Compositional Model Checking of Real Time Systems

François Laroussinie
Kim G. Larsen
Compositional Model Checking
of Real Time Systems *

François Laroussinie           Kim G. Larsen
BRICS†, Aalborg Univ., Denmark†                 BRICS, Aalborg Univ., Denmark

Abstract

A major problem in applying model checking to finite-state systems is the potential combinatorial explosion of the state space arising from parallel composition. Solutions of this problem have been attempted for practical applications using a variety of techniques. Recent work by Andersen [And95] proposes a very promising compositional model checking technique, which has experimentally been shown to improve results obtained using Binary Decision Diagrams.

In this paper we make Andersen’s technique applicable to systems described by networks of timed automata. We present a quotient construction, which allows timed automata components to be gradually moved from the network expression into the specification. The intermediate specifications are kept small using minimization heuristics suggested by Andersen. The potential of the combined technique is demonstrated using a prototype implemented in CAML.

---

*This work has been supported by the European Communities under CONCUR2, BRA 7166
†Basic Research in Computer Science, Centre of the Danish National Research Foundation.
‡Dept. of Computer Science, Aalborg University, Fredrik Bajers Væj 7-E, DK-9220 Aalborg, Denmark, (email: {fl,kgl}@iesd.auc.dk) fax: (45) 98.15.81.29
## Contents

1. Introduction .................................................. 3  
2. Timed Transition Systems and Automata .................. 4  
3. Timed Logic .................................................... 7  
4. Regions .......................................................... 9  
5. Quotienting .................................................... 12  
6. Minimizations .................................................. 15  
7. Conclusion ..................................................... 17  

A. Proof of Theorem 2 ........................................... 20
1 Introduction

Within the last decade model checking has turned out to be a useful technique for verifying temporal properties of finite state systems. Efficient model checking algorithms for finite state systems have been obtained with respect to a number of logics, and in the last few years, model checking techniques have been extended to real-time systems and logics using the region technique of Alur, Courcoubetis and Dill [ACD90]. However, the major problem in applying model checking even to moderate-size systems is the potential combinatorial explosion of the state space arising from parallel composition. For real-time systems an additional explosion is induced in the number of regions. In order to avoid this problem algorithms have been sought that avoid exhaustive state (region) space exploration, either by symbolic representation of the states space such as in [HINSY92] and in the use of Binary Decision Diagrams [BCM+90], by application of partial order methods [GW91, Val90] which suppress unnecessary interleavings of transitions, or by application of abstractions and symmetries [CFJ93, CGL92, EJ93].

So far the most successful results for larger systems have been obtained using the heuristics of Binary Decision Diagrams. However, recent work by Andersen [And95] introduces a new very promising heuristic model checking technique for finite state systems, for which experimental results on specific examples 1 shows an improvement compared with Binary Decision Diagrams. The technique is based on compositional proof rules for parallel composition.

Our aim of this paper is to make this new successful (compositional) model checking technique by Andersen [And95] applicable to real-time systems. For example, consider the following typical model checking problem

\[(S_1 | \ldots | S_n) \models \varphi\]

where the $S_i$:s are real-time systems (described as timed automata [AD94]). We want to verify that the parallel composition of these timed automata satisfies the formula $\varphi$ without having to construct the complete state (region) space of the process $(S_1 | \ldots | S_n)$. We will avoid this complete construction by removing the components $S_i$ one by one while simultaneously transforming the formula accordingly. Thus, when removing the component $S_n$ we will transform the formula $\varphi$ into the quotient formula $\varphi / S_n$ such that

\[(S_1 | \ldots | S_n) \models \varphi \text{ if and only if } (S_1 | \ldots | S_{n-1}) \models \varphi / S_n \quad (1)\]

Now clearly, if the quotient is not much larger than the original formula we have succeeded in simplifying the problem. Repeated application of quotienting yields

\[(S_1 | \ldots | S_n) \models \varphi \text{ if and only if } 1 \models \varphi / S_n / S_{n-1} / \ldots / S_1 \quad (2)\]

where 1 is the unit with respect to parallel composition.

1using a prototype implementation in Standard ML
For finite state systems the quotient with respect to parallel composition is an immediate application of work on compositional reasoning due to Andersen, Larsen, Stirling, Winskel and Xinxin [Lar86, LX91, AW92, ASW94]. However, based on these ideas alone, (2) provides no solution to the problem as the explosion will now occur in the size of the final quotient formula instead. The crucial and experimentally “verified” observation by Andersen was that each quotienting should be followed by a minimization of the formula based on a collection of few, efficiently implementable strategies.

In this paper we provide the basis for and make an initial experimental investigation of the application of Andersen’s compositional model checking technique for real–time systems (timed automata). In particular,

- We give an effective construction of the quotient formula \( \varphi / S \) satisfying the requirement of (1) for \( \varphi \) a formula of the timed logic \( L_\nu \) introduced in [LLW95] and \( S \) a real–time system given in terms of a timed automaton;
- Based on a prototype implemented in CAML we make an experimental investigation of the above quotient construction combined with (some of) the minimization heuristics of Andersen. In the examples we consider the minimized quotient formulas have been subject to dramatic reductions and are comparable in size to the original formulas. Thus, we may expect compositional model checking to be successful also for real–time systems.

The remainder of this paper is organized as follows: in the next section we give a short presentation of the notion of timed automata and composition used in this paper; in section 3, the logic \( L_\nu \) is shortly presented, and in section 4 we review the region technique by Alur, Courcoubetis and Dill [ACD90]. Section 5 presents the quotient construction, whereas section 6 presents and investigates the consequences of minimization.

## 2 Timed Transition Systems and Automata

Let \( \mathcal{A} \) be a finite set of actions ranged over by \( a, b, c, \ldots \). We denote by \( \mathbb{N} \) the set of natural numbers and by \( \mathbb{R} \) the set of non–negative real numbers. \( \mathcal{D} \) denotes the set of delay actions \( \{\varepsilon(d)\mid d \in \mathbb{R}\} \), and \( \mathcal{L} \) denotes the union \( \mathcal{A} \cup \mathcal{D} \).

**Definition 1** A timed transition system over \( \mathcal{A} \) is a tuple \( \mathcal{S} = (S, s_0, \rightarrow) \), where \( S \) is a set of states, \( s_0 \) is the initial state and \( \rightarrow \subseteq S \times \mathcal{L} \times S \) is a transition relation. We require that for any \( s \in S \) and \( d \in \mathbb{R} \), there exists a (unique) state \( s^d \) such that \( s \xrightarrow{\varepsilon(d)} s^d \). Moreover \( (s^d)^e = s^{d+e} \).

\(^2\)The existence of \( s^d \) corresponds to transition liveness, its unicity corresponds to time-determinism and the property \( (s^d)^e = s^{d+e} \) corresponds to time-continuity (or time-additivity) in [Yi90].
Obviously, we may apply the standard notion of bisimulation [Par81, Mil89] to timed transition systems. For \( S = \langle S, s_0, \rightarrow \rangle \) a timed transition system, strong (timed) bisimulation \( \sim \) is defined as the largest symmetric relation over \( S \) such that whenever \( s_1 \sim s_2 \) and \( \ell \in \mathcal{A} \cup \mathcal{D} \) then

- Whenever \( s_1 \xrightarrow{\ell} s_1' \) then there exists \( s_2' \) such that \( s_2 \xrightarrow{\ell} s_2' \) and \( s_1' \sim s_2' \).

