Translating Chi models to UPPAAL timed automata

Citation for published version (APA):

Document status and date:
Published: 01/01/2007

Document Version:
Publisher’s PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:
- A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher’s website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the “Taverne” license above, please follow below link for the End User Agreement:
www.tue.nl/taverne

Take down policy
If you believe that this document breaches copyright please contact us at:
openaccess@tue.nl
providing details and we will investigate your claim.
Translating $\chi$ models to UPPAAL timed automata

E.M. Bortnik, J.M. van de Mortel-Fronczak, J.E. Rooda
## Contents

1. Introduction ......................................................... 2
2. Translated subset of timed $\chi$ .................................... 2
3. UPPAAL timed automata ........................................... 3
   3.1 The formal definition of UPPAAL timed automaton .......... 3
   3.2 UPPAAL Semantics ........................................... 4
4. Translation scheme .................................................. 6
   4.1 Translation function $T_M$ .................................. 6
   4.2 Translation function $T_q$ .................................. 7
5. Correctness of the translation scheme .............................. 13
   5.1 Preliminaries ................................................ 13
   5.2 Theorem 1 ................................................... 16
   5.3 Theorem 2 ................................................... 24
   5.4 Theorem 3 ................................................... 32
6. Informal translation .................................................. 34
   6.1 Guarded skip and multi-assignment ......................... 34
   6.2 Guarded Send and Receive ................................ 35
   6.3 Guarded repetition .......................................... 35
   6.4 Some notes ................................................. 36
7. Case Study: Verification of the Turntable System ............... 36
   7.1 System description .......................................... 36
   7.2 Design rules and assumptions ............................... 38
   7.3 Verified properties ........................................ 38
   7.4 $\chi$ model of the turntable ................................ 39
   7.5 UPPAAL model of the turntable ............................. 40
   7.6 Verification ................................................ 40
8. Conclusions and future work ....................................... 41

Appendices

1. Timed Chi semantics used in the report ........................... 42
   1.1 Skip and Multi-assignment ................................ 43
   1.2 Variable trajectories ...................................... 43
   1.3 SOS Rules ................................................ 43
2. The $\chi$ and UPPAAL models of the turntable ..................... 46
   2.1 The $\chi$ model of the turntable .......................... 46
   2.2 The UPPAAL model of the turntable ....................... 49
Abstract

Due to increasing system complexity and growing competition and costs, powerful techniques are needed to design and analyze manufacturing systems. One of the most popular techniques to do performance analysis is simulation. However, simulation-based analysis cannot guarantee the correctness of a system. Our research focuses on examining other methods to make performance analysis and functional analysis, and combining the two. One of the approaches is to translate a simulation model that is used for performance analysis to a model written in an input language of an existing verification tool. The process algebraic language χ is intended for modeling, simulation, verification and real-time control and has been used extensively to simulate large manufacturing systems. UPPAAL is an integrated tool environment for modeling, validation and verification of real-time systems and has been applied successfully in case studies ranging from communication protocols to multimedia applications. In this report, we represent a translation scheme that is used to translate simulation models written in χ language to UPPAAL timed automata. As an example we apply the translation scheme to a model of a manufacturing system and show some of the properties that can be verified in UPPAAL.
1 Introduction

Nowadays, due to increasing system complexity and growing competition and costs, industry makes high demands on powerful tools and techniques used to design and analyze manufacturing systems. One of the most popular techniques to do performance analysis is simulation. However, simulation-based analysis becomes insufficient since it cannot guarantee the correctness of a system. The objective of the TIPSy project\(^1\) (Tools and Techniques for Integrating Performance Analysis and System Verification) is to combine performance and functional analysis, particularly in the $\chi$ environment.

The $\chi$ language is intended for modeling, simulation, verification, and real-time control of manufacturing systems \[11\]. It is used to model and simulate discrete-event, continuous or combined, so-called hybrid, systems. The $\chi$ language has formal semantics which makes it suitable for verification. The language and simulator have been successfully applied to a large number of industrial cases, such as an integrated circuit manufacturing plant, a brewery and process industry plants \[13\].

Since we do not expect that a dedicated verification tool for $\chi$, that would be able to compete with existing optimized model checkers, could be built within reasonable time, our aim is to translate $\chi$ models to input languages of existing verification tools. As the first step, a model was manually translated to $\mu$CRL, Promela and UPPAAL timed automata, and verified in CADP, Spin and UPPAAL, respectively \[4\]. In this report, a general translation scheme from $\chi$ to UPPAAL is described, and its correctness is proved. Using the scheme, the $\chi$ toolset is extended with the translator to make possible to verify $\chi$ models in UPPAAL.

UPPAAL is a tool for modeling, simulation, validation and verification of real-time systems that can be modeled as a collection of non-deterministic processes with a finite control structure and real-valued clocks \[8,14\]. The UPPAAL model checking engine allows to verify properties that are expressed in the UPPAAL Requirement Specification Language. This language is a subset of timed computation tree logic (TCTL), where primitive expressions are location names, variables, and clocks from the modeled system.

The remainder of the report is organized as follows. In Section 2, the translated subset of $\chi$ is described. Then, in Section 3, the formal definition of UPPAAL timed automata is given. The translation is defined in Section 4 and proved in Section 5. The informally translated process terms are described in Section 6. In Section 7, an example of the translation of a part of a manufacturing system is shown and the properties which can be verified are described. Finally, in Section 8, conclusions are drawn.

2 Translated subset of timed $\chi$

In order to model timed discrete-event systems only, the hybrid $\chi$ language has been simplified, resulting in timed $\chi$ \[12\]. In the remainder of this report, we refer to timed $\chi$ as $\chi$.

The set $M$ of $\chi$ models that can be translated using this translation scheme consists of models $M \in M$, where $M$ is of the form $(\partial_{\lambda}, (v_{H}(p)), \sigma, E), p \in P$ is a $\chi$ process term, $\sigma$ is a valuation. The environment $E$ is a tuple $(J, H, R)$, where $J$ is a set of jumping variables, $H$ is a set of urgent channels, and $R$ denotes a set of recursive process definitions. We restrict the environment

---

\(^1\) supported by the Dutch Organization for Scientific Research (NWO), project number 612.064.205
in the following way:

- The set of the jumping variables \( J = \emptyset \). This disallows arbitrary changes of the values of the variables, which are not used in communication.
- All channels in the model are urgent \( H = H_1 \), where \( H_1 \) is a set of urgent channels.
- There are no recursive process definitions \( R = \emptyset \).

Moreover, for all transitions, the domain of the valuation \( \sigma \) equals the domain of valuation \( \sigma' \), \( \text{dom}(\sigma) = \text{dom}(\sigma') \), and environment \( E \) equals environment \( E' \), \( E = E' \).

Formally, the set \( P \) consists of process terms \( p \), where \( p \) is defined by:

\[
p ::= q \mid q \parallel q.
\]

The set \( Q \) consists of the following process terms: skip, multi-assignment \( x_n := e_n \), send \( h!!e_n \) and receive \( h??x_n \). \( x_n \) and \( e_n \) denote the vectors \((x_1, \ldots, x_n)\) and \((e_1, \ldots, e_n)\), deadlock \( \delta \) and inconsistent process term \( \bot \), delay \( \Delta d \), any delay operator \([q]\), repetition \( \ast q \), sequential composition \( q_1; q_2 \), and alternative composition \( q_1 \langle q_2 \rangle \). Formally, the set \( Q \) consists of process terms \( q \), where \( q \) is defined by:

\[
q ::= \text{skip} \mid x_n := e_n \mid h!!e_n \mid h??x_n \mid \delta \mid \bot \mid \Delta d \mid [q] \mid \ast q \mid q_1; q_2 \mid q_1 \langle q_2 \rangle.
\]

Parallel composition is not allowed inside the process terms \( q \), since a UPPAAL model is a collection of sequential processes (represented by UPPAAL timed automata) working in parallel.

3 UPPAAL timed automata

The model-checker UPPAAL is based on the theory of timed automata [1], where a system is modeled as a network of timed automata [2] extended with variables, guards and invariants that might involve both clocks and variables, notion of urgency (urgent and committed locations, urgent channels), etc. There are several formal definitions of UPPAAL timed automata [2, 10, 3]. For the translation we have chosen the formal description [10] as it covers most of the features of UPPAAL timed automata that are implemented in the tool. For the expressions and assignments in UPPAAL automata we will use UPPAAL notation, where \( c == d \) denotes equality and \( x = y \) denotes assignment of the value of \( y \) to variable \( x \).

3.1 The formal definition of UPPAAL timed automaton

Definition 3.1. A UPPAAL timed automaton \( \mathcal{A} \) is a tuple \( (L, l_0, E, V, C, \text{Init}, \text{Inv}, T_1) \), where:

- \( L \) is a finite set of locations
- \( l_0 \) is the initial location

\[3\] The translation of the multi-assignment process term has following restriction. Let \( Y \) be a set of variables over which the expression \( e_n \) are defined, then the translation is restricted to the cases, where \( \forall x_i \in x_n \cdot x_i \notin Y \).

\[3\] The translation is restricted to the cases, where \( c(d) \in \mathbb{N}^* \). Moreover, the value of the expression \( d \) cannot be changed during delay.
• $E$ is the set of the edges defined by $E \subseteq L \times G(C, V) \times \text{Sync} \times \text{Act} \times L$, where:
  
  – $G(C, V)$ is the set of constraints allowed in guards,
  
  – Sync is a set of synchronization actions which includes actions, co-actions, and the internal $\tau_n$-action. An action send over a channel $h$ is denoted by $h!$ and its co-action receive is denoted by $h?$. The $\tau_n$-action is an internal action which cannot synchronize and does not have a co-action.
  
  – Act is a set of sequences of assignment actions of the form $x_i = e_i$, $i = 1, \ldots, n$, where $e_i$ are integer expressions, clock resets and the $\tau_n$-assignment. The $\tau_n$-assignment is an empty assignment, i.e., an assignment that does not change the values of the variables.

• $V$ denotes the set of integer variables,

• $C$ denotes the set of real-valued clocks ($C \cap V = \emptyset$),

• $\text{Init} \subseteq \text{Act}$ is a set of assignments that assigns the initial values to variables.

• $\text{Inv} : L \rightarrow \text{Inv}(C, V)$ is a function, that assigns an invariant to each location. $\text{Inv}(C, V)$ is the set of invariants over clocks $C$ and variables $V$.

• $T_i : L \rightarrow \{o, u, c\}$ the function, that assigns the type (ordinary, urgent or committed) to each location. The system cannot delay if there is a process in an urgent or committed location. The transitions via the outgoing edges of a committed location have priority.

Definition 3.2. A network of timed automata $N_A$ is a tuple $(\bar{\mathcal{A}}, \mathcal{I}_o, V', C, H, T_{1H}, \text{Init}')$, where $\bar{\mathcal{A}} = \{A_1, \ldots, A_n\}$ is a vector of $n$ timed automata $A_i = (I_i, [\rho_i], E_i, V_i, C_i, \text{Init}_i, \text{Inv}_i, T_{1i})$, for $1 \leq i \leq n$. $I_o = (l_0^1, \ldots, l_0^n)$ is the initial location vector, $V'$ and $C'$ are the sets of global (shared) variables and clocks, respectively, $(V' \cap C' = \emptyset)$, and $H$ is a set of channels $(V' \cap H = \emptyset$ and $C' \cap H = \emptyset)$. The function $T_{1H} : H \rightarrow \{o, u\}$ assigns the type (ordinary or urgent) to each channel. In case $H = \emptyset$, function $T_{1H}$ is undefined and is then informally denoted by $\emptyset$. $\text{Init}'$ is the set of assignments that assigns the initial values to the global variables.

3.2 UPPAAL Semantics

Below we give the description of the UPPAAL timed automata semantics. The description is based on [10]. For simplicity sake, the notation is changed to comply with the one used in $\chi$. Furthermore, in [10] two valuation functions are defined (clock valuation $\sigma_c : C \rightarrow \mathbb{R}_{\geq 0}$ and variable valuation $\sigma_v : V \rightarrow \mathbb{Z}$). Here we define a single valuation function $\sigma : C \cup V \rightarrow \mathbb{R}_{\geq 0} \cup \mathbb{Z}$, such that $\text{dom}(\sigma) = \text{dom}(\sigma_c) \cup \text{dom}(\sigma_v)$ and $\forall c \in C : \sigma(c) = \sigma_c(c), \forall x \in V : \sigma(x) = \sigma_v(x)$. The set of all possible valuations is denoted as $A$.

We use $\alpha' = a(\alpha)$ to denote how the valuation $\alpha$ is changed due to assignment $a$. Note that if there are more than one assignment on the edge, they are performed sequentially: if $a$ is of the form $\{x_i = e_i, i = 1, \ldots, n\}$, then $\forall i, j, j < i \leq n : a'(x_i) = a(e_i[x_j \mapsto e_j])$, where $e_i[x_j \mapsto e_j]$ denotes that all occurrences of $x_j$ in the expression $e_i$ are replaced by the expression $e_j$, and $\forall k, k > n : a'(x_k) = a(x_k)$. For instance, if $a$ is of the form $\{x = 3, y = x + 1\}$, then $a'(x) = 3, a'(y) = 4$.

The state of the timed automaton is defined by the location and valuation $s = (l, \alpha)$. The initial valuations $a_c(c) = 0$ for all $c \in C$, $a_v(x) = \text{Init}(x)$ for all $x \in V$. Let $\alpha \vdash \text{Inv}(l)$ denote that $\alpha$ satisfies $\text{Inv}(l)$.

A vector of locations $\bar{l}$ is a $n$-tuple. In With $[\bar{l'}]/\bar{l}$ we denote a vector where the $i$th element $l_i$ of $\bar{l}$ is replaced by $l'_i$. Similarly, with $[\bar{l'}/\bar{l}, \bar{f'}/\bar{l}]$ we denote a vector where the $i$th element $l_i$ of $\bar{l}$ is replaced by $l'_i$, and the $j$th element $l_j$ of $\bar{l}$ is replaced by $l'_j$. 
The semantics of a network of timed automata is defined as a transition system \( \langle S, s_0, \rightarrow \rangle \), where \( S = (L_1 \times \ldots \times L_n) \times A \) is the set of states, \( s_0 = (\overline{l_0}, \alpha_0) \) is the initial state, and \( \rightarrow \subseteq S \times S \) is the transition relation defined by the following rules.

### 3.2.1 Simple Action

An simple action \((\overline{l}, \alpha) \xrightarrow{a} ([l'_i/l_i], \alpha')\) can be performed, if there exists an edge \( l_i \xrightarrow{g \land h, a} l'_i \in E, l_i \in \overline{l} \) such that

- The guard \( g \) is satisfied in \( \alpha \)
  \( \alpha \models g \)
- The invariants are satisfied in \( \alpha' \)
  \( \forall l_j \in \overline{l} : \alpha' \models \text{Inv}_j(l_j) \)
- The source location is committed or there is no other committed location in \( \overline{l} \)
  \( T_L(l_i) = c \lor \forall l_j \in \overline{l}, i /= j : T_L(l_j) /= c \)
- \( \alpha' = a(\alpha) \)

### 3.2.2 Synchronization Action

A synchronized action \((\overline{l}, \alpha) \xrightarrow{h} ([l'_i/l_i, l'_j/l_j], \alpha')\) can be performed, if for \( i /= j \) there exist \( l_i \xrightarrow{g_i \land h, a_i} l'_i \in E_i, l_i \in \overline{l} \) and \( l_j \xrightarrow{g_j \land h, a_j} l'_j \in E_j, l_j \in \overline{l} \) such that

- Both guards are satisfied in \( \alpha \)
  \( \alpha \models (g_i \land g_j) \)
- Invariants will be satisfied
  \( \forall l_k \in \overline{l} : \alpha' \models \text{Inv}_k(l_k) \)
- One or both of the processes is in the committed location or there is not any other committed location in \( \overline{l} \)
  \( T_L(l_i) = c \lor T_L(l_j) = c \lor \exists l_k \in \overline{l} : T_L(l_k) = c \)
- The valuation \( \alpha' = a_j(a_i(\alpha)) \).

### 3.2.3 Delay

A delay \((\overline{l}, \alpha) \xrightarrow{t} ([l'_i/l_i], \alpha')\) can be performed, if all following holds

- There is not any process in the committed location;
  \( \forall l_i \in \overline{l} : T_L(l_i) /= c \)
- There is not any process in the urgent location;
  \( \forall l_i \in \overline{l} : T_L(l_i) /= u \)
4 Translation scheme

For the purpose of translation we assume existence of a set of model variables \( V \), a set of communication variables \( V_h \), and a set of clocks \( C \), such that \( V \cap V_h = \emptyset \), and \( C \cap (V \cup V_h) = \emptyset \). The set of clocks \( C \) is used for the translation of the delay operator.

The translation of timed \( \chi \) to UPPAAL timed automata is defined by means of three translation functions. Function \( T_M : M \rightarrow \text{NA} \) translates a \( \chi \) model \( M \) to a UPPAAL network of automata \( \text{NA} \) using function \( T_p \). The function \( T_p : P \rightarrow \mathcal{P}(A_\chi) \) translates a \( \chi \) process term \( p \in P \) to a set of extended timed automata using the function \( T_h \). The function \( T_h : Q \rightarrow A_\chi \) translates a \( \chi \) process term \( q \in Q \) to an extended timed automaton \( A_\chi \in A_\chi \). The definition of an extended timed automaton \( A_\chi \) is based on the definition of the UPPAAL timed automaton, extended with two additional elements: \( A_\chi = (L, L_0, E, V, V_h, C, \text{Init}, \text{Inv}, T_l, l_0) \), where \( V_h \subseteq V \) denotes an additional set of variables, that is used for the translation of communication actions, and \( l_0 \) denotes a final location. The final location \( l_0 \in L \cup \{ \top \} \) is used for the translation of sequential and alternative composition operators. The sign \( \top \) denotes that there is no final location, and \( \text{Inv}(l_0) = \text{true}, T_l(l_0) = 0, \) if \( l_0 \in L \).

4.1 Translation function \( T_M \)

The translation function \( T_M \) translates a \( \chi \) model \( M \) of the form \( \langle \partial_{A_{\text{ia}}} (v_H[p]), \sigma, E \rangle \), where \( A_{\text{ia}} \) is a set of the internal send and receive actions and \( H_{\text{si}} \) is a set of channels, and it is assumed that \( \text{dom}(\sigma) \setminus \{ \text{time} \} \subseteq V \), \( H_{\text{si}} \cap (V \cup V_h \cup C) = \emptyset \), to a network of UPPAAL timed automata \( \text{NA} = (\overline{A}, \overline{I}_0, V, \overline{E}, H_{\text{si}}, T_{\overline{I}_0}, T_{\overline{E}}, \text{Init}') \). The function \( T_M \) is defined as follows:

\[
T_M(M) = (\overline{A}, \overline{I}_0, V', \{ \text{time} \}, H_{\text{si}}, T_{\overline{I}_0}, \text{Init}')
\]

where \( \overline{A} \) is a vector of UPPAAL timed automata obtained by means of the function \( F \). The function \( F : \mathcal{P}(A_{\chi}) \rightarrow \overline{A} \times \mathcal{P}(V_h) \) transforms a set of extended automata into a vector of UPPAAL timed automata by extracting the sets of the communication variables \( V_h = \bigcup_{i = 1}^{\#A_{\chi}} V_h^i \), \( V_h^i \in A_{\chi_i}, A_{\chi_i} \subseteq A_{\chi} \), removing the final locations \( l_{i_0} \in A_{\chi_i} \), and defining the order of the automata \( A_i \) in the vector \( \overline{A} \).

Furthermore, \( \overline{I}_0 = (\overline{I}_0^0, \ldots, \overline{I}_0^\#A_{\chi}) \) is a vector of the initial locations \( \overline{I}_0^i \) of the automaton \( A_i \in \overline{A} \); \( V' = V_h \cup (\text{dom}(\sigma) \setminus \{ \text{time} \}) \). Since all the channels in the model \( M \) are urgent, \( \forall h \in H_{\text{si}} : T_{\overline{I}_0}(h) = 0 \).

