Formula Based Abstractions of Transition Systems for Real-Time Model Checking

Roberto Barbuti[1], Nicoletta De Francesco[2], Antonella Santone[2], and Gigliola Vaglini[2]

[1] Dipartimento di Informatica, Università di Pisa, I-56125 Pisa, Italy
barbuti@di.unipi.it

[2] Dipartimento di Ingegneria dell'Informazione, Università di Pisa, I-56126 Pisa, Italy
{nico,santone,gigliola}@iet.unipi.it

Abstract. When verifying concurrent systems described by transition systems, state explosion is one of the most serious problems. If quantitative temporal information (expressed by clock ticks) are considered, state explosion is even more serious. In this paper we present a non-standard (abstract) semantics for the ASTP language able to produce reduced transition systems. The important point is that the abstract semantics produces transition systems equivalent to the standard ones for what concerns the satisfiability of a given set of formulae of a temporal logic with quantitative modal operators. The equivalence of transition systems with respect to formulae is expressed by means of $\langle\rho, n\rangle$-equivalence: two $\langle\rho, n\rangle$-equivalent transition systems give the same truth value to all formulae such that the actions occurring in the modal operators are contained in ρ, and with time constraints whose values are less than or equal to n.

1 Introduction

In this paper we address the problem of verifying systems in which time plays a fundamental role for a correct behaviour. We refer to the *Algebra of Timed Processes* (ATP) [22] as a formalism able both to model time dependent systems and to prove their properties. ATP is an extension of traditional process algebras in order to capture *discrete quantitative timing aspects* with respect to a global clock.

The semantics of such a language is given in terms of labeled transition systems where some transitions are labeled by the special action χ, called *time action*. Such an action represents the progress of time and can be viewed as a clock tick.

One widely used method for verification of properties is *model checking* [8, 7, 18, 23]. Model checking is a technique that proves the correctness of a system specification with respect to a desired behavior by checking whether a structure, representing the specification, satisfies a temporal logic formula describing the expected behavior. Most existing verification techniques, and in particular those

J. Wing, J. Woodcock, J. Davies (Eds.): FM'99, Vol. I, LNCS 1708, pp. 289–306, 1999.

defined for concurrent calculi, like CCS [21], are based on a representation of the system by means of a labeled transition system. In this case, model checking consists in checking whether a labeled transition system is a model for a formula.

When representing systems specifications by transition systems, state explosion is one of the most serious problems: often we have to deal with transition systems with a prohibitive number of states. In such cases model checking is inapplicable. Moreover, when in system specifications quantitative temporal information (expressed by clock ticks) is considered, state explosion is even more serious, the reason for this being that a new state is generated for every clock tick. Fortunately, in several cases, to check the validity of a property, it is not necessary to consider the whole transition system, but only an abstraction of it that maintains the information which "influences" the property. This consideration has been used in the definition of abstraction criteria for reducing transition systems in order to prove properties efficiently. Abstraction criteria of such kind are often based on equivalence relations defined on transition systems: minimizations with respect to different notions of equivalence are in fact used in many existing verification environments (see, for instance, [10, 13, 16]).

In this paper we present a notion of abstraction of transition systems, where the abstraction is driven by the formulae of a quantitative temporal logic. This logic, which we call *qu-mu-calculus*, is similar to the mu-calculus [19] (in particular to a variant of it [4]), in which the modal operators are redefined to include the definition of time constraints. Many logics have been defined to deal with time aspects, see, for example [2, 14]. Although all of them handle quantitative time aspects, they can be used either in conjunction with a dense time domain [1, 3, 20] or with a discrete time domain [15, 14]. A fundamental feature of qu-mu-calculus is that its formulae can be used to drive the abstraction: in particular, given the actions and the time constraints occurring in the modal operators of a formula ϕ of the qu-mu-calculus, we use them in defining an abstract (reduced) transition system on which the truth value of ϕ is equivalent to its value on the standard one.

Equivalence of transition systems with respect to formulae is expressed by means of $\langle \rho, n \rangle$-equivalence: two transition systems are $\langle \rho, n \rangle$-equivalent if and only if they give the same truth value to all formulae such that the actions occurring in the modal operators are contained in ρ, and with time constraints whose values are less than or equal to n. Some interesting properties of such an equivalence are presented.

In the paper we present also a non-standard (abstract) semantics for the ASTP [22] language able to produce abstract transition systems. ASTP is the sequential subset of ATP; actually, this is not a limitation: our abstract semantics is easily applicable to the concurrent operators and its ability in reducing the transition system can be suitably investigated also on the sequential part. Though the paper addresses the problem of defining, for an ASTP program and a formula, ϕ, a reduced transition system preserving ϕ at a very abstract level, such an abstract definition can be usefully exploited as a guide in implementing an algorithm to build the reduced system.

After the preliminaries of Section 2, we introduce our logic in Section 3 and the abstract semantics in Section 4. Section 5 concludes.

2 Preliminaries

2.1 The Algebra of Timed Processes

Let us now quickly recall the main concepts about the Algebra of Timed Processes [22], which is used in the specification of real-time concurrent and distributed systems.

For simplicity, we consider here only the subset of ATP, called ASTP (Algebra of Sequential Timed Processes), not containing parallel operators.

The syntax of *sequential process terms* (*processes* or *terms* for short) is the following:

$$p ::= 0 \mid x \mid \alpha p \mid p \oplus p \mid \ \lfloor p \rfloor (q)$$

where α ranges over a finite set of *asynchronous actions* $\mathcal{A}^\alpha = \{a, b, ...\}$. We denote by $\mathcal{A}$ the set $\mathcal{A}^\alpha \cup \{\chi\}$, ranged over by $\mu, \nu \ldots$. The action χ (*time action*) is not user-definable and represents the progress of time. x ranges over a set of *constant* names: each constant x is defined by a constant definition $x \overset{def}{=} p$. We denote the set of process terms by $\mathcal{P}$.

The standard *operational semantics* [22] is given by a relation $\longrightarrow \subseteq \mathcal{P} \times \mathcal{A} \times \mathcal{P}$, where $\mathcal{P}$ is the set of all processes: $\longrightarrow$ is the least relation defined by the rules in Figure 1.

Rule **Act** manages the prefixing operator: αp evolves to p by a transition labeled by α. The operator $\oplus$ behaves as a standard nondeterministic choice for processes with asynchronous initial actions (rule **Sum**$_1$ and the symmetric one not shown). Moreover, if p and q can perform a χ action reaching respectively p' and q', then $p \oplus q$ can perform a χ action, reaching $p' \oplus q'$ (rule **Sum**$_2$). The process $\lfloor p \rfloor (q)$ can perform the same asynchronous initial actions as p (rule **Delay**$_1$). Moreover $\lfloor p \rfloor (q)$ can perform a χ action, reaching the process q (rule **Delay**$_2$). Finally, rule **Con** says that a constant x behaves as p if $x \overset{def}{=} p$ is its definition. Note that there is no rule for the process 0, which thus cannot perform any move.

