BRICS

Basic Research in Computer Science

A Complete Equational Axiomatization for Prefix Iteration with Silent Steps

Luca Aceto
Anna Ingólfsdóttir

BRICS Report Series **RS-95-5**

ISSN 0909-0878 **January 1995**

Copyright © 1995, BRICS, Department of Computer Science University of Aarhus. All rights reserved.

Reproduction of all or part of this work is permitted for educational or research use on condition that this copyright notice is included in any copy.

See back inner page for a list of recent publications in the BRICS Report Series. Copies may be obtained by contacting:

BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK - 8000 Aarhus C
Denmark

Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@daimi.aau.dk

A Complete Equational Axiomatization for Prefix Iteration with Silent Steps

Luca Aceto* Anna Ingólfsdóttir†

BRICS‡
Department of Mathematics and Computer Science
Aalborg University
Fredrik Bajersvej 7E
9220 Aalborg Ø, Denmark

Abstract

Fokkink ((1994) *Inf. Process. Lett.* **52**: 333–337) has recently proposed a complete equational axiomatization of strong bisimulation equivalence for $\mathrm{MPA}^*_\delta(A_\tau)$, i.e., the language obtained by extending Milner's basic CCS with prefix iteration. Prefix iteration is a variation on the original binary version of the Kleene star operation p^*q obtained by restricting the first argument to be an atomic action. In this paper, we extend Fokkink's results to a setting with the unobservable action τ by giving a complete equational axiomatization of Milner's observation congruence over $\mathrm{MPA}^*_\delta(A_\tau)$. The axiomatization is obtained by extending Fokkink's axiom system with two of Milner's standard τ-laws and the following three equations that describe the interplay between the silent nature of τ and prefix iteration:

$$\begin{array}{rcl} \tau.x & = & \tau^*x \\ a^*(x+\tau.y) & = & a^*(x+\tau.y+a.y) \\ \tau.(a^*x) & = & a^*(\tau.a^*x) \ . \end{array}$$

Using a technique due to Groote, we also show that the resulting axiomatization is ω-complete, i.e., complete for equality of open terms.

AMS Subject Classification (1991): 68Q40, 68Q42.
CR Subject Classification (1991): D.3.1, F.3.2, F.4.2.
Keywords and Phrases: Minimal Process Algebra, prefix iteration, equational logic, ω-completeness, observation congruence.

1 Introduction

The research literature on process theory has recently witnessed a resurgence of interest in the study of Kleene star-like operations (cf., e.g., the papers [11, 3, 9, 8, 23, 7]).

*On leave from the School of Cognitive and Computing Sciences, University of Sussex, Brighton BN1 9QH, UK. Partially supported by HCM project EXPRESS. Email: luca@iesd.auc.dk.

†Partially supported by a grant from the Danish Research Council. Email: annai@iesd.auc.dk.

‡Basic Research in Computer Science, Centre of the Danish National Research Foundation.

Some of these studies, notably [3], have studied the expressive power of variations on standard process description languages in which infinite behaviours are defined by means of Kleene's star operation [17, 6] rather than by means of systems of recursion equations. Some others (see, e.g., [11, 23, 9, 10]) have investigated the possibility of giving finite equational axiomatizations of strong bisimulation equivalence [21, 19] over simple process algebras that include variations on Kleene's star operation. De Nicola and his co-workers have instead focused on the study of tree-based models for what they call "nondeterministic Kleene algebras", and on the proof systems these models support to reason about regular expressions and more expressive languages built on top of those; see, e.g., [8, 7] for details on this line of research.

This paper aims at giving a contribution to the study of complete equational axiomatizations for Kleene star-like operations from the point of view of process theory. Our starting point is the work presented in [9]. In that reference, Fokkink has proposed a complete equational axiomatization of strong bisimulation equivalence for $\mathbf{MPA}^*_\delta(A_\tau)$, i.e., the language obtained by extending the fragment of Milner's CCS [20] containing the basic operations needed to express finite synchronization trees with prefix iteration. Prefix iteration is a variation on the original binary version of the Kleene star operation p^*q [17] obtained by restricting the first argument to be an atomic action. Intuitively, at any time the process term μ^*p can decide to perform action μ and evolve to itself, or an action from p, after which it exits the μ-loop. The behaviour of μ^*p is captured very clearly by the rules that give its Plotkin-style structural operational semantics:

$$\frac{}{\mu^*p \xrightarrow{\mu} p} \qquad \frac{p \xrightarrow{\gamma} p'}{\mu^*p \xrightarrow{\gamma} p'}$$

Equationally, as shown by Fokkink, such an operation can be completely characterized by the following two natural laws:

$$\begin{aligned} \mu.(\mu^*x) + x &= \mu^*x \\ \mu^*(\mu^*x) &= \mu^*x \end{aligned}$$

The reader familiar with Hennessy's work on complete axiomatizations for the delay operation of Milner's SCCS [13, 14] will have noticed the similarity between the above laws and those presented in [13] (see also [2, Page 40]). This is not surprising as such a delay operation is nothing but an instance of the prefix iteration construct studied by Fokkink.

In this paper, we extend Fokkink's results to a setting with the unobservable action τ by giving a complete equational axiomatization of Milner's observation congruence [20] over $\mathbf{MPA}^*_\delta(A_\tau)$. The axiomatization is obtained by extending Fokkink's axiom system with two of Milner's standard τ-laws and the following three laws that describe the interplay between the silent nature of τ and prefix iteration:

$$\begin{aligned} \tau.x &= \tau^*x \\ a^*(x + \tau.y) &= a^*(x + \tau.y + a.y) \\ \tau.(a^*x) &= a^*(\tau.a^*x) \ . \end{aligned}$$

The first of these equations was introduced in [3] under the name of *Fair Iteration Rule*, and expresses a fundamental property of observation congruence, namely the abstraction from τ-loops, that underlies the soundness of *Koomen's Fair Abstraction Rule* [4]. The other two equations are, to the best of our knowledge, new. They describe a rather subtle interplay between prefix iteration and τ, and will play a crucial role in the proof of our completeness theorem. Using a technique due to Groote [12], we also show that the resulting axiomatization is ω-complete, i.e., complete for equality of open terms over the signature of $\mathbf{MPA}^*_\delta(A_\tau)$.

The paper is organized as follows. Section 2 introduces the language of minimal process algebra with prefix iteration, $\mathbf{MPA}^*_\delta(A_\tau)$, and its operational semantics. In that section we also review the definition of observation congruence, and present several properties of this relation that will be used in the remainder of the paper. The set of equations that will be shown to completely characterize observation congruence over $\mathbf{MPA}^*_\delta(A_\tau)$ is analyzed in Sect. 3. Section 4 is entirely devoted to a detailed proof of the completeness of our axiom system with respect to observation congruence over $\mathbf{MPA}^*_\delta(A_\tau)$. The structure of the proof the completeness theorem (Thm. 4.9) follows standard lines in the process algebra literature and bears strong connections with the proofs of results in Hennessy's paper [13]. The details, however, are very different and rather involved. For this reason, we have chosen to present the proof of Thm. 4.9 in full detail to allow the reader to judge its correctness. Finally, we prove in Sect. 5 that our axiomatization is also strong enough to completely characterize observation congruence of open terms over the signature of $\mathbf{MPA}^*_\delta(A_\tau)$.

2 Minimal Process Algebra with Iteration

We assume a countably infinite set A of observable actions not containing the distinguished symbol τ. Following Milner [20], the symbol τ will be used to denote an internal, unobservable action of a system. We define $A_\tau \triangleq A \cup \{\tau\}$, and use a, b to range over A and μ, γ to range over A_τ. We also assume a countable set of process variables Var, ranged over by x, y, w, z.

The language of minimal process algebra with prefix iteration, denoted by $\mathsf{MPA}^*_\delta(A_\tau)$, is given by the following BNF grammar:

$$P ::= x \mid \delta \mid \mu.P \mid P + P \mid \mu^* P$$

where $x \in \mathsf{Var}$ and $\mu \in A_\tau$. We shall use P, Q, T (possibly subscripted and/or superscripted) to range over $\mathsf{MPA}^*_\delta(A_\tau)$. In writing terms over the above syntax, we shall always assume that the operations μ^* and $\mu._$ bind stronger than $+$. We shall use the symbol $\equiv$ to stand for syntactic equality of terms. The set of closed terms, i.e., terms that do not contain occurrences of process variables, generated by the above grammar will be denoted by $\mathbf{MPA}^*_\delta(A_\tau)$. We shall use p, q, r, t, u (possibly subscripted and/or superscripted) to range over $\mathbf{MPA}^*_\delta(A_\tau)$.

The operational semantics for the language $\mathbf{MPA}^*_\delta(A_\tau)$ is given by the labelled transition system [16, 22] $(\mathbf{MPA}^*_\delta(A_\tau), \left\{\xrightarrow{\mu} \mid \mu \in A_\tau\right\})$, where the transition relations $\xrightarrow{\mu}$ are

the smallest subsets of $\mathbf{MPA}^*_\delta(A_\tau) \times \mathbf{MPA}^*_\delta(A_\tau)$ satisfying the rules in Fig. 1. We say that a term $p \in \mathbf{MPA}^*_\delta(A_\tau)$ is *stable* iff $p \xrightarrow{\tau} q$ for no $q \in \mathbf{MPA}^*_\delta(A_\tau)$.

$$\frac{}{\mu.p \xrightarrow{\mu} p} \qquad \frac{p \xrightarrow{\mu} p'}{p + q \xrightarrow{\mu} p'} \qquad \frac{q \xrightarrow{\mu} q'}{p + q \xrightarrow{\mu} q'}$$

$$\frac{}{\mu^* p \xrightarrow{\mu} \mu^* p} \qquad \frac{p \xrightarrow{\mu} p'}{\gamma^* p \xrightarrow{\mu} p'}$$