Finally, \( \text{Init}' = R(\sigma) \), where \( R(\sigma) \) translates the valuation \( \{ x_0 \mapsto c_0, \ldots, x_n \mapsto c_n \} \) to the set of assignments \( \{ x_0 = c_0, \ldots, x_n = c_n \} \).
The function \( T_p : P \rightarrow \mathcal{P}(A_s) \) translates a process term \( p \in P \) to a set of extended automata and is defined in the following way:

\[
T_p(p) = \begin{cases} 
\{ T_q(q) \} & \text{if } p \in Q \\
\{ T_q(q_1), T_q(q_2) \} & \text{if } p \equiv q_1 \parallel q_2, q_1, q_2 \in Q.
\end{cases}
\]

The function \( T_q : Q \rightarrow A_s \) translates a \( \chi \) process term \( q \in Q \) to an extended automaton.

### 4.2 Translation function \( T_q \)

In this section, the translation function \( T_q(p) \) is defined inductively.

#### 4.2.1 Translation of the atomic process terms

**Skip**

The process term \( \text{skip} \) is an abbreviation for an action predicate that can only perform an internal action without changing the valuation.

\[
T_q(\text{skip}) = \langle \{ l_0, l_1 \}, l_0, \{(l_0, \text{true}, \tau_h, \tau_a, l_1) \}, l_0, l_0, l_1 \rangle,
\]

where \( \text{Inv}(l_0) = \text{true}, \text{Inv}(l_1) = \text{true}, T_{L_l}(l_0) = u, T_{L_l}(l_1) = o \) (Fig. 1).

![Figure 1: Extended automaton \( T_q(\text{skip}) \)](image)

**Multi-assignment**

Multi-assignment \( x_n := e_n, n \geq 1 \) is an abbreviation for an internal action that changes the values of the variables \( x_1, \ldots, x_n \) to the values of expressions \( e_1, \ldots, e_n \).

\[
T_q(x_n := e_n) = \langle \{ l_0, l_1 \}, l_0, \{(l_0, \text{true}, \tau_h, \{x_1 = e_1, \ldots, x_n = e_n\}, l_1) \}, l_0, l_0, l_1 \rangle,
\]

where \( \text{Inv}(l_0) = \text{true}, \text{Inv}(l_1) = \text{true}, T_{L_l}(l_0) = u, T_{L_l}(l_1) = o \) (Fig. 2).

**Send and Receive**

Undelayable send and receive process terms \( h!!e_n \) and \( h??x_n \) denote undelayable sending of expressions \( e_n \) via channel \( h \) and undelayable receiving via channel \( h \) into variables \( x_n \).
In UPPAAL, the values are not transmitted via a channel. Instead, additional shared variables $y_1, \ldots, y_n$ are used. We assume existence of a bijective function $f^* : H \times \mathbb{N} \rightarrow V_h$ that generates unique names of the communication variables: $y_i = f^*(h, i), i \in [1, n]$.

$$\begin{align*}
T_q(x_n := e_n) &= \langle \{l_0, l_1\}, l_0, \{\langle l_0, \text{true}, h!, \{y_1 = e_1, \ldots, y_n = e_n\}, l_1 \rangle\} \\
&\quad \cup \{\langle l_0, \text{true}, h?, \{x_1 = y_1, \ldots, x_n = y_n\}, l_1 \rangle\}, \\
&\quad \emptyset, \emptyset, \emptyset, \emptyset, \emptyset, \emptyset, \text{Inv}, T_L, l_1 \rangle,
\end{align*}$$

where $\text{Inv}(l_0) = \text{true}$, $\text{Inv}(l_1) = \text{true}$, $T_L(l_0) = u$, $T_L(l_1) = o$ (Fig. 3).

$$\begin{align*}
T_q(\delta) &= \langle \{l_0\}, l_0, \emptyset, \emptyset, \emptyset, \emptyset, \emptyset, \text{Inv}, T_L, \top \rangle,
\end{align*}$$

where $\text{Inv}(l_0) = \text{true}$, $\text{Inv}(l_1) = \text{true}$, $T_L(l_0) = u$, $T_L(l_1) = o$ (Fig. 4).

**Deadlock**

The deadlock process term cannot perform actions or delays but it is consistent. The corresponding extended timed automaton is

$$\begin{align*}
T_q(\delta) &= \langle \{l_0\}, l_0, \emptyset, \emptyset, \emptyset, \emptyset, \emptyset, \text{Inv}, T_L, \top \rangle,
\end{align*}$$
where $\text{Inv}(l_o) = \text{true}, T_L(l_o) = u$.

**Inconsistent process term**

The inconsistent process term $\bot$ is inconsistent for all valuations and cannot perform any action or delay. The corresponding extended timed automaton is

$$T_Q(\bot) = (\{l_o\}, l_o, \emptyset, \emptyset, \emptyset, \emptyset, \emptyset, \text{Inv}, T_L, \top),$$

where $\text{Inv}(l_o) = \text{false}, T_L(l_o) = u$.

### 4.2.2 Translation of the operators

In the translation of the operators, the extended automaton that is obtained by translating the process term $q \in Q$ is denoted by $T_Q(q) = A_Q^{q}$, where $A_Q^{q} = (L^q, F^q, E^q, V^q, V^\text{inv}, C^q, \text{Init}^q, \text{Inv}^q, T_L^q, T^q)$.

In a similar way, $A_Q^r$ denotes $T_Q(r), r \in Q$.

For the translation some additional functions are needed. The restriction of a function $f : A \rightarrow B$ to $C \subseteq A$ is denoted by $f \mid C$. If $f$ and $g$ are functions and $\text{dom}(f) \cap \text{dom}(g) = \emptyset$, then $f \cup g$ denotes function $h$ with the domain $\text{dom}(h) = \text{dom}(f) \cup \text{dom}(g)$, where $h(c) = f(c)$ if $c \in \text{dom}(f)$, and $h(c) = g(c)$ if $c \in \text{dom}(g)$.

For arbitrary sets $E, L, A, C$, where $E$ is a set of edges, $L$ is a set of locations, $A$ is a set of assignments, and $C$ is a set of clocks, four functions are defined. Function $\gamma : \mathcal{P}(E) \times L \times \mathcal{P}(A) \rightarrow \mathcal{P}(E)$ transforms the set of edges by adding a set of assignments to the assignment part of all incoming edges of a location. For instance, $\gamma(E, l, \{x = 1, y = 3\})$ returns a set of edges, where the set of assignments $\{x = 1, y = 3\}$ is added to the assignment parts of all incoming edges of the location $l$. Function $\sigma_1 : \mathcal{P}(E) \times L \times L \rightarrow \mathcal{P}(E)$ transforms the set of edges by replacing all occurrences of the first location as a source location with the second one. For instance, the function $\sigma_1(E, l, l')$ returns the set of edges, where all occurrences of the location $l$ as a source location are replaced with $l'$. Function $\sigma_2 : \mathcal{P}(E) \times L \times L \rightarrow \mathcal{P}(E)$ transforms the set of edges by replacing all occurrences of the first location as a sink location with the second one. For instance, the function $\sigma_2(E, l, l')$ returns the set of edges, where all occurrences of the location $l$ as a sink location are replaced with $l'$. Function $\varphi : \mathcal{P}(E) \times L \times \mathcal{P}(C) \rightarrow \mathcal{P}(E)$ transforms the set of edges by removing all outgoing edges of a location, that have an expression over clocks as (a part of) a guard.

### Delay

The abbreviation $\triangle d$ denotes a process term that first delays for $d$ time units, and then terminates by means of an internal action $\tau$.

To translate the delay operator, additional fresh clock variables are used. We assume that a unique name of the variable $c \in C$ is generated by some bijective function $f^c : L \rightarrow C$.

$$T_Q(\triangle d) =$$

\[
\{ l_o, l_i \}, \{ l_o, c = d, \tau_b, \tau_s, l_i \}, \emptyset, \emptyset, \{ c = 0 \}, \text{Inv}, T_L, l_i
\],

where $c = f^c(l_o)$, $\text{Inv}(l_o) = \{ c \leq d \}$, $\text{Inv}(l_i) = \text{true}, T_L(l_o) = 0, T_L(l_i) = 0$ (Fig. 5).

### Any delay operator

The any delay operator $[q]$ allows time transitions of arbitrary duration for the behavior of
Due to the introduction of the location \( l_0 \), the location \( l_0 \) can become unreachable.

**Repetition**

Process term \(*q\) represents infinite repetition of process term \( q\). If the extended automaton \( A_q^d = T_q(q) \) has a final location, \( l_q^f \in L^d \), then the incoming edges of the final location are redirected to the initial location, and the initializations are added to the assignment parts of these edges. If the extended automaton \( A_q^d \) does not have a final location, \( l_q^f = \top \), then \( T_q(*q) = A_q^d \). The resulting extended automaton is defined in the following way.

\[
T_q(*q) = \langle L^* \cup \{ l_q^f \}, l_q, E, V^*, V^{hq}, C^*, Init^*, Inv, T_L, l_0^f \rangle,
\]

where \( E = q(E^* \cup \sigma_1(E^*, l_q^f, l_q, C^*), Inv(l_q) = true, Inv \mid L^* = Inv^q, T_L(l_q) = 0 \), and \( T_L \mid L^* = T_1^q \).

As an example the extended automaton \( T_q([\text{skip}]) \) is shown in Fig. 6. There the locations \( l' \) and \( l_1 \) are the initial and final locations of the automaton \( T_q([\text{skip}]) \), respectively, and \( l_0 \) is a new initial location.

Due to the introduction of the location \( l_0 \), the location \( l_0^f \) can become unreachable.

**Sequential composition**

The sequential composition of process terms \( q \) and \( r \) behaves as process term \( q \) until \( q \) terminates, and then continues to behave as process term \( r \). In order to combine two automata in one it is necessary that \( L^q \cap L^r = \emptyset \) and \( C^q \cap C^r = \emptyset \). For that the renaming function
Alternative composition

Alternative composition operator $q \parallel r$ models a non-deterministic choice between $q$ and $r$ for action transitions. The passage of time by itself cannot result in making a choice. In order to combine two automata in one it is necessary that $L^q \cap L^r = \emptyset$ and $C^q \cap C^r = \emptyset$. For that the renaming function $f$ is used: $A^q_r = f(T_q(r), L^q, C^q)$.

The alternative composition $q \parallel r$ is translated by adding the initial location and merging the final locations of the extended automata $A^q_r$ and $A^r_r$ in the following way.

$$T_q(q \parallel r) = \langle L, l_0, E, V^q \cup V^r, V^{\text{hr}} \cup V^{\text{hr}}, C^q \cup C^r, \text{Init}^q \cup \text{Init}^r, \text{Inv}, T_L, l_f \rangle,$$

where $E = \sigma_2(\gamma(E^q, l_0, \text{Init}^q), E^r, l_1, l_f)$, and $\text{Inv} = (\text{Inv}^q \cup \left(L^q \setminus \{l_f\}\right)) \cup \text{Inv}^r, T_L = (T_L^q \cup \left(L^q \setminus \{l_f\}\right)) \cup T_L^r$.
where if \( l_q^f \neq \top \) and \( l_r^f \neq \top \), then \( L = ((L_q \cup L_r) \cup \{l_o\}) \setminus \{l_r^f\} \), and \( l_f = l_q^f \).

\[
\begin{array}{c}
\text{U} \\
\text{true, } \tau, \tau \Rightarrow \text{U} \\
\text{true, } \tau, \tau \Rightarrow \text{U} \\
\end{array}
\]

Figure 9: Extended automata \( T_q(x_n := e_n[\text{skip}]) \).

Otherwise, \( L = (L_q \cup L_r) \cup \{l_o\} \), and if \( l_q^f = \top \) then \( l_f = l_q^f \), otherwise \( l_f = l_r^f \).

The set of edges \( E = E' \cup \sigma_1(E', l_0^r, l_0^r, l_0^s, l_0^s) \), where \( E' = \sigma_2(E, l_q^f, l_f) \cup \sigma_2(E, l_r^f, l_f) \).

The function \( \text{Inv} \) is defined as follows: \( \text{Inv}(l_0) = \text{Inv}^q(l_0) \land \text{Inv}^r(l_0) \), and \( \text{Inv} \mid (L \setminus \{l_o\}) = (\text{Inv}^q \cup \text{Inv}^r) \mid (L \setminus \{l_o\}) \).

Finally, if \( T_q(l_o^r) = u \), then \( T_L(l_o) = T_q(l_o^r) \). Furthermore, \( T_L \mid (L \setminus \{l_o\}) = (T_q \cup T_r) \mid (L \setminus \{l_o\}) \).

The case when both automata have final locations \( (T_q(x_n := e_n[\text{skip}])) \) is shown in Fig. [9] where \( l_0^r \) and \( l_0^r \) are the initial and the final location of the extended automaton \( T_q(\text{skip}) \), and \( l_o \) is a new initial location.

The case when only one automaton has a final location \( (T_q(x_n := e_n[\text{skip}])) \) is shown in Fig. [10] where \( l_0^r \) and \( l_0^r \) are the initial and the final location of \( T_q(x_n := e_n) \), \( l_0^r \) is the initial location of the extended automaton \( T_q(\ast \text{skip}) \), and \( l_0 \) is a new initial location.

\[
\begin{array}{c}
\text{U} \\
\text{true, } \tau, \tau \Rightarrow \text{U} \\
\text{true, } \tau, \tau \Rightarrow \text{U} \\
\end{array}
\]

Figure 10: Extended automata \( T_q(x_n := e_n[\text{skip}]). \)
5 Correctness of the translation scheme

5.1 Preliminaries

In this section we give some notions, which will be used in the subsequent theorems. First, we provide the semantics of the repetition and delay operators. Then, we give the definition of the corresponding states in $\chi$ and UPPAAL transition systems. After that we prove one preliminary lemma.

In UPPAAL semantics there are conditions, saying that some action is possible if there are no committed locations in $\mathcal{L}$. Since, in the translation committed locations are never used, we skip in the proofs of these conditions.

5.1.1 The semantics of the repetition and delay operators

In [12] the semantics of the repetition and delay operators is given in terms of other language elements. Since those elements have not been included into the translated set of the process terms, we provide here the deduction rules for the repetition [9] and delay operators, which do not include other language elements. It can be shown that these deduction rules coincide with the formal semantics, though we omit the proofs here.

The semantics of the repetition operator

$$
\frac{\langle p, \sigma, E \rangle \xrightarrow{\sigma, a, \sigma'} \langle \checkmark', \sigma', E \rangle}{\langle *p, \sigma, E \rangle \xrightarrow{\sigma, a, \sigma'} \langle *p', \sigma', E \rangle}
$$

$$
\frac{\langle p, \sigma, E \rangle \xrightarrow{t, \rho} \langle p', \sigma', E \rangle}{\langle *p, \sigma, E \rangle \xrightarrow{t, \rho} \langle *p', \sigma', E \rangle}
$$

$$
\frac{\langle p, \sigma, E \rangle \xrightarrow{\sigma} \langle *p, \sigma, E \rangle}{\langle *p, \sigma, E \rangle \xrightarrow{\sigma} \langle *p, \sigma, E \rangle}
$$

The semantics of the delay operator

$$
\sigma(d) = 0
$$

$$
\frac{\langle \Delta d, \sigma, E \rangle \xrightarrow{\sigma, t, \sigma} \langle \checkmark, \sigma, E \rangle}{\rho \in \mathcal{O}(\sigma, t), t \leq \sigma(d)}
$$

$$
\frac{\langle \Delta d, \sigma, E \rangle \xrightarrow{\rho} \langle \Delta(d - t), \rho(t), E \rangle}{\rho \in \mathcal{O}(\sigma, t), t \leq \sigma(d)}
$$
During the time transition the valuation at each time point \( s \in [0, t] \) is given by \( \rho(s) \in \Omega(\sigma, \tau) \).

### 5.1.2 Definition of corresponding states

The transition system of the \( \chi \) model \( M \) is denoted by \( \mathcal{M} \), and the transition system of the UPPAAL model \( \mathcal{T}_M(M) \) is denoted by \( \mathcal{T}_M(M) \). If the transition system contains a transition, it is denoted by \( \mathcal{T} \).

The correspondence between states of hybrid transition system of \( \chi \) and states of state transition system of UPPAAL is defined as follows.

Let \( L_t \) be a set of final locations, and \( Corr : (L_t \times \ldots \times L_n) \times \mathcal{P}(L_t) \rightarrow (L_t \times \ldots \times L_m) \cup \{ \emptyset \} \) be a function that transforms a vector of locations \( (l_1, \ldots, l_n) \) into a vector of locations \( (l'_1, \ldots, l'_m) \) by removing all final locations: \( \forall i, 1 \leq i \leq n, l_i \in L_t : (\forall j, 1 \leq j \leq m, l'_j \neq l_i) \), and preserving all non-final location: \( \forall j, 1 \leq j \leq m : (\exists i, 1 \leq i \leq n) : l'_j = l_i \). Moreover, the order of the locations is not changed: \( \forall i, j, 1 \leq i \leq n, 1 \leq j \leq n, i < j, l'i_i \neq l'_j \). If all locations are final, the function returns \( \emptyset \), where \( \emptyset \) denotes an empty vector. A vector is a mapping with a domain \( \{1, \ldots, n\} \); an empty vector shows the absence of such mapping.

**Definition 5.1.**

1. The initial states \( (\partial_{a_0}(v_{10}(q_0), \ldots, v_{m0}(q_n)), \sigma_0), E) \) and \( (l_1, \ldots, l_n), a_0 \) are corresponding, if \( \forall i : 1 \leq i \leq n, l_i \in T_{\delta}(q_i), l_i \) \( l_i \) is an initial location of the automaton \( T_{\delta}(q_i) \), \( a_0 | \{0, \ldots, m-1\} \subset \text{dom}(\sigma_0) = \sigma_0 \).

2. The intermediate states \( (\partial_{a_0}(v_{10}(q_0), \ldots, v_{m0}(q_n)), \sigma', E') \) and \( (l'_1, \ldots, l'_n), a' \) are corresponding, if \( Corr((l'_1, \ldots, l'_n), L_I) = (l'_1, \ldots, l'_n) \) and \( \forall i : 1 \leq i \leq m, l'_i \) is an initial location of \( T_{\delta}(q_i) \), \( a' | \{0, \ldots, m-1\} \subset \text{dom}(\sigma') = \sigma' \).

3. The final states \( (\chi, \sigma'', E') \) and \( (l''_1, \ldots, l''_n), a'' \) are corresponding if \( Corr((l''_1, \ldots, l''_n), L_I) = \emptyset \) and \( a'' | \{0, \ldots, m-1\} \subset \text{dom}(\sigma'') = \sigma'' \).

4. There are no other corresponding states.

### 5.1.3 Preliminary lemma

To prove the correctness of the translation scheme we need two additional lemmas. In \( \chi \) semantics the process term \( [q] \) has the same action behaviour as \( q \) and it may also perform an arbitrary time transition. To translate it we added a new location into the automaton \( T_{\delta}(q) \) in which the automaton can delay. With the first lemma we show that the action behaviour stays the same nevertheless.

**Lemma 1.**

\[
[ T_{\delta}([q], \sigma, E) ] \models (l_0, a) \overset{a}{\rightarrow} (l_1, a') \iff [ T_{\delta}([q], \sigma, E) ] \models (l'_0, a) \overset{a}{\rightarrow} (l'_1, a'),
\]

where \( l_0 = (l'_0), l_1 = (l'_1), l_1' = (l_0) \) is the initial location of \( T_{\delta}(q) \), \( l'_1 \) is a location of \( T_{\delta}(q) \), \( l_0 \) is the initial location of \( T_{\delta}([q]) \).
Proof (Lemma 2).

First, we prove that \( \mathcal{T}(\langle q, \sigma, E \rangle) \) is not possible via an edge with an expression over clocks in its guard. Let \( \mathcal{T}(\langle q, \sigma, E \rangle) \) have the initial location \( \mathcal{L}_0 \), a location \( \mathcal{L}_1 \), and an edge \( e^\sigma = \langle \mathcal{L}_2, g^\sigma, \tau_n, a^\sigma, \mathcal{L}_3 \rangle \). Moreover, \( \alpha \vdash \text{Inv}(\mathcal{L}_2), \alpha \vdash g^\sigma, \alpha' \vdash \text{Inv}(\mathcal{L}_3) \), and \( \alpha' = a^\sigma(\alpha) \).

Applying \( \mathcal{T}(\langle q, \sigma, E \rangle) \) adds a new initial location \( \mathcal{L}_4 \) into an extended automaton \( \mathcal{T}(\langle q, \sigma, E \rangle) \), such that Inv(\mathcal{L}_4) = true. Moreover, new edges are added such that the location \( \mathcal{L}_5 \) has a time edge leading to \( \mathcal{L}_6 \) with no expression over the clock in the guard, than \( \mathcal{L}_5 \) will have an outgoing edge with the same guard, synchronization label and assignment, leading to the location \( \mathcal{L}_7 \).

