Observational Congruence in a Stochastic Timed Calculus with Maximal Progress

Holger Hermanns Markus Lohrey

October 1997 IMMD VII-7/97

Technischer Bericht

Institut für
Mathematische Maschinen
und Datenverarbeitung
der
Friedrich-Alexander-Universität
Erlangen-Nürnberg

Lehrstuhl für Informatik VII
(Rechnerarchitektur
und Verkehrstheorie)
Prof. Dr.-Ing. U. Herzog

IMMD VII
Martensstr. 3
D-91058 Erlangen

Telefon
+49-9131/85-7041

Observational Congruence in a Stochastic Timed Calculus with Maximal Progress

Holger Hermanns
Universität Erlangen
IMMD VII
91058 Erlangen, Germany
hrherman@informatik.uni-erlangen.de

Markus Lohrey
Technische Universität Dresden
Institut für Softwaretechnik I
01062 Dresden, Germany
lohrey@orchid.inf.tu-dresden.de

Abstract

During the last decade, CCS has been extended in different directions, among them priority and real time. One of the most satisfactory results for CCS is Milner's complete proof system for observational congruence [31]. Observational congruence is fair in the sense that it is possible to escape divergence, reflected by the axiom $\mathrm{rec}X.(\tau.X + P) = \mathrm{rec}X.\tau.P$. In this paper we discuss observational congruence in the context of a simple stochastic timed CCS with maximal progress. This property implies that observational congruence becomes unfair, i.e. it is not always possible to escape divergence. This problem also arises in calculi with priority. Therefore, completeness results for such calculi modulo observational congruence have been unknown until now. We obtain a complete proof system by replacing the above axiom by a set of axioms allowing to escape divergence by means of a silent alternative. This treatment can be profitably adapted to other calculi.

1 Introduction

One of the outstanding results for CCS [30] is Milner's complete proof system for regular expressions modulo observational congruence [31]. The task of proving completeness is divided into three parts. First, only guarded recursive expressions are considered where guards are visible actions. This means that divergent expressions (that perform an infinite number of silent steps) are excluded. The core of this part is to show that two congruent expressions satisfy the same set of recursive equations. The second important property is that every set of recursive defining equations has a unique solution. Divergent expressions cannot be handled in this way, since, for instance, the recursive equation $X = \tau.X$ has infinitely many solutions. Therefore completeness is obtained by adding further axioms. In particular, a divergent expression can be equated to a non-divergent expressions by applying essentially the axiom

$$\mathrm{rec}X.(\tau.X + P) = \mathrm{rec}X.\tau.P.$$

Walker [41] studies divergence in the context of CCS and observational congruence. The possibility of escaping from divergence is known as fairness. Koomen [29] was the first to define a fair abstraction rule (KFAR) similar to the one above.

Fairness is mostly regarded as a desirable feature. Therefore, the issue of obtaining fairness has been extensively studied in the literature. Baeten *et al.* [6] discusses fairness in the context of failure semantics. In [7], Bergstra *et al.* introduce a weaker version of fair abstraction (WFAR) that allows to escape divergence only if a silent alternative exists. Fair testing equivalences have been developed in [33, 9].

In recent years, CCS has been extended in different directions, among them priority and real time. Different prioritised process algebras have been developed [5, 11, 16, 34, 10, 38, 13]. Investigations of observational congruence in the presence of priority have been restricted to finite, i.e. recursion free processes [34]. In that approach priority is nicely reflected by the following axiom, where $\underline{a}$ has a lower priority than b:

$$\tau.P + \underline{a}.Q = \tau.P.$$

A variety of timed process algebras has also been proposed [40, 21, 32, 4, 43, 36, 2, 12]. A thorough overview of the basic ingredients is given in [35]. Complete proof systems for regular expressions have been obtained for some of these calculi [23, 1, 15]. One of the typical features of CCS based timed process algebras is a notion of maximal progress, also called minimal delay or τ-urgency. This property says that a system cannot wait if it has something internal to do. It is characterised by the following law, where $delay(T)$ usually stands for a fixed time delay of length T:

$$\tau.P + delay(T).Q = \tau.P.$$

The concepts of priority and maximal progress arose at different corners in concurrency theory. Weak bisimulation semantics incorporating one of these ingredients, however, have a common feature: Divergence implies unfairness. In particular, the above KFAR axiom is not sound[1]. Thus, KFAR cannot be used to equate divergent expressions to non-divergent expressions. So, completeness is not attainable in this way. But the equation $X = \tau.X$ still has infinitely many solutions. As a consequence, to the best of our knowledge, no complete proof system for observational congruence for regular CCS including either priority or maximal progress has been given until now.

In recent years also stochastic timed calculi have emerged, where delays are not fixed but given by continuous probability distribution functions. This fits neatly to interleaving semantics, if only exponential distributions are considered. Then $delay(T)$ stands for a delay, say t, with mean duration T and distribution $Prob(delay \leq t) = 1 - e^{-\lambda t}$, where the parameter λ is the reciprocal value of T. We mention TIPP of Götz *et al.* [20], Hillston's PEPA [26], and Bernardo&Gorrieri's EMPA [8] as representatives of this approach. Their

[1] In the timed case, a counterexample is $\mathrm{rec}X.(\tau.X + delay(T).Q)$. KFAR equates this expression to $\mathrm{rec}X.\tau.delay(T).Q$ while maximal progress leads to $\mathrm{rec}X.\tau.X$. Since the latter (using KFAR) can be equated to termination, both expressions obviously describe distinct behaviours.

unifying feature is that their semantics can be transformed into a continuous time Markov chain, a stochastic model widely used for performance evaluation purposes, see e.g. [39]. The issue of weak bisimulation and observational congruence in stochastic timed calculi has been addressed in [24].

The contribution of this paper is threefold. Concerning ordinary CCS we present a slight modification of Milner's observational congruence that permits to escape divergence *only* if a silent alternative exists. This is exactly the effect of WFAR in the style of [7]. Our notion of observational congruence is truly contained in Milner's observational congruence. This compares favourably to the treatment of divergence in [41] that is incomparable with the original definition.

We exploit this feature in order to develop a sound and complete proof system for observational congruence in a *stochastic timed* extension of CCS with maximal progress. This is achieved by replacing KFAR by a set of axioms allowing to escape divergence by means of a silent alternative.

As a side result we obtain a sound and complete proof system for observational congruence with WFAR on CCS. Since our treatment of divergence is orthogonal to the stochastic timing aspects we highlight that this treatment can be adapted to other calculi with either maximal progress or priority for which similar completeness results have been unknown until now.

The stochastic timed calculi of [20, 26, 8] all attach exponentially distributed delays to actions. Their subtle differences are mainly based on different interpretations of the delay of synchronised actions. We deviate from these calculi and split delays and actions into two orthogonal parts. This separation rules out any ambiguity in the timing of synchronisation. It has been pointed out e.g. in [32] and [35] that such a separation is conceptionally favourable for timed process algebras.

An extension of our basic stochastic timed calculus has been developed to study performance properties of parallel and distributed systems. In [25] it is applied to specify a CSMA/CD protocol stack. The whole system turns out to have 37136 reachable states. It can be proven to be observational congruent to a system with 411 states which can be directly transformed into a Markov Chain to study temporal properties of the protocol stack. That case study has indeed initiated our study of equational properties of observational congruence. With the results presented in this paper we have a complete proof system for establishing observational congruence of such systems on the language level.

The paper is organised as follows. Section 2 briefly describes the calculus and defines congruence relations on it. Section 3 presents a set of equational laws that are sound for observational congruence. The proof of completeness requires some degree of detail, it is sketched in Section 4. Section 5 discusses the relation to WFAR, ordinary CCS and extensions thereof. Section 6 contains some concluding remarks.

2 A Simple Stochastic Timed Calculus

In this section we introduce the basic definitions and properties of the calculus we investigate. It includes a distinct type of prefixing to specify exponentially distributed delays. Instead of a broad introduction into their theory we briefly summarise some important properties enjoyed by exponential distributions. Details can be found in various textbooks, e.g. [14].

(A) An exponential distribution $Prob\{delay \leq t\} = 1 - e^{-\lambda t}$ is characterised by a single parameter λ, a positive real value, usually referred to as the *rate* of the distribution.

(B) Exponential distributions possess the so called *Markov property*. The remaining delay after some time t_0 has elapsed is a random variable with the same distribution as the whole delay: $Prob\{delay \leq t + t_0 \mid delay > t_0\} = Prob\{delay \leq t\}$.

(C) The class of exponential distributions is closed under minimum, which is exponentially distributed with the sum of the rates: $Prob\{\min(delay_1, delay_2) \leq t\} = 1 - e^{-(\lambda_1+\lambda_2)t}$ if $delay_1$ ($delay_2$, respectively) is exponentially distributed with rate λ_1 (λ_2).

While property (A) allows a compact syntactic representation of delays in our calculus, the Markov property (B) is important to employ an interleaving semantics. It ensures that distributions of delays do not have to be recalculated after some (causally independent) delay has elapsed. Therefore, the usual expansion law can be applied straightforwardly. This substantially simplifies the definition of parallel composition. Property (C) is decisive for our interpretation of the choice operator in the presence of delays: If all alternatives of a choice involve an exponentially distributed delay the decision is taken as soon as the first of these delays elapses. This finishing delay determines the subsequent behaviour. The time instant of this decision is obviously given by the minimum of distributions. As a consequence of property (C), the overall delay until the decision is taken is exponentially distributed.

After these preliminaries we introduce the calculus we investigate. We assume a set of process variables *Var*, a set of actions *Act* containing a distinguished silent action τ and let $I\!R$ denote the set of positive reals. We use λ, μ, ... to range over $I\!R$ and a, b, ... for elements of *Act*. The basic calculus does not contain parallel composition, we defer the discussion of this operator to Section 5.

Definition 2.1 Let $\lambda \in I\!R$, $a \in Act$ and $X \in Var$. We define the language STC as the set of expressions given by the following grammar.

$$\mathcal{E} ::= 0 \quad | \quad (\lambda).\mathcal{E} \quad | \quad a.\mathcal{E} \quad | \quad \mathcal{E} + \mathcal{E} \quad | \quad X \quad | \quad \mathrm{rec}X.\mathcal{E}$$

The expression $(\lambda).P$ describes a behaviour that will delay its subsequent behaviour P for an exponentially distributed time with a mean duration of $1/\lambda$. The meaning of the other operators is as usual. We use E, F, ... to range over expressions of STC. With the usual notion of free variables and free and closed expressions we let STP denote the set of closed expressions, ranged over by P, Q, ... , called processes. $Var(E)$ denotes the set of free variables of E.

A variable X is strongly guarded in an expression E if every occurrence of X in E is strongly guarded, i.e. guarded by a prefix "$a.$" (with $a \neq \tau$) or "$(\lambda).$'. Weak guardedness is the same, but includes the prefix "$\tau.$". A variable is said to be fully unguarded if it is not weakly guarded. An expression E is said to be strongly (weakly) guarded, if, for every subexpression of the form $\mathrm{rec}X.E'$, the variable X is strongly (weakly) guarded in E'.

Definition 2.2 We define the set of *well-defined* expressions $\mathsf{STC}_\downarrow$ as the smallest subset of STC such that

- $Var \subseteq \mathsf{STC}_\downarrow$ and $0 \in \mathsf{STC}_\downarrow$,
- if $E \in \mathsf{STC}_\downarrow$ and $F \in \mathsf{STC}_\downarrow$ then $E + F \in \mathsf{STC}_\downarrow$,
- if $E\{\mathrm{rec}X.E/X\} \in \mathsf{STC}_\downarrow$ then $\mathrm{rec}X.E \in \mathsf{STC}_\downarrow$.

The complementary set containing all *ill-defined* processes, will be denoted $\mathsf{STC}_\uparrow$. We write $E\downarrow$ ($E\uparrow$) if $E \in \mathsf{STC}_\downarrow$ ($E \in \mathsf{STC}_\uparrow$).

The semantics of each expression is defined as an equivalence class of transition systems. We define a transition system for each expression below by means of structural operational rules. We define two transition relations, one for actions and one to represent the impact of time. We have taken the liberty to shift the complexity of our calculus from the definition of the transition system towards the definition of equivalences. As a consequence, the operational rules are very simple, whereas the definition of a suitable equivalence becomes more challenging.

Definition 2.3 The *action transition* relation $\longrightarrow\ \subset \mathsf{STC} \times Act \times \mathsf{STC}$ and the *timed transition* relation $\dashrightarrow\ \subset \mathsf{STC} \times I\!R \times \{l, r\}^* \times \mathsf{STC}$ are the least relations given by the rules in Figure 1.

In the rules for timed transitions we use words over $\{l, r\}$ to generate multiple transitions for expressions like $(\lambda).0 + (\lambda).0$ by encoding their different proof trees. This is known from probabilistic calculi like PCCS [19], ε denotes the empty word. The need to represent multiplicities stems from our interpretation of choice in the presence of delays. It is assumed that the decision is taken as soon as the first of the delays elapses. Property (C) implies that this delay is again governed by an exponential distribution given by the sum of the rates. In other words, the behaviour of $(\lambda).0 + (\lambda).0$ is the same as that of $(2\lambda).0$. Thus idempotence of choice does not hold. Our notion of bisimilarity is therefore similar to probabilistic bisimilarity as introduced by Larsen&Skou [27] regarding timed transitions. The definition requires to calculate the sum of all rates leading from a single expression into a set of expression (where the latter set will be an equivalence class of expressions).

$$(a^I)\ \frac{}{a.E \xrightarrow{a} E} \qquad (\lambda^M)\ \frac{}{(\lambda).E \overset{\lambda,\varepsilon}{\dashrightarrow} E}$$

$$(+_l^I)\ \frac{E \xrightarrow{a} E'}{E+F \xrightarrow{a} E'} \qquad (+_l^M)\ \frac{E \overset{\lambda,w}{\dashrightarrow} E'}{E+F \overset{\lambda,lw}{\dashrightarrow} E'}$$

$$(+_r^I)\ \frac{F \xrightarrow{a} F'}{E+F \xrightarrow{a} F'} \qquad (+_r^M)\ \frac{F \overset{\lambda,w}{\dashrightarrow} F'}{E+F \overset{\lambda,rw}{\dashrightarrow} F'}$$

$$(\mathrm{rec}^I)\ \frac{E\{\mathrm{rec}X.E/X\} \xrightarrow{a} E'}{\mathrm{rec}X.E \xrightarrow{a} E'} \qquad (\mathrm{rec}^M)\ \frac{E\{\mathrm{rec}X.E/X\} \overset{\lambda,w}{\dashrightarrow} E'}{\mathrm{rec}X.E \overset{\lambda,w}{\dashrightarrow} E'}$$

Figure 1: Operational semantic rules for $\mathsf{STC}^{\perp}$

Definition 2.4 Let $C \subseteq \mathsf{STC}$. We define the cumulative rate function $\gamma : \mathsf{STC} \times 2^{\mathsf{STC}} \longrightarrow I\!R$ as follows

$$\gamma(E, C) = \sum_{w \in \{l,r\}^*} \{\lambda \mid \exists F \in C : E \overset{\lambda,w}{\dashrightarrow} F\}$$

The interrelation of timed and action transitions resulting, for instance, from $(\lambda).P + \tau.Q$ is not evident from the operational rules. From a stochastic perspective, the silent action may happen *instantaneously* because nothing may prevent or delay it. On the other hand, property (A) implies that the probability that an exponentially distributed delay finishes instantaneously, is zero ($Prob\{delay \leq 0\} = 0$). We therefore employ the *maximal progress assumption*. We assume that a process that may perform a silent action is not allowed to let time pass. The above process is therefore equal to $\tau.Q$. Since this equality is not evident from the operational rules it will become part of the definition of strong and weak bisimilarity. For this purpose, we distinguish the elements of STC according to their ability to perform a silent action. We use $E\not\surd$ to denote *unstable* expressions satisfying $\exists F : E \xrightarrow{\tau} F$ and $E\surd$ to denote the converse. Expressions with the latter property will be called *stable* expressions in the sequel. Intuitively, only stable expressions may spend time whereas unstable expressions follow the maximal progress assumption. Note that $\surd$ can be equally defined by means of a syntactic predicate on STC. For expressions E that are stable as well as well-defined we use the shorthand notation $E\surd\!\downarrow$.

We are now ready to introduce strong and weak bisimilarity on STC. As usual we define them for closed expressions, and afterwards lift them to STC. The set of equivalence classes of a given equivalence relation $\mathcal{B}$ on a set STC is denoted $\mathsf{STC}/\mathcal{B}$. $[E]_{\mathcal{B}}$ denotes the equivalence class of $\mathcal{B}$ containing E.

Definition 2.5 An equivalence relation $\mathcal{B}$ on STP is a strong bisimulation iff $P \;\mathcal{B}\; Q$ implies for all $a \in Act$

1. $P \xrightarrow{a} P'$ implies $Q \xrightarrow{a} Q'$ for some Q' with $P' \;\mathcal{B}\; Q'$,
2. $P\surd\!\downarrow$ implies that $Q\surd\!\downarrow$ and that $\gamma(P, C) = \gamma(Q, C)$ for all $C \in \mathsf{STP}/\mathcal{B}$.

Two processes P and Q are strongly bisimilar (written $P{\sim}Q$) if they are contained in some strong bisimulation.

