> In process algebra model-checking consists in checking a suitable behavioural relationship (bisimilarity, say) between the implementation and the specification.

describing the sufficient and necessary requirement to  $X$  in order for (1) to hold; i.e.:

$$X \text{ sat } S' \quad \text{if and only if} \quad (A_1 \mid \dots \mid A_n \mid X) \text{ sat } S \quad (2)$$

Second, a real time system satisfying  $S'$  is generated (if possible) using a *direct* model-construction algorithm.

Our work can be seen as a real time extension of existing model-constructing algorithms for finite-state systems. For  $n = 0$  the model-construction problem for (1) extends classical model-construction methods. For  $S$  a process algebraic specification the model-construction problem for (1) is a real time extension of the equation solving problem studied in [LX90a, Shi86, Par89, LQ90]. For  $S$  a logical specification our work is related to and extends the work on contexts as property transformers studied in [LX91, LS92].

Our method assumes that the network components  $A_1 \dots A_n$  and  $X$  are all regular timed agents [Yi90] or equivalently one-clock timed automata [AD94]. For reasons of clarity we have chosen to present our solution method in a somewhat simplified setting, where the notion of parallel composition is simply that of interleaving on actions and the specification language considered is a timed extension of the well-known Hennessy-Milner Logic [HM85]. In the concluding remarks suggestions for extensions will be discussed in more detail. Also, a prototype implementation of the implicit model-construction method for the full extensions has been given and is available as part of the EPSILON tool [CGL93].

## 1 Timed Processes and Timed Logic

Let  $\mathcal{A}$  be a fixed set of actions ranged over by  $a, b, c, \dots$ . We denote by  $\mathbf{R}_{>0}$  the set of positive reals ranged over by  $d, d_1, d_2, \dots, d', d'', \dots$ . Similarly  $\mathbf{R}$  denotes the set of non-negative reals,  $\mathbf{N}$  denotes the set of natural numbers (including 0), and  $\mathcal{D}$  denotes the set  $\{\epsilon(d) \mid d \in \mathbf{R}_{>0}\}$ . Regular timed agents are terms of the following grammar:

$$A ::= \sum_{i=1}^n [l_i, u_i].a_i.A_i \mid N$$

where  $l_i, u_i \in \mathbf{N}$ ,  $a_i \in \mathcal{A}$  and  $N$  ranges over a finite set of agent identifiers. For each agent identifier we assume a defining equation  $N \stackrel{def}{=} A$ . Intuitively, the term  $\sum_{i=1}^n [l_i, u_i].a_i.A_i$  describes an agent which is able to perform the action  $a_i$  between the time bounds  $l_i$  and  $u_i$  after which the agent will perform according to  $A_i$ . On occasions we will use the expanded notation  $[l_1, u_1].a_1.A_1 + \dots + [l_n, u_n].a_n.A_n$  for the general summation. We shall use *nil* to denote the empty summation. However, we shall often omit trailing *nil*'s; hence  $[4, 5].a$  denotes the agent  $[4, 5].a.nil$ .

Formally, the semantics of regular timed agents are given in terms of a  $\mathcal{A} \cup \mathcal{D}$  labelled transition system, where the *configurations* are pairs of the form  $\langle A, v \rangle$ , with  $v \in \mathbf{R}$  denoting the amount by which the agent  $A$  has been delayed. The

transitions between configurations are either delay- or action-transitions and are given by the rules (3), (4) and (5):

$$\langle A, v \rangle \xrightarrow{\epsilon(d)} \langle A, v + d \rangle \quad (3)$$

$$\langle \sum_i [l_i, u_i].a_i.A_i, v \rangle \xrightarrow{a_i} \langle A_i, 0 \rangle \text{ if } v \in [l_i, u_i] \quad (4)$$

$$\frac{\langle A, v \rangle \xrightarrow{a} \langle A', v' \rangle}{\langle N, v \rangle \xrightarrow{a} \langle A', v' \rangle} \text{ if } N \stackrel{def}{=} A \quad (5)$$

Thus, we adopt the two-phase functioning principle [NSY91] present in most real-time process algebras: i.e. the behaviour of a system is regarded as being split in two alternating phases, one where all components agree to let time progress, and one where the components compute. For an agent  $A$  The maximum delay  $M(A)$  is defined recursively as  $M(\sum_{i=1}^n [l_i, u_i].a_i.A_i) = \max\{u_i, M(A_i) \mid i = 1 \dots n\}$ , and  $M(N) = M(A)$  where  $N \stackrel{def}{=} A$ .