To prove that \( \mathcal{T}(\langle q, \sigma, E \rangle) \) is not possible via an edge with an expression over clocks in its guard.

To prove that \( \mathcal{T}(\langle q, \sigma, E \rangle) \) is not possible via an edge with an expression over clocks in its guard.

To prove that \( \mathcal{T}(\langle q, \sigma, E \rangle) \) is not possible via an edge with an expression over clocks in its guard.

Proof (Lemma 2).

The proof is straightforward. According to the UPPAAL semantics, \( NA \) can make a time transition for \( t \) time units if the invariant stays satisfied, i.e. \( t \in [0, d - t_0] \). Similarly, \( NA' \) can make a time transition for \( t \) time units if the invariant stays satisfied, i.e. \( t \in [0, d'] \). Knowing that \( d' = d - t_0 \), we can say that the time behaviour of these two automata is the same.
5.2 Theorem 1

Theorem 1. Let $p$ and $p'$ be closed process terms, $\sigma$, $\sigma'$, $a$, $a'$ be valuations, such that $\text{dom}(\sigma) = \text{dom}(\sigma')$ and $\text{dom}(a) = \text{dom}(a')$, $E$ be an environment, $I$ be a location vector, and the states $(p, \sigma, E)$ and $(I, a)$ be corresponding states. Then:

Lemma 1.1. for any non-communication action $a$

$\| M \| = (p, \sigma, E) \xrightarrow{a} (\sigma', E) \Rightarrow \exists \tau', a': T_{M}(M) \| = (I, a) \xrightarrow{\tau, a'} (I', a')$, and $(\sigma', E)$ and $(I', a')$ are corresponding states.

Lemma 1.2. for any non-communication action $a$

$\| M \| = (p, \sigma, E) \xrightarrow{\sigma(a), a'} (\sigma', E) \Rightarrow \exists \tau', a': T_{M}(M) \| = (I, a) \xrightarrow{\tau, a'} (I', a')$, and $(\sigma', E)$ and $(I', a')$ are corresponding states.

Lemma 1.3. for any communication action $ca$

$\| M \| = (p, \sigma, E) \xrightarrow{\sigma(a), cs, a'} (\sigma', E) \Rightarrow \exists \tau', a': T_{M}(M) \| = (I, a) \xrightarrow{\tau, a'} (I', a')$, and $(\sigma', E)$ and $(I', a')$ are corresponding states.

Lemma 1.4. for any communication action $ca$

$\| M \| = (p, \sigma, E) \xrightarrow{\sigma(a), cs, a'} (\sigma', E) \Rightarrow \exists \tau', a': T_{M}(M) \| = (I, a) \xrightarrow{\tau, a'} (I', a')$, and $(\sigma', E)$ and $(I', a')$ are corresponding states.

Lemma 1.5. for any time transition

$\| M \| = (p, \sigma, E) \xrightarrow{\tau} (p', \sigma', E) \Rightarrow \exists \tau', a': T_{M}(M) \| = (I, a) \xrightarrow{\tau, a'} (I', a')$, and $(\sigma', E)$ and $(I', a')$ are corresponding states.

The proofs are by induction on the structure of the closed process term $p$.

Proof (Lemma 1.1). According to the rules [1.2-2] [1.2-5] the process term $(\partial_{\alpha_{l}}(v_{l}(p)), \sigma, E)$ can perform an action $a$ and then terminate if a process term $p$ can perform an action $a$ and terminate:

1. Let us consider the case when $p \in Q$. In the $\chi$ semantics there are no termination transition rules (with $a$ as specified) defined for deadlock, inconsistent process term, send, receive, sequential composition and repetition, therefore the lemma holds trivially for these cases. The proofs for the other cases are given below.

(a) The process term skip is an abbreviation for an action predicate $\emptyset : true \Rightarrow \tau$ (1.1) that performs an internal action $\tau$ without changing valuation $\sigma = \sigma'$ and then terminates (1.3). According to the translation scheme, the corresponding extended automaton $T_{\emptyset}(\text{skip})$ has the initial location $l_{o}$, final location $l_{f}$, the only edge $(l_{o}, true, l_{f}, l_{f}, l_{f})$, and $\text{Inv}(l_{o}) = true, \text{Inv}(l_{f}) = true$.

Since the translation functions $T_{p}$ and $T_{M}$ do not change locations and edges, $\| T_{M}(\partial_{\alpha_{l}}(v_{l}(\text{skip})), \sigma, E) \| = (I, a) \xrightarrow{\alpha' \downarrow \text{dom}(\sigma')} (I[l_{f}, l_{f}], a')$. According to the UPPAAL semantics, the empty assignment $\tau_{o}$ does not change the valuation, $\sigma' = \sigma' \uparrow \text{dom}(\sigma')$. Since the location $l_{f}$ is a final
location \((\text{Corr}(l_i), \{l_i\}) = \emptyset\) and \(\sigma' = \alpha' \mid \text{dom}(\sigma')\), the states \((\check{\omega}, \sigma', E')\) and \((\check{\omega}, \alpha')\) are corresponding.

(b) Multi-assignment \(x_n := e_n, n \geq 1\) is an abbreviation for an action predicate \(\{x_n\} := e_i \wedge \ldots \wedge x_n = e_n \Rightarrow \tau\) that performs an internal action \(\tau\) and assigns the values of the expressions \(e_i, \ldots, e_n\) to the variables \(x_i, \ldots, x_n\) respectively. According to the translation scheme, the corresponding extended automaton \(T_\delta(x_n := e_n)\) has the initial location \(l_0\), final location \(l_1\), and the only edge \((l_0, \text{true}, \tau, \{x_i := e_i, \ldots, x_n := e_n\}, l_1)\), and \(\text{Inv}(l_0) = \text{true}, \text{Inv}(l_1) = \text{true}\).

Since the translation functions \(T_\delta\) and \(T_\tau\) do not change locations and edges, \(\llbracket T_\delta((\partial_{x_n} v_{i_1 k}(x_n := e_n), \sigma, E)) \rrbracket \models \llbracket \rho[l_1/l_2], \alpha' \rrbracket\).

Since the translation functions \(T_\delta\) and \(T_\tau\) do not change locations and edges, \(\llbracket T_\tau ((\partial_{x_n} v_{i_1 k}(x_n := e_n), \sigma, E)) \rrbracket \models \llbracket \rho[l_1/l_2], \alpha' \rrbracket\).

(c) The process term \(\Delta d\) can perform an internal action \(\tau\) without changing valuation \((\sigma = \sigma')\) and terminate if \(\sigma(d) = 0\) \((\check{\omega})\). According to the translation scheme, the corresponding extended automaton \(T_\delta(\Delta d)\) has the initial location \(l_0\), final location \(l_1\), the only edge \((l_0, \epsilon := d, \tau, \tau, l_1)\), and \(\text{Inv}(l_0) = \epsilon \leq d, \text{Inv}(l_1) = \text{true}\.

From the proof of the Lemma \(\check{\omega}\) if \(\sigma(d) = 0\), delay is finished and \(\epsilon(0) = d\).

Since the translation functions \(T_\delta\) and \(T_\tau\) do not change locations and edges, \(\llbracket T_\delta((\partial_{x_n} v_{i_1 k}(\Delta d), \sigma, E)) \rrbracket \models \llbracket \rho[l_1/l_2], \alpha' \rrbracket\).

According to the UpPAAAL semantics, the empty assignment \(\tau_\delta\) does not change the valuation, \(\alpha = \alpha'\). Hence, \(\sigma' = \alpha' \mid \text{dom}(\sigma')\). Since the location \(l_i\) is a final location \((\text{Corr}(l_i), \{l_i\}) = \emptyset\) and \(\sigma' = \alpha' \mid \text{dom}(\sigma')\), the states \((\check{\omega}, \sigma', E')\) and \((\check{\omega}, \alpha')\) are corresponding.

(d) According to the \(\chi\) semantics, the process term \([q]\) can perform an action \(a\) and then terminate if \(q\) can perform an action \(a\) and then terminate \((\check{\omega})\). As the induction step, it is assumed that if \(\llbracket M \rrbracket \models \langle q, \sigma, E \rangle \xrightarrow{a, \alpha} \langle \check{\omega}, \sigma', E' \rangle\), and the corresponding extended automaton \(T_\delta([q])\) has the initial location \(l_0\), final location \(l_1\), and the edge \(e = \langle l_0, g^a, \tau, \alpha', l_1 \rangle\). Furthermore, \(\alpha \models \text{Inv}(l_0), \alpha \models g^a, \text{and } \alpha' \models \text{Inv}(l_1)\). Moreover, \(\alpha' \mid \text{dom}(\sigma') = \sigma'\).

According to the lemma \(\check{\omega}\), the extended automaton \(T_\delta([q])\) will have the initial location \(l_0\), final location \(l_1\), and the edge \(e = \langle l_0, g^a, \tau, \alpha', l_1 \rangle\). Furthermore, \(\text{Inv}(l_0) = \text{true}, \alpha \models g^a, \text{and } \alpha' \models \text{Inv}(l_1)\). Moreover, \(\alpha' \mid \text{dom}(\sigma') = \sigma'\).

Since the functions \(T_\delta\) and \(T_\tau\) do not change the locations, edges and invariants, \(\llbracket T_\delta((\partial_{x_n} v_{i_1 k}([q]), \sigma, E)) \rrbracket \models \llbracket \rho[l_1/l_2], \alpha' \rrbracket\).

Since \(l_0^{\alpha'}\) is a final location \((\text{Corr}(l_0^{\alpha'}), \{l_0^{\alpha'}\}) = \emptyset\) and \(\sigma' = \alpha' \mid \text{dom}(\sigma')\), the states \((\check{\omega}, \sigma', E')\) and \((\check{\omega}, \alpha')\) are corresponding.

(e) The process term \([q]\), \([q_1]\), can perform an action \(a\) and then terminate, only if either \(q_1\) or \(q_2\) can perform this action \(a\) and terminate \((\check{\omega})\). Since the proofs for both cases are similar, only the proof for the case, when \(q_1\) can make an action \(a\) and terminate, has been given.

As the induction step, it is assumed that \(\llbracket \partial_{x_n} v_{i_1 k}(\{q_1\}, \sigma, E) \rrbracket \models \langle q_1, \sigma, E \rangle \xrightarrow{a, \alpha'} \langle \check{\omega}, \sigma', E' \rangle\), and the corresponding extended automaton \(T_\delta([q_1])\) has the initial location \(l_0^{\alpha'}\), final location \(l_1^{\alpha'}\), and the edge \(e = \langle l_0^{\alpha'}, g^a, \tau, \alpha', l_1^{\alpha'} \rangle\). Furthermore, \(\alpha \models \text{Inv}(l_0^{\alpha'}), \alpha \models g^a, \text{and } \alpha' \models \text{Inv}(l_1^{\alpha'})\). Moreover, \(\sigma' = \alpha' \mid \text{dom}(\sigma')\).
The function $T_\mathcal{Q}(q_1 \| q_2)$ adds a new initial location $l_o$, such that $\text{Inv}(l_o) = \text{Inv}(l_1^0) \land \text{Inv}(l_2^0)$, and redirects the edges so that $\forall e \in T_\mathcal{Q}(q_1), e = \langle l_1^0, g^0, \tau_h, a^0, l_1^0 \rangle : \exists e' \in T_\mathcal{Q}(q_1 \| q_2), e' = \langle l_2^0, g^0, \tau_h, a^0, l_2^0 \rangle$, where $l_1$, $l_2$ are the initial and final locations of $T_\mathcal{Q}(q_1 \| q_2)$.

Since the functions $T_\mathcal{Q}$ and $T_M$ do not change the locations, edges and invariants, $\llbracket T_M(M) \rrbracket \models \langle \ell, \alpha \rangle \xrightarrow{\gamma} \langle \llbracket l_0 \rrbracket, \alpha' \rangle$.

Since $l_f$ is the final location $(\text{Corr}(l_f), \{l_f\}) = \varnothing$ and $\sigma' = \alpha' \mid \text{dom}(\sigma')$, the states $(\varnothing, \sigma', E')$ and $(\tilde{\ell}, \alpha')$ are corresponding.

2. If $p$ is of the form $q_1 \| q_2$, the lemma holds trivially, since in $\chi$ semantics there are no termination transition rules (with $a$ as specified) defined for parallel composition.

\begin{center} $\square$ \end{center}

\textbf{Proof (Lemma 1.3).}

According to the rules 1.22 1.23 the process term $\langle \partial_\mathcal{H}(v_H(p)), \sigma, E \rangle$ can perform an action $a$ and then continue as $p'$ if a process term $p$ performs an action $a$ and continue as $p'$.

1. Let’s first consider the case, when $p \in \chi$. In the $\chi$ semantics there is no transition rules (with $a$ as specified) defined for skip, assignment, deadlock, inconsistent process term, send, receive, and delay, therefore the lemma holds trivially for these cases.

(a) According to the $\chi$ semantics, the process term $[q]$ can perform an action $a$ and then continue as $p'$ if $q$ can perform an action $a$ and then continue as $p'$. As the induction step, it is assumed that if $\llbracket (q, \sigma, E) \rrbracket \models \langle q, \sigma, E \rangle \xrightarrow{\sigma a \sigma'} \langle p', \sigma', E' \rangle$, then the corresponding extended automaton $T_\mathcal{Q}(q)$ has the initial location $l_0$, location $l_i^0 \mapsto l_f$, and the edge $e = \langle l_0^0, g^0, \tau_h, a^0, l_0^0 \rangle$. Furthermore, $\alpha \models \text{Inv}(l_0)$, $\alpha \models g^0$, and $\alpha' \models \text{Inv}(l_f)$.

Moreover, the location $l_i^0$ is an initial location of the extended automaton $T_\mathcal{Q}(p')$, and $\sigma' = \alpha' \mid \text{dom}(\sigma')$.

Applying $T_\mathcal{Q}([q])$ adds a new initial location $l_0$ into an extended automaton $T_\mathcal{Q}(q)$, such that $\text{Inv}(l_0) = \chi$, the outgoing edges as the location $l_i^0$ are duplicated and reconnected to the location $l_0$, except for the edges with clock expressions in guards. From the proof of the Lemma 1.3 follows that the extended automaton $T_\mathcal{Q}([q])$ has the edge $e = \langle l_0, g^0, \tau_h, a^0, l_0 \rangle$. Since the functions $T_\mathcal{Q}$ and $T_M$ do not change the locations, edges and invariants, $\llbracket T_M((\partial_\mathcal{H}(v_H([q])), \sigma, E)) \rrbracket \models \langle \ell, \alpha \rangle \xrightarrow{\gamma} \langle \llbracket [l_0] \rrbracket, \alpha' \rangle$.

Since $l_i^0$ is an initial location of $T_\mathcal{Q}(p')$ $(\text{Corr}(l_i^0), \{l_i^0\}) = \{l_f\})$ and $\sigma' = \alpha' \mid \text{dom}(\sigma')$, the states $(\varnothing, \sigma', E')$ and $(\tilde{\ell}, \alpha')$ are corresponding.

(b) The process term $q_1 \| q_2$ can perform an action $a$ and then continue as $p'$ in two cases: if $q_1$ performs an action $a$ and terminates, $p' \equiv q_2$, 1.11 or if $q_1$ performs an action $a$ and then continues as $q_1'$, $p' \equiv q_1'; q_2$. 1.12.

- Let’s first consider the case when $q_1$ can perform an action $a$ and terminate. As the induction step, it is assumed that the corresponding extended automaton $T_\mathcal{Q}(q_1)$ has the initial location $l_i^0$, the final location $l_f^0$ and the edge $\langle l_i^0, g, \tau_h, a^0, l_f^0 \rangle$, such that $\text{Inv}(l_i^0)$ and $g$ are evaluated as true in $a$, and $\text{Inv}(l_f^0)$ is true. Furthermore, the extended automaton $T_\mathcal{Q}(q_1)$ has the initial location $l_i^0$. Moreover, $\forall x, \sigma(x) \equiv \sigma'(x) : x \equiv e \in a^0$.
The translation function $T_q(q_i; q_a)$ reconnects all input edges of the location $l^q_i$ to the location $l^q_a$ and removes $l^q_a$. Since the functions $T_F$ and $T_M$ do not change the locations, edges and invariants, $\mathbb{T}_M((\partial_{h(a)}, v_{lh_a}(q_i; q_a), q, E)) \equiv (\langle l, h \rangle, a) \mapsto (\langle l^q_i / l^q_a \rangle, a)\). 

Since $l^q_i$ is an initial location of $T_q(q_i) (\text{Corr}((l^q_i), \{l^q_i\}))$ and $\alpha' = \alpha ' \upharpoonright \text{dom}(\sigma')$, the states $(p', \alpha', E')$ and $(\langle l, \alpha' \rangle)$ are corresponding.

- Let's consider the case when $q_i$ performs an action $a$ and then continues as $q'_i$. As the induction step, it is assumed that the corresponding extended automaton $T_q(q_i)$ has the initial location $l^q_i$, a non-final location $l^q_i$, and the edge $\langle l^q_i, g, \tau_h, a^\alpha, l^q_i \rangle$, such that $\text{inv}(l^q_i)$ and $g^\alpha$ are evaluated as true in $\alpha$, and $\text{inv}(l^q_i)$ = true. Furthermore, the extended automaton $T_q(q'_i)$ has the initial location $l^q_i$. Moreover, $\alpha' \setminus \text{dom}(\sigma') = \sigma'$.

Since the translation function $T_q(q_i; q_a)$ does not change the locations $l^q_i$, $l^q_i$, and the edge $\langle l^q_i, g, \tau_h, a^\alpha, l^q_i \rangle$, and the functions $T_F$ and $T_M$ do not change the locations, edges and invariants, $\mathbb{T}_M((\partial_{h(a)}, v_{lh_a}(q_i; q_a), q, E)) \equiv (\langle l, h \rangle, a) \mapsto (\langle l^q_i / l^q_a \rangle, a')\). 

Since $l^q_i$ is an initial location of $T_q(q_i) (\text{Corr}((l^q_i), \{l^q_i\}))$ and $\alpha' = \alpha ' \upharpoonright \text{dom}(\sigma')$, the states $(p', \alpha', E')$ and $(\langle l, \alpha' \rangle)$ are corresponding.

(c) The process term $q_i$, $\parallel q_a$ can perform an action $a$ and then continue as $p'$, only if either $q_i$ can perform an action $a$ and continue as $q'_i$, $p' \equiv q'_i$, or $q_a$ can perform an action $a$ and continue as $q_a'$, $p' \equiv q_a'$. \(\{T,F\}\). Since the proofs for both cases are similar, only the proof for the case, when $q_i$ can make an action $a$ and then continue as $q'_i$, has been given.

As the induction step, it is assumed that $\mathbb{T}_M((\partial_{h(a)}, q_i, q, E)) \equiv (\langle q_i, q, \sigma, E \rangle) \mapsto (\langle q_i, q, q', \sigma', E' \rangle)$, and the corresponding extended automaton $T_q(q_i)$ has the initial location $l^q_i$, a non-final location $l^q_i$, and $\exists \in \epsilon = \langle l^q_i, g^\alpha, \tau_h, a^\alpha, l^q_i \rangle$. Furthermore, $\alpha \equiv \text{inv}(l^q_i)$, $\alpha \equiv g^\alpha$, and $\alpha' \equiv \text{inv}(l^q_i)$. The location $l^q_i$ is the initial location of the extended automaton $T_q(q_i)$. Moreover, $\alpha' \upharpoonright \text{dom}(\sigma') = \sigma'$.

The function $T_q(q_i, q_a)$ adds a new initial location $l_0$, such that $\text{inv}(l_0) = \text{inv}(l^q_i) \land \text{inv}(l^q_i)$, and redirects the edges so that $\forall e_i \in T_q(q_i), e_i = \langle l_0, g^\alpha, \tau_h, a^\alpha, l^q_i \rangle$ : $\exists e'_i \in T_q(q_i, q_a), e'_i = \langle l_0, g^\alpha, \tau_h, a^\alpha, l^q_i \rangle$, where $l_0$ is the initial location of $T_q(q_i, q_a)$. Since the functions $T_F$ and $T_M$ do not change the locations, edges and invariants, $\mathbb{T}_M((\partial_{h(a)}, v_{lh_a}(q_i, q_a), q, E)) \equiv (\langle l, h \rangle, a) \mapsto (\langle l_0/l_0 \rangle, \alpha')\). 