Figure 1: Transition Rules for $\mathbf{MPA}^*_\delta(A_\tau)$

Following Milner [20], we shall use $\hat{\mu}$ to stand for ε if $\mu = \tau$, and for μ otherwise. The derived transition relations $\stackrel{\varepsilon}{\Rightarrow}$ and $\stackrel{\mu}{\Rightarrow}$ are defined in the standard way as follows:

$$p \stackrel{\varepsilon}{\Rightarrow} q \quad \Leftrightarrow \quad p \xrightarrow{\tau}{}^* q, \text{ where } \xrightarrow{\tau}{}^* \text{ stands for the reflexive, transitive closure of } \xrightarrow{\tau}$$
$$p \stackrel{\mu}{\Rightarrow} q \quad \Leftrightarrow \quad \exists p_1, p_2 : \; p \stackrel{\varepsilon}{\Rightarrow} p_1 \xrightarrow{\mu} p_2 \stackrel{\varepsilon}{\Rightarrow} q \;\; .$$

Definition 2.1 *For $\mu \in A_\tau$ and $p, q \in \mathbf{MPA}^*_\delta(A_\tau)$, we say that q is a μ-*derivative *of p iff $p \stackrel{\mu}{\Rightarrow} q$. The set of μ-derivatives of a term $p \in \mathbf{MPA}^*_\delta(A_\tau)$ will be denoted by $\mathsf{der}(p, \mu)$. For $p, q \in \mathbf{MPA}^*_\delta(A_\tau)$, we say that q is a* derivative *of p iff there exist a natural number $n \geq 0$ and a sequence $p_1 \mu_1 p_2 \ldots \mu_n p_{n+1}$ of terms $p_i \in \mathbf{MPA}^*_\delta(A_\tau)$ and actions $\mu_i \in A_\tau$ such that $p \equiv p_1$, and, for every $1 \leq i \leq n$, $p_{i+1} \in \mathsf{der}(p_i, \mu_i)$.*

The following basic fact can be easily shown by structural induction on terms:

Fact 2.2 *For every $p \in \mathbf{MPA}^*_\delta(A_\tau)$, the set of derivatives of p is finite.*

The notion of equivalence over process terms in $\mathbf{MPA}^*_\delta(A_\tau)$ that will be considered in this study is that of observation congruence [20]. This we now proceed to define for the sake of completeness.

Definition 2.3 (Bisimulation and Observation Equivalence) *A binary relation $\mathcal{R}$ over $\mathbf{MPA}^*_\delta(A_\tau)$ is a* bisimulation *iff it is symmetric and, whenever $p \mathcal{R} q$,*

if $p \xrightarrow{\mu} p'$ then $q \stackrel{\hat{\mu}}{\Rightarrow} q'$ for some q' such that $p' \mathcal{R} q'$.

Two process terms p, q are observation equivalent*, denoted by $p \approx q$, iff there exists a bisimulation $\mathcal{R}$ such that $p \mathcal{R} q$.*

As it is well-known [20], $\approx$ is an equivalence relation over $\mathbf{MPA}^*_\delta(A_\tau)$. However, for the standard reasons explained at length in, e.g., Milner's textbook [20], observation equivalence is not a congruence with respect to the summation operation of $\mathbf{MPA}^*_\delta(A_\tau)$. In fact, it is also the case that $\approx$ is *not* preserved by the prefix iteration operation. As a simple example of this phenomenon, consider the terms $b.\delta$ and $\tau.b.\delta$. As it is well-known, $b.\delta \approx \tau.b.\delta$; however, it is not difficult to check that $a^*(b.\delta) \not\approx a^*(\tau.b.\delta)$. The

largest congruence over $\mathbf{MPA}^*_\delta(A_\tau)$ contained in $\approx$, denoted by $\approx^c$, will be referred to as *observation congruence*, and can be described in the following well-known way:

$$p \approx^c q \quad \Leftrightarrow \quad p + a.\delta \approx q + a.\delta \ \text{ for some } a \in A \text{ not occurring in } p \text{ and } q \ .$$

The following standard characterization of $\approx^c$ will be useful in what follows. The interested reader is invited to consult [20, Chapter 7] for details.

Fact 2.4 *For all $p, q \in \mathbf{MPA}^*_\delta(A_\tau)$, $p \approx^c q$ iff for all $\mu \in A_\tau$,*

1. *if $p \xrightarrow{\mu} p'$, then $q \stackrel{\mu}{\Rightarrow} q'$ for some q' such that $p' \approx q'$;*
2. *if $q \xrightarrow{\mu} q'$, then $p \stackrel{\mu}{\Rightarrow} p'$ for some p' such that $p' \approx q'$.*

Observation congruence can be naturally extended to open terms as follows:

Definition 2.5 *For all $P, Q \in \mathsf{MPA}^*_\delta(A_\tau)$, $P \approx^c Q$ iff $P\sigma \approx^c Q\sigma$ for every substitution $\sigma : \mathsf{Var} \to \mathbf{MPA}^*_\delta(A_\tau)$.*

In the remainder of this paper, we shall make use of several basic properties of the relations of observation congruence and observation equivalence that may mostly be found in [20, Chapter 7]. For ease of reference, we collect these properties in the following lemma.

Lemma 2.6 *For every $p, q \in \mathbf{MPA}^*_\delta(A_\tau)$, the following statements hold:*

1. [Hennessy's Theorem] *$p \approx q$ iff $p \approx^c q$ or $\tau.p \approx^c q$ or $p \approx^c \tau.q$.*
2. *$p \approx q$ implies $\mu.p \approx^c \mu.q$, for all $\mu \in A_\tau$.*
3. *If $p \approx q$ and p, q are stable, then $p \approx^c q$.*
4. *Assume that $a^*p \approx a^*q$. Suppose further that $q \stackrel{\tau}{\Rightarrow} q'$ for some q' such that $a^*p \approx q'$. Then $\tau.a^*p \approx^c q$.*
5. *If $p \approx q + r$, for some $r \in \mathbf{MPA}^*_\delta(A_\tau)$, then $\tau.p \approx^c \tau.p + q$.*

Proof: The proofs of statements 1–3 may be found in [20, Chapter 7]. Statements 4–5 are easy to check using the characterization of $\approx^c$ given in Fact 2.4. □

Definition 2.7 *Let $p \in \mathbf{MPA}^*_\delta(A_\tau)$ and let $\langle a_n \mid n \in \mathbb{N}\rangle$ be an infinite sequence of actions in A. We say that p* exhibits the sequence *$\langle a_n \mid n \in \mathbb{N}\rangle$ iff there exist terms p_n, $n \in \mathbb{N}$, such that $p_0 \equiv p$ and $p_n \stackrel{a_n}{\Rightarrow} p_{n+1}$, for every $n \geq 0$.*

The following small result about the expressivity of the language $\mathbf{MPA}^*_\delta(A_\tau)$ will be useful in the proof of the main result of this paper.

Proposition 2.8

1. *Let $p \in \mathbf{MPA}^*_\delta(A_\tau)$ and let $\langle a_n \mid n \in \mathbb{N}\rangle$ be an infinite sequence of actions in A. Assume that p exhibits the sequence $\langle a_n \mid n \in \mathbb{N}\rangle$. Then this sequence must be eventually constant,* i.e., *there exist $k \in \mathbb{N}$ and $a \in A$ such that $a_n = a$ for all $n \geq k$.*

2. *Let $a, b \in A$ be distinct. Then, for all $p, q \in \mathbf{MPA}^*_\delta(A_\tau)$, $a^*p \not\approx b^*q$.*

Proof: The first statement can be easily shown by structural induction on terms. To prove the second, assume, towards a contradiction, that $a^*p \approx b^*q$. Then there exist terms $p', q' \in \mathbf{MPA}^*_\delta(A_\tau)$ such that:

- $a^*p \stackrel{b}{\Rightarrow} p' \approx b^*q$, and
- $b^*q \stackrel{a}{\Rightarrow} q' \approx a^*p$.

This implies that a^*p and b^*q both exhibit, for example, the infinite sequence $\langle a_n \mid n \in \mathbb{N}\rangle$, where $a_n = a$ for even n, and $a_n = b$ otherwise. This contradicts the first statement of the proposition. □

3 Axiomatization and Soundness

The main aim of this study is to provide a complete equational axiomatization of the relation of observation congruence over the language $\mathbf{MPA}^*_\delta(A_\tau)$. In this section, we present the axiom system that will be shown to completely characterize observation congruence over the language $\mathbf{MPA}^*_\delta(A_\tau)$, and prove its soundness. We also present some derived equations that will be useful in the proof of the promised completeness theorem.

Consider the set $\mathcal{E}$ of equations in Fig. 3. This set of equations contains all of the equational theory $\mathcal{F}$ in Fig. 2. Apart from the law

$$\tau^*(\tau^*x) \quad = \quad \tau^*x$$

which is derivable in the presence of the other equations, the axiom system $\mathcal{F}$ is the one that was shown in [9] to characterize strong bisimulation over $\mathbf{MPA}^*_\delta(A_\tau)$. In addition, the equational theory $\mathcal{E}$ includes equations which express the unobservable nature of the τ action. Two of these laws, namely **(T1)** and **(T3)**, are well-known from the theory of observation congruence over CCS-like languages (cf., e.g., [20]). The remaining three laws, namely **(FIR)** and **(MT1)**-**(MT2)**, describe the interplay between τ and prefix iteration. Equation **(FIR)** was introduced in [3] under the name of **(FIR$_1$)** (*Fair Iteration Rule*). In [3] it is also noted that this law is an equational formulation of *Koomen's Fair Abstraction Rule* [4][1]. This powerful equation will play a major role in our completeness theorem, and, together with the laws in the axiom system $\mathcal{F}$, can be used to derive, for instance, Milner's second τ-law, namely

$$\tau.x \quad = \quad \tau.x + x \quad .$$

Equations **(MT1)**–**(MT2)** are, to the best of our knowledge, new. They express a rather subtle interplay between prefix iteration and τ, and will play a crucial role in reducing terms to normal forms (cf. Lem. 4.7) and in our completeness proof, respectively.

[1] To be precise, Koomen's Fair Abstraction Rule is a general name for a family of proof rules **KFAR**$_n$, $n \geq 1$. **FIR** corresponds to KFAR$_1$.

Notation 3.1 *We write $\mathcal{E} \vdash P = Q$ iff the equation $P = Q$ is provable from the axiom system $\mathcal{E}$ using the rules of equational logic. We also write $P =_{AC} Q$ iff the terms P, Q are identical modulo commutativity and associativity of $+$,* i.e., *iff the equality $P = Q$ can be proved from the equations* (A1)-(A2).

