An Algebraic Theory of Distributed Real-Time

Rance Cleaveland[*] and Gerald Lüttgen[†]
e-mail: {rance,luettgen}@eos.ncsu.edu

Technical Report TR-96-04
Department of Computer Science
North Carolina State University
Raleigh, NC 27695-8206, USA
March 1996

Abstract

This paper develops a real-time process algebra, TPL$^{\mathsf{mc}}$, for modeling and reasoning about distributed real-time systems. Like the algebra PMC, TPL$^{\mathsf{mc}}$ includes operators for binding processes to different clocks; unlike PMC, however, TPL$^{\mathsf{mc}}$ includes a version of the *maximal progress assumption*. Using simple examples, we motivate why these features are useful and in some cases necessary for modeling and verifying distributed systems; we also present a behavioral congruence based on Milner's observational equivalence and develop logical characterizations of the behavioral relations.

Keywords: process algebras, distributed systems, real-time, multiple clocks, maximal progress assumption, bisimulation.

1 Introduction

Process algebras [4, 12, 14, 16] provide a well-studied framework for modeling and verifying concurrent systems [7, 10]. These theories typically consist of a simple language with a rigorously defined semantics mapping terms to labeled transition systems. They also usually support equational reasoning as a basis for system verification: an equivalence on processes is defined that relates systems on the basis of their observable behavior, and this relation is used to relate specifications, which describe desired system behavior, and implementations. In order to support *compositional reasoning*, researchers have typically concentrated on equivalences that are also congruence relations for the given languages.

Traditionally, process algebras have been developed with a view toward modeling the nondeterministic behavior of concurrent and distributed systems. More recent work has incorporated

[*] Research supported by NSF/DARPA grant CCR-9014775, NSF grant CCR-9120995, ONR Young Investigator Award N00014-92-J-1582, NSF Young Investigator Award CCR-9257963, NSF grant CCR-9402807, and AFOSR grant F49620-95-1-0508.

[†] Research support provided by the German Academic Exchange Service under grant D/95/09026 (Doktorandenstipendium HSP II / AUFE).

other aspects of system behavior, including real time [2, 3, 13, 18, 24], priorities [6, 8, 9] and probability [23]. Most of this later work, however, has been devoted to modeling centralized, as opposed to distributed systems; the real-time work, in particular, has (implicitly or explicitly) focused on systems with a single clock. In this paper we present a temporal process algebra, called $\mathsf{TPL}^{\mathsf{mc}}$, which is aimed at modeling distributed real-time systems that contain a number of different clocks. The algebra extends Hennessy and Regan's TPL [13] with operators from PMC [3] for managing multiple clocks. Like Yi's real-time calculus [24], TPL enjoys the *maximal progress assumption*, which has been shown in practice to ease greatly the task of modeling real-time systems [11], but it only supports the modeling of systems with a single clock. PMC can model systems with many clocks, but in practice its lack of maximal progress limits its utility for verification purposes. Combining the two features into one model yields semantic subtleties whose solutions constitute the body of this paper.

The rest of the paper is organized as follows. The remainder of this section is devoted to an example illustrating the desirability of multiple clocks and maximal progress in modeling real-time distributed systems. The next section defines the syntax and semantics of $\mathsf{TPL}^{\mathsf{mc}}$, while Section 3 provides two further examples illustrating the utility of our language. In the next section strong bisimulation [17] is adapted to our language, and its theory is developed, while the corresponding observational theory is presented in Section 5. The final section contains our conclusions and directions for future research, while the appendices contain proofs of some of the results stated in the paper.

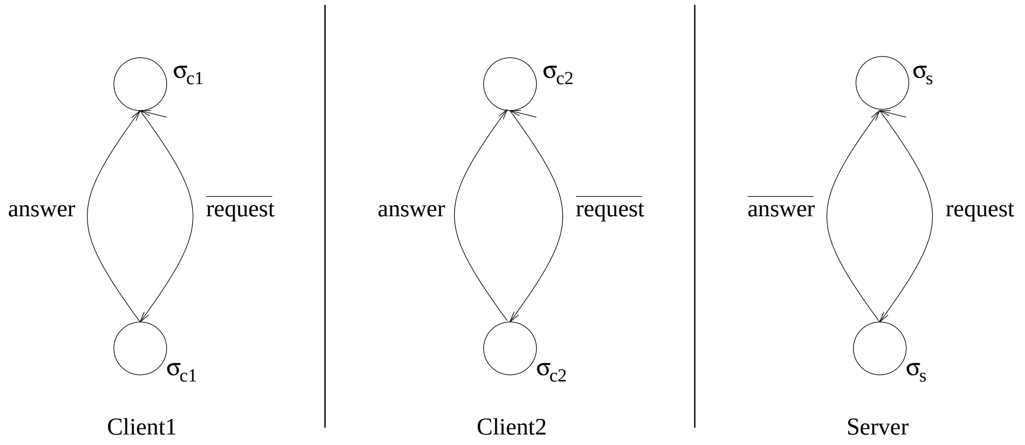

Figure 1: Client-server model

Motivating Example. We motivate the two main characteristics of $\mathsf{TPL}^{\mathsf{mc}}$, *multiple clocks* and *maximal progress*, by a generic example. Consider the basic architecture of a *client-server system* as given in Figure 1. The clients and the server are physically different computers having their own clocks σ_{c1} , σ_{c2} , and σ_s , respectively. Clients repeatedly attempt to send requests to the server, which is capable of processing one such request at a time. A client whose request is accepted then awaits an answer, while the other client idles until the server is ready to process another request. The server waits for a request, which he processes directly, and offers the answer to the requesting client. Receiving the answer from the server, the client starts over again. From the description of the system, it is clear that an adequate model for it should include support for multiple clocks, since the system components are running on different machines. Moreover, clients should receive responses as soon as they are offered; any delay could force the server to wait, which is unacceptable in practice. This argues for the inclusion of a maximal progress assumption. Moreover, the example shows why we would like a *localized* version of the maximal progress assumption. Suppose that we have one client which engages in an infinite, internal computation. Although this situation seems to be artificial at first sight, it naturally occurs when abstracting from timing aspects of some *part* of a distributed system, e.g. from the timing behavior of a particular client. Ideally, this should not effect the proper work at other sites. Unfortunately, the usual maximal progress assumption has the side-effect that no clock is able to tick in such a situation. Thus, by localizing the maximal progress assumption we formalize an important aspect of our intuition of *distributed* systems.

2 Syntax and Semantics of $\mathsf{TPL}^{\mathsf{mc}}$

In this section, we define the syntax and semantics of our language $\mathsf{TPL}^{\mathsf{mc}}$ which is based on the temporal process algebras TPL [13] and PMC [3].

2.1 Syntax of $\mathsf{TPL}^{\mathsf{mc}}$

The syntax of $\mathsf{TPL}^{\mathsf{mc}}$ is essentially the same as in PMC. It differs from CCS by the introduction of *timed actions*, a *timeout operator*, and an *ignore operator*.

Formally, let Λ be a countable set of action labels, not including the so called *silent* or *internal* action τ. For every *input action* $a \in \Lambda$, there exists a *complementary action* $\overline{a}$, the corresponding *output action*. Further, let $\overline{\Lambda} =_{\mathrm{df}} \{\overline{a} \,|\, a \in \Lambda\}$, and let us denote the set of all actions $\Lambda \cup \overline{\Lambda} \cup \{\tau\}$, where $\tau \notin \Lambda$, by $\mathcal{A}$. Intuitively, an action indicates that a process is willing to perform a synchronization on the *port* associated with the action name, i.e. an action a means that the process wants to receive a message from port a whereas $\overline{a}$ means that the process wants to send a message via port a. The action τ either indicates an internal action of a process or the synchronization of two processes on some port in order to communicate with each other. Finally, we let $a, b, \ldots$ range over Λ and $\alpha, \beta, \ldots$ over $\mathcal{A}$.

We extend the set $\mathcal{A}$ of ordinary actions by a finite set $\mathcal{T}$ of *timed actions*. Sometimes we refer to a timed action as a *clock* or a *timer*. We let $\sigma, \sigma', \ldots$ range over $\mathcal{T}$. A timed action σ models idling until the next clock cycle of the clock σ. In contrast to the synchronization of ordinary actions on complementary ports, timed actions synchronize in a broadcasting fashion in which all components of a parallel composition or a summation have to take part. For the sake of simplicity, we write γ for a representative of $\mathcal{A} \cup \mathcal{T}$.

Further, we use the standard definitions for *sort* of a process, where timed actions are never included in sorts, *free* and *bound variables*, *open* and *closed terms*, and *contexts*. A process variable is called *guarded* in a process term if each occurrence of the variable is in the scope of a prefix or in the scope of the second argument of a timeout (see below). We refer to closed and guarded terms as *processes* and denote syntactic equality on $\mathcal{P}$ by $\equiv$. Let $P, Q, R, \ldots$ range over the set $\mathcal{P}$ of processes. The syntax of our language is defined by the BNF presented in Table 1 where $f : \mathcal{A} \to \mathcal{A}$ is a *finite relabeling*, $L \subseteq \mathcal{A} \setminus \{\tau\}$ a *restriction set*, and C a *process constant*.

A finite relabeling satisfies the properties $f(\tau) = \tau$ and $|\{\alpha \,|\, f(\alpha) \neq \alpha\}\,| < \infty$. Moreover, $\uparrow$ is called *ignore operator* and $\lfloor\cdot\rfloor\sigma(\cdot)$ *timeout operator*.

Table 1: Syntax of $\mathsf{TPL}^{\mathsf{mc}}$

P	$::=$	$\mathbf{0}$	$\mid$	$\gamma.P$	$\mid$	$P + P$	$\mid$	$P \mid P$	$\mid$	$P[f]$	$\mid$
		$P \setminus L$	$\mid$	$P \uparrow \sigma$	$\mid$	$\lfloor P \rfloor \sigma(P)$	$\mid$	$C \overset{\text{def}}{=} P$			

In order to avoid too many parentheses we refine the 'binding power'-hierarchy of CCS [17]. Our operators have decreasing binding power in the following order: restriction and relabeling and ignore, prefix and timeout, parallel composition, summation.

2.2 Semantics of $\mathsf{TPL}^{\mathsf{mc}}$

The (*operational*) *semantics* of a $\mathsf{TPL}^{\mathsf{mc}}$ process $P \in \mathcal{P}$ is given by a labeled transition system $\langle \mathcal{P}, \mathcal{A}, \Leftrightarrow\!\!\rightarrow, P \rangle$ where $\mathcal{P}$ is the set of states, $\mathcal{A}$ the alphabet, $\Leftrightarrow\!\!\rightarrow$ the transition relation, and P the start state.

We define the semantics in such a fashion that communications must occur if they are possible. This assumption, which is often referred to as *maximal progress*, ensures that a process cannot delay if it is able to perform a communication. However, we are dealing with *distributed* systems. As discussed in the introduction, it is natural to localize the maximal progress assumption with respect to clocks. Incorporating maximal progress in the PMC-style semantics or local clocks in the TPL-style semantics leads to a more intuitive operational semantics as discussed in the previous example. Despite its intuitivity, our new semantics provides several challenges in developing a semantic theory. In contrast to the PMC-semantics we do not choose a time-stop interpretation for $\mathbf{0}$ and prefixing since we feel that time cannot be stopped. Therefore, $a.P$ should model a process which waits for a communication partner on port a and does not deadlock if no such partner is available immediately. Avoiding unnatural time-stops also helps us to define an intuitive notion of equivalence on processes.

The transition relation $\Leftrightarrow\!\!\rightarrow \subseteq \mathcal{P} \times (\mathcal{A} \cup \mathcal{T}) \times \mathcal{P}$ for $\mathsf{TPL}^{\mathsf{mc}}$ is defined in Table 3 using Plotkin-style [21] operational rules. We write $P \overset{\gamma}{\Leftrightarrow\!\!\rightarrow} P'$ instead of $\langle P, \gamma, P' \rangle \in \Leftrightarrow\!\!\rightarrow$. We say that P *may engage in action* γ *and thereafter behaves like process* P'. Sometimes it is convenient to write $P \overset{\gamma}{\Leftrightarrow\!\!\rightarrow}$ for $\exists P' \in \mathcal{P}.\, P \overset{\gamma}{\Leftrightarrow\!\!\rightarrow} P'$.

The presentation of the operational rules requires *initial action sets*. Beside the usual definition $\mathrm{I}(P)$ for the initial action set of a process P – where $\mathrm{I}(P \uparrow \sigma)$ and $\mathrm{I}(\lfloor P \rfloor \sigma(Q))$ are given by $\mathrm{I}(P)$ – we define the set $\mathrm{I}_\sigma(P)$ of all initial actions of P within the scope of the timer σ as the least set satisfying the rules in Table 2. We also define analogue initial actions sets ignoring τ-actions by $\mathbb{I}(P) =_{\text{df}} \mathrm{I}(P) \setminus \{\tau\}$ and $\mathbb{I}_\sigma(P) =_{\text{df}} \mathrm{I}_\sigma(P) \setminus \{\tau\}$, respectively. The definition $\mathrm{I}_\sigma(P \uparrow \sigma) = \emptyset$ reflects our intuition of localizing clocks. The initial actions of $P \uparrow \sigma$ are not in the scope of the clock σ , i.e. the process P is not attached to σ or, in other words, P ignores σ . Note that these action sets are defined independently from the transition relation $\Leftrightarrow\!\!\rightarrow$. Therefore, $\Leftrightarrow\!\!\rightarrow$ is well-defined although its definition contains negative premises (side conditions) [5].