We may compare states from different timed transition systems by considering their disjoint union. Two timed transition systems \( S_1 \) and \( S_2 \) are said to be strong (timed) bisimilar, written \( S_1 \sim S_2 \), in case their initial states are strong bisimilar.

In order to study compositionality problems we introduce a parallel composition between timed transition systems. Following [HL89] we suggest a composition parameterized with a synchronization function generalizing a large range of existing notions of parallel compositions. A synchronization function \( f \) is a partial function \( (\mathcal{A} \cup \{0\}) \times (\mathcal{A} \cup \{0\}) \rightarrow \mathcal{A} \), where 0 denotes a distinguished no-action symbol \(^3\). Now, let \( \mathcal{S}_i = \langle S_i, s_i,0, \rightarrow_i \rangle \), \( i = 1,2 \), be two timed transition systems and let \( f \) be a synchronization function. Then the parallel composition \( \mathcal{S}_1 \parallel \mathcal{S}_2 \) is the timed transition system \( \langle S, s_0, \rightarrow \rangle \), where \( s_1 \parallel s_2 \in S \) whenever \( s_1 \in S_1 \) and \( s_2 \in S_2 \), \( s_0 = s_1,0 \parallel s_2,0 \), and \( \rightarrow \) is given by the rule \(^4\):

\[
\frac{s_1 \xrightarrow{a} s_1', \ s_2 \xrightarrow{b} s_2'}{s_1 \parallel s_2 \xrightarrow{c} s_1' \parallel s_2'}
\]

and the requirement that for any \( d \in \mathbb{R} \), \((s_1 \parallel s_2)^d = (s_1^d \parallel s_2^d)\).

Syntactically, timed transition systems are described by timed automata [AD94], which are finite automata extended with a finite collection of real-valued clocks \(^5\). If \( C \) is a set of clocks, \( \mathcal{B}(C) \) denotes the set of formulas built using boolean connectives over atomic formulas of the form \( x \leq m \), \( m \leq x \), \( x \leq y + m \) and \( y + m \leq x \) with \( x,y \in C \) and \( m \in \mathbb{N} \). Moreover \( \mathcal{B}_M(C) \) denotes the subset of \( \mathcal{B}(C) \) with no constant greater than \( M \).

**Definition 2** A timed automaton \( A \) over \( \mathcal{A} \) is a tuple \( \langle N, \eta_0, C, E \rangle \) where \( N \) is a finite set of nodes, \( \eta_0 \) is the initial node, \( C \) is a finite set of clocks, and \( E \subseteq N \times N \times \mathcal{A} \times \mathcal{C} \times \mathcal{B}(C) \) corresponds to the set of edges. \( e = \langle \eta, \eta', a, r, b \rangle \in E \) represents an edge from the node \( \eta \) to the node \( \eta' \) with action \( a, r \) denoting the set of clocks to be reset and \( b \) is the enabling condition over the clocks of \( A \).

**Example 1** Consider the automata \( A_d, B_d \) and \( C_d,e \) in Figure 1 \((d,e \in \mathbb{N})\). The automaton \( C_d,e \) has four nodes, \( \mu_0, \mu_1, \mu_2 \) and \( \mu_3 \), two clocks \( x \) and \( y \), and three edges. The edge between \( \mu_1 \) and \( \mu_2 \) has \( b \) as action, \( \{x,y\} \) as reset set and the enabling condition for the edge is \( y > d \). \( \square \)

---

\(^3\) We extend the transition relation of a timed transition system such that \( s \xrightarrow{\ell} s' \) iff \( s = s' \).

\(^4\) \( f(a, b) \approx c \) holds if \( f \) is defined for the pair \((a, b)\) and the result is \( c \).

\(^5\) Timed transition systems may alternatively be described using timed process calculi.
Informally, the system starts at node $\eta_0$ with all its clocks initialized to 0. The values of the clocks increase synchronously with time. At any time, the automaton whose current node is $\eta$ can change node by following an edge $(\eta, \eta', a, r, b) \in E$ provided the current values of the clocks satisfy $b$. With this transition the clocks in $r$ get reset to 0.

Formally a time assignment $v$ for $C$ is a function from $C$ to $\mathbb{R}$. We denote by $\mathbb{R}^C$ the set of time assignments for $C$. For $v \in \mathbb{R}^C$, $x \in C$ and $d \in \mathbb{R}$, $v + d$ denotes the time assignment which maps each clock $x$ in $C$ to the value $v(x) + d$. For $C' \subseteq C$, $[C' \rightarrow 0]v$ denotes the assignment for $C$ which maps each clock in $C'$ to the value 0 and agrees with $v$ over $C \setminus C'$. Whenever $v \in \mathbb{R}^C$, $u \in \mathbb{R}^K$ and $C$ and $K$ are disjoint $vu$ denotes the time assignment over $C \cup K$ such that $(vu)(x) = v(x)$ if $x \in C$ and $(vu)(x) = u(x)$ if $x \in K$. Given a condition $b \in \mathcal{B}(C)$ and a time assignment $v \in \mathbb{R}^C$, $b(v)$ is a boolean value describing whether $b$ is satisfied by $v$ or not. Finally a $k$-clock automaton is a timed automata $(N, \eta_0, C, E)$ such that $|C| = k$.

A state of an automaton $A$ is a pair $(\eta, v)$ where $\eta$ is a node of $A$ and $v$ a time assignment for $C$. The initial state of $A$ is $(\eta_0, v_0)$ where $v_0$ is the time mapping all clocks in $C$ to 0. The semantics of $A$ is given by the timed transition system $\mathcal{S}_A = \langle S_A, \sigma_0, \rightarrow_A \rangle$, where $S_A$ is the set of states of $A$, $\sigma_0$ is the initial state $(\eta_0, v_0)$, and $\rightarrow_A$ is the transition relation defined as follows:

$$ (\eta, v) \xrightarrow{a} (\eta', v') \quad \text{iff} \quad \exists r, b. \ (\eta, \eta', a, r, b) \in E \land b(v) \land v' = [r \rightarrow 0]v $$

$$ (\eta, v) \xrightarrow{d} (\eta', v') \quad \text{iff} \quad \eta = \eta' \land v' = v + d $$

Example 2 Reconsider the automaton $C_{d,e}$ of Figure 1. The coordinate systems in Figure 2 indicates (some of) the states of $C_{d,e}$. Each point of the coordinate systems represents a unique time assignment, with the coordinate systems representing states involving the nodes $\mu_0, \mu_1$, and $\mu_2$ respectively. We
have indicated the following typical transition sequence (where \( f \geq 0, d' > d \) and \( e' \geq e \)):

\[
(\mu_0, (0,0)) \xrightarrow{a(f)} (\mu_0, (f,f)) \xrightarrow{a} (\mu_1, (f,0)) \xrightarrow{e(d')} (\mu_1, (f + d', d')) \\
\text{and} \quad (\mu_1, (f + d', d')) \xrightarrow{b} (\mu_2, (0,0)) \xrightarrow{e'(e')} (\mu_2, (e', e')) \xrightarrow{c} 
\]

\[\square\]

Parallel composition may now be extended to timed automata in the obvious way: for two timed automata \( A \) and \( B \) and a synchronization function \( f \), the parallel composition \( A \upharpoonright f B \) denotes the timed transition system \( S_A \upharpoonright f S_B \). For two automata \( A \) and \( B \) and a synchronization function \( f \) one may effectively construct an automaton \( A \otimes_j B \) such that \( S_A \upharpoonright f S_B \) is strong bisimilar to \( S_A \upharpoonright f S_B \). The nodes of \( A \otimes_j B \) is simply the product of \( A \)'s and \( B \)'s nodes, the set of clocks is the (disjoint) union of \( A \)'s and \( B \)'s clocks, and the edges are based on synchronizable \( A \) and \( B \) edges with enabling conditions conjuncted and reset–sets unioned.