A *labeled transition system* (or *transition system* for short) is a quadruple $T = (\mathcal{S}, \mathcal{A}, \longrightarrow_T, p)$, where $\mathcal{S}$ is a set of states, $\mathcal{A}$ is a set of transition labels (actions), $p \in \mathcal{S}$ is the initial state, and $\longrightarrow_T \subseteq \mathcal{S} \times \mathcal{A} \times \mathcal{S}$ is the transition relation. If $(p, \mu, q) \in \longrightarrow_T$, we write $p \xrightarrow{\mu}_T q$.

If $\delta \in \mathcal{A}^*$ and $\delta = \mu_1 \ldots \mu_n, n \geq 1$, we write $p \xrightarrow{\delta}_T q$ to mean $p \xrightarrow{\mu_1}_T \cdots \xrightarrow{\mu_n}_T q$. Moreover $p \xrightarrow{\lambda}_T p$, where λ is the empty sequence. Given $p \in \mathcal{S}$, with $\mathcal{R}_{\longrightarrow_T}(p) = \{q \mid p \xrightarrow{\delta}_T q,\ \delta \in \mathcal{A}^*\}$ we denote the set of the states reachable from p by $\longrightarrow_T$.

$$\textbf{Act}\quad \frac{}{\alpha p \xrightarrow{\alpha} p}$$

$$\textbf{Sum}_1\quad \frac{p \xrightarrow{\alpha} p'}{p \oplus q \xrightarrow{\alpha} p'} \qquad \textbf{Sum}_2\quad \frac{p \xrightarrow{\chi} p',\ q \xrightarrow{\chi} q'}{p \oplus q \xrightarrow{\chi} p' \oplus q'}$$

$$\textbf{Delay}_1\quad \frac{p \xrightarrow{\alpha} p'}{\lfloor p \rfloor (q) \xrightarrow{\alpha} p'} \qquad \textbf{Delay}_2\quad \frac{}{\lfloor p \rfloor (q) \xrightarrow{\chi} q}$$

$$\textbf{Con}\quad \frac{p \xrightarrow{\mu} p'}{x \xrightarrow{\mu} p'}\ x \overset{def}{=} p$$

Fig. 1. *Standard operational semantics of ASTP*

Given a process p and a set of constant definitions, the *standard transition system* for p is defined as $S(p) = (\mathcal{R}_{\longrightarrow}(p), \mathcal{A}, \longrightarrow, p)$. Note that, with abuse of notation, we use $\longrightarrow$ for denoting both the operational semantics and the transition relation among the states of the transition system.

On ASTP processes equivalence relations can be defined [22], based on the notion of bisimulation between states of the related transition systems.

3 Quantitative Temporal Logic and Abstractions

In order to perform quantitative temporal reasoning, we define a logic, that we call *qu-mu-calculus*, which is an extension of the mu-calculus [19] and in particular of the selective mu-calculus [4]. The syntax is the following, where Z ranges over a set of variables:

$$\phi ::= \texttt{tt} \mid \texttt{ff} \mid Z \mid \phi_1 \vee \phi_2 \mid \phi_1 \wedge \phi_2 \mid [\alpha]_{R,<n}\,\phi \mid [\alpha]_{R,\geq n}\,\phi \mid \langle\alpha\rangle_{R,<n}\,\phi \mid$$
$$\langle\alpha\rangle_{R,\geq n}\,\phi \mid \nu Z.\phi \mid \mu Z.\phi$$

The satisfaction of a formula ϕ by a state p of a transition system, written $p \models \phi$, is defined as follows: any state satisfies $\texttt{tt}$ and no state satisfies $\texttt{ff}$; a state satisfies $\phi_1 \vee \phi_2$ ($\phi_1 \wedge \phi_2$) if it satisfies ϕ_1 or (and) ϕ_2.
$[\alpha]_{R,<n}\,\phi$, $\langle\alpha\rangle_{R,<n}\,\phi$ and $[\alpha]_{R,\geq n}\,\phi$, $\langle\alpha\rangle_{R,\geq n}\,\phi$ are the quantitative modal operators. For each quantitative operator,

- $R \subseteq \mathcal{A}^{\alpha}$;
- $n \in N$, where N is the set of natural numbers; n is called *time value*. In $\langle\alpha\rangle_{R,<n}\,\phi$ and $[\alpha]_{R,<n}\,\phi$ it must be $n > 0$.

The informal meaning of the operators is the following:

> $\langle\alpha\rangle_{R,<n}\,\phi$ is satisfied by a state which can evolve to a state satisfying ϕ by executing α, not preceded by actions in $R \cup \{\alpha\}$, within n time units.
>
> $[\alpha]_{R,<n}\,\phi$ is satisfied by a state which, for every execution of α occurring within n time units and not preceded by actions in $R \cup \{\alpha\}$, evolves to a state satisfying ϕ.
>
> $\langle\alpha\rangle_{R,\geq n}\,\phi$ is satisfied by a state which can evolve to a state satisfying ϕ by executing α, not preceded by actions in $R \cup \{\alpha\}$, after at least n time units.
>
> $[\alpha]_{R,\geq n}\,\phi$ is satisfied by a state which, for every execution of α occurring after at least n time units and not preceded by actions in $R \cup \{\alpha\}$, evolves to a state satisfying ϕ.

As in standard mu-calculus, a fixed point formula has the form $\mu Z.\phi$ ($\nu Z.\phi$) where μZ (νZ) *binds* free occurrences of Z in ϕ. An occurrence of Z is free if it is not within the scope of a binder μZ (νZ). A formula is *closed* if it contains no free variables. $\mu Z.\phi$ is the least fix point of the recursive equation $Z = \phi$, while $\nu Z.\phi$ is the greatest one. We consider only closed formulae.

The precise definition of the satisfaction of a closed formula ϕ by a state p of a transition system T is given in Table 1. It uses the relation $\Longrightarrow_T^{\rho,n}$:

Definition 1 ($\Longrightarrow_T^{\rho,n}$ relation). *Given a transition system $T = (\mathcal{S}, \mathcal{A}, \longrightarrow_T, p)$, a set of actions $\rho \subseteq \mathcal{A}^\alpha$, and $n \in N$, we define the relation $\Longrightarrow_T^{\rho,n} \subseteq \mathcal{S} \times \rho \times \mathcal{S}$ such that, for each $\alpha \in \rho$*

$$p \overset{\alpha}{\Longrightarrow}{}_T^{\rho,n}\, q = p \xrightarrow{\delta\alpha}_T q, \text{ with } \delta \in (\mathcal{A} - \rho)^*,\ |\delta \downarrow_\chi| = n.$$

where $|\delta \downarrow_\chi|$ is the number of χ actions occurring in δ.