Since $l^q_i$ is the initial location of the extended automaton $T_q(q_i) (\text{Corr}((l^q_i), \{l^q_i\})) = (l^q_i)$ and $\alpha' = \alpha ' \upharpoonright \text{dom}(\sigma')$, the states $(q'_i, \alpha', E')$ and $(\langle l, \alpha' \rangle)$ are corresponding.

(d) According to the $\chi$ semantics, $*q$ can make an action $a$ and continue as $p'$ if $q$ can make an action $a$ and terminate, $p' \equiv *q$, or if $q$ can make an action $a$ and continue as $q_a$, $p' \equiv q'_a$. \(\{T,F\}\).

- In case when $p' \equiv *q$, as an induction step it is assumed that the corresponding extended automaton $T_q(q_i)$ has the initial location $l^q_i$, final location $l^q_i$, and the edge $\langle l^q_i, g^\alpha, \tau_h, a^\alpha, l^q_i \rangle$, and $\text{inv}(l^q_i)$, and $g^\alpha$ are evaluated as true in the valuation $\alpha$, and $\text{inv}(l^q_i)$ = true. Moreover, $\alpha' \setminus \text{dom}(\sigma') = \sigma'$.

The translation function $T_q(*q)$ redirects the edges, such that $\forall e_i \in T_q(q_i), e_i = \langle l^q_i, g^\alpha, \tau_h, a^\alpha, l^q_i \rangle$ : $\exists e_\gamma \in T_q(q_i, q_a), e_\gamma = \langle l^q_i, g^\alpha, \tau_h, a^\alpha, l^q_i \rangle$.

Since the functions $T_F$ and $T_M$ do not change the locations, edges and invariants, $\mathbb{T}_M((\partial_{h(a)}, v_{lh_a}(q_i; q_a), q, E)) \equiv (\langle l, h \rangle, a) \mapsto (\langle l^q_i / l^q_i \rangle, a)\). 

Since $l^q_i$ is the initial location of the extended automaton $T_q(*q) (\text{Corr}((l^q_i), \{l^q_i\})) = (l^q_i)$ and $\alpha' = \alpha ' \upharpoonright \text{dom}(\sigma')$, the states $(*q, \alpha', E')$ and $(\langle l, \alpha' \rangle)$ are corresponding.
In case when \( p' \equiv q' \vdash q \), as an induction step it is assumed that the corresponding extended automaton \( T_\delta(q) \) has the initial location \( l_0^0 \), non-final location \( l_1^0 \), and the edge \( \langle l_0^0, g^0, \tau_0^0, \alpha^0, l_1^0 \rangle \). The location \( l_1^0 \) is the initial location of the extended automaton \( T_\delta(q' \vdash q) \). Moreover, \( \text{Inv}(l_2^0) \), and \( g^0 \) are evaluated as true in the valuation \( \alpha \), and \( \text{Inv}(l_3^0) \) is evaluated as true in \( \alpha' \). Furthermore, \( \alpha' \upharpoonright \text{dom}(\alpha) = \alpha' \).

The translation function \( T_\delta(q \vdash q) \) does not affect non-final locations and the edges between them. Hence, the corresponding extended automaton \( T_\delta(q \vdash q) \) has the edge \( \langle l_0^0, g^0, \tau_0^0, \alpha^0, l_1^0 \rangle \). Moreover, both \( \text{Inv}(l_2^0) \) and \( g^0 \) are evaluated as true in \( \alpha \), and \( \text{Inv}(l_3^0) \) is evaluated as true in \( \alpha' \).

Since the functions \( T_\delta \) and \( T_M \) do not change the locations, edges and invariants, \( \llbracket T_M((\delta_{\alpha_0}(v_{1H}(q)), \sigma, E)) \rrbracket \equiv \llbracket (l_2^0/l_2^0, \alpha') \rrbracket \).

Since \( l_2^0 \) is a non-final location \( (\text{Corr}(l_2^0), [l_2^0]) = (l_2^0) \) and \( \alpha' = \alpha' \upharpoonright \text{dom}(\alpha') \), the states \( (q_1, \sigma', E') \) and \( (l', \alpha') \) are corresponding.

2. In the case, when \( p = \| q_2, p \) can make an action \( a \) and continue as \( p' \) in following cases (1-19):

   (a) \( q_1 \) can perform the action \( a \) and terminate \( (p' \equiv q_2) \)
   (b) \( q_1 \) can perform the action \( a \) and continue as \( q'_1 \) \( (p' \equiv q'_1 \| q_2) \)
   (c) \( q_2 \) can perform the action \( a \) and terminate \( (p' \equiv q_2) \)
   (d) \( q_2 \) can perform the action \( a \) and continue as \( q'_2 \) \( (p' \equiv q_2 \| q'_2) \)

Since the proofs for the cases (a), (c) and (b), (d) are similar, only the proofs for the first two cases have been given.

Let’s consider the case, when \( q_1 \) can perform the action \( a \) and terminate \( (p' \equiv q_2) \).

Then, according to the translation scheme, the corresponding extended automaton \( T_\delta(q_1) \) has the initial location \( l_0^2 \), final location \( l_0^2 \), and the edge \( \langle l_0^2, g_i^0, \tau_0^0, \alpha^0, l_1^0 \rangle \), and \( \text{Inv}(l_2^0) \), and \( g^0 \) are evaluated as true in the valuation \( \alpha \), and \( \text{Inv}(l_3^0) = \text{true} \).

Moreover, the extended automaton \( T_\delta(q_1) \) has the initial location \( l_0^2 \). \( \text{Inv}(l_2^0) \) is evaluated as true in the valuations \( \alpha \) and \( \alpha' \). Furthermore, \( \alpha' \upharpoonright \text{dom}(\alpha) = \alpha' \).

Since the functions \( T_\delta \) and \( T_M \) do not change the locations, edges and invariants, \( \llbracket T_M((\partial_{\alpha_0}(v_{1H}(q_1 \| q_2)), \sigma, E)) \rrbracket \equiv \llbracket (l_2^0/l_2^0, \alpha') \rrbracket \).

Since the location \( l_0^2 \) is in \( (\text{Corr}(l_0^0, l_1^0), (l_1^0, l_2^0)) = (l_2^0) \) and \( \alpha' = \alpha' \upharpoonright \text{dom}(\alpha') \), the states \( (q_1, \sigma', E') \) and \( (l', \alpha') \) are corresponding.

In case when \( q_2 \) can perform the action \( a \) and continue as \( q'_2 \) \( (p' \equiv q'_2 \| q_3) \), the corresponding extended automaton \( T_\delta(q_2) \) has the initial location \( l_0^2 \), some non-final location \( l_1^2 \), and the edge \( \langle l_0^2, g_i^0, \tau_0^0, \alpha^0, l_1^2 \rangle \), and \( \text{Inv}(l_2^0) \), and \( g^0 \) are evaluated as true in the valuation \( \alpha \), and \( \text{Inv}(l_3^0) = \text{true} \).

Moreover, the extended automaton \( T_\delta(q_2) \) has the initial location \( l_0^2 \). \( \text{Inv}(l_2^0) \) is evaluated as true in the valuations \( \alpha \) and \( \alpha' \). Furthermore, \( \alpha' \upharpoonright \text{dom}(\alpha) = \alpha' \).

Since the functions \( T_\delta \) and \( T_M \) do not change the locations, edges and invariants, \( \llbracket T_M((\partial_{\alpha_0}(v_{1H}(q_2 \| q_3)), \sigma, E)) \rrbracket \equiv \llbracket (l_2^0/l_2^0, \alpha') \rrbracket \).

Since the location \( l_0^2 \) is an initial location of the extended automaton \( T_\delta(q_2) \), i.e. \( \text{Corr}(l_0^0, l_2^0), (l_1^0, l_2^0) \rangle = (l_2^0, l_2^0) \rangle \) and \( \alpha' = \alpha' \upharpoonright \text{dom}(\alpha') \), the states \( (q_2, \sigma', E') \) and \( (l', \alpha') \) are corresponding.
Proof (Lemma 1.3). According to the rules \([T-22], [T-25]\), the process term \(\langle \partial_{\lambda_{k}}(v_{\lambda_{k}}(p)), \sigma, E \rangle\) can perform a communication action \(ca\) and then terminate if a process term \(p\) perform an action \(ca\) and then terminate.

1. In case \(p \in Q\), the lemma holds trivially, since in \(\chi\) semantics there are no transition rules with \(ca\) as specified defined for non-parallel processes.

2. In case if \(p\) is of the form \(q_{1} \parallel q_{2}\), the process term \(p\) can perform an action \(ca\) and then terminate in the following cases (\([T-18]\):

(a) if \(q_{1}\) can perform a send action and then terminate, and \(q_{2}\) can perform a receive action and then terminate
(b) if \(q_{1}\) can perform a receive action and then terminate, and \(q_{2}\) can perform a send action and terminate

Since the proofs for both cases are similar, only the proof of the first case has been given.

The lemma holds trivially for skip, assignment, deadlock, inconsistent process term, delay, repetition and sequential composition, since in \(\chi\) semantics there is no transition rules with \(ca\) as specified.

The send action can be performed by the process terms send \(h!!e_{n}\), any delay operator \([q]\), and alternative composition \(q_{1} \parallel q_{2}\). Similarly, the receive action can be performed by the process terms receive \(h??x_{n}\), any delay operator \([q]\), and alternative composition \(q_{1} \parallel q_{2}\).

Let’s consider the case, when \(q_{1} \equiv h!!e_{n}\). According to the translation scheme an extended automaton \(T_{q}(h!!e_{n})\) has the initial location \(l_{0}^{V}\), final location \(l_{f}^{V}\), and the edge \(\langle l_{0}^{V}, g^{V}, h, \{y_{1} = e_{1}, \ldots, y_{n} = e_{n}\}, l_{f}^{V} \rangle\). The invariant \(Inv(l_{0}^{V})\) and a guard \(g^{V}\), are evaluated as true in the valuation \(\sigma\), and \(Inv(l_{f}^{V})\) is true. Since the functions \(T_{p}\) and \(T_{M}\) preserve all edges, the corresponding \(UPPAAL\) automaton \(A_{q}\) contains the edge \(\langle l_{0}^{A}, g^{A}, h, \{y_{1} = e_{1}, \ldots, y_{n} = e_{n}\}, l_{f}^{A} \rangle\).

In any delay operator and alternative composition, it can be proved that the corresponding \(UPPAAL\) automaton \(A_{q}\) contains the initial location \(l_{0}^{A}\), final location \(l_{f}^{A}\), and the edge \(\langle l_{0}^{A}, g^{A}, h, \{y_{1} = e_{1}, \ldots, y_{n} = e_{n}\}, l_{f}^{A} \rangle\). Furthermore, the invariant \(Inv(l_{0}^{A})\) and a guard \(g^{A}\), are evaluated as true in the valuation \(\sigma\), and \(Inv(l_{f}^{A})\) is true. The proofs for these cases are similar to the ones in the proof of the Lemma 1.1 (cases \([id]\) \([re]\), thus we do not aduct them here.

In the similar way it can be shown that if a process term \(q_{2}\) can perform a receive action and terminate, that the corresponding \(UPPAAL\) automaton contains the initial location \(l_{0}^{A}\), final location \(l_{f}^{A}\), and the edge \(\langle l_{0}^{A}, g^{A}, h, \{x_{1} = y_{1}, \ldots, x_{n} = y_{n}\}, l_{f}^{A} \rangle\).

Then, according to the \(UPPAAL\) semantics \(I \in T_{M}(\langle \partial_{\lambda_{k}}(v_{\lambda_{k}}(q_{2})), \sigma, E \rangle) \|\|= (\langle I, \alpha \rangle \stackrel{h}{\rightarrow} (I', \alpha'), \text{where } I = \{l_{0}^{A}, l_{1}^{A}, l_{f}^{A}\}, \text{and } \alpha' = a^{A}(a)\).

Since the location \(l_{0}^{A}\) and \(l_{f}^{A}\) are final \((Corr(l_{0}^{A}, l_{f}^{A}), \{l_{0}^{A}, l_{f}^{A}\}) = \emptyset\), and \(\sigma' = \alpha' \upharpoonright \text{dom}(\sigma')\), the states \(\langle q_{2}, \sigma', E' \rangle\) and \(\langle I', \alpha' \rangle\) are corresponding.

21 Correctness of the translation scheme
Proof (Lemma 1.2). According to the rules [T-22], [T-23], the process term \( (\partial_{\alpha}(v_{ik}(p)), \sigma, E) \) can perform a communication action \( ca \) and then continue as \( p' \) if a process term \( p \) perform an action \( ca \) and continue as \( p' \):

1. In case if \( p \in Q \), the lemma holds trivially, since in \( \chi \) semantics there is no transition rules with \( ca \) as specified defined for non-parallel processes.

2. In case if \( p \) is of the form \( q_1 \parallel q_2 \), the process term \( p \) can perform an action \( ca \) and then continue as \( p' \) if one of the process terms can perform a send action and the other one can perform a receive action over the same channel, and at least one of the process terms does not terminate (T-28). Since the proofs for most cases are similar, only the proofs for the following cases have been given:

   (a) if \( q_1 \) can perform a send action and then continue as \( q'_1 \), and \( q_2 \) can perform a receive action and then terminate

   (b) if \( q_1 \) can perform a send action and then continue as \( q'_1 \), and \( q_2 \) can perform a receive action and continue as \( q'_2 \)

According to the \( \chi \) semantics only the process terms any delay, sequential composition, repetition and alternative composition can perform a send (receive) action and then continue as \( q'_1 \) (\( q'_2 \)). The process term receive, any delay and alternative composition can perform a send or receive action an then terminate.

In the same way as it was done in the proof of the Lemma 1.2 it can be shown that an extended automaton \( T_{\delta}(q_1) \) has the initial location \( l^0_{\delta} \), some non-final location \( l^1_{\delta} \), and the edge \( (l^0_{\delta}, g^0, h^0, \{y_1 = e_1, \ldots, y_n = e_n\}, l^1_{\delta}) \). The invariant Inv\((l^0_{\delta})\) and a guard \( g^0 \), are evaluated as true in the valuation \( \alpha \), and Inv\((l^0_{\delta})\) = true.

Let us consider the first case. From the proof of the Lemma 1.3 it follows that \( T_{\delta}(q_2) \) contains an edge \( (l^0_{\delta}, g^0, h^0, \{x_1 = y_1, \ldots, x_n = y_n\}, l^1_{\delta}) \), where \( l^0_{\delta} \) is a final location.

Then, according to the UPPAAL semantics \( I \vdash T_{\delta}(v_{ik}(q_{12}), \sigma, E) \) \( \Vdash \langle \overline{1}, \overline{a} \rangle \stackrel{h}{\longrightarrow} \langle \overline{1}, \overline{a'} \rangle \), where \( \overline{1} = \left[ l^0_{\delta} / l^1_{\delta} / l^1_{\delta} / l^1_{\delta} \right] \), and \( \overline{a'} = a^0(a^0(\overline{a})) \).

Since the location \( l^0_{\delta} \) is the initial location of the extended automaton \( T_{\delta}(q'_1) \), \( l^0_{\delta} \) is a final location \( \langle Corr((l^0_{\delta}, q'_1), (l^1_{\delta}, q'_1)) \rangle = (l^0_{\delta}) \), and \( \overline{a'} = a' \upharpoonright \text{dom}(\overline{a'}) \), the states \( \langle q'_1, \overline{a'}, E' \rangle \) and \( \langle \overline{1}, \overline{a'} \rangle \) are corresponding.

In the second case in the similar way, it can be shown that the automaton \( T_{\delta}(q_2) \) contains the edge \( (l^0_{\delta}, g^0, h^0, \{x_1 = y_1, \ldots, x_n = y_n\}, l^1_{\delta}) \), \( l^0_{\delta} \) is a non-final location.

Then, according to the UPPAAL semantics \( I \vdash T_{\delta}(v_{ik}(q_{12}), \sigma, E) \) \( \Vdash \langle \overline{1}, \overline{a} \rangle \stackrel{h}{\longrightarrow} \langle \overline{1}, \overline{a'} \rangle \), where \( \overline{1} = \left[ l^0_{\delta} / l^1_{\delta} / l^1_{\delta} / l^1_{\delta} \right] \), and \( \overline{a'} = a^0(a^0(\overline{a})) \).

Since the location \( l^0_{\delta} \) and \( l^1_{\delta} \) are the initial locations of the extended automata \( T_{\delta}(q'_1) \) and \( T_{\delta}(q'_2) \) respectively \( \langle Corr((l^0_{\delta}, q'_1), (l^1_{\delta}, q'_1)) \rangle = (l^0_{\delta}) \) and \( \overline{a'} = a' \upharpoonright \text{dom}(\overline{a'}) \), the states \( \langle q'_1, \overline{a'}, E' \rangle \) and \( \langle \overline{1}, \overline{a'} \rangle \) are corresponding.

\( \Box \)

Proof (Lemma 1.7).
According to the rules [I-23], [I-26] the process term \( \langle \partial_{\text{L}}(v_{14}(p)), \sigma, E \rangle \) can make a time transition \( t \) and then continue as \( \langle \partial_{\text{L}}(v_{14}(p')), \sigma', E' \rangle \) if a process term \( p \) can make a delay transition \( t \) and continue as \( p' \) and no communication is possible during the delay.

According to the UPPAAL semantics, delays are performed in the locations, thus \( \bar{l} = \bar{t} \). For simplicity below we write \( \bar{l} \) instead of \( \bar{t} \).

1. Let us first consider the case if \( p \in Q \). The lemma holds trivially for skip, multi-assignment, send, receive, deadlock, and inconsistent process term, since there are no time transition rules defined for these process terms.

(a) The process term \( \Delta d \) can make a delay transition for \( t \) time units and continue as \( p' \equiv \Delta(d - t) \), if \( \rho \in \Omega(\sigma, t) \) and \( t \leq d \) [I-3]. Furthermore, \( \sigma' = \rho(t) \) and \( \forall x, x \in (\text{dom}(\sigma) \setminus \{\text{time}\}) : \sigma'(x) = \sigma(x) \), and \( \sigma'(\text{time}) = \sigma(\text{time}) + t \).

According to the translation scheme, the extended automaton \( T_{\bar{q}}(\Delta d) \) has the initial location \( \bar{q}_0 \), such that \( \text{Inv}(\bar{q}_0) = \{c \mid c \leq d\} \), where \( c \in C \), \( a(c) = 0 \), \( T_{\bar{q}}(\bar{q}_0) = 0 \). Since \( \bar{q}_0 \) is the only location in \( \bar{q} \), \( t \leq d \), and the functions \( T_{\bar{p}} \) and \( T_{\bar{m}} \) do not change the locations, edges and invariants, \( \| T_{\bar{m}}(\langle \partial_{\text{L}}(v_{14}(\Delta d)), \sigma, E \rangle) \|l \mapsto (\bar{l}, \alpha) \rightarrow (\bar{l}, \alpha') \).

Furthermore, according to the UPPAAL semantics, during a delay values of all clock variables are changed synchronously and values of all non-clock variables remain the same: \( \forall c \in C : a'(c) = a(c) + t \). According to the translation scheme time is the only clock variable in \( \text{dom}(\sigma) \), thus \( a' \upharpoonright (\text{dom}(\sigma) \setminus \{\text{time}\}) = a \).

Since we do not translate the process term \( \Delta(d - t) \), we cannot refer to its initial location. However from the Lemma [I-2] follows that after time units, \( a(c) = t \), \( T_{\bar{m}}(\langle \partial_{\text{L}}(v_{14}(\Delta d)), \sigma, E \rangle) \) has the same time behaviour as \( T_{\bar{m}}(\langle \partial_{\text{L}}(v_{14}(\Delta(d - t))), \sigma, E \rangle) \). Moreover, since \( a'(\text{time}) = a(\text{time}) + t \) and \( \forall x \in a' \upharpoonright (\text{dom}(\sigma) \setminus \{\text{time}\}) : a(x) = a'(x) \), the states \( \langle p', \sigma', E' \rangle \) and \( \langle \bar{l}, \alpha' \rangle \) are corresponding.

(b) The process term \( \lceil q \rceil \) can make an arbitrary time transition \( t \) and continue as \( p' \equiv \lceil q \rceil \) [I-3], if \( p \in \Omega(\sigma, t) \). Moreover, \( \forall x, x \in (\text{dom}(\sigma) \setminus \{\text{time}\}) : \sigma'(x) = \sigma(x) \), and \( \sigma'(\text{time}) = \sigma(\text{time}) + t \).