For $I = \{i_1, \ldots, i_n\}$ a finite index set, we write $\sum \{P_i \mid i \in I\}$ for $P_{i_1} + \cdots + P_{i_n}$. By convention, $\sum \{P_i \mid i \in \emptyset\}$ stands for δ.

A1	$x + y$	$=$	$y + x$
A2	$(x + y) + z$	$=$	$x + (y + z)$
A3	$x + x$	$=$	x
A4	$x + \delta$	$=$	x
MI1	$\mu.(\mu^* x) + x$	$=$	$\mu^* x$
MI2	$a^*(a^* x)$	$=$	$a^* x$

Figure 2: Fokkink's axiom system $\mathcal{F}$

T1	$\mu.\tau.x$	$=$	$\mu.x$
T3	$a.(x + \tau.y)$	$=$	$a.(x + \tau.y) + a.y$
FIR	$\tau.x$	$=$	$\tau^* x$
MT1	$a^*(x + \tau.y)$	$=$	$a^*(x + \tau.y + a.y)$
MT2	$\tau.(a^* x)$	$=$	$a^*(\tau.(a^* x))$

Figure 3: The axiom system $\mathcal{E}$ is $\mathcal{F}$ plus the above equations

First of all, we establish the soundness of the axiom system $\mathcal{E}$.

Proposition 3.2 *For all $P, Q \in \mathsf{MPA}^*_\delta(A_\tau)$, $\mathcal{E} \vdash P = Q$ implies $P \approx^c Q$.*

Proof: As $\approx^c$ is a congruence, it is sufficient to show that each equation in $\mathcal{E}$ is sound with respect to it. The equations in the axiom system $\mathcal{F}$ are known to be sound with respect to strong bisimulation equivalence over $\mathbf{MPA}^*_\delta(A_\tau)$; therefore they are, a *fortiori*, sound with respect to $\approx^c$. The soundness of equations (T1) and (T3) is well-known, and that of (FIR) and (MT1)–(MT2) is easy to check. □

In the following lemma we present several derived equations to illustrate the power of the axiom system $\mathcal{E}$. Some of these laws will be very useful in the technical developments to follow.

Lemma 3.3 *The following equations are derivable from those in $\mathcal{E}$:*

DMI1	$\mu^* x$	$=$	$\mu^* x + x$
T2	$\tau.x + x$	$=$	$\tau.x$
DT2	$\tau.(x + y)$	$=$	$x + \tau.(x + y)$
MT3	$a^*(x + \tau.y)$	$=$	$a^*(x + \tau.y) + a.y$

Proof: We only show how to derive equation **MT3**, and leave the remaining verifications to the reader. To derive **MT3**, we argue as follows:

$$\begin{array}{rcll} a^*(x+\tau.y) & = & a^*(x+\tau.y+a.y) & \textbf{(MT1)} \\ & = & a^*(x+\tau.y+a.y)+x+\tau.y+a.y & \textbf{(DMI1)} \\ & = & a^*(x+\tau.y+a.y)+x+\tau.y+a.y+a.y & \textbf{(A3)} \\ & = & a^*(x+\tau.y)+a.y \ . & \end{array}$$

Axiom **(MT1)** is not necessary to derive equation **(MT3)**. In fact, there is an alternative derivation of this equation from the axiom system $\mathcal{E}$ that uses only **(MI1)** and **(T3)**. □

We conclude this section by addressing the issue of the relative independence of the equations **(FIR)** and **(MT1)**–**(MT2)**. More precisely, we shall prove that these laws cannot be derived from each other.

Proposition 3.4

1. $\mathcal{E} \setminus \{\textbf{FIR}\} \not\vdash \textbf{FIR}$.
2. $\mathcal{E} \setminus \{\textbf{MT1}\} \not\vdash \textbf{MT1}$.
3. $\mathcal{E} \setminus \{\textbf{MT2}\} \not\vdash \textbf{MT2}$.

Proof: From Birkhoff's classic completeness theorem for equational logic [5] (see, e.g., [15, Chapter 1] for a modern textbook presentation), an equation is derivable from an equational theory iff it is valid in every model of the theory. To show each of the above statements, it is therefore sufficient to exhibit a model of the equational theory under consideration in which the equation we are trying to disprove does not hold. As this kind of argument is quite tedious, we shall only present the details of the construction of the model used in the proof of statement 2, and limit ourselves to giving the intuition underlying the construction of the models used in the proofs of statements 1 and 3.

Sketch of the Proof of 1: Intuitively, the reason why equation **FIR** is not derivable from the theory $\mathcal{E} \setminus \{\textbf{FIR}\}$ is that **FIR** is the only equation that can be used to completely eliminate occurrences of the operation τ^* from terms.

Proof of 2: Intuitively, the reason why **MT1** cannot be derived from the other equations is that all of the axioms in $\mathcal{E} \setminus \{\textbf{MT1}\}$ preserve the maximum depth of the nesting of a-prefixes within the scope of an a^* operation, while **MT1** does not.

Formally, define a denotational semantics for $\mathsf{MPA}^*_\delta(A_\tau)$ in the domain of natural numbers $\mathbb{N}$ by:

$$\begin{array}{rcl} [\![x]\!]\rho & = & \rho(x) \\ [\![\delta]\!]\rho & = & 0 \\ [\![\mu.P]\!]\rho & = & [\![P]\!]\rho \\ [\![P+Q]\!]\rho & = & \max\{[\![P]\!]\rho, [\![Q]\!]\rho\} \\ [\![\tau^*P]\!]\rho & = & [\![P]\!]\rho \end{array}$$

$$
\begin{array}{rcl}
[\![a^*x]\!]\rho & = & \rho(x) \\
[\![a^*\delta]\!]\rho & = & 0 \\
[\![a^*(P+Q)]\!]\rho & = & \max\{[\![a^*P]\!]\rho, [\![a^*Q]\!]\rho\} \\
[\![a^*(\mu.P)]\!]\rho & = & \begin{cases} 1 + [\![P]\!]\rho & \text{if } \mu = a \\ [\![P]\!]\rho & \text{otherwise} \end{cases} \\
[\![a^*(\mu^*P)]\!]\rho & = & [\![\mu^*P]\!]\rho
\end{array}
$$

where $\rho : \mathsf{Var} \to \mathbb{N}$. It is now simple to check that this is a model for the equational theory $\mathcal{E} \setminus \{\mathbf{MT1}\}$, but

$$[\![a^*(x + \tau.y)]\!](\lambda x.\, 0) = 0 \neq 1 = [\![a^*(x + \tau.y + a.y)]\!](\lambda x.\, 0)$$

and so it is not a model of $\mathcal{E}$.

Sketch of the Proof of 3: The construction of the model proceeds along the lines presented above, but now one counts the maximum depth of the nesting of τ-prefixes within the scope of an a^* operation.

□

4 Completeness

This section is entirely devoted to a detailed proof of the completeness of the axiom system $\mathcal{E}$ with respect to observation congruence over the language $\mathbf{MPA}^*_\delta(A_\tau)$. Before tackling the proof of completeness, we present several intermediate results that will be most useful in the technical developments to follow.

The following lemma is a standard tool in proofs of completeness theorems for process algebras (cf., e.g., [13, 20]), and we shall use it heavily in the proof of our main result.

Lemma 4.1 (Absorption Lemma) *For all $p, q \in \mathbf{MPA}^*_\delta(A_\tau)$, $\mu \in A_\tau$, if $p \stackrel{\mu}{\Rightarrow} q$ then $\mathcal{E} \vdash p = p + \mu.q$.*

Proof: By induction on the length of the derivation $p \stackrel{\mu}{\Rightarrow} q$. The proof of the inductive basis, i.e. when $p \stackrel{\mu}{\to} q$, proceeds by induction on the depth of the proof of the transition, and uses only axioms **(A1)**–**(A3)** and **(MI1)**. The proof for the inductive step uses in addition axioms **(T2)** and **(T3)**. The details are standard and are therefore omitted. □

As a first application of the properties in Lem. 2.6 and of the above results, we establish a decomposition property of prefix iteration with respect to the relation of observation congruence that will find application in the main result of this paper. A similar decomposition property for the delay operation of Milner's SCCS [19] with respect to a notion of strong bisimulation preorder was, to our knowledge, first shown by Hennessy in [13].

Definition 4.2 *An $\mathbf{MPA}^*_\delta(A_\tau)$-term of the form μ^*p is said to be* initially μ-saturated *iff for all $q \in \mathbf{MPA}^*_\delta(A_\tau)$, $p \stackrel{\tau}{\Rightarrow} q$ implies $p \stackrel{\mu}{\Rightarrow} q$.*

Lemma 4.3 *Let $p, q \in \mathbf{MPA}^*_\delta(A_\tau)$ and $\mu \in A_\tau$. Suppose that $\mu^* p$ and $\mu^* q$ are both initially μ-saturated. Then $\mu^* p \approx^c \mu^* q$ iff $\mu^* p \approx^c q$ or $p \approx^c \mu^* q$ or $p \approx^c q$.*

Proof: The "if" implication follows immediately from the fact that $\approx^c$ is a congruence and the soundness of equation **MI2**. To show the "only if" implication, it is sufficient to prove that:

$$\mu^* p \approx^c \mu^* q \text{ and } \mu^* p \not\approx^c q \text{ and } p \not\approx^c \mu^* q \quad \Rightarrow \quad p \approx^c q \ . \tag{1}$$

We prove that (1) holds. To this end, let us assume that $\mu^* p \approx^c \mu^* q$, $\mu^* p \not\approx^c q$ and $p \not\approx^c \mu^* q$. By symmetry and Fact 2.4, to prove that $p \approx^c q$ must hold, it is sufficient to show that, for all $\gamma \in A_\tau$, $p' \in \mathbf{MPA}^*_\delta(A_\tau)$:

$$p \xrightarrow{\gamma} p' \quad \Rightarrow \quad \exists q' : \ q \stackrel{\gamma}{\Rightarrow} q' \text{ and } p' \approx q' \ . \tag{2}$$

This we now proceed to show. Assume that $p \xrightarrow{\gamma} p'$. By the operational semantics, this implies that $\mu^* p \xrightarrow{\gamma} p'$. As $\mu^* p \approx^c \mu^* q$, it follows that $\mu^* q \stackrel{\gamma}{\Rightarrow} q'$ for some q' such that $p' \approx q'$. If $q \stackrel{\gamma}{\Rightarrow} q'$, then we are done. Otherwise, as $\mu^* q$ is initially μ-saturated, it must be case that $\gamma = \mu$ and $q' \equiv \mu^* q$. We show that this leads to a contradiction.