Syntactically a timed network agent is a parallel composition of a number of regular timed agents; thus network agents are terms  $(A_1 \mid \dots \mid A_n)$ . Behaviourally, we shall simply assume that a network agent interleaves component actions, whereas components are required to synchronize with respect to delay. Formally, a *network configuration* is a pair  $\langle \bar{A}, \bar{v} \rangle$ , where  $\bar{A} = A_1 \mid \dots \mid A_n$  is a network and  $\bar{v} = (v_1, \dots, v_n)$  is a delay vector, indicating how much each component of the network has been delayed. The transitions between network configurations are given by the rules (6) and (7), where for  $d \in \mathbf{R}_{>0}$ ,  $\bar{v} + d$  denotes the delay vector  $(v_1 + d, \dots, v_n + d)$ , and  $\bar{v}[v_i := 0]$  denotes the delay vector obtained by replacing  $v_i$  with 0 in the vector  $\bar{v}$ :

$$\langle \bar{A}, \bar{v} \rangle \xrightarrow{\epsilon(d)} \langle \bar{A}, \bar{v} + d \rangle \quad (6)$$

$$\frac{\langle A_i, v_i \rangle \xrightarrow{a} \langle A'_i, 0 \rangle}{\langle A_1 \mid \dots \mid A_i \mid \dots \mid A_n, \bar{v} \rangle \xrightarrow{a} \langle A_1 \mid \dots \mid A'_i \mid \dots \mid A_n, \bar{v}[v_i := 0] \rangle} \quad (7)$$

*Example 1.* Consider the network agents  $[0, 2].a \mid [2, 3].b$  and  $nil \mid [2, 3].b$ . Using the inference rules we can infer the following transitions from the initial network configuration:

$$\begin{aligned} A &= \langle [0, 2].a \mid [2, 3].b, (0, 0) \rangle \xrightarrow{\epsilon(1.5)} B = \langle [0, 2].a \mid [2, 3].b, (1.5, 1.5) \rangle \xrightarrow{a} \\ C &= \langle nil \mid [2, 3].b, (0, 1.5) \rangle \xrightarrow{\epsilon(1)} D = \langle nil \mid [2, 3].b, (1, 2.5) \rangle \xrightarrow{b} \langle nil \mid nil, (1, 0) \rangle \end{aligned}$$

□

The specification language used in this presentation is the Extended Timed Modal Logic introduced in [HLY92], here referred to as TL. The logic is an extension of the well-known Hennessy–Milner Logic [HM85], and the formulae of the logic are given by the following abstract syntax:

$$\phi ::= tt \mid \phi_1 \wedge \phi_2 \mid \neg \phi \mid \langle a \rangle \phi \mid \exists [l, u] \phi$$

We shall freely use  $\text{ff}$  as abbreviation for  $\neg\text{tt}$ ,  $\phi_1 \vee \phi_2$  for  $\neg(\neg\phi_1 \wedge \neg\phi_2)$ ,  $[a]\phi$  for  $\neg\langle a \rangle\neg\phi$  and  $\forall[l, u]\phi$  for  $\neg\exists[l, u]\neg\phi$ . For the interpretation of TL we define the satisfaction relation  $\models$  between network configurations  $K$  and TL formulae  $\phi$  inductively as follows:

- i)  $K \models \text{tt} \Leftrightarrow \text{true}$
- ii)  $K \models \phi_1 \wedge \phi_2 \Leftrightarrow K \models \phi_1 \text{ and } K \models \phi_2$
- iii)  $K \models \neg\phi \Leftrightarrow \text{not } K \models \phi$
- iv)  $K \models \langle a \rangle\phi \Leftrightarrow \exists K'. K \xrightarrow{a} K' \text{ and } K' \models \phi$
- v)  $K \models \exists[l, u]\phi \Leftrightarrow \exists K', d. d \in [l, u] \text{ and } K \xrightarrow{\epsilon(d)} K' \text{ and } K' \models \phi$

We shall often write  $\bar{A} \models \phi$  for  $\langle \bar{A}, \bar{0} \rangle \models \phi$ , where  $\bar{0}$  is the (initial) delay vector with all components being 0. In this case we say that the network  $\bar{A}$  satisfies the property  $\phi$ .

*Example 2.* Consider the network  $[0, 2].a \mid [2, 3].b$  from Example 1. Then it is easily seen that this network satisfies the formula  $\forall[1, 2]\langle a \rangle\forall[1, 1]\langle b \rangle\text{tt}$ . To see this simply observe that whenever  $x \in [1, 2]$  we can infer the following transition sequence:

$$\begin{aligned} \langle [0, 2].a \mid [2, 3].b, (x, x) \rangle &\xrightarrow{a} \langle \text{nil} \mid [2, 3].b, (0, x) \rangle \xrightarrow{\epsilon(1)} \\ \langle \text{nil} \mid [2, 3].b, (1, x+1) \rangle &\xrightarrow{b} \end{aligned}$$

□

## 2 Symbolic Processes and Model Checking

Using the by now well-known region technique of Alur and Dill [ACD90] one may obtain an algorithm for model-checking: i.e. an algorithm for deciding whether a given network agent satisfies a TL formula. The region technique provides an abstract interpretation of network agents sufficiently complete that all information necessary for model-checking with respect to TL is maintained. At the same time the abstract interpretation yields a finite-state symbolic representation of networks thus enabling standard algorithmic model-checking techniques to be applied.