In this definition, maximal progress is realized because the stochastic timing behaviour (evaluated by means of γ) is irrelevant for unstable expressions. Furthermore we do not compare the timing behaviour of ill-defined processes. The reason is best explained by means of an example. An ill-defined process like $\mathrm{rec}X.(X + (\lambda).0)$ may possess an infinitely branching transition system (for each $n \in I\!N_0$ we have $\mathrm{rec}X.(X + (\lambda).0) \overset{\lambda, l^n r}{\dashrightarrow} 0$). Our restriction to well-defined expressions thus avoids the need to calculate and compare infinite sums of rates.

Timed versions of bisimilarity (e.g. [32, 43]) usually require to cumulate subsequent time intervals. This is sometimes called *time additivity*. In our calculus, time additivity is not possible. The reason is that sequences of exponentially exponentially distributed delays are not exponentially distributed, since the class of exponential distributions is *not* closed under convolution. (There is no λ satisfying $Prob\{delay_1 + delay_2 \leq t\} = 1 - e^{\lambda t}$ if $delay_1$ and $delay_2$ are exponentially distributed.) In other words, it is impossible to replace a sequence of timed transitions by a single timed transition without affecting the probability distribution of the total delay. We thus demand that timed transitions have to be bisimulated in the strong sense, even for weak bisimilarity (in contrast to action transitions). We let $\overset{a}{\Longrightarrow}$ and $\overset{\widehat{a}}{\Longrightarrow}$ abbreviate $\xrightarrow{\tau}{}^{*} \xrightarrow{a} \xrightarrow{\tau}{}^{*}$ except if $a = \tau$. In this case, $\overset{\tau}{\Longrightarrow}$ denotes $\xrightarrow{\tau}{}^{+}$ and $\overset{\widehat{\tau}}{\Longrightarrow}$ denotes $\xrightarrow{\tau}{}^{*}$. For a set of expressions C we define C^τ as the set of expressions that may silently evolve into an element of C, i.e. $C^\tau = \{E \mid \exists F \in C : E \overset{\widehat{\tau}}{\Longrightarrow} F\}$.

Definition 2.6 An equivalence relation $\mathcal{B}$ on STP is a weak bisimulation iff $P \;\mathcal{B}\; Q$ implies for all $a \in Act$

1. $P \overset{\widehat{a}}{\Longrightarrow} P'$ implies $Q \overset{\widehat{a}}{\Longrightarrow} Q'$ for some Q' with $P' \;\mathcal{B}\; Q'$,
2. $P \overset{\widehat{\tau}}{\Longrightarrow} P'$ and $P'\surd\!\downarrow$ imply $Q \overset{\widehat{\tau}}{\Longrightarrow} Q'$ for some $Q'\surd\!\downarrow$ such that $\gamma(P', C^\tau) = \gamma(Q', C^\tau)$ for all $C \in \mathsf{STP}/\mathcal{B}$.

Two processes P and Q are weakly bisimilar (written $P{\approx}Q$) if they are contained in some weak bisimulation.

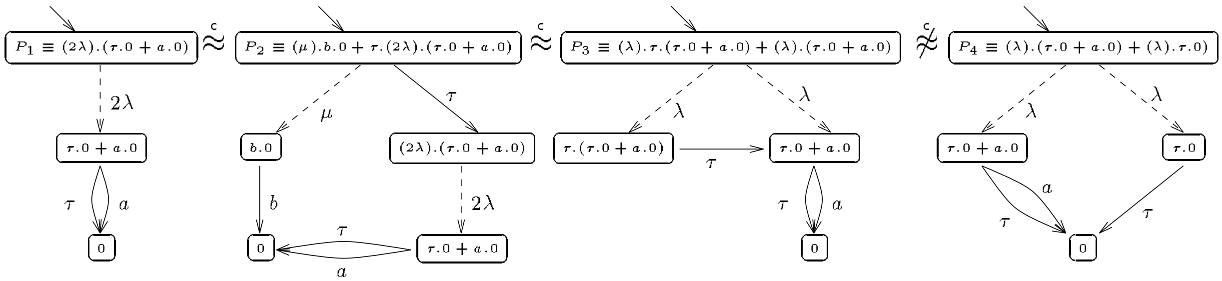


Figure 2: Some characteristic examples for weak bisimilarity.

It can be shown that $\approx$ ($\sim$, respectively) is a weak (strong) bisimulation. We illustrate the distinguishing power of $\approx$ by means of some examples, depicted in Figure 2. (We have used $\equiv$ to denote syntactic identity.) The first two processes, P_1 and P_2, are equivalent because P_2 is unstable (thus the μ-branch is irrelevant) but may silently evolve to a stable process that is identical (thus equivalent) to P_1. The process P_3 is equivalent to the former two, because $\gamma(P_1, ([0]_\approx)^\tau) = 2\lambda = \gamma(P_3, ([0]_\approx)^\tau)$ and $\gamma(P_1, ([\tau.0 + a.0]_\approx)^\tau) = 2\lambda = \gamma(P_3, ([\tau.0 + a.0]_\approx)^\tau)$ (all other values of γ are 0 in either case). In contrast, $\gamma(P_4, ([\tau.0 + a.0]_\approx)^\tau) = \lambda$ whence we have that P_4 is not weakly bisimilar to the former three processes.

The shape of this last example sheds some interesting light on our definition. Assume, for the moment, that λ is just an action like all the others. Then, P_3 and P_4 would be equated under the usual notion of weak bisimilarity while they would *not* under *branching* bisimilarity. Branching bisimilarity has been introduced by van Glabbeek&Weijland [18]. Here, however, weak bisimilarity already distinguishes the two, because multiplicities of timed transitions are relevant. (That is the reason why $\gamma(P_1, ([0]_\approx)^\tau) = 2\lambda = \gamma(P_4, ([0]_\approx)^\tau)$ but $\gamma(P_1, ([\tau.0 + a.0]_\approx)^\tau) \neq \gamma(P_4, ([\tau.0 + a.0]_\approx)^\tau)$.) In general, it is possible to reformulate weak bisimilarity such that silent steps following a timed transition are treated as in branching bisimilarity. This is particularly expressed in the following lemma, where the equivalence class C has replaced C^τ.

Lemma 2.7 An equivalence relation $\mathcal{B}$ on STP is a weak bisimulation iff $P\ \mathcal{B}\ Q$ implies for all $a \in Act$

1. $P \xrightarrow{a} P'$ implies $Q \stackrel{\widehat{a}}{\Longrightarrow} Q'$ for some Q' with $P'\ \mathcal{B}\ Q'$,
2. $P\surd\!\!\downarrow$ implies $Q \stackrel{\widehat{\tau}}{\Longrightarrow} Q'$ for some $Q'\surd\!\!\downarrow$ such that $\gamma(P, C) = \gamma(Q', C)$ for all $C \in \mathsf{STP}/\mathcal{B}$.

Proof: Condition (2) of Definition 2.6 is an immediate consequence of the second condition of this lemma since each C^τ is a union of equivalence classes of $\mathcal{B}$. The converse direction is shown by an induction on the number of equivalence classes subsumed by C^τ. Interchangeability of the respective first conditions is straightforward. $\square$

We shall frequently use this reformulation in the sequel. Unsurprisingly, $\approx$ is not substitutive with respect to choice. We therefore proceed as usual and define the (provably) coarsest congruence contained in $\approx$.

Definition 2.8 P and Q are observational congruent, written $P \overset{c}{\approx} Q$, iff for all $a \in Act$ and all $C \in \mathsf{STP}/\approx$:

1. $P \overset{a}{\longrightarrow} P'$ implies $Q \overset{a}{\Longrightarrow} Q'$ for some Q' with $P' \approx Q'$,
2. $Q \overset{a}{\longrightarrow} Q'$ implies $P \overset{a}{\Longrightarrow} P'$ for some P' with $P' \approx Q'$,
3. $P\surd\!\downarrow$ (or $Q\surd\!\downarrow$) implies $\gamma(P, C) = \gamma(Q, C)$
4. $P\surd\!\downarrow$ iff $Q\surd\!\downarrow$.

Definition 2.9 Let $\mathcal{R}$ be a relation on $\mathsf{STP} \times \mathsf{STP}$. We extend it to $\mathsf{STC} \times \mathsf{STC}$ as follows. Let E, $F \in \mathsf{STC}$. Then $E \;\mathcal{R}\; F$ iff $\forall P_1, \ldots, P_n \in \mathsf{STP} : E\{\vec{P}/\vec{X}\} \;\mathcal{R}\; F\{\vec{P}/\vec{X}\}$, where $\vec{X}$ denotes the vector of occurring free variables and $\{\vec{E}/\vec{X}\}$ denotes the simultaneous substitution of each X_i by E_i.

It can be shown that $\approx \;\supset\; \overset{c}{\approx} \;\supset\; \sim$. In addition, strong bisimilarity and observational congruence are compositional relations indeed.

Theorem 1 $\overset{c}{\approx}$ is a congruence with respect to the operators of STC.

Proof: See Appendix A. □

3 Axiomatisation

In this section we develop a set of equational laws that is sound and complete with respect to $\overset{c}{\approx}$. To achieve completeness is by far not straightforward, due to the presence of maximal progress. Divergent expressions, performing an infinite number of silent steps (e.g. $\mathrm{rec}X.\tau.X + (\lambda).0$), will be our main concern. In ordinary CCS the KFAR law $\mathrm{rec}X.\tau.X + E = \mathrm{rec}X.\tau.E$ is responsible to remove such infinite sequences. This law is not sound in our calculus. To illustrate this phenomenon suppose $\mathrm{rec}X.(\tau.X + (\lambda).0) \overset{c}{\approx} \mathrm{rec}X.(\tau.(\lambda).0)$. This implies $\mathrm{rec}X.(\tau.X + (\lambda).0) \approx (\lambda).0$. But, since $(\lambda).0\surd\!\downarrow$ there must be some $P\surd\!\downarrow$ with $\mathrm{rec}X.(\tau.X + (\lambda).0) \overset{\hat{\tau}}{\Longrightarrow} P$ which is not the case. Hence, we are forced to treat such loops of silent actions in a different way. We make them explicit by means of a distinguished symbol $\perp$ indicating ill-defined expressions. We equate divergent and ill-defined expressions. This is inspired by [41], but divergence (and ill-definedness) can be abstracted away if a silent computation is possible. For this purpose, we introduce a particular axiom ($\perp$):

$$\perp + \tau.E = \tau.E.$$

The symbol $\perp$ is not part of the language STC we are aiming to axiomatise. It will however be an essential part of the laws. For instance, in order to equate the expressions $\text{rec}X.(\tau.X+\tau.0)$ and $\tau.0$ the symbol $\perp$ appears (and vanishes again) inside the proof. We therefore define an extended language $\text{STC}^{\perp}$ as follows:

Definition 3.1 Let $\lambda \in I\!R$, $a \in Act$ and $X \in Var$. We define the language STC as the set of expressions given by the following grammar.

$$\mathcal{E} ::= \; 0 \quad | \quad \perp \quad | \quad (\lambda).\mathcal{E} \quad | \quad a.\mathcal{E} \quad | \quad \mathcal{E}+\mathcal{E} \quad | \quad X \quad | \quad \text{rec}X.\mathcal{E}.$$

All definitions introduced in Section 2 can be equally defined for this langage, in particular observational congruence, according to Definition 2.8, we denote this extended observational congruence by $\overset{c}{\approx}^{\perp}$. Also the properties stated in Section 2 remain completely valid for this extended language. The reason is twofold. First, no transitions are derivable for $\perp$ by means of the operational rules in Figure 1. Furthermore, $\perp$ is ill-defined according to (the redefinition of) Definition 2.2, it is not contained in the inductively defined set $\text{STC}^{\perp}_{\downarrow}$, hence $\perp\uparrow$.

The language STC is a subset of $\text{STC}^{\perp}$. The following lemma justifies that a proof system for $\overset{c}{\approx}^{\perp}$ can equally be used as a proof system for $\overset{c}{\approx}$, since both relations coincide on STC.

Lemma 3.2 For $E, F \in \text{STC}$, $E \overset{c}{\approx} F$ if and only if $E \overset{c}{\approx}^{\perp} F$.

We are now ready to introduce a proof system for $\overset{c}{\approx}^{\perp}$ on $\text{STC}^{\perp}$ (and thus for $\overset{c}{\approx}$ on STC). Figure 3 lists relevant axioms grouped into different sets. We omit the usual rules for structural congruence. The axioms of $\mathcal{A} \cup \mathcal{A}^{\text{rec}} \cup \mathcal{A}^{I}$ are standard laws forming a complete proof system of observational congruence for strongly guarded regular CCS [31]. Our axiomatisation is based on this system, but with a slight modification. We require to replace idempotence $\mathcal{A}^{I}$ by a set of laws $\mathcal{A}^{I^*}$. This refinement[2] is needed because of the presence of stochastic time [24]. Delay rate quantities have to be cumulated according to property (C) in order to represent the stochastic timing behaviour of expressions like $(\lambda).E + (\lambda).E$.

As we will see in Section 4 the axiom system $\widehat{\mathcal{A}} = \mathcal{A} \cup \mathcal{A}^{\text{rec}} \cup \mathcal{A}^{I^*} \cup \mathcal{A}^{\lambda} \cup \mathcal{A}^{\perp}$ is complete for $\text{STC}^{\perp}$ modulo observational congruence. The system $\mathcal{A}^{\lambda}$ is a collection of laws that cover the impact of stochastic time in $\text{STC}^{\perp}$. Law $(\tau 4)$ is an obvious adaption of $(\tau 1)$ while law $(I5)$ axiomatises property (C) (and is the reason why (I) is invalidated in general). The laws $(MP1)$ and $(MP2)$ express maximal progress: No time will be spent if a silent (possibly diverging) computation is possible.

The most interesting aspect of our proof system is the treatment of divergence and ill-definedness reflected in $\mathcal{A}^{\perp}$. Law $(\perp)$ is the key to escape ill-definedness by means of a silent alternative. Law (rec4) states that fully unguardedness is ill-defined. The last two laws for recursion explicitly handle divergent expressions that may perform an infinite

[2]Note, however, that $\mathcal{A} \cup \mathcal{A}^{\text{rec}} \cup \{(I1)\}$ gives rise to a complete proof system of observational congruence for strongly guarded regular CCS.

$(B1)$	$E+0$	$=$	E	$(\tau 1)$	$a.\tau.E$	$=$	$a.E$
$(B2)$	$E+F$	$=$	$F+E$	$(\tau 2)$	$E+\tau.E$	$=$	$\tau.E$
$(B3)$	$(E+F)+G$	$=$	$E+(F+G)$	$(\tau 3)$	$a.(E+\tau.F)+a.F$	$=$	$a.(E+\tau.F)$

Axiom system $\mathcal{A}$

(rec1)	$\mathrm{rec}X.E \;=\; \mathrm{rec}Y.(E\{Y/X\})$ provided that Y is not free in $\mathrm{rec}X.E$.
(rec2)	$\mathrm{rec}X.E \;=\; E\{\mathrm{rec}X.E/X\}$
(rec3)	$F = E\{F/X\}$ implies $F = \mathrm{rec}X.E$ provided that X is strongly guarded in E.

Axiom system $\mathcal{A}^{\mathrm{rec}}$

$$(I) \quad E+E \;=\; E$$

Axiom system $\mathcal{A}^{I}$

$(I1)$	$a.E+a.E$	$=$	$a.E$	$(I3)$	$E+E+\perp$	$=$	$E+\perp$
$(I2)$	$E+E+\tau.F$	$=$	$E+\tau.F$	$(I4)$	$\perp+\perp$	$=$	$\perp$

Axiom system $\mathcal{A}^{I^*}$

$(\tau 4)$	$(\lambda).\tau.E$	$=$	$(\lambda).E$	$(MP1)$	$(\lambda).E+\tau.F$	$=$	$\tau.F$
$(I5)$	$(\lambda).E+(\mu).E$	$=$	$(\lambda+\mu).E$	$(MP2)$	$(\lambda).E+\perp$	$=$	$\perp$

Axiom system $\mathcal{A}^{\lambda}$

$(\perp)$	$\perp+\tau.E$	$=$	$\tau.E$
(rec4)	$\mathrm{rec}X.(X+E)$	$=$	$\mathrm{rec}X.(\perp+E)$
(rec5)	$\mathrm{rec}X.(\tau.X+E)$	$=$	$\mathrm{rec}X(\tau.(\perp+E))$
(rec6)	$\mathrm{rec}X.(\tau.(\sum_{i=1}^{n} X+E)+F)$	$=$	$\mathrm{rec}X.(\tau.X+E+F)$
	provided that X is weakly guarded in E.		

Axiom system $\mathcal{A}^{\perp}$

Figure 3: Axioms for observational congruence.

number of silent steps. Law (rec5) replaces Milner's KFAR axiom, it basically equates divergence and ill-definedness for loops of length 1. Law (rec6) reduces the length of loops of silent steps such that they can eventually be handled by (rec5). The laws (rec5) and (rec6) are essential in order to handle weakly guarded expressions that are not strongly guarded (cf. Theorem 4).

It is worth to point out that the fair abstraction rule of unstable divergence (WFAR) of Bergstra *et al.* [7] is valid in the presence of maximal progress while KFAR is not sound.

A WFAR axiom can be formulated as follows:

$$\text{rec}X.(\tau.X + \tau.E + F) = \text{rec}X.(\tau.(\tau.E + F)),$$

and can be derived by means of law (rec5) and ($\perp$), i.e.

$$\text{rec}X.(\tau.X + \tau.E + F) = \text{rec}X.(\tau.(\perp + \tau.E + F)) = \text{rec}X.(\tau.(\tau.E + F)).$$

This derivation is indeed a simple example where the symbol $\perp$ appears and vanishes inside the proof. We shall write $\widehat{\mathcal{A}} \vdash E = F$ when $E = F$ may be proved from $\widehat{\mathcal{A}}$. We conclude this section by stating that $\widehat{\mathcal{A}}$ is indeed sound with respect to observational congruence on $\mathsf{STC}^{\perp}$.