**Example 3** Let \( f \) be the synchronization function completely specified by \( f(a,0) = a, f(b,b) = b \) and \( f(0,c) = c \). Then the automaton \( C_{d,e} \) in Figure 1 is isomorphic to the part of \( B_d \otimes_j A_e \) which is reachable from \((\rho_0, \eta_0)\).

\[\square\]

### 3 Timed Logic

We consider a dense–time logic \( L_\mu \) with clocks and recursion. This logic may be seen as a certain fragment \(^6\) of the \( \mu \)-calculus \( T_\mu \) presented in [HNSY92]. In [LLW95] it has been shown that this logic is sufficiently expressive that for any timed automaton one may construct a single characteristic formula uniquely characterizing the automaton up to timed bisimilarity. Also, decidability of a satisfiability \(^7\) problem is demonstrated.

\(^6\)allowing only maximal recursion and using a slightly different notion of model

\(^7\)Bounded in the number of clocks and maximal constant allowed in the satisfying automata.
\[ \langle s, u \rangle \models_D \text{ tt} \quad \Rightarrow \quad \text{true} \]
\[ \langle s, u \rangle \models_D \text{ ff} \quad \Rightarrow \quad \text{false} \]
\[ \langle s, u \rangle \models_D \varphi \land \psi \quad \Rightarrow \quad \langle s, u \rangle \models_D \varphi \quad \text{and} \quad \langle s, u \rangle \models_D \psi \]
\[ \langle s, u \rangle \models_D \exists \varphi \quad \Rightarrow \quad \exists \delta \in \mathbb{R} \cdot \langle s', u + \delta \rangle \models_D \varphi \]
\[ \langle s, u \rangle \models_D \varphi \quad \Rightarrow \quad \exists s'. \ s \xrightarrow{a} s' \quad \text{and} \quad \langle s', u \rangle \models_D \varphi \]
\[ \langle s, u \rangle \models_D x + m \sim y + n \quad \Rightarrow \quad u(x) + m \sim u(y) + n \]
\[ \langle s, u \rangle \models_D x \in \varphi \quad \Rightarrow \quad \langle s, u' \rangle \models_D \varphi \quad \text{where} \quad u' = \{ \{ x \} \rightarrow 0 \} u \]
\[ \langle s, u \rangle \models_D D(Z) \quad \Rightarrow \quad \langle s, u \rangle \models_D D(Z) \]

Table 1: Definition of satisfiability.

**Definition 3** Let \( K \) a finite set of clocks, \( \text{ld} \) a set of identifiers and \( k \) an integer. The set \( \text{L}_\varphi \) of formulae over \( K, \text{ld} \) and \( k \) is generated by the abstract syntax with \( \varphi \) and \( \psi \) ranging over \( \text{L}_\varphi \):

\[
\varphi ::= \text{tt} \mid \text{ff} \mid \varphi \land \psi \mid \varphi \lor \psi \mid \exists \varphi \mid \forall \varphi \mid \langle a \rangle \varphi \mid [a] \varphi \\
\mid x \in \varphi \mid x + n \sim y + m \mid Z
\]

where \( a \in A; x, y \in K; n, m \in \{0, 1, \ldots, k\}; \sim \in \{=, <, \leq, >, \geq\} \) and \( Z \in \text{ld} \).

The meaning of the identifiers is specified by a declaration \( D \) assigning a formula of \( \text{L}_\varphi \) to each identifier. When \( D \) is understood we write \( Z \overset{\text{def}}{=} \varphi \) for \( D(Z) = \varphi \). The \( K \) clocks are called formula clocks and a formula \( \varphi \) is said to be **closed** if every formula clock \( x \) occurring in \( \varphi \) is in the scope of an "\( x \text{ in} \ldots \)" operator.

Given a timed transition system \( \mathcal{S} \) we interpret the \( \text{L}_\varphi \) formulas over an **extended state** \( \langle s, u \rangle \), where \( s \) is a state of \( \mathcal{S} \) and \( u \) is a time assignment for \( K \). Informally, \( \exists \varphi \) holds in an extended state if there is a delay transition leading to an extended state satisfying \( \varphi \). Thus \( \exists \) denotes existential quantification over (arbitrary) delay transitions. Similarly, \( \forall \) denotes universal quantification over delay transitions, and \( \langle a \rangle \) (resp. \( [a] \)) denotes existential (resp. universal) quantification over \( a \)-transitions. The formula \( (x \in \varphi) \) initializes the formula clock \( x \) to 0; i.e. an extended state satisfies the formula in case the modified state with \( x \) being reset to 0 satisfies \( \varphi \). Introduced formula clocks are used by formulas of the type \( (x + n \sim y + m) \), which is satisfied by an extended state provided the values of the named formula clocks satisfies the required relationship. Finally, an extended state satisfies an identifier \( Z \) if it satisfies the corresponding declaration (or definition) \( D(Z) \). Formally, the satisfaction relation \( \models_D \) between extended states and formulas is defined as the largest relation satisfying the implications of Table 1. We have left out the cases for \( \forall, [a] \) and \( \exists \) as they are immediate duals.

Any relation satisfying the implications in Table 1 is called a **satisfiability** relation. It follows from standard fixpoint theory [Tar55] that \( \models_D \) is the union of all satisfiability relations and that the implications in Table 1 in fact are bi-implications for \( \models_D \). We say that \( \mathcal{S} \) satisfies a closed \( \text{L}_\varphi \) formula \( \varphi \) and write
$S \models \varphi$ when $\langle s_0, u \rangle \models_{D} \varphi$ for any $u$. Note that if $\varphi$ is closed, then $\langle s, u \rangle \models_{D} \varphi$ iff $\langle s, u' \rangle \models_{D} \varphi$ for any $u, u' \in R^K$. Similarly, we say that a timed automaton $A$ satisfies a closed $L_{\nu}$ formula $\varphi$ in case $S_A \models_{D} \varphi$. We write $A \models_{D} \varphi$ in this case.