For  $t \in \mathbf{R}$ , let  $\lfloor t \rfloor \stackrel{\text{def}}{=} \max\{n \in \mathbf{N} \mid n \leq t\}$  denote the integral part of  $t$ , and let  $\{t\} \stackrel{\text{def}}{=} t - \lfloor t \rfloor$  denote its fractional part. We now recall from [ACD90]:

**Definition 1.** Let  $\bar{m} \in \mathbf{N}^n$  be a delay vector. Then  $\bar{u}, \bar{v} \in \mathbf{R}^n$  are equivalent with respect to  $\bar{m}$ , denoted by  $\bar{u} \doteq \bar{v}$  if

- For each  $i = 1 \dots n$ ,  $u_i > m_i$  iff  $v_i > m_i$ ,
- For each  $i = 1 \dots n$  such that  $u_i \leq m_i$ 
  1.  $\lfloor u_i \rfloor = \lfloor v_i \rfloor$
  2.  $\{u_i\} = 0$  iff  $\{v_i\} = 0$

- For each  $i, j = 1 \dots n$  such that  $u_i \leq m_i$  and  $u_j \leq m_j$ , it is the case that  $\{u_i\} \leq \{u_j\}$  iff  $\{v_i\} \leq \{v_j\}$

Observe that  $\mathbf{R}^n / \doteq$  is finite. For  $\bar{v} \in \mathbf{R}^n$ , we denote by  $[\bar{v}]$  the equivalence class of  $\bar{v}$  under  $\doteq$ . The equivalence classes determined by  $\doteq$  are called *regions*. For model-checking with respect to TL it is important to note that integer delays of equivalent delay vectors are again equivalent. Thus, whenever  $\bar{u} \doteq \bar{v}$  then  $\bar{u} + n \doteq \bar{v} + n$  whenever  $n \in \mathbf{N}$ . Hence, we may without ambiguity write  $[\bar{u}] + n$  for the region  $[\bar{u} + n]$ . In general, it can be shown (see e.g. [LY93]) that two equivalent delay vectors  $\bar{u}$  and  $\bar{v}$  go through the same future regions; i.e.  $\{[\bar{u} + d] \mid d \in R\} = \{[\bar{v} + d] \mid d \in R\}$ . Moreover,  $\bar{u}$  and  $\bar{v}$  also agree on the order in which these regions are visited according to the following notion of successor region: Let  $\gamma = [\bar{v}]$  be a region. Then the *successor* region  $\text{succ}(\gamma)$  is the region  $[\bar{v}']$ , where:

$$v'_i = \begin{cases} v_i + \min\{1 - \{v_j\} \mid j = 1 \dots n\} & \text{if } \forall i. \{v_i\} > 0 \\ v_i + \min\{1 - \{v_j\} \mid j = 1 \dots n\} / 2 & \text{if } \exists i. \{v_i\} = 0 \end{cases}$$

We denote by  $\text{succ}^k(\gamma)$  the region obtained by applying  $\text{succ}$   $k$  times to  $\gamma$ . Now, it may be shown that the future regions from a delay vector  $\bar{u}$  are precisely the regions  $[\bar{u}], \text{succ}^1([\bar{u}]), \text{succ}^2([\bar{u}]), \text{succ}^3([\bar{u}]), \dots$  and that they are visited in this order. For  $\gamma$  a region and  $n$  a natural number we shall denote by  $n_\gamma$  the unique successor number such that  $\gamma + n = \text{succ}^{n_\gamma}(\gamma)$ . Thus, when  $d$  ranges between two integer bounds  $l$  and  $u$  the delay vector  $\bar{v} + d$  resides in regions between  $\text{succ}^{l_{[\bar{v}]}}([\bar{v}])$  and  $\text{succ}^{u_{[\bar{v}]}}([\bar{v}])$ . Also, as agents enable actions within integer bounds, two network configurations with identical network agent and equivalent delay vectors agree on the action transitions they can perform in the sense that if  $\bar{A}$  is a network agent and  $\bar{u} \doteq \bar{v}$  then if  $\langle \bar{A}, \bar{u} \rangle \xrightarrow{a} \langle \bar{A}', \bar{u}' \rangle$ , then also  $\langle \bar{A}, \bar{v} \rangle \xrightarrow{a} \langle \bar{A}', \bar{v}' \rangle$  for some  $\bar{v}'$  such that  $\bar{v}' \doteq \bar{u}'$ . Based on the above observations it can be concluded that network configurations with equivalent delay vectors satisfy the same TL formulae:

**Theorem 2.** *Let  $\bar{A}$  be a network agent,  $\bar{u}, \bar{v}$  two delay vectors, and  $\phi$  a TL formula. Then if  $\bar{u} \doteq \bar{v}$  the following holds:  $\langle \bar{A}, \bar{u} \rangle \models \phi \Leftrightarrow \langle \bar{A}, \bar{v} \rangle \models \phi$*

To obtain the model-checking algorithm we extract a finite-state symbolic semantics of network configurations, by identifying configurations with equivalent delay vectors. Thus *symbolic* network configurations (or simply symbolic states) are pairs of the form  $[\bar{A}, \gamma]$ , where  $\bar{A}$  is a network agent and  $\gamma$  is a  $\doteq$ -equivalence class with respect to the delay vector  $\bar{m} = M(\bar{A}) = (M(A_1), \dots, M(A_n))$ . As network agents have only finitely many sub-terms<sup>4</sup>, and there are only finitely many regions with respect to  $M(\bar{A})$  it follows that the set of symbolic states reachable from  $[\bar{A}, \gamma]$  is finite. The transitions between symbolic states are either

<sup>4</sup> with the usual application of unfolding in the case of recursive definition

un-quantified delay transitions (labelled  $\chi$ ) or action transitions and are defined by the axiom and rule in (8).

$$[\overline{A}, \gamma] \xrightarrow{\chi} [\overline{A}, \text{succ}(\gamma)] \quad \frac{\langle \overline{A}, \overline{v} \rangle \xrightarrow{a} \langle \overline{B}, \overline{u} \rangle}{[\overline{A}, [\overline{v}]] \xrightarrow{a} [\overline{B}, [\overline{u}]]} \quad (8)$$

Moreover, symbolic transitions may be computed effectively. This rests on an effective representation of regions<sup>5</sup> allowing effective computation of a representative of a region as well as effective computation of the region from a delay vector. Also it suffices to consider a single representative  $\overline{v}$  of  $\gamma$  when inferring symbolic action transitions. We may now give an alternative interpretation of TL based on the above symbolic semantics of networks.