Applying \( T_{\bar{q}}(\lceil q \rceil) \) adds a new initial location \( \bar{q}_0 \) into an extended automaton \( T_{\bar{q}}(\lceil q \rceil) \), such that \( \text{Inv}(\bar{q}_0) = \text{true} \), and \( T_{\bar{q}}(\bar{q}_0) = 0 \). Since the functions \( T_{\bar{p}} \) and \( T_{\bar{m}} \) do not change the locations, edges and invariants, \( \| T_{\bar{m}}(\langle \partial_{\text{L}}(v_{14}(\lceil q \rceil)), \sigma, E \rangle) \|l \mapsto (\bar{l}, \alpha) \rightarrow (\bar{l}, \alpha') \).

Moreover, since \( a'(\text{time}) = a(\text{time}) + t \) and \( \forall x \in a' \upharpoonright (\text{dom}(\sigma) \setminus \{\text{time}\}) : a(x) = a'(x) \), the states \( \langle p', \sigma', E' \rangle \) and \( \langle \bar{l}, \alpha' \rangle \) are corresponding.

(c) The process term \( q_1; q_2 \) can make a delay transition and continue as \( p' \) if \( q_2 \) can make a delay transition and continue as \( q'_1 \) \( \langle p' \equiv q'_1; q_2 \rceil \) [I-13]. By induction, the corresponding extended automaton \( T_{\bar{q}}(q_1) \) has the initial location \( \bar{q}_0 \), such that \( T_{\bar{q}}(\bar{q}_0) = 0, \alpha \mapsto \text{Inv}(\bar{q}_0), \alpha' \mapsto \text{Inv}(\bar{q}_0), \) and \( a' \upharpoonright (\text{dom}(\sigma)) = \sigma' \). Furthermore, the extended automaton \( T_{\bar{q}}(q_1) \) has the same initial location \( \bar{q}_0 \).

Since the translation function \( T_{\bar{q}}(q_1; q_2) \) does not change the location \( \bar{q}_0 \), and the functions \( T_{\bar{p}} \) and \( T_{\bar{m}} \) do not change the locations, edges and invariants, \( \| T_{\bar{m}}(\langle \partial_{\text{L}}(v_{14}(q_1; q_2)), \sigma, E \rangle) \|l \mapsto (\bar{l}, \alpha) \rightarrow (\bar{l}, \alpha') \).

Moreover, since \( a'(\text{time}) = a(\text{time}) + t \) and \( \forall x \in a' \upharpoonright (\text{dom}(\sigma) \setminus \{\text{time}\}) : a(x) = a'(x) \), the states \( \langle p', \sigma', E' \rangle \) and \( \langle \bar{l}, \alpha' \rangle \) are corresponding.

(d) The process term \( q_1 \lceil q_2 \rceil \) can make a delay transition for \( t \) time units and continue as \( p' \) if both \( q_1 \) and \( q_2 \) can make a delay transition for \( t \) time units, \( p' \equiv q'_1 \lceil q'_2 \rceil \) [I-16]. By induction, the extended automata \( T_{\bar{q}}(q_1) \) and \( T_{\bar{q}}(q_2) \) have the initial locations \( \bar{q}_0 \) and \( \bar{q}_0 \), respectively. Moreover, \( \alpha \mapsto \text{Inv}(\bar{q}_0), \alpha \mapsto \text{Inv}(\bar{q}_0), \alpha' \mapsto \text{Inv}(\bar{q}_0), \alpha' \mapsto \text{Inv}(\bar{q}_0) \).

23 Correctness of the translation scheme
5.3 Theorem 2

Theorem 2. Let $p$ and $p'$ be closed process terms, $\sigma$, $\sigma'$, $\alpha$, $\alpha'$ be valuations, $E = \{I, H, \emptyset\}$ be an environment, and $\vec{l}$ be a location vector, such that the states $\langle p, \sigma, E \rangle$ and $\langle \vec{l}, \alpha \rangle$ are corresponding. Then:

Lemma 2.1. for any non-communication action $a$

\[
\text{If } \langle p, \sigma, E \rangle \models \langle \vec{l}, \alpha \rangle \quad \forall l \in L \Rightarrow \\
\exists \sigma' : [M] \models (\partial_{\alpha}(v_{H}(p)), \sigma, E) \xrightarrow{\sigma, a, \sigma'} (\partial_{\alpha}(v_{H}(\sigma)), \sigma', E'), \\
\text{and } \langle \vec{l}, \alpha' \rangle \text{ and } \langle \vec{l}', \alpha' \rangle \text{ are corresponding states.}
\]

Lemma 2.2. for any non-communication action $a$

\[
\text{If } \langle p, \sigma, E \rangle \models \langle \vec{l}, \alpha \rangle \quad \forall l \in L \Rightarrow \\
\exists \sigma' : [M] \models (\partial_{\alpha}(v_{H}(p)), \sigma, E) \xrightarrow{\sigma, a, \sigma'} (\partial_{\alpha}(v_{H}(p')), \sigma', E'), \\
\text{and } \langle \vec{l}, \alpha' \rangle \text{ and } \langle \vec{l}', \alpha' \rangle \text{ are corresponding states.}
\]

Lemma 2.3. for any communication action $ca$

\[
\text{If } \langle p, \sigma, E \rangle \models \langle \vec{l}, \alpha \rangle \quad \forall l \in L \Rightarrow \\
\exists \sigma' : [M] \models (\partial_{\alpha}(v_{H}(p)), \sigma, E) \xrightarrow{\sigma, ca[h, cs], \sigma'} (\partial_{\alpha}(v_{H}(p')), \sigma', E'), \\
\text{and } \langle \vec{l}, \alpha' \rangle \text{ and } \langle \vec{l}', \alpha' \rangle \text{ are corresponding states.}
\]

Lemma 2.4. for any communication action $ca$

\[
\text{If } \langle p, \sigma, E \rangle \models \langle \vec{l}, \alpha \rangle \quad \forall l \in L \Rightarrow \\
\exists \sigma' : [M] \models (\partial_{\alpha}(v_{H}(p)), \sigma, E) \xrightarrow{\sigma, ca[h, cs], \sigma'} (\partial_{\alpha}(v_{H}(p')), \sigma', E')
\]

2. In case if $p$ is of the form $q_i \parallel q_d$, the proof is similar to the proof for the alternative composition.

\[\Box\]
for any time transition $T_{-22}$ $T_{-25}$ $T_{-1}$ $l$

According to the translation scheme the extended automaton $A$

2.1

Let us first consider the case if

2.5

Proof (Lemma 2.3).

1. Let us first consider the case if $p \in Q$. According to the translation scheme, the extended automata $T_{0}(\delta)$, $T_{0}(\bot)$, $T_{0}(h!! e_{n})$, $T_{0}(h?? x_{n})$, $T_{0}(?) q$, $T_{0}(q; g)$ do not have an edge $l_{1}, l_{1} \in L_{t}$, thus, the lemma holds trivially for these process terms.

(a) According to the translation scheme the extended automaton $T_{0}(\text{skip})$ has the initial location $l_{0}$, final location $l_{1}$ and the edge $e = \langle l_{0}, \text{true}, l_{1}, l_{1} \rangle$. Moreover, Inv$(l_{0}) = \text{true}$, Inv$(l_{1}) = \text{true}$.

According to the $\chi$ semantics, the process term skip can make an internal action and terminate (T-1). Then, from $T_{-22}$ $T_{-25}$

Since $\forall l \in \tilde{T}$ : $l \in L_{t}$ and valuation $\alpha' \upharpoonright \text{dom}(\alpha) = \alpha'$ (as $\alpha = \alpha'$, $\sigma = \sigma'$), the states $\langle \tilde{l}, \alpha' \rangle$ and $\langle p', \sigma', E' \rangle$ are corresponding.

(b) According to the translation scheme the extended automaton $T_{0}(x_{n} := e_{n})$ has the initial location $l_{0}$, final location $l_{1}$ and the edge $e = \langle l_{0}, \text{true}, l_{1}, l_{1} \rangle$. Moreover, Inv$(l_{0}) = \text{true}$, Inv$(l_{1}) = \text{true}$.

According to the $\chi$ semantics, the process term $x_{n} := e_{n}$ can make an internal action and terminate (T-1). Then, from $T_{-22}$ $T_{-25}$

From UP$\text{PAAL}$ semantics, $\alpha' = \alpha(a)$. According to $\chi$ semantics, the multi-assignment process term changes the value of the variables $x_{1}, \ldots, x_{n}$ to the values of the expressions $e_{1}, \ldots, e_{n}$, respectively, leaving the rest of the variables unchanged. Hence, $\alpha' \upharpoonright \text{dom}(\alpha) = \alpha'$.

Since $\forall l \in \tilde{T}$ : $l \in L_{t}$ and valuation $\alpha' \upharpoonright \text{dom}(\alpha) = \alpha'$, the states $\langle \tilde{l}, \alpha' \rangle$ and $\langle p', \sigma', E' \rangle$ are corresponding.

(c) According to the translation scheme the extended automaton $T_{0}(\Delta d)$ has the initial location $l_{0}$, final location $l_{1}$ and the edge $e = \langle l_{0}, c \leftarrow d, l_{1}, l_{1} \rangle$. Moreover, Inv$(l_{0}) = c \leq d$, Inv$(l_{1}) = \text{true}$.

According to the $\chi$ semantics, the process term $\Delta d$ can make an internal action and terminate, if $\sigma(d) = \alpha(\text{time})$. Since the states $\langle \tilde{l}, \alpha \rangle$ and $\langle p, \sigma, E \rangle$ are corresponding, $\alpha(\text{time})$. From the proof of the Lemma 2.3, $\sigma(d) = \alpha$. Then, from $T_{-22}$ $T_{-25}$

Since $\forall l \in \tilde{T}$ : $l \in L_{t}$ and valuation $\alpha' \upharpoonright \text{dom}(\alpha) = \alpha'$ (as $\alpha = \alpha'$, $\sigma = \sigma'$), the states $\langle \tilde{l}, \alpha' \rangle$ and $\langle p', \sigma', E' \rangle$ are corresponding.

(d) According to the translation scheme the extended automaton $T_{0}(q)$ has the initial location $l_{0}$, final location $l_{1}$ and the edge $e = \langle l_{0}, g, l_{1}, l_{1} \rangle$, such that $\alpha \models \text{Inv}(l_{0})$, $\alpha' \models \text{Inv}(l_{0})$, $\alpha \models g$. Moreover, from the translation scheme and from Lemma 2.3

\[ \wedge c_{0} = \alpha'(y_{1}) \wedge \ldots \wedge c_{n} = \alpha'(y_{n}), \]

and $\langle \tilde{l}, \alpha' \rangle$ and $\langle \partial_{\alpha}(v_{1}(p')), \sigma', E' \rangle$ are corresponding states.

\[ \text{Lemma 2.5.} \] for any time transition

\[ \| T_{M}(\mathcal{M}) \|_{l, \alpha} \rightarrow \langle \tilde{l}', \alpha' \rangle \wedge \exists l \in \tilde{T} : l \notin L_{t} \Rightarrow \exists \sigma', p' : \mathcal{M} \|_{l, \alpha} \rightarrow \| \partial_{\alpha}(v_{1}(p)), \sigma, E \|_{l, \alpha} \rightarrow \| \partial_{\alpha}(v_{1}(p')), \sigma', E' \|_{l, \alpha}, \]

and $\langle \tilde{l}', \alpha' \rangle$ and $\langle \partial_{\alpha}(v_{1}(p')), \sigma', E' \rangle$ are corresponding states.

Proof (Lemma 2.3).
follows that the extended automaton \( T_q(q) \) has the initial location \( l_0 \), final location \( l_0' = l_0 \), and the edge \( \epsilon' = (l_0', g, \tau, a, l_0') \), such that \( g^q = g, \alpha' = a \).

By induction we assume that the process term \( q \) can make an action and terminate, and the extended automaton \( T_q(q) \) has the initial location \( l_0' \), final location \( l_0' \), and the edge \( \epsilon = (l_0', g, \tau, a, l_0') \). Moreover, \( a \models \text{Inv}(l_0), a' \models \text{Inv}(l_0), a \models \text{dom}(\epsilon) = \sigma, a' \models \text{dom}(\epsilon') = \sigma' \).

According to the \( \chi \) semantics, if \( q \) can make an \( a \) action and terminate, then the process term \( [q] \) can make an action \( a \) and terminate. Then, from \( T-23 \) \( T-25 \)

\[
\langle \partial_{\text{Inv}}(\mathcal{V}(l_0)), \sigma, E \rangle \xrightarrow{\epsilon, \epsilon'} \langle \sigma', \sigma', E' \rangle.
\]

Since \( \forall l \in I : l \in L_e \) and valuation \( \alpha' \models \text{dom}(\epsilon) = \sigma' \), the states \( (l', \alpha') \) and \( (l', \sigma') \) are corresponding.

(c) According to the translation scheme the extended automaton \( T_q(q, \parallel q_2) \) has the initial location \( l_0 \), final location \( l_0 \), and the edge \( \epsilon = (l_0, g, \tau, a, l_0) \), such that \( a \models \text{Inv}(l_0), a' \models \text{Inv}(l_0), a \models \text{dom}(\epsilon) = \sigma, a' \models \text{dom}(\epsilon') = \sigma' \).

From the translation scheme \( T_q(q_1) \) and \( T_q(q_2) \) have the initial locations \( l_0, l_0' \), respectively, such that \( a \models \text{Inv}(l_0) \) and \( a \models \text{Inv}(l_0') \). Furthermore, \( \exists \epsilon' = (l', g, \tau, a, l') \) such that \( (1) l = l_0, l' = l_0' \) or \( (2) l = l_0, l' = l_0' \). Since the proofs for both cases are similar, we show the proof for the first case.

By induction we assume, that the process term \( q_1 \) can make an action \( a \) and terminate, and \( a' \models \text{dom}(\epsilon) = \sigma \). Then, according to the \( \chi \) semantics, the process term \( q_1 \parallel q_2 \) can make an action \( a \) and terminate. From \( T-22 \) \( T-25 \)

\[
\langle \partial_{\text{Inv}}(\mathcal{V}(l_0)), \sigma, E \rangle \xrightarrow{\epsilon, \epsilon'} \langle \sigma', \sigma', E' \rangle.
\]

Since \( \forall l \in I : l \in L_e \) and valuation \( \alpha' \models \text{dom}(\epsilon) = \sigma' \), the states \( (l', \alpha') \) and \( (l', \sigma') \) are corresponding.

2. Let us now consider the case if \( p \) is of the form \( q_1 \parallel q_2 \). Then, according to the translation scheme \( \exists l_0, l_0' \in I \) such that \( l_0 \) and \( l_0' \) are the initial locations of the extended automata \( T_q(q_1) \) and \( T_q(q_2) \), respectively, and \( l_0, l_0' \notin L_e \). That means that after performing an action \( a \), there will be at least one non-final location in \( I \), thus, the lemma hold trivially.

Proof (Lemma 2.2).

1. Let us first consider the case, when \( p \in Q \). According to the translation scheme, the extended automata \( T_q(\text{skip}) \), \( T_q(\text{e}_a), T_q(\text{h} \parallel \text{e}_a) \), \( T_q(\text{h} \parallel \text{e}_a) \), \( T_q(\Delta) \), \( T_q(\perp) \), do not have an edge \( l_0 \xrightarrow{\epsilon, \epsilon', \Delta, \perp, \Delta, l_0} l_0 \), thus, the lemma hold trivially in these cases.

(a) According to the translation scheme the extended automaton \( T_q([q]) \) has the initial location \( l_0 \), a non-final location \( k \), and an edge \( \epsilon = (l_0, g, \tau, a, k) \), such that \( \text{Inv}(l_0), a \models \text{dom}(\epsilon) = a, a', g \models a \).

Furthermore, from the translation scheme follows that the extended automaton \( T_q([q]) \) has the initial location \( l_0 \), a non-final location \( k \), and the edge \( \epsilon' = (l_0', g, \tau, a, k) \). As it proved in \( T-22 \) applying \( T_q([q]) \) does not change action behavior. That means that the edge \( \epsilon = (l_0, g, \tau, a, k) \) will be in \( T_q([q]) \).

By induction we assume that the process term \( q \) can make an action \( a \) and continue as \( q' \). Moreover, \( l_0 \) is the initial location of \( T_q(q') \), and \( a' \models \text{dom}(\epsilon') = \sigma \).
Let us consider the case, when $T_{\alpha'} | \text{dom}(\sigma) = \sigma'$. From $T\text{-}22$ $T\text{-}25$ $\{ (\partial_{A_0}(v_{h_1}(q_0)), \sigma, E) \}$ $\xrightarrow{\sigma, a, \delta'} ( \partial_{A_0}(v_{h_1}(q_0)), \sigma', E')$.

Since $l_0$ is the initial location of $T_q(q')$ and valuation $\alpha' | \text{dom}(\sigma) = \sigma'$, the states $\langle l_0 \alpha' \rangle$ and $\langle y' \alpha', E' \rangle$ are corresponding.

According to the translation scheme the extended automaton $T_q(q')$ has the initial location $l_0$, a non-final location $l_1$, and an edge $e = \langle l_0, g, \tau_h, a, l_1 \rangle$, such that $a \models \text{Inv}(l_0), \alpha' \models \text{Inv}(l_1), a \models g$.

Furthermore, from the translation scheme follows that the extended automaton $T_q(q)$ has the initial location $l_0$, a location $l_m$ and the edge $e^m = \langle l_0, g, \tau_h, a, l_m \rangle$.

Let us consider the case, when $l_m \in L_r$. Applying $T_q(q')$ redirects the edge $e^m$ to the initial location $l_0$ and adds initialization part $\text{Init}^q$ to the assignment part of the edge. Since, according to the translation scheme, it is only clock resets that can be in the $\text{Init}^q$, it will not make influence on $\alpha' | \text{dom}(\sigma')$.

By induction we assume that the process term $q$ can make an action and terminate. Moreover, $\alpha' | \text{dom}(\sigma') = \sigma'$. Then, according to the $\chi$ semantics, the process term $\ast q$ can make an action $a$ and continue as $\ast q$ $\text{eq}$, and $\alpha' | \text{dom}(\sigma') = \sigma'$. From $T\text{-}22$ $T\text{-}25$ $\{ (\partial_{A_0}(v_{h_1}(q_0)), \sigma, E) \}$ $\xrightarrow{\sigma, a, \delta'} ( \partial_{A_0}(v_{h_1}(q_0)), \sigma', E')$.

Since $l_0$ is the initial location of $T_q(q')$ and valuation $\alpha' | \text{dom}(\sigma) = \sigma'$, the states $\langle l_0 \alpha' \rangle$ and $\langle y' \alpha', E' \rangle$ are corresponding.

According to the translation scheme the extended automaton $T_q(q'; q_2)$ has the initial location $l_0$, a non-final location $l_1$, and an edge $e = \langle l_0, g, \tau_h, a, l_1 \rangle$, where $l_1 \in T_q(q_0), l_0 \notin L_r$ or $l_1$ is the initial location of $T_q(q_0)$.

Let us consider the case, when $l_1 \in T_q(q_0), l_0 \notin L_r$. By induction we assume that the process term $q_0$ can make an action $a$ and continue as $q_0'$. Moreover, $\alpha' | \text{dom}(\sigma') = \sigma'$. Then, according to the $\chi$ semantics, the process term $\ast q_0$ can make an action $a$ and continue as $\ast q_0$ $\text{eq}$, and $\alpha' | \text{dom}(\sigma') = \sigma'$. From $T\text{-}22$ $T\text{-}25$ $\{ (\partial_{A_0}(v_{h_1}(q_0)), \sigma, E) \}$ $\xrightarrow{\sigma, a, \delta'} ( \partial_{A_0}(v_{h_1}(q_0)), \sigma', E')$.

Since $l_0$ is the initial location of $T_q(q'; q_2)$ and valuation $\alpha' | \text{dom}(\sigma) = \sigma'$, the states $\langle l_0 \alpha' \rangle$ and $\langle y' \alpha', E' \rangle$ are corresponding.

Let us consider the case, when $l_1$ is the initial location of $T_q(q_0)$. By induction we assume that the process term $q_0$ can make an action $a$ and continue, and $\alpha' | \text{dom}(\sigma') = \sigma'$.