**Example 4** Consider the following declaration $\mathcal{F}$ of the identifiers $X_g$ and $Z_g$ where $g \in \mathbb{N}$.

$$\mathcal{F} = \left\{ X_g \overset{\text{def}}{=} \left[ y \in Z_g \right], \ Z_g \overset{\text{def}}{=} (y > g) \lor \left( [c] f \land [a] Z_g \land [b] Z_g \land \forall Z_g \right) \right\}$$

That is $X_g$ expresses the property that the accumulated time between an initial $a$– and a following $c$–transition must exceed $g$. Thus for any transition sequence of the form (where $\alpha_i \in \{a, b\}$):

$$s_0 \xrightarrow{a} t_0 \xrightarrow{\epsilon(d_1)} s_1 \xrightarrow{c_1} t_1 \xrightarrow{\epsilon(d_2)} s_2 \xrightarrow{a_2} \cdots \xrightarrow{\epsilon(d_n)} s_n \xrightarrow{c}$$

$\sum d_i > g$. Now, reconsider the automata $A_e$, $B_d$ and $C_{d,e}$ of Figure 1 and Examples 1 and 2. Then it may be argued that $C_{d,e} \models_{\mathcal{F}} X_{d+e}$ and (consequently), that $B_d \models_{\mathcal{F}} A_e$.

Combining the parameterized parallel composition with $L_{\nu}$ we are able to express timed bisimilarity between timed transition systems as a single formula. This provides a timed extension of a similar characterization of strong bisimilarity for finite state systems [And94]: First we close the action set $\mathcal{A}$ under tagging; i.e. $\mathcal{A}' = \mathcal{A} \cup \mathcal{A} \times \{l\} \cup \mathcal{A} \times \{r\}$. Now consider the ‘interleaving’ synchronization function $h$ over $\mathcal{A}'$ completely defined by $h(a, 0) = a$, and $h(0, a) = a_r$ where $a \in \mathcal{A}$ (i.e. $h$ is undefined for all other pairs). Consider the following declaration $\mathcal{E}$ of the identifier $\mathcal{Z}$:

$$\mathcal{Z} \overset{\text{def}}{=} \bigwedge_{a \in \mathcal{A}} \left( [a]_l (a_r)_l \mathcal{Z} \land (a_r)_l (a)_l \mathcal{Z} \right) \land \forall \mathcal{Z}$$

Then timed bisimilarity between timed transition systems is characterized as follows $^8$:

**Theorem 1** Let $S$ be a timed transition system over $\mathcal{A}$, and let $s_1, s_2$ be states of $S$. Then $s_1 \sim s_2$ if and only if $s_1 \models_{\mathcal{E}} s_2 \models_{\mathcal{E}} \mathcal{Z}$.

4 Regions

The model-checking problem for $L_{\nu}$ consists in deciding if a given timed automata $A$ satisfies a given specification $\varphi$ in $L_{\nu}$. In [LLW95] this problem has been shown decidable using the region technique of Alur and Dill [AD94, ACD90]. The region technique provides an abstract interpretation of timed automata sufficiently complete that all information necessary for model–checking

$^8$It may be shown that the speed relation of [FT91] is characterized in a similar manner by $Y$ defined recursively by $Y \overset{\text{def}}{=} \bigwedge_{a \in \mathcal{A}} ([a]_l (a_r)_l Y \land (a_r)_l (a)_l Y) \land \forall Y$. 

9
with respect to $L_\nu$ is maintained, yet finitary and thus enabling standard algorithmic model-checking techniques to be applied.

The basic idea is that, given a timed automaton $A$, two states $(\eta, v_1)$ and $(\eta, v_2)$ which are close enough with respect to their clocks values (we will say that $v_1$ and $v_2$ are in the same region) can perform the same actions, and two extended states $((\eta, v_1), u_1)$ and $((\eta, v_2), u_2)$ where $v_1 u_1$ and $v_2 u_2$ are in the same region, satisfy the same $L_\nu$ formulas \(^9\). The notion of region is defined as an equivalence class of a relation over time assignments [ACD90] \(^10\). First, for $t \in \mathbb{R}$, let $\lfloor t \rfloor \overset{\text{def}}{=} \max \{ n \in \mathbb{N} \mid n \leq t \}$ denote the integral part of $t$, and let $\{ t \} \overset{\text{def}}{=} t - \lfloor t \rfloor$ denote its fractional part. Moreover we have: $\lfloor t \rfloor \overset{\text{def}}{=} \min \{ n \in \mathbb{N} \mid t \leq n \}$.

**Definition 4** Let $k \in \mathbb{N}$ and let $C$ be a set of clocks. Then $u, u' \in \mathbb{R}^C$ are equivalent with respect to $k$, denoted by $u \equiv u'$ iff:

i) $\forall x \in C. \ u(x) > k \iff u'(x) > k$

ii) $\forall x \in C \ s.t. \ u(x) \leq k. \ \lfloor u(x) \rfloor = \lfloor u'(x) \rfloor \text{ and } \{ u(x) \} = 0 \Leftrightarrow \{ u'(x) \} = 0$

iii) $\forall x, y \in C. \ u(x) - u(y) > k \iff u'(x) - u'(y) > k$

iv) $\forall x, y \in C \ s.t. \ 0 \leq u(x) - u(y) \leq k. \ \lfloor u(x) - u(y) \rfloor = \lfloor u'(x) - u'(y) \rfloor \text{ and } \{ u(x) - u(y) \} = 0 \Leftrightarrow \{ u'(x) - u'(y) \} = 0$

The equivalence classes under $\equiv$ are called regions, and $[u]$ denotes the region which contains the time assignment $u$. $R^C_k$ denotes the set of all regions for a set $C$ of clocks and the maximal constant $k$. From a decision point of view it is important to note that $R^C_k$ is finite.

Note that for any condition $b$ in $B(C)$ with no constant greater than $k$, we have $b(u) \Leftrightarrow b(u')$, whenever $u$ and $u'$ belong to the same region in $R^C_k$. Thus for a region $\gamma \in R^C_k$, we can define $b(\gamma)$ as the truth value of $b(u)$ for any $u$ in $\gamma$. Conversely given a region $\gamma$, we can easily build a formula of $B(C)$, called $\beta(\gamma)$, such that $\beta(\gamma)(u) = \top$ iff $u \in \gamma$ \(^11\). Thus, given a region $\gamma'$, $\beta(\gamma)(\gamma')$ is mapped to the value $\top$ precisely when $\gamma = \gamma'$. Finally, note that $\beta(\gamma)$ itself can be viewed as an $L_\nu$ formula.

Given a region $[u]$ in $R^C_k$ and $C' \subseteq C$ we define the following reset operator: $[C' \to 0][u] = [[C' \to 0]|u]$. Moreover, for a region $[u]$, we define the successor region (denoted by $\text{succ}(\{u\})$) as the region $[u']$, where:

$$u'(x) = \begin{cases} u(x) + f & \forall x \in C. \ u(x) > k \lor \{ u(x) \} \neq 0 \\ u(x) + f/2 & \exists x \in C. \ u(x) \leq k \land \{ u(x) \} = 0 \end{cases}$$

where $f = \min\{1 - \{u(x)\} \mid u(x) \leq k\} \overset{12}{=}$. Informally the change from $\gamma$ to $\text{succ}(\gamma)$ correspond to the minimal elapse of time which can modify the enabled actions of the current state.

\(^9\)Without loss of generality, we will in all the following assume that that the formula clock set $K$ and the automaton clock set $C$ are disjoint.