Assume that $p \xrightarrow{\mu} p' \approx \mu^* q$. Then:

$$\begin{array}{rcll} p & \approx^c & p + \mu.p' & \text{(By Lemmas 4.1 and 3.2)} \\ & \approx^c & p + \mu.(\mu^* q) & (p' \approx \mu^* q \text{ and Lem. 2.6(2))} \\ & \approx^c & p + \mu.(\mu^* p) & (\mu^* p \approx^c \mu^* q) \\ & \approx^c & \mu^* p & \text{(Soundness of } \mathbf{MI1}) \\ & \approx^c & \mu^* q & (\mu^* p \approx^c \mu^* q) \end{array}$$

This contradicts the assumption that $p \not\approx^c \mu^* q$. □

It is interesting to note that the above lemma does *not* hold for terms that are not initially μ-saturated. Consider, for example, the terms $p \equiv a^*(\tau.\delta + a.\delta)$ and $q \equiv a^*(\tau.\delta)$. It is not hard to see that $p \approx^c q$. However, none of the possible decompositions of this equality afforded by Lem. 4.3 applies. Note that q is not initially a-saturated, whereas p is. As it will become clear from the technical developments to follow (see Lem. 4.7), axiom **(MT1)** will be used to make sure that every sub-term of the form $a^* t$ of a normal form will be initially a-saturated. This will allow us to use Lem. 4.3 to reason about equalities between such terms.

Definition 4.4 *For $p, q \in \mathbf{MPA}^*_\delta(A_\tau)$ and $\mu \in A_\tau$, we say that $\mu.q$ is a* summand *of p iff $p =_{AC} r + \mu.q$ for some $r \in \mathbf{MPA}^*_\delta(A_\tau)$.*

The proof of the completeness theorem relies, as usual, on the isolation of some notion of normal form for terms. This is introduced in the following definition.

Definition 4.5 (Normal Forms) *A term $p \in \mathbf{MPA}^*_\delta(A_\tau)$ is τ^*-*free *iff it does not contain occurrences of the τ^* operation.*

A τ^*-free term p is a normal form *iff whenever $a^* q$ is a sub-term of p and, for some $q' \in \mathbf{MPA}^*_\delta(A_\tau)$, $q \stackrel{\tau}{\Rightarrow} q'$, then $a.q'$ is a summand of q.*

For example, the term $a^*(\tau.\delta + a.\delta)$ is a normal form, while $a^*(\tau.\delta)$ is not.

The following result collects some elementary, but extremely useful, properties of normal forms that we state for the sake of clarity.

Fact 4.6 *Let $p \in \mathbf{MPA}^*_\delta(A_\tau)$ be a normal form. Then:*

1. *Every sub-term of p is also a normal form.*
2. *For every $q \in \mathbf{MPA}^*_\delta(A_\tau)$, $\mu \in A_\tau$, if $p \xrightarrow{\mu} q$, then q is a normal form.*
3. *Let a^*p be a normal form. Then a^*p is initially a-saturated.*

We now show that, using the axiom system $\mathcal{E}$, every term is provably equal to a normal form. Not surprisingly, axioms **(FIR)** and **(MT1)** play a vital role in the proof of the following result.

Lemma 4.7 (Normalization) *For every $p \in \mathbf{MPA}^*_\delta(A_\tau)$ there exists a normal form $\mathsf{nf}(p)$ such that $\mathcal{E} \vdash p = \mathsf{nf}(p)$.*

Proof: By structural induction on p. To illustrate the use of axioms **(FIR)** and **(MT1)**, we only give the proof for the case $p \equiv \mu^* q$ for some $q \in \mathbf{MPA}^*_\delta(A_\tau)$.

First of all, note that, by applying the inductive hypothesis to q, we can infer that $\mathcal{E} \vdash p = \mu^* \mathsf{nf}(q)$. If $\mu = \tau$, then equation **(FIR)** gives that $\mathcal{E} \vdash p = \tau.\mathsf{nf}(q)$. In this case we are done because $\tau.\mathsf{nf}(q)$ is easily seen to be a normal form.

Otherwise, $\mu = a \in A$. In this case we argue as follows (using the fact that, by Fact 2.2, the set $\mathsf{der}(r, \tau)$ is finite for every $r \in \mathbf{MPA}^*_\delta(A_\tau)$):

$$
\begin{array}{rcl}
\mathcal{E} \vdash \quad p & = & a^* \mathsf{nf}(q) \\
& = & a^* \Big(\mathsf{nf}(q) + \sum \{ \tau.q' \mid q' \in \mathsf{der}(\mathsf{nf}(q), \tau) \} \Big) \\
& & \text{(By repeated use of Lem. 4.1)} \\
& = & a^* \Big(\mathsf{nf}(q) + \sum \{ \tau.q' \mid q' \in \mathsf{der}(\mathsf{nf}(q), \tau) \} + \sum \{ a.q' \mid q' \in \mathsf{der}(\mathsf{nf}(q), \tau) \} \Big) \\
& & \text{(By repeated use of } \mathbf{(MT1)}\text{)} \\
& = & a^* \Big(\mathsf{nf}(q) + \sum \{ a.q' \mid q' \in \mathsf{der}(\mathsf{nf}(q), \tau) \} \Big) \\
& & \text{(By repeated use of Lem. 4.1)}
\end{array}
$$

We claim that the term $\mathsf{nf}(p) \equiv a^* \Big(\mathsf{nf}(q) + \sum \{ a.q' \mid q' \in \mathsf{der}(\mathsf{nf}(q), \tau) \} \Big)$ is a normal form. This follows from the fact that $\mathsf{nf}(q)$ is a normal form by the inductive hypothesis, the fact that each $q' \in \mathsf{der}(\mathsf{nf}(q), \tau)$ is a normal form by Fact 4.6(2) and the construction of $\mathsf{nf}(p)$. $\square$

For example, the normal form associated with the term $a^*(\tau.\delta)$ is, modulo $=_{AC}$, the term $a^*(\tau.\delta + a.\delta)$.

In the proof of the completeness result to come, we shall make use of a weight function on terms $w : \mathbf{MPA}^*_\delta(A_\tau) \to \mathbb{N}$. This is defined by structural recursion on terms as follows:

$$
w(\delta) \quad = \quad 1
$$

$$
\begin{aligned}
w(\mu.p) &= 1 + w(p) \\
w(p+q) &= 1 + w(p) + w(q) \\
w(\mu^* p) &= 2 + w(p)
\end{aligned}
$$

The following lemma collects some basic facts about the interplay between the above weight function and the operational semantics for processes.

Lemma 4.8 *For all $p, q \in \mathbf{MPA}^*_\delta(A_\tau)$, the following statements hold:*

1. *for every $\mu \in A_\tau$, $p \xrightarrow{\mu} q$ implies $w(q) \leq w(p)$;*
2. *if p is τ^*-free and $p \xrightarrow{\tau} q$, then $w(q) < w(p)$;*
3. *if $p \xrightarrow{\mu} q$ and $w(q) + 1 = w(p)$, then $p \equiv \mu.q$;*
4. *if $p \xrightarrow{\mu} q$ and $w(p) = w(q)$, then $p \equiv q \equiv \mu^* r$ for some $r \in \mathbf{MPA}^*_\delta(A_\tau)$;*
5. *if $p \equiv a^* t \stackrel{a}{\Rightarrow} q$ and $w(q) + 2 > w(p)$, then $p \equiv q$.*

We are now in a position to prove our main result of the paper, namely that the set of equations $\mathcal{E}$ in Fig. 3 is complete with respect to $\approx^c$ over the language $\mathbf{MPA}^*_\delta(A_\tau)$. This is the import of the following result. Unfortunately, the proof of the completeness theorem is combinatorial in nature and consists of the examination of a fairly large number of cases. For this reason, we have chosen to present the proof in a structured style following the spirit, albeit not the letter, of the proposal in [18]. We hope that this type of presentation will help the reader judge the correctness of the proof, in much the same way as it has helped us convince ourselves that the proof is, to the best of our knowledge, correct.

Theorem 4.9 (Completeness) *For all $p, q \in \mathbf{MPA}^*_\delta(A_\tau)$, $p \approx^c q$ implies $\mathcal{E} \vdash p = q$.*

Proof: In view of Lem. 4.7, it is sufficient to prove the claim for normal forms in $\mathbf{MPA}^*_\delta(A_\tau)$. In fact, it is even sufficient to prove that

$$\text{for all normal forms } p, q \in \mathbf{MPA}^*_\delta(A_\tau),\ p \approx^c p + q \ \text{ implies } \ \mathcal{E} \vdash p = p + q \ . \qquad (3)$$

In fact, let us assume that we have established the above claim and that p and q are normal forms such that $p \approx^c q$. For such terms, both the equivalences $p \approx^c p + q$ and $q \approx^c q + p$ hold. Then claim (3) and **(A1)** give $\mathcal{E} \vdash p = p + q = q + p = q$, and we are done.