Table 2: Initial action sets

$$\mathrm{I}_\sigma(\alpha.P) =_{\mathrm{df}} \{\alpha\}$$

$$\mathrm{I}_\sigma(P+Q) =_{\mathrm{df}} \mathrm{I}_\sigma(P) \cup \mathrm{I}_\sigma(Q) \qquad \mathrm{I}_\sigma(C) =_{\mathrm{df}} \mathrm{I}_\sigma(P) \text{ where } C \overset{\mathrm{def}}{=} P$$

$$\mathrm{I}_\sigma(P[f]) =_{\mathrm{df}} \{f(\alpha) \mid \alpha \in \mathrm{I}_\sigma(P)\} \qquad \mathrm{I}_\sigma(P \setminus L) =_{\mathrm{df}} \mathrm{I}_\sigma(P) \setminus (L \cup \overline{L})$$

$$\mathrm{I}_\sigma(P|Q) =_{\mathrm{df}} \mathrm{I}_\sigma(P) \cup \mathrm{I}_\sigma(Q) \cup \{\tau \mid \mathbb{I}_\sigma(P) \cap \overline{\mathbb{I}}(Q) \neq \emptyset \text{ or } \mathbb{I}_\sigma(Q) \cap \overline{\mathbb{I}}(P) \neq \emptyset\}$$

$$\mathrm{I}_\sigma(\lfloor P \rfloor \sigma'(Q)) =_{\mathrm{df}} \mathrm{I}_\sigma(P) \qquad \mathrm{I}_\sigma(P \uparrow \sigma') =_{\mathrm{df}} \begin{cases} \emptyset & \text{if } \sigma = \sigma' \\ \mathrm{I}_\sigma(P) & \text{otherwise} \end{cases}$$

The semantics of $\mathsf{TPL}^{\mathsf{mc}}$ for ordinary action transitions is the same as the usual TPL or PMC semantics which is basically that of CCS. The difference to PMC arises by the side conditions in the rules for timed transitions, which guarantee that our localized maximal progress assumption holds (cf. Proposition 2.3), and by disallowing time-stops. The process $\alpha.P$ may engage in action α and then behave like P. If $\alpha \neq \tau$ it may also idle for each timer σ. Similarly, $\sigma.P$ can perform the timed action σ and become P or idle for all other clocks. The *summation operator* $+$ denotes *nondeterministic choice*. The process $P + Q$ may behave like process P (Q). Time has to proceed equally on both sides of summation, i.e. $P + Q$ can engage in a timed action and, thus, delay the nondeterministic choice if and only if both P and Q can engage in the timed action. The *restriction operator* $\setminus L$ prohibits the execution of actions in $L \cup \overline{L}$. Thus, the restriction operator permits the *scoping* of actions. $P[f]$ behaves exactly as the process P where ordinary actions are renamed with respect to the *relabeling* f. The process $P|Q$ stands for the *parallel composition* of P and Q according to an *interleaving semantics* with *synchronized communication* on complementary actions resulting in the internal action τ. Also here, time has to proceed equally on both sides of the operator. The side conditions ensure that $P|Q$ can only idle on σ, if it cannot engage in an internal computation which is in the scope of σ. The process $P \uparrow \sigma$ behaves like the process P for all actions but the timed action σ. Additionally, $P \uparrow \sigma$ is capable of performing a timed action σ to $P \uparrow \sigma$ itself, i.e. P *ignores* σ. This allows the scoping of clocks in such a way that the traditional temporal semantics for the summation and parallel operator needs not to be changed. A central operator in a temporal process algebra is the *timeout* operator. The process $\lfloor P \rfloor \sigma(Q)$ behaves as the process P but it can perform a σ-action only to the process Q whenever P cannot engage in an internal action which is in the scope of the clock σ. Finally, $C \overset{\mathrm{def}}{=} P$ denotes a *constant definition*, i.e. C is a recursively defined process which behaves as a distinguished solution of the equation $C = P$.

We want to remark that the side condition of Rule tCOM can be written as $\tau \notin \mathrm{I}_\sigma(P|Q)$ (cf. Proposition 2.3 below). Although this is a shorter notation, the one used in the operational semantic Rule tCom is more convenient for the proofs of our main theorems which we present in the appendices of the paper. In contrast to PMC timed prefixing is no longer a derived operator since the semantics of the processes $\sigma.P$ and $\lfloor \mathbf{0} \rfloor \sigma(P)$ are different. The former process can engage in a timed action σ' to $\sigma.P$, where $\sigma' \neq \sigma$, while the latter can only engage in a σ'-transition to the process $\mathbf{0}$ which is obviously semantically different from the process $\sigma.P$ for most processes P.

Table 3: Operational semantics for $\mathsf{TPL}^{\mathsf{mc}}$

		tNil	$\frac{-}{\mathbf{0} \xrightarrow{\sigma} \mathbf{0}}$
		tAct1	$\frac{-}{a.P \xrightarrow{\sigma} a.P}$
Act	$\frac{-}{\alpha.P \xrightarrow{\alpha} P}$	tAct2	$\frac{-}{\sigma.P \xrightarrow{\sigma} P}$
		tAct3	$\frac{-}{\sigma.P \xrightarrow{\sigma'} \sigma.P}\ \sigma \neq \sigma'$
Sum1	$\frac{P \xrightarrow{\alpha} P'}{P + Q \xrightarrow{\alpha} P'}$	tSum	$\frac{P \xrightarrow{\sigma} P' \quad Q \xrightarrow{\sigma} Q'}{P + Q \xrightarrow{\sigma} P' + Q'}$
Sum2	$\frac{Q \xrightarrow{\alpha} Q'}{P + Q \xrightarrow{\alpha} Q'}$		
Rel	$\frac{P \xrightarrow{\alpha} P'}{P[f] \xrightarrow{f(\alpha)} P'[f]}$	tRel	$\frac{P \xrightarrow{\sigma} P'}{P[f] \xrightarrow{\sigma} P'[f]}$
Res	$\frac{P \xrightarrow{\alpha} P'}{P \setminus L \xrightarrow{\alpha} P' \setminus L}\ \alpha \notin L \cup \overline{L}$	tRes	$\frac{P \xrightarrow{\sigma} P'}{P \setminus L \xrightarrow{\sigma} P' \setminus L}$
Com1	$\frac{P \xrightarrow{\alpha} P'}{P \mid Q \xrightarrow{\alpha} P' \mid Q}$		
Com2	$\frac{Q \xrightarrow{\alpha} Q'}{P \mid Q \xrightarrow{\alpha} P \mid Q'}$	tCom	$\frac{P \xrightarrow{\sigma} P' \quad Q \xrightarrow{\sigma} Q'}{P \mid Q \xrightarrow{\sigma} P' \mid Q'}$ $\mathrm{I\!I}_\sigma(P) \cap \overline{\mathrm{I\!I}}(Q) = \emptyset$ and $\mathrm{I\!I}_\sigma(Q) \cap \overline{\mathrm{I\!I}}(P) = \emptyset$
Com3	$\frac{P \xrightarrow{a} P' \quad Q \xrightarrow{\overline{a}} Q'}{P \mid Q \xrightarrow{\tau} P' \mid Q'}$		
Ign	$\frac{P \xrightarrow{\alpha} P'}{P \uparrow \sigma \xrightarrow{\alpha} P' \uparrow \sigma}$	tIgn1	$\frac{-}{P \uparrow \sigma \xrightarrow{\sigma} P \uparrow \sigma}$
		tIgn2	$\frac{P \xrightarrow{\sigma'} P'}{P \uparrow \sigma \xrightarrow{\sigma'} P' \uparrow \sigma}\ \sigma \neq \sigma'$
TO	$\frac{P \xrightarrow{\alpha} P'}{\lfloor P \rfloor \sigma(Q) \xrightarrow{\alpha} P'}$	tTO1	$\frac{-}{\lfloor P \rfloor \sigma(Q) \xrightarrow{\sigma} Q}\ \tau \notin \mathrm{I}_\sigma(P)$
		tTO2	$\frac{P \xrightarrow{\sigma'} P'}{\lfloor P \rfloor \sigma(Q) \xrightarrow{\sigma'} P'}\ \sigma \neq \sigma'$
Con	$\frac{P \xrightarrow{\alpha} P'}{C \xrightarrow{\alpha} P'}\ C \overset{\mathrm{def}}{=} P$	tCon	$\frac{P \xrightarrow{\sigma} P'}{C \xrightarrow{\sigma} P'}\ C \overset{\mathrm{def}}{=} P$

The presented operational semantics for $\mathsf{TPL}^{\mathsf{mc}}$ possesses the following important properties.

Proposition 2.1 (Associativity & Commutativity)
The summation and the parallel operator of $\mathsf{TPL}^{\mathsf{mc}}$ *are associative and commutative modulo renaming of states.*

The following proposition is essential for the congruence proofs of some of the behavioral relations presented in the next sections. Its validity is a consequence of the idling capability of the processes $\mathbf{0}$ and $a.P$ for $a \in \mathcal{A} \setminus \{\tau\}$ and $P \in \mathcal{P}$.

Proposition 2.2 *Let* $P \in \mathcal{P}$ *and* $\sigma \in \mathcal{T}$ *satisfying* $\tau \notin \mathrm{I}_\sigma(P)$. *Then,* $P \overset{\sigma}{\Rrightarrow}$ *holds.*

Moreover, the semantics satisfies the *local maximal progress* and the *local time determinacy* property. Both are adaptions of the well-known *maximal progress* and *time determinacy* properties [24], which deal with a global notion of time, to our situation of multiple, *local* clocks.

Proposition 2.3 (Local Maximal Progress)
Let $P \in \mathcal{P}$ *and* $\sigma \in \mathcal{T}$. *Then,* $P \overset{\sigma}{\Rrightarrow}$ *implies* $\tau \notin \mathrm{I}_\sigma(P)$.

Proposition 2.4 (Local Time Determinacy)
Let $P, P', P'' \in \mathcal{P}$ *and* $\sigma \in \mathcal{T}$ *satisfying* $P \overset{\sigma}{\Rrightarrow} P'$ *and* $P \overset{\sigma}{\Rrightarrow} P''$. *Then,* $P' \equiv P''$ *holds.*

Both propositions can easily be checked by induction on the depth of the derivation tree of $P \overset{\sigma}{\Rrightarrow} P'$ and the maximum of the depths of the derivation trees of $P \overset{\sigma}{\Rrightarrow} P'$ and $P \overset{\sigma}{\Rrightarrow} P''$, respectively.

3 Examples

In this section, we demonstrate that our operators and their semantics are well-chosen. In the first part, we deal with modeling *distributed control systems*. This example shows the usefulness of multiple, local, abstract clocks in a specification language. In the second part, we deal with a simple communication protocol which shows that our algebra is more suitable for verification purposes than PMC.

3.1 Modeling a Distributed Control System

A distributed control system typically consists of several sensors which continuously measure sizes of an environment, e.g. temperature and wind, and of several evaluators who use the data collected by the sensors to compute values of interest, e.g. the wind-chill temperature. Figure 2 depicts the architecture of a typical distributed control system consisting of three sensors and two evaluators where dashed lines represent clocks and solid lines represent usual communication channels. `Evaluator1` is connected to `Sensor1` via port v_1 and to `Sensor2` via port v_2. Similarly, `Evaluator2` is connected to `Sensor2` via port v_2 and to Sensor3 via port v_3. Moreover, `Sensor1`, `Sensor2`, and `Evaluator1` share the clock σ_{E1}, whereas `Sensor2`, `Sensor3`, and `Evaluator2` share the clock σ_{E2}.

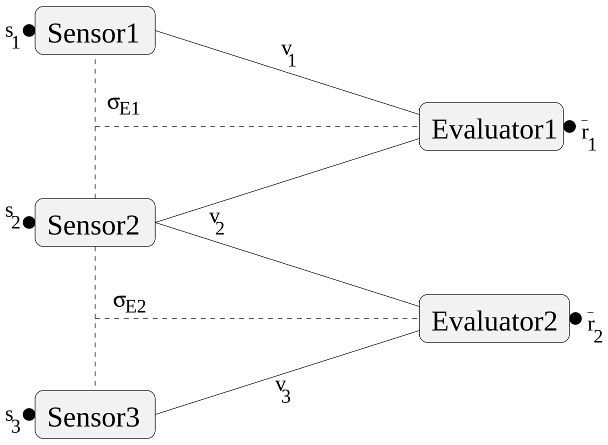

Figure 2: Distributed control system

Each sensor measures continuously its environment. The event of measuring is modeled by the action s_i, $1 \leq i \leq 3$. Upon a tick of the clock σ_{E1} the sensors `Sensor1` and `Sensor2` send their latest values via channels v_1 and v_2, respectively, to `Evaluator1`. Similarly, `Sensor2` and `Sensor3` send their latest values via channels v_2 and v_3 to `Evaluator2` at each tick of the clock σ_{E2}, respectively. Upon reception of the values, each evaluator computes a new value depending on the values received and offers it via the output channel $\overline{r}_1$ ($\overline{r}_2$).