- i)  $[\overline{A}, \gamma] \models \text{tt} \quad \Leftrightarrow \text{true}$
- ii)  $[\overline{A}, \gamma] \models \phi_1 \wedge \phi_2 \Leftrightarrow [\overline{A}, \gamma] \models \phi_1 \text{ and } [\overline{A}, \gamma] \models \phi_2$
- iii)  $[\overline{A}, \gamma] \models \neg\phi \quad \Leftrightarrow \text{not } [\overline{A}, \gamma] \models \phi$
- iv)  $[\overline{A}, \gamma] \models \langle a \rangle \phi \quad \Leftrightarrow \exists [\overline{B}, \eta]. [\overline{A}, \gamma] \xrightarrow{a} [\overline{B}, \eta] \text{ and } [\overline{B}, \eta] \models \phi$
- v)  $[\overline{A}, \gamma] \models \exists [l, u] \phi \Leftrightarrow \exists l_\gamma \leq k \leq u_\gamma. [\overline{A}, \text{succ}^k(\gamma)] \models \phi$

Clearly, due to the finite-state nature of the symbolic semantics of networks, the above symbolic interpretation is decidable using classical finite-state model-checking techniques. Moreover, the symbolic interpretation of TL is closely related to the standard interpretation as stated in the following theorem:

**Theorem 3.** *Let  $\overline{A}$  be a network agent,  $\overline{v}$  a delay vector, and  $\phi$  a TL formula. Then the following equivalence holds:  $[\overline{A}, [\overline{v}]] \models \phi \Leftrightarrow \langle \overline{A}, \overline{v} \rangle \models \phi$*

### 3 Symbolic Contexts

We want to decompose logical properties required of a network agent into necessary and sufficient properties of one of its agents. More precisely, for any given regular agents  $A_1, \dots, A_n$  and any given TL formula  $\phi$ , we want to find a formula  $\psi$  such that the following holds:

$$(A_1 \mid \dots \mid A_n \mid X) \models \phi \quad \text{if and only if} \quad X \models \psi \quad (9)$$

Clearly, the component property  $\psi$  will in general depend on the overall property  $\phi$  as well as the agents  $A_1, \dots, A_n$ . In the next section we shall define a *property transformer*  $\mathcal{W}$ , that — given the network agent  $\overline{A} = (A_1 \mid \dots \mid A_n)$  and the property  $\phi$  — will construct a property  $\psi = \mathcal{W}(\overline{A}, \phi)$  satisfying the requirement of (9).

In (9), the property  $\phi$  expresses constraints on transitions of the complete network  $(A_1 \mid \dots \mid A_n \mid X)$ , whereas  $\psi$  constrains transitions of the component agent

<sup>5</sup> The obvious effective representation of a region is as a linear inequation system. An alternative effective representation where each region has a canonical representation is given in [God94].

$X$ . Thus, in order to solve the above decomposition problem we must have a way of interrelating transitions of a network with transitions of one of its components. To achieve this we provide a symbolic operational semantics of the network contexts  $C = (A_1 | \dots | A_n | [ ])$  in terms of *action transducers*. That is, a network context is semantically viewed as an object which consumes actions from its component agent and produces actions for the external environment, thus acting as an interface between the two. Obviously, we expect the new operational semantics of network contexts to be consistent with the existing operational semantics of network agents. That is, if the component agent  $X$  has an  $a$  transition, and the context  $(A_1 | \dots | A_n | [ ])$  can consume this action while producing the action  $b$ , then we expect the combined network  $(A_1 | \dots | A_n | X)$  to have a  $b$ -transition.

The idea of modelling contexts as action transducers has already been pursued for finite state systems [LX90b, LX91]. In our real-time setting we need in addition to take into account the delay of the context agents  $A_1, \dots, A_n$  as well as the delay of the component to be placed in the hole  $[ ]$ . However, as our transductional semantics is intended to provide the basis of an effective transformation of properties, we deal with delays in a symbolic manner using regions. Thus, formally, a symbolic  $n + 1$ -ary network context is a pair of the form:

$$\left[ (A_1 | \dots | A_n | [ ]), [(v_1 \dots v_n, v)] \right]$$

Here  $[(v_1 \dots v_n, v)]$  is an  $n + 1$ -ary region with  $(v_1 \dots v_n)$  giving delay information of  $A_1, \dots, A_n$  and  $v$  providing the delay information of the  $[ ]$ -component. The transductions between symbolic network contexts is given by the axioms and rule (10), (11) and (12). For  $\gamma$  being an  $n + 1$ -ary region  $[(v_1 \dots v_n, v)]$ ,  $\gamma^\downarrow$  denotes the unary region  $[v]$ <sup>6</sup>. For  $\bar{v} = (v_1 \dots v_n)$  an  $n$ -ary delay vector and  $u$  a non-negative real,  $\bar{v}u$  denotes the  $n + 1$ -ary delay vector  $(v_1 \dots v_n, u)$ .