By $p \overset{\alpha}{\Longrightarrow}{}_T^{\rho,k}\, q$ we express the fact that it is possible to pass from p to q by executing a (possibly empty) sequence of actions not belonging to ρ and containing exactly k χ, followed by the action α in ρ.

A transition system T satisfies a formula ϕ iff its initial state satisfies ϕ. An ASTP process p satisfies a formula ϕ iff $S(p)$ satisfies ϕ.

3.1 Formula Driven Equivalence

A formula ϕ of the qu-mu-calculus can be used to define a bisimulation equivalence between transition systems. The bisimulation is defined by considering only the asynchronous actions occurring in the quantitative operators belonging to the formula (denoted by $\mathcal{O}(\phi)$), and the maximum time value of the quantitative operators occurring in the formula (denoted by $\max(\phi)$). Thus all formulae

$$\begin{array}{ll}
p \not\models \texttt{ff} & \\
p \models \texttt{tt} & \\
p \models \phi \wedge \psi & \text{iff } p \models \phi \text{ and } p \models \psi \\
p \models \phi \vee \psi & \text{iff } p \models \phi \text{ and } p \models \psi \\
p \models [\alpha]_{R,<n}\, \phi & \text{iff } \forall p'.\forall k < n. p \overset{\alpha}{\Longrightarrow}_T^{R\cup\{\alpha\},k} p' \text{ implies } p' \models \phi \\
p \models \langle\alpha\rangle_{R,<n}\, \phi & \text{iff } \exists p'.\exists k < n. p \overset{\alpha}{\Longrightarrow}_T^{R\cup\{\alpha\},k} p' \text{ and } p' \models \phi \\
p \models [\alpha]_{R,\geq n}\, \phi & \text{iff } \forall p'.\forall k \geq n. p \overset{\alpha}{\Longrightarrow}_T^{R\cup\{\alpha\},k} p' \text{ implies } p' \models \phi \\
p \models \langle\alpha\rangle_{R,\geq n}\, \phi & \text{iff } \exists p'.\exists k \geq n. p \overset{\alpha}{\Longrightarrow}_T^{R\cup\{\alpha\},k} p' \text{ and } p' \models \phi \\
p \models \nu Z.\phi & \text{iff } p \models \nu Z^m.\phi \text{ for all m} \\
p \models \mu Z.\phi & \text{iff } p \models \mu Z^m.\phi \text{ for some m}
\end{array}$$

where, for each m, $\nu Z^m.\phi$ and $\mu Z^m.\phi$ are defined as:

$$\begin{array}{ll}
\nu Z^0.\phi = \texttt{tt} & \mu Z^0.\phi = \texttt{ff} \\
\nu Z^{m+1}.\phi = \phi[\nu Z^m.\phi/Z] & \mu Z^{m+1}.\phi = \phi[\mu Z^m.\phi/Z]
\end{array}$$

where the notation $\phi[\psi/Z]$ indicates the substitution of ψ for every free occurrence of the variable Z in ϕ.

Table 1. *Satisfaction of a formula by a state*

with the same set of occurring actions and the same maximum time value define the same bisimulation.

Given a set $\rho \subseteq \mathcal{A}^\alpha$ of actions and a time value n, the $\langle\rho, n\rangle$-bisimulation equivalence relates states p and q if: i) for each path starting from p, containing $k < n$ time actions and no action in ρ and ending with $\alpha \in \rho$, there is a path starting from q, containing exactly k time actions and no action in ρ and ending with $\alpha \in \rho$, such that the reached states are bisimilar, and ii) for each path starting from p, containing $k \geq n$ time actions and no action in ρ and ending with $\alpha \in \rho$, there is a path starting from q, containing $m \geq n$ (possibly $m \neq k$) time actions and no action in ρ and ending with $\alpha \in \rho$, such that the reached states are bisimilar.

Definition 2 ($\langle\rho, n\rangle$-bisimulation, $\langle\rho, n\rangle$-equivalence).
Let $T = (\mathcal{S}_T, \mathcal{A}, \longrightarrow_T, p)$ and $\Sigma = (\mathcal{S}_\Sigma, \mathcal{A}, \longrightarrow_\Sigma, p')$ be transition systems, let $\rho \subseteq \mathcal{A}^\alpha$ and $n \in N$.

- *A $\langle\rho, n\rangle$-*bisimulation*, $\mathcal{B}$, is a binary relation on $\mathcal{S}_T \times \mathcal{S}_\Sigma$ such that $r\mathcal{B}q$ implies:*

i) $r \stackrel{\alpha}{\Longrightarrow}{}^{\rho,j}_{T} r'$*, with* $j < n$*, implies* $\exists q'.q \stackrel{\alpha}{\Longrightarrow}{}^{\rho,j}_{\Sigma} q'$ *with* $r'\mathcal{B}q'$*; and*

ii) $q \stackrel{\alpha}{\Longrightarrow}{}^{\rho,j}_{\Sigma} q'$*, with* $j < n$*, implies* $\exists r'.r \stackrel{\alpha}{\Longrightarrow}{}^{\rho,j}_{T} r'$ *with* $r'\mathcal{B}q'$*; and*

iii) $r \stackrel{\alpha}{\Longrightarrow}{}^{\rho,j}_{T} r'$*, with* $j \geq n$*, implies* $\exists i \geq n, \exists q'.q \stackrel{\alpha}{\Longrightarrow}{}^{\rho,i}_{\Sigma} q'$*, with* $r'\mathcal{B}q'$*; and*

iv) $q \stackrel{\alpha}{\Longrightarrow}{}^{\rho,j}_{\Sigma} q'$*, with* $j \geq n$*, implies* $\exists i \geq n, \exists r'.\ r \stackrel{\alpha}{\Longrightarrow}{}^{\rho,i}_{T} r'$*, with* $r'\mathcal{B}q'$*.*

- T *and* Σ *are* $\langle \rho, n \rangle$-equivalent *(*$T \approx_{\rho,n} \Sigma$*) iff there exists a* $\langle \rho, n \rangle$*-bisimulation* $\mathcal{B}$ *containing the pair* (p, p')*.*

The following proposition holds, relating equivalences with different ρ and n.

Proposition 1. *For each* $\rho, \rho' \subseteq \mathcal{A}^{\alpha}$*,* $n, n' \in N$*, if* $\rho \subseteq \rho'$ *and* $n \leq n'$*, then* $\approx_{\rho',n'} \subseteq \approx_{\rho,n}$*.*

Proof. *See Appendix.*

In order to relate $\langle \rho, n \rangle$-equivalence with quantitative temporal properties, we introduce the following definition, concerning equivalences based on sets of formulae.