Then, according to the $\chi$ semantics, the process term $q_0; q_2$ can make an action $a$ and continue as $q_0 \sa T\text{-}12$ and $\alpha' | \text{dom}(\sigma') = \sigma'$. From $T\text{-}22$ $T\text{-}25$ $\{ (\partial_{A_0}(v_{h_1}(q_0)), \sigma, E) \}$ $\xrightarrow{\sigma, a, \delta'} ( \partial_{A_0}(v_{h_1}(q_0)), \sigma', E')$.

Since $l_1$ is the initial location of $T_q(q'; q_2)$ and valuation $\alpha' | \text{dom}(\sigma) = \sigma'$, the states $\langle l_0 \alpha' \rangle$ and $\langle y' \alpha', E' \rangle$ are corresponding.
(d) According to the translation scheme the extended automaton $T_\alpha(q_i, \| q_i)$ has the initial location $l_0$, a non-final location $l$, and the edge $e = \langle l_0, g, \tau_h, l, l \rangle$, such that $a \vdash \text{Inv}(l_0)$, $a' \vdash \text{Inv}(l)$, and $a \vdash g$.

From the translation scheme $T_\alpha(q_i)$ and $T_\alpha(q_2)$ have the initial locations $l_0$, respectively, such that $a \vdash \text{Inv}(l_0)$ and $a \vdash \text{Inv}(l_0)$. Furthermore, $\exists q' = \langle l', g, \tau_h, a, l'' \rangle$, such that (1) $p = l_0$, $p' = l_0$, $p'' \notin L_f$ or (2) $p = l', p' = l''$, $q'' \notin L_f$, and $a \vdash g$. Since the proofs for both cases are similar, we show the proof for the first case.

By induction we assume, that the process term $q_i$ can make an action $a$ and continue as $q_i$. Moreover, $l_0$ is the initial location of $T_\alpha(q_i)$ and $a' \vdash \text{dom}(\sigma) = \sigma'$. Then, according to the $\chi$ semantics, the process term $q_i \| q_2$ can make an action $a$ and continue as $q_i$. From $T_{1-15}$ and $T_{1-25} [T_{1-25}] (\partial_{\alpha_1}(v_{\beta}(q_i, \| q_2)), \sigma, E) \vdash (\partial_{\alpha_2}(v_{\beta}(q_i, \| q_2)), \sigma', E')$.

Since $l_0$ is the initial location of $T_\alpha(q_i)$ and valuation $a' \vdash \text{dom}(\sigma) = \sigma'$, the states $\langle \tilde{t}, \alpha' \rangle$ and $\langle \tilde{t}', \sigma', E' \rangle$ are corresponding.

2. Let us consider the case, if $p$ is of the form $q_i \| q_2$. Then, we can distinguish following cases:

(a) $l_0, l_0' \in l_0 \in \tilde{t}$, $\| \tilde{t}, e = \langle l_0, g, \tau_h, a, l_0 \rangle, l_0 \notin L_f, l_0' \notin L_f$.

(b) $l_0, l_0' \in l_0 \in \tilde{t}$, $\| \tilde{t}, e = \langle l_0, g, \tau_h, a, l_0 \rangle, l_0 \notin L_f, l_0' \notin L_f$.

(c) $l_0, l_0' \in l_0 \in \tilde{t}$, $\| \tilde{t}, e = \langle l_0, g, \tau_h, a, l_0 \rangle, l_0 \notin L_f, l_0' \notin L_f$.

(d) $l_0, l_0' \in l_0 \in \tilde{t}$, $\| \tilde{t}, e = \langle l_0, g, \tau_h, a, l_0 \rangle, l_0 \notin L_f, l_0' \notin L_f$.

Since the proofs for first two cases and second two cases are similar, we only give proofs for the cases [2a] and [2b].

(a) By induction we assume that the process term $q_i$ can make an action $a$ and terminate. Moreover, $l_0$ is the initial location of $T_\alpha(q_i)$, $l_0'$ is the final location of $T_\alpha(q_i)$, and $l_0'$ is the initial location of $T_\alpha(q_2)$. Furthermore, $a' \vdash \text{dom}(\sigma) = \sigma'$.

Then, according to the $\chi$ semantics, the process term $q_i \| q_2$ can make an action $a$ and continue as $q_i$. From $T_{1-15}$ and $T_{1-25} [T_{1-25}] (\partial_{\alpha_1}(v_{\beta}(q_i, \| q_2)), \sigma, E) \vdash (\partial_{\alpha_2}(v_{\beta}(q_i, \| q_2)), \sigma', E')$.

Since $l_0$ is the initial location of $T_\alpha(q_i)$, $l_0'$ is the final location of $T_\alpha(q_i)$ and valuation $a' \vdash \text{dom}(\sigma) = \sigma'$, the states $\langle \tilde{t}, \alpha' \rangle$ and $\langle \tilde{t}', \sigma', E' \rangle$ are corresponding.

(b) By induction we assume that the process term $q_i$ can make an action $a$ and continue as $q_i$. Moreover, $l_0$ is the initial location of $T_\alpha(q_i)$, $l_0'$ is the initial location of $T_\alpha(q_i)$, and $l_0'$ is the initial location of $T_\alpha(q_2)$. Furthermore, $a' \vdash \text{dom}(\sigma) = \sigma'$.

Then, according to the $\chi$ semantics, the process term $q_i \| q_2$ can make an action $a$ and continue as $q_i$. From $T_{1-15}$ and $T_{1-25} [T_{1-25}] (\partial_{\alpha_1}(v_{\beta}(q_i, \| q_2)), \sigma, E) \vdash (\partial_{\alpha_2}(v_{\beta}(q_i, \| q_2)), \sigma', E')$.

Since $l_0$ is the initial location of $T_\alpha(q_i)$, $l_0' \| l_0$ is the initial location of $T_\alpha(q_2)$ and valuation $a' \vdash \text{dom}(\sigma) = \sigma'$, the states $\langle \tilde{t}, \alpha' \rangle$ and $\langle \tilde{t}', \sigma', E' \rangle$ are corresponding.

$\blacksquare$

Proof (Lemma 2.3).
1. Let us first consider the case, when $p \in Q$. Then, according to the translation scheme, there is only one automaton in the UPPAAL model. Thus, the lemma hold trivially.

2. If $p$ is of the form $q_1 || q_2$, than either of the following holds:

   (a) The initial location of $T_q(q_1)$ $I^1 \subseteq \hat{T}$ has an outgoing edge $e_1 \xrightarrow{g_{1},a_{1}} I^0$, $I^0 \subseteq L_t$. And the initial location of $T_q(q_2)$ $I^2 \subseteq \hat{T}$ has an outgoing edge $e_2 \xrightarrow{g_{2},a_{2}} I^0$, $I^0 \subseteq L_t$.

   (b) The initial location of $T_q(q_2)$ $I^2 \subseteq \hat{T}$ has an outgoing edge $e_2 \xrightarrow{g_{2},a_{2}} I^0$, $I^0 \subseteq L_t$. And the initial location of $T_q(q_2)$ $I^2 \subseteq \hat{T}$ has an outgoing edge $e_2 \xrightarrow{g_{2},a_{2}} I^0$, $I^0 \subseteq L_t$.

   Since the proofs for both cases are similar, only the proof for the first case is given.

   According to the translation scheme the extended automata $T_q(\text{skip})$, $T_q(x_n := e_n)$, $T_q(\delta)$, $T_q(\perp)$, $T_q(\Delta_d)$, $T_q(\pi q)$, $T_q(\alpha q)$ do not have an edge $e \xrightarrow{g_{n},a_{n}} l$, or $e \xrightarrow{g_{n},a_{n}} l$, or $l \in L_t$, thus, the lemma holds trivially for these process terms.

   According to the translation scheme, the extended automaton $T_q(q_1)$ can have an edge $e_1 = \langle l^n, g^n, a^n, h^n \rangle$ if $q_1$ is either $h!!e_n$ or $[q_1]$, or $q_1 \parallel r$. And the extended automaton $T_q(x_n)$ can have an edge $e_1 = \langle l^n, g^n, a^n, h^n \rangle$ if $q_2$ is either $h??e_n$ or $[q_2]$, or $q_2 \parallel r$.

   Let us first consider the case if $q_1 \equiv h!!e_n$. Then, according to the $\chi$ semantics ([1-3]), $\models (q_1, \sigma, E) \models (q_1, \sigma, E) \models \langle q_1, \sigma, E \rangle \models (\chi, \sigma', E')$ and $\sigma = \chi$.

   In the cases when $q_1 \equiv [q]$ or $q_1 \equiv q \parallel r$, it can be proved that $\models (q_1, \sigma, E) \models \langle q_1, \sigma, E \rangle \models \langle q_1, \sigma, E \rangle \models \langle (\chi, \sigma', E') \rangle$ and $\sigma = \chi$, in the way similar to the proof of the Lemma 2.3 (cases (a) and (d) respectively). Thus we do not adnuce these proofs here.

   Similar, if $q_2 \equiv h??e_n | [q] | q \parallel r$, $\models (q_2, \sigma, E) \models (q_2, \sigma, E) \models (q_2, \sigma, E) \models \langle (\chi, \sigma', E') \rangle$ and $\sigma'(x_n) = c_n$.

   Then, according to the $\chi$ semantics ([1-3]), the process term $q_1 || q_2$ can make a communication action and terminate: $\models (q_1 || q_2, \sigma, E) \models (q_2, \sigma, E) \models (q_2, \sigma, E) \models (\chi, \sigma', E')$ and $\sigma'(x_n) = \chi(x_n)$.

   From [1-22] $\models (\chi, \sigma', E')$, then $\models (q_1 || q_2, \sigma, E) \models (q_1 || q_2, \sigma, E) \models (q_2, \sigma, E) \models (\chi, \sigma', E')$. Note, that since the actions isa, ira \in $A_{isa}$, they cannot be executed.

   According to the UPPAAL semantics, $\forall x_i \in x_n : \alpha'(x_i) = e_i$ and from the translation scheme $\forall x_i \notin x_n : x \in \text{dom}(\sigma) : \alpha'(x) = \alpha(x)$. Since $\forall l \in T : \sigma \in L_t$ and valuation $\alpha' \parallel \text{dom}(\sigma) = \sigma'$, the states $(T', \alpha')$ and $(\chi, \sigma', E')$ are corresponding.

\[ \square \]

**Proof (Lemma 2.3).**

1. Let us first consider the case if $p \in Q$. Then, according to the translation scheme there is only one automaton in UPPAAL model. Thus, the lemma hold trivially.

29 Correctness of the translation scheme
2. If \( p \) is of the form \( q_1 \parallel q_2 \), than a synchronization action is possible if:

(a) The initial location of \( T_\phi(q_1) \) has an outgoing edge \( T_\phi(q_1) \xrightarrow{g,h,a} \phi \). And the initial location of \( T_\phi(q_2) \) has an outgoing edge \( T_\phi(q_2) \xrightarrow{g,h,a} \phi \).

(b) The initial location of \( T_\phi(q_1) \) has an outgoing edge \( T_\phi(q_1) \xrightarrow{g,h,a} \phi \). And the initial location of \( T_\phi(q_2) \) has an outgoing edge \( T_\phi(q_2) \xrightarrow{g,h,a} \phi \).

Since the proofs for both cases are similar, only the proof for the first case is given. Here we consider three subcases:

(a) \( l_0 \in L_\ell, l_0 \not\in L_\ell \)

(b) \( l_0 \not\in L_\ell, l_0 \in L_\ell \)

(c) \( l_0 \not\in L_\ell, l_0 \not\in L_\ell \)

The proofs for the subcases are similar, so we only prove the first one.

From the Part 3 [REF] of this proof follows that if the extended automaton \( T_q(q_1) \) has an edge \( e_a = (l_0, g^a, h!, a^a, l_0) \), then \( (q_1, \sigma, E) \xrightarrow{\sigma, (a,h)} (q_1', \sigma', E') \) and \( \sigma = \sigma' \). According to the translation scheme, the extended automaton \( T_q(q_2) \) can have an edge \( e_a = (l_0, g^a, h^!, a^a, l_0) \) if \( q_2 \) is either \( [q] \), or \( \ast q \), or \( q \); \( \nabla q \). In the similar way as it was done in the proof [14], it can be shown that \( (q_2, \sigma, E) \xrightarrow{\sigma, (a,h)} (q_2', \sigma', E') \) and \( \sigma'(x_0) = c_a \). Note, that \( l_0 \) is the initial location of \( T_q(q_4) \).

Then, according to the \( \chi \) semantics (10.8), the process term \( (q_1 \parallel q_2) \) can make a communication action and continue as \( q_2' \); \( (q_1 \parallel q_2 \sigma, E) \xrightarrow{\sigma, (a,h)} (q_2', \sigma', E') \) and \( \sigma'(x_0) = \sigma(x_0) \). From the rule [12.21] if \( (q_1 \parallel q_2 \sigma, E) \xrightarrow{\sigma, (a,h)} (q_2', \sigma', E') \), then \( (q_1 \parallel q_2 \sigma, E) \xrightarrow{\sigma, (a,h)} (q_2', \sigma', E') \). Note, that since the actions \( isa \), \( ira \in L_\ell \), they cannot be executed.

According to the \UPPAAL semantics, \( \forall x \in x_0 : a'(x_0) = c_a \) and from the translation scheme \( \forall x \not\in x_0 \in dom(\sigma) : a'(x) = a(x) \). Since \( \forall l \in L_\ell, l /\sim l_0 \) and valuation \( \alpha' \upharpoonright dom(\sigma) = \sigma' \), the states \( (l_0, \alpha') \) and \( (q_2', \sigma', E') \) are corresponding.

\[ \square \]

**Proof (Lemma 2.3).**

According to the \UPPAAL semantics, delays are performed in the locations, thus \( I = I' \). For simplicity below we write \( I \) instead of \( I' \).

1. Let us consider the case, when \( p \in Q \). According to the translation scheme, in the extended automata \( T_{\phi}(skip) \), \( T_{\phi}(x_0) := e_0 \), \( T_{\phi}(h!!e_0) \), \( T_{\phi}(h??x_0) \), \( T_{\phi}(\delta) \), \( T_{\phi}(\bot) \), the initial locations are urgent, thus, the lemma hold trivially in these cases.
(a) According to translation scheme the extended automaton $T_\varphi(\Delta d)$ has the initial location $l_0$, such that Inv$(l_0) = \varphi \in d$, $T_1(l_0) = 0$. According to the UPPAAL semantics, $T_M((\partial_{\alpha}(v_{1\varphi}((\Delta d))), \sigma, E))$ can make a time transition for $t$ time units, $t \leq d$. Note, that the communication is not possible. Moreover, $a' \upharpoonright (\text{dom}(\sigma) \setminus \{\text{time}\}) = \sigma$, and $a'('time') = a('time') + t$.

According to the $\chi$ semantics, the process term $\Delta d$ can make a time transition for $t$ time units, $t \leq d$ and continue as $\Delta(d - t)$ \textcolor{red}{(5.3)}. Moreover, $\sigma' \upharpoonright (\text{dom}(\sigma') \setminus \{\text{time}\}) = \sigma'$, and $\sigma'('time') = \sigma('time') + t$.

From $T\textcolor{red}{(1.23)}$, $T\textcolor{red}{(1.26)}$: $(\partial_{\alpha}(v_{1\varphi}((\Delta d))), \sigma', E) \models_{\chi} (\partial_{\alpha}(v_{1\varphi}((\Delta d))), \sigma, E) \overset{t \leq d}{\rightarrow} (\partial_{\alpha}(v_{1\varphi}((\Delta(d - t)))), \sigma', E)$.

Since we do not translate the process term $\Delta(d - t)$, we cannot refer to its initial location. However, from the Lemma $\textcolor{red}{2}$ follows that after $t$ time units, $a(c) = t$, $T_M((\partial_{\alpha}(v_{1\varphi}((\Delta d))), \sigma, E))$ has the same time behavior as $T_M((\partial_{\alpha}(v_{1\varphi}((\Delta(d - t)))), \sigma, E))$.

Since valuation $a' \upharpoonright \text{dom}(\sigma) = \sigma'$, the states $\langle l, a' \rangle$ and $\langle \rho', c', E' \rangle$ are corresponding.

(b) According to translation scheme the extended automaton $T_\varphi([q])$ has the initial location $l_0$, such that Inv$(l_0) = \text{true}$, $T_1(l_0) = 0$. According to the UPPAAL semantics, $T_M((\partial_{\alpha}(v_{1[q]}([q]))), \sigma, E))$ can make a time transition for $t$ time units. Note, that the communication is not possible. Moreover, $a' \upharpoonright (\text{dom}(\sigma) \setminus \{\text{time}\}) = \sigma$, and $a'('time') = a('time') + t$.

According to the $\chi$ semantics, the process term $[q]$ can make a time transition for $t$ time units and continue as $[q]$ \textcolor{red}{(1.5)}. Note, that $[q]$ disregards time behavior of $q$. Moreover, $\sigma' \upharpoonright (\text{dom}(\sigma') \setminus \{\text{time}\}) = \sigma'$, and $\sigma'('time') = \sigma('time') + t$.

From $T\textcolor{red}{(1.23)}$, $T\textcolor{red}{(1.26)}$: $(\partial_{\alpha}(v_{1[q]}([q])), \sigma', E) \models_{\chi} (\partial_{\alpha}(v_{1[q]}([q])), \sigma, E) \overset{t \leq d}{\rightarrow} (\partial_{\alpha}(v_{1[q]}([q])), \sigma', E)$.

Since $l_0$ is the initial location of $T_\varphi([q])$ and valuation $a' \upharpoonright \text{dom}(\sigma) = \sigma'$, the states $\langle l, a' \rangle$ and $\langle \rho', c', E' \rangle$ are corresponding.

(c) According to the translation scheme the extended automaton $T_\varphi(+q)$ has the initial location $l_0$, $a \models \text{Inv}(l_0)$. $T_1(l_0) = 0$. From the translation scheme follows that the extended automaton $T_\varphi(q)$ has the initial location $l_0 = l_0 \boxplus = \text{Inv}(l_0) = \text{Inv}(l_0), T_1(l_0) = 0$.

That means that $\varphi \models T_M(q) \models_{\chi} \langle l, a' \rangle \overset{t \leq d}{\rightarrow} \langle l, a' \rangle, a' \upharpoonright (\text{dom}(\sigma) \cup \{\text{time}\}) = \sigma, a'('time') = a('time') + t$.

By induction we assume that the process term $q$ can make a time transition for $t$ time units and continue as $q$. Moreover, $a' \upharpoonright \text{dom}(\sigma') = \sigma'$ and $l_0$ is the initial location of $T_\varphi(q')$. Then, according to the $\chi$ semantics, the process term $+q$ can make a time transition for $t$ time units and continue as $q$ \textcolor{red}{[REF]}, and $a' \upharpoonright \text{dom}(\sigma') = \sigma'$.

From $T\textcolor{red}{(1.23)}$, $T\textcolor{red}{(1.26)}$: $\varphi \models_{\chi} (\partial_{\alpha}(v_{1[q]}(+q))), \sigma, E \overset{t \leq d}{\rightarrow} (\partial_{\alpha}(v_{1[q]}(*q)), \sigma', E)$.

Since the initial location of $T_\varphi(q')$ and valuation $a' \upharpoonright \text{dom}(\sigma) = \sigma'$, the states $\langle l, a' \rangle$ and $\langle \rho', c', E' \rangle$ are corresponding.

(d) According to the translation scheme the extended automaton $T_\varphi(q_1; q_2)$ has the initial location $l_0$, $a \models \text{Inv}(l_0)$.

From the translation scheme follows that the extended automaton $T_\varphi(q_1)$ has the initial location $l_0 = l_0 \boxplus = \text{Inv}(l_0) = \text{Inv}(l_0), T_1(l_0) = 0$. That means that $\varphi \models T_M(q_1) \models_{\chi} \langle l, a' \rangle \overset{t \leq d}{\rightarrow} \langle l, a' \rangle, a' \upharpoonright (\text{dom}(\sigma) \cup \{\text{time}\}) = \sigma, a'('time') = a('time') + t$.

By induction we assume that the process term $q_1$ can make a time transition for $t$ time units and continue as $q'$. Moreover, $l_0$ is the initial location of $T_\varphi(q')$, and $a' \upharpoonright \text{dom}(\sigma') = \sigma$. 