\(^10\)The notion of region used in the present paper is slightly more refined.

\(^11\)An obvious way of building $\beta(\gamma)$ is to consider the conjunction of all $B(C, k)$ formulas satisfied by $\gamma$, where $B(C, k)$ denotes the finite set (modulo boolean reductions) of $B(C)$ formulas with no constant greater than $k$.

\(^12\)if this set is empty, then $f = 0$.
We denote by \( \gamma^l \) the \( l^{th} \) successor region of \( \gamma \) (i.e. \( \gamma^l = \text{succ}(\gamma) \)). From any region \( \gamma \), it is possible to reach a region \( \gamma' \) s.t. \( \text{succ}(\gamma') = \gamma' \), and we denote by \( l_{\gamma} \) the required number of steps s.t. \( \gamma'^{l_{\gamma}} = \text{succ}(\gamma'^{l_{\gamma}}) \).

**Example 5** Figure 3 gives an overview of the set of regions defined by two clocks \( x \) and \( y \), and the maximal constant 1. In this case there are 32 different regions, of which only 17 are numbered in the figure. Corresponding \( B(C) \)-formulas as well as successor regions are indicated for some of the regions. In general successor regions are determined by following 45° lines upwards to the right. \( \square \)

Given a timed automata \( A = \langle N, \eta_0, C, E \rangle \), let \( k_A \) be the maximal constant occurring in the enabling condition of the edges \( E \). Then for any \( k \geq k_A \) we can define a symbolic semantics of \( A \) over symbolic states \([\eta, \gamma]_A\) where \( \eta \in S \) and \( \gamma \in \mathcal{R}_k^C \) as follows:

\[
[\eta, \gamma]_A \xrightarrow{a} [\eta', \gamma']_A \quad \text{iff} \quad \exists u \in \gamma, \ (\eta, u) \xrightarrow{a} (\eta', u') \quad \text{and} \quad u' \in \gamma' \\
[\eta, \gamma]_A \xrightarrow{\gamma} [\eta, \text{succ}(\gamma)]_A \quad \text{iff} \quad \text{true}
\]

Consider now \( L_\nu \) with respect to formula clock set \( K \) and maximal constant \( k_L \). Also consider a given timed automata \( A = \langle N, \eta_0, C, E \rangle \) (s.t. \( K \) and \( C \) are disjoint). Then an extended symbolic state is a pair \([\eta, \gamma]_{A+}\) where \( \eta \in N \) and \( \gamma \in \mathcal{R}_k^{C \cup K} \) with \( k = \max(k_A, k_L) \). Whenever \( \gamma \) is a region over \( C \cup K \) we denote by \( \gamma|_C \) the set of time assignments in \( \gamma \) restricted to the (automata) clock set \( C \). Similarly, \( \gamma|_K \) denotes the projection of all time assignments in \( \gamma \) to the (formula) clock set \( K \). Observe that \( \gamma|_C \in \mathcal{R}^C \) and \( \gamma|_K \in \mathcal{R}^K \).

Using the finitary symbolic semantics of timed automata a symbolic interpretation of \( L_\nu \) is defined in [LLW95] faithfully reflecting the standard interpretation in Table 1. This symbolic interpretation provides the basis for decidability of model-checking for \( L_\nu \), and consequently (due to Theorem 1) for decidability of timed bisimilarity between timed automata.
\[
\begin{align*}
\tau \vdash [\eta, \gamma] &= \tau \\
\alpha \vdash [\eta, \gamma] &= \alpha \\
(\varphi_1 \land \varphi_2) \vdash [\eta, \gamma] &= (\varphi_1 \vdash [\eta, \gamma]) \land (\varphi_2 \vdash [\eta, \gamma]) \\
\langle a \rangle \varphi \vdash [\eta, \gamma] &= \bigvee_{b, [\eta', \gamma'] \in E(\eta, \gamma, a)} \langle b \rangle (r_{\gamma'} \in \varphi \vdash [\eta', \gamma']) \\
\exists \varphi \vdash [\eta, \gamma] &= \exists_{\gamma' \in [0, \gamma]} \bigvee_{i=0}^{\gamma'} (\beta(\gamma^i) \land \varphi \vdash [\eta, \gamma^i]) \\
(x + c \sim y + d) \vdash [\eta, \gamma] &= (x + c \sim y + d)(\gamma) \\
(x \in \varphi) \vdash [\eta, \gamma] &= x \in (\varphi \vdash [\eta, \gamma'] \text{ where } \gamma' = [\{x\} \to 0] \gamma \\
Z \vdash [\eta, \gamma] &= Z^{[0, \gamma]}
\end{align*}
\]

Table 2: Structural definition of quotient, \(\varphi \vdash [\eta, \gamma]\).

5 Quotienting

Given an \(L_\nu\) formula \(\varphi\), and two timed transition systems \(S_1\) and \(S_2\) we aim at constructing a formula (called the quotient) \(\varphi \vdash S_2\) such that

\[
S_1 \vdash S_2 \models \varphi \text{ if and only if } S_1 \models \varphi \vdash S_2
\]  

(3)

The bi-implication indicates that we are moving parts of the parallel system into the formula. Clearly, if the quotient is not much larger than the original formula, we have simplified the task of model checking, as the (symbolic) semantics of \(S_1\) is significantly smaller than that of \(S_1 \vdash S_2\).

In general it will not be possible to express within \(L_\nu\) such a quotienting formula. However, whenever \(S_2\) is described using a timed automata we are able to express the quotient using the (extended) symbolic semantics of automata. More precisely, whenever \(\varphi\) is a formula over \(K\) and \(A\) is a timed automaton over \(C\), we define quotient formulas \(\varphi \vdash [\eta, \gamma]\) over \(C \cup K\), where \([\eta, \gamma]\) is an extended symbolic state. For \(\eta_0\) the initial node of \(A\) and \(\gamma_0\) the initial region, \(\varphi \vdash [\eta_0, \gamma_0]\) will express the sufficient and necessary requirement to a timed transition system \(S\) in order that \(S_1 \vdash S_A\) satisfies \(\varphi\) — see also Corollary 3 below. The quotient construction is defined structurally in Table 2. We have left out the cases for \([a], \forall,\) and \(\mathbb{W}\) as they are immediate duals. The Table uses the following notation: \(b, [\eta', \gamma'] \in E(\eta, \gamma, a)\) iff \([\eta', \gamma'] \vdash \gamma_0\) and \(f(b, c) \vdash a\) for some \(c\). We denote by \(r_{\gamma}\) the set of \(C\) clocks which has the value \(0\) in \(\gamma\). Moreover \((r \in \varphi)\) is an abbreviation for \((x_1 \in (x_2 \in \ldots (x_n \in \varphi))\) whenever \(r \in \{x_1, \ldots, x_n\\}\). Finally, \(\langle 0 \rangle \varphi = \varphi\).

Note that the quotient construction for identifiers introduces new identifiers of the form \(Z^{[0, \gamma]}\), where \(Z \in \mathbb{I}_d\). The definition of these are collected in the
(quotient) declaration $D_A$ given by:

$$ Z^{[\eta, \gamma]} \overset{\text{def}}{=} \ D(Z) \big/_{\eta, \gamma} \] $$

The following Theorem and Corollary shows that the quotient construction of Table 2 satisfies the requirements of (3). A proof of Theorem 2 is sketched in Appendix A.