Definition 3 (logic-based equivalence). *Let* T *and* Σ *be two transition systems, and* Γ *be a set of closed formulae:*

$$T \equiv_{\Gamma} \Sigma \textit{ iff } \{\phi \in \Gamma : T \models \phi\} = \{\phi \in \Gamma : \Sigma \models \phi\}$$

The following theorem states that $\langle \rho, n \rangle$-equivalent transition systems satisfy the same set of formulae with occurring actions in ρ and maximum time value less than or equal to n.

Theorem 1. *Let* $T = (\mathcal{S}_T, \mathcal{A}, \longrightarrow_T, p)$ *and* $\Sigma = (\mathcal{S}_\Sigma, \mathcal{A}, \longrightarrow_\Sigma, q)$ *be transition systems and let* $\rho \subseteq \mathcal{A}^{\alpha}$ *and* $n \in N$*.*

$$T \approx_{\rho,n} \Sigma \quad \textit{implies} \quad T \equiv_{\Phi^{\rho,n}} \Sigma$$

where

$$\Phi^{\rho,n} = \{\phi : \phi \textit{ is a closed formula of the qu-mu-calculus such that } \mathcal{O}(\phi) \subseteq \rho \textit{ and } \max(\phi) \leq n\}.$$

Proof. *See Appendix.*

4 Abstract Transition Systems and Abstract Semantics

In order to reduce the number of states of a transition system for model checking, we now define an abstraction of the transition system on which a formula ϕ can be equivalently checked. Given a transition system T, let us denote as *time path* each path $p_1 \xrightarrow{\chi}_T \cdots \xrightarrow{\chi}_T p_n$ such that

- no $p_i, 1 \leq i \leq n$, occurs more than once in the sequence;
- no $p_i, 1 \leq i \leq n$, is able to perform any asynchronous action.

Let T be a transition system and ϕ be a formula with occurring actions ρ and maximum time value n. A $\langle \rho, n \rangle$-abstraction T' of T has the following properties:

- all asynchronous actions labeling the transitions of T' belong to ρ;
- the length of each time path of T' is less than or equal to n;
- $T' \;\approx_{\rho,n}\; T$.

Given an ASTP process p and a pair $\langle \rho, n \rangle$, we define an abstract transition system by means of a non-standard semantics which consists of a set of inference rules that skip actions not in ρ and produce time paths not longer than n.

The non standard rules are shown in Figure 2 (the symmetric rules of **Sum**$_1$ and **Sum**$_2$ are not shown). They use a transition relation $\longrightarrow^m_{\rho,n}$ parameterized by an integer $m \leq n$. The ideas on which the semantics is based are the following:

- the actions in ρ are always performed (rules **Act**$_1$, **Delay**$_4$ and **Sum**$_1$)
- the actions not in ρ are skipped: when an action not in ρ is encountered, a "look-ahead" is performed in order to reach either an action in ρ or a time action (rules **Act**$_2$, **Delay**$_3$ and **Sum**$_2$);
- when a time action is encountered, it is skipped only if the process we reach by this action can perform a sequence of n time units. In order to count the time units we use the superscript of $\longrightarrow^m_{\rho,n}$: the transition $p \xrightarrow{\mu}{}^{m}_{\rho,n} q$ occurs when an action belonging to ρ can be executed after m time actions starting from p. In fact, in order to generate the transition $p \xrightarrow{\mu}{}^{m}_{\rho,n} q$, we first prove that $q \xrightarrow{\mu}{}^{m-1}_{\rho,n} q'$ for some q' (rules **Delay**$_1$ and **Delay**$_2$, **Sum**$_3$ and **Sum**$_4$). Successive applications of **Delay**$_2$ and **Sum**$_4$ allow us to skip all time actions in a sequence but the last n ones.

Note that in the premises of rules **Delay**$_3$, **Delay**$_4$, **Sum**$_1$, **Sum**$_2$ **Sum**$_3$ and **Sum**$_4$ the standard operational relation $\longrightarrow$ is used, in order to know the first action of the process and consequently to respect the standard behavior of the operators, which is different depending on whether the first action is a time action or not.

The following proposition characterizes the transitions of the non-standard semantics:

Proposition 2. *Let $\rho \subseteq \mathcal{A}^\alpha$ and $n \in N$. For each ASTP process p,*

1. $p \xrightarrow{\alpha}{}^{j}_{\rho,n} q$ *implies* $\alpha \in \rho$ *and* $j = 0$*;*
2. $p \xrightarrow{\chi}{}^{m}_{\rho,n} q$ *implies* $1 \leq m \leq n$*.*

Proof. See Appendix.

The proposition states that there are two kinds of transitions: the first one represents the execution of action $\alpha \in \rho$; the second one represents both the fact that p can perform a χ action and the fact that a path composed by χ actions starts from q, with length $m - 1$, and reaches a state where an action in ρ can be performed. Moreover the rules ensures that m is always less then or equal to n.

The following results hold, relating the standard transition relation with the non-standard one:

Proposition 3. *Let $\rho \subseteq \mathcal{A}^\alpha$ and $n \in N$. For each ASTP process p,*

$p \overset{\alpha}{\Longrightarrow}{}^{\rho,j}_{S(p)} q$ *iff*

1. $j \leq n$ *and* $p \xrightarrow{\chi}{}^{j}_{\rho,n} p_1 \xrightarrow{\chi}{}^{j-1}_{\rho,n} p_2 \cdots p_j \xrightarrow{\alpha}{}^{0}_{\rho,n} q$ *or;*
2. $j \geq n$ *and* $p \xrightarrow{\chi}{}^{n}_{\rho,n} p_1 \xrightarrow{\chi}{}^{n-1}_{\rho,n} p_2 \cdots p_n \xrightarrow{\alpha}{}^{0}_{\rho,n} q$*.*

Proof. See Appendix.

Now we formally define the notion of abstract transition system.

Definition 4 (abstract transition system). *For each ASTP process p, given $\rho \subseteq A^\alpha$ and $n \in N$ the abstract transition system for p is defined as*

$$\mathcal{N}_{\rho,n}(p) = (\mathcal{R}_{\rightarrow_{\mathcal{N}_{\rho,n}(p)}}(p),\ \rho \cup \{\chi\},\ \rightarrow_{\mathcal{N}_{\rho,n}(p)},\ p)$$

where $q \xrightarrow{\mu}_{\mathcal{N}_{\rho,n}(p)} q'$ *if and only if* $\exists j. q \xrightarrow{\mu}{}^{j}_{\rho,n} q'$*.*

The following theorem holds, stating that the transition system defined by the non-standard semantics is a $\langle \rho, n \rangle$-abstraction of $S(p)$ for each process p.