We now proceed to prove (3). The proof proceeds by complete induction on $w(p) + w(q)$. Let us assume, as inductive hypothesis, that p, q are normal forms in $\mathbf{MPA}^*_\delta(A_\tau)$, that $p \approx^c p + q$ and that (3) holds for all pairs of normal forms $p', q' \in \mathbf{MPA}^*_\delta(A_\tau)$ such that $p' \approx^c p' + q'$ and $w(p') + w(q') < w(p) + w(q)$. We show that, under these assumptions, $\mathcal{E} \vdash p = p + q$. Note that, by a reasoning similar to the one in the previous paragraph, the inductive hypothesis gives that, for all normal forms $p', q' \in \mathbf{MPA}^*_\delta(A_\tau)$:

$$p' \approx^c q' \text{ and } w(p') + w(q') < w(p) + w(q) \ \Rightarrow \ \mathcal{E} \vdash p' = q' \ . \qquad (4)$$

We shall make use of the above fact repeatedly in the proof below.
First of all, as q is a normal form, it follows that q can have one of the following forms:

1. $q \equiv \delta$;
2. $q \equiv t + r$, for some normal forms $t, r \in \mathbf{MPA}^*_\delta(A_\tau)$;
3. $q \equiv \tau.r$, for some normal form $r \in \mathbf{MPA}^*_\delta(A_\tau)$;
4. $q \equiv a.r$, for some normal form $r \in \mathbf{MPA}^*_\delta(A_\tau)$; or
5. $q \equiv a^*r$, for some normal form r.

The proof of (3) proceeds by a case analysis on the form q takes. Throughout the proof, we shall make repeated use, without further mention, of the fact that, by Fact 4.6(1)–(2), the set of normal forms is closed under transitions and taking sub-terms.

1. Case: $q \equiv \delta$.

   The claim follows immediately by applying **(A4)**.

2. Case: $q \equiv t + r$.

   First of all, note that $p \approx^c p + q$ and $q \equiv t + r$ imply that $p \approx^c p + t$ and $p \approx^c p + r$. As $w(t) < w(q)$ and $w(r) < w(q)$, we may apply the inductive hypothesis to both these equalities to derive that:

$$\mathcal{E} \vdash \quad p \quad = \quad p + t \tag{5}$$
$$\mathcal{E} \vdash \quad p \quad = \quad p + r \quad . \tag{6}$$

   We now argue as follows:

$$\begin{array}{rcll} \mathcal{E} \vdash \quad p & = & p + r & (6) \\ & = & p + t + r & (5) \\ & = & p + q & (q \equiv t + r) \end{array}$$

   and we are done.

3. Case: $q \equiv \tau.r$.

   As $p \approx^c p + q$ and $q \equiv \tau.r \xrightarrow{\tau} r$, there exists a term p' such that $p \stackrel{\tau}{\Rightarrow} p'$ and $p' \approx r$. By Lem. 2.6(1), $p' \approx r$ implies

$$p' \approx^c r \text{ or } \tau.p' \approx^c r \text{ or } p' \approx^c \tau.r \quad . \tag{7}$$

   As p is τ^*-free and $q \equiv \tau.r$, we have that $w(p') < w(p)$ and $w(r) < w(q)$. Thus we may apply (4) to each one of the disjuncts in (7) to derive that:

$$\mathcal{E} \vdash p' = r \text{ or } \mathcal{E} \vdash \tau.p' = r \text{ or } \mathcal{E} \vdash p' = \tau.r \quad .$$

   In each one of the above cases, after possibly applying **(T1)**, we infer that

$$\mathcal{E} \vdash \tau.p' = \tau.r \quad . \tag{8}$$

   Therefore,

$$\begin{array}{rcll} \mathcal{E} \vdash \quad p & = & p + \tau.p' & (\text{Lem. 4.1, as } p \stackrel{\tau}{\Rightarrow} p') \\ & = & p + \tau.r & (8) \end{array}$$

   and we are done.

4. Case: $q \equiv a.r$.

As $p \approx^c p + q$ and $q \equiv a.r \xrightarrow{a} r$, there exists a term p' such that:

$$p \stackrel{a}{\Rightarrow} p' \text{ and } p' \approx r \quad . \tag{9}$$

By Lem. 2.6(1), $p' \approx r$ implies

$$p' \approx^c r \text{ or } \tau.p' \approx^c r \text{ or } p' \approx^c \tau.r \quad . \tag{10}$$

Moreover, by Lem. 4.8(1), the weight of p' is no greater than that of p, i.e. $w(p') \leq w(p)$. We proceed by considering the following two sub-cases:

(a) $w(p') < w(p)$ or $p' \approx^c r$; or

(b) $w(p') = w(p)$ and $p' \not\approx^c r$.

We examine these two possibilities in turn.

(a) Case: $w(p') < w(p)$ or $p' \approx^c r$.

In both of the cases, as $w(r) < w(q)$, we may apply (4) to the relevant disjuncts in (10), and possibly **(T1)**, to derive that:

$$\mathcal{E} \vdash \tau.p' = \tau.r \quad . \tag{11}$$

Therefore,

$$\begin{array}{rcll} \mathcal{E} \vdash \quad p & = & p + a.p' & \text{(Lem. 4.1, as } p \stackrel{a}{\Rightarrow} p') \\ & = & p + a.\tau.p' & \textbf{(T1)} \\ & = & p + a.\tau.r & (11) \\ & = & p + a.r & \textbf{(T1)} \end{array}$$

and we are done.

(b) Case: $w(p') = w(p)$ and $p' \not\approx^c r$.

First of all, note that, as $w(p') = w(p)$ and $p \stackrel{a}{\Rightarrow} p'$, by Lem. 4.8(2) and Lem. 4.8(4), it must be the case that $p \equiv a^*t$ for some $t \in \mathbf{MPA}^*_\delta(A_\tau)$, and that $p \xrightarrow{a} p \equiv p'$. Now, as $p' \equiv p \equiv a^*t \approx r$, but $p \equiv p' \not\approx^c r$, it must be the case that either of these two statements hold:

i. there exists a term r' such that $r \xrightarrow{\tau} r'$, $p \equiv p' \equiv a^*t \approx r'$, and r' is inequivalent to every τ-derivative of a^*t; or, symmetrically,

ii. there exists a term t' such that $a^*t \xrightarrow{\tau} t'$, $t' \approx r$, and t' is inequivalent to every τ-derivative of r.

We proceed by examining these two possibilities in turn.

i. Case: there exists a term r' such that $r \xrightarrow{\tau} r'$, $p \equiv p' \equiv a^*t \approx r'$, and r' is inequivalent to every τ-derivative of a^*t.

With the above hypotheses, an application of Lem. 2.6(1) to the equivalence $p \equiv a^*t \approx r'$ gives that:

$$a^*t \approx^c r' \text{ or } \tau.a^*t \approx^c r' \quad . \tag{12}$$

As $r \xrightarrow{\tau} r'$ and r is τ^*-free, by Lem. 4.8(2) and the form of q, it follows that $w(r') < w(r) < w(q)$. Thus we may apply (4) to both the disjuncts in (12) to derive that:

$$\mathcal{E} \vdash a^*t = r' \text{ or } \mathcal{E} \vdash \tau.a^*t = r' \ . \tag{13}$$

In both the above cases, after possibly applying **(T1)**, we obtain that:

$$\mathcal{E} \vdash \tau.a^*t = \tau.r' \ . \tag{14}$$

The above equality will be used repeatedly in the remainder of the proof for this case.

We now proceed by a case analysis on the form that the term r may take. As $r \xrightarrow{\tau} r'$ and r is τ^*-free, an examination of the rules in Fig. 1 shows that there are three possibilities to examine, namely:

A. $r \equiv \tau.r'$; or

B. $r =_{AC} r_1 + r_2$ for terms r_1, r_2 such that $r_1 \xrightarrow{\tau} r'$; or

C. $r \equiv a^*u$ for some term u such that $u \xrightarrow{\tau} r'$.

We remark here that, as $a^*t \approx r$, by Propn. 2.8, r can*not* take the form b^*u for some $b \neq a$.

We proceed by examining the above cases in turn.

A. Case: $r \equiv \tau.r'$.

In this case we argue as follows:

$$\begin{array}{rcll} \mathcal{E} \vdash \quad p \equiv a^*t & = & p + a.(a^*t) & (\text{Lem. 4.1, as } p \xrightarrow{a} a^*t) \\ & = & p + a.\tau.(a^*t) & (\mathbf{T1}) \\ & = & p + a.\tau.r' & (14) \\ & = & p + a.r & (r \equiv \tau.r') \end{array}$$

and we are done.

B. Case: $r =_{AC} r_1 + r_2$ for terms r_1, r_2 such that $r_1 \xrightarrow{\tau} r'$.

As $p \equiv a^*t \approx r =_{AC} r_1 + r_2$, by Propn. 3.2 and the fact that $\approx^c$ is contained in $\approx$, we have that

$$p \equiv a^*t \approx r_1 + r_2 \ .$$

Lem. 2.6(5) now gives that:

$$\begin{array}{rcl} \tau.p & \approx^c & \tau.p + r_1 \\ \tau.p & \approx^c & \tau.p + r_2 \ . \end{array}$$

We aim at applying the inductive hypothesis to both the above pairs of observation congruent terms. This is indeed possible because, for $i = 1, 2$,

$$\begin{array}{rcll} w(r_i) + 2 & \leq & w(r_1 + r_2) & (w(r_i) \geq 1) \\ & < & w(a.r) & (r =_{AC} r_1 + r_2 \Rightarrow w(r) = w(r_1 + r_2)) \\ & = & w(q) \ . & \end{array}$$

Therefore, by the inductive hypothesis, we derive that:

$$\mathcal{E} \vdash \quad \tau.p \quad = \quad \tau.p + r_1 \tag{15}$$
$$\mathcal{E} \vdash \quad \tau.p \quad = \quad \tau.p + r_2 \ . \tag{16}$$

We can now argue as follows:

$$\begin{array}{rcll}
\mathcal{E} \vdash \quad p \equiv a^*t & = & p + a.(a^*t) & (\text{Lem. 4.1, as } p \xrightarrow{a} a^*t) \\
& = & p + a.\tau.(a^*t) & \textbf{(T1)} \\
& = & p + a.(\tau.(a^*t) + r_2) & (16) \\
& = & p + a.(\tau.(a^*t) + r_1 + r_2) & (15) \\
& = & p + a.(\tau.r' + r_1 + r_2) & (14) \\
& = & p + a.(r_1 + r_2) & (\text{Lem. 4.1, as } r_1 \xrightarrow{\tau} r') \\
& = & p + a.r & (r =_{AC} r_1 + r_2)
\end{array}$$

and we are done.