Theorem 2 For $E, F \in \mathsf{STC}^{\perp}$ it holds that $\quad \widehat{\mathcal{A}} \vdash E = F \quad$ implies $\quad E \overset{c}{\approx}^{\perp} F$.

Proof: Routine, except for the rec laws. Detailed proofs for these laws are contained in Appendix B. □

4 Completeness

In this section we will address the question whether our set of laws is complete, i.e. enough to allow the deduction all semantic equalities. We closely follow the lines of Milner and use mutually recursive systems of defining equations to capture the impact of rec. We refer to the explanations in [31] concerning (guarded and saturated) standard equation systems (SES).

Definition 4.1 Let $\mathcal{W} = \{W_1, \ldots, W_m\}$ and $\mathcal{X} = \{X_1, \ldots, X_n\}$ be two disjoint sets of variables.

1. An equation set (ES) with free variables $\mathcal{W}$ and formal variables $\mathcal{X}$ is a set $S = \{X_i = F_i \mid 1 \leq i \leq n\}$ of equations such that $Var(F_i) \subseteq \mathcal{W} \cup \mathcal{X}$ and $F_i \in \mathsf{STC}^{\perp}$ $(1 \leq i \leq n)$. In addition, for all $i, j \in \{1, \ldots, n\}$ the variable X_i is weakly guarded in F_j.

2. A standard equation set (SES) with free variables $\mathcal{W}$ and formal variables $\mathcal{X}$ is an equation set $S = \{X_i = F_i \mid 1 \leq i \leq n\}$ such that $F_i \in \mathsf{STC}^{\perp}$ for $1 \leq i \leq n$ is of the form
$$F_i \equiv \sum_{j=1}^{r(i)} a_{i,j}.X_{f(i,j)} + \sum_{k=1}^{s(i)} (\lambda_{i,k}).X_{g(i,k)} + \sum_{l=1}^{t(i)} W_{h(i,l)} + \sum_{m=0}^{u_i} \perp .$$
An empty sum denotes 0.

3. Let $S = \{X_i = F_i \mid 1 \leq i \leq n\}$ be a ES with formal variables $\mathcal{X}$. An expression A provably satisfies S if there are expressions $A_i \in \mathsf{STC}^{\perp}$ $(i \in \{1, \ldots, n\})$ such that $A \in \{A_1, \ldots, A_n\}$ and
$$\widehat{\mathcal{A}} \vdash A_i = F_i\{\vec{A}/\vec{X}\}.$$

Definition 4.2 Let $S = \{X_i = F_i \mid 1 \leq i \leq n\}$ be a fixed ES with free variables $\mathcal{W} = \{W_1, \ldots, W_m\}$ and $W \in \mathcal{W}$, $a \in Act$. We define

1. $X_i \xrightarrow{a}_S X_j$ iff $F_i \xrightarrow{a} X_j$.
2. $X_i \rhd_S W$ iff there is some fully unguarded occurrence of W in F_i.
3. S is strongly guarded iff $\xrightarrow{\tau}_S^+$ is irreflexive.

Definition 4.3 An SES $S = \{X_i = F_i \mid 1 \leq i \leq n\}$ with free variables $\mathcal{W}$ and formal variables $\mathcal{X}$ is saturated iff for all $X_i, X_j \in \mathcal{X}$ and all $W \in \mathcal{W}$ it holds that

1. $X_i \xrightarrow{\tau}_S^* \xrightarrow{a}_S \xrightarrow{\tau}_S^* X_j$ implies $X_i \xrightarrow{a}_S X_j$, and
2. $X_i \xrightarrow{\tau}_S^* \rhd_S W$ implies $X_i \rhd_S W$.

Lemma 4.4 (Milner) For each strongly guarded $E \in \mathsf{STC}^\perp$ there is a guarded SES in the free variables of E that E provably satisfies.

Lemma 4.5 (Milner) If $E \in \mathsf{STC}^\perp$ provably satisfies a guarded SES then there is a guarded and saturated SES that E provably satisfies.

Lemma 4.6 (Milner) If $E, F \in \mathsf{STC}^\perp$ satisfy a single guarded and saturated SES in the free variables of E and F then $\widehat{\mathcal{A}} \vdash E = F$.

These lemmas are easily shown by a straightforward adaption of the proof of [31]. Now, the main effort is to bridge the gap between Lemma 4.5 and Lemma 4.6. To this end we have to verify that two separate SES, each satisfied by some expression, can be merged into a single SES if both expressions are observational congruent. Verifying this is a lot more involved than the usual proofs owed to the presence of stochastic timing and maximal progress. We therefore sketch the proof in some detail.

Theorem 3 Let $A, B \in \mathsf{STC}^\perp$ and $A \overset{c}{\approx}^\perp B$. Furthermore let A (B, respectively) provably satisfy the guarded, saturated SES $S_1 = \{X_i = F_i \mid 1 \leq i \leq n\}$ ($S_2 = \{Y_j = G_j \mid 1 \leq j \leq m\}$). Then there is a guarded SES S, that both, A and B provably satisfy.

Proof: (Sketch) Let $F_i \equiv \sum_{k_1=1}^{r_1(i)} (\lambda_{i,k_1}).X_{f_1(i,k_1)} + \sum_{l_1=1}^{s_1(i)} a_{i,l_1}.X_{g_1(i,l_1)} + \sum_{m_1=1}^{t_1(i)} W_{h_1(i,m_1)} + \sum_{n_1=1}^{u_1(i)} \perp$, and $G_j \equiv \sum_{k_2=1}^{r_2(j)} (\mu_{j,k_2}).Y_{f_2(j,k_2)} + \sum_{l_2=1}^{s_2(j)} b_{j,l_2}.Y_{g_2(j,l_2)} + \sum_{m_2=1}^{t_2(j)} W_{h_2(j,m_2)} + \sum_{n_2=1}^{u_2(j)} \perp$.

Because of law $(I4)$ we can assume that $u_1(i), u_2(j) \in \{0, 1\}$. By assumption, there are some expressions $A_i \in \mathsf{STC}^\perp$ ($i \in \{1, \ldots, n\}$) and $B_j \in \mathsf{STC}^\perp$ ($j \in \{1, \ldots, m\}$) such that $\widehat{\mathcal{A}} \vdash A_i = F_i\{\vec{A}/\vec{X}\}$, $\widehat{\mathcal{A}} \vdash B_j = G_j\{\vec{B}/\vec{Y}\}$, and (w.l.o.g.) $A_1 \equiv A \wedge B_1 \equiv B$. We use the following abbreviations.

- $I = \{(i,j) \mid 1 \leq i \leq n \ \wedge \ 1 \leq j \leq m \ \wedge \ A_i \approx^{\perp} B_j\}$,
- $J_{i,j} = \{(k_1,k_2) \in \{1,\ldots,r_1(i)\} \times \{1,\ldots,r_2(j)\} \mid (f_1(i,k_1), f_2(j,k_2)) \in I\}$,
- $K_{i,j} = \{(l_1,l_2) \in \{1,\ldots,s_1(i)\} \times \{1,\ldots,s_2(j)\} \mid a_{i,l_1} = b_{j,l_2} \ \wedge \ (g_1(i,l_1), g_2(j,l_2)) \in I\}$.

Since $A \overset{c}{\approx}^{\perp} B$ we have $(1,1) \in I$. In the sequel we use $X_i \in \mathcal{M}$ (respectively $Y_j \in \mathcal{M}$) to denote that $F_i \in \mathcal{M}$ ($G_j \in \mathcal{M}$) if $\mathcal{M}$ is an arbitrary subset of $\mathsf{STC}^{\perp}$. For arbitrary sets M, N, $O \subseteq M \times N$ let $\pi^{(1)}(O)$ (respectively $\pi^{(2)}(O)$) denote the projections on M (N), i.e. $\pi^{(1)}(O) = \{m \in M \mid \exists n \in N \ : \ (m,n) \in O\}$.

With this notation we are able to state the following properties that are of central importance for the proof of Theorem 3.

> Let $(i,j) \in I$, i.e. $A_i \approx^{\perp} B_j$. This implies $F_i\{\vec{A}/\vec{X}\} \approx^{\perp} G_j\{\vec{B}/\vec{Y}\}$. Since both S_1 and S_2 are saturated and strongly guarded the following properties hold [3] for each $C \in \mathsf{STC}^{\perp}/\approx^{\perp}$ and each $a \in Act$.
>
> (i) $X_i \xrightarrow{a}_{S_1} X_k$ implies $\exists l\, (Y_j \xrightarrow{a}_{S_2} Y_l \ \wedge \ (k,l) \in I) \ \vee \ (a = \tau \ \wedge \ (k,j) \in I)$,
>
> (ii) $Y_j \xrightarrow{b}_{S_2} Y_l$ implies $\exists k\, (X_i \xrightarrow{b}_{S_1} X_k \ \wedge \ (k,l) \in I) \ \vee \ (b = \tau \ \wedge \ (i,l) \in I)$,
>
> (iii) $X_i \surd\!\downarrow$ implies either $Y_j \not\surd$ or $(Y_j \surd\!\downarrow \ \wedge \ \gamma(F_i\{\vec{A}/\vec{X}\}, C) = \gamma(G_j\{\vec{B}/\vec{Y}\}, C))$,
>
> (iv) $Y_j \surd\!\downarrow$ implies either $X_i \not\surd$ or $(X_i \surd\!\downarrow \ \wedge \ \gamma(F_i\{\vec{A}/\vec{X}\}, C) = \gamma(G_j\{\vec{B}/\vec{Y}\}, C))$,
>
> (v) $\{W_{h_1(i,1)}, \ldots, W_{h_1(i,t_1(i))}\} = \{W_{h_2(j,1)}, \ldots, W_{h_2(j,t_2(j))}\}$. In addition, if $X_i \surd\!\downarrow$ and $Y_j \surd\!\downarrow$ then $\{\!|W_{h_1(i,1)}, \ldots, W_{h_1(i,t_1(i))}|\!\} = \{\!|W_{h_2(j,1)}, \ldots, W_{h_2(j,t_2(j))}|\!\}$.

The proof of these properties requires a characterisation of $\approx^{\perp}$ on open expressions. This characterisation is developed im Lemma C.1.

Property (i) implies that for each $l_1 \in \{1,\ldots,s_1(i)\}$ there is some $l_2 \in \{1,\ldots,s_2(j)\}$ such that

$$(a_{i,l_1} = b_{j,l_2} \ \wedge \ (g_1(i,l_1), g_2(j,l_2)) \in I) \ \vee \ (a_{i,l_1} = \tau \ \wedge \ (g_1(i,l_1), j) \in I), \tag{1}$$

Using the above notation this disjunction implies that if $l_1 \notin \pi^{(1)}(K_{i,j})$ then $a_{i,l_1} = \tau$ and $(g_1(i,l_1), j) \in I$. Analogously, property (ii) implies that if $l_2 \notin \pi^{(2)}(K_{i,j})$ then $b_{j,l_2} = \tau$ and $(i, g_2(j,l_2)) \in I$. By means of a characterisation of $\overset{c}{\approx}^{\perp}$ on open expressions, similar to the one mentioned above, our assumption $A_1 \equiv A \overset{c}{\approx}^{\perp} B \equiv B_1$ can now be used to derive (via $F_1\{\vec{A}/\vec{X}\} \overset{c}{\approx}^{\perp} G_1\{\vec{B}/\vec{Y}\}$) that for $(i,j) = (1,1)$ the first alternative of the disjunction in (1) is fulfilled. In other words,

$$\pi^{(1)}(K_{1,1}) = \{1,\ldots,s_1(1)\} \ \ \wedge \ \ \pi^{(2)}(K_{1,1}) = \{1,\ldots,s_2(1)\}. \tag{2}$$

In addition to $(i,j) \in I$, let us now assume $X_i \surd\!\downarrow$ and $Y_j \surd\!\downarrow$. Property (iii) (or (iv)) implies

$$\forall C \in \mathsf{STC}^{\perp}/\approx^{\perp} \ : \ \gamma(F_i\{\vec{A}/\vec{X}\}, C) = \gamma(G_j\{\vec{B}/\vec{Y}\}, C).$$

[3] We use $\{\!|$ and $|\!\}$ and to delimit a multiset.

Let $(k_1, k_2) \in J_{i,j}$.Then, since $(k_1, u) \in J_{i,j}$ iff $B_{f_2(j,u)} \approx^{\perp} A_{f_1(i,k_1)} \approx^{\perp} B_{f_2(j,k_2)}$, we have

$$\sum_{\substack{u=1 \\ (k_1,u)\in J_{i,j}}}^{r_2(j)} \mu_{j,u} = \gamma(G_j\{\vec{B}/\vec{Y}\}, [B_{f_2(j,k_2)}]_{\approx^{\perp}}) = \gamma(F_i\{\vec{A}/\vec{X}\}, [A_{f_1(i,k_1)}]_{\approx^{\perp}}) = \sum_{\substack{u=1 \\ (u,k_2)\in J_{i,j}}}^{r_1(i)} \lambda_{i,u}.$$

We abbreviate this sum with γ_{k_1,k_2} (though this suggests a dependence from both, k_1 and k_2 that obviously is not there). We can now create a standard equation set $S = \{Z_{i,j} = H_{i,j} \mid (i,j) \in I\}$ with new formal variables $\{Z_{i,j} \mid (i,j) \in I\}$ that serves our purposes. Let

$$\begin{aligned} H_{i,j} \equiv & \sum_{(l_1,l_2)\in K_{i,j}} a_{i,l_1}.Z_{g_1(i,l_1),g_2(j,l_2)} + \sum_{l_1\notin\pi^{(1)}(K_{i,j})} \tau.Z_{g_1(i,l_1),j} + \sum_{l_2\notin\pi^{(2)}(K_{i,j})} \tau.Z_{i,g_2(j,l_2)} \\ & + \begin{cases} \displaystyle\sum_{(k_1,k_2)\in J_{i,j}} \left(\frac{\lambda_{i,k_1}\cdot\mu_{j,k_2}}{\gamma_{k_1,k_2}}\right).Z_{f_1(i,k_1),f_2(j,k_2)} & \text{if } X_i\surd\!\downarrow \text{ and } Y_j\surd\!\downarrow \\ 0 & \text{else} \end{cases} \\ & + \left\{\begin{array}{ll} \displaystyle\sum_{m_1=1}^{t_1(i)} W_{h_1(i,m_1)} & \text{if } X_i\surd\!\downarrow \\ \displaystyle\sum_{m_2=1}^{t_2(j)} W_{h_2(j,m_2)} & \text{else} \end{array}\right\} + \begin{cases} \perp & \text{if } X_i\uparrow \text{ or } Y_j\uparrow \\ 0 & \text{else.} \end{cases} \end{aligned}$$

Our claim is that A provably satisfies the SES S (where A will be equated with $Z_{1,1}$). The proof that B provably satisfies S is completely symmetric. In order to show the former we define expressions $C_{i,j}$ ($(i,j) \in I$) as follows:

$$C_{i,j} \equiv \begin{cases} A_i & \text{if } \{1,\ldots,s_2(j)\} = \pi^{(2)}(K_{i,j}) \\ \tau.A_i & \text{if } \{1,\ldots,s_2(j)\} \neq \pi^{(2)}(K_{i,j}) \end{cases}$$

First, observe that (2) implies $C_{1,1} \equiv A_1 \equiv A$. We proceed with our proof by constructing the expression $H_{i,j}\{\vec{C}/\vec{Z}\}$. Besides of variables $W_{h_1(i,m_1)}$ and $\perp$ summands of the form $a.A_i$, $a.\tau.A_i$, $(\lambda).A_i$ and $(\lambda).\tau.A_i$ may occur in this expression. Because of law $(\tau 1)$ and $(\tau 2)$ we have

$$\begin{aligned} \widehat{\mathcal{A}} \vdash H_{i,j}\{\vec{C}/\vec{Z}\} = & \sum_{(l_1,l_2)\in K_{i,j}} a_{i,l_1}.A_{g_1(i,l_1)} + \sum_{l_1\notin\pi^{(1)}(K_{i,j})} \tau.A_{g_1(i,l_1)} + \sum_{l_2\notin\pi^{(2)}(K_{i,j})} \tau.A_i \\ & + \begin{cases} \displaystyle\sum_{(k_1,k_2)\in J_{i,j}} \left(\frac{\lambda_{i,k_1}\cdot\mu_{j,k_2}}{\gamma_{k_1,k_2}}\right).A_{f_1(i,k_1)} & \text{if } X_i\surd\!\downarrow \text{ and } Y_j\surd\!\downarrow \\ 0 & \text{else} \end{cases} \end{aligned}$$

$$+\begin{Bmatrix} \sum_{m_1=1}^{t_1(i)} W_{h_1(i,m_1)} & \text{if } X_i\surd\downarrow \\ \sum_{m_2=1}^{t_2(j)} W_{h_2(j,m_2)} & \text{else} \end{Bmatrix} + \begin{cases} \perp & \text{if } X_i\uparrow \text{ or } Y_j\uparrow \\ 0 & \text{else.} \end{cases}$$

We now aim to further simplify the sums occurring in the above expression. Concerning the sum $\sum_{(l_1,l_2)\in K_{i,j}} a_{i,l_1}.A_{g_1(i,l_1)} + \sum_{l_1\notin\pi^{(1)}(K_{i,j})} \tau.A_{g_1(i,l_1)}$ we can use, as derived above, that $l_1 \notin \pi^{(1)}(K_{i,j})$ implies $\tau = a_{i,l_1}$ to obtain $\sum_{(l_1,l_2)\in K_{i,j}} a_{i,l_1}.A_{g_1(i,l_1)} + \sum_{l_1\notin\pi^{(1)}(K_{i,j})} a_{i,l_1}.A_{g_1(i,l_1)}$. Since every summand $a_{i,l_1}.A_{g_1(i,l_1)}$ ($l_1 \in \{1,\ldots,s_1(i)\}$) occurs at least once in this sum we transform it, with the help of law $(I1)$, to $\sum_{l_1=1}^{s_1(i)} a_{i,l_1}.A_{g_1(i,l_1)}$.