Theorem 2. *Let $\rho \subseteq \mathcal{A}^\alpha$ and $n \in N$. For each ASTP process p,*

1. *the transitions of $\mathcal{N}_{\rho,n}(p)$ are labeled only either by actions in ρ or by χ;*
2. *the length of each time path without repetition in $\mathcal{N}_{\rho,n}(p)$ is less than or equal to n;*
3. $S(p) \approx_{\rho,n} \mathcal{N}_{\rho,n}(p)$*.*

Proof. *See Appendix.*

Note that, if $n = 0$, the abstract transition system $\mathcal{N}_{\rho,0}(p)$ for a process p does not contain transitions labeled by time actions and expresses only the precedence properties between the asynchronous actions in ρ. The following propositions relates $\approx_{\rho,n}$-equivalences with different ρ and n.

Proposition 4. *Let $\rho, \rho' \subseteq \mathcal{A}^{\alpha}$, $n \in N$, $n' \in N \cup \{\omega\}$, $\rho \subseteq \rho'$ and $n \leq n'$. For each ASTP process p,*

$$\mathcal{N}_{\rho,n}(p) \ \approx_{\rho,n} \ \mathcal{N}_{\rho',n'}(p).$$

Proof. By Proposition 1 and by Theorem 2.3.

$$\mathbf{Act}_1 \ \frac{}{\alpha p \xrightarrow{\alpha}{}^{0}_{\rho,n} p} \ \alpha \in \rho \qquad \mathbf{Act}_2 \ \frac{p \xrightarrow{\mu}{}^{m}_{\rho,n} p'}{\alpha p \xrightarrow{\mu}{}^{m}_{\rho,n} p'} \ \alpha \notin \rho$$

$$\mathbf{Delay}_1 \ \frac{q \xrightarrow{\mu}{}^{m}_{\rho,n} q'}{\lfloor p \rfloor (q) \xrightarrow{\chi}{}^{m+1}_{\rho,n} q} \ m < n \qquad \mathbf{Delay}_2 \ \frac{q \xrightarrow{\mu}{}^{n}_{\rho,n} q'}{\lfloor p \rfloor (q) \xrightarrow{\mu}{}^{n}_{\rho,n} q'}$$

$$\mathbf{Delay}_3 \ \frac{p \xrightarrow{\alpha} p', \ p' \xrightarrow{\mu}{}^{m}_{\rho,n} p''}{\lfloor p \rfloor (q) \xrightarrow{\mu}{}^{m}_{\rho,n} p''} \ \alpha \notin \rho \qquad \mathbf{Delay}_4 \ \frac{p \xrightarrow{\alpha} p'}{\lfloor p \rfloor (q) \xrightarrow{\alpha}{}^{0}_{\rho,n} p'} \ \alpha \in \rho$$

$$\mathbf{Sum}_1 \ \frac{p \xrightarrow{\alpha} p'}{p \oplus q \xrightarrow{\alpha}{}^{0}_{\rho,n} p'} \ \alpha \in \rho \qquad \mathbf{Sum}_2 \ \frac{p \xrightarrow{\alpha} p', \ p' \xrightarrow{\mu}{}^{m}_{\rho,n} p''}{p \oplus q \xrightarrow{\mu}{}^{m}_{\rho,n} p''} \ \alpha \notin \rho$$

$$\mathbf{Sum}_3 \ \frac{p \xrightarrow{\chi} p', \ q \xrightarrow{\chi} q', \ p' \oplus q' \xrightarrow{\mu}{}^{m}_{\rho,n} r}{p \oplus q \xrightarrow{\chi}{}^{m+1}_{\rho,n} p' \oplus q'} \ m < n \quad \mathbf{Sum}_4 \ \frac{p \xrightarrow{\chi} p', \ q \xrightarrow{\chi} q', \ p' \oplus q' \xrightarrow{\mu}{}^{n}_{\rho,n} r}{p \oplus q \xrightarrow{\mu}{}^{n}_{\rho,n} r}$$

$$\mathbf{Con} \ \frac{p \xrightarrow{\mu}{}^{m}_{\rho,n} p'}{x \xrightarrow{\mu}{}^{m}_{\rho,n} p'} \ x \overset{def}{=} p$$

Fig. 2. *Non-standard operational semantics for ASTP*

Example 1. In the following we use $\chi.p$ to denote the term $\lfloor 0 \rfloor(p)$; this process can perform only the action χ and then becomes the process p. Moreover we define $\chi^n.p$ $(n > 1)$ as:

$$\chi^n.p = \lfloor 0 \rfloor(\chi^{n-1}.p)$$
$$\chi^1.p = \chi.p$$

Let us consider a vending machine with a time-dependent behavior. The machine allows a user to obtain different services: a soft drink immediately after the request; a coffee after a delay of a time unit; a cappuccino after a delay of two time units; a cappuccino with chocolate after a delay of three time units. Moreover, it is possible to recollect the inserted coin, if requested within only one time unit. The *ASTP* specification of the machine is:

$$\begin{aligned}
V &= \mathit{coin}\ \lfloor \mathit{recollect}\, \overline{\mathit{money}}\, V \rfloor (V_1)\\
V_1 &= \mathit{coffee}\, V_2 \oplus \mathit{cappuccino}\ V_3 \oplus \mathit{choc\_cappuccino}\ V_4 \oplus \mathit{soft\_drink}\, V_5\\
V_2 &= \chi.(\overline{\mathit{collect\_coffee}}\ V)\\
V_3 &= \chi^2.(\overline{\mathit{collect\_cappuccino}}\ V)\\
V_4 &= \chi^3.(\overline{\mathit{collect\_choc\_cappuccino}}\ V)\\
V_5 &= \overline{\mathit{collect\_soft\_drink}}\, V
\end{aligned}$$

The standard transition for the vending machine contains 14 states and 18 transitions.
Let us suppose that we have to verify the following two formulae:

$\psi_1 = \nu Z.[\mathit{coin}]_{\emptyset,\geq 0}\langle\overline{\mathit{collect\_soft\_drink}}\rangle_{\emptyset,<2}Z$:

"it alway holds that, after a coin has been inserted, a soft drink can be collected within two time units".

$\psi_2 = [\mathit{coin}]_{\emptyset,\geq 0}[\overline{\mathit{money}}]_{\{\mathit{coin}\},\geq 1}\mathtt{ff}$:

" it is not possible to recollect the inserted coin after more than one time unit".

The formula ψ_1 can be checked on the abstract transition system $\mathcal{N}_{\rho_1,n_1}(V)$, with $\rho_1 = \mathcal{O}(\psi_1) = \{\mathit{coin}, \overline{\mathit{collect\_soft\_drink}}\}$ and $n_1 = \max(\psi_1) = 2$, which has 8 states and 14 transitions, while ψ_2 can be checked on $\mathcal{N}_{\rho_2,n_2}(V)$, with $\rho_2 = \mathcal{O}(\psi_2) = \{\mathit{coin}, \overline{\mathit{money}}\}$ and $n_2 = \max(\psi_2) = 1$, which has 6 states and 13 transitions.