$$\left[ \bar{A} | [ ], \gamma \right] \xrightarrow{x} \left[ \bar{A} | [ ], \text{succ}(\gamma) \right] \text{ if } \text{succ}(\gamma)^\downarrow = \text{succ}(\gamma^\downarrow) \quad (10)$$

$$\left[ \bar{A} | [ ], \gamma \right] \xrightarrow{0} \left[ \bar{A} | [ ], \text{succ}(\gamma) \right] \text{ if } \text{succ}(\gamma)^\downarrow = \gamma^\downarrow \quad (11)$$

$$\left[ \bar{A} | [ ], [\bar{v}u] \right] \xrightarrow{a} \left[ \bar{A} | [ ], [\bar{v}0] \right] \quad \frac{\langle \bar{A}, \bar{v} \rangle \xrightarrow{a} \langle \bar{B}, \bar{w} \rangle}{\left[ \bar{A} | [ ], [\bar{v}u] \right] \xrightarrow{a} \left[ \bar{B} | [ ], [\bar{w}u] \right]} \quad (12)$$

Transductions may be inferred in two ways depending on whether the  $[ ]$ -component “participates” in the transduction or not. Thus for action transductions the axiom in (12) requires the  $[ ]$ -component to perform the  $a$ -action (after which the  $[ ]$ -delay is reset to 0). In the rule in (12), the  $a$ -action is performed entirely by the network context  $\bar{A}$  without any involvement of the  $[ ]$ -component. This is modelled by a transduction using a unique 0-action (i.e.  $0 \notin \mathcal{A}$ ). The symbolic semantics is extended in the obvious way to 0-actions by  $[\bar{A}, \gamma] \xrightarrow{0} [\bar{A}', \gamma']$

<sup>6</sup> In the unary case regions are either integer points  $[n, n]$ , open intervals  $]n, n + 1[$  or open infinite intervals  $]m, \infty[$ , where  $m$  is the maximum delay bound.

if and only if  $\bar{A}' = \bar{A}$  and  $\gamma' = \gamma$ . Delay transductions model progression to a successor region. The two delay transduction axioms reflect that the projected  $[\ ]$ -region may either remain unchanged or change to its (unary) successor region, see axioms (10) and (11). The following Lemma demonstrates that the transductional semantics of contexts does indeed provide the key to relating symbolic transitions of a network and its component:

**Lemma 4.** *Let  $\bar{A} = (A_1 | \dots | A_n)$  be an  $n$ -ary network agent,  $X$  a regular timed agent,  $\gamma$  an  $n+1$ -ary region, and let  $\alpha \in \mathcal{A} \cup \{\chi\}$ . Then  $[\bar{A}|X, \gamma] \xrightarrow{\alpha} [\bar{A}'|X', \gamma']$  if and only if  $[\bar{A}|[\ ], \gamma] \xrightarrow[\beta]{\alpha} [\bar{A}'|[\ ], \gamma']$  and  $[X, \gamma^\downarrow] \xrightarrow{\beta} [X', \gamma'^\downarrow]$  for  $\beta = \alpha$  or  $\beta = 0$ .*

## 4 Contexts as Property Transformers

As shown in the previous Lemma 4, contexts relate *symbolic* transitions of networks with *symbolic* transitions of their components. To facilitate the transformation of logical properties we extend our logic TL with a modality explicitly concerned with symbolic delay transitions ( $\xrightarrow{\chi}$ ). Syntactically, we add the production  $\phi ::= \odot\phi$  to the syntax for formulae: We refer to the extended logic as  $\text{TL}^\odot$ . Formulae with no occurrence of  $\exists[l, u]$ -modalities are called *pure* and the corresponding sublogic is referred to as  $\text{TL}_p^\odot$ . Semantically, we interpret formulae  $\odot\phi$  with respect to (standard) network configurations as well as symbolic network configurations thus extending the two existing interpretations of TL:

$$\begin{aligned} \langle \bar{A}, \bar{u} \rangle \models \odot\phi &\Leftrightarrow \langle \bar{A}, \bar{v} \rangle \models \phi \text{ for some } \bar{v} \in \text{succ}([\bar{u}]) \\ [\bar{A}, \gamma] \models \odot\phi &\Leftrightarrow [\bar{A}, \text{succ}(\gamma)] \models \phi \end{aligned}$$