31 Correctness of the translation scheme
Then, according to the \( \chi \) semantics, the process term \( q_1 \parallel q_2 \) can make a time transition for \( t \) time units and continue as \( q' [REF] \) and \( \alpha' \parallel \sigma' = \sigma' \). From \( \text{T-23} \),

\[
\begin{align*}
\mathcal{T}_q(q_1, q_2, \sigma, E) \iff \mathcal{T}_q(\psi_{1h}(q_1, q_2), \sigma, E) \xrightarrow{q'} \mathcal{T}_q(\psi_{1h}(q'), \sigma, E).
\end{align*}
\]

Since \( l_0 \) is the initial location of \( \mathcal{T}_q(q') \) and valuation \( \alpha' \parallel \sigma' = \sigma', \) the states \( (l, \alpha') \) and \( (p', \sigma', E') \) are corresponding.

(e) According to the translation scheme, the extended automaton \( \mathcal{T}_q(q_1, q_2) \) has the initial location \( l_0 \), and \( \alpha \models \text{Inv}(l_0) \).

From the translation scheme \( \mathcal{T}_q(q_1) \) and \( \mathcal{T}_q(q_2) \) have the initial locations \( l_0^1, l_0^2 \), respectively, such that \( \alpha \models \text{Inv}(l_0^1) \) and \( \alpha \models \text{Inv}(l_0^2) \).

That means that \( \mathcal{T}_q(q_1) \parallel \mathcal{T}_q(q_2) \iff (l, \alpha') \models \{ \text{time} \} = \alpha, \alpha'(\text{time}) = \alpha(\text{time}) + t. \) And \( \mathcal{T}_q(q_1) \parallel \mathcal{T}_q(q_2) \iff (l, \alpha') \models \{ \text{time} \} = \alpha, \alpha'(\text{time}) = \alpha(\text{time}) + t. \) Note, that the communication is not possible.

By induction we assume, that the process terms \( q_1 \) and \( q_2 \) can make a time transition \( t \) and continue as \( q' \) and \( \alpha' \parallel \sigma' = \sigma'. \) Then, according to the \( \chi \) semantics, the process term \( q_1 \parallel q_2 \) can make a time transition \( t \) and continue as \( q' [REF], \) and \( \alpha' \parallel \sigma' = \sigma'. \) From \( [REF], \) \( \mathcal{M} \parallel \mathcal{T}_q(\psi_{1h}(q_1, q_2), \sigma, E) \xrightarrow{c, \alpha, \sigma} \mathcal{T}_q(\psi_{1h}(q'), \sigma, E). \)

Since \( l_0 \) is the initial location of \( \mathcal{T}_q(q') \) and valuation \( \alpha' \parallel \sigma' = \sigma', \) the states \( (l, \alpha') \) and \( (p', \sigma', E') \) are corresponding.

2. The proof for the case, when \( p :: = q_1 \parallel q_2 \) is similar to the proof for the alternative composition \( \text{[Lc]} \).

\( \Box \)

5.4 Theorem 3

**Theorem 3.** Let \( p \) be closed process term, \( \sigma \) and \( \alpha \) be valuations, \( E = (J, H, \mathcal{O}) \) be an environment, and \( l \) be a location vector, such that the states \( (p, \sigma, E) \) and \( (l, \alpha) \) are corresponding. Then:

\[ \forall l \in l : \alpha \models \text{Inv}(l) \Leftrightarrow (\mathcal{T}_h(p), \sigma, E) \xrightarrow{\sigma, \alpha, \sigma}. \]

Let us first prove that \( \forall l \in l : \alpha \models \text{Inv}(l) \Rightarrow (\mathcal{T}_h(p), \sigma, E) \xrightarrow{\sigma, \alpha, \sigma}. \)

**Proof (Lemma 4).**

1. Let us consider the case when \( p \in \mathcal{Q} \). Then, according to the translation \( l = (l_0) \), where \( l_0 \) is the initial location of the automaton \( \mathcal{T}_h(p) \). By induction we assume that \( (p, \sigma, E) \xrightarrow{\sigma, \alpha, \sigma}. \) Then, according to the rules \( \text{T-24} \) and \( \text{T-27} \) the process term \( (\mathcal{T}_h(p), \sigma, E) \) is consistent.

Furthermore, according to the translation scheme, the invariants of the initial locations of the automata \( \mathcal{T}_q(\text{skip}), \mathcal{T}_q(\text{h} ! \text{e}_n), \mathcal{T}_q(\text{h} !! \text{e}_n), \mathcal{T}_q(\text{h} ?, \text{x}_n), \mathcal{T}_q(\text{h} \&), \) and \( \mathcal{T}_q(\text{g}[g]) \) are always true. The proofs for these cases are trivial, since according to the rules \( \text{T-2}, \text{T-5}, \text{T-6}, \text{T-7}, \) and \( \text{T-10} \) these process terms are always consistent.

(a) According to the translation scheme, the invariant of the initial location \( l_0 \) of the automaton \( \mathcal{T}_q(\bot) \) is always false. The proof is trivial, since the inconsistent process term \( \bot \) is not consistent in any valuation.
(b) The invariant of the initial location of the automaton $T_q(\Delta d)$ is of the form $c \leq d$, where $c$ is a clock variable and $d$ is an expression. According to the UPPAAL semantics, the invariant must stay satisfied during delay, thus $t \in [c, d]$.

According to the $\chi$ semantics the process term $\langle \Delta d, \sigma, E \rangle$ can delay for $t$ time units, $0 \leq t \leq \sigma(d)$, and is always consistent\[5.6\]

(c) According to the translation scheme, the initial location $l_o$ of the automaton $T_q(\ast q)$ is also the initial location of the automaton $T_q(q)$. By induction we assume that the process term $\langle q, \sigma, E \rangle$ is consistent. Then, according to the rule $\mathbf{5.3}$, $\langle \ast q, \sigma, E \rangle \rightarrow_c$.

(d) According to the translation scheme, the initial location $l_o$ of the automaton $T_q(q_1; q_2)$ is also the initial location of the automaton $T_q(q_1)$. By induction we assume that the process term $\langle q_1, \sigma, E \rangle$ is consistent. Then, according to the rule $\mathbf{T-24}$, $\langle q_1; q_2, \sigma, E \rangle \rightarrow_c$.

(e) According to the translation scheme, the invariant of the initial location $l_o$ of the automaton $T_q(q_1; q_2)$ is $\text{Inv}(l_o) = \text{Inv}^a(l_o^1) \land \text{Inv}^b(l_o^2)$. By induction we assume that the process terms $\langle q_1, \sigma, E \rangle$ and $\langle q_2, \sigma, E \rangle$ are consistent. Then, according to the rule $\mathbf{T-27}$, $\langle q_1; q_2, \sigma, E \rangle \rightarrow_c$.

2. Let us now consider the case when $p$ is of the form $q_1 \parallel q_2$. Then, according to the translation $l_o^1, l_o^2 \in I$. By induction we assume that the process terms $\langle q_1, \sigma, E \rangle$ and $\langle q_2, \sigma, E \rangle$ are consistent. Then, according to the rule $\mathbf{T-24}$, $\langle q_1; q_2, \sigma, E \rangle \rightarrow_c$. Then, according to the rules $\mathbf{T-24}$ and $\mathbf{T-27}$, the process term $\langle \partial_{\lambda}(v_{14}(p)), \sigma, E \rangle$ is consistent.

Now we prove that $\langle \partial_{\lambda}(v_{14}(p)), \sigma, E \rangle \rightarrow_c \forall l \in I : a \models \text{Inv}(l)$.

\textbf{Proof (Lemma ).}

1. According to the rules $\mathbf{T-24}$ and $\mathbf{T-27}$, the process term $\langle \partial_{\lambda}(v_{14}(p)), \sigma, E \rangle$ is consistent only if $\langle p, \sigma, E \rangle \rightarrow_c$. By induction we assume that $\forall l' \in I : a \models \text{Inv}(l')$. Since from the translation scheme $l = l'$, the proof is trivial.

2. Let us consider the case when $p \in Q$. According to the rules $\mathbf{T-2}$, $\mathbf{T-5}$, $\mathbf{T-6}$, $\mathbf{T-7}$, and $\mathbf{T-10}$, the process terms $\text{skip}, x_n := e_n, h \mid e_n, h ? ? x_n, \delta$, and $[q]$ are always consistent. The proofs for these cases are trivial, since according to the translation scheme, the invariants of the initial locations of the automata $T_q(\text{skip}), T_q(x_n := e_n), T_q(h \mid e_n), T_q(h ? ? x_n), T_q(\delta)$, and $T_q([q])$ are always true.

(a) According to $\chi$ semantics, the inconsistent process term $\bot$ is not consistent in any valuation. The proof is trivial, since from the translation scheme the invariant of the initial location $l_o$ of the automaton $T_q(\bot)$ is false.

(b) According to the $\chi$ semantics the process term $\langle \Delta d, \sigma, E \rangle$ is always consistent\[5.6\] and $0 \leq t \leq \sigma(d)$.

The invariant of the initial location of the automaton $T_q(\Delta d)$ is of the form $c \leq d$, where $c$ is a clock variable and $d$ is an expression. Since $t \in [c, d]$, the invariant is always satisfied.

(c) From the rule $\mathbf{5.3}$, the process term $\langle \ast q, \sigma, E \rangle$ is consistent only if $\langle q, \sigma, E \rangle \rightarrow_c$. By induction we assume that $a \models \text{Inv}(l_o^1)$. The proof is trivial, since from the translation scheme $l_o = l_o^1$. 33 Correctness of the translation scheme
(d) From the rule T-14, the process term \( q_1; q_2, \sigma, E \) is consistent only if \( q_1, \sigma, E \rightarrow_\sigma \).
By induction we assume that \( \alpha \models \text{Inv}^\delta(l_0) \). The proof is trivial, since from the translation scheme \( l_0 = l_0^\delta \).

(e) From the rule T-17, the process term \( q_1 \parallel q_2, \sigma, E \) is consistent only if \( q_1, \sigma, E \rightarrow_\sigma \) and \( q_2, \sigma, E \rightarrow_\sigma \). By induction we assume that \( \alpha \models \text{Inv}^\delta(l_0^\delta) \land \text{Inv}^\delta(l_0^\delta) \). The proof is trivial, since from the translation scheme \( \text{Inv}(l_0) = \text{Inv}^\delta(l_0^\delta) \land \text{Inv}^\delta(l_0^\delta) \).

3. Let us consider the case when the process term \( p \) is of the form \( q_1 \parallel q_2 \). From the rule T-21, the process term \( q_1 \parallel q_2, \sigma, E \) is consistent only if \( q_1, \sigma, E \rightarrow_\sigma \) and \( q_2, \sigma, E \rightarrow_\sigma \). By induction we assume that \( \alpha \models \text{Inv}^\delta(l_0^\delta) \land \text{Inv}^\delta(l_0^\delta) \). The proof is trivial, since from the translation scheme \( l_0^\delta, l_0^\delta \in l \).

\[ \square \]

6 Informal translation

For several \( \chi \) language constructs, like guard operator or guarded repetition, we have not found a general translation. However, in some special cases the translation is possible and is implemented. In this section we present these cases.

6.1 Guarded skip and multi-assignment

The guarded skip and multi-assignment in \( \chi \) behave as follows. If guard is true, the action transition is performed without a delay. If guard is false, the process term delays till it becomes true.

Since there is no notion of urgent actions in timed automata, the translation of the guarded skip and multi-assignment is not possible. However, if the guard expression does not involve the variable time, time \( \not\in b \), the possible solution is to introduce a new automaton, which has only one location \( l_0 \). Inv\((l_0) = true \), \( T_1 = 0 \) and the only edge \( e = \langle l_0, true, dummy? \rangle \). Then, the extended automaton \( T_\cdot(b \rightarrow skip) \) can be defined as follows:

\[
T_\cdot(b \rightarrow skip) =
\langle \{ l_0, l_1 \}, l_0, \{ l_0, b, dummy?, \tau_\cdot, l_1 \} \\
\bigcup \{ \varnothing, \varnothing, \varnothing, \varnothing, \text{Inv}, T_1, l_1 \} \rangle,
\]

where Inv\((l_0) = true \), Inv\((l_1) = true \), \( T_1(l_0) = 0 \), \( T_1(l_1) = 0 \).

Similarly, the extended automaton \( T_\cdot(b \rightarrow x_\cdot := e_\cdot) \) is defined as follows:

\[
T_\cdot(x_\cdot := e_\cdot) =
\langle \{ l_0, l_1 \}, l_0 \\
\bigcup \{ \{ l_0, b, dummy?, \{ x_1 = e_1, \ldots, x_n = e_n \}, l_1 \} \\
\bigcup \{ \varnothing, \varnothing, \varnothing, \varnothing, \text{Inv}, T_1, l_1 \} \rangle,
\]

where Inv\((l_0) = true \), Inv\((l_1) = true \), \( T_1(l_0) = 0 \), \( T_1(l_1) = 0 \).
Then, it is possible to show that for any non-communication action \( a \) and \( p \equiv \text{skip} \mid x_n := e_n \):
\[
\ll M \rrl \vdash \langle b \rightarrow p, \sigma, E \rangle \xrightarrow{\{ p', \sigma', E \}} \exists ! \langle l, \alpha \rangle : \ll M \rrl \vdash \langle l, \alpha \rangle \xrightarrow{\text{dummy}} \langle l', \alpha' \rangle,
\]
and \( \langle p', \sigma', E \rangle \) and \( \langle l', \alpha' \rangle \) are corresponding states. With \( \nu \) we denote two possible cases: \( p \) can make a transition \( a \) and terminate or \( p \) can make a transition \( \alpha \) and continue as \( p' \). We restrict the guard expressions so that \( \text{time} \not\geq b \), because in UPPAAL it is not allowed to have a guard with expression over clock variables on transitions with urgent communication.

### 6.2 Guarded Send and Receive

According to the \( \chi \) semantics the guarded send and receive process terms behave as follows. If the guards in false, the process term delays till the guard becomes true. Then, the send or receive action is performed without delay. If the guard is true and the communication action is not possible, the process is deadlocked. Remember, that the action encapsulation operator \( \partial \lambda_a \) disallows internal send and receive transitions. Although we did not find the proper translation for these process terms, we were able to define the translation of the guarded delayable send and receive, i.e. \( b \rightarrow [h!!e_n] \) and \( b \rightarrow [h??x_n] \) under the condition \( \text{time} \not\geq b \).

\[
\begin{align*}
T_0(h!!e_n) &= \langle \{ l_0, l_1 \}, \lambda_0 \rangle, \\
&\quad \{ \{ l_0, b, h!, \{ y_1 = e_1, \ldots, y_n = e_n \}, l_1 \} \}, \\
&\quad \{ \{ l_0, \}, \lambda_1 \rangle, \langle y_1, \ldots, y_n \}, \lambda, \lambda, \text{Inv}, T_L, l_1 \\
T_0(h??x_n) &= \langle \{ l_0, l_1 \}, \lambda_0 \rangle, \\
&\quad \{ \{ l_0, b, h?, \{ x_1 = y_1, \ldots, x_n = y_n \}, l_1 \} \}, \\
&\quad \{ \{ l_0, \}, \lambda_1 \rangle, \langle y_1, \ldots, y_n \}, \lambda, \lambda, \text{Inv}, T_L, l_1 \\
\end{align*}
\]

where \( \text{Inv}(l_0) = \text{true}, \text{Inv}(l_1) = \text{true}, T_L(l_0) = o, T_L(l_1) = o \).

### 6.3 Guarded repetition

In timed \( \chi \) there are two repetition operators, repetition and guarded repetition, which are defined by means of recursion variables. We did not translate recursion variables and to prove the correctness of the translation of the repetition operator we used the SOS rules, defined in [9], which does not involve recursion variables. However, there is no such rules defined for the guarded repetition. So without proving the correctness we define \( T_0(b \xrightarrow{a} p) \) as follows.

Let \( T_0(p) = (L^0, \ell_0^0, E^0, V^0, V^{\text{hp}}, C^0, \text{Init}^0, \text{Inv}^0, T_L^0, \ell_F^0) \). Then,
\[
T_0(b \xrightarrow{a} p) = (L^0 \cup \{ l_0, l_k \} \setminus \{ \ell_0^0, \} \), \langle E, V^0, V^{\text{hp}}, C^0, \text{Init}^0, \text{Inv}^0, T_L, l_k \rangle),
\]

- \( l_0 \) and \( l_k \) are new initial and final locations.
- \( E = \sigma_1(E^0, \ell_1^0, l_0) \cup \{ l_0, b, \tau_h, \tau_s, \ell_0 \}, \langle l_0, \neg b, \tau_h, \tau_s, l_k \} \).
- \( \text{Inv} \mid (L^0 \setminus \{ \ell_0^0, \} = \text{Inv}^0 \mid (L^0 \setminus \{ \ell_0^0, \}) \) and \( \text{Inv}(l_0) = \text{true}, \text{Inv}(l_k) = \text{true} \).
- \( T_L \mid (L^0 \setminus \{ \ell_0^0, \}) = T_L^0 \mid (L^0 \setminus \{ \ell_0^0, \}) \) and \( T_L(l_0) = u, T_L(l_k) = 0 \).
6.4 Some notes

We were not able to translate a guarded delay, \( b \rightarrow \Delta d \). The main problem here is the time behaviour. For instance, if \( b \) is false, the process term \( b \rightarrow \Delta d \) delays till \( b \) becomes true, disregarding the time behaviour of \( \Delta d \). That means, that if first the guard \( b \) is true, the process term \( b \rightarrow \Delta d \) starts delaying. If after \( t \) time units, \( t < d \), the guard becomes false, the process term \( b \rightarrow \Delta(d - t) \) delays till \( b \) becomes true disregarding the time behaviour of \( \Delta(d - t) \). Then, if \( b \) is true, it continues to delay as \( \Delta(d - t) \).

Nevertheless, many of the \( \chi \) guarded process terms can be translated using the informal translation given above, as well as using the properties of \( \chi \) operators given in \([9]\). For instance, the non-translated guarded sequential composition \( b \rightarrow (p; q) \) may become translatable after re-writing it as \((b \rightarrow p); q\).

Furthermore, although we omit the proofs here, for the given subset of timed \( \chi \) under the condition that there is no clocks in guard expressions, it can be shown that \([b \rightarrow p]\) is bisimilar to \( b \rightarrow [p] \) and \( b_1 \rightarrow b_2 \rightarrow p \) is bisimilar to \( b_1 \wedge b_2 \rightarrow p \).

The other thing to be considered is that there is no notion of successful termination in timed automata. Thus, to check if there is no deadlocks in the model we have to use the property \( A[\ldots a_1.\text{end} \text{ and } a_2.\text{end} \text{ and } \ldots \text{ and } a_n.\text{end} \implies \neg \text{deadlock} \), where \( a_1.\text{end}, a_2.\text{end}, \ldots, a_n.\text{end} \) are the final locations.

7 Case Study: Verification of the Turntable System

7.1 System description

As an example we consider the translation of a part of a turntable system. The turntable system illustrates a part of real-life manufacturing system belonging to the application domain of (real-time) control research \([5,6,7]\). In \([4]\) the \( \chi_\sigma \) model of the system was manually translated to Promela, \( \mu \)CRL and UPPAAL timed automata, and then verified using the Spin, CADP and UPPAAL toolsets, respectively. In this case study we created a new turntable model using only translatable subset of timed \( \chi \). After that we used the translator to obtain the corresponding UPPAAL model. Finally, it was verified using UPPAAL model checker.

The turntable system consists of a round turntable, a clamp, a drill and a testing device (Figure 11). The turntable transports products to the drill and the testing device. The drill drills holes in the products. After drilling a hole, the products are delivered to the tester, where the depth of the hole is measured, since it is possible that drilling went wrong. To control the turntable system, sensors and actuators are used. A sensor detects a physical phenomenon, and changes its state. The controller reads the state of the sensor, and sends output to actuators. The actuators translate output from the controller to a physical change in the machine.

The turntable has four slots that can hold a product. Each slot can hold at most one product and can be in input, drill, test or output position. There are three sensors attached to the turntable: the sensor \( s_1 \) at the input position (to detect if a product has been added by the environment), the sensor \( s_3 \) in the output position (to detect if a product has been removed by the environment) and the sensor \( s_2 \) that detects whether the turntable has completed the turn.
The drilling module consists of the drill and the clamp. Every product should be locked before drilling and unlocked afterwards. To detect whether the clamp is locked or not two sensors are used (c1 and c2 respectively). The drill also has two sensors to detect whether the drill is in its up (d1) or down (d2) position. These sensors are located above the surface of the turntable, so it is not possible to say whether the product has been drilled successfully or not.

In the testing position there are two sensors to detect whether the tester has reached its up (t1) or down (t2) position. If the tester has reached its down position the test result of the product is good and if the sensor at the down position did not send a signal during a certain amount of time the test result of the product is bad.