Using the process algebra $\mathsf{TPL}^{\mathsf{mc}}$ we can formalize the distributed control system `System` as follows.

$$\begin{aligned}\mathtt{System} \stackrel{\text{def}}{=} \; & (\mathtt{Sensor1}\upharpoonright\sigma_{E2} \mid \mathtt{Sensor2} \mid \mathtt{Sensor3}\upharpoonright\sigma_{E1} \mid \\ & \;\mathtt{Evaluator1}\upharpoonright\sigma_{E2} \mid \mathtt{Evaluator2}\upharpoonright\sigma_{E1} \\ &) \setminus \{v_1, v_2, v_3\}\end{aligned}$$

where

$$\begin{aligned}
\mathtt{Sensor1} &\stackrel{\text{def}}{=} \lfloor s_1.\mathtt{Sensor1}\rfloor\sigma_{E1}(\overline{v_1}.\mathtt{Sensor1}) \\
\mathtt{Sensor2} &\stackrel{\text{def}}{=} \lfloor\lfloor s_2.\mathtt{Sensor2}\rfloor\sigma_{E1}(\overline{v_2}.\mathtt{Sensor2})\rfloor\sigma_{E2}(\overline{v_2}.\mathtt{Sensor2}) \\
\mathtt{Sensor3} &\stackrel{\text{def}}{=} \lfloor s_3.\mathtt{Sensor3}\rfloor\sigma_{E2}(\overline{v_3}.\mathtt{Sensor3}) \\
\mathtt{Evaluator1} &\stackrel{\text{def}}{=} \sigma_{E1}.v_1.v_2.\tau.\overline{r_1}.\mathtt{Evaluator1} \\
\mathtt{Evaluator2} &\stackrel{\text{def}}{=} \sigma_{E2}.v_2.v_3.\tau.\overline{r_2}.\mathtt{Evaluator2}
\end{aligned}$$

This example makes intensive use of the timeout operator. The timeout operator enables us to model *interrupts* invoked by the ticking of the attached clocks. Our maximal progress assumption plays an essential role in our model. One would intuitively demand the property that the sequence of actions v_1, v_2, and τ and the sequence of actions v_2, v_3, and τ are executed atomically, i.e. no ticking of the clocks σ_{E1} and σ_{E2} can interfere or delay the sequences, respectively. This is important since an evaluator can typically only produce a useful result when its parameters v_1 and v_2, or v_2 and v_3 have been measured at approximately the same time. Our maximal progress assumption ensures the atomicity of the mentioned sequences. However, the above intuition can also be modeled in PMC by using the time-stop prefixing operator in those sequences. A time-stop prefixing of a process P with an action a disallows a tick to occur after the execution of a and before the execution of P. However, we give an example below, where time-stop prefixing cannot 'replace' our maximal progress assumption.

We want to remark on our *localized* version of the maximal progress property. In this example, we have abstracted from the internal clocks of the sensors since we are not concerned about real-time constraints of the measuring processes. This concept of abstraction emphasizes again the utility of the localized maximal progress assumption; e.g. if we model the environment of `Sensor1` by $\mathtt{Env}_1 =_{\mathrm{df}} \overline{s}_1.\mathtt{Env}_1$, then we introduce a τ-loop in our system. Thus, the usual maximal progress assumption would prevent the ticking of any clock. This shows that our notion of localized maximal progress is necessary when dealing with *abstraction from local timing constraints* and with *multiple clocks* in one process algebra.

Distributed control systems represent a large class of real-time systems where multiple clocks which run independent from each other are a useful mean for modeling. Moreover, this class of systems shows that time constraints often introduce qualitative aspects which effect the causal behavior of a system. Those constraints are in practice often more important than constraints dealing with quantitative aspects of time.

3.2 A Simple Communication Protocol

The next example models a simple *communication protocol*. It consists of a sender, a medium, and a receiver. Both, sender and receiver, possess an own clock since they are supposed to be at different physical locations, e.g. the sender and the receiver are two computers. The following equation `Protocol` defines the protocol formally in $\mathsf{TPL}^{\mathsf{mc}}$.

$$\begin{aligned}\mathtt{Protocol} \overset{\text{def}}{=} \; & (\mathtt{Sender} \uparrow \sigma_R \mid \\ & \;\mathtt{Medium} \uparrow \sigma_S \uparrow \sigma_R \mid \\ & \;\mathtt{Receiver} \uparrow \sigma_S \\ &) \setminus \{\mathtt{s}, \mathtt{r}, \mathtt{s}_{\mathtt{ack}}, \mathtt{r}_{\mathtt{ack}}, \mathtt{s}_{\mathtt{fail}}, \mathtt{r}_{\mathtt{fail}}\}\end{aligned}$$

where

$$\begin{aligned}\mathtt{Sender} &\overset{\text{def}}{=} \mathtt{send}.\sigma_S.S \\ S &\overset{\text{def}}{=} \overline{\mathtt{s}}.(\mathtt{r}_{\mathtt{ack}}.\mathtt{Sender} + \mathtt{r}_{\mathtt{fail}}.S) \\ \\ \mathtt{Medium} &\overset{\text{def}}{=} \mathtt{s}.\overline{\mathtt{r}}.\mathtt{Medium} + \mathtt{s}_{\mathtt{ack}}.\overline{\mathtt{r}}_{\mathtt{ack}}.\mathtt{Medium} + \mathtt{s}_{\mathtt{fail}}.\overline{\mathtt{r}}_{\mathtt{fail}}.\mathtt{Medium} \\ \\ \mathtt{Receiver} &\overset{\text{def}}{=} \lfloor \mathtt{r}.R \rfloor \sigma_R(\overline{\mathtt{s}}_{\mathtt{fail}}.\mathtt{Receiver}) \\ R &\overset{\text{def}}{=} \overline{\mathtt{s}}_{\mathtt{ack}}.\mathtt{receive}.R\end{aligned}$$

The sender accepts a message from its environment and puts it on the medium immediately after the next clock tick σ_S. Then it waits for an acknowledgment, after which the sender is ready to accept a new message from the environment, or a failure message, which indicates that the receiver has not received a message for a 'long' time. In such a case the message is resent. We consider a reliable medium, i.e. every message and acknowledgment put in the medium is delivered and cannot get lost. Moreover, we abstract from the delay which could be caused by transporting a message since we are not interested in the timing behavior of the medium. However, we plug a receiver 'out of the box' in our system which, as the sender, can also handle unreliable media. The receiver works in the following fashion. It waits to receive a message from the medium. However, if no message is offered from the medium, then the receiver may timeout and send a failure message back to the sender. A received message is acknowledged and delivered to the environment before the receiver is ready to accept a new message.

The point of this example is that `Protocol` can deadlock when we interprete the operators as in PMC, also if the prefix operator is interpreted as *relaxed prefix*, i.e. the semantics for prefixing is as in $\mathsf{TPL}^{\mathsf{mc}}$. One path to a deadlock, which is a state without outgoing transitions, is given by performing the action `send`, a synchronization on `s`, and a timeout on σ_R. The reason for this is that the receiver can choose to timeout although a message is offered from the medium. However, in $\mathsf{TPL}^{\mathsf{mc}}$ the localized maximal progress assumption forces the synchronization on `r` to occur such that the timeout on σ_R is preempted. This shows that the new temporal process algebra $\mathsf{TPL}^{\mathsf{mc}}$ is more suitable for verifying systems than PMC. Another example showing the same phenomenon as above is the well-known Alternating Bit Protocol.

In the following sections we develop a semantic theory for $\mathsf{TPL}^{\mathsf{mc}}$.

4 Temporal Strong Bisimulation

In this section, we present a congruence on $\mathsf{TPL}^{\mathsf{mc}}$ processes which is based on bisimulation [20]. Our aim is to characterize the largest congruence contained in the standard strong bisimulation [16] where we treat timed actions as any other action.

Definition 4.1 (Naive Strong Bisimulation)
A symmetric relation $\mathcal{R} \subseteq \mathcal{P} \times \mathcal{P}$ is called naive strong bisimulation *if for every $\langle P, Q \rangle \in \mathcal{R}$, $\alpha \in \mathcal{A}$, and $\sigma \in \mathcal{T}$ the following conditions hold.*

1. $P \overset{\alpha}{\Rrightarrow} P'$ *implies* $\exists Q'. \, Q \overset{\alpha}{\Rrightarrow} Q'$ *and* $\langle P', Q' \rangle \in \mathcal{R}$.
2. $P \overset{\sigma}{\Rrightarrow} P'$ *implies* $\exists Q'. \, Q \overset{\sigma}{\Rrightarrow} Q'$ *and* $\langle P', Q' \rangle \in \mathcal{R}$.

We write $P \sim_{\times} Q$ if there exists a naive strong bisimulation $\mathcal{R}$ such that $\langle P, Q \rangle \in \mathcal{R}$.

It is straightforward to establish that $\sim_{\times}$ is the *largest* naive strong bisimulation and that $\sim_{\times}$ is an equivalence relation. Unfortunately, $\sim_{\times}$ is *not* a congruence which is a necessary requirement for an equivalence relation to be suitable for compositional reasoning. The lack of compositionality is demonstrated by the following example involving the parallel operator. We have

$$a.\mathbf{0} \sim_{\times} a.\mathbf{0} \uparrow \sigma$$

but

$$a.\mathbf{0}\,|(\overline{a}.\mathbf{0} \uparrow \sigma) \not\sim_{\times} (a.\mathbf{0} \uparrow \sigma)\,|(\overline{a}.\mathbf{0} \uparrow \sigma)$$

since the latter can do a σ-transition while the corresponding σ-transition of the former process is preempted because the a-transition of the former process is in the scope of the timer σ.

The above observation is not surprising because the scope of timers has influence on the preemption of transitions and, consequently, on the bisimulation. Thus, in order to find the largest congruence relation $\sim^{+}$ contained in $\sim_{\times}$ we have to take the scopes of timers into account. In the following, we define $\sim^{+}$ which repairs the congruence defect of $\sim_{\times}$ shown above.

Definition 4.2 (Temporal Strong Bisimulation)
A symmetric relation $\mathcal{R} \subseteq \mathcal{P} \times \mathcal{P}$ is a temporal strong bisimulation *if for every $\langle P, Q\rangle \in \mathcal{R}$, $\alpha \in \mathcal{A}$, and $\sigma \in \mathcal{T}$ the following conditions hold.*

1. *$P \overset{\alpha}{\Rrightarrow} P'$ implies $\exists Q'.\, Q \overset{\alpha}{\Rrightarrow} Q'$ and $\langle P', Q'\rangle \in \mathcal{R}$.*
2. *$P \overset{\sigma}{\Rrightarrow} P'$ implies $\exists Q'.\, Q \overset{\sigma}{\Rrightarrow} Q'$, $\mathbb{I}_{\sigma}(Q) \subseteq \mathbb{I}_{\sigma}(P)$, and $\langle P', Q'\rangle \in \mathcal{R}$.*

We write $P \sim^{+} Q$ if there exists a temporal strong bisimulation $\mathcal{R}$ such that $\langle P, Q\rangle \in \mathcal{R}$.

The difference between this definition and the definition of $\sim_{\times}$ is the additional requirement concerning the initial action sets – parameterized in the appropriate timer – in the second condition. Intuitively, the initial action set of a process with respect to some clock is a measure of the preemptive power of the process relative to the clock. Thus, the second condition of Definition 4.2 states that a timed action σ of the process P has to be matched by the same timed action of Q. Moreover, the preemptive power of Q with respect to σ is at most as strong as the preemptive power of P with respect to σ.

Theorem 4.3 *The relation $\sim^{+}$ is a congruence with respect to all operators, i.e. for all* $\mathsf{TPL}^{\mathsf{mc}}$ *contexts C we have: $P \sim^{+} Q$ implies $C[P] \sim^{+} C[Q]$.*

It is worth mentioning the following observation.

Remark 4.4 *If we would adopt the semantics of* $\mathbf{0}$ *and the prefix operator, as presented in [3] where time-stops are intended, then the relation $\sim^{+}$ would not be a congruence. In order to see this, take a look at the processes $\tau.\mathbf{0} \uparrow \sigma + a.\mathbf{0}$ and $\tau.\mathbf{0} + a.\mathbf{0}$ which are temporal strong bisimular according to the modified semantics. However, $\lfloor \tau.\mathbf{0} \uparrow \sigma + a.\mathbf{0} \rfloor \sigma(b.\mathbf{0})$ and $\lfloor \tau.\mathbf{0} + a.\mathbf{0} \rfloor \sigma(b.\mathbf{0})$ are* not *temporal strong bisimular since the former can timeout on σ to become the process $b.\mathbf{0}$. The latter process cannot timeout since the τ-action is in the scope of σ. Therefore, such a step* *would contradict our maximal progress assumption. It is relatively easy to see that a necessary condition for* $\sim^+$ *to be compositional with respect to the timeout operator would be*

$$P \sim^+ Q \;\; \textit{implies} \;\; (\tau \in \mathrm{I}_\sigma(P) \;\Leftrightarrow\; \tau \in \mathrm{I}_\sigma(Q)) \ .$$

However, this condition is not sufficient since it is in conflict with the compositionality of the parallel operator. As an example, take the processes $(a.\mathbf{0} \upharpoonright \sigma) \,|\, b.\mathbf{0}$ *and* $a.\mathbf{0} \,|\, b.\mathbf{0}$ *and the context* $C[X] =_{\mathrm{df}} X \,|(\overline{a}.\mathbf{0} \upharpoonright \sigma)$ *. Thus, our definition of the semantics of* $\mathbf{0}$ *and the prefix operator which prohibits time-stop is not only more intuitive than the PMC-semantics but also better treatable from a technical point of view.*

Before we continue to present the theoretical results concerning temporal strong bisimulation, we provide an example.