Assuming $X_i\surd\downarrow$ and $Y_j\surd\downarrow$ we can transform the sum of delay prefixes, using law $(I5)$,

$$\sum_{(k_1,k_2)\in J_{i,j}} \left(\frac{\lambda_{i,k_1}\cdot\mu_{j,k_2}}{\gamma_{k_1,k_2}}\right).A_{f_1(i,k_1)} = \sum_{k_1=1}^{r_1(i)} \left(\sum_{\substack{k_2=1 \\ (k_1,k_2)\in J_{i,j}}}^{r_2(j)} \frac{\lambda_{i,k_1}\cdot\mu_{j,k_2}}{\gamma_{k_1,k_2}} \right).A_{f_1(i,k_1)}$$

The sums of rates appearing inside this expression can be simplified as follows.

$$\sum_{\substack{k_2=1 \\ (k_1,k_2)\in J_{i,j}}}^{r_2(j)} \frac{\lambda_{i,k_1}\cdot\mu_{j,k_2}}{\gamma_{k_1,k_2}} = \lambda_{i,k_1}\cdot \sum_{\substack{k_2=1 \\ (k_1,k_2)\in J_{i,j}}}^{r_2(j)} \frac{\mu_{j,k_2}}{\sum_{\substack{u=1 \\ (k_1,u)\in J_{i,j}}}^{r_2(j)} \mu_{j,u}} = \lambda_{i,k_1}\cdot \frac{\sum_{\substack{k_2=1 \\ (k_1,k_2)\in J_{i,j}}}^{r_2(j)} \mu_{j,k_2}}{\sum_{\substack{u=1 \\ (k_1,u)\in J_{i,j}}}^{r_2(j)} \mu_{j,u}} = \lambda_{i,k_1}$$

In other words, we can equate $\sum_{(k_1,k_2)\in J_{i,j}} \left(\frac{\lambda_{i,k_1}\cdot\mu_{j,k_2}}{\gamma_{k_1,k_2}}\right).A_{f_1(i,k_1)}$ and $\sum_{k_1=1}^{r_1(i)} (\lambda_{i,k_1}).A_{f_1(i,k_1)}$.

Finally, the sum of free variables reduces to $\sum_{m_1=1}^{t_1(i)} W_{h_1(i,m_1)}$ even if $X_i\surd\downarrow$ does not hold. This is a consequence of property (v) ensuring that the sum $\sum_{m_2=1}^{t_2(j)} W_{h_2(j,m_2)}$ contains the same variables as the former sum. We can therefore apply law $(I2)$ or $(I3)$ to add or remove as many variables as required to match this sum.

In the remainder of this proof we use the following abbreviations.

$$E_1 \equiv \sum_{l_1=1}^{s_1(i)} a_{i,l_1}.A_{g_1(i,l_1)} + \sum_{m_1=1}^{t_1(i)} W_{h_1(i,m_1)},\ E_3 \equiv \sum_{k_1=1}^{r_1(i)} (\lambda_{i,k_1}).A_{f_1(i,k_1)},\ \text{and } E_2 \equiv \sum_{l_2\notin\pi^{(2)}(K_{i,j})} \tau.A_i.$$

With this notation we have, in summary, achieved so far:

$$\widehat{\mathcal{A}} \vdash H_{i,j}\{\vec{C}/\vec{Z}\} = E_1 + E_2 + \begin{cases} E_3 & \text{if } X_i\surd\!\downarrow \text{ and } Y_j\surd\!\downarrow \\ \bot & \text{if } X_i\!\uparrow \text{ or } Y_j\!\uparrow \\ 0 & \text{else} \end{cases} \tag{3}$$

We distinguish two cases, dependent on the fact if $\pi^{(2)}(K_{i,j})$ is equal or different from $\{1,\ldots,s_2(j)\}$. If $\pi^{(2)}(K_{i,j}) = \{1,\ldots,s_2(j)\}$ then $C_{i,j} \equiv A_i$, and E_2 denotes an empty sum. Still, $\widehat{\mathcal{A}} \vdash H_{i,j}\{\vec{C}/\vec{Z}\} = C_{i,j}$ has to be checked in 16 different subcases, resulting as a combination of $X_i\surd$, $X_i\!\uparrow$, $Y_j\surd$, $Y_j\!\uparrow$, and their respective negations. Fortunately six cases can be ruled out immediately.

- $X_i\surd \ \wedge \ X_i\!\downarrow \ \wedge \ Y_j\surd \ \wedge \ Y_j\!\uparrow$ is impossible because of property (iii),
- property (iv) rules out $X_i\surd \ \wedge \ X_i\!\uparrow \ \wedge \ Y_j\surd \ \wedge \ Y_j\!\downarrow$,
- $X_i\surd$ and $Y_j\not\surd$ is impossible (covering four cases), because $\pi^{(2)}(K_{i,j}) = \{1,\ldots,s_2(j)\}$ implies that $\forall l_2 \in \{1,\ldots,s_2(j)\}\ \exists l_1 \in \{1,\ldots,s_1(i)\} \ : \ a_{i,l_1} = b_{j,l_2}$.

We only sketch one of the remaining cases. If $X_i\surd \ \wedge \ X_i\!\uparrow \ \wedge \ Y_j\surd \ \wedge \ Y_j\!\downarrow$ then (3) gives $\widehat{\mathcal{A}} \vdash H_{i,j}\{\vec{C}/\vec{Z}\} = E_1 + \bot$ which can be transformed to the desired result $E_1 + E_3 + \bot = A_i \equiv C_{i,j}$ with the help of law $(MP2)$. The other cases are similar.

If, on the other hand $\pi^{(2)}(K_{i,j}) \neq \{1,\ldots,s_2(j)\}$, then $C_{i,j} \equiv \tau.A_i$ and $H_{i,j}\{\vec{C}/\vec{Z}\}$ contains a summand $\tau.A_i$ at least once, resulting from E_2. Multiple applications of law $(I1)$ and of law $(MP1)$ transform this expression to

$$E_1 + \tau.A_i + E_3 + \begin{cases} \bot & \text{if } X_i\!\uparrow \text{ or } Y_j\!\uparrow \\ 0 & \text{else.} \end{cases}$$

Since either $A_i = E_1 + E_3$ or $A_i = E_1 + E_3 + \bot$ holds we can transform the above with law $(\bot)$ to $A_i + \tau.A_i$. Law $(\tau 2)$ eventually produces $\widehat{\mathcal{A}} \vdash H_{i,j}\{\vec{C}/\vec{Z}\} = A_i + \tau.A_i = \tau.A_i \equiv C_{i,j}$.

We have thus shown that A provably satisfies the SES S. As mentioned above, the proof that B provably satisfies S is completely symmetric and therefore omitted. This completes the proof of Theorem 3. □

Hitherto we have restricted ourselves to strongly guarded expressions, i.e. expressions where every recursive variable is proceeded by an action prefix different from τ or a delay prefix (λ). In CCS weakly guarded expressions are easily handled, because KFAR can be used to remove loops of τs. As discussed above the presence of maximal progress does not allow this treatment since loops of τs cause divergence, except if a silent alternative exists. On a syntactic level this is achieved by the laws (rec4)-(rec6). We will now show that these laws are indeed sufficient to deduce all semantic equivalences that involve unguardedness. First, extending law (rec4), we point out that ill-definedness is not only caused by fully unguardedness but also by the absence of strong guardedness.

Lemma 4.7 If X is not strongly guarded in E then $\widehat{\mathcal{A}} \vdash E + \perp = E + X + \perp$.

Proof: By structural induction. □

Theorem 4 For each $E \in \mathsf{STC}^{\perp}$ there exists a strongly guarded $F \in \mathsf{STC}^{\perp}$ such that $\widehat{\mathcal{A}} \vdash E = F$.

Proof: By induction on the structure of E. The only interesting case is recursion. We show the following stronger property.

If $E \in \mathsf{STC}^{\perp}$ then there is some strongly guarded $F \in \mathsf{STC}^{\perp}$ such that

- X is strongly guarded in F
- Each not strongly guarded occurrence of any variable $Y \in \mathit{Var}(F)$ does not lie within the scope of a recursion $\mathrm{rec}Z.G$ of F.
- $\widehat{\mathcal{A}} \vdash \mathrm{rec}X.E = \mathrm{rec}X.F$

We only consider the case that each not strongly guarded occurrence of any variable $Y \in \mathit{Var}(E)$ does not lie within the scope of a recursion $\mathrm{rec}Z.G$ where $\mathrm{rec}Z.G$ is a subexpression of E. The general case can be reduced to this special case in complete analogy to [31].

Under the above assumptions, we only have to remove not strongly guarded occurrences of X where none of them appears inside the scope of a recursion. All fully unguarded occurrences of X can be eliminated (transformed into $\perp$) by means of (rec4). So we only have to consider occurrences of X that are not strongly, but weakly guarded, i.e. guarded by τ. Those of them that appear in E on top level (i.e. E is of the form $\tau.X + \ldots$) can be eliminated by means of law (rec5).

All other not strongly but weakly guarded occurrences of X can be transformed such that (rec5) is applicable. To achieve this we perform an iterative procedure that either lifts (possibly multiple) occurrences of X such that they are directly preceded by a τ guard or reduces the number of τ guards of some X.

Case 1: $E \equiv \tau.(\sum_{i=1}^{n} X + E') + F'$
We choose n such that X is weakly guarded in E'. Law (rec6) implies

$$\widehat{\mathcal{A}} \vdash \mathrm{rec}X.E \equiv \mathrm{rec}X(\tau.(\sum_{i=1}^{n} X + E') + F') = \mathrm{rec}X.(\tau.X + E' + F').$$

We continue with expression $\tau.X + E' + F'$.

Case 2: $E \equiv \tau.E' + F'$, where X occurs not strongly but weakly guarded in E'.
By assumption, this occurrence does not lie within the scope of a recursion. E' must hence be of the form $G + \tau.E''$. Law ($\perp$) then gives

$$\widehat{\mathcal{A}} \vdash E' = G + \tau.E'' + \perp = E' + \perp .$$

Since X is not strongly guarded in E' we can use Lemma 4.7 to obtain

$$\widehat{\mathcal{A}} \vdash E' = E' + \bot = E' + \bot + X = E' + X.$$

We can proceed with $\tau.(X + E') + F'$ by resorting to Case 1.

Iterating the above two steps will eventually lead to an expression F where all not strongly but weakly guarded occurrences of X appear on top level (i.e. F is of the form $\tau.X + \dots$). They can be eliminated by applying law (rec5). □

We now have the necessary means to prove completeness for arbitrary expressions.

Theorem 5 Let $E, F \in \mathsf{STC}^{\bot}$. $E \overset{c}{\approx}{}^{\bot} F$ implies $\widehat{\mathcal{A}} \vdash E = F$.

Proof: Theorem 4 implies the existence of guarded E', F' with $\widehat{\mathcal{A}} \vdash E = E'$ and $\widehat{\mathcal{A}} \vdash F = F'$. Correctness of the laws gives $E' \overset{c}{\approx}{}^{\bot} F'$. Using Lemma 4.4 there are guarded SES S_1 and S_2, such that E' provably satisfies S_1 and F' provably satisfies S_2. Because of Lemma 4.5 we can assume that S_1 and S_2 are saturated. Theorem 3 implies the existence of a guarded SES S, provably satisfying both, E' and F'. Now, Lemma 4.6 implies that S has a unique solution. Therefore, $\widehat{\mathcal{A}} \vdash E' = F'$ and hence $\widehat{\mathcal{A}} \vdash E = F$. □

Corollary 4.1 For $E, F \in \mathsf{STC}^{\bot}$, $E \overset{c}{\approx}{}^{\bot} F$ if and only if $\widehat{\mathcal{A}} \vdash E = F$.

5 Discussion and Applications

Observational congruence treats divergence in the style of WFAR, it allows to escape divergence only if a silent alternative exists. It is interesting to discuss $\overset{c}{\approx}{}^{\bot}$ in the context of ordinary CCS that arises from STC by disallowing delay prefixing. We use STC_{χ} to denote this subset of STC. With the technical means of Section 4 the following result is easy to show.

Theorem 6 For $E, F \in \mathsf{STC}_{\chi}$, $E \overset{c}{\approx} F$ if and only if $(\mathcal{A} \cup \mathcal{A}^{\mathrm{rec}} \cup \mathcal{A}^{I} \cup \mathcal{A}^{\bot}) \vdash E = F$.

Stated differently, we have obtained a complete proof system for CCS modulo observational congruence with WFAR. The proof system differs from other treatments of divergence in CCS. Walker has studied divergence sensitive bisimilarity [41] (see also [22]). His basic notion is a preorder rather than an equivalence. The induced equivalence turns out to be incomparable with Milner's original notion of observational congruence.

Our notion of observational congruence does neither coincide with Milner's divergence insensitive notion (denoted $\overset{c}{\approx}_{\mathrm{Milner}}$) nor with Walker's divergence sensitive variant ($\overset{c}{\approx}_{\mathrm{Walker}}$). Roughly, the reason is that, different from Walker, it is possible to escape from *unstable* divergence. But, deviating from Milner, it is not possible to escape from *stable* divergence. As a whole, it can be shown that $\overset{c}{\approx}$ is incomparable with Walker's notion (cf. the first and last pair in Figure 4 [18]). In contrast, $\overset{c}{\approx}$ turns out to be strictly finer than Milner's observational congruence.

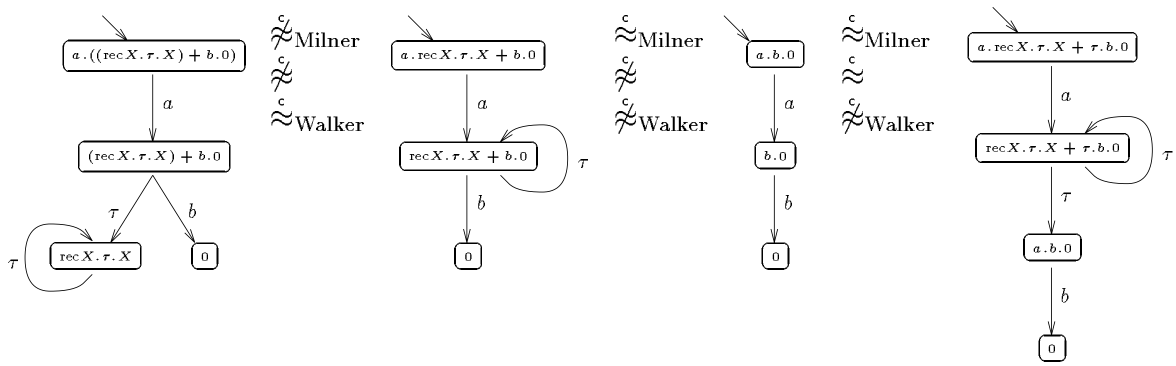


Figure 4: Observational Congruence is finer than Milner's notion and incomparable with Walker's.

Theorem 7 For $E, F \in \mathsf{STC}_{\not\chi}$ it holds that $\quad E \overset{c}{\approx} F \quad$ implies $\quad E \overset{c}{\approx}_{\text{Milner}} F$.

The inclusion is strict, as testified by the middle pair in Figure 4.

The language $\mathsf{STC}^{\perp}$ does not possess means to express parallel composition of expressions. However, parallel composition '|' (as well as relabelling and restriction) can be easily added, as in [30]. The only particularity that has to be clarified is the semantics of delayed expressions. Indeed, property (B) justifies to simply interleave delays, i.e. extending the definition of $\dashrightarrow$ (Definition 2.3) essentially by

$$\frac{E \overset{\lambda, w}{\dashrightarrow} E'}{E|F \overset{\lambda, l\,w}{\dashrightarrow} E'|F} \qquad\qquad \frac{F \overset{\lambda, w}{\dashrightarrow} F'}{E|F \overset{\lambda, l\,w}{\dashrightarrow} E|F'}.$$

In the same way we can establish an expansion law that allows to equate

$$(\lambda).E \mid (\mu).F \quad = \quad (\lambda).(\ E \mid (\mu).F\ ) + (\mu).(\ (\lambda).E \mid F\ ).$$

As a consequence, the complete proof system introduced in Section 3 can be straightforwardly extended to cover the usual operators of a process algebra.