C. Case: $r \equiv a^*u$ for some term u such that $u \xrightarrow{\tau} r'$.
In this case, as $p \equiv p' \equiv a^*t \approx r$ by (9) and $u \xrightarrow{\tau} r' \approx a^*t$, by Lem. 2.6(4) we derive that

$$\tau.a^*t \approx^c u \ . \tag{17}$$

As $w(u) + 2 = w(r) < w(a.r) = w(q)$, we may apply (4) to (17) to infer that:

$$\mathcal{E} \vdash \quad \tau.a^*t = u \ . \tag{18}$$

Therefore,

$$\begin{array}{rcll}
\mathcal{E} \vdash \quad p \equiv a^*t & = & p + a.(a^*t) & (\text{Lem. 4.1, as } p \xrightarrow{a} a^*t) \\
& = & p + a.\tau.(a^*t) & \textbf{(T1)} \\
& = & p + a.a^*(\tau.a^*t) & \textbf{(MT2)} \\
& = & p + a.a^*u & (18) \\
& = & p + a.r & (r \equiv a^*u)
\end{array}$$

and we are done.

As we have considered all the possible forms r may take, the proof for this sub-case is complete.

ii. Case: there exists a term t' such that $p \equiv a^*t \xrightarrow{\tau} t'$, $t' \approx r$, and t' is inequivalent to every τ-derivative of r.
By Lem. 2.6(1) and the hypotheses for this case, $t' \approx r$ implies

$$t' \approx^c r \text{ or } t' \approx^c \tau.r \ . \tag{19}$$

By the operational semantics, the transition $a^*t \xrightarrow{\tau} t'$ must hold because $t \xrightarrow{\tau} t'$. Thus, as t is τ^*-free, $w(t') < w(t) < w(a^*t) = w(p)$. Hence, as $w(\tau.r) = w(q)$, we may apply (4) to both the disjuncts in (19) to derive that:

$$\mathcal{E} \vdash t' = r \text{ or } \mathcal{E} \vdash t' = \tau.r \ .$$

In both cases, after possibly applying **(T1)**, we can infer that:

$$\mathcal{E} \vdash \tau.t' = \tau.r \quad . \tag{20}$$

Now we argue as follows:

$$\begin{array}{rcll} \mathcal{E} \vdash \quad p \equiv a^*t & = & a^*(t + \tau.t') & (\text{Lem. 4.1, as } t \xrightarrow{\tau} t') \\ & = & a^*(t + \tau.\tau.t') & \mathbf{(T1)} \\ & = & a^*(t + \tau.\tau.r) & (20) \\ & = & a^*(t + \tau.\tau.r) + a.\tau.r & \mathbf{(MT3)} \\ & = & p + a.r & \mathbf{(T1)} \end{array}$$

and we are done.

The proof for the case $w(p) = w(p')$ and $p' \not\approx^c r$ is now complete.

This completes the proof for the case $q \equiv a.r$.

5. Case: $q \equiv a^*r$.

First of all, let us note that, as $p \approx^c p + q$ and $q \equiv a^*r$, it follows that:

$$p \approx^c p + r \quad . \tag{21}$$

In fact,

$$\begin{array}{rcll} p & \approx^c & p + a^*r & \\ & \approx^c & p + a^*r + r & (\text{Soundness of } \mathbf{DMI1}) \\ & \approx^c & p + r & \end{array}$$

As $w(r) < w(q)$, we may apply the inductive hypothesis to (21) to derive that:

$$\mathcal{E} \vdash p = p + r \quad . \tag{22}$$

We shall repeatedly make use of this fact to show that $\mathcal{E} \vdash p = p + a^*r$.

As $p \approx^c p + a^*r$ and $p + a^*r \xrightarrow{a} a^*r$, there exists a term p' such that:

$$p \stackrel{a}{\Rightarrow} p' \text{ and } p' \approx a^*r \quad . \tag{23}$$

By Lem. 2.6(1), $p' \approx a^*r$ implies

$$p' \approx^c a^*r \text{ or } \tau.p' \approx^c a^*r \text{ or } p' \approx^c \tau.a^*r \quad . \tag{24}$$

We now proceed by examining the relationship between $w(p')$ and $w(p)$. We know, by Lem. 4.8(1), that $w(p') \leq w(p)$. We consider two possibilities, depending on whether $w(p') + 2 \leq w(p)$ or not.

(a) Case: $w(p') + 2 \leq w(p)$.

In this case, we may apply (4) to each of the disjuncts in (24) to obtain that:

$$\mathcal{E} \vdash p' = a^*r \text{ or } \mathcal{E} \vdash \tau.p' = a^*r \text{ or } \mathcal{E} \vdash p' = \tau.a^*r \quad .$$

By possibly applying equation (**T1**), in each case we derive that:

$$\mathcal{E} \vdash \tau.p' = \tau.a^*r \quad . \tag{25}$$

We now reason as follows:

$$\begin{array}{rcll} \mathcal{E} \vdash \quad p & = & p + a.p' & (\text{Lem. 4.1, as } p \stackrel{a}{\Rightarrow} p') \\ & = & p + a.\tau.p' & (\mathbf{T1}) \\ & = & p + a.\tau.a^*r & (25) \\ & = & p + a.a^*r & (\mathbf{T1}) \\ & = & p + r + a.a^*r & (22) \\ & = & p + a^*r & (\mathbf{A1} \text{ and } \mathbf{MI1}) \end{array}$$

and we are done.

(b) Case: $w(p') + 2 > w(p)$.

In this case, p must consist of a single summand, otherwise the a-transition leading from p to p' would have to discard other summands and $w(p') + 2 \leq w(p)$ would then follow. As $p \stackrel{a}{\Rightarrow} p'$ by (23) and p is τ^*-free, such a p can only take one of the following forms:

i. $p \equiv \tau.t$ for some $t \in \mathbf{MPA}^*_\delta(A_\tau)$ such that $t \stackrel{a}{\Rightarrow} p'$; or

ii. $p \equiv a.t$ for some $t \in \mathbf{MPA}^*_\delta(A_\tau)$ such that $t \stackrel{\varepsilon}{\Rightarrow} p'$; or

iii. $p \equiv a^*t$ for some $t \in \mathbf{MPA}^*_\delta(A_\tau)$. Note that the case $p \equiv b^*t$ for some $b \neq a$ does not apply here. In fact, if $b \neq a$ and $p \equiv b^*t \stackrel{a}{\Rightarrow} p'$, it would have to be the case that $t \stackrel{a}{\Rightarrow} p'$. In this case, we would be able to infer that $w(p') + 2 \leq w(p)$ because $w(p') \leq w(t)$ and $w(t) + 2 = w(p)$.

We proceed by examining the three cases above separately.

i. Case: $p \equiv \tau.t$ for some t such that $t \stackrel{a}{\Rightarrow} p'$.

To proceed with the proof, note, first of all, that, as we are assuming that $w(p') + 2 > w(p)$, it can only be the case that $w(p') = w(t)$. In fact, if $w(p') < w(t)$, then

$$w(p') < w(t) \text{ and } w(t) + 1 = w(p)$$

would hold, i.e., $w(p') + 2 \leq w(p)$. Hence, let us assume that $w(p') = w(t)$. As $t \stackrel{a}{\Rightarrow} p'$, by Lem. 4.8(2) and Lem. 4.8(4), this is only possible if $t \equiv p' \equiv a^*t'$ for some $t' \in \mathbf{MPA}^*_\delta(A_\tau)$. Instantiating (24), we obtain that:

$$a^*t' \approx^c a^*r \text{ or } \tau.a^*t' \approx^c a^*r \text{ or } a^*t' \approx^c \tau.a^*r \quad . \tag{26}$$

If $t \equiv a^*t' \approx^c a^*r$, then, as $w(t) < w(p)$, we may apply (4) to derive that

$$\mathcal{E} \vdash a^*t' = a^*r \quad . \tag{27}$$

Thus:

$$\begin{array}{rcll} \mathcal{E} \vdash \quad p \equiv \tau.a^*t' & = & \tau.a^*t' + a^*t' & (\mathbf{T2}) \\ & = & p + a^*r & (27) \end{array}$$

and we are done.

Otherwise, we have that $a^*t' \approx a^*r$, but $a^*t' \not\approx^c a^*r$. This can only be because either:

A.1 $t \equiv a^*t' \xrightarrow{\tau} t''$ for some $t'' \approx a^*r$ which is inequivalent to every τ-derivative of a^*r; or, symmetrically,

A.2 $a^*r \xrightarrow{\tau} r'$ for some $r' \approx a^*t' \equiv t$ which is inequivalent to every τ-derivative of $a^*t' \equiv t$.

We examine these two cases in turn.

A.1 Case: $t \equiv a^*t' \xrightarrow{\tau} t''$ for some $t'' \approx a^*r$ which is inequivalent to every τ-derivative of a^*r.

As $a^*t' \xrightarrow{\tau} t''$, it must be the case that $t' \xrightarrow{\tau} t''$. Therefore, as t' is τ^*-free, Lem. 4.8(3) gives $w(t'') < w(t')$. Moreover,

$$\begin{aligned} w(t') + 2 &= w(a^*t') \\ &< w(p) \quad (p \equiv \tau.a^*t') \ . \end{aligned}$$

As $t'' \approx a^*r$, it follows by Lem. 2.6(2) that

$$\tau.t'' \approx^c \tau.a^*r \ . \tag{28}$$

By the above considerations on the relationship between $w(t'')$ and $w(p)$, we may apply (4) to (28) to derive that

$$\mathcal{E} \vdash \tau.t'' = \tau.a^*r \ . \tag{29}$$

Therefore,

$$\begin{aligned} \mathcal{E} \vdash \quad p &= \tau.a^*t' && (p \equiv \tau.a^*t') \\ &= p + a^*t' && (\mathbf{T2}) \\ &= p + a^*(t' + \tau.t'') && (\text{Lem. 4.1, as } t' \xrightarrow{\tau} t'') \\ &= p + a^*(t' + \tau.t'') + a.t'' && (\mathbf{MT3}) \\ &= p + a.\tau.t'' && (\mathbf{T1}) \\ &= p + a.\tau.a^*r && (29) \\ &= p + a.a^*r && (\mathbf{T1}) \\ &= p + r + a.a^*r && (22) \\ &= p + a^*r && (\mathbf{A1} \text{ and } \mathbf{MI1}) \end{aligned}$$

and we are done.