It is straightforward to show that with these semantic definitions both Theorem 2 and Theorem 3 generalize to  $\text{TL}^\odot$ . Furthermore, for any given network configuration,  $\langle \bar{A}, \bar{v} \rangle$  the original (interval) delay modalities of TL  $\exists[l, u]\phi$  can be expressed using the new  $\odot$ -modality as follows:  $\bigvee \{\odot^k\phi \mid l_{[\bar{v}]} \leq k \leq u_{[\bar{v}]}\}$ . For  $C = [\bar{A}|[\ ], \gamma]$  an  $n+1$ -ary context and  $\phi$  a  $\text{TL}^\odot$ -formula we now define the *transformed formula*  $\mathcal{W}(C, \phi)$  as follows:

$$\begin{aligned} \text{i) } \mathcal{W}(C, \text{tt}) &= \text{tt} & \text{ii) } \mathcal{W}(C, \langle a \rangle\phi) &= \bigvee_{C \xrightarrow[a]{\alpha} C'} \langle a \rangle\mathcal{W}(C', \phi) \vee \bigvee_{C \xrightarrow[0]{\alpha} C'} \mathcal{W}(C', \phi) \\ \text{iii) } \mathcal{W}(C, \phi_1 \wedge \phi_2) &= \mathcal{W}(C, \phi_1) \wedge \mathcal{W}(C, \phi_2) & \text{iv) } \mathcal{W}(C, \neg\phi) &= \neg\mathcal{W}(C, \phi) \\ \text{v) } \mathcal{W}(C, \exists[l, u]\phi) &= \mathcal{W}(C, \bigvee_{k=l_\gamma}^{u_\gamma} \odot^k\phi) & \text{vi) } \mathcal{W}(C, \odot\phi) &= \begin{cases} \mathcal{W}(C', \phi) & \text{if } C \xrightarrow[0]{\chi} C' \\ \odot\mathcal{W}(C', \phi) & \text{if } C \xrightarrow[\chi]{\chi} C' \end{cases} \end{aligned}$$

Note that  $\mathcal{W}(C, \phi)$  is always a pure  $\text{TL}^\odot$ -formula. The following Theorem shows that the transformer  $\mathcal{W}$  does indeed yield the sufficient and necessary requirement to a network component in order that the network itself satisfy a given property:

**Theorem 5.** Let  $C = [\overline{A}][\ ] , \gamma$  be an  $n + 1$ -ary context,  $X$  a regular timed agent and let  $\overline{v}u \in \gamma$ . Then the following equivalences hold:

- i)  $[\overline{A}|X, \gamma] \models \phi \Leftrightarrow [X, \gamma^\dagger] \models \mathcal{W}(C, \phi)$
- ii)  $\langle \overline{A}|X, \overline{v}u \rangle \models \phi \Leftrightarrow \langle X, u \rangle \models \mathcal{W}(C, \phi)$
- iii)  $[\overline{A}|X] \models \phi \Leftrightarrow X \models \mathcal{W}([\overline{A}][\ ] , [\overline{0}]), \phi$

*Example 3.* Using  $\mathcal{W}$  we may now compute the necessary and sufficient requirement to the component  $X$  in order that  $[0, 2].a | X$  satisfies  $\phi = \forall[1, 2]\langle a \rangle \forall[1, 1]\langle b \rangle \text{tt}$ . After some calculations based on the transductional semantics of  $[0, 2].a[\ ]$  we get the following:

$$\begin{aligned} \mathcal{W}\left([0, 2].a[\ ] , [\overline{0}]\right), \phi &= \odot^2\left(\odot^2\langle b \rangle \text{tt} \vee \langle a \rangle \odot^2\langle b \rangle \text{tt}\right) \wedge \\ &\odot^3\left(\odot^2\langle b \rangle \text{tt} \vee \langle a \rangle \odot^2\langle b \rangle \text{tt}\right) \wedge \odot^4\left(\odot^2\langle b \rangle \text{tt} \vee \langle a \rangle \odot^2\langle b \rangle \text{tt}\right) \end{aligned}$$

□

## 5 Direct Model Construction

In this section we provide an algorithm that given a pure  $\text{TL}^\odot$ -formula  $\phi$  will decide whether  $\phi$  is satisfiable by some regular agent. Moreover if  $\phi$  is satisfiable the algorithm will construct a satisfying agent. The technique applied is based on classical tableau methods applied for modal logic (see e.g. [HC68]). To simplify this part of the presentation we use an alternative version of  $\text{TL}_p^\odot$  with no negation but with all dual operators included (i.e.  $\text{ff}$ ,  $\vee$  and  $[a]$ ).

Let  $\Gamma$  be the set of all unary regions of the form  $[n, n]$  and  $]n, n + 1[$ , where  $n \in \mathbf{N}$ . Then a *problem*  $\Pi$  is a finite subset of  $\Gamma \times \text{TL}_p^\odot$ . We say that a problem  $\Pi$  is *satisfiable* if there exists a regular timed agent  $X$  such that  $[X, \gamma] \models \phi$  whenever  $(\gamma, \phi) \in \Pi$ . In this case we call  $X$  a *solution* to  $\Pi$ . It follows from the results of the previous sections that if  $X$  is a solution to an *initial* problem of the form  $\{(\mathcal{O}, \phi)\}$  where  $\mathcal{O} = \{0\}$  then  $X \models \phi$ .