5 Conclusions

In this paper we have presented an approach to the problem of the reduction of the number of states of a transition system. Many abstraction criteria for system specifications not including time constraints have been defined, see for example [4, 6, 9, 11, 12]. For real-time systems the work [17] define abstractions for transition systems with quantitative labels, but there the abstraction is not driven by the property to be proved.

We have introduced an abstract semantics for ASTP processes in order to formally define the abstract transition system. The abstract semantics can be implemented in order to design a tool for automatically building an abstract transition system. In the implementation, some care must be taken to manage infinite loops which can occur in the look-ahead process.

The reduction performed by the abstract semantics depends on the set ρ of actions and on the bound n. In particular, the reduction can be significant either when the set ρ is a small subset of $\mathcal{A}$ or when the bound n is small with respect to the length of time paths in the standard transition system. Obviously, no reduction is performed if $\rho = \mathcal{A}$ and n is greater than the longest time path in the standard transition system.

References

[1] L. Aceto, A. Burgueño, K.G. Larsen. *Model Checking via Reachability Testing for Timed Automata.* In Proceedings of TACAS'98, Lecture Notes in Computer Science 1384, 1998. 263–280.

[2] R. Alur, T.A. Henzinger. *Logics and Models of Real Time: A Survey.* In Proceedings of Real-Time: Theory in Practice, Lecture Notes in Computer Science 600, 1991. 74–106.

[3] R. Alur, T.A. Henzinger. *A Really Temporal Logic.* J. ACM, 41(1), 1994. 181–204.

[4] R. Barbuti, N. De Francesco, A. Santone, G. Vaglini. *Selective mu-calculus: New Modal Operators for Proving Properties on Reduced Transition Systems.* In Proceedings of FORTE X/PSTV XVII '97. Chapman & Hall, 1997. 519-534.

[5] R. Barbuti, N. De Francesco, A. Santone, G. Vaglini. *Selective mu-calculus and Formula-Based Equivalence of Transition Systems.* To appear on Journal of Computer and System Sciences, 1999.

[6] S. Bensalem, A. Bouajjani, C. Loiseaux, J. Sifakis. *Property Preserving Simulations.* In Proceedings of Workshop on Computer Aided Verification (CAV'92), Lecture Notes in Computer Science 663, 1992. 260–273.

[7] J. Bradfield, C. Stirling. Verifying Temporal Properties of Processes. In Proceedings of International Conference on Concurrency Theory (CONCUR'90), Lecture Notes in Computer Science 458, 1990. 115–125.

[8] E.M. Clarke, E.A. Emerson, A.P. Sistla. *Automatic Verification of Finite-state Concurrent Systems using Temporal Logic Verification.* ACM Transactions on Programming Languages and Systems, 8, 1986. 244–263.

[9] E.M. Clarke, O.Grumberg, D.E. Long. *Model Checking and Abstraction.* ACM Transactions on Programming Languages and Systems, 16, 1992. 343–354.

[10] R. Cleaveland, S. Sims. *The NCSU Concurrency Workbench.* In Proceedings of Workshop on Computer Aided Verification (CAV'96), Lecture Notes in Computer Science 1102, 1996. 394–397.

[11] D. Dams, O. Grumberg, R. Gerth. *Generation of Reduced Models for Checking Fragments of CTL.* In Proceedings of Workshop on Computer Aided Verification (CAV'93), Lecture Notes in Computer Science 697, 1993. 479–490.

[12] D. Dams, O. Grumberg, R. Gerth. *Abstract Interpretation of Reactive Systems.* ACM Transaction of Programming Languages and Systems, 19, 1997. 253-291.

[13] R. De Simone, D. Vergamini. *Aboard AUTO.* INRIA Technical Report 111, 1989.

[14] E.A. Emerson. *Real-Time and the Mu-Calculus.* In Proceedings of Real-Time: Theory in Practice, Lecture Notes in Computer Science 600, 1991. 176–194.

[15] E.A. Emerson, R.F. Trefler. *Generalized Quantitative Temporal Reasoning: An Automata-Theoretic Approach.* In Proceedings of TAPSOFT'97, Lecture Notes in Computer Science 1214, 1997. 189–200.

[16] J.C. Fernandez et al. *CADP A Protocol Validation and Verification Toolbox.* In Proceedings of the Third International Conference on Computer-Aided Verification, Lecture Notes in Computer Science 1102, 1996. 437–440.

[17] G. Juanole, L. Gallon. *Concept of Quantified Abstract Quotient Automaton and its advantage.* In Proceedings of FORTE X/PSTV XVII '97. Chapman & Hall, 1997. 223-238.

[18] T.A. Henzinger, X. Nicollin, J. Sifakis, S. Yovine. *Symbolic Model Checking for real-time Systems.* Information and Computation, 111, 1994. 193-244.

[19] D. Kozen. *Results on the propositional mu-calculus.* Theoretical Computer Science, 27, 1983. 333–354.

[20] F. Laroussinie, K.G. Larsen, C. Weise. *From Timed Automata to Logic - and Back.* In Proceedings of MFCS'95, Lecture Notes in Computer Science 969, 1995. 529–538.

[21] R. Milner. *Communication and Concurrency.* Prentice-Hall, 1989.

[22] X. Nicollin, J. Sifakis. *The Algebra of Timed Processes, ATP: Theory and Application.* Information and Computation, 114, 1994. 131–178.

[23] O.V. Sokolsky, S.A. Smolka. *Local Model Checking for Real-Time Systems.* In Proceedings of Workshop on Computer Aided Verification (CAV'95), Lecture Notes in Computer Science 939, 1995. 211–224.

Appendix

Proof of Proposition 1

Proposition 1. *For each* $\rho, \rho' \subseteq \mathcal{A}^{\alpha}$, $n, n' \in N$, *if* $\rho \subseteq \rho'$ *and* $n \leq n'$, *then* $\approx_{\rho',n'} \subseteq \approx_{\rho,n}$.

Proof. Let $T = (\mathcal{S}_T, \mathcal{A}, \longrightarrow_T, p)$ and $\Sigma = (\mathcal{S}_\Sigma, \mathcal{A}, \longrightarrow_\Sigma, p')$ be two transition systems. We show that each $\langle \rho', n' \rangle$-bisimulation $\mathcal{B} \subseteq \mathcal{S}_T \times \mathcal{S}_\Sigma$ is a $\langle \rho, n \rangle$-bisimulation.