A.2 Case: $a^*r \xrightarrow{\tau} r'$ for some $r' \approx a^*t' \equiv t$ which is inequivalent to every τ-derivative of $a^*t' \equiv t$.

As $a^*r \xrightarrow{\tau} r'$, it must be the case that $r \xrightarrow{\tau} r'$. Thus, reasoning as in the previous case, we may apply (4) to infer that, as $p \equiv \tau.a^*t' \approx^c \tau.r'$ and $w(r') + 2 < w(a^*r) = w(q)$,

$$\mathcal{E} \vdash p = \tau.r' \ . \tag{30}$$

We now reason as follows:

$$\begin{aligned} \mathcal{E} \vdash \quad p &= \tau.a^*t' && (p \equiv \tau.a^*t') \\ &= \tau.a^*t' + \tau.a^*t' && (\mathbf{A3}) \\ &= \tau.a^*t' + a^*(\tau.a^*t') && (\mathbf{MT2}) \\ &= p + a^*(p + r) && (p \equiv \tau.a^*t' \text{ and } (22)) \\ &= p + a^*(\tau.r' + r) && (30) \\ &= p + a^*r && (\text{Lem. 4.1, as } r \xrightarrow{\tau} r') \end{aligned}$$

and we are done.
The proof for this case is then complete.

ii. CASE: $p \equiv a.t$ for some $t \in \mathbf{MPA}^*_\delta(A_\tau)$ such that $t \stackrel{\varepsilon}{\Rightarrow} p' \approx a^*r \equiv q$.
First of all, note that, as $p \approx^c p + r$ by (21), it must be the case that r is stable. Therefore, as $p' \approx a^*r$, any τ-transition from p' must be matched by a^*r standing still, i.e., by the transition $a^*r \stackrel{\varepsilon}{\Rightarrow} a^*r$. As p' is τ^*-free and τ-transitions decrease the weight of τ^*-free terms, there exists a term p'' such that

$$p' \stackrel{\varepsilon}{\Rightarrow} p'' \text{ and } p'' \approx a^*r \text{ and } p'' \text{ is stable} \quad .$$

By Lem. 2.6(3), it follows that

$$p'' \approx^c a^*r \quad . \tag{31}$$

As $w(p'') \leq w(p') < w(p)$, we may now apply (4) to (31) to derive that:

$$\mathcal{E} \vdash p'' = a^*r \quad . \tag{32}$$

Therefore,

$$\begin{array}{rcll} \mathcal{E} \vdash \quad p & = & p + a.p'' & (\text{Lem. 4.1, as } p \stackrel{a}{\Rightarrow} p'') \\ & = & p + a.(a^*r) & (32) \\ & = & p + r + a.(a^*r) & (22) \\ & = & p + a^*r & (\mathbf{A1} \text{ and } \mathbf{MI1}) \end{array}$$

and we are done.

iii. CASE: $p \equiv a^*t$ for some $t \in \mathbf{MPA}^*_\delta(A_\tau)$ and $p \stackrel{a}{\Rightarrow} p' \approx a^*r$.
First of all, note that, as we are assuming that $w(p') + 2 > w(p)$, by Lem. 4.8(5) the transition $p \stackrel{a}{\Rightarrow} p'$ must in fact be of the form $p \equiv a^*t \stackrel{a}{\rightarrow} a^*t \equiv p'$. Thus $p \equiv a^*t \approx a^*r \equiv q$. Note further that, as $p \approx^c p + q$, any τ-transition emanating from $q \equiv a^*r$ must be matched by a τ-transition from $p \equiv a^*t$. If the converse is also true, then, in fact, $p \equiv a^*t \approx^c a^*r \equiv q$ holds. In this case, as p and q are normal forms and, a *fortiori*, initially a-saturated, we may apply Lem. 4.3, to derive that

$$t \approx^c r \text{ or } a^*t \approx^c r \text{ or } t \approx^c a^*r \quad .$$

In each of the above cases, we may apply (4) to obtain that

$$\mathcal{E} \vdash t = r \text{ or } \mathcal{E} \vdash t = a^*r \text{ or } \mathcal{E} \vdash a^*t = r \quad .$$

In each case, after possibly applying (**MI2**), we derive that

$$\mathcal{E} \vdash p \equiv a^*t = a^*r \equiv q$$

from which $\mathcal{E} \vdash p = p + q$ follows immediately by (**A3**).

Otherwise, $p \equiv a^*t \not\approx^c a^*r \equiv q$ because there exists a term t' such that $p \xrightarrow{\tau} t'$, $t' \approx q$ and t' is inequivalent to every τ-derivative of q. By applying Lem. 2.6(1) to $t' \approx a^*r$, we infer that

$$t' \approx^c a^*r \text{ or } \tau.t' \approx^c a^*r \text{ or } t' \approx^c \tau.a^*r \quad . \tag{33}$$

Note now that, as $p \equiv a^*t \xrightarrow{\tau} t'$, it must be the case that $t \xrightarrow{\tau} t'$. As $w(t') + 3 \leq w(p)$, we may apply (4) to each one of the disjuncts in (33) to derive that:

$$\mathcal{E} \vdash t' = a^*r \text{ or } \mathcal{E} \vdash \tau.t' = a^*r \text{ or } \mathcal{E} \vdash t' = \tau.a^*r \quad .$$

In each one of these cases, after possibly applying **(T1)**, we have that

$$\mathcal{E} \vdash \tau.t' = \tau.a^*r \quad . \tag{34}$$

Therefore,

$$\begin{array}{rcll}
\mathcal{E} \vdash \quad p & = & a^*t & (p \equiv a^*t) \\
 & = & a^*(t + \tau.t') & (\text{Lem. 4.1, as } t \xrightarrow{\tau} t') \\
 & = & a^*(t + \tau.t') + a.t' & (\mathbf{MT3}) \\
 & = & p + a.\tau.t' & (\mathbf{T1}) \\
 & = & p + a.\tau.a^*r & (34) \\
 & = & p + a.a^*r & (\mathbf{T1}) \\
 & = & p + r + a.a^*r & (22) \\
 & = & p + a^*r & (\mathbf{A1} \text{ and } \mathbf{MI1})
\end{array}$$

and we are done.

The proof for the case $q \equiv a^*r$ is now complete.

As we have examined all the possible forms that q may take, the proof of theorem is complete. □

5 ω-Completeness

In the previous section we showed that the equational theory $\mathcal{E}$ is complete with respect to observation congruence over the language $\mathbf{MPA}^*_\delta(A_\tau)$. We shall now prove that $\mathcal{E}$ is in fact ω-complete, i.e., that for all $P, Q \in \mathsf{MPA}^*_\delta(A_\tau)$,

$$P \approx^c Q \;\Rightarrow\; \mathcal{E} \vdash P = Q \quad . \tag{35}$$

This we show by using a technique based on inverted substitutions which is due to Groote [12], and that can often be used to give elegant, model-independent proofs of ω-completeness results.

Before applying Groote's technique to prove (35), we outline its general ideas in the setting of this study. Assume that $P, Q \in \mathsf{MPA}^*_\delta(A_\tau)$ are observation congruent, i.e., that

$$\text{for every substitution } \sigma : \mathsf{Var} \to \mathbf{MPA}^*_\delta(A_\tau),\ P\sigma \approx^c Q\sigma.$$

Theorem 4.9 then gives that, for every substitution $\sigma : \mathsf{Var} \to \mathbf{MPA}^*_\delta(A_\tau)$,

$$\mathcal{E} \vdash P\sigma = Q\sigma \ . \tag{36}$$

We show that (36) implies that:

$$\mathcal{E} \vdash P = Q \ . \tag{37}$$

The result presented by Groote in [12, Thm. 3.1] allows us to infer (37) from (36) provided we can find a substitution $\rho : \mathsf{Var} \to \mathbf{MPA}^*_\delta(A_\tau)$ and a function $R : \mathbf{MPA}^*_\delta(A_\tau) \to \mathsf{MPA}^*_\delta(A_\tau)$ satisfying the following conditions:

1. For $T \equiv P$ and $T \equiv Q$,
$$\mathcal{E} \vdash R(T\rho) = T \ . \tag{38}$$

2. For all $p_1, q_1 \in \mathbf{MPA}^*_\delta(A_\tau)$ and $\mu \in A_\tau$:
$$\mathcal{E} \cup \{p_1 = q_1, R(p_1) = R(q_1)\} \vdash R(\mu.p_1) = R(\mu.q_1) \tag{39}$$
and
$$\mathcal{E} \cup \{p_1 = q_1, R(p_1) = R(q_1)\} \vdash R(\mu^* p_1) = R(\mu^* q_1) \ . \tag{40}$$

3. For all $p_i, q_i \in \mathbf{MPA}^*_\delta(A_\tau)$ $(i = 1, 2)$:
$$\mathcal{E} \cup \{p_i = q_i, R(p_i) = R(q_i) \mid i = 1, 2\} \vdash R(p_1 + p_2) = R(q_1 + q_2) \ . \tag{41}$$

4. For each axiom $(P_1 = Q_1) \in \mathcal{E}$ and substitution $\sigma : \mathsf{Var} \to \mathbf{MPA}^*_\delta(A_\tau)$,
$$\mathcal{E} \vdash R(P_1\sigma) = R(Q_1\sigma) \ . \tag{42}$$

If for every pair of terms $P, Q \in \mathsf{MPA}^*_\delta(A_\tau)$ for which (36) holds we may find such a ρ and R, then Thm. 3.1 in [12] gives that:

Theorem 5.1 (ω-Completeness) *$\mathcal{E}$ is ω-complete,* i.e., *for all $P, Q \in \mathsf{MPA}^*_\delta(A_\tau)$, $P \approx^c Q$ implies $\mathcal{E} \vdash P = Q$.*

Therefore, all we need to do to show the ω-completeness of our axiomatization is to devise appropriate functions ρ and R for each pair of observation congruent terms $P, Q \in \mathsf{MPA}^*_\delta(A_\tau)$, and prove that conditions (38)–(42) are satisfied by them. This we now proceed to do. The interested reader is referred to [12, 1] for further examples of applications of the technique outlined above.