A problem  $\Pi$  is called *simple* if whenever  $(\gamma, \phi) \in \Pi$  then  $\phi$  is of the form  $\langle a \rangle \psi$  or  $[a]\psi$ ; i.e. all outer conjunctions, disjunctions and  $\odot$ -modalities have been resolved. As we shall see in the following it is particularly easy to decide satisfiability of simple problems. However, we first provide a reduction mechanism for transforming problems into simple ones. The reduction relation  $\rightsquigarrow$  between problems is defined as the least relation satisfying the following axioms <sup>7</sup>:

- i)  $\Pi \uplus \{(\gamma, \text{tt})\} \rightsquigarrow \Pi$
- ii)  $\Pi \uplus \{(\gamma, \phi_1 \wedge \phi_2)\} \rightsquigarrow \Pi \cup \{(\gamma, \phi_1)\} \cup \{(\gamma, \phi_2)\}$
- iii)  $\Pi \uplus \{(\gamma, \phi_1 \vee \phi_2)\} \rightsquigarrow \Pi \cup \{(\gamma, \phi_1)\}$
- iv)  $\Pi \uplus \{(\gamma, \phi_1 \vee \phi_2)\} \rightsquigarrow \Pi \cup \{(\gamma, \phi_2)\}$
- v)  $\Pi \uplus \{(\gamma, \odot \phi)\} \rightsquigarrow \Pi \cup \{(\text{succ}(\gamma), \phi)\}$

<sup>7</sup>  $\uplus$  denotes disjoint union of sets.

As the use of  $\rightsquigarrow$  always strictly decreases the total size of the formulae in  $\Pi$  it is clear that any reduction sequence from  $\Pi$  must be finite. In fact any problem determines a finite reduction tree with the leaves being the irreducible reductions of  $\Pi$ ; i.e.  $\Pi'$  is an irreducible reduction of  $\Pi$  if  $\Pi \rightsquigarrow^* \Pi'$  and  $\Pi' \not\rightsquigarrow$ . Now it follows directly from the semantic definition of the various operators of  $\text{TL}_p^\odot$  that there is a close connection between the satisfiability of a problem and its irreducible reductions:

**Lemma 6.** *A problem is satisfiable if and only if one of its irreducible reductions is satisfiable.*

Moreover, it is clear from the definition of  $\rightsquigarrow$  that any irreducible problem is either simple or contains a pair of the form  $(\gamma, \text{ff})$  in which case it is obviously not satisfiable. Thus, we are left with the problem of deciding satisfiability of simple problems. First we define for  $a \in \mathcal{A}$ ,  $\gamma \in \Gamma$  and  $\Pi$  a problem the *projected* problem  $\Pi_a^\gamma$  as follows:  $\Pi_a^\gamma = \{(\mathcal{O}, \phi) \mid (\gamma, [a]\phi) \in \Pi\}$  From the symbolic interpretation of  $[a]\phi$  it follows directly that whenever  $X$  is a solution to  $\Pi$  and  $[X, \gamma] \xrightarrow{a} [X', \mathcal{O}]$ , then  $X'$  is a solution to  $\Pi_a^\gamma$ . Moreover, when  $\gamma = ]n, n+1[$ ,  $X'$  is also a solution to  $\Pi_a^{[n, n]}$  and  $\Pi_a^{[n+1, n+1]}$  as regular agents enable actions within *closed* integer-bound intervals.

**Theorem 7.** *Let  $\Pi$  be a simple problem. Then  $\Pi$  is satisfiable if and only if whenever  $([n, n], \langle a \rangle \phi) \in \Pi$  then (a)  $\{(\mathcal{O}, \phi)\} \cup \Pi_a^{[n, n]}$  is satisfiable, and whenever  $(]n, n+1[, \langle a \rangle \phi) \in \Pi$  then (b)  $\{(\mathcal{O}, \phi)\} \cup \Pi_a^{[n, n]} \cup \Pi_a^{[n, n+1[} \cup \Pi_a^{[n+1, n+1]}$  is satisfiable.*

It now follows from the properties of  $\rightsquigarrow$  and Theorem 7 that satisfiability of problems is decidable: to determine satisfiability of a problem  $\Pi$  first (non-deterministically) reduce it to a simple problem  $\Pi'$  and then use the construction of Theorem 7. This leaves the satisfiability of the problems in (a) and (b) to be settled. However, as these problems all have strictly smaller maximum modal depth than  $\Pi'$  (and  $\Pi$ ) we can apply the method recursively, with termination guaranteed.

## Concluding Remarks

The presentation of this paper has been based on a somewhat simplified setting, and we want here to comment in slightly more detail on how our results extend.

The logic TL considered may be extended with constructs for defining properties recursively. The symbolic interpretation of TL extends easily to this recursive extension, thus providing the basis for decidability of model-checking. As for transforming recursive properties the techniques given in [LX90b, LX91] can be directly applied. Our direct model-construction method extends to maximal recursively defined properties using the techniques of [JL93].

The notion of parallel composition considered in this paper is simply that of interleaving of actions. However, our results extend to a variety of parallel compositions via parameterization on a *synchronization function* as studied in [HL89]. Thus, we may consider *parameterized* network of the form  $(A_1, \dots, A_n)|_f$ , where  $f$  is a synchronization (partial) function of type  $(\mathcal{A} \cup \{0\})^n \hookrightarrow \mathcal{A}$ . The use of the special no-action 0 enables the modelling of synchronizations where only some components participate. Also, the partiality of  $f$  enables synchronization of certain combinations of actions to be disallowed.