**Theorem 2** Let $S = \langle S, s_0, \longrightarrow \rangle$ be a timed transition system, let $A = \langle N, \eta_0, C, E \rangle$ be a timed automaton, and let $\varphi$ be an $L_\nu$ formula over clock set $K$, all over action set $A$. Then for any $s \in S$, $\eta \in N$, $v \in R^C$, and $u \in R^K$:

$$ \langle s, (\eta, v), u \rangle \models_\mathcal{D} \varphi \text{ if and only if } \langle s, v, u \rangle \models_{D_A} \varphi_{/\eta} \ ]$$

**Corollary 3** Let $S$ be a timed transition system, let $A$ be a timed automaton with clock set $C$, and let $\varphi$ be a closed $L_\nu$ formula over clock set $K$, all over action set $A$. Then:

$$ S \models_\mathcal{D} \varphi \text{ if and only if } S \models_{D_A} \varphi_{/A} $$

where $\varphi_{/A}$ abbreviates $\varphi_{/\eta_0, \gamma_0}$ with $\eta_0$ being the initial node of $A$ and $\gamma_0$ the initial region over $C \cup \hat{K}$.

**Example 6** Recall the timed automata and declaration from Examples 1 and 4. The quotient $X_1 \overset{\text{def}}{=} A_1$ describes the sufficient and necessary requirement to a timed transition system $S$ in order that $S \models S_{A_1}$ satisfies $X_1$. Clearly, we expect the timed automata $B_0$ to satisfy this property. Now using a CAML prototype implementation of the quotient construction $X_1 \overset{\text{def}}{=} A_1$ is computed. The definition of $X_1 \overset{\text{def}}{=} A_1$ is found in the quotient declaration $\mathcal{F}_{A_1}$ part of which is given below:

$$ X_1 \overset{\text{def}}{=} [a] y \in Z_1^{[\eta_0, \gamma_0]} $$

$$ Z_1^{[\eta_0, \gamma_0]} \overset{\text{def}}{=} \text{if} \forall [u \land ([b] \text{in } Z_1^{[\eta_1, \gamma_1, \gamma_0]} ) \land ([a] \text{in } Z_1^{[\eta_0, \gamma_0]} ) ] \land \forall (\beta(\gamma_0) \Rightarrow Z_1^{[\eta_0, \gamma_0]} \land \beta(1) \Rightarrow Z_1^{[\eta_0, \gamma_1]} \land \beta(2) \Rightarrow Z_1^{[\eta_0, \gamma_1]} \land \beta(3) \Rightarrow Z_1^{[\eta_0, \gamma_1]} ) $$

$$ Z_1^{[\eta_1, \gamma_0]} \overset{\text{def}}{=} \text{if} \forall [u \land ([b] \text{in } Z_1^{[\eta_1, \gamma_1, \gamma_0]} ) \land ([a] \text{in } Z_1^{[\eta_0, \gamma_0]} ) ] \land \forall (\beta(\gamma_0) \Rightarrow Z_1^{[\eta_0, \gamma_0]} \land \beta(1) \Rightarrow Z_1^{[\eta_0, \gamma_1]} \land \beta(2) \Rightarrow Z_1^{[\eta_0, \gamma_1]} \land \beta(3) \Rightarrow Z_1^{[\eta_0, \gamma_1]} ) $$

$$ Z_1^{[\eta_0, \gamma_1]} \overset{\text{def}}{=} \text{if} \forall [u \land ([b] \text{in } Z_1^{[\eta_1, \gamma_1, \gamma_1]} ) \land ([a] \text{in } Z_1^{[\eta_0, \gamma_0]} ) ] \land \forall (\beta(\gamma_0) \Rightarrow Z_1^{[\eta_0, \gamma_0]} \land \beta(1) \Rightarrow Z_1^{[\eta_0, \gamma_1]} \land \beta(2) \Rightarrow Z_1^{[\eta_0, \gamma_1]} \land \beta(3) \Rightarrow Z_1^{[\eta_0, \gamma_1]} ) $$

$$ Z_1^{[\eta_1, \gamma_1]} \overset{\text{def}}{=} \text{if} \forall [u \land ([b] \text{in } Z_1^{[\eta_1, \gamma_1, \gamma_1]} ) \land ([a] \text{in } Z_1^{[\eta_0, \gamma_0]} ) ] \land \forall (\beta(\gamma_0) \Rightarrow Z_1^{[\eta_0, \gamma_0]} \land \beta(1) \Rightarrow Z_1^{[\eta_0, \gamma_1]} \land \beta(2) \Rightarrow Z_1^{[\eta_0, \gamma_1]} \land \beta(3) \Rightarrow Z_1^{[\eta_0, \gamma_1]} ) $$

$$ Z_1^{[\eta_0, \gamma_1]} \overset{\text{def}}{=} \text{if} \forall [u \land ([b] \text{in } Z_1^{[\eta_1, \gamma_1, \gamma_1]} ) \land ([a] \text{in } Z_1^{[\eta_0, \gamma_0]} ) ] \land \forall (\beta(\gamma_0) \Rightarrow Z_1^{[\eta_0, \gamma_0]} \land \beta(1) \Rightarrow Z_1^{[\eta_0, \gamma_1]} \land \beta(2) \Rightarrow Z_1^{[\eta_0, \gamma_1]} \land \beta(3) \Rightarrow Z_1^{[\eta_0, \gamma_1]} ) $$

13
The quotient declaration $F_{A_1}$ contains in total definitions of 96 identifiers. We expect $X_1/ A_1$ to express that the accumulated time between an initial $a$–action and a following $b$–action must be strictly greater than 0 as described by the following property $U_0$:

$$
U_0 \overset{\text{def}}{=} [a] \left( y \in V_0 \right) \quad \quad V_0 \overset{\text{def}}{=} (y > 0) \lor \left( [b] \land [a] V_0 \land \forall V_0 \right)
$$

In the next section we will present effective minimization strategies, which essentially transforms the large quotient declaration $F_{A_1}$ into the small yet equivalent declaration above.

Now, let $\pi$ be the synchronization function completely specified by $\pi(0, a) = a$ for all $a \in A$ (i.e. the left argument to $\pi$ is completely ignored). Then it is easy to see that for any timed transition system $S$, $S_A$ and $S_1 S_A$ satisfies the same formulas. In particular $S_A$ and $S_1 S_A$ satisfies the same formula, where $1$ is the 0–clock timed automaton with just one (initial) node and no edges. Using this observation, the quotient construction can be used to obtain alternative model–checking algorithms for $I_\nu$ as follows:

**Corollary 4** Let $A$ be a timed automaton with clock set $C$, and let $\varphi$ be a closed $L_\nu$ formula over clock set $K$, all over an action set $A$. Then:

$$
A \models \varphi \quad \text{if and only if} \quad 1 \models_{D_A} \varphi / A \quad \text{if and only if} \quad \varphi / A \models \top
$$

Due to the projective nature of $\pi$ it is clear that $\varphi / A$ contains no action modalities, and it is easy to build a special purpose model checker for the simple automata $1$.