Let $P, Q \in \mathsf{MPA}^*_\delta(A_\tau)$ be terms for which (36) holds. We define $\rho : \mathsf{Var} \to \mathbf{MPA}^*_\delta(A_\tau)$ by:

$$\rho(x) \ \triangleq \ a_x.\delta \tag{43}$$

where, for each $x \in \mathsf{Var}$, a_x is a distinguished action in A which occurs neither in P nor in Q. (Note that such an injective assignment of actions in A to variables can always be

found because A is countably infinite and the set of actions occurring in P or Q is, of course, finite.) The function $R : \mathbf{MPA}^*_\delta(A_\tau) \to \mathsf{MPA}^*_\delta(A_\tau)$ is instead defined by structural recursion on closed terms as follows:

$$R(\delta) \triangleq \delta \tag{44}$$

$$R(\mu.p) \triangleq \begin{cases} x & \text{if } \mu = a_x \text{ for some } x \in \mathsf{Var} \\ \mu.R(p) & \text{otherwise} \end{cases} \tag{45}$$

$$R(p+q) \triangleq R(p) + R(q) \tag{46}$$

$$R(\mu^* p) \triangleq \begin{cases} x + R(p) & \text{if } \mu = a_x \text{ for some } x \in \mathsf{Var} \\ \mu^* R(p) & \text{otherwise} \end{cases} \tag{47}$$

Note that R is well-defined because the assignment of actions to variables is injective.

We now show that conditions (38)–(42) are met by such a ρ and R, thus establishing the ω-completeness of the equational theory $\mathcal{E}$.

Lemma 5.2 *Statements (38)–(42) hold for ρ and R.*

Proof: We proceed by checking each of the conditions in turn.

Proof of Statement (38).

The result follows immediately from the following stronger claim, that may easily be proven by structural induction on $T \in \mathsf{MPA}^*_\delta(A_\tau)$.

Claim: For every $T \in \mathsf{MPA}^*_\delta(A_\tau)$ not containing occurrences of actions a_x, $x \in \mathsf{Var}$, $R(T\rho) \equiv T$.

The straightforward details of the proof of this claim are omitted.

Proof of Statements (39)–(41).

We only give the details of the proof for statement (40). Assume that $p_1, q_1 \in \mathbf{MPA}^*_\delta(A_\tau)$ and $\mu \in A_\tau$. We show that (40) holds by distinguishing two cases, depending on whether $\mu = a_x$ for some $x \in \mathsf{Var}$, or not.

1. Assume that $\mu = a_x$ for some $x \in \mathsf{Var}$. Then we can argue as follows:

$$\begin{array}{lrcll} \mathcal{E} \cup \{p_1 = q_1, R(p_1) = R(q_1)\} \vdash & R(\mu^* p_1) & = & x + R(p_1) & (47) \\ & & = & x + R(q_1) & (R(p_1) = R(q_1)) \\ & & = & R(\mu^* q_1) & (47) \end{array}$$

   and we are done.

2. Assume that $\mu \neq a_x$ for all $x \in \mathsf{Var}$. Then we can argue as follows:

$$\begin{array}{lrcll} \mathcal{E} \cup \{p_1 = q_1, R(p_1) = R(q_1)\} \vdash & R(\mu^* p_1) & = & \mu^* R(p_1) & (47) \\ & & = & \mu^* R(q_1) & (R(p_1) = R(q_1)) \\ & & = & R(\mu^* q_1) & (47) \end{array}$$

   and we are done.

The statements corresponding to the other operations in the signature of $\mathbf{MPA}^*_\delta(A_\tau)$ may be shown in similar fashion.

Proof of Statement (42).

Let $\sigma : \mathsf{Var} \to \mathbf{MPA}^*_\delta(A_\tau)$ be a substitution. We show that for every axiom $(P_1 = Q_1) \in \mathcal{E}$,

$$\mathcal{E} \vdash R(P_1\sigma) = R(Q_1\sigma) \ .$$

As the reader can easily imagine, this verification is long and extremely tedious. Hence we only present a few selected cases. In what follows, we assume, for notational convenience, that $\sigma(x) = p$ and $\sigma(y) = q$ for some process terms $p, q \in \mathbf{MPA}^*_\delta(A_\tau)$.

Axiom (MI1).

We distinguish two cases, depending on whether $\mu = a_w$ for some $w \in \mathsf{Var}$ or not.

1. Assume that $\mu = a_w$ for some $w \in \mathsf{Var}$. Then:

$$\begin{array}{rcll} \mathcal{E} \vdash \quad R(\mu.(\mu^* p) + p) & = & R(\mu.(\mu^* p)) + R(p) & (46) \\ & = & w + R(p) & (45) \\ & = & R(\mu^* p) & (47) \end{array}$$

   and we are done.

2. Assume that $\mu \neq a_w$ for all $w \in \mathsf{Var}$. Then:

$$\begin{array}{rcll} \mathcal{E} \vdash \quad R(\mu.(\mu^* p) + p) & = & R(\mu.(\mu^* p)) + R(p) & (46) \\ & = & \mu.R(\mu^* p) + R(p) & (45) \\ & = & \mu.\mu^* R(p) + R(p) & (47) \\ & = & \mu^* R(p) & \textbf{(MI1)} \\ & = & R(\mu^* p) & (47) \end{array}$$

   and we are done.

Axiom (MT1).

Again, we distinguish two cases, depending on whether $a = a_w$ for some $w \in \mathsf{Var}$ or not.

1. Assume that $a = a_w$ for some $w \in \mathsf{Var}$. Then:

$$\begin{array}{rcll} \mathcal{E} \vdash \quad R(a^*(p + \tau.q)) & = & w + R(p + \tau.q) & (47) \\ & = & w + w + R(p + \tau.q) & \textbf{(A3)} \\ & = & w + R(a.q) + R(p + \tau.q) & (45) \\ & = & w + R(a.q + (p + \tau.q)) & (46) \\ & = & w + R(p + \tau.q + a.q) & \textbf{(A1–A2)} \\ & = & R(a^*(p + \tau.q + a.q)) & (47) \end{array}$$

   and we are done.

2. Assume that $\mu \neq a_w$ for all $w \in \mathsf{Var}$. Then:

$$\begin{array}{rcll} \mathcal{E} \vdash \quad R(a^*(p+\tau.q)) & = & a^* R(p+\tau.q) & (47) \\ & = & a^*(R(p)+R(\tau.q)) & (46) \\ & = & a^*(R(p)+\tau.R(q)) & (45) \\ & = & a^*(R(p)+\tau.R(q)+a.R(q)) & \textbf{(MT1)} \\ & = & a^*(R(p)+R(\tau.q)+R(a.q)) & (45) \\ & = & a^* R(p+\tau.q+a.q) & (46) \\ & = & R(a^*(p+\tau.q+a.q)) & (47) \end{array}$$

and we are done.

Axiom (MT2).

As before, we distinguish two cases, depending on whether $a = a_w$ for some $w \in \mathsf{Var}$ or not.

1. Assume that $a = a_w$ for some $w \in \mathsf{Var}$. Then:

$$\begin{array}{rcll} \mathcal{E} \vdash \quad R(\tau.(a^*p)) & = & \tau.R(a^*p) & (45) \\ & = & \tau.(w+R(p)) & (47) \\ & = & w+\tau.(w+R(p)) & \textbf{(DT2)} \\ & = & w+R(\tau.(a^*p)) & \text{(First two lines of the proof)} \\ & = & R(a^*(\tau.(a^*p))) & (47) \end{array}$$

and we are done.

2. Assume that $\mu \neq a_w$ for all $w \in \mathsf{Var}$. Then:

$$\begin{array}{rcll} \mathcal{E} \vdash \quad R(\tau.(a^*p)) & = & \tau.R(a^*p) & (45) \\ & = & \tau.(a^*R(p)) & (47) \\ & = & a^*(\tau.(a^*R(p))) & \textbf{(MT2)} \\ & = & a^*(\tau.R(a^*p)) & (47) \\ & = & a^*R(\tau.(a^*p)) & (45) \\ & = & R(a^*(\tau.(a^*p))) & (47) \end{array}$$

and we are done.

This completes the proof of the lemma. □

For each pair of observation congruent terms $P, Q \in \mathsf{MPA}^*_\delta(A_\tau)$ we have thus shown how to construct mappings ρ and R that, by the above lemma, satisfy Groote's conditions (38)–(42). By Thm. 3.1 of [12], we have therefore proven Thm. 5.1.

Acknowledgements: We are most grateful to Wan Fokkink for his careful proof-reading of a draft of this paper and for his support.

References

[1] L. Aceto, *Full abstraction for series-parallel pomsets*, in Proceedings TAPSOFT '91, S. Abramsky and T. Maibaum, eds., vol. 493 of Lecture Notes in Computer Science, Springer-Verlag, 1991, pp. 1–25. A full version appeared as Computer Science Technical Report 2/90, University of Sussex, March 1990.

[2] L. Aceto, B. Bloom, and F. Vaandrager, *Turning SOS rules into equations*, Information and Computation, 111 (1994), pp. 1–52.

[3] J. Bergstra, I. Bethke, and A. Ponse, *Process algebra with iteration and nesting*, Computer Journal, 37 (1994), pp. 243–258.

[4] J. Bergstra and J. Klop, *Process algebra for synchronous communication*, Information and Computation, 60 (1984), pp. 109–137.

[5] G. Birkhoff, *On the structure of abstract algebras*, in Proceedings of the Cambridge Philosophical Society 31(4), 1935, pp. 433–454.

[6] I. Copi, C. Elgot, and J. Wright, *Realization of events by logical nets*, J. Assoc. Comput. Mach., 5 (1958), pp. 181–196.

[7] F. Corradini, R. D. Nicola, and A. Labella, *Fully abstract models for nondeterministic Kleene algebras (extended abstract)*, 1995. Unpublished manuscript.

[8] R. De Nicola and A. Labella, *A completeness theorem for nondeterministic Kleene algebras*, in Proceedings of MFCS '94, vol. 841 of Lecture Notes in Computer