Our axiomatic treatment of WFAR also allows to tackle completeness for CCS with priority. To illustrate this, we give a different interpretation of the ingredients of our calculus. Assume that $(\lambda).P$ denotes that P is preceded by a low priority action instead of a stochastic delay. In other words, we now assume $\lambda \in Act$ and use $(\_)$ to denote that λ has low priority, while ordinary prefix, say $\lambda.P$, denotes high priority. In this scenario we may define a prioritised strong bisimulation following the lines of Definition 2.5, but we replace the cumulative rate function γ by a boolean function $\gamma^{\mathrm{P}}(E, \lambda, C)$ that is true only if there is some $\overset{\lambda,w}{\dashrightarrow}$ transition from E into the class C. (This is inspired by [19] where this replacement is done in the opposite direction.)

Definition 5.1 Let $C \subseteq \mathsf{STC}^{\perp}$. We define a function $\gamma : \mathsf{STC} \times Act \times 2^{\mathsf{STC}^{\perp}} \longrightarrow \{\mathtt{true}, \mathtt{false}\}$ as follows

$$\gamma^{\mathrm{P}}(E, \lambda, C) = \begin{cases} \mathtt{true} & \text{if } \exists F \in C : E \overset{\lambda, w}{\dashrightarrow} F, \\ \mathtt{false} & \text{else.} \end{cases}$$

Definition 5.2 An equivalence relation $\mathcal{B}$ on $\mathsf{STP}^{\perp}$ is a prioritised strong bisimulation iff $P \; \mathcal{B} \; Q$ implies for all $a, \lambda \in Act$

1. $P \xrightarrow{a} P'$ implies $Q \xrightarrow{a} Q'$ for some Q' with $P' \; \mathcal{B} \; Q'$,
2. $P\surd\!\downarrow$ implies that $Q\surd\!\downarrow$ and that $\gamma^{\mathrm{P}}(P, \lambda, C) = \gamma^{\mathrm{P}}(Q, \lambda, C)$ for all $C \in \mathsf{STP}^{\perp}/\mathcal{B}$.

It can be shown that this definition agrees with the definition of prioritised strong bisimulation of Natarjan *et al.* [34] for weakly guarded expressions. The technical difference is that we realise priority of $\xrightarrow{\tau}$ transitions by means of an additional constraint in condition (2) while Natarjan *et al.* incorporate this priority inside their operational rules by means of negative premises.

Defining a simple prioritised weak bisimulation and observational congruence can follow the lines of Lemma 2.7, respectively Definition 2.8, without introducing any problems. The set of axioms $(\mathcal{A} \cup \mathcal{A}^{\mathrm{rec}} \cup \mathcal{A}^{I} \cup \mathcal{A}^{\perp} \cup \{(\tau 4), (MP1), (MP2)\})$ gives a complete proof system for this prioritised observational congruence. In particular, $(MP1)$ becomes the priority axiom mentioned in our introduction. This prioritised observational congruence is weak in the sense that it abstracts from sequences of silent *high* priority actions. *Low* prioritised silent actions, however, are treated as in strong bisimulation. This is the main simplification with respect to the approach of [34] where most of the complexity is due to a weak transition relation that involves silent actions of both, high and low priority.

6 Concluding remarks

In this paper we have investigated weak bisimilarity and observational congruence in a stochastic timed calculus with maximal progress. The notions refine the usual notions on CCS because they allow to escape from divergence (only) if a silent alternative exists. This takes the effect of WFAR. The refinement is needed in order to capture the interplay of maximal progress and divergence. We have obtained a sound and complete proof system for arbitrary expressions. Since Milner's law $\mathrm{rec}X.\tau.X + P = \mathrm{rec}X.\tau.P$ is invalidated by maximal progress we have replaced it by a set of laws that allow abstraction of unstable divergence.

As a side result we obtain a sound and complete proof system for observational congruence with WFAR on CCS. Since our treatment of divergence is orthogonal to the aspects of stochastic time, it seems obvious that it can be profitably adapted to other calculi. As far as we know, this paper is the first succesfull attempt to provide a complete proof system for observational congruence for calculi with recursion including either priority or maximal progress. The proof system for WFAR should allow to fill some of the existing gaps of incomplete proof systems. Of particular interest is weak prioritised bisimilarity of [34] and its successor [13]. Indeed, we have provided a complete proof system for CCS with priority modulo a simplified notion of prioritised observational congruence.

It is well known that many strong and weak equivalences can be characterised by means of simple modal logic characterisations. We plan to investigate such characterisations for the equivalence notion discussed here. This would be beneficial for the specification and verification of particular stochastic timed properties. Currently, properties of a specification are evaluated by transforming the transition system into a Markov Chain and subsequent calculation of state probabilities. The interpretation of these probabilities is not easy because the behavioural view is lost on the level of the Markov Chain. Even though of a speculative nature, we would prefer a model checking approach to this problem, inspired by [3].

Appendix

A Congruence with respect to Recursion

Congruence of $\approx$ with respect to the operators of $\mathsf{STC}^{\perp}$ follows the lines of [24], except for recursion. In order to prove congruence with respect to recursion we use a notion of 'bisimulation up to $\approx$' [37]. We only consider closed expressions $P \in \mathsf{STP}^{\perp}$. Once we have shown for closed $\mathrm{rec}X.E$ and $\mathrm{rec}X.F$ that $E \overset{c}{\approx}^{\perp} F$ implies $\mathrm{rec}X.E \overset{c}{\approx}^{\perp} \mathrm{rec}X.F$, Definition 2.9 assures that this implication also holds for arbitrary expressions.

Let $\mathcal{S}$ be a binary relation on $\mathsf{STP}^{\perp}$. A sequence $(R_1, \ldots, R_n)$ with $n \geq 1$ and $R_i \in \mathsf{STP}^{\perp}$ for $i \in \{1, \ldots, n\}$ is a $(\mathcal{S} \cup \approx^{\perp})$-path (or a path, for short) if:

1. $\forall i \in \{1, \ldots, n-1\} \;:\; R_i \;(\mathcal{S} \cup \approx^{\perp})\; R_{i+1}$
2. $\forall i \in \{1, \ldots, n-2\} \;(R_i \approx^{\perp} R_{i+1} \;\;\Rightarrow\;\; R_{i+1} \not\approx^{\perp} R_{i+2})$

It is worth to remark that the second requirement can always be guaranteed, due to the transitivity of $\approx^{\perp}$. In the sequel we will use $\mathcal{P}$, $\mathcal{P}'$, $\mathcal{Q}$, $\mathcal{Q}'$, $\mathcal{R}\ldots$ to denote paths. If $\mathcal{P} = (R_1, \ldots, R_n)$ is a path, let

1. $\mathcal{P}_i \equiv R_i \;\; (1 \leq i \leq n)$
2. $l(\mathcal{P}) = n$,
3. $\mathcal{P}^{(i)} = (R_i, R_{i+1}, \ldots, R_n) \;\; (1 \leq i \leq n)$ and
4. $S(\mathcal{P}) = |\{i \mid 1 \leq i \leq n-1 \;\wedge\; R_i \not\approx^{\perp} R_{i+1}\}|$.

For two paths, $\mathcal{P} = (P_1, \ldots, P_n)$ and $\mathcal{Q} = (Q_1, \ldots, Q_m)$ with $P_n \equiv Q_1$, we let

$$\mathcal{P}\mathcal{Q} = \begin{cases} (P_1, \ldots, P_n, Q_2, \ldots, Q_m) & \text{if } P_{n-1} \not\approx^{\perp} P_n \text{ or } Q_1 \not\approx^{\perp} Q_2 \\ (P_1, \ldots, P_{n-1}, Q_2, \ldots, Q_m) & \text{else} \end{cases}$$

Definition A.1 Let $\mathcal{S}$ be a symmetric relation on $\mathsf{STP}^\perp$. Thus, $\mathcal{T} = (\mathcal{S} \cup \approx^\perp)^*$ is an equivalence relation on $\mathsf{STP}^\perp$. $\mathcal{S}$ is an observational congruence up to $\approx^\perp$ iff $P \mathcal{S} Q$ implies for all $a \in Act$, $C \in \mathsf{STP}^\perp/\mathcal{T}$ and $P' \in \mathsf{STP}^\perp$ that

1. $P \xrightarrow{a} P'$ implies $Q \stackrel{a}{\Longrightarrow} Q'$ and $P' \mathcal{S} R \approx^\perp Q'$ for some $R, Q' \in \mathsf{STP}^\perp$,
2. $P\surd\!\downarrow$ (or $Q\surd\!\downarrow$) implies $\gamma(P, C) = \gamma(Q, C)$ and
3. $P\surd\!\downarrow$ iff $Q\surd\!\downarrow$.

We are aiming to show that $P \stackrel{c}{\approx}^\perp Q$ holds already if there is an observational congruence up to $\approx^\perp$ between P and Q. This will be expressed in Lemma A.6. We need the following lemmas beforehand.

Lemma A.2 Let $\mathcal{B}_1$, $\mathcal{B}_2$ be equivalence relations on $\mathsf{STC}^\perp$. $\mathcal{B}_1 \subseteq \mathcal{B}_2$ implies that

$$\text{if} \quad \forall C_1 \in \mathsf{STC}^\perp/\mathcal{B}_1 \;:\; \gamma(E, C_1) = \gamma(F, C_1) \quad \text{then} \quad \forall C_2 \in \mathsf{STC}^\perp/\mathcal{B}_2 \;:\; \gamma(E, C_2) = \gamma(F, C_2).$$

Lemma A.3 For P, $Q \in \mathsf{STP}^\perp$, $P \approx^\perp Q$ holds iff for every $a \in Act$

1. $P \xrightarrow{a} P'$ implies $Q \stackrel{\widehat{a}}{\Longrightarrow} Q'$ and $P' \approx^\perp Q'$ for some $Q' \in \mathsf{STP}^\perp$,
2. $Q \xrightarrow{a} Q'$ implies $P \stackrel{\widehat{a}}{\Longrightarrow} P'$ and $P' \approx^\perp Q'$ for some $P' \in \mathsf{STP}^\perp$,
3. $P\surd\!\downarrow$ implies $\exists Q'\surd\!\downarrow\, (Q \xrightarrow{\tau}{}^* Q' \;\wedge\; \forall C \in \mathsf{STP}^\perp/\approx^\perp \;:\; \gamma(P, C) = \gamma(Q', C))$,
4. $Q\surd\!\downarrow$ implies $\exists P'\surd\!\downarrow\, (P \xrightarrow{\tau}{}^* P' \;\wedge\; \forall C \in \mathsf{STP}^\perp/\approx^\perp \;:\; \gamma(P', C) = \gamma(Q, C))$.

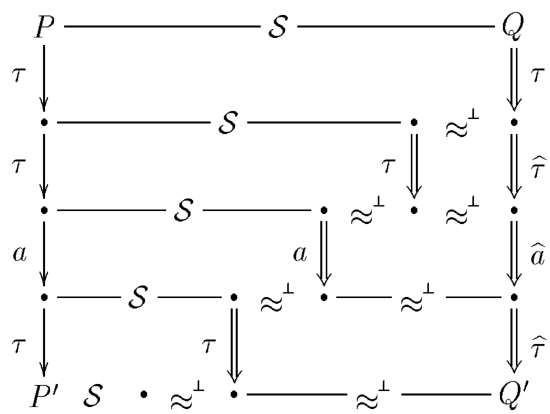
The proofs of both lemmas are very easy.

Lemma A.4 If $\mathcal{S}$ is an observational congruence up to $\approx^\perp$ then $P \mathcal{S} Q$ and $P \stackrel{a}{\Longrightarrow} P'$ imply $Q \stackrel{a}{\Longrightarrow} Q'$ and $P' \mathcal{S} R \approx^\perp Q'$ for some $Q', R \in \mathsf{STP}^\perp$.

Proof: It is obviously sufficient to show

$$P' \mathcal{S} R' \approx^\perp Q' \;\wedge\; P' \xrightarrow{a} P'' \quad \Rightarrow \quad \exists Q'', R'' \in \mathsf{STP}^\perp\; (Q' \stackrel{\widehat{a}}{\Longrightarrow} Q'' \;\wedge\; P'' \mathcal{S} R'' \approx^\perp Q'')$$

because this implies that we can trace the chain $P \stackrel{a}{\Longrightarrow} P'$ transition by transition. choosing $R' \equiv Q$ for the first step. Since the first step, according to (1) of Definition A.1 and $P \mathcal{S} Q$ implies that we will perform at least one transition from Q we can deduce that $Q \stackrel{a}{\Longrightarrow} Q'$ instead of the weaker $Q \stackrel{\widehat{a}}{\Longrightarrow} Q'$. So, let $P' \mathcal{S} R' \approx^\perp Q' \;\wedge\; P' \xrightarrow{a} P''$. From $P' \xrightarrow{a} P''$, $P' \mathcal{S} R'$ we derive using property (1) of Definition A.1 $R' \stackrel{a}{\Longrightarrow} R'''$ and $P'' \mathcal{S} R'' \approx^\perp R'''$ for some $R'', R''' \in \mathsf{STP}^\perp$. Now, $R' \stackrel{a}{\Longrightarrow} R'''$ and $R' \approx^\perp Q'$ imply $Q' \stackrel{\widehat{a}}{\Longrightarrow} Q''$ and $R''' \approx^\perp Q''$ for some $Q'' \in \mathsf{STP}^\perp$. As a whole, we obtain $P'' \mathcal{S} R'' \approx^\perp R''' \approx^\perp Q''$. The above reasoning is illustrated (for a specific example) by the following diagram.



$\square$

Lemma A.5 If $\mathcal{S}$ is an observational congruence up to $\approx^{\perp}$ then $\mathcal{T} = (\mathcal{S} \cup \approx^{\perp})^*$ is a weak bisimulation.

Proof: Since $\mathcal{S}$ is symmetric, $\mathcal{T}$ is an equivalence relation. In order to show condition (1) of Lemma 2.7, assume $P \; \mathcal{T} \; Q$. Thus, there is a $(\mathcal{S} \cup \approx^{\perp})$–path $\mathcal{P}$ with $\mathcal{P}_1 \equiv P$ and $\mathcal{P}_{l(\mathcal{P})} \equiv Q$. In order to simplify the proof of condition (2) of Lemma 2.7 it is helpful to show the following stronger condition (1') instead of (1).

> Let $\mathcal{P}$ be a path with $P \equiv \mathcal{P}_1$ and $Q \equiv \mathcal{P}_{l(\mathcal{P})}$ and let $P \stackrel{a}{\Longrightarrow} P'$. Then there is a path $\mathcal{Q}$ and $Q' \in \mathsf{STP}^{\perp}$ such that $Q \stackrel{\widehat{a}}{\Longrightarrow} Q' \;\wedge\; \mathcal{Q}_1 \equiv P' \;\wedge\; \mathcal{Q}_{l(\mathcal{Q})} \equiv Q'$. In addition, $\mathcal{Q}$ has the following properties.
>
> - $P \equiv \mathcal{P}_1 \approx^{\perp} \mathcal{P}_2 \;\Rightarrow\; S(\mathcal{Q}) \leq S(\mathcal{P})$
> - $P \equiv \mathcal{P}_1 \not\approx^{\perp} \mathcal{P}_2 \;\Rightarrow\; ((\mathcal{Q}_1 \not\approx^{\perp} \mathcal{Q}_2 \;\wedge\; S(\mathcal{Q}) \leq S(\mathcal{P})) \;\vee\; S(\mathcal{Q}) < S(\mathcal{P}))$

The proof of (1') is by induction on $S(\mathcal{P})$. So, let $\mathcal{P}$ be a path with $P \equiv \mathcal{P}_1$ and $Q \equiv \mathcal{P}_{l(\mathcal{P})}$ and let $P \stackrel{a}{\Longrightarrow} P'$.

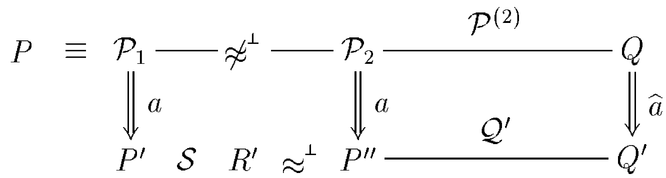
First, assume $S(\mathcal{P}) = 0$, i.e. $P \approx^{\perp} Q$. Then $P \stackrel{a}{\Longrightarrow} P'$ implies, as expected, that there is some Q' such that $Q \stackrel{\widehat{a}}{\Longrightarrow} Q' \;\wedge\; P' \approx^{\perp} Q'$. We therefore choose $\mathcal{Q} = (P', Q')$.

Now, let $S(\mathcal{P}) > 0$. We distinguish the following two cases.

Case 1: $P \equiv \mathcal{P}_1 \not\approx^{\perp} \mathcal{P}_2$

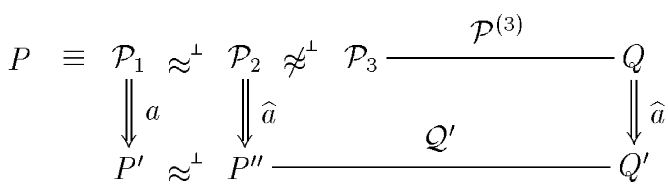
This implies $\mathcal{P}_1 \; \mathcal{S} \; \mathcal{P}_2$. From $P \stackrel{a}{\Longrightarrow} P'$ and Lemma A.4 we derive that there are some $P'', R' \in \mathsf{STP}^{\perp}$ such that $\mathcal{P}_2 \stackrel{a}{\Longrightarrow} P'' \;\wedge\; P' \; \mathcal{S} \; R' \approx^{\perp} P''$. Since we also know that $S(\mathcal{P}^{(2)}) < S(\mathcal{P})$ holds we make use of the induction hypotheses for the path $\mathcal{P}^{(2)}$ and the chain of transitions $\mathcal{P}_2 \stackrel{a}{\Longrightarrow} P''$ in order to deduce that there is some $Q' \in \mathsf{STP}^{\perp}$ such that $Q \stackrel{\widehat{a}}{\Longrightarrow} Q'$, as well as a path $\mathcal{Q}'$ satisfying $\mathcal{Q}'_1 \equiv P''$ and $\mathcal{Q}'_{l(\mathcal{Q}')} \equiv Q'$ as well as $S(\mathcal{Q}') \leq S(\mathcal{P}^{(2)})$.