Example 4.5 *We return to the example of the communication protocol introduced in Section 3. Considering the semantics of* `Protocol` *it is easy to see that* `Protocol` $\sim^+$ $\mathtt{Spec}_s$ *where*

$$\mathtt{Spec}_s \stackrel{\mathrm{def}}{=} \mathtt{send}.\sigma_S.\tau.\tau.(\tau.\mathtt{receive}.\mathtt{Spec}_s + \mathtt{receive}.\tau.\mathtt{Spec}_s) \ .$$

The next theorem states the main result of this section.

Theorem 4.6 *The congruence* $\sim^+$ *is the* largest *congruence contained in* $\sim_\times$ *.*

We conclude this section by providing a logical characterization of $\sim^+$. We adapt the well-known *Hennessy-Milner Logic* [17] by changing the semantics of the modal operators.

The syntax of the logic we use is defined by the following BNF where $L \subseteq \mathcal{A} \setminus \{\tau\}$.

$$\Phi \quad ::= \quad tt \quad | \quad \neg\Phi \quad | \quad \Phi \wedge \Phi \quad | \quad \langle\alpha\rangle\Phi \quad | \quad \langle\sigma, L\rangle\Phi$$

The set of all formulae, which can be generated by the BNF above, is denoted by $\mathcal{F}$ and ranged over by $\Phi, \Psi, \ldots$. For convenience, we also introduce the following dual operators: $tt =_{\mathrm{df}} \neg ff$, $\Phi \vee \Psi =_{\mathrm{df}} \neg(\neg\Phi \wedge \neg\Psi)$, $[\alpha]\Phi =_{\mathrm{df}} \neg\langle\alpha\rangle(\neg\Phi)$, and $[\sigma, L]\Phi =_{\mathrm{df}} \neg\langle\sigma, L\rangle(\neg\Phi)$. Further, we abbreviate $\Phi_1 \wedge \Phi_2 \wedge \ldots \wedge \Phi_n$ for some $n \in \mathbb{N}$ by $\bigwedge_{i=1}^n \Phi_i$.

We define the *satisfaction relation* $\models \; \subseteq \mathcal{P} \times \mathcal{F}$ between processes and formulae inductively on the structure of formulae.

$$\begin{array}{lll}
 & P \models tt & \\
 & & \\
P \models \neg\Phi & \text{if} & \text{not } P \models \Phi \\
 & & \\
P \models \Phi \wedge \Psi & \text{if} & P \models \Phi \text{ and } P \models \Psi \\
 & & \\
P \models \langle\alpha\rangle\Phi & \text{if} & \exists P' \in \mathcal{P}.\ P \overset{\alpha}{\Rrightarrow} P' \text{ and } P' \models \Phi \\
 & & \\
P \models \langle\sigma, L\rangle\Phi & \text{if} & \exists P' \in \mathcal{P}.\ P \overset{\sigma}{\Rrightarrow} P' ,\ \mathbb{I}_\sigma(P) \subseteq L ,\ \text{and } P' \models \Phi
\end{array}$$

Intuitively, P satisfies $\langle \sigma, L \rangle \Phi$ if P possesses a σ-transition to a process satisfying Φ. Moreover, the preemptive power of P with respect to the clock σ may be at most L.

The above defined logic characterizes temporal strong bisimulation.

Theorem 4.7 (Characterization of $\sim^+$)
Let $P, Q \in \mathcal{P}$. We have $P \sim^+ Q$ if and only if $\{\Phi \in \mathcal{F} \,|\, P \models \Phi\} = \{\Phi \in \mathcal{F} \,|\, Q \models \Phi\}$.

5 Temporal Observation Congruence

The semantic congruence developed in the previous section is too strong for verifying systems in practice. Temporal strong bisimulation requires that two equivalent systems have to match exactly each others transitions, even those labeled with internal actions. Therefore, we want to abstract from internal actions and develop a semantic congruence from the point of view of an external observer.

Our approach follows the lines of [17]. We start off with the definition of a naive temporal weak bisimulation which abstracts from internal actions. This relation is an adaption of observation equivalence [17].

Definition 5.1 (Naive Temporal Weak Transition Relation)
We define:

1. $\hat{\alpha} =_{\mathrm{df}} \epsilon$ *if* $\alpha = \tau$ *and* $\hat{\alpha} =_{\mathrm{df}} \alpha$, *otherwise.*
2. $\stackrel{\epsilon}{\Longrightarrow}_{\times} =_{\mathrm{df}} \xrightarrow{\tau}{}^{*}$
3. $\stackrel{\alpha}{\Longrightarrow}_{\times} =_{\mathrm{df}} \stackrel{\epsilon}{\Longrightarrow}_{\times} \circ \xrightarrow{\alpha} \circ \stackrel{\epsilon}{\Longrightarrow}_{\times}$
4. $\stackrel{\sigma}{\Longrightarrow}_{\times} =_{\mathrm{df}} \stackrel{\epsilon}{\Longrightarrow}_{\times} \circ \xrightarrow{\sigma} \circ \stackrel{\epsilon}{\Longrightarrow}_{\times}$

Now, we define *naive temporal weak bisimulation* as follows.

Definition 5.2 (Naive Temporal Weak Bisimulation)
A symmetric relation $\mathcal{R} \subseteq \mathcal{P} \times \mathcal{P}$ is a naive temporal weak bisimulation *if for every $\langle P, Q \rangle \in \mathcal{R}$, $\alpha \in \mathcal{A}$, and $\sigma \in \mathcal{T}$ the following conditions hold.*

1. $P \xrightarrow{\alpha} P'$ *implies* $\exists Q'. \, Q \stackrel{\hat{\alpha}}{\Longrightarrow}_{\times} Q'$ *and* $\langle P', Q' \rangle \in \mathcal{R}$.
2. $P \xrightarrow{\sigma} P'$ *implies* $\exists Q'. \, Q \stackrel{\sigma}{\Longrightarrow}_{\times} Q'$ *and* $\langle P', Q' \rangle \in \mathcal{R}$.

We write $P \approx_{\times} Q$ if there exists a naive temporal weak bisimulation $\mathcal{R}$ such that $\langle P, Q \rangle \in \mathcal{R}$.

Since no initial action sets are considered, it is easy to see that $\approx_\times$ is not a congruence. In order to get closer to our goal to define a temporal observation congruence, we redefine the weak transition relation for timed actions.

Definition 5.3 (Temporal Weak Transition Relation)
We introduce the following notation where $L, M \subseteq \mathcal{A} \setminus \{\tau\}$ *.*

1. $P \overset{\epsilon}{\Longrightarrow} P'$ *iff* $P \overset{\epsilon}{\Longrightarrow}_\times P'$ *.*
2. $P \overset{\alpha}{\Longrightarrow} P'$ *iff* $P \overset{\alpha}{\Longrightarrow}_\times P'$ *.*
3. $P \underset{L,M}{\overset{\sigma}{\Longrightarrow}} P'$ *iff* $\exists P''.\, P \overset{\epsilon}{\Longrightarrow} P'' \xrightarrow{\sigma} \circ \overset{\epsilon}{\Longrightarrow} P'$ *,* $\mathbb{I}_\sigma(P'') \subseteq L$ *and* $\mathbb{I}(P'') \subseteq M$ *.*

In the remainder, we drop the operator $\circ$ which denotes the relation product. Recall that the visible initial action set of a process (with respect to a clock) is a measure for its preemptive power. There are two slightly different perspectives of preemption which are encoded in the sets L and M in the definition of $P \underset{L,M}{\overset{\sigma}{\Longrightarrow}} P'$, respectively. Whereas L is concerned with the influence of the environment, i.e. a parallel context, on the timed action σ , the set M reflects the impact of P'' on potential synchronization partners (cf. Rule tCom). Accordingly, we define the following notion of *temporal weak bisimulation.*

Definition 5.4 (Temporal Weak Bisimulation)
A symmetric relation $\mathcal{R} \subseteq \mathcal{P} \times \mathcal{P}$ *is a* temporal weak bisimulation *if for every* $\langle P, Q \rangle \in \mathcal{R}$ *,* $\alpha \in \mathcal{A}$ *, and* $\sigma \in \mathcal{T}$ *the following conditions hold.*

1. $P \xrightarrow{\alpha} P'$ *implies* $\exists Q'.\, Q \overset{\hat{\alpha}}{\Longrightarrow} Q'$ *and* $\langle P', Q' \rangle \in \mathcal{R}$ *.*
2. $P \xrightarrow{\sigma} P'$ *implies* $\exists Q'.\, Q \underset{L,M}{\overset{\sigma}{\Longrightarrow}} Q',\ L = \mathbb{I}_\sigma(P),\ M = \mathbb{I}(P),$ *and* $\langle P', Q' \rangle \in \mathcal{R}$ *.*

We write $P \underline{\approx} Q$ *if there exists a temporal weak bisimulation* $\mathcal{R}$ *such that* $\langle P, Q \rangle \in \mathcal{R}$ *.*

From this definition, we may conclude that $\underline{\approx}$ is the *largest* temporal weak bisimulation, and that $\underline{\approx}$ is an equivalence relation. Moreover, we have the following proposition.

Proposition 5.5 *The equivalence relation* $\underline{\approx}$ *is a congruence with respect to all* $\mathsf{TPL}^{\mathsf{mc}}$ *operators except the summation operator, the timeout operator, and recursion.*

The reason for the non-compositionality of the summation and the recursion operators is similar to that with respect to observation equivalence in CCS [17]. In order to see why $\underline{\approx}$ is not compositional with respect to the timeout operator, take a look at the processes $\mathbf{0}$ and $\tau.\mathbf{0}$, which are temporal weak bisimular, and the context $C[X] =_{\mathrm{df}} \lfloor X \rfloor \sigma(a.\mathbf{0})$. Observe that $C[\mathbf{0}]$ can engage in a σ-transition but $C[\tau.\mathbf{0}]$ cannot because $\tau \in \mathrm{I}_\sigma(\tau.\mathbf{0})$.

The summation fix presented in [17] is not sufficient in order to achieve a congruence relation. This is first because of the same reason that naive strong bisimulation is not a congruence with respect to parallel composition in $\mathsf{TPL}^{\mathsf{mc}}$ and second because of the semantics of the timeout operator.

Definition 5.6 (Temporal Observation Congruence)
We define $P \underline{\approx}^+ Q$ if for all $\alpha \in \mathcal{A}$ and $\sigma \in \mathcal{T}$ the following conditions hold.

1. $P \xrightarrow{\alpha} P'$ *implies* $\exists Q'. Q \overset{\alpha}{\Longrightarrow} Q'$ *and* $P' \underline{\approx} Q'$.
2. $P \xrightarrow{\sigma} P'$ *implies* $\exists Q'. Q \xrightarrow{\sigma} \overset{\epsilon}{\Longrightarrow} Q'$, $\mathbb{I}_\sigma(Q) \subseteq \mathbb{I}_\sigma(P)$, $\mathbb{I}(Q) \subseteq \mathbb{I}(P)$, *and* $P' \underline{\approx} Q'$.
3. $Q \xrightarrow{\alpha} Q'$ *implies* $\exists P'. P \overset{\alpha}{\Longrightarrow} P'$ *and* $P' \underline{\approx} Q'$.
4. $Q \xrightarrow{\sigma} Q'$ *implies* $\exists P'. P \xrightarrow{\sigma} \overset{\epsilon}{\Longrightarrow} P'$, $\mathbb{I}_\sigma(P) \subseteq \mathbb{I}_\sigma(Q)$, $\mathbb{I}(P) \subseteq \mathbb{I}(Q)$, *and* $P' \underline{\approx} Q'$.

The timeout operator is also responsible that a σ-transition has to be matched by a weak σ-transition not having any leading τ's. E.g., the processes $\sigma.\mathbf{0}$ and $\tau.\sigma.\mathbf{0}$ are not observation congruent since the context $C[X] =_{\mathrm{df}} \lfloor X \rfloor \sigma(a.\mathbf{0})$ distinguishes them.

Again, we take a look at our example of the communication protocol.

Example 5.7 *Let* `Protocol` *be the communication protocol introduced in Section 3 and define*

$$\mathtt{Spec}_w \overset{\mathrm{def}}{=} \mathtt{send}.\sigma_S.\mathtt{receive}.\mathtt{Spec} \ .$$

Then we have $\mathtt{Protocol} \underline{\approx}^+ \mathtt{Spec}_w$.