**Example 7** Recall once more the timed automata and declaration from Examples 1 and 4. From these Examples we expect that $C_{0, 1}$ satisfies the property $X_1$. Now, using the Corollary 4 we may verify this by showing that the quotient formula $X_1 / C_{0, 1}$ is either valid or satisfied by $1$. $X_1 / C_{0, 1}$ is defined in the following quotient declaration $F_{C_{0, 1}}$:

$$
X_{1}^{[\mu, \gamma_0]} \overset{\text{def}}{=} \text{$x$ in $y$ in } Z_{1}^{[\mu, \gamma_0]}
$$

$$
Z_{1}^{[\mu, \gamma_0]} \overset{\text{def}}{=} \forall \left( \beta(\gamma_0) \Rightarrow Z_{1}^{[\mu, \gamma_0]} \land \beta(\gamma_1) \Rightarrow Z_{1}^{[\mu, \gamma_1]} \land \beta(\gamma_2) \Rightarrow Z_{1}^{[\mu, \gamma_1]} \right)
$$

$$
Z_{1}^{[\mu, \gamma_1]} \overset{\text{def}}{=} \left( x \in Z_{1}^{[\mu_2, \gamma_1]} \land \forall \left( \beta(\gamma_0) \Rightarrow Z_{1}^{[\mu, \gamma_0]} \land \beta(\gamma_1) \Rightarrow Z_{1}^{[\mu, \gamma_1]} \land \beta(\gamma_2) \Rightarrow Z_{1}^{[\mu, \gamma_1]} \right) \right)
$$

$$
Z_{1}^{[\mu_2, \gamma_1]} \overset{\text{def}}{=} \forall \left( \beta(\gamma_1) \Rightarrow Z_{1}^{[\mu_2, \gamma_1]} \land \beta(\gamma_2) \Rightarrow Z_{1}^{[\mu_2, \gamma_1]} \right)
$$

$$
Z_{1}^{[\mu_2, \gamma_2]} \overset{\text{def}}{=} \forall \left( \beta(\gamma_1) \Rightarrow Z_{1}^{[\mu_2, \gamma_1]} \land \beta(\gamma_2) \Rightarrow Z_{1}^{[\mu_2, \gamma_1]} \right)
$$

$$
Z_{1}^{[\mu_2, \gamma_3]} \overset{\text{def}}{=} \forall \left( \beta(\gamma_1) \Rightarrow Z_{1}^{[\mu_2, \gamma_1]} \land \beta(\gamma_2) \Rightarrow Z_{1}^{[\mu_2, \gamma_1]} \right)
$$

\[13\] Found using the CAML prototype with subsequent application of boolean simplifications.
\[ Z_1^{[\mu_1, \gamma_2]} \overset{\text{def}}{=} \{ x \in Z_1^{[\mu_2, \gamma_2]} \} \land \forall (\beta(\gamma_0) \Rightarrow Z_1^{[\mu_1, \gamma_0]} \land \beta(\gamma_1) \Rightarrow Z_1^{[\mu_1, \gamma_1]} \land \\
\beta(\gamma_2) \Rightarrow Z_1^{[\mu_1, \gamma_2]} ) \}
\]

\[ Z_1^{[\mu_2, \gamma_2]} \overset{\text{def}}{=} \forall (\beta(\gamma_2) \Rightarrow Z_1^{[\mu_2, \gamma_2]} ) \]

Finally, combining the characterization of timed bisimulation in Theorem 1 with the quotient construct of Table 2, we can for any timed automaton \( A \) construct a characteristic \( L_\nu \) formula uniquely characterizing the automaton up to timed bisimilarity in the following manner: Let \( \mathcal{E}, \mathcal{Z} \) and \( h \) be as in Theorem 1. Then for any timed transition system \( \mathcal{S} \) the following holds:

\[ \mathcal{S} \sim \mathcal{S}_A \text{ if and only if } \mathcal{S} \models \mathcal{Z} /_h [\eta_0, \gamma_0] \]

where \( \eta_0 \) is the initial node of \( A \) and \( \gamma_0 \) is the initial region over the clocks of \( A \) (note that \( Z \) is an \( L_\nu \) formula over the empty set of clocks). This provides an alternative characteristic formula construction compared with [LLW95].

6 Minimizations

It is evident from the examples in the previous section that repeated quotienting leads to an explosion in the formula. A similar phenomena was observed by Andersen for the quotient construction of modal \( \mu \)-calculus formulas with respect to finite–state systems. The crucial observation by Andersen is that simple and cost effective transformations of the formulas in practice often lead to significant reductions.

We have implemented in CAML the quotient construction of the previous section as well as (simplified versions of some of) Andersen’s minimization strategies. In the investigated examples the minimization strategies lead to dramatic reductions. Below we describe the transformations considered in terms of transformations on formulas and declarations (defining equations).

**Reachability:** When considering an initial quotient formula \( \varphi /_h [\eta_0, \gamma_0] \) not all identifiers of \( \mathcal{D}_A \) may be relevant or reachable. In our CAML implementation an “on-the-fly” technique insures that only the reachable part of \( \mathcal{D}_A \) is generated.

**Boolean Simplification:** Formulas may be simplified using the following simple boolean equations and their duals: \( f \land \varphi \equiv f, \top \land \varphi \equiv \varphi, \varphi \circ f \equiv f, \exists f \equiv f, x \in f \equiv f, \varphi \land [a] f \equiv f. \]

**Constant Propagation:** Identifiers which are declared to either \( \top \) or \( f \) may be removed while substituting their definitions in the declaration of all other identifiers.
**Trivial Equation Elimination:** Equations of the form $X \overset{\text{def}}{=} [a]X$ are easily seen to have $X = \mathbf{t}$ as solution. More generally, whenever $X \overset{\text{def}}{=} \varphi$ where $\varphi[\mathbf{t}/X] \overset{14}{=} \varphi$ can be simplified to $\mathbf{t}$, we can perform a removal of the identifier $X$ provided the value $\mathbf{t}$ is propagated to all uses of $X$ (as under Constant Propagation).

**Equivalence Reduction:** If two identifiers $X$ and $Y$ are equivalent (i.e., are satisfied by the same timed transition systems) we may collapse them into a single identifier. To obtain a cost effective strategy we approximate equivalence of identifiers with the following check: whenever $X \overset{\text{def}}{=} \varphi$ and $Y \overset{\text{def}}{=} \psi$ such that $\varphi[Y/X]$ is syntactically identical to $\psi[Y/X]$ we conclude that $X$ and $Y$ are equivalent and may be identified.

We apply the above transformation strategies repeatedly on quotient formulas and declarations. As can be seen in Table 2, quotienting transforms atomic propositions of the form $x + c \sim y + d$ into either $\mathbf{t}$ or $\mathbf{f}$, thus yielding high applicability of Boolean Simplification and Constant Propagation. Also, quotient versions of the same original formula tend to have same structure thus making applicability of Equivalence Reduction high.

In our CAML prototype implementation we have implemented the above reported very simple strategies for Trivial Equation Elimination and Equivalence Reduction. Generalized and more sophisticated (yet still efficient) strategies can of course easily be given. However, even with the implemented simple versions we obtain a very high degree of reduction as observed in the following examples.