If $P' \not\approx^{\perp} R'$ define a path $\mathcal{Q}$ as $\mathcal{Q} = (P', R', P'')\mathcal{Q}'$. Then, $\mathcal{Q}_1 \equiv P' \not\approx^{\perp} R' \equiv \mathcal{Q}_2$ and $S(\mathcal{Q}) = S(\mathcal{Q}') + 1 \leq S(\mathcal{P}^{(2)}) + 1 = S(\mathcal{P})$. Hence $\mathcal{Q}$ satisfies all requirements. If, otherwise $P' \approx^{\perp} R'$, then $R' \approx^{\perp} P''$ implies $P' \approx^{\perp} P''$. Define $\mathcal{Q} = (P', P'')\mathcal{Q}'$. Then $S(\mathcal{Q}) = S(\mathcal{Q}') \leq S(\mathcal{P}^{(2)}) < S(\mathcal{P})$ holds as required. A diagram illustrates the proof of Case 1:



Case 2: $P \equiv \mathcal{P}_1 \approx^{\perp} \mathcal{P}_2$

Thus, $\mathcal{P}_2 \not\approx^{\perp} \mathcal{P}_3$ necessarily holds. $P \overset{a}{\Longrightarrow} P'$ however implies that there is some P'' such that $\mathcal{P}_2 \overset{\hat{a}}{\Longrightarrow} P'' \;\wedge\; P' \approx^{\perp} P''$. In case that $a = \tau$ and $\mathcal{P}_2 \equiv P''$ hold choose $Q' \equiv Q \;\wedge\; \mathcal{Q} = (P', P'')\mathcal{P}^{(2)}$ (note that $\mathcal{P}^{(2)}_1 \equiv \mathcal{P}_2 \equiv P''$). Otherwise $\mathcal{P}_2 \overset{a}{\Longrightarrow} P''$ holds. We can therefore resort to Case 1 with $\mathcal{P}^{(2)}$ and the chain of transitions $\mathcal{P}_2 \overset{a}{\Longrightarrow} P''$. We obtain that there is some Q' such that $Q \overset{\hat{a}}{\Longrightarrow} Q'$, as well as a path $\mathcal{Q}'$ satisfying $\mathcal{Q}'_1 \equiv P''$ and $\mathcal{Q}'_{l(\mathcal{Q}')} \equiv Q'$ as well as $S(\mathcal{Q}') \leq S(\mathcal{P}^{(2)})$. We now choose $\mathcal{Q} = (P', P'')\mathcal{Q}'$ and obtain $S(\mathcal{Q}) = S(\mathcal{Q}') \leq S(\mathcal{P}^{(2)}) = S(\mathcal{P})$. Again a diagram is helpful to illustrate the proof of $(1')$ for Case 2.



We are now ready to verify condition (2) of Lemma 2.7. Let $P \;\mathcal{T}\; Q$ and $P\surd\!\downarrow$. Furthermore let $\mathcal{P}$ be a path satisfying $\mathcal{P}_1 \equiv P$ and $\mathcal{P}_{l(\mathcal{P})} \equiv Q$. We show the following property by induction on $S(\mathcal{P})$.

$$\exists Q'\surd\!\downarrow \forall C \in \mathsf{STP}^{\perp}/\mathcal{T}\; (Q \xrightarrow{\tau}{}^{*} Q' \;\wedge\; \gamma(P, C) = \gamma(Q', C)) \tag{4}$$

The base case, $S(\mathcal{P}) = 0$, (i.e. $P \approx^{\perp} Q$) follows directly from property (3) of Lemma A.3 and Lemma A.2 because $\approx^{\perp} \subseteq \mathcal{T}$. Now let $S(\mathcal{P}) > 0$. Again we distinguish two cases.

Case 1: $P \equiv \mathcal{P}_1 \not\approx^{\perp} \mathcal{P}_2$

So, $\mathcal{P}_1 \;\mathcal{S}\; \mathcal{P}_2$ holds. Since $P \equiv \mathcal{P}_1\surd\!\downarrow$ we obtain (using condition (2) and (3) of Definition A.1) that $\mathcal{P}_2\surd\!\downarrow$ and

$$\forall C \in \mathsf{STP}^{\perp}/\mathcal{T} : \gamma(P, C) = \gamma(\mathcal{P}_2, C). \tag{5}$$

Since $S(\mathcal{P}^{(2)}) < S(\mathcal{P})$ and $\mathcal{P}_2\surd\!\downarrow$ we make use of our induction hypotheses for the path $\mathcal{P}^{(2)}$. We obtain

$$\exists Q'\surd\!\downarrow \forall C \in \mathsf{STP}^{\perp}/\mathcal{T}\; (Q \xrightarrow{\tau}{}^{*} Q' \;\wedge\; \gamma(\mathcal{P}_2, C) = \gamma(Q', C)).$$

Using (5) this implies (4).

Case 2: $P \equiv \mathcal{P}_1 \approx^{\perp} \mathcal{P}_2$
Thus, necessarily $\mathcal{P}_2 \not\approx^{\perp} \mathcal{P}_3$. From $P\surd\!\downarrow$ and $P \approx^{\perp} \mathcal{P}_2$ we deduce, using $\approx^{\perp} \ \subseteq \mathcal{T}$ and Lemma A.2, that

$$\exists P'\surd\!\downarrow \forall C \in \mathsf{STP}^{\perp}/\mathcal{T} \ (\mathcal{P}_2 \xrightarrow{\tau}{}^{*} P' \ \wedge \ \gamma(P,C) = \gamma(P',C)). \tag{6}$$

If $\mathcal{P}_2 \equiv P'$, we resort to Case 1 with the path $\mathcal{P}^{(2)}$ taking into account that $\mathcal{P}_1^{(2)} \equiv P'\surd\!\downarrow$ holds. We obtain

$$\exists Q'\surd\!\downarrow \forall C \in \mathsf{STP}^{\perp}/\mathcal{T} \ (Q \xrightarrow{\tau}{}^{*} Q' \ \wedge \ \gamma(P',C) = \gamma(Q',C)).$$

Together with (6) this implies (4). Therefore we can assume that $\mathcal{P}_2 \stackrel{\tau}{\Longrightarrow} P'$. We can now make use of property (1') for the path $\mathcal{P}^{(2)}$ and the chain $\mathcal{P}_1^{(2)} \equiv \mathcal{P}_2 \stackrel{\tau}{\Longrightarrow} P'$ taking into account that $\mathcal{P}_1^{(2)} \equiv \mathcal{P}_2 \not\approx^{\perp} \mathcal{P}_3 \equiv \mathcal{P}_2^{(2)}$. We obtain that there is some $Q'' \in \mathsf{STP}^{\perp}$ such that $Q \xrightarrow{\tau}{}^{*} Q''$, as well as a path $\mathcal{Q}$ satisfying

- $\mathcal{Q}_1 \equiv P'$ and $\mathcal{Q}_{l(\mathcal{Q})} \equiv Q''$ and
- $(\mathcal{Q}_1 \not\approx^{\perp} \mathcal{Q}_2 \ \wedge \ S(\mathcal{Q}) \leq S(\mathcal{P}^{(2)}) = S(\mathcal{P})) \ \vee \ S(\mathcal{Q}) < S(\mathcal{P}^{(2)}) = S(\mathcal{P})$.

If $S(\mathcal{Q}) < S(\mathcal{P}^{(2)}) = S(\mathcal{P})$ holds, we can directly use our induction hypotheses for the path $\mathcal{Q}$ taking $\mathcal{Q}_1 \equiv P'\surd\!\downarrow$ into account. We obtain

$$\exists Q'\surd\!\downarrow \forall C \in \mathsf{STP}^{\perp}/\mathcal{T} \ (Q'' \xrightarrow{\tau}{}^{*} Q' \ \wedge \ \gamma(P',C) = \gamma(Q',C)).$$

As a whole, we get $Q \xrightarrow{\tau}{}^{*} Q'' \xrightarrow{\tau}{}^{*} Q'\surd\!\downarrow$, thus $Q \xrightarrow{\tau}{}^{*} Q'\surd\!\downarrow$ and, using (6),

$$\forall C \in \mathsf{STP}^{\perp}/\mathcal{T} : \ \gamma(P,C) = \gamma(Q',C).$$

If, otherwise, $\mathcal{Q}_1 \not\approx^{\perp} \mathcal{Q}_2$ and $S(\mathcal{Q}) \leq S(\mathcal{P}^{(2)}) = S(\mathcal{P})$, we can resort to Case 1 with path $\mathcal{Q}$ taking (again) $\mathcal{Q}_1 \equiv P'\surd\!\downarrow$ into account. We obtain

$$\exists Q'\surd\!\downarrow \forall C \in \mathsf{STP}^{\perp}/\mathcal{T} \ (Q'' \xrightarrow{\tau}{}^{*} Q' \ \wedge \ \gamma(P',C) = \gamma(Q',C)).$$

As above, this results in (4), completing the proof of Lemma A.5. □

Lemma A.6 If $\mathcal{S}$ is an observational congruence up to $\approx^{\perp}$, then $\mathcal{S} \subseteq \stackrel{c}{\approx}^{\perp}$.

Proof: Lemma A.5 says that $\mathcal{T} = (\mathcal{S} \cup \approx^{\perp})^{*}$ is a weak bisimulation, implying $\mathcal{S} \subseteq (\mathcal{S} \cup \approx^{\perp})^{*} \subseteq \approx^{\perp}$. We can therefore deduce the following properties from $P \ \mathcal{S} \ Q$:

1. Let $P \xrightarrow{a} P'$. This implies (using (1) of Definition A.1) $Q \stackrel{a}{\Longrightarrow} Q'$ and $P' \ \mathcal{S} \ R \approx^{\perp} Q'$ for some $Q', R \in \mathsf{STP}^{\perp}$. $P' \ \mathcal{S} \ R$ now implies (using $\mathcal{S} \subseteq \approx^{\perp}$) that $P' \approx^{\perp} R$ and thus $P' \approx^{\perp} Q'$.

2. Symmetrically, $Q \xrightarrow{a} Q'$ implies that there is some $P' \in \mathsf{STP}^\perp$ such that $P \xRightarrow{a} P' \wedge P' \approx^\perp Q'$.
3. Let $P, Q \surd\downarrow$. Condition (2) of Definition A.1 implies $\gamma(P,C) = \gamma(Q,C)$ for every $C \in \mathsf{STP}^\perp/\mathcal{T}$. Since $\mathcal{T} \subseteq\ \approx^\perp$, Lemma A.2 implies $\gamma(P,C) = \gamma(Q,C)$ for every $C \in \mathsf{STP}^\perp/\approx^\perp$.
4. Condition (3) of Definition A.1 gives rise to $P\surd\downarrow$ iff $Q\surd\downarrow$.

These four properties are equivalent to $P \overset{c}{\approx}{}^\perp Q$ (Definition 2.8). □

In order to prove $\mathrm{rec}X.E \overset{c}{\approx}{}^\perp \mathrm{rec}X.F$ (if $E, F \in \mathsf{STC}^\perp$ and $E \overset{c}{\approx}{}^\perp F$) it is sufficient to construct an observational congruence up to $\approx^\perp$ containing the pair $(\mathrm{rec}X.E, \mathrm{rec}X.F)$. We will construct such an $\mathcal{S}$ in Lemma A.12. First, we state some simple lemmas.

Lemma A.7 Let $H, G, E \in \mathsf{STC}^\perp$. Then $G \xrightarrow{a} H$ implies $G\{E/X\} \xrightarrow{a} H\{E/X\}$. Analogously, $G \overset{\lambda,w}{\dashrightarrow} H$ implies $G\{E/X\} \overset{\lambda,w}{\dashrightarrow} H\{E/X\}$.

Lemma A.8 Let $G, E \in \mathsf{STC}^\perp$. If $E \xrightarrow{a} E'$ and X is fully unguarded in G then $G\{E/X\} \xrightarrow{a} E'$.

Lemma A.9 Let $G\{E/X\} \xrightarrow{a} F$. This implies that X is fully unguarded in G and $E \xrightarrow{a} F$ or that $G \xrightarrow{a} H$ and $F \equiv H\{E/X\}$. Furthermore, if X is strongly guarded in G and $a = \tau$, then X is strongly guarded in H.

Similarly, if $G\{E/X\} \overset{\lambda,w}{\dashrightarrow} F$ and X is weakly guarded in G then $G \overset{\lambda,w}{\dashrightarrow} H$ and $F \equiv H\{E/X\}$.

Each of the above three lemmas requires a simple induction on the structure of the respective proof trees. The following two lemmas need structural induction on $\mathsf{STC}^\perp_\downarrow$.

Lemma A.10 Let $H, E \in \mathsf{STC}^\perp$. Then $H\{E/X\} \in \mathsf{STC}^\perp_\downarrow$ implies $H \in \mathsf{STC}^\perp_\downarrow$.

Lemma A.11 Let $H \in \mathsf{STC}^\perp_\downarrow$. If X is weakly guarded in H or $E \in \mathsf{STC}^\perp_\downarrow$ then $H\{E/X\} \in \mathsf{STC}^\perp_\downarrow$.

Lemma A.12 Let $\mathit{Var}(E) \cup \mathit{Var}(F) \subseteq \{X\}$, $\mathrm{rec}X.E, \mathrm{rec}X.F \in \mathsf{STP}^\perp$ and $E \overset{c}{\approx}{}^\perp F$. Furthermore let $\mathcal{R} = \{(G\{\mathrm{rec}X.E/X\}, G\{\mathrm{rec}X.F/X\}) \mid \mathit{Var}(G) \subseteq \{X\}\}$. Then, $\mathcal{S} = (\mathcal{R} \cup \mathcal{R}^{-1})$ is an observational congruence up to $\approx^\perp$.

Proof: (Sketch) We have to check condition (1)-(3) of Definition A.1, which is only necessary for pairs in $\mathcal{R}$ due to symmetry. Each condition involves a case analysis concerning the outermost operator of G. Condition (1) is shown by an induction on the height of the proof tree for $G\{\mathrm{rec}X.E/X\} \xrightarrow{a} P'$. To show (2) we perform an induction on the sum of the heights of all proof trees for $\dashrightarrow$ transitions emanating $G\{\mathrm{rec}X.E/X\}$. Structural induction on the definition of $\mathsf{STC}^\perp_\downarrow$ is needed to show condition (3). The complete proof is carried out in [28]. We only consider the most difficult case $G \equiv X$, i.e. the pair $(\mathrm{rec}X.E, \mathrm{rec}X.F)$.

Assume $\mathrm{rec}X.E \xrightarrow{a} P$. Thus $E\{\mathrm{rec}X.E/X\} \xrightarrow{a} P$, which can be derived by a smaller proof tree. Thus, the induction hypothesis implies $E\{\mathrm{rec}X.F/X\} \stackrel{a}{\Longrightarrow} Q'$ and $P \; \mathcal{S} \; R {\approx^{\perp}} Q'$ for some Q'. Since $E \stackrel{c}{\approx}^{\perp} F$, i.e. (using Definition 2.9) $E\{\mathrm{rec}X.F/X\} \stackrel{c}{\approx}^{\perp} F\{\mathrm{rec}X.F/X\}$ this implies $F\{\mathrm{rec}X.F/X\} \stackrel{a}{\Longrightarrow} Q \;\wedge\; Q' {\approx^{\perp}} Q$ for some Q and thus finally $\mathrm{rec}X.F \stackrel{a}{\Longrightarrow} Q \;\wedge P \; \mathcal{S} \; R {\approx^{\perp}} Q' {\approx^{\perp}} Q$.

In order to verify condition (2) of Definition A.1 assume $\mathrm{rec}X.E\surd\!\downarrow$ and $\mathrm{rec}X.F\surd\!\downarrow$. Thus, $E\{\mathrm{rec}X.E/X\}\surd\!\downarrow$, $F\{\mathrm{rec}X.F/X\}\surd\!\downarrow$. Furthermore, $\mathrm{rec}X.E \in \mathsf{STC}^{\perp}_{\downarrow}$ implies that X is weakly guarded in E. Lemma A.7, A.9, A.10 and A.11 imply $E\{\mathrm{rec}X.F/X\}\surd\!\downarrow$. Therefore, for every $C \in \mathsf{STP}^{\perp}/(\mathcal{S} \cup {\approx^{\perp}})^*$

$$
\begin{array}{rcl}
\gamma(\mathrm{rec}X.E, C) & = & (\text{rule } (\mathrm{rec}^M)) \\
\gamma(E\{\mathrm{rec}X.E/X\}, C) & = & (\text{induction hypothesis}) \\
\gamma(E\{\mathrm{rec}X.F/X\}, C) & = & (E\{\mathrm{rec}X.F/X\} \stackrel{c}{\approx}^{\perp} F\{\mathrm{rec}X.F/X\}, \text{ Lemma A.2}) \\
\gamma(F\{\mathrm{rec}X.F/X\}, C) & = & (\text{rule } (\mathrm{rec}^M)) \\
\gamma(\mathrm{rec}X.F, C). & &
\end{array}
$$

Finally condition (3) of Definition A.1 can be shown as follows. Assume $\mathrm{rec}X.E\surd\!\downarrow$. As in the proof of condition (2) it follows $E\{\mathrm{rec}X.F/X\}\surd\!\downarrow$. Since $E \stackrel{c}{\approx}^{\perp} F$, i.e. $E\{\mathrm{rec}X.F/X\} \stackrel{c}{\approx}^{\perp} F\{\mathrm{rec}X.F/X\}$, this implies $F\{\mathrm{rec}X.F/X\}\surd\!\downarrow$, i.e. $\mathrm{rec}X.F\surd\!\downarrow$. □

Eventually, we have all the means to derive that $\stackrel{c}{\approx}^{\perp}$ is a congruence with respect to rec.