The turntable control system consists of the main controller, turntable controller, drill controller, and tester controller. The main controller supervises the other controllers and the environment. It stores current information about products and operations being performed and based on this information it issues commands to the other controllers and the environment to start operations. When operations are completed the main controller updates the information about the products.

The turntable controller gets signals from the turntable sensors and passes them to the main controller. It also starts rotation of the turntable at the command of the main controller.

The drill controller supervises the drill and the clamp. It switches the drill on/off and commands to lock/unlock the clamp or to start or stop drilling. The drill controller also gets signals from the drill and clamp sensors.

The test controller sends a signal to the tester to start the operation. Then it waits for a signal from the sensor at the down position. If the hole is not deep enough, the sensor is not activated and the current product should be rejected.

The operation-routing sequence of each product is following: add a product to the input
position, make a turn (now product is in the drilling position), lock the clamp, switch on the
drill, drill, switch off the drill, unlock the clamp, make another turn (now product is in the
test position), test, and make a turn again (product is in the removing position).

No product can be added if the adding slot is not empty. No drilling, testing or removing can
be performed if the corresponding slot is empty. The turntable can treat up to four products
at the same time, that means that the operations can be done in parallel.

7.2 Design rules and assumptions

Creating the model we consider only “good weather” behavior, i.e. the assumption is that
the system works without faults and there is no product loss. The initial state is defined as
follows: all slots are empty and no operation is started.

For reasons of simplicity, we decided to concentrate on the control system. That means that
we do not model material flow as this information can be obtained from the information
stored by the main controller.

We assume that the main controller sends messages to the environment to allow adding and
removing of products and the environment informs the main controller when the operations
are completed. The environment can skip the adding or removing operations. A product
can be removed from the removing position only if it has been drilled properly. If a product
has a good test result and it has not been removed, it should not be drilled and tested again.
If a product has a bad test result it must be drilled and tested again. That means that the
information whether product has been added or removed is necessary only after the rotation
of the turntable.

We also assume that the order of starting and ending of the adding, drilling, testing and
removing operations is not known in advance.

The execution of each turntable operation requires a certain amount of time. Because the
duration of the turntable operations has not been defined anywhere, we have decided to use
the delays, that have been defined in other turntable models, like [6]. We assume that the
environment needs 2 time units to perform adding or removing of a product. The clamp
needs 2 time units to lock or unlock a product. The drilling operation takes 3 time units and
returning the drill to its up position takes 2 time units. Testing and returning the tester to its
initial (up) position require 2 time units each.

Since the turntable model is going to be verified in UPPAAL, we restrict ourselves to use only
the translated subset of timed $\chi$.

7.3 Verified properties

The following properties were verified in this case study:

1. The system does not contain a deadlock, i.e. it cannot come to a state from which it
cannot continue operating.

2. The turntable doesn’t rotate while drilling.

3. If the product has a bad test result then the product remains on the table and is drilled
again.
4. No drilling takes place if there is no product in the slot and no adding is performed if there is a product in the slot.

7.4 $\chi$ model of the turntable

The turntable system architecture is depicted in Figure 12. The mechanical components are Tester, Drill, Clamp and Table. These components are controlled by switching commands: $c_{DrillSwitch}$ switches the drill on/off, $c_{DrillMove}$ instructs the drill to start or stop drilling, $c_{ClampSwitch}$ instructs the clamp to lock or unlock the product, and $c_{TesterMove}$ instructs the tester to start or stop testing. The other signals that are used are $c_{Turn}$ (commands the turntable to start rotating), $c_{EnvAdd}$, $c_{EnvRemove}$ (inform the environment that it can perform adding or removing operations respectively).

![Turntable architecture diagram]

The control system model consists of the main controller, drill and clamp controller, tester controller and turntable controller: Main controller, Drill controller, and Tester controller, respectively. The component Environment represent the environment.

Although in Figure 12 eight components are depicted, the $\chi$ model of the turntable consists of ten parallel processes. The reason for that is that some components consist of two independent parts. Two of the processes model the environment (adding and removing a product). The other two model the drill, since the power switch and the drill part are handling commands independently. One process is used to specify the table itself, and another one is used to specify the tester. There are also three controllers: a main controller, drill controller and a tester controller. The environment is represented by two processes; one is for removing products and the other one is for adding products on the table.

Figure 12: Turntable architecture.
Below we show a turntable process as an example. The complete χ model is given in the Appendix 2.1.

The turntable process models the table itself (Fig. 13). It has 4 positions for adding, drilling, testing and removing, modeled as variables $t_1, t_2, t_3$ and $t_4$, respectively. These variables can have a value 0, if there is no product in the slot, or 1, if there is a product in the slot. The signals from the environment notify the turntable process if a product added or removed via the channels $cEnvAdded, cEnvRemoved$ respectively. If there is a product in the adding or removing position, the main controller is informed via the channels $cAdded$ and $cRemoved$ respectively. When the turntable process gets a command to turn ($cTurn$) from the main controller, it rotates. The rotation takes 4 time units; the slot states are changed accordingly. After that the turntable process informs the main controller that the turn is finished ($cTurned$).

7.5 UPPAAL model of the turntable

The χ model of the turntable was translated to UPPAAL model automatically. The UPPAAL model consists of ten automata, nine of them correspond to the χ processes. The additional dummy process has been created to translate guarded assignments and guarded skip.

As an example we show the automaton, which corresponds to the turntable process (Figure 14). The rest of the automata are given in Appendix 2.2.

7.6 Verification

After translating the χ model of the complete turntable system to UPPAAL it becomes possible to verify properties such as:

- The absence of deadlock.
- The turntable is not rotating if any of operations (drilling, testing, adding or removing) is being performed.
- The test result of a product will be known not later than 31 seconds after the product has been added.
8 Conclusions and future work

Nowadays, system specification and modeling become more and more important for handling increasing system complexity. Satisfying industry demands on reducing the development time (time-to-market), costs, and increasing reliability of systems requires early detection of the design errors, which reduces the amount of re-work. One of the most popular techniques to make performance analysis is simulation. The process algebraic language $\chi$ has been used extensively to model and simulate the manufacturing systems. However, simulation-based performance analysis becomes insufficient since it cannot guarantee the correctness of the system. In order to check correctness of the systems designed in $\chi$ we suggest to translate $\chi$ models to UPPAAL timed automata and verify their properties using UPPAAL model-checking tool.

In this report, the translation scheme of the subset of $\chi$ to UPPAAL has been presented. The subset includes following process terms: skip, multiple assignment, communication actions send and receive, deadlock, inconsistent process term, delay and delay enabling operator, repetition, sequential and alternative composition. Moreover, the informal (not proved) translation is defined for such process terms as guarded skip and multi-assignment, guarded delayable send and receive, and guarded repetition.

The translation scheme has been implemented as a part of the $\chi$ toolset and the translator from $\chi$ to UPPAAL has been used to verify a part of an industrial system.

The future work includes the proofs for the informal part of the translation, as well as formal translation of such $\chi$ constructs as variable scope operator and process instantiation. There is also a necessity of improving the graphical layout of the translated automata.

Figure 14: Turntable process in UPPAAL.
Bibliography


1 Timed Chi semantics used in the report

1.1 Skip and Multi-assignment

Process term skip is an abbreviation for an action predicate that can only perform an internal action (τ) without changing the valuation.

$$\text{skip} \triangleq \emptyset : \text{true} \triangleright \tau$$

Multi-assignment $$x_n := e_n$$ for $$n \geq 1$$ is an abbreviation for an internal action that changes variables $$x_1, \ldots, x_n$$ to the values of expressions $$e_1, \ldots, e_n$$, respectively. For $$n = 1$$, this gives a normal assignment $$x := e$$.

$$x_n := e_n \triangleq \{ x_n \} : x_1 = e_1^{-} \land \cdots \land x_n = e_n^{-} \triangleright \tau$$

Here $$e^{-}$$ denotes the result of replacing all variables $$v$$ in $$e$$ by their ’$$^{-}$$’ superscripted version $$v^{-}$$. For example, the translation of process term $$x := 2x + yz$$ is defined as $$\{ x \} : x = 2x^{-} + y^{-}z$$, and the translation of $$x, y := x + y, x - y$$ is defined as $$\{ x, y \} : (x = x^{-} + y^{-}) \land (y = x^{-} - y^{-})$$.

1.2 Variable trajectories

During the time transition the valuation at each time point $$s \in [0, t]$$ is given by $$\rho(s) \in \Omega(\sigma, t)$$, which is defined in the following way.

$$\Omega(\sigma, t) = \left\{ \begin{array}{l} \rho \in [0, t] \mapsto (\text{dom}(\sigma) \to \Lambda) \\
\quad \downarrow 0 \\
\forall x \in \text{dom}(\sigma) \setminus \{\text{time}\} : \rho \downarrow x \text{ is a constant function} \\
\forall x \in \text{dom}(\sigma) : (\rho \downarrow x)(o) = \sigma(x) \\
\forall s \in [0, t] : \rho(s)(\text{time}) = \sigma(\text{time}) + s \\
\end{array} \right\}$$

where $$\rho \downarrow x$$ denotes the function, such that $$\text{dom}(\rho \downarrow x) = \text{dom}(\rho)$$ and $$(\rho \downarrow x)(y) = \rho(y)(x)$$ for each $$y \in \text{dom}(\rho \downarrow x)$$.

1.3 SOS Rules

The semantics of timed $$\chi$$ is defined through so-called deduction rules [12]. Below we show the SOS rules, which were referred in this report. A deduction rule is of the form $$H \vdash r$$, where $$H$$ is a number of hypotheses separated by commas and $$r$$ is the result of the rule. The result of a deduction rule can be derived if all of its hypotheses are derived. In case the set of hypotheses is empty, the deduction rule is called an axiom.

Action predicate

$$\sigma' \in \Xi(\sigma, J \cup W), \sigma \cup \sigma' \vdash r \quad \frac{\{ J, R \} \vdash \{ W : r \triangleright l, \sigma \}}{\sigma' \triangleright \{ \hat{\sigma}, \sigma' \}}$$

T-1
Send and receive

\[
\sigma' \in \Xi(\sigma, J) \quad \frac{\Gamma \models \langle \mathrm{h} :: \mathrm{e}_n, \sigma \rangle}{\sigma', \mathrm{h}(\sigma', \mathrm{e}_n)) \quad \langle \checkmark, \sigma' \rangle}
\]

\[
\sigma' \in \Xi(\sigma, J \cup \{x_n\}) \quad \sigma'(x_n) = c_n \quad \frac{\Gamma \models \langle \mathrm{h} ?? \mathrm{x}_n, \sigma \rangle}{\sigma', \mathrm{h}(\sigma', \{x_n\))) \quad \langle \checkmark, \sigma' \rangle}
\]

Consistent deadlock

\[
\frac{\Gamma \models \langle \delta, \sigma \rangle}{\sigma} \quad \text{T-7}
\]

Inconsistent process term  

Inconsistent process term \(\bot\) is considered to be in a inconsistent state from its start. It cannot perform neither action transitions, nor time transitions.

Any delay operator

\[
\frac{E \langle p, \sigma \rangle \overset{a}{\longrightarrow} (p', \sigma')}{(p), \sigma} \quad \text{T-8}
\]

\[
\frac{E \rho \in \Omega(\sigma, t)}{(p), \sigma} \overset{\rho}{\longrightarrow} (\rho(t)) \quad \text{T-9}
\]

Sequential composition operator

\[
\frac{E \langle p, \sigma \rangle \overset{a}{\longrightarrow} (p', \sigma'), \langle q, \sigma' \rangle \overset{\sigma'}{\longrightarrow} (q, \sigma'' \rangle}{\langle p; q, \sigma \rangle \overset{a}{\longrightarrow} (p', q, \sigma'')} \quad \text{T-11}
\]

\[
\frac{E \langle p, \sigma \rangle \overset{\sigma}{\longrightarrow} (p', \sigma')}{\langle p; q, \sigma \rangle \overset{\sigma}{\longrightarrow} (p'; q, \sigma'')} \quad \text{T-12}
\]

\[
\frac{E \langle p, \sigma \rangle \overset{\sigma}{\longrightarrow} (p', \sigma')}{\langle p; q, \sigma \rangle \overset{\sigma}{\longrightarrow} (p'; q, \sigma'')} \quad \text{T-13}
\]

\[
\frac{E \langle p, \sigma \rangle \overset{\sigma}{\longrightarrow} (p', \sigma')}{\langle p; q, \sigma \rangle \overset{\sigma}{\longrightarrow} (p'; q, \sigma'')} \quad \text{T-14}
\]
Alternative composition operator

\[ \langle p, \sigma \rangle^\tau \stackrel{E}{\rightarrow} \langle p', \sigma' \rangle^\tau, \langle q, \sigma \rangle^\tau \]

Parallel composition operator

\[ (J \cup W, R) \vdash \langle p, \sigma \rangle^\tau, \langle q, \sigma \rangle^\tau \]

\[ (J, R) \vdash \langle q, \sigma \rangle^\tau \]

\[ (J, R) \vdash \langle q, \sigma \rangle^\tau \]

\[ (J, R) \vdash \langle q, \sigma \rangle^\tau \]

45 Timed Chi semantics used in the report
Action encapsulation operator

\[ E \langle p, \sigma \rangle \xrightarrow{\sigma, a^\sigma \cdot \langle \cdot \rangle} \langle \partial_A(p), \sigma \rangle \xrightarrow{\sigma, a^\sigma \cdot \langle \cdot \rangle} \langle \partial_A(p'), \sigma' \rangle, a \in A \]  

\[ E \langle p, \sigma \rangle \xrightarrow{t^p} \langle p', \sigma' \rangle \xrightarrow{t^p} \langle \partial_A(p), \sigma \rangle \xrightarrow{t^p} \langle \partial_A(p'), \sigma' \rangle \]

Urgent communication operator

\[ E \langle p, \sigma \rangle \xrightarrow{\alpha} \langle \sqrt{\cdot}, \sigma' \rangle \xrightarrow{\alpha} \langle \sqrt{\cdot}, \sigma' \rangle \]

\[ E \langle p, \sigma \rangle \xrightarrow{\forall \in [0, \delta]} \langle (p, \sigma \cdot p, \sigma) \xrightarrow{t^p} \langle p', \sigma' \rangle, \forall \in H \langle (p, \sigma, E) \xrightarrow{\text{ca}(h, \cdot)} \rangle \rangle \xrightarrow{\forall \in [0, \delta]} \langle v_H(p'), \sigma' \rangle \]

\[ E \langle v_H(p), \sigma \rangle \xrightarrow{\forall \in [0, \delta]} \langle v_H(p'), \sigma' \rangle \]

\[ E \langle v_H(p), \sigma \rangle \xrightarrow{\forall \in [0, \delta]} \langle v_H(p'), \sigma' \rangle \]

\[ E \langle v_H(p), \sigma \rangle \xrightarrow{\forall \in [0, \delta]} \langle v_H(p'), \sigma' \rangle \]

2 The \( \chi \) and UPPAAL models of the turntable

2.1 The \( \chi \) model of the turntable

model Turntable() =

| chan cEnvAdded!?, cEnvRemoved!?, cTurn!??: void |
| , cAdd!?, cRemoved!??: nat |
| , cAdd!??, cRemove!??: nat |
| , cClampSwitch!??: void, cLocked!??: nat |
| , cDrillSwitch!??, cDrillMove!??: void |
| , cDrillSwitched!??, cDrillMoved!??: nat |
| , cTesterMove!??: void, cTesterMoved!??: nat |
| , cTest!??: void, cTested!??: nat |
| , cDrill!??: void |
| , var t1: nat = 0, t2: nat = 0, t3: nat = 0, t4: nat = 0, ts: nat |
| , add_allowed: nat = 0, remove_allowed: nat = 0 |
| , clamp_on: nat = 0 |
| , drill_on: nat = 0, drill_up: nat = 0 |
, tester_up: nat = 0
, d: nat = 0, drill_error: nat = 0
, t: nat = 0, tester_error: nat = 0, test_result: nat = 0
, p1: nat = 0, p2: nat = 0, p3: nat = 0, p4: nat = 0, ps: nat, m: nat

//Table
:: *( [cEnvAdded??]; t1 := 1
| [cEnvRemoved??]; t4 := 0
| [cAdded??t1]
| [cRemoved!!t4]
| [cTurn??]
; delay 4
; ts:=t4; t4:=t3; t3:=t2; t2:=t1; t1:=ts
; [cTurned!!] )

//Enviroment - Add
|| *( [cAdd??add_allowed]
; ( add_allowed = 1 -> [cEnvAdded!!]
| skip
)

//Enviroment - Remove
|| *( [cRemove??remove_allowed]
; ( remove_allowed = 1 -> [cEnvRemoved!!]
| skip
)

//Clamp
|| *( [cClampSwitch??]
; ( clamp_on = 1 -> clamp_on := 0
| clamp_on = 0 -> clamp_on := 1
)
; delay 2
; [cLocked!!clamp_on]
)

//Drill - Switch
|| *( [cDrillSwitch??]
; ( drill_on = 1 -> drill_on := 0
| drill_on = 0 -> drill_on := 1
)
; delay 2
; [cDrillSwitched!!drill_on]
)

//Drill - Move
|| *( [cDrillMove??]
; ( drill_up = 1 -> drill_up := 0; delay 2
| drill_up = 0 -> drill_up := 1; delay 3
)
; [cDrillMoved!!drill_up]
)

//Tester
|| *( [cTesterMove??]
; ( tester_up = 1 -> tester_up := 0; delay 2
| tester_up = 0 -> tester_up := 1; delay 2
); [cTesterMoved!!tester_up]

47 The $\chi$ and UPPAAL models of the turntable
| tester_up = 0 -> tester_up := 1; delay 2 |
|
// Drill Controller
|| *( [cDrill??] |
| [cClampSwitch!!]; [cLocked??d] |
| ( d = 0 -> drill_error := 1 |
| d /= 0 -> [cDrillSwitch!!]; [cDrillSwitched??d] |
| ( d = 0 -> drill_error := 2 |
| d /= 0 -> [cDrillMove!!]; [cDrillMoved??d] |
| ( d = 0 -> drill_error := 3 |
| d /= 0 -> [cDrillMove!!]; [cDrillMoved??d] |
| ( d = 1 -> drill_error := 4 |
| d /= 1 -> [cDrillSwitch!!] |
| [cDrillSwitched??d] |
| ( d = 1 -> drill_error := 5 |
| d /= 1 -> [cClampSwitch!!] |
| [cLocked??d] |
| ( d = 1 -> drill_error := 6 |
| d /= 1 -> [cDrilled!!] |
|
|
// Tester Controller
|| *( [cTest??] |
| [cTesterMove!!] |
| ( [cTesterMoved??t] |
| ( t = 0 -> tester_error := 1 |
| t /= 0 -> test_result := 1 |
| delay 3; test_result := 0 |
| |
| [cTesterMove!!] |
| [cTesterMoved??t] |
| ( t = 1 -> tester_error := 2 |
| t /= 1 -> [cTested!!test_result] |
|
// Main controller
|| *( ( p1 = 0 -> [cAdd!!1] | p1 /= 0 -> skip ) |
| ( p4 = 3 -> [cRemove!!1] | p4 /= 3 -> skip ) |
| ( p2 = 1 -> [cDrill!!] | p2 /= 1 -> skip ) |
| ( p3 = 2 -> [cTest!!] | p3 /= 2 -> skip ) |
| ( p3 /= 2 -> skip |
| p3 = 2 -> [cTested??m]; ( m = 0 -> p3 := 1 | m /= 0 -> p3 := 3 ) |
| ) |
| ( p2 = 1 -> [cDrilled??]; p2 := 2 | p2 /= 1 -> skip ) |
| [cAdd!!0]; [cRemove!!0] |
| [cAdded??p1]; [cRemoved??p4] |
| [cTurn!!]; ps:=p4; p4:=p3; p3:=p2; p2:=p1; p1:=ps; [cTurned??] |
|
48
2.2 The UPPAAL model of the turntable

Figure 15: Turntable process.

Figure 16: Adding process of the environment.
Figure 17: Removing process of the environment.

Figure 18: Clamp process.

Figure 19: Switching process of the drill.

Figure 20: Moving process of the drill.
Figure 21: Tester process.

Figure 22: Drill controller process.

51 The $\chi$ and UPPAAL models of the turntable
Figure 23: Tester controller process.

Figure 24: Main controller process.

Figure 25: Dummy process.