In this presentation we have not yet considered implicit process algebraic specifications; i.e. specifications of the form:

$$(A_1 \mid \dots \mid A_n \mid X) \equiv B \quad (13)$$

where  $B$  is a regular timed agent and  $\equiv$  is some abstracting equivalence (timed bisimilarity, say). However, (13) may easily be transformed into an equivalent logical implicit specification by using a *characteristic formula*  $\phi_B$  for  $B$ ; i.e. a formula such that  $A \equiv B$  if and only if  $A \models \phi_B$ . Both for timed and time-abstracting bisimilarity such characteristic formulae can be effectively constructed. Future work includes extension of our method to implicit specifications for arbitrary  $n$ -clock automata.

## References

- [ACD90] R. Alur, C. Courcoubetis, and D. Dill. Model-checking for Real-Time Systems. In *Proceedings of Logic in Computer Science*, pages 414–425. IEEE Computer Society Press, 1990.
- [AD94] R. Alur and D. Dill. Automata for Modelling Real-Time Systems. *Theoretical Computer Science*, 126(2):183–236, April 1994.
- [AH89] R. Alur and T. A. Henzinger. A Really Temporal Logic. In *Proceeding of IEEE Symp. on Foundations of Computer Science*, Foundations of Computer Science, 1989.
- [Cer92] Karlis Cerans. Decidability of bisimulation equivalences for parallel timer processes. In *Proceedings of CAV'92*, volume 663 of *Lecture Notes in Computer Science*, Springer Verlag, Berlin, 1992. Springer Verlag.
- [CGL93] K. Cerans, J. C. Godskesen, and K. G. Larsen. Timed modal specifications — theory and tools. In *Proceedings of 5th International Conference on Computer Aided Verification*, volume 697 of *Lecture Notes in Computer Science*, 1993.
- [God94] J. C. Godskesen. *Timed Modal Specifications — A theory for verification of real-time concurrent systems*. PhD thesis, Aalborg University, 1994.
- [HC68] G. E. Hughes and M. J. Cresswell. *An Introduction to Modal Logic*. Methuen and Co., 1968.
- [HL89] H. Hüttel and K. G. Larsen. The Use of Static Constructs in a Modal Process Logic. In *Logic at Botik'89.*, volume 363 of *Lecture Notes in Computer Science*, 1989.
- [HLY92] U. Holmer, K.G. Larsen, and W. Yi. Decidability of bisimulation equivalence between regular timed processes. In *Proceedings of CAV'91*, volume 575 of *Lecture Notes in Computer Science*, Springer Verlag, Berlin, 1992.

- [HM85] M. Hennessy and R. Milner. Algebraic laws for nondeterminism and concurrency. *Journal of the Association for Computing Machinery*, pages 137–161, 1985.
- [HNSY92] T. A. Henzinger, Z. Nicollin, J. Sifakis, and S. Yovine. Symbolic model checking for real-time systems. In *Logic in Computer Science*, 1992.
- [JLJL93] O.H. Jensen, J.T. Lang, C. Jeppesen, and K.G. Larsen. Model construction for implicit specifications in modal logic. In *Proceedings of 4th International Conference on Concurrency Theory*, volume 715 of *Lecture Notes in Computer Science*, 1993.
- [LQ90] P. Lewis and H. Qin. Factorization of finite state machines under observational equivalence. *Lecture Notes in Computer Science, Springer Verlag*, 458, 1990.
- [LS92] K.G. Larsen and A. Skou. Compositional verification of probabilistic processes. In *Proceedings of CONCUR'92. To appear in Lecture Notes in Computer Science.*, 1992.
- [LX90a] K. G. Larsen and L. Xinxin. Equation Solving Using Modal Transition systems. In *Proceedings of Logic in Computer Science*, 1990.
- [LX90b] K.G. Larsen and L. Xinxin. Compositionality through an operational semantics of contexts. In *proceedings of ICALP'90*, volume 443 of *Lecture Notes in Computer Science*, 1990.
- [LX91] K.G. Larsen and L. Xinxin. Compositionality through an operational semantics of contexts. *Journal of Logic and Computation*, 1(6):761–795, 1991.
- [LY93] K. G. Larsen and W. Yi. Time Abstracted Bisimulation: Implicit Specifications and Decidability. In *Proceedings of MFPS*, 1993.
- [NRJV90] X. Nicollin, J. L. Richierand, J.Sifakis, and J. Voiron. ATP: an algebra for timed processes,. In *Proceedings of the IFIP TC 2 Working Conference on Programming Concepts and Methods*, IFIP, 1990.
- [NSY91] X. Nicollin, J. Sifakis, and S. Yovine. From ATP to Timed Graphs and Hybrid Systems. volume 600 of *Lecture Notes in Computer Science*, 1991. In *Real-Time: Theory in Practice*.
- [Par89] J. Parrow. Submodule construction as equation solving in CCS. *Theoretical Computer Science*, 68, 1989.
- [Shi86] M.W. Shields. A note on the simple interface equation. Technical Report SE/079/1, University of Kent at Canterbury, Electronic Engineering Laboratories University, June 1986.
- [Yi90] W. Yi. Real-Time Behaviour of Asynchronous Agents. In *Theories of Concurrency: Unification and Extension*, volume 458 of *Lecture Notes in Computer Science*, 1990.