**Example 8** Recall Example 6. Applying the minimization strategies of the CAML prototype we find that $X_1/A_1$ is equivalent to $Y_0$ with the following definition:

\[
\begin{align*}
Y_0 \overset{\text{def}}{=} & [a]y \in Y_1 \\
Y_1 \overset{\text{def}}{=} & [b]f \land [a]Y_1 \land \varphi (\beta(\gamma_0) \Rightarrow Y_1 \land (\beta(\gamma_1) \lor \beta(\gamma_2)) \Rightarrow Y_2) \\
Y_2 \overset{\text{def}}{=} & [a]Y_2 \land \varphi (\beta(\gamma_0) \Rightarrow Y_1 \land (\beta(\gamma_1) \lor \beta(\gamma_2)) \Rightarrow Y_2)
\end{align*}
\]

During minimization only 23 identifiers of $\mathcal{F}_{A_1}$ were found to be reachable from $X_1/A_1$, 14 respectively 3 of which were found to be equivalent to $\mathbf{t}$ respectively $\mathbf{f}$. The remaining 6 identifiers were finally partitioned into 3 classes. Though dramatically reduced, the declaration leaves room for one additional simplification as it may be observed that $(\beta(\gamma_1) \lor \beta(\gamma_2)) \Rightarrow Y_2$ is equivalent to $\mathbf{t}$. With this observation we finally obtain:

\[
\begin{align*}
Y'_0 \overset{\text{def}}{=} & [a]y \in Y'_1 \\
Y'_1 \overset{\text{def}}{=} & [b]f \land [a]Y'_1 \land \varphi (\beta(\gamma_0) \Rightarrow Y'_1)
\end{align*}
\]

which clearly meets the expectations of 6. Minimization of the quotient formula $X_7/A_{10}$ leads directly to the formula $\mathbf{t}$ indicating that for any timed transition

\[14 \varphi[\mathbf{t}/X] \text{ is the formula obtained by substituting all occurrences of } X \text{ in } \varphi \text{ with the formula } \mathbf{t}.\]
system $S$ the composition $S|_{A_{10}}$ satisfies $X_7$. Intuitively this is clear as the 
component $A_{10}$ by itself ensures the delay required by $X_7$. The corresponding 
quotient declaration contains 3498 identifiers 617 of which were found to be 
reachable. Subsequently all these were simplified to $\mathbf{t}$. $\square$

**Example 9** Recall Example 7. Using the minimization strategies of the CAML 
prototype we find directly that $X_1|_{C_{0,1}}$ simplifies to $\mathbf{t}$ thus implying that 
$C_{0,1}$ satisfies the property $X_1$. Similarly, minimization of the quotient formula 
$X_2|_{C_{0,1}}$ yields $\mathbf{f}$ confirming that $C_{0,1}$ does not satisfy $X_2!$ $\square$

**Example 10** Now we want to confirm that $B_0$ does indeed satisfy the re-
quirement $X_1|_{A_1}$ and hence that $B_0|_{A_1}$ satisfies $X_1$. Using the equivalent, 
minimized formula $Y_0$ from Example 8 it suffices according to Corollary 4 to 
verify validity of the quotient formula $Y_0|_{B_0}$. The CAML prototype confirms 
this through immediate minimization to $\mathbf{t}$. $\square$

### 7 Conclusion

This paper has presented the basis for a compositional model checking technique 
for real-time systems. Based on initial experiments with the CAML prototype 
we conjecture that compositional model checking will prove not only a feasible 
but also an efficient technique for real-time systems. However, it is clear that 
many more experiments must be performed before the conjecture can be finally 
settled, and in this process we will need to extend our prototype with more 
advanced minimization strategies as the success of compositional model check-
ing is completely determined by these.

Our work on quotient formulas extends that of [AKLN95], where a quo-
tient construction for 1-clock automata has been given. Moreover it can be 
generalized trivially to logics with minimal fixpoint constructs (such as $T_\mu$ in 
[HN92]) as quotienting is easily seen to distribute over negation.

### Acknowledgement

The authors would like to thank Henrik Reif Andersen for interesting and enlightening discussions on the topic of compositional (partial) model-checking.
References


A Proof of Theorem 2

Proof We only sketch the proof for the identifier free formulas of $L_v$ using structural induction on $\varphi$. Consequently we drop declaration subscripts on $\models$. The full proof follows the structure used in [LX90].

We consider only the cases $\langle a \rangle \varphi$, $\exists \varphi$ and $x \in \varphi$ leaving the remaining more trivial cases to the reader.

- Assume $\langle s \rangle (\eta, v), u \models \langle a \rangle \varphi$. Then we have:

  \[
  \langle s \rangle (\eta, v), u \models \langle a \rangle \varphi \\
  \iff \langle s' \rangle (\eta', v'), u \models \varphi \quad \text{for some } s \xrightarrow{a_1} s' \text{ and } \exists (\eta, \eta', a_2, r, b) \in E \text{ s.t. } v' = [r \rightarrow 0]v \text{ and } b(v) = \ast \text{ and } f(a_1, a_2) \simeq a \\
  \iff \langle s', v' u \rangle \models \varphi / \eta', [v' u] \\
  \iff \langle s', v u \rangle \models r \in \varphi / \eta', [v' u] \\
  \iff \langle s, v u \rangle \models \bigvee_{a_1, s' \models [v'] \in \Sigma(v) \forall v \neq a} (a_1)(r \in \varphi / \eta', [v' u]) \\
  \iff \langle s, v u \rangle \models (\langle a \rangle \varphi) / \eta, [v u] \\
  \]

- Assume $\langle s \rangle (\eta, v), u \models \exists \varphi$. Then we have:

  \[
  \langle s \rangle (\eta, v), u \models \exists \varphi \\
  \iff \langle s^d \rangle (\eta, v + d), u + d \models \varphi \quad \text{for some } d \in \mathbb{R} \\
  \iff \langle s^d \rangle (v + d u + d), [v + d u + d] \models \varphi / \eta, [v u] \quad \text{by IH} \\
  \iff \langle s^d \rangle (v + d u + d), [v u]^i \models \varphi / \eta, [v u] \quad \text{where } (v + d u + d) \in [v u]^i \\
  \iff \langle s^d \rangle (v + d u + d), [v u]^i \models \beta([v u]^i) \land \varphi / \eta, [v u]^i \\
  \iff \langle s, v u \rangle \models (\exists \varphi) / \eta, [v u] \\
  \]

- Assume $\langle s \rangle (\eta, v), u \models x \in \varphi$. Then we have:

  \[
  \langle s \rangle (\eta, v), u \models x \in \varphi \\
  \iff \langle s \rangle (\eta, v), u' \models \varphi \quad \text{with } u' = [x \rightarrow 0]u \\
  \iff \langle s, v u' \rangle \models \varphi / \eta, [v u'] \quad \text{by IH} \\
  \iff \langle s, v u \rangle \models x \in \varphi / \eta, [v u] \\
  \iff \langle s, v u \rangle \models (x \in \varphi) / \eta, [v u] \\
  \]

\[ \square \]
Recent Publications in the BRICS Report Series