Consider $(r, q) \in \mathcal{B}$.

i) $r \overset{\alpha}{\Longrightarrow}{}_{T}^{\rho,j} r'$, with $j < n$

$\Rightarrow \qquad \{ \rho \subseteq \rho' \}$

$r \overset{\delta\alpha}{\Longrightarrow}{}_{T}^{\rho',j} r'$, for some $\delta \in (\rho' - \rho)^*$

$\Rightarrow \qquad \{ (r, q) \in \mathcal{B} \}$

$q \overset{\delta\alpha}{\Longrightarrow}{}_{\Sigma}^{\rho',j} q'$, with $(r', q') \in \mathcal{B}$

$\Rightarrow \qquad \{ \delta \in (\rho' - \rho)^* \text{ and } \alpha \in \rho \}$

$q \overset{\alpha}{\Longrightarrow}{}_{\Sigma}^{\rho,j} q'$ and $j < n$.

ii) The proof of this condition follows by a symmetric argument.

iii) $r \overset{\alpha}{\Longrightarrow}{}_{T}^{\rho,j} r'$, with $j \geq n$

$\Rightarrow \qquad \{ \rho \subseteq \rho' \}$

$r \overset{\delta\alpha}{\Longrightarrow}_T^{\rho',j} r'$, for some $\delta \in (\rho' - \rho)^*$

$\Rightarrow$ $\{ \ (r, q) \in \mathcal{B} \ \}$

$\exists i \geq n', \exists q'.\ q \overset{\delta\alpha}{\Longrightarrow}_\Sigma^{\rho',i} q'$, with $(r', q') \in \mathcal{B}$

$\Rightarrow$ $\{ \ \delta \in (\rho' - \rho)^*, \ \alpha \in \rho$ and $n \leq n' \ \}$

$q \overset{\alpha}{\Longrightarrow}_\Sigma^{\rho,i} q'$ and $i \geq n$.

iv) The proof of this condition follows by a symmetric argument.

Proof of Theorem 1

Theorem 1. *Let $T = (\mathcal{S}_T, \mathcal{A}, \longrightarrow_T, p)$ and $\Sigma = (\mathcal{S}_\Sigma, \mathcal{A}, \longrightarrow_\Sigma, q)$ be transition systems and let $\rho \subseteq \mathcal{A}^\alpha$ and $n \in N$.*

$$T \approx_{\rho,n} \Sigma \quad \textit{implies} \quad T \equiv_{\Phi^{\rho,n}} \Sigma$$

where

$\Phi^{\rho,n} = \{\phi : \phi$ *is a closed formula of the qu-mu-calculus such that* $\mathcal{O}(\phi) \subseteq \rho$ *and* $\max(\phi) \leq n\}$.

Proof. We prove that, given a state p belonging to T and a state q belonging to Σ

$$p \approx_{\rho,n} q \quad \text{implies} \quad p \equiv_{\Phi^{\rho,n}} q$$

By induction on the structure of the formulae without recursion.
Base. `tt`, `ff`: straightforward.
Induction step. Let us suppose that the theorem holds for ϕ and ψ, with $\mathcal{O}(\phi) \subseteq \rho$ and $\mathcal{O}(\psi) \subseteq \rho$.

- $\phi \vee \psi$. By inductive hypothesis.

- $\phi \wedge \psi$. By inductive hypothesis.

- $\langle \alpha \rangle_{R,<n}\, \phi$.

  $p \models \langle \alpha \rangle_{R,<n}\, \phi$

  $\Rightarrow$ $\{$ definition of satisfaction $\}$

  for some $k < n$, $p \overset{\alpha}{\Longrightarrow}_T^{R \cup \{\alpha\},k} p'$ with $p' \models \phi$

$\Rightarrow$ { Definition 1 and $R \cup \{\alpha\} \subseteq \rho$ }

$p \overset{\beta_1}{\Longrightarrow}{}^{\rho,k_1}_{T} p_1 \cdots p_{r-1} \overset{\beta_r}{\Longrightarrow}{}^{\rho,k_r}_{T} p_r \overset{\alpha}{\Longrightarrow}{}^{\rho,k_{r+1}}_{T} p_{r+1} = p'$,

$r \geq 0,\ \beta_i \in (\rho - (\{\alpha\} \cup R)),\ k_1 + \cdots + k_{r+1} = k$

$\Rightarrow$ { definition of $\langle \rho, n \rangle$-equivalence

and $k_i < n$, $1 \leq i \leq r+1$ }

$q \overset{\beta_1}{\Longrightarrow}{}^{\rho,k_1}_{\Sigma} q_1 \cdots q_{r-1} \overset{\beta_r}{\Longrightarrow}{}^{\rho,k_r}_{\Sigma} q_r \overset{\alpha}{\Longrightarrow}{}^{\rho,k_{r+1}}_{\Sigma} q_{r+1}$, with $p_i \approx_{\rho,n} q_i,\ 1 \leq i \leq r+1$

$\Rightarrow$ { Definition 1 }

$q \overset{\alpha}{\Longrightarrow}{}^{\{\alpha\} \cup R, k}_{\Sigma} q_{r+1}$

$\Rightarrow$ { inductive hypothesis ($q_{r+1} \models \phi$)

and definition of satisfaction }

$q \models \langle \alpha \rangle_{R,<n} \phi$. The same holds if $q \models \langle \alpha \rangle_{R,<n} \phi$.

- $[\alpha]_{R,<n} \phi$, $\langle \alpha \rangle_{R,\geq n} \phi$, $[\alpha]_{R,\geq n} \phi$. Similar to the $\langle \alpha \rangle_{R,<n} \phi$ case.

For $\mu Z.\phi$ (resp. $\nu Z.\phi$) formulae the thesis follows since the truth value of such formulae corresponds (the transition systems we deal with are finite and finitely branching [22]) to the $\vee$ (resp. the $\wedge$) of an enumerable set of finite non-recursive formulae.

Proof of Proposition 2

Proposition 2. Let $\rho \subseteq \mathcal{A}^{\alpha}$ and $n \in N$. For each ASTP process p,

1. $p \xrightarrow{\alpha}{}^{j}_{\rho,n} q$ implies $\alpha \in \rho$ and $j = 0$;
2. $p \xrightarrow{\chi}{}^{m}_{\rho,n} q$ implies $1 \leq m \leq n$.

Proof. Both points 1 and 2 can be proved by induction on depth of inference. We prove only point 2. Point 1 can be proved in a similar way.

Point 2. We consider in turn each transition rule as the last rule applied in the inference.

αp **Act**$_1$: is not applicable.