Corollary A.1 If $E, F \in \mathsf{STC}^{\perp}$ then $E \stackrel{c}{\approx}^{\perp} F$ implies $\mathrm{rec}X.E \stackrel{c}{\approx}^{\perp} \mathrm{rec}X.F$.

Proof: Because of Definition 2.9 it is sufficient to consider only those $E, F \in \mathsf{STC}^{\perp}$ where $\mathit{Var}(E) \cup \mathit{Var}(F) \subseteq \{X\}$. Assume that $E \stackrel{c}{\approx}^{\perp} F$ holds. Then the relation $\mathcal{S}$ appearing in Lemma A.12 is an observational congruence up to $\approx^{\perp}$. Choosing $G \equiv X$ implies $\mathrm{rec}X.E \; \mathcal{S} \; \mathrm{rec}X.F$. Theorem A.6 now implies $\mathrm{rec}X.E \stackrel{c}{\approx}^{\perp} \mathrm{rec}X.F$. □

B Soundness of Laws for Recursion

This Appendix deals with correctness of the laws (rec1)-(rec6) The first two need few justification. Law (rec1) states that bound variables can be renamed if no additional bindings are introduced. Law (rec2) is immediate from the structure of the operational rules for recursion. A central law, on the other hand, is (rec3). This law, also known as the recursive specification principle, states that certain types of equations possess a unique solution. We develop a detailed correctness proof for (rec3) closely following the proof of congruence with respect to rec (Appendix A). Afterwards we focus on (rec4)-(rec6) that are specific for the treatment of divergence in the presence of maximal progress. We will make use of a similar 'up to' technique but we use a slightly different definition of observational congruence up to $\approx^{\perp}$. Instead of introducing a different name we abuse notation for the remainder of this chapter and redefine observational congruence up to $\approx^{\perp}$ as follows.

Definition B.1 Let $\mathcal{S}$ be a symmetric relation on $\mathsf{STP}^{\perp}$. Thus, $\mathcal{T} = (\mathcal{S} \cup \approx^{\perp})^*$ is an equivalence relation. $\mathcal{S}$ is an observational congruence up to $\approx^{\perp}$ iff $P\ \mathcal{S}\ Q$ implies for all $a \in Act$, $C \in \mathsf{STP}^{\perp}/\mathcal{T}$ and $P' \in \mathsf{STP}^{\perp}$ that

1. $P \stackrel{a}{\Longrightarrow} P'$ implies $Q \stackrel{a}{\Longrightarrow} Q'$ and $P' {\approx^{\perp}} R_1\ \mathcal{S}\ R_2 {\approx^{\perp}} Q'$ for some $R_1, R_2, Q' \in \mathsf{STP}^{\perp}$,
2. $P{\surd\downarrow}$ (or $Q{\surd\downarrow}$) implies $\gamma(P, C) = \gamma(Q, C)$,
3. If $\mathcal{P}$ is a $(\mathcal{S} \cup \approx^{\perp})$–path and $\mathcal{P}_1{\surd\downarrow}$ then there is some $(\mathcal{S} \cup \approx^{\perp})$–path $\mathcal{P}'$ such that $\mathcal{P}'_1 \equiv \mathcal{P}_1$, $\forall i \in \{1, \ldots, l(\mathcal{P}')\} : \mathcal{P}'_i{\surd\downarrow}$, and $\mathcal{P}_{l(\mathcal{P})} \stackrel{\tau}{\longrightarrow}^* \mathcal{P}'_{l(\mathcal{P}')}$,
4. $P{\surd\downarrow}$ iff $Q{\surd\downarrow}$.

Lemma B.2 If $\mathcal{S}$ is an observational congruence up to $\approx^{\perp}$, then $\mathcal{S} \subseteq \stackrel{c}{\approx}^{\perp}$.

Proof: The strategy is analogous to that in Appendix A. Apart from proving that $\mathcal{T} = (\mathcal{S} \cup \approx^{\perp})^*$ is a weak bisimulation the proof follows the lines of that for Lemma A.6.

Let $P\ \mathcal{T}\ Q$. Condition (1) of Lemma 2.7 directly follows from the fact that if $P \stackrel{a}{\Longrightarrow} P'$ and $\mathcal{P}$ is an $(\mathcal{S} \cup \approx^{\perp})$–path with $\mathcal{P}_1 \equiv P$ and $\mathcal{P}_{l(\mathcal{P})} \equiv Q$ then there is some $(\mathcal{S} \cup \approx^{\perp})$–path $\mathcal{Q}$ such that $\mathcal{Q}_1 \equiv P'$ and $Q \stackrel{\widehat{a}}{\Longrightarrow} \mathcal{Q}_{l(\mathcal{Q})}$. To prove this observation requires a simple induction on $l(\mathcal{P})$ using condition (1) of Definition B.1.

In order to show condition (2) of Lemma 2.7 we use properties (2) and (3) of Definition B.1 as follows. Let $P\,\mathcal{T}\,Q$ and $P{\surd\downarrow}$ and let $\mathcal{P}$ be an $(\mathcal{S} \cup \approx^{\perp})$–path satisfying $\mathcal{P}_1 \equiv P$ and $\mathcal{P}_{l(\mathcal{P})} \equiv Q$. (3) implies the existence of some $(\mathcal{S} \cup \approx^{\perp})$–path $\mathcal{P}'$ such that $\mathcal{P}'_1 \equiv P$, $\forall i \in \{1, \ldots, l(\mathcal{P}')\} : \mathcal{P}'_i{\surd\downarrow}$, and $Q \stackrel{\tau}{\longrightarrow}^* \mathcal{P}'_{l(\mathcal{P}')}$. Using (2) of Definition B.1 we can show $\gamma(P, C) = \gamma(\mathcal{P}'_i, C)$ for every $i \in \{1, \ldots, l(\mathcal{P}')\}$ and $C \in \mathsf{STP}^{\perp}/\mathcal{T}$ by induction on i. □

Lemma B.3 Let $E \in \mathsf{STC}^{\perp}$ and $P, Q \in \mathsf{STP}^{\perp}$, with X strongly guarded in E and $\mathit{Var}(E) \subseteq \{X\}$. Furthermore, suppose $P \stackrel{c}{\approx}^{\perp} E\{P/X\}$ and $Q \stackrel{c}{\approx}^{\perp} E\{Q/X\}$ and define the relation $\mathcal{R} = \{(G\{P/X\}, G\{Q/X\}) \mid \mathit{Var}(G) \subseteq \{X\}\}$. Then the relation $\mathcal{S} = (\mathcal{R} \cup \mathcal{R}^{-1})$ is an observational congruence up to $\approx^{\perp}$.

Proof: We have to check conditions (1) - (4) of Definition B.1. For symmetry reasons it is sufficient to restrict ourselves to pairs contained in $\mathcal{R}$. We let $\mathcal{T}$ denote $(\mathcal{S} \cup \approx^{\perp})^*$. The proof of (1) is a slight adaption of the one in [30, Prop.13].

(2): Let $\mathit{Var}(G) \subseteq \{X\}$ and $G\{P/X\}, G\{Q/X\}{\surd\downarrow}$. We have to show

$$\forall C \in \mathsf{STP}^{\perp}/\mathcal{T}\ :\ \gamma(G\{P/X\}, C) = \gamma(G\{Q/X\}, C).$$

We fix some $C \in \mathsf{STP}^{\perp}/\mathcal{T}$. We first prove the following weaker property (2').

If X is strongly guarded in G and $Var(G) \subseteq \{X\}$ then $\gamma(G\{P/X\}, C') = \gamma(G\{Q/X\}, C')$ for every $C' \in \mathsf{STP}^\perp/\mathcal{T}$.

Since X is weakly guarded in G, Lemma A.7 and A.9 implies that for each transition $G\{P/X\} \overset{\lambda,w}{\dashrightarrow} G'\{P/X\}$ there is a unique corresponding transition $G\{Q/X\} \overset{\lambda,w}{\dashrightarrow} G'\{Q/X\}$ and vice versa. Since $G'\{P/X\}\ \mathcal{S}^*\ G'\{Q/X\}$, we obtain $\gamma(G\{P/X\}, D) = \gamma(G\{Q/X\}, D)$ for every $D \in \mathsf{STP}^\perp/\mathcal{S}^*$. This in turn implies (2'), because of $\mathcal{S}^* \subseteq \mathcal{T}$ and Lemma A.2.

Concerning (2) we can derive from $P \overset{c}{\approx}{}^\perp E\{P/X\}$, $Q \overset{c}{\approx}{}^\perp E\{Q/X\}$ that $G\{P/X\} \overset{c}{\approx}{}^\perp G\{E/X\}\{P/X\}$ as well as $G\{Q/X\} \overset{c}{\approx}{}^\perp G\{E/X\}\{Q/X\}$. Because of $\approx^\perp \subseteq \mathcal{T}$ and Lemma A.2 we have $\gamma(G\{P/X\}, C) = \gamma(G\{E/X\}\{P/X\}, C)$ and $\gamma(G\{Q/X\}, C) = \gamma(G\{E/X\}\{Q/X\}, C)$. Since X is strongly guarded in $G\{E/X\}$ we can apply (2') to obtain $\gamma(G\{E/X\}\{P/X\}, C) = \gamma(G\{E/X\}\{Q/X\}, C)$ implying (2).

(3): We show the following generalisation (3').

Let $\mathcal{P}$ be a $(\mathcal{S} \cup \approx^\perp)$–path such that $\mathcal{P}_1 \xrightarrow{\tau}{}^* P'\surd\!\downarrow$. Then there is some $(\mathcal{S} \cup \approx^\perp)$–path $\mathcal{P}'$ such that $\mathcal{P}'_1 \equiv P'$, $\mathcal{P}_{l(\mathcal{P})} \xrightarrow{\tau}{}^* \mathcal{P}'_{l(\mathcal{P}')}$ and $\mathcal{P}'_i\surd\!\downarrow$ for every $i \in \{1, \ldots, l(\mathcal{P}')\}$.

W.l.o.g., assume that for every $i \in \{1, \ldots, l(\mathcal{P})\}$ it holds that if $\mathcal{P}_i \not\approx^\perp \mathcal{P}_{i+1}$ there is some H satisfying

$$\mathcal{P}_i \equiv H\{P/X\}\ \wedge\ \mathcal{P}_{i+1} \equiv H\{Q/X\}\ \wedge\ X \text{ strongly guarded in } H. \tag{7}$$

(This can be achieved by replacing all subpaths in $\mathcal{P}$ of the form $(G\{P/X\},\ G\{Q/X\})$ satisfying $G\{P/X\} \not\approx^\perp G\{Q/X\}$ but where X appears not strongly guarded in G by subpaths of the form $(G\{P/X\},\ G\{E/X\}\{P/X\},\ G\{E/X\}\{Q/X\},\ G\{Q/X\})$.) We prove (3') by an induction on $l(\mathcal{P})$. The base case $l(\mathcal{P}) = 0$ is trivial. We distinguish two cases.

If $\mathcal{P}_1 \approx^\perp \mathcal{P}_2$ then $\mathcal{P}_1 \xrightarrow{\tau}{}^* P'$ implies that there is some R'' such that $\mathcal{P}_2 \xrightarrow{\tau}{}^* R''\ \wedge\ P' \approx^\perp R''$. From $P'\surd\!\downarrow$ and $P' \approx^\perp R''$ we obtain that there is some R' such that $R'' \xrightarrow{\tau}{}^* R'\surd\!\downarrow$. Now, $P' \approx^\perp R''$ and $P'\surd$ implies $P' \approx^\perp R'$. We have thus obtained $\mathcal{P}_2 \xrightarrow{\tau}{}^* R'\surd\!\downarrow$. Applying the induction hypothesis to the path $\mathcal{P}^{(2)}$ and the chain of transitions $\mathcal{P}_2 \xrightarrow{\tau}{}^* R'$ returns a path $\mathcal{P}''$ satisfying the conditions of (3'). Thus $\mathcal{P}' = (P', R')\,\mathcal{P}''$ is a path as required in (3').

If, otherwise, $\mathcal{P}_1 \not\approx^\perp \mathcal{P}_2$ holds, (7) says that there is some $H \in \mathsf{STC}^\perp$ such that $\mathcal{P}_1 \equiv H\{P/X\}$, $\mathcal{P}_2 \equiv H\{Q/X\}$ and X strongly guarded in H. Iterative application of Lemma A.7 and A.9 to the chain of transitions $\mathcal{P}_1 \xrightarrow{\tau}{}^* P'$ leads to some R' such that $\mathcal{P}_2 \xrightarrow{\tau}{}^* R'\ \wedge\ P'\ \mathcal{S}\ R'$. Anticipating that we will show below that (4) of Definition B.1 holds, $P'\surd\!\downarrow$ and $P'\ \mathcal{S}\ R'$ implies $R'\surd\!\downarrow$. We can therefore apply the induction hypothesis to the path $\mathcal{P}^{(2)}$ and the chain of transitions $\mathcal{P}_2 \xrightarrow{\tau}{}^* R'\surd\!\downarrow$. We obtain a path $\mathcal{P}''$ such that $\mathcal{P}' = (P', R')\,\mathcal{P}''$ satisfies the requirements of (3').

(4): It holds $G\{P/X\}\surd\!\downarrow$ iff $G\{E/X\}\{P/X\}\surd\!\downarrow$ (since $G\{P/X\} \stackrel{c}{\approx}^{\perp} G\{E/X\}\{P/X\}$) iff $G\{E/X\}\{Q/X\}\surd\!\downarrow$ (since X is strongly guarded in $G\{E/X\}$, using Lemma A.7, A.9, A.10 and A.11) iff $G\{Q/X\}\surd\!\downarrow$ (since $G\{E/X\}\{Q/X\} \stackrel{c}{\approx}^{\perp} G\{Q/X\}$). This completes the proof of Lemma B.3. □

Lemma B.4 Let $E \in \mathsf{STC}^{\perp}$ and $P, Q \in \mathsf{STP}^{\perp}$, X strongly guarded in E and $Var(E) \subseteq \{X\}$. If $P \stackrel{c}{\approx}^{\perp} E\{P/X\}$ and $Q \stackrel{c}{\approx}^{\perp} E\{Q/X\}$ then $P \stackrel{c}{\approx}^{\perp} Q$.

Proof: We obtain $P \stackrel{c}{\approx}^{\perp} Q$ by applying Lemma B.2 to the relation $\mathcal{R}$ appearing in Lemma B.3 where we choose G to be the variable X. □

Lemma B.5 Let $E \in \mathsf{STC}^{\perp}$ and $P \in \mathsf{STP}^{\perp}$, X strongly guarded in E and $Var(E) \subseteq \{X\}$. If $P \stackrel{c}{\approx}^{\perp} E\{P/X\}$ then $P \stackrel{c}{\approx}^{\perp} \mathrm{rec}X.E$.

Proof: $Var(E) \subseteq \{X\}$ implies $\mathrm{rec}X.E \in \mathsf{STP}^{\perp}$ and soundness of (rec2) assures $\mathrm{rec}X.E \stackrel{c}{\approx}^{\perp} E\{\mathrm{rec}X.E/X\}$. We can therefore use Lemma B.4 (with $Q \equiv \mathrm{rec}X.E$) to deduce $P \stackrel{c}{\approx}^{\perp} \mathrm{rec}X.E$. □

Definition 2.9 implies that this lemma holds also for arbitrary expressions in $\mathsf{STC}^{\perp}$.

After having shown soundness of (rec3) we now turn our attention towards the remaining laws of recursion that are specific for the treatment of divergence. We will discuss (rec5) in some detail in order to give some insight into the proof. The proofs for (rec4) and (rec6) are instances of the same proof technique and will therefore be only sketched.

In the sequel let $E \in \mathsf{STC}^{\perp}$. To prove correctness of (rec5) we have to show that $P \stackrel{c}{\approx}^{\perp} Q$ where $P \equiv \mathrm{rec}X.(\tau.X + E)$ and $Q \equiv \mathrm{rec}X.(\tau.(\perp + E))$. Definition 2.9 enables us to restrict ourselves to the case where $Var(E) \subseteq \{X\}$. We now define the following relations $\mathcal{R}_0$, $\mathcal{R}_1$, $\mathcal{R}$, $\mathcal{S}$ and $\mathcal{B}$

- $\mathcal{R}_0 = \{(H\{P/X\},\ H\{Q/X\}) \mid Var(H) \subseteq \{X\}\}$
- $\mathcal{R}_1 = \{(P,\ \perp + E\{Q/X\})\}$
- $\mathcal{S} = \mathcal{R}_0 \cup \mathcal{R}_0^{-1} \cup \mathcal{R}_1 \cup \mathcal{R}_1^{-1}$
- $\mathcal{B} = \mathcal{S}^*$

In order to show that $\mathcal{B}$ is a weak bisimulation we use the following lemma.