Since both `Protocol` *and* $\mathtt{Spec}_w$ *are stable, i.e. they can initially engage only in visible actions, it is by Definitions 5.4 and 5.6 sufficient to show that* $\mathtt{Protocol} \underline{\approx} \mathtt{Spec}_w$. *Consider the following relation* $\mathcal{R}$ *where* $L =_{\mathrm{df}} \{\mathtt{s}, \mathtt{r}, \mathtt{s}_{\mathtt{ack}}, \mathtt{r}_{\mathtt{ack}}, \mathtt{s}_{\mathtt{fail}}, \mathtt{r}_{\mathtt{fail}}\}$.

$$\begin{array}{lll}
\mathcal{R} & =_{\mathrm{df}} \{ & \langle \mathtt{Protocol}, \mathtt{Spec}_w \rangle, \\
 & & \langle (\sigma_S.S \,|\, \mathtt{Medium} \,|\, \mathtt{Receiver}) \setminus L, \sigma_S.S \rangle, \\
 & & \langle (S \,|\, \mathtt{Medium} \,|\, \mathtt{Receiver}) \setminus L, \mathtt{receive}.\mathtt{Spec}_w \rangle \\
 & & \langle ((\mathtt{r}_{\mathtt{ack}}.\mathtt{Sender} + \mathtt{r}_{\mathtt{fail}}.S) \,|\, \overline{\mathtt{r}}.\mathtt{Medium} \,|\, \mathtt{Receiver}) \setminus L, \mathtt{receive}.\mathtt{Spec}_w \rangle \\
 & & \langle ((\mathtt{r}_{\mathtt{ack}}.\mathtt{Sender} + \mathtt{r}_{\mathtt{fail}}.S) \,|\, \mathtt{Medium} \,|\, R) \setminus L, \mathtt{receive}.\mathtt{Spec}_w \rangle \\
 & & \langle ((\mathtt{r}_{\mathtt{ack}}.\mathtt{Sender} + \mathtt{r}_{\mathtt{fail}}.S) \,|\, \overline{\mathtt{r}}_{\mathtt{ack}}.\mathtt{Medium} \,|\, \mathtt{receive}.R) \setminus L, \mathtt{receive}.\mathtt{Spec}_w \rangle \\
 & & \langle (\mathtt{Sender} \,|\, \mathtt{Medium} \,|\, \mathtt{receive}.R) \setminus L, \mathtt{receive}.\mathtt{Spec}_w \rangle \\
 & & \langle ((\mathtt{r}_{\mathtt{ack}}.\mathtt{Sender} + \mathtt{r}_{\mathtt{fail}}.S) \,|\, \overline{\mathtt{r}}_{\mathtt{ack}}.\mathtt{Medium} \,|\, R) \setminus L, \mathtt{Spec}_w \rangle \ \}
\end{array}$$

Then the symmetric closure of $\mathcal{R}$ *is a temporal weak bisimulation which includes the pair* $\langle \mathtt{Protocol}, \mathtt{Spec}_w \rangle$. *We leave it to the interested reader to check that* $\mathcal{R}$ *is indeed a temporal weak bisimulation according to Definition 5.4.*

Now, we are able to present the main theorem of this section.

Theorem 5.8 *The relation* $\underline{\approx}^+$ *is the* largest congruence *contained in* $\approx_\times$.

We want to conclude this section by a remark on the logical characterization of $\underline{\approx}$. Defining a suitable logic can simply be done by replacing the $\langle \sigma, L \rangle$ operators from the logic in the previous section by new operators $\langle\langle \sigma, L, M \rangle\rangle$ where a process $P \in \mathcal{P}$ satisfies the formulae $\langle\langle \sigma, L, M \rangle\rangle \Phi$ if there exists a process $P' \in \mathcal{P}$ such that $P \underset{L,M}{\overset{\sigma}{\Longrightarrow}} P'$ and $P' \models \Phi$. Additionally, the operators $\langle \alpha \rangle$ have to be replaced by operators $\langle\langle \alpha \rangle\rangle$. We define $P \models \langle\langle \alpha \rangle\rangle \Phi$ if $\exists P' \in \mathcal{P}\,.\,P \overset{\alpha}{\Longrightarrow} P'$ and $P' \models \Phi$. The proof that the new logic characterizes $\underset{\sim}{\approx}$ can be done along the lines of [17].

6 Conclusions and Future Work

We have presented a temporal process algebra with multiple clocks and localized maximal progress assumption which is closely related to the process algebras TPL and PMC. Whereas TPL does not deal with multiple clocks, and the semantics of PMC does not ensure maximal progress, our process algebra combines both features. In contrast to PMC, we concentrate in defining an intuitive operational semantics and provide a semantic equivalence in terms of bisimulations. The characterizations of the largest congruences in the usual strong and weak bisimulation are of special importance for compositional reasoning which underlies most of the existing verification techniques.

Future work should especially focus on two aspects. On the one hand, an adaption of standard partitioning algorithms [15, 19] to compute temporal strong and weak equivalence is necessary in order to incorporate $\mathsf{TPL}^{\mathsf{mc}}$ in automatic verification tools, e.g. the NCSU Concurrency Workbench. On the other hand, an axiomatic characterization of the behavioral relations would support a better understanding of the underlying semantic theory and simplify a comparison with other temporal process algebras.

Acknowledgments. The second author would like to thank V. Natarajan for many helpful discussions.

References

[1] J. Leach Albert, B. Monien, and M. Rodrı́guez Artalejo, editors. *Automata, Languages and Programming (ICALP '91)*, volume 510 of *Lecture Notes in Computer Science*, Madrid, July 1991. Springer-Verlag.

[2] H.R. Andersen and M. Mendler. Complete axiomatization of observational congruence for PMC. Technical Report ID-TR:1993-126, Department of Computer Science, Technical University of Denmark, December 1993.

[3] H.R. Andersen and M. Mendler. A process algebra with multiple clocks. Technical Report ID-TR:1993-122, Department of Computer Science, Technical University of Denmark, August 1993.

[4] J.C.M. Baeten and W.P. Weijland. *Process Algebra*, volume 18 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, Cambridge, England, 1990.

[5] R.N. Bol and J.F. Groote. The meaning of negative premises in transition system specifications. In Albert et al. [1], pages 481–494.

[6] J. Camilleri and G. Winskel. CCS with priority choice. In *Sixth Annual Symposium on Logic in Computer Science (LICS '91)*, pages 246–255, Amsterdam, July 1991. IEEE Computer Society Press.

[7] R. Cleaveland. Analyzing concurrent systems using the Concurrency Workbench. In P.E. Lauer, editor, *Functional Programming, Concurrency, Simulation and Automated Reasoning*, volume 693 of *Lecture Notes in Computer Science*, pages 129–144. Springer-Verlag, 1993.

[8] R. Cleaveland and M.C.B. Hennessy. Priorities in process algebra. *Information and Computation*, 87(1/2):58–77, July/August 1990.

[9] R. Cleaveland, G. Lüttgen, and V. Natarajan. A process algebra with distributed priorities. Technical Report TR-96-02, North Carolina State University, March 1996.

[10] R. Cleaveland, J. Parrow, and B. Steffen. The Concurrency Workbench: A semantics-based tool for the verification of finite-state systems. *ACM Transactions on Programming Languages and Systems*, 15(1):36–72, January 1993.

[11] W. Elseaidy, R. Cleaveland, and J. Baugh. Verifying an intelligent structure control system: A case study. In *Proceedings of the Real-Time Systems Symposium*, pages 271–275, San Juan, Puerto Rico, December 1994. IEEE Computer Society Press.

[12] M.C.B. Hennessy. *Algebraic Theory of Processes.* MIT Press, Boston, 1988.

[13] M.C.B. Hennessy and T. Regan. A process algebra for timed systems. Technical Report 2/90, University of Sussex, Brighton, England, April 1990.

[14] C.A.R. Hoare. *Communicating Sequential Processes.* Prentice-Hall, London, 1985.

[15] P. Kanellakis and S.A. Smolka. CCS expressions, finite state processes, and three problems of equivalence. *Information and Computation*, 86(1):43–68, May 1990.

[16] R. Milner. *A Calculus of Communicating Systems*, volume 92 of *Lecture Notes in Computer Science.* Springer-Verlag, Berlin, 1980.

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

[18] F. Moller and C. Tofts. A temporal calculus of communicating systems. In J.C.M. Baeten and J.W. Klop, editors, *CONCUR '90*, volume 458 of *Lecture Notes in Computer Science*, pages 401–415, Amsterdam, August 1990. Springer-Verlag.

[19] R. Paige and R.E. Tarjan. Three partition refinement algorithms. *SIAM Journal of Computing*, 16(6):973–989, December 1987.

[20] D.M.R. Park. Concurrency and automata on infinite sequences. In *Proceedings of 5th G.I. Conference on Theoretical Computer Science*, volume 104 of *Lecture Notes in Computer Science*, pages 167–183. Springer-Verlag, 1980.

[21] G.D. Plotkin. A structural approach to operational semantics. Technical Report DAIMI-FN-19, Computer Science Department, Aarhus University, Denmark, 1981.

[22] D. Sangiorgi and R. Milner. The problem of 'weak bisimulation up to'. In R. Cleaveland, editor, *CONCUR '92*, volume 630 of *Lecture Notes in Computer Science*, pages 32–46, Stony Brook, New York, August 1992. Springer-Verlag.

[23] R. van Glabbeek, S.A. Smolka, B. Steffen, and C.M.N. Tofts. Reactive, generative and stratified models of probabilistic processes. In *Fifth Annual Symposium on Logic in Computer Science (LICS '90)*, pages 130–141, Philadelphia, June 1990. IEEE Computer Society Press.

[24] W. Yi. CCS + time = an interleaving model for real time systems. In Albert et al. [1], pages 217–228.

A Congruence Proofs

A.1 Temporal Strong Bisimulation

In this section, we present an outline of the proof that $\sim^+$ is a congruence. Since the semantics of all operators beside prefixing, parallel composition and timeout is the same as in PMC we obtain the compositionality relatively easy by adapting the results presented in [3] under consideration of the definition of visible initial action sets with respect to the scope of timed actions. Therefore, we concentrate on the more interesting cases.

Lemma A.1 *$P \sim^+ Q$ implies $P \,|\, R \sim^+ Q \,|\, R$ for all $P, Q, R \in \mathcal{P}$.*

Proof: According to the definition of $\sim^+$ it is sufficient to prove that

$$\mathcal{R} =_{\mathrm{df}} \{\langle P \,|\, R, Q \,|\, R\rangle \mid P \sim^+ Q\}$$

is a temporal strong bisimulation.

The case $P \,|\, R \xRightarrow{\alpha} S$ for some $\alpha \in \mathcal{A}$ and $S \in \mathcal{P}$ is the same as the corresponding case in CCS [17] and, therefore, we omit it here.

Let $P \,|\, R \xRightarrow{\sigma} S$ for some $\sigma \in \mathcal{T}$ and $S \in \mathcal{P}$. According to the only applicable semantic Rule tCom we know that $P \xRightarrow{\sigma} P'$ for some $P' \in \mathcal{P}$, $\mathbb{I}_\sigma(P) \cap \overline{\mathbb{I}}(R) = \emptyset$, $R \xRightarrow{\sigma} R'$ for some $R' \in \mathcal{P}$, $\mathbb{I}_\sigma(R) \cap \overline{\mathbb{I}}(P) = \emptyset$, and $S \equiv P' \,|\, R'$. Since $P \sim^+ Q$ there exists a process $Q' \in \mathcal{P}$ such that $Q \xRightarrow{\sigma} Q'$, $\mathbb{I}_\sigma(Q) \subseteq \mathbb{I}_\sigma(P)$, and $P' \sim^+ Q'$. Additionally, $P \sim^+ Q$ implies that $\mathbb{I}(P) = \mathbb{I}(Q)$. Therefore, we may conclude that $Q \,|\, R \xRightarrow{\sigma} Q' \,|\, R'$ by Rule tCom. Moreover, $\langle P', Q'\rangle \in \mathcal{R}$ holds, and we have finished the proof. □

Now, we deal with the timeout operator.

Lemma A.2 *$P \sim^+ Q$ and $R \sim^+ S$ imply $\lfloor P \rfloor \sigma(R) \sim^+ \lfloor Q \rfloor \sigma(S)$ for all processes $P, Q, R, S \in \mathcal{P}$ and all timed actions $\sigma \in \mathcal{T}$.*

Proof: Let $P, Q, R, S \in \mathcal{P}$ satisfying $P \sim^+ Q$ and $R \sim^+ S$. Moreover, let $\sigma \in \mathcal{T}$. We show that $\lfloor P \rfloor \sigma(R) \sim^+ \lfloor Q \rfloor \sigma(S)$.

Let $\lfloor P \rfloor \sigma(R) \xRightarrow{\alpha} P'$ for some $P' \in \mathcal{P}$. According to the only applicable semantic Rule TO of $\mathsf{TPL}^{\mathsf{mc}}$ we know that $P \xRightarrow{\alpha} P'$. Since $P \sim^+ Q$ holds, the existence of some $Q' \in \mathcal{P}$ such that $Q \xRightarrow{\alpha} Q'$ and $P' \sim^+ Q'$ is guaranteed. By Rule TO we may conclude that $\lfloor Q \rfloor \sigma(S) \xRightarrow{\alpha} Q'$.

Let $\lfloor P \rfloor \sigma(R) \xRightarrow{\sigma'} P'$ for some $P' \in \mathcal{P}$ where $\sigma' \neq \sigma$. Thus, $P \xRightarrow{\sigma'} P'$ by Rule tTO2. Since $P \sim^+ Q$ it follows that $Q \xRightarrow{\sigma'} Q'$, $\mathbb{I}_{\sigma'}(Q) \subseteq \mathbb{I}_{\sigma'}(P)$, and $P' \sim^+ Q'$ for some $Q' \in \mathcal{P}$. According to Rule tTO2 we conclude that $\lfloor Q \rfloor \sigma(S) \xRightarrow{\sigma'} Q'$. Moreover, we have $\mathbb{I}_{\sigma'}(\lfloor Q \rfloor \sigma(S)) \subseteq \mathbb{I}_{\sigma'}(\lfloor P \rfloor \sigma(R))$ because $\mathbb{I}_{\sigma'}(\lfloor Q \rfloor \sigma(S)) = \mathbb{I}_{\sigma'}(Q)$ and $\mathbb{I}_{\sigma'}(\lfloor P \rfloor \sigma(R)) = \mathbb{I}_{\sigma'}(P)$.

Finally, let $\lfloor P \rfloor \sigma(R) \xrightarrow{\sigma} P'$ for some $P' \in \mathcal{P}$. By Rule tTO1 we know that $P' \equiv R$ and $\tau \notin \mathrm{I}_\sigma(Q)$. Moreover, Proposition 2.2 guarantees that $P \xrightarrow{\sigma}$. Because $P \sim^+ Q$, also $Q \xrightarrow{\sigma}$ is satisfied. Thus, $\tau \notin \mathrm{I}_\sigma(Q)$ by our maximal progress assumption (cf. Proposition 2.3) and $\lfloor Q \rfloor \sigma(R) \xrightarrow{\sigma} R$. The observation $R \sim^+ R$ concludes this case. □

Also the prefixing of timed actions respects the compositionality of $\sim^+$. The compositionality of the ignore operator with respect to temporal strong bisimulation is trivial since $\mathbb{I}_\sigma(P \upharpoonright \sigma) = \emptyset$ for all processes $P \in \mathcal{P}$. However, the compositionality of recursion requires to introduce a notion of *temporal strong bisimulation up to*. This can be done according to the lines of CCS with respect to strong bisimulation (cf. [17]).

A.2 Temporal Weak Congruence

In this section, we show that $\underline{\approx}^+$ is the largest congruence contained in $\underline{\approx}$. We start off by proving that $\underline{\approx}^+$ is in fact a congruence. Most cases are standard and can be checked along the lines of [17]. Therefore, we restrict ourselves to the more interesting proof parts.

Lemma A.3 *$P \underline{\approx} Q$ implies $P \,|\, R \underline{\approx} Q \,|\, R$ for all $P, Q, R \in \mathcal{P}$.*

Proof: According to the definition of $\underline{\approx}$ it is sufficient to prove that

$$\mathcal{R} =_{\mathrm{df}} \{\langle P \,|\, R, Q \,|\, R\rangle \,|\, P \underline{\approx} Q\}$$

is a temporal weak bisimulation.

The case where $P \,|\, R \xrightarrow{\alpha} S$ for some $S \in \mathcal{P}$ and $\alpha \in \mathcal{A}$ is standard.

Consider the case $P \,|\, R \xrightarrow{\sigma} S$ for some $S \in \mathcal{P}$ and $\sigma \in \mathcal{T}$. By the only applicable Rule tCom we know that $P \xrightarrow{\sigma} P'$ for some $P' \in \mathcal{P}$, $\mathbb{I}_\sigma(P) \cap \overline{\mathbb{I}}(R) = \emptyset$, $R \xrightarrow{\sigma} R'$ for some $R' \in \mathcal{P}$, $\mathbb{I}_\sigma(R) \cap \overline{\mathbb{I}}(P) = \emptyset$, and $S \equiv P' \,|\, R'$. Since $P \underline{\approx} Q$ we know of the existence of a process $Q' \in \mathcal{P}$ such that $Q \overset{\sigma}{\underset{L,M}{\Longrightarrow}} Q'$ and $P' \underline{\approx} Q'$ where $L = \mathbb{I}_\sigma(P)$ and $M = \mathbb{I}(P)$. This means that $Q \overset{\epsilon}{\Longrightarrow} Q'' \xrightarrow{\sigma} Q''' \overset{\epsilon}{\Longrightarrow} Q'$, $\mathbb{I}_\sigma(Q'') \subseteq L$, and $\mathbb{I}(Q'') \subseteq M$ for some $Q'', Q''' \in \mathcal{P}$. First observe, that $(\mathbb{I}_\sigma(Q'') \cap \overline{\mathbb{I}}(R)) \subseteq (\mathbb{I}_\sigma(P) \cap \overline{\mathbb{I}}(R)) = \emptyset$ and $(\mathbb{I}_\sigma(R) \cap \overline{\mathbb{I}}(Q'')) \subseteq (\mathbb{I}_\sigma(R) \cap \overline{\mathbb{I}}(P)) = \emptyset$. Applying our semantic rules again we conclude that $Q \,|\, R \overset{\epsilon}{\Longrightarrow} Q'' \,|\, R \xrightarrow{\sigma} Q''' \,|\, R' \overset{\epsilon}{\Longrightarrow} Q' \,|\, R'$ since $\mathbb{I}(Q'' \,|\, R) = \mathbb{I}(Q'') \cup \mathbb{I}(R) \subseteq \mathbb{I}(P) \cup \mathbb{I}(R) = \mathbb{I}(P \,|\, R)$ and $\mathbb{I}_\sigma(Q'' \,|\, R) = \mathbb{I}_\sigma(Q'') \cup \mathbb{I}_\sigma(R) \subseteq \mathbb{I}_\sigma(P) \cup \mathbb{I}_\sigma(R) = \mathbb{I}_\sigma(P \,|\, R)$ holds. Obviously, we also have $\langle P' \,|\, R', Q' \,|\, R'\rangle \in \mathcal{R}$. □

Observe that in the proofs of the standard cases of the above lemma a τ-derivation is matched by at least one τ-transition. Moreover, $\mathcal{R}$ is defined symmetrically. Therefore, $\underline{\approx}^+$ is compositional with respect to the parallel operator, too.

In the following, we establish the compositionality of $\underline{\approx}^+$ with respect to the timeout operator.

Lemma A.4 *$P \underline{\approx}^+ Q$ and $R \underline{\approx} S$ imply $\lfloor P \rfloor \sigma(R) \underline{\approx}^+ \lfloor Q \rfloor \sigma(S)$ for all processes $P, Q, R, S \in \mathcal{P}$ and all timed actions $\sigma \in \mathcal{T}$.*

Proof: Let $P, Q, R, S \in \mathcal{P}$ satisfying $P \underline{\approx}^+ Q$ and $R \underline{\approx} S$. Moreover, let $\sigma \in \mathcal{T}$. We show that $\lfloor P \rfloor \sigma(R) \underline{\approx}^+ \lfloor Q \rfloor \sigma(S)$.

The case where $\lfloor P \rfloor \sigma(R) \overset{\alpha}{\Leftrightarrow} P'$ for some $\alpha \in \mathcal{A}$ and $P' \in \mathcal{P}$ is straightforward.

Therefore, we directly consider the non-standard case where $\lfloor P \rfloor \sigma(R) \overset{\sigma'}{\Leftrightarrow} P'$ for some $P' \in \mathcal{P}$ and $\sigma \neq \sigma'$. According to the only applicable Rule tTO2 we have $P \overset{\sigma'}{\Leftrightarrow} P'$. Since $P \underline{\approx}^+ Q$ there exists some $Q' \in \mathcal{P}$ such that $Q \overset{\sigma'}{\Leftrightarrow} \overset{\epsilon}{\Longrightarrow} Q'$, $\mathbb{I}_{\sigma'}(Q) \subseteq \mathbb{I}_{\sigma'}(P)$, $\mathbb{I}(Q) \subseteq \mathbb{I}(P)$, and $P' \underline{\approx} Q'$. Applying Rule tTO2 again, we conclude $\lfloor Q \rfloor \sigma(S) \overset{\sigma'}{\Leftrightarrow} \overset{\epsilon}{\Longrightarrow} Q'$. Moreover, the necessary inclusion conditions hold since $\mathbb{I}(\lfloor Q \rfloor \sigma(S)) = \mathbb{I}(Q) \subseteq \mathbb{I}(P) = \mathbb{I}(\lfloor P \rfloor \sigma(R))$ and $\mathbb{I}_{\sigma'}(\lfloor Q \rfloor \sigma(S)) = \mathbb{I}_{\sigma'}(Q) \subseteq \mathbb{I}_{\sigma'}(P) = \mathbb{I}_{\sigma'}(\lfloor P \rfloor \sigma(R))$. We also have $Q' \underline{\approx} Q'$ because $\underline{\approx}$ is an equivalence relation.

Finally, let $\lfloor P \rfloor \sigma(R) \overset{\sigma}{\Leftrightarrow} P'$ for some $P' \in \mathcal{P}$. By Rule tTO1 we know that $P' \equiv R$. Since $P \underline{\approx}^+ Q$ we conclude the existence of some $Q' \in \mathcal{P}$ such that $Q \overset{\sigma}{\Leftrightarrow} \overset{\epsilon}{\Longrightarrow} Q'$, $\mathbb{I}_{\sigma}(Q) \subseteq \mathbb{I}_{\sigma}(P)$, $\mathbb{I}(Q) \subseteq \mathbb{I}(P)$, and $P' \underline{\approx} Q'$. Because of Proposition 2.3 and Rule tTO1 we have $\lfloor Q \rfloor \sigma(S) \overset{\sigma}{\Leftrightarrow} S$. The required initial action set inclusions follow similarly to the case above. Additionally, we also have $P' \equiv R \underline{\approx} S$.

Because of symmetry reasons, we have finished the proof. □

In order to show that $\underline{\approx}^+$ is compositional with respect to recursion, we need to define a notion of *temporal weak bisimulation up to* $\underline{\approx}$ [22]. With this definition, the proof is completely standard (cf. [17]).

Definition A.5 (Temporal Weak Bisimulation up to $\underline{\approx}$)
A relation $\mathcal{R} \subseteq \mathcal{P} \times \mathcal{P}$ is a temporal weak bisimulation up to $\underline{\approx}$ *if for every $\langle P, Q \rangle \in \mathcal{R}$, $\alpha \in \mathcal{A}$, and $\sigma \in \mathcal{T}$ the following conditions hold.*

1. *$P \overset{\alpha}{\Leftrightarrow} P'$ implies $\exists Q'.\, Q \overset{\alpha}{\Longrightarrow} Q'$ and $P' \,\mathcal{R} \underline{\approx}\, Q'$.*
2. *$P \overset{\sigma}{\Leftrightarrow} P'$ implies $\exists Q'.\, Q \overset{\sigma}{\underset{L,M}{\Longrightarrow}} Q'$, $L = \mathbb{I}_{\sigma}(P)$, $M = \mathbb{I}(P)$, and $P' \,\mathcal{R} \underline{\approx}\, Q'$.*
3. *$Q \overset{\alpha}{\Leftrightarrow} Q'$ implies $\exists P'.\, P \overset{\alpha}{\Longrightarrow} P'$ and $P' \,\underline{\approx} \mathcal{R}\, Q'$.*
4. *$Q \overset{\sigma}{\Leftrightarrow} Q'$ implies $\exists P'.\, P \overset{\sigma}{\underset{L,M}{\Longrightarrow}} P'$, $L = \mathbb{I}_{\sigma}(Q)$, $M = \mathbb{I}(Q)$, and $P' \,\underline{\approx} \mathcal{R}\, Q'$.*

As expected, this notion satisfies the property that, if $\mathcal{R}$ is a *temporal weak bisimulation up to* $\underline{\approx}$, then $\mathcal{R} \subseteq \underline{\approx}$.

Now, we prove another property of $\underline{\approx}^+$ which turns out to be useful in the next section.

Proposition A.6 *The congruence $\underline{\approx}^+$ is the* largest *congruence contained in $\underline{\approx}$.*

Proof: Since the relation $\underline{\approx}^+$ is a congruence, it is sufficient to show that for all $\mathsf{TPL}^{\mathsf{mc}}$-contexts C and processes $P, Q \in \mathcal{P}$ satisfying $C[P] \underline{\approx} C[Q]$ we have $P \underline{\approx}^+ Q$. Moreover, it is sufficient to deal with the contexts $C_{\sigma}[X] =_{\mathrm{df}} \lfloor X + c.\mathbf{0} \rfloor \sigma(d.\mathbf{0})$ where $c, d \notin \mathcal{S}(P) \cup \mathcal{S}(Q)$ and $\sigma \in \mathcal{T}$.

Let $C_\sigma[P] \overset{\alpha}{\Leftrightarrow} P'$ for some $P' \in \mathcal{P}$, some $\alpha \in \mathcal{A}$, and some $\sigma \in \mathcal{T}$. Since $P \underline{\approx} Q$ there exists a process $Q' \in \mathcal{P}$ satisfying $C[Q] \overset{\hat{\alpha}}{\Longrightarrow} Q'$ and $P' \underline{\approx} Q'$. We know that $Q' \not\equiv C_\sigma[Q]$ because $P' \underline{\approx} Q'$ and P' is *not* capable of performing the distinguished c-transition. Therefore, the matching step is necessary, even if $\alpha = \tau$.

Now, let $C_\sigma[P] \overset{\sigma}{\Leftrightarrow} S$ for some $\sigma \in \mathcal{T}$. By Rule tTO1 we know that $\tau \notin \mathrm{I}_\sigma(P)$ and $S \equiv d.\mathbf{0}$. Because of the fact that $C_\sigma[P] \underline{\approx} C_\sigma[Q]$ we have $S \underline{\approx} T$ and $C_\sigma[Q] \underset{L,M}{\overset{\sigma}{\Longrightarrow}} T$ where $L = \mathbb{I}_\sigma(C_\sigma[P])$ and $M = \mathbb{I}(C_\sigma[P])$. Since d is a distinguished action we may conclude by Rule tTO1 that $T \equiv d.\mathbf{0}$, $C_\sigma[Q] \overset{\sigma}{\Leftrightarrow} d.\mathbf{0}$, and $\tau \notin \mathrm{I}_\sigma(Q)$, as desired.

Similarly, the symmetric properties hold, too. Thus, all conditions of Definition 5.6 are satisfied, and we obtain $P \underline{\approx}^+ Q$, as desired. □

B Proof of the Main Theorems

In this section, we proof Theorems 4.6 and 5.8 which state that $\sim^+$ is the *largest* congruence contained in $\sim_\times$ and $\underline{\approx}^+$ is the *largest* one contained in $\approx_\times$, respectively.

In both proofs, we use (parts of) the following fact from universal algebra.

Fact B.1 *Let X and Y be equivalence relations. Then the largest congruence X^+ in X exists. X^+ is characterized by $X^+ = \{\langle P, Q\rangle \mid \forall\, \mathsf{TPL}^{\mathsf{mc}}$-contexts $C.\, \langle C[P], C[Q]\rangle \in X\}$. Moreover, if $X^+ \subseteq Y \subseteq X$ then $X^+ = Y^+$.*

In the following, we construct contexts which include the summation operator over sorts. Since $\mathsf{TPL}^{\mathsf{mc}}$ just provides a binary summation operator, i.e. only finite summations can be expressed in $\mathsf{TPL}^{\mathsf{mc}}$, the following lemma is important to show the well-definedness of these contexts.

Lemma B.2 (Finite Sorts)
Let $P \in \mathcal{P}$ be a $\mathsf{TPL}^{\mathsf{mc}}$ process. Then the sort of P, i.e. the set of actions occurring in the transition system for P, is finite. We denote the sort of P by $\mathcal{S}(P)$.

This observation is an immediate consequence of the fact that process terms are finite, and relabelings f satisfy the condition $|\{\alpha \mid f(\alpha) \neq \alpha\}| < \infty$.

B.1 Proof of Theorem 4.6

By Theorem 4.3 we know already that the relation $\sim^+$ is a congruence, and we know by Fact B.1 that the largest congruence in $\sim_\times$ exists. Therefore, it remains to show that $P \sim^+ Q$ for some processes $P, Q \in \mathcal{P}$ whenever $C[P] \sim_\times C[Q]$ for all $\mathsf{TPL}^{\mathsf{mc}}$-contexts C. For this it suffices to consider the equivalence relation

$$\sim_{\mathrm{a}} =_{\mathrm{df}} \{\langle P, Q\rangle \mid C_{PQ}[P] \sim_\times C_{PQ}[Q]\} \ .$$

Here, using the abbreviation $S =_{\mathrm{df}} \mathcal{S}(P) \cup \mathcal{S}(Q)$, we define

$$C_{PQ}[X] =_{\mathrm{df}} X \,|\, H_{PQ}$$

and

$$H_{PQ} \overset{\mathrm{def}}{=} \sum_{\substack{L \subseteq \overline{S}, \\ \sigma \in \mathcal{T}}} \tau.(\lfloor (D_L \uparrow \sigma) + d_{\sigma,L}.\mathbf{0} \rfloor \sigma(H_{PQ})) \ .$$

Note that H_{PQ} is well-defined because of Lemma B.2 and the finiteness of $\mathcal{T}$. Moreover, the process D_L is defined as $\sum_{d \in L} d.\mathbf{0}$. The actions $d_{\sigma,L}$ are supposed to be 'fresh' actions, i.e. they are not in the sorts of the processes P and Q. The following proposition contains the necessary inclusion which has to be established.

Proposition B.3 *The inclusion $\sim_{\mathrm{a}} \subseteq \sim_{\times}$ holds.*

Proof: It is sufficient to show that $\sim_{\mathrm{a}}$ is a temporal strong bisimulation. Let $P, Q \in \mathcal{P}$ satisfying $P \sim_{\mathrm{a}} Q$, i.e. by the definition of $\sim_{\mathrm{a}}$ we have $C_{PQ}[P] \sim_{\times} C_{PQ}[Q]$. In the following, we consider two cases distinguishing if the process P performs a transition labeled with an action in $\mathcal{A}$ or in $\mathcal{T}$. This transitions of P lead to transitions of $C_{PQ}[P]$. According to the definition of $\sim_{\times}$, matching sequences have to exist which mimic each step by a corresponding transition. From these transitions, we may extract additional conditions which have to be satisfied according to the semantics of $\mathsf{TPL}^{\mathsf{mc}}$. Those conditions are sufficient to conclude that $\sim_{\mathrm{a}}$ is a temporal strong bisimulation.

Case 1 Let $P \overset{\alpha}{\Rightarrow} P'$ for some process $P' \in \mathcal{P}$ and some action $\alpha \in \mathcal{A}$. According to our operational semantics we have $C_{PQ}[P] \equiv P \,|\, H_{PQ} \overset{\alpha}{\Rightarrow} P' \,|\, H_{PQ} \equiv C_{PQ}[P']$. This transition can only be matched by a corresponding transition of the process Q, say $Q \overset{\alpha}{\Rightarrow} Q'$ for some process $Q' \in \mathcal{P}$. This is even true in the case $\alpha = \tau$ because the τ-successors of H_{PQ} have the distinguished actions $d_{\sigma,L}$ enabled. Therefore, we have $C_{PQ}[Q] \equiv Q \,|\, H_{PQ} \overset{\alpha}{\Rightarrow} Q' \,|\, H_{PQ} \equiv C_{PQ}[Q']$ and $C_{PQ}[P'] \sim_{\times} C_{PQ}[Q']$. Because $\mathcal{S}(P') \subseteq \mathcal{S}(P)$ and $\mathcal{S}(Q') \subseteq \mathcal{S}(Q)$, also $C_{P'Q'}[P'] \sim_{\times} C_{P'Q'}[Q']$ holds. Thus, $P' \sim_{\mathrm{a}} Q'$.

Case 2 Let $P \overset{\sigma}{\Rightarrow} P'$ for some process $P' \in \mathcal{P}$ and some timed action $\sigma \in \mathcal{T}$. As illustrated in Figure 3, we let $C_{PQ}[P]$ perform a τ-transition to $P \,|\, H_{\sigma,L}$, where

$$H_{\sigma,L} =_{\mathrm{df}} \lfloor (D_L \uparrow \sigma) + d_{\sigma,L}.\mathbf{0} \rfloor \sigma(H_{PQ})$$

and $L =_{\mathrm{df}} \{\overline{c} \,|\, c \in S \setminus \mathbb{I}_{\sigma}(P)\}$. Now, $P \,|\, H_{\sigma,L}$ can perform a σ-transition to $P' \,|\, H_{PQ}$ according to Rule tCom.

The process $C_{PQ}[Q]$ has to match the first step by a τ-transition to the process $Q \,|\, H_{\sigma,L}$ since only this process has the distinguished action $d_{\sigma,L}$ enabled.

Now, we take a closer look at the second step. We have to match a σ-transition. Therefore, Q has to perform a σ-transition to some process $Q' \in \mathcal{P}$ and the process $H_{\sigma,L}$ must perform its only

$$\begin{tikzcd}
P \mid & H_{PQ} \arrow[d, "\tau"] & \sim_{\times} & Q \mid & H_{PQ} \arrow[d, "\tau"] \\
P \arrow[d, "\sigma"] & \mid(\lfloor(D_L + d_{\sigma,L}.\mathbf{0}) \upharpoonright \sigma \rfloor \sigma(H_{PQ})) & \sim_{\times} & Q \arrow[d, "\sigma"] & \mid(\lfloor(D_L + d_{\sigma,L}.\mathbf{0}) \upharpoonright \sigma \rfloor \sigma(H_{PQ})) \\
P' \mid & H_{PQ} & \sim_{\times} & Q' \mid & H_{PQ}
\end{tikzcd}$$

Figure 3: Largest congruence proof of $\sim^+$ – illustration of Case 2

σ-transition to the state H_{PQ}, i.e. $Q \mid H_{\sigma,L} \overset{\sigma}{\Longrightarrow} Q' \mid H_{PQ} \equiv C_{PQ}[Q']$ and $C_{PQ}[P'] \sim_{\times} C_{PQ}[Q']$. According to Rule tCom, the condition $\mathbb{I}_\sigma(Q) \cap \overline{\mathbb{I}}(H_{\sigma,L}) = \emptyset$ has to be satisfied. Because of the choice of L, this implies $\mathbb{I}_\sigma(Q) \subseteq \mathbb{I}_\sigma(P)$. Since $\mathcal{S}(P') \subseteq \mathcal{S}(P)$ and $\mathcal{S}(Q') \subseteq \mathcal{S}(Q)$ it follows that $C_{P'Q'}[P'] \sim_{\times} C_{P'Q'}[Q']$, i.e. $P' \sim_{\mathrm{a}} Q'$, as desired.

□

B.2 Proof of Theorem 5.8

Here, we make a stronger use of Fact B.1. We choose $X = \approx_{\times}{}^+$ and $Y = \underline{\approx}$. The inclusion $\underline{\approx} \subseteq \approx_{\times}$ follows immediately from the definition of the naive and the temporal weak transition relation. In order to apply Fact B.1, we have to establish $\approx_{\times}{}^+ \subseteq \underline{\approx}$. This inclusion turns out to be difficult to show. Therefore, we define the equivalence relation

$$\underline{\approx}_{\mathrm{a}} =_{\mathrm{df}} \{\langle P, Q\rangle \mid C_{PQ}[P] \approx_{\times} C_{PQ}[Q]\} \ .$$

Here, abbreviating $\mathcal{S}(P) \cup \mathcal{S}(Q)$ by S, the process $C_{PQ}[X]$ represents $X \mid H_{PQ}$ where

$$H_{PQ} \overset{\mathrm{def}}{=} e.\mathbf{0} + \sum_{\substack{L,M \subseteq \overline{S}, \\ \sigma \in \mathcal{T}}} \tau.(\lfloor D_L + d_{\sigma,L,M}.\mathbf{0} + (D_M \upharpoonright \sigma) \rfloor \sigma(H_{PQ}))$$

The processes H_{PQ} are well-defined because of Lemma B.2 and the finiteness of the set $\mathcal{T}$, and D_L and D_M are defined by $\sum_{d \in L} d.\mathbf{0}$ and $\sum_{d \in M} d.\mathbf{0}$, respectively. The actions $d_{\sigma,L,M}$ are supposed to be 'fresh' actions, i.e. they are not in the sort of the processes P and Q. By Fact B.1, we may immediately conclude that $\approx_{\times}{}^+ \subseteq \underline{\approx}_{\mathrm{a}}$. The other necessary inclusion can be established by using the following proposition.

Proposition B.4 *The inclusion* $\underset{\approx}{\approx}_{\mathrm{a}} \subseteq \underset{\approx}{\approx}$ *holds.*

Proof: It is sufficient to show that $\underset{\approx}{\approx}_{\mathrm{a}}$ is a temporal weak bisimulation. Let $P, Q \in \mathcal{P}$ satisfying $P \underset{\approx}{\approx}_{\mathrm{a}} Q$.

Case 1 Let $P \overset{\alpha}{\Leftrightarrow} P'$ for some process $P' \in \mathcal{P}$ and some action $\alpha \in \mathcal{A}$. According to our operational semantics we may derive $C_{PQ}[P] \equiv P \,|\, H_{PQ} \overset{\alpha}{\Leftrightarrow} P' \,|\, H_{PQ} \equiv C_{PQ}[P']$. This transition can only be matched by a corresponding weak transition of the process Q, say $Q \overset{\hat{\alpha}}{\Longrightarrow}_{\times} Q'$ for some $Q' \in \mathcal{P}$, since only the process H_{PQ} has the distinguished action c enabled. Therefore, we have $C_{PQ}[Q] \equiv Q \,|\, H_{PQ} \overset{\hat{\alpha}}{\Longrightarrow}_{\times} Q' \,|\, H_{PQ} \equiv C_{PQ}[Q']$ and $C_{PQ}[P'] \approx_{\times} C_{PQ}[Q']$. Because $\mathcal{S}(P') \subseteq \mathcal{S}(P)$ and $\mathcal{S}(Q') \subseteq \mathcal{S}(Q)$, also $C_{P'Q'}[P'] \approx_{\times} C_{P'Q'}[Q']$ holds. Thus, $P' \underset{\approx}{\approx}_{\mathrm{a}} Q'$.

Case 2 Let $P \overset{\sigma}{\Leftrightarrow} P'$ for some process $P' \in \mathcal{P}$ and some timed action $\sigma \in \mathcal{T}$. As illustrated in Figure 4, we let $C_{PQ}[P]$ perform a τ-transition to the process $P \,|\, H_{\sigma,L,M}$, where

$$H_{\sigma,L,M} =_{\mathrm{df}} \lfloor D_L + d_{\sigma,L,M}.\mathbf{0} + (D_M \upharpoonright \sigma) \rfloor \sigma(H_{PQ})) \, ,$$

$L =_{\mathrm{df}} \{\overline{c} \,|\, c \in S \setminus \mathbb{I}(P)\}$, and $M =_{\mathrm{df}} \{\overline{c} \,|\, c \in S \setminus \mathbb{I}_{\sigma}(P)\} \setminus L$. Now, $P \,|\, H_{\sigma,L,M}$ can perform a σ-transition to $P' \,|\, H_{PQ}$ according to Rule tCom.

$$\begin{tikzcd}
P \,|\, H_{PQ} \arrow[d, "\tau"] & \approx_{\times} & Q \,|\, H_{PQ} \arrow[d, Rightarrow, "\epsilon", "\times"' near end] \\
P \,|\, H_{\sigma,L,M} \arrow[d, "\sigma"] & \approx_{\times} & \overline{Q} \,|\, H_{\sigma,L,M} \arrow[d, Rightarrow, "\sigma", "\times"' near end] \\
P' \,|\, H_{PQ} & \approx_{\times} & Q' \,|\, H_{PQ}
\end{tikzcd}$$

Figure 4: Largest congruence proof of $\underset{\approx}{\approx}^{+}$ – illustration of Case 2

Consider the first step. Since $C_{PQ}[P] \approx_{\times} C_{PQ}[P]$, we have $C_{PQ} \overset{\epsilon}{\Longrightarrow}_{\times} W$ for some $W \in \mathcal{P}$. We know that H_{PQ} has to perform a τ-transition to $H_{\sigma,L,M}$ since $d_{\sigma,L,M}$ is a distinguished action. However, Q may be able to perform some τ-transitions to some state $\overline{Q} \in \mathcal{P}$, i.e. $Q \overset{\epsilon}{\Longrightarrow}_{\times} \overline{Q}$ and $P' \,|\, H_{\sigma,L,M} \approx_{\times} \overline{Q} \,|\, H_{\sigma,L,M}$.

Now, we take a look at the more interesting second step. Since $P \,|\, H_{\sigma,L,M} \approx_{\times} \overline{Q} \,|\, H_{\sigma,L,M}$, we know that some $\overline{W}' \in \mathcal{P}$ exist such that $\overline{Q} \,|\, H_{\sigma,L,M} \overset{\sigma}{\Longrightarrow}_{\times} \overline{W}'$ and $C_{PQ}[P'] \approx_{\times} \overline{W}'$. According to our operational semantics $\overline{Q}$ and $H_{\sigma,L,M}$ have to perform a naive weak σ-transition. Since e is a distinguished action we know that $H_{\sigma,L,M} \overset{\sigma}{\Leftrightarrow} H_{PQ}$. Therefore, $W \equiv Q' \,|\, H_{PQ}$ for some process $Q' \in \mathcal{P}$ such that $\overline{Q} \overset{\sigma}{\Longrightarrow}_\times Q'$, i.e.

$$\exists s,t \in \mathbb{N}\, \forall 0 \leq i < s\, \forall 0 < j < t.\, \exists Q_i, Q_{s+j} \in \mathcal{P}.\; Q_0 \equiv \overline{Q}, Q_{s+t} \equiv Q'$$

such that

1. $Q_i \,|\, H_{\sigma,L,M} \overset{\tau}{\Leftrightarrow} Q_{i+1} \,|\, H_{\sigma,L,M}$,
2. $Q_s \,|\, H_{\sigma,L,M} \overset{\sigma}{\Leftrightarrow} Q_{s+1} \,|\, H_{PQ}$, and
3. $Q_{s+j} \,|\, H_{PQ} \overset{\tau}{\Leftrightarrow} Q_{s+j+1} \,|\, H_{PQ}$.

According to the Rule tCom the following conditions must be satisfied in order that the timed action $\sigma \in \mathcal{T}$ may occur.

1. $\mathbb{I}_\sigma(Q_s) \cap \overline{\mathbb{I}}(H_{\sigma,L,M}) = \emptyset$ which implies $\mathbb{I}_\sigma(Q_s) \subseteq \mathbb{I}_\sigma(P)$.
2. $\mathbb{I}_\sigma(H_{\sigma,L,M}) \cap \overline{\mathbb{I}}(Q_s) = \emptyset$ which implies $\mathbb{I}(Q_s) \subseteq \mathbb{I}(P)$.

We have shown that $Q \overset{\sigma}{\underset{L,M}{\Longrightarrow}} Q'$ according to the definition of the temporal weak transition relation. We also have $C_{P'Q'}[P'] \approx_\times C_{P'Q'}[Q']$, i.e. $P' \underline{\approx}_{\mathrm{a}} Q'$ since $C_{PQ}[P'] \approx_\times C_{PQ}[Q']$, $\mathcal{S}(P') \subseteq \mathcal{S}(P)$, and $\mathcal{S}(Q') \subseteq \mathcal{S}(Q)$. Therefore, the proof is finished. □

Now, we are able to put our proof parts together in order to obtain Theorem 5.8. Proposition A.6 states that $\underline{\approx}^+$ is the *largest* congruence contained in $\underline{\approx}$. Moreover, ${\approx_\times}^+$ is contained in $\underline{\approx}$ according to Proposition B.4 and the inclusion ${\approx_\times}^+ \subseteq \underline{\approx}_{\mathrm{a}}$. Therefore, we may conclude by Fact B.1 that $\underline{\approx}^+ = {\approx_\times}^+$, i.e. $\underline{\approx}^+$ is the largest congruence contained in $\approx_\times$. Figure 5 depicts the proof situation where an arrow from some relation R_1 to a relation R_2 means that $R_1 \subseteq R_2$.

$$\begin{tikzcd}
 & & \approx_\times \\
 & & \underline{\approx} \arrow[u] \\
 & \underline{\approx}_{\mathrm{a}} \arrow[ur] & \\
{\approx_\times}^+ \arrow[ur] \arrow[rr, leftrightarrow] & & \underline{\approx}^+ \arrow[uu]
\end{tikzcd}$$

Figure 5: Situation in the proof of Theorem 5.8

C Proof of the Logical Characterization of $\sim^{+}$

In this section, we prove Theorem 4.7. Most proof parts are similar to the corresponding ones presented in [17].

First, we define a characterization of temporal strong bisimulation for finite-branching transition systems over $\mathcal{A} \cup \mathcal{T}$. A transition system $\langle \mathcal{P}, \mathcal{A} \cup \mathcal{T}, \Leftrightarrow, P \rangle$ is called *finite-branching* if the set $\{P'' \mid P' \overset{\gamma}{\Leftrightarrow} P'', \gamma \in \mathcal{A} \cup \mathcal{T}\}$ is finite for all reachable states P' of the process P.

Definition C.1 *Let $\langle \mathcal{P}, \mathcal{A} \cup \mathcal{T}, \Leftrightarrow\!\!\rightarrow, P \rangle$ and $\langle \mathcal{P}, \mathcal{A} \cup \mathcal{T}, \Leftrightarrow\!\!\rightarrow, Q \rangle$ be finite-branching transition systems. We define ${\sim^{+}}_{0} =_{\mathrm{df}} \mathcal{P} \times \mathcal{P}$ and $P \,{\sim^{+}}_{k+1}\, Q$ for some $k \in \mathbb{N}$ if the following properties hold:*

1. *$P \overset{\alpha}{\Leftrightarrow} P'$ implies $\exists Q'.\, Q \overset{\alpha}{\Leftrightarrow} Q'$ and $P' \,{\sim^{+}}_{k}\, Q'$.*
2. *$P \overset{\sigma}{\Leftrightarrow} P'$ implies $\exists Q'.\, Q \overset{\sigma}{\Leftrightarrow} Q'$, $\mathbb{I}_{\sigma}(Q) \subseteq \mathbb{I}_{\sigma}(P)$, and $P' \,{\sim^{+}}_{k}\, Q'$.*
3. *$Q \overset{\alpha}{\Leftrightarrow} Q'$ implies $\exists P'.\, P \overset{\alpha}{\Leftrightarrow} P'$ and $P' \,{\sim^{+}}_{k}\, Q'$.*
4. *$Q \overset{\sigma}{\Leftrightarrow} Q'$ implies $\exists P'.\, P \overset{\sigma}{\Leftrightarrow} P'$, $\mathbb{I}_{\sigma}(P) \subseteq \mathbb{I}_{\sigma}(Q)$, and $P' \,{\sim^{+}}_{k}\, Q'$.*

The proof of the next proposition follows the lines in [17]. Note that for all processes in $\mathsf{TPL}^{\mathsf{mc}}$ the according transition systems are finite-branching.

Proposition C.2 *Let $P, Q \in \mathcal{P}$. We have $P \sim^{+} Q$ if and only if $P \,{\sim^{+}}_{k}\, Q$ for all $k \in \mathbb{N}$.*

Now we are able to prove Theorem 4.7. By Proposition C.2 it is sufficient to establish the following two lemmata.

Lemma C.3 *Let $P, Q \in \mathcal{P}$, $k \in \mathbb{N}$, and $\Phi \in \mathcal{F}$ such that $P \,{\sim^{+}}_{k}\, Q$ and $P \models \Phi$. Then $Q \models \Phi$ holds.*

Proof: We prove the lemma by induction on k where the induction step is divided into several cases according to the structure of Φ. The only non-standard case is $\Phi = \langle \sigma, L \rangle \Psi$ for $\sigma \in \mathcal{T}$ and $L \subseteq \mathcal{A} \setminus \{\tau\}$. By the definition of $\models$ we conclude the existence of a process $P' \in \mathcal{P}$ such that $P \overset{\sigma}{\Leftrightarrow} P'$, $\mathbb{I}_{\sigma}(P) \subseteq L$, and $P' \models \Psi$. Since $P \,{\sim^{+}}_{k}\, Q$ we also know of the existence of some $Q' \in \mathcal{P}$ such that $Q \overset{\sigma}{\Leftrightarrow} Q'$, $\mathbb{I}_{\sigma}(Q) \subseteq \mathbb{I}_{\sigma}(P)$, and $P' \,{\sim^{+}}_{k-1}\, Q'$. Thus, $\mathbb{I}_{\sigma}(Q) \subseteq L$ and, by the induction hypothesis, that $Q' \models \Psi$. Therefore, $Q \models \langle \sigma, L \rangle \Psi$, as desired. □

Lemma C.4 *Let $P, Q \in \mathcal{P}$ and $k \in \mathbb{N}$ such that $P \,{\not\sim^{+}}_{k}\, Q$ holds. It exists a formula $\Phi \in \mathcal{F}$ such that $P \models \Phi$ but $Q \not\models \Phi$.*

Proof: We prove this lemma by induction on k. The induction base is trivial since the premise $P \not\succsim^{+}{}_{0}\, Q$ does not hold. Now, let $k > 0$ and $P \not\succsim^{+}{}_{k}\, Q$. We have to find a formula $\Phi \in \mathcal{F}$ such that $P \models \Phi$ and $Q \not\models \Phi$. Since $P \not\succsim^{+}{}_{k}\, Q$ we have $P \overset{\gamma}{\Leftrightarrow} P'$ for some $\gamma \in \mathcal{A} \cup \mathcal{T}$ and $P' \in \mathcal{P}$ which cannot be matched by a step of Q. The case where $\gamma \in \mathcal{A}$ follows the standard lines. Now, let $\gamma = \sigma \in \mathcal{T}$, i.e. we know that whenever $Q \overset{\sigma}{\Leftrightarrow} Q'$ and $\mathrm{I\!I}_\sigma(Q) \subseteq \mathrm{I\!I}_\sigma(P)$ then $P' \not\succsim^{+}{}_{k-1}\, Q'$. Let $\{Q' \,|\, Q \overset{\sigma}{\Leftrightarrow} Q' \text{ and } \mathrm{I\!I}_\sigma(Q) \subseteq \mathrm{I\!I}_\sigma(P)\} = \{Q_i \,|\, i \in I\}$ for some index set I. Note that I is a finite set, because the transition system for Q is finite-branching. By induction hypothesis we conclude the existence of formulae Ψ_i, for $i \in I$, such that $P' \models \Psi_i$ and $Q_i \not\models \Psi_i$. Now, define $\Phi =_{\mathrm{df}} \langle \sigma, L \rangle \bigwedge_{i \in I} \Psi_i$ where $L =_{\mathrm{df}} \mathrm{I\!I}_\sigma(P)$. Because of the choice of L, it is easy to see that $P \models \Phi$. Since no σ-derivative of Q with $\mathrm{I\!I}_\sigma(Q) \subseteq L$ satisfies $\bigwedge_{i \in I} \Psi_i$, we have $Q \not\models \Phi$. □