Act$_2$: $p \xrightarrow{\chi}{}^{m}_{\rho,n} p'$

$\Rightarrow$ { inductive hypothesis }

$1 \leq m \leq n.$

$\Rightarrow$ { application of $\mathbf{Act}_2$ }

$\alpha p \xrightarrow{\chi}{}^{m}_{\rho,n} p'.$

$\lfloor p \rfloor (q)$ $\mathbf{Delay}_1$: $q \xrightarrow{\chi}{}^{m}_{\rho,n} q'$

$\Rightarrow$ { inductive hypothesis }

$1 \leq m \leq n.$

$\Rightarrow$ { application of $\mathbf{Delay}_1$ $(m < n)$ }

$\lfloor p \rfloor (q) \xrightarrow{\chi}{}^{m+1}_{\rho,n} q$ and $1 \leq m + 1 \leq n.$

$\mathbf{Delay}_2$: $q \xrightarrow{\chi}{}^{m}_{\rho,n} q'$

$\Rightarrow$ { inductive hypothesis }

$1 \leq m \leq n.$

$\Rightarrow$ { application of $\mathbf{Delay}_2$ $(m = n)$ }

$\lfloor p \rfloor (q) \xrightarrow{\chi}{}^{m}_{\rho,n} q'$

$\mathbf{Delay}_3$: if $p \xrightarrow{\alpha} p'$ and $p' \xrightarrow{\chi}{}^{m}_{\rho,n} p''$

$\Rightarrow$ { inductive hypothesis }

$1 \leq m \leq n.$

$\Rightarrow$ { application of $\mathbf{Delay}_3$ }

$\lfloor p \rfloor (q) \xrightarrow{\chi}{}^{m}_{\rho,n} p''.$

$\mathbf{Delay}_4$: is not applicable.

$p \oplus q, x$ Similarly to proofs above.

5.1 Proof of Proposition 3

Proposition 3. Let $\rho \subseteq \mathcal{A}^{\alpha}$ and $n \in N$. For each ASTP process p,

$p \overset{\alpha}{\Longrightarrow}{}^{\rho,j}_{S(p)} q$ iff

1. $j \leq n$ and $p \xrightarrow{\chi}{}^{j}_{\rho,n} p_1 \xrightarrow{\chi}{}^{j-1}_{\rho,n} p_2 \cdots p_j \xrightarrow{\alpha}{}^{0}_{\rho,n} q$ or;

2. $j \geq n$ and $p \xrightarrow{\chi}{}^{n}_{\rho,n} p_1 \xrightarrow{\chi}{}^{n-1}_{\rho,n} p_2 \cdots p_n \xrightarrow{\alpha}{}^{0}_{\rho,n} q$.

Proof. *Point 1.* By induction on j.
Base. $j = 0$. $p \overset{\alpha}{\Longrightarrow}{}^{\rho,0}_{S(p)} q$

$\Leftrightarrow$ { Definition 1 }

$p \xrightarrow{\delta\alpha} q$, $\delta \in (\mathcal{A} - \rho - \{\chi\})^*$

$\Leftrightarrow$ { definition of the non standard semantics }

$p \xrightarrow{\alpha}{}^{0}_{\rho,n} q$

Induction step. Let us suppose that the proposition holds for $j < n$.

$p \overset{\alpha}{\Longrightarrow}{}^{\rho,j+1}_{S(p)} q$

$\Leftrightarrow$ { Definition 1 }

$p \xrightarrow{\delta_1\chi} p' \overset{\alpha}{\Longrightarrow}{}^{\rho,j}_{S(p)} q$, $\delta_1 \in (\mathcal{A} - \rho - \{\chi\})^*$

$\Leftrightarrow$ { inductive hypothesis }

$p' \xrightarrow{\chi}{}^{j}_{\rho,n} p_1 \xrightarrow{\chi}{}^{j-1}_{\rho,n} p_2 \cdots p_j \xrightarrow{\alpha}{}^{0}_{\rho,n} q$

$\Leftrightarrow$ { definition of non standard semantics }

$p \xrightarrow{\alpha}{}^{j+1}_{\rho,n} p'$.

Point 2. By induction on $j - n$.
Base. $j - n = 0$. The thesis follows by point 1.

Induction step. Let us suppose that the proposition holds for $j - n = k$. Suppose that $j - n = k + 1$.

$p \overset{\alpha}{\Longrightarrow}{}^{\rho,n+k+1}_{S(p)} q$

$\Leftrightarrow$ { Definition 1 }

$p \xrightarrow{\delta_1\chi} p' \overset{\alpha}{\Longrightarrow}{}^{\rho,n+k}_{S(p)} q$, $\delta_1 \in (\mathcal{A} - \rho - \{\chi\})^*$

$\Leftrightarrow$ { inductive hypothesis }

$p' \xrightarrow{\chi}{}^{n}_{\rho,n} p_1 \xrightarrow{\chi}{}^{n-1}_{\rho,n} p_2 \cdots p_n \xrightarrow{\alpha}{}^{0}_{\rho,n} q$

$\Leftrightarrow$ { definition of non standard semantics }

$p \xrightarrow{\alpha}{}^{n}_{\rho,n} p_1$.

Proof Theorem 2

Theorem 2. Let $\rho \subseteq \mathcal{A}^{\alpha}$ and $n \in N$. For each ASTP process p,

1. the transitions of $\mathcal{N}_{\rho,n}(p)$ are labeled only either by actions in ρ or by χ;
2. the length of each time path without repetition in $\mathcal{N}_{\rho,n}(p)$ is less than or equal to n;
3. $S(p) \approx_{\rho,n} \mathcal{N}_{\rho,n}(p)$.

Proof.

1. By Proposition 2.
2. Since in the relations $\longrightarrow^{m}_{\rho,n}$, used to define $\mathcal{N}_{\rho,n}(p)$, we have that $m \leq n$.
3. Let $T = S(p)$ and $\Sigma = \mathcal{N}_{\rho,n}(p)$. We show that $\mathcal{B}$ is a $\langle \rho, n \rangle$-bisimulation, where:
$$\mathcal{B} = \{(p, p) \mid p \in T \text{ and } p \in \Sigma\}$$

i) $p \overset{\alpha}{\Longrightarrow}{}^{\rho,j}_{T}\, p'$, with $j < n$

$\Rightarrow$ { Proposition 3 }

$p \overset{\chi}{\longrightarrow}{}^{j}_{\rho,n}\, p_1 \overset{\chi}{\longrightarrow}{}^{j-1}_{\rho,n}\, p_2 \cdots p_j \overset{\alpha}{\longrightarrow}{}^{0}_{\rho,n}\, p'$

$\Rightarrow$ { Definition 1 }

$p \overset{\alpha}{\Longrightarrow}{}^{\rho,j}_{\Sigma}\, p'$.

ii) The proof of this condition follows by a symmetric argument.

iii) $p \overset{\alpha}{\Longrightarrow}{}^{\rho,j}_{T}\, p'$, with $j \geq n$

$\Rightarrow$ { Proposition 3 }

$p \overset{\chi}{\longrightarrow}{}^{n}_{\rho,n}\, p_1 \overset{\chi}{\longrightarrow}{}^{n-1}_{\rho,n}\, p_2 \cdots p_n \overset{\alpha}{\longrightarrow}{}^{0}_{\rho,n}\, p'$

$\Rightarrow$ { Definition 1 }

$p \overset{\alpha}{\Longrightarrow}{}^{\rho,n}_{\Sigma}\, p'$.

iv) The proof of this condition follows by a symmetric argument.