Lemma B.6 If $F\ \mathcal{S}\ G$ then

1. $F \xrightarrow{a} F'$ implies
   - $F\ (\mathcal{R}_0 \cup \mathcal{R}_0^{-1})\ G \quad \Rightarrow \quad \exists G'\ (G \stackrel{a}{\Longrightarrow} G' \ \wedge\ F'\ \mathcal{S}\ G')$
   - $F\ (\mathcal{R}_1 \cup \mathcal{R}_1^{-1})\ G \quad \Rightarrow \quad \exists G'\ (G \stackrel{\widehat{a}}{\Longrightarrow} G' \ \wedge\ F'\ \mathcal{S} G')$
2. $F\surd\!\downarrow$ and $G\surd\!\downarrow$ imply $\forall C \in \mathsf{STP}^{\perp}/\mathcal{B}\ :\ \gamma(F, C) = \gamma(G, C)$

Proof: (Sketch) In order to proof (1), first the case $F\ (\mathcal{R}_0 \cup \mathcal{R}_0^{-1})\ G$ has to be dealt by an induction on the height of the proof tree for the transition $F \xrightarrow{a} F'$. The case $F\ (\mathcal{R}_1 \cup \mathcal{R}_1^{-1})\ G$ follows then easily.

(2) can be proven by an induction on the sum of the heights of all proof trees for $\dashrightarrow$ transitions emanating F. Note that the case $F\ (\mathcal{R}_1 \cup \mathcal{R}_1^{-1})\ G$ is trivial since the premise $F\surd\!\downarrow$ and $G\surd\!\downarrow$ is not satisfied in this case. The details of proof can be found in [28]. □

Lemma B.7 $\mathcal{B}$ is a weak bisimulation.

Proof: Let $E\ \mathcal{B}\ F$, i.e. there is some $n \geq 0$ with $E\,\mathcal{S}^n\,F$. We have to check condition (1) and (2) of Lemma 2.7.

(1): Let $E \xrightarrow{a} E'$. We prove the existence of some F' with $F \stackrel{\widehat{a}}{\Longrightarrow} F'$ and $E'\ \mathcal{B}\ F'$ by induction on n. The base case, $n = 0$, is trivial. So, let $n > 0$, i.e. there is some $G \in \mathsf{STP}^{\perp}$ satisfying $E\ \mathcal{S}^{n-1}\ G\ \mathcal{S}\ F$. Applying our induction hypotheses to (E, G) we obtain some G' such that $G \stackrel{\widehat{a}}{\Longrightarrow} G' \ \wedge\ E'\ \mathcal{B}\ G'$. If $a = \tau$ and $G \equiv G'$ we can choose the transition $F \stackrel{\widehat{\tau}}{\Longrightarrow} F' \equiv F$ for F. Otherwise $G \stackrel{a}{\Longrightarrow} G'$ holds. Iterative application of property (1) of Lemma B.6 leads to some F' such that $F \stackrel{\widehat{a}}{\Longrightarrow} F' \ \wedge\ G'\ \mathcal{S} F'$. As a whole we have $E'\ \mathcal{B}\ F'$.

(2): Let $E\surd\!\downarrow$. Since $E\,\mathcal{S}^n\,F$, there are E_i such that $E \equiv E_1\,\mathcal{S}\,E_2\,\mathcal{S} \ldots \mathcal{S}\,E_n \equiv F$. We claim that $E_i\surd\!\downarrow$ for every $i \in \{1, \ldots, n\}$ and show this by an induction on n. The base case $n = 1$ is clear by assumption. So let $n > 1$. Our induction hypotheses implies $E_{n-1}\surd\!\downarrow$. Therefore, the case $E_{n-1}(\mathcal{R}_1 \cup \mathcal{R}_1^{-1})E_n$ is impossible. Assume $E_{n-1}\ \mathcal{R}_0\ E_n$, i.e. $(E_{n-1}, E_n) = (H\{P/X\}, H\{Q/X\})$ and thus $H\{P/X\}\surd\!\downarrow$. Since $P\not\surd$, Lemma A.8 implies that X is weakly guarded in H. Using Lemma A.7, A.9, A.10 and A.11 we obtain $H\{Q/X\}\surd\!\downarrow$. The case $E_{n-1}\ \mathcal{R}_0^{-1}\ E_n$ proceeds analogously.

Having shown that $E_i\surd\!\downarrow$ holds for all $i \in \{1, \ldots, n\}$ we deduce from Lemma B.6 that $F\surd\!\downarrow \ \wedge\ \forall C \in \mathsf{STP}^{\perp}/\mathcal{B}\ :\ \gamma(E, C) = \gamma(F, C)$. This obviously is a special case of condition (2) of Lemma 2.7. □

Now we are able to show soundness of (rec5).

Lemma B.8 $P \equiv \mathrm{rec}X.(\tau.X + E) \stackrel{c}{\approx}^{\perp} \mathrm{rec}X.(\tau.(\perp + E)) \equiv Q$.

Proof: We have to show that condition (1) to (4) of Definition 2.8 are satisfied.

(1): Let $P \equiv \mathrm{rec}X.(\tau.X + E) \xrightarrow{a} P'$ which implies $\tau.P + E\{P/X\} \xrightarrow{a} P'$. If $\tau.P \xrightarrow{a} P'$ then $a = \tau$ and $P' \equiv P$. We can choose $Q \equiv \mathrm{rec}X.(\tau.(\perp + E)) \xrightarrow{\tau} \perp + E\{Q/X\}$ as a transition for Q because Lemma B.7 implies $P \approx^{\perp} \perp + E\{Q/X\}$.

If, otherwise, $E\{P/X\} \xrightarrow{a} P'$ Lemma B.6 assures that there is some Q' such that $E\{Q/X\} \stackrel{a}{\Longrightarrow} Q' \ \wedge\ P'\ \mathcal{S}\ Q'$, i.e. $P'\ \mathcal{B}\ Q'$. Lemma B.7 implies $P' \approx^{\perp} Q'$. Hence, as expected, $Q \equiv \mathrm{rec}X.(\tau.(\perp + E)) \xrightarrow{\tau} \perp + E\{Q/X\} \stackrel{a}{\Longrightarrow} Q'$.

(2): Let $Q \equiv \text{rec}X.(\tau.(\perp + E)) \xrightarrow{a} Q'$ which implies $\tau.(\perp + E\{Q/X\}) \xrightarrow{a} Q'$. Hence, $a = \tau$ and $Q' \equiv \perp + E\{Q/X\}$. We choose the transition $P \equiv \text{rec}X.(\tau.X + E) \xrightarrow{\tau} P$ for P because Lemma B.7 assures $\perp + E\{Q/X\} \approx^{\perp} P$.

This completes the proof, because $P \not\surd$ and $Q \not\surd$ directly imply (3) and (4) of Definition 2.8. $\square$

The proof of soundness for law (rec6) follows the same lines but uses the relation $\mathcal{R}_1 = \{(\sum_{i=1}^{n} P + E\{P/X\},\, Q)\}$, where $P \equiv \text{rec}X.(\tau.(\sum_{i=1}^{n} X + E) + F)$ and $Q \equiv \text{rec}X.(\tau.X + E + F)$.

The proof of soundness of law (rec5) can also be directly adopted to prove law (rec4). In this case $\mathcal{R}_1 = \{(P + E\{P/X\},\, \perp + E\{Q/X\})\}$ where $P \equiv \text{rec}X.(X + E)$ and $Q \equiv \text{rec}X.(\perp + E)$.

C Observational Congruence on open expressions

In order to show property (i) to (v) appearing in the proof of Theorem 3 we require a characterisation of $\approx^{\perp}$ on open expressions.

Lemma C.1 $E \approx^{\perp} F$ holds iff E and F are contained in an equivalence relation $\mathcal{B} \subseteq \mathsf{STC}^{\perp} \times \mathsf{STC}^{\perp}$, such that $(E', F') \in \mathcal{B}$ iff for all $a \in Act$ and $X \in Var$ it holds that

1. $E \xrightarrow{a} E'$ implies $F \xRightarrow{\hat{a}} F'$ and $E' \,\mathcal{B}\, F'$ for some $F' \in \mathsf{STC}^{\perp}$,
2. X not weakly guarded in E implies $F \xrightarrow{\tau}{}^{*} F'$ and X not weakly guarded in F' for some $F' \in \mathsf{STC}^{\perp}$,
3. $E\surd$ implies for some $F' \in \mathsf{STC}^{\perp}$ that $E \xrightarrow{\tau}{}^{*} F'\surd$, $\gamma(E, C) = \gamma(F', C)$ for every $C \in \mathsf{STC}^{\perp}/\mathcal{B}$ and the number of fully unguarded occurrences of Y in E and F, respectively, are equal for every $X \in Var$.

Proof: (Sketch) Call an equivalence relation on $\mathsf{STC}^{\perp}$ that satisfies the condition (1) to (3) of the above lemma an extended weak bisimulation, briefly ewb. We only consider the case $n = 1$, i.e. $Var(E) \cup Var(F) = \{X\}$. First we prove that Lemma 2.7 implies Lemma C.1. Thus, assume $E \approx^{\perp} F$. Let $a \in Act \backslash \{\tau\}$ such that a does not appear in G or H. Define a relation $\mathcal{R}$ by

$$\mathcal{R} = \{(G, H) \mid G\{a.0/X\} \approx^{\perp} H\{a.0/X\} \;\wedge\; a \text{ does not appear in } G \text{ or } H\}$$

Since $E \,\mathcal{R}\, F$ it suffices to prove that $(\mathcal{R} \cup \mathcal{R}^{-1})^{*}$ is an ewb, which is straightforward.

In order to prove the converse direction (that Lemma C.1 implies Lemma 2.7), assume that $\mathcal{B}'$ is an ewb such that $E \,\mathcal{B}'\, F$. Then it can be shown that the relation $(\mathcal{R} \cup \mathcal{R}^{-1})^{*}$ where

$$\mathcal{R} = \{(G\{P/X\}, H\{P/X\}) \mid G \,\mathcal{B}\, H \text{ for some ewb } \mathcal{B}, P \in \mathsf{STP}^{\perp}, Var(G) \cup Var(H) \subseteq \{X\}\}.$$

is a weak bisimulation. Since $E\{P/X\} \;\mathcal{R}\; F\{P/X\}$ for every $P \in \mathsf{STP}^{\perp}$ this implies $E \approx^{\perp} F$. $\square$

References

[1] L. Aceto and A. Jeffrey. A Complete Axiomatization of Timed Bisimulation for a Class of Timed Regular Behaviours. *Theoretical Computer Science* 152:251-268, 1995.

[2] H. R. Andersen and M. Mendler. Describing a Signal Analyzer in the Process Algebra PMC — A Case Study. In Proceedings *TAPSOFT 95*, Springer LNCS 915:620-635.

[3] A. Aziz, K. Sanwal, V. Singhal, and R.K. Brayton. *Verifying Continuous Time Markov Chains*. In Proceedings *CAV 96*, Springer LNCS 1102:269-276,1996.

[4] J.C.M. Baeten and J.A. Bergstra. Real Time Process Algebra. *Formal Aspects of Computing* 3:142-188, 19991.

[5] J.C.M. Baeten, J.A. Bergstra, and J.W. Klop. Syntax and Defining Equations for an Interrupt Mechanism in Process Algebra. *Fundamenta Informaticae* IX:127-168, 1986.

[6] J.C.M. Baeten, J.A. Bergstra, and J.W. Klop. On the Consistency of Koomen's Fair Abstraction Rule. *Theoretical Computer Science* 51:129-176, 1987.

[7] J.A. Bergstra, J.W. Klop, and E.-R. Olderog. Failures Without Chaos: A New Process Semantics for Fair Abstraction. In *Formal Description of Programming Concepts - III.* Elsevier Science Publisher B.V., 1987.

[8] M. Bernardo and R. Gorrieri. Extended Markovian Process Algebra. In Proceedings *CONCUR 96*, Springer LNCS 1119:315-330, 1996.

[9] E. Brinksma, A. Rensink, and W. Vogler. Fair Testing. In Proceedings *CONCUR 95*, Springer LNCS 962:313-327, 1995.

[10] J. Camilieri and G. Winskel. CCS with Priority Choice. *Information and Computation* 116:26-37,1995.

[11] R. Cleaveland and M. Hennessy. Priorities in Process Algebra. *Information and Computation* 87:58-77,1990.

[12] R. Cleaveland, G. Lüttgen, and M. Mendler. An Algebraic Theory of Multiple Clocks. In Proceedings *CONCUR 97*, Springer LNCS 1243:166-180, 1997.

[13] R. Cleaveland, G. Lüttgen, and V. Natarjan. A Process Algebra with Distributed Priorities. In Proceedings *CONCUR 96*, Springer LNCS 1119:34-49,1996.

[14] W. Feller.*An Introduction to Probability Theory and Its Applications.* John Wiley & Sons, 1968.

[15] W. Fokkink. An Axiomatization for Regular Processes in Timed Branching Bisimulation. Accepted for *Fundamenta Informaticae.*

[16] R. Gerber and I. Lee. A Resource-Based Prioritized Bisimulation for Real-Time Systems. *Information and Computation*, 113:102-142, 1994.

[17] R.J. van Glabbeek A Complete Axiomatization for Branching Bisimulation Congruence of Finite-State Behaviours. In Proceedings *MFCS 93*, Springer LNCS 711:473-484, 1993.

[18] R. van Glabbeek and W. Weijland. Branching Time and Abstraction in Bisimulation Semantics. *Journal of the ACM* 43(3):555-600,1996.

[19] R.J. van Glabbeek, S.A. Smolka, and B. Steffen. Reactive, Generative, and Stratified Models of Probabilistic Processes. *Information and Computation* 121:59-80, 1995.

[20] N. Götz, U. Herzog, and M. Rettelbach. Multiprocessor and distributed system design: The integration of functional specification and performance analysis using stochastic process algebras. In Proceedings *PERFORMANCE 93*, Springer LNCS 729: 1993.

[21] H. Hansson and B. Jonsson. A Calculus of Communicating Systems with Time and Probability. In Proceedings *RTSS 90*, IEEE-CS Press, 1990.

[22] M. Hennessy and G.D. Plotkin. *A term model for CCS.* In Proceedings *MFCS 80*, Springer LNCS 88:261-274.

[23] M. Hennessy and T. Regan. A process algebra for timed systems. *Information and Computation*, 117(2):221-239, 1995.

[24] H. Hermanns, M. Rettelbach, and T. Weiß. Formal Characterisation of Immediate Actions in an SPA with Non-Deterministic Branching. *The Computer Journal*, 38(7):530-541 1995.

[25] H. Hermanns, U. Herzog, and V. Mertsiotakis. Stochastic Process Algebras – Between LOTOS and Markov Chains. To appear in *Computer Networks and ISDN Systems.*

[26] J. Hillston. A Compositional Approach to Performance Modelling. PhD thesis, University of Edinburgh, 1994.

[27] K.G. Larsen and A. Skou. Bisimulation through Probabilistic Testing. *Information and Computation* 94:1-28, 1991.

[28] M. Lohrey. Vollständige Axiomensysteme für eine Prozeßalgebra mit probabilistischen, Markovschen und instantanen Elementen. Diplomarbeit, IMMD7, Universität Erlangen, 1996.

[29] C.J. Koomen. Algebraic Specification and Verification of Communication Protocols. *Science of Computer Programming* 5:1-36, 1985.

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

[31] R. Milner. A Complete Axiomatization for Observational Congruence of Finite-State Behaviours. *Information and Computation* 81:227-247, 1989.

[32] F. Moller and C. Tofts. A Temporal Calculus of Communicating Systems. In Proceedings *CONCUR 90*, Springer LNCS 458:401-415, 1990.

[33] V. Natarjan and R. Cleaveland. Divergence and Fair Testing. In Proceedings *ICALP 95*, Springer LNCS 944:648-659, 1995.

[34] V. Natarajan, I.Christoff, and L.Christoff, R.Cleaveland. Priorities and Abstraction in Process Algebra. In Proceedings *FST&TCS 94*, Springer LNCS 880:217-230, 1994.

[35] X. Nicollin and J. Sifakis. An Overview and Synthesis on Timed Process Algebras. In *Real-Time: Theory in Practice*, Springer LNCS 600, 1991.

[36] X. Nicollin and J. Sifakis. The Algebra of Timed Processes ATP: Theory and Application. *Information and Computation* 114:131-178, 1991.

[37] D. Sangiorgi and R. Milner. The problem of 'weak bisimulation up to'. In Proceedings *CONCUR 92*, Springer LNCS 630:32-46, 1992.

[38] S. Smolka and B. Steffen. Priority as Extremal Probability. *Formal Aspects of Computing* 8:585-606, 1996.

[39] W.J. Stewart. *Introduction to the Numerical Solution of Markov Chains*. Princeton University Press, 1994.

[40] G.M. Reed and A.W. Roscoe. A Timed Model for Communicating Sequential Processes. *Theoretical Computer Science* 58:249-261, 1988.

[41] D.J. Walker. Bisimulation and Divergence. *Information and Computation* 85:202-241, 1990.

[42] W. Yi. Real-time Behaviour of Asynchronous Agents. In Proceedings *CONCUR 90*, Springer LNCS 458:502-520, 1990.

[43] W. Yi. CCS + Time = An Interleaving Model for Real Time Systems. In Proceedings *ICALP 91*, Springer LNCS 510:217-228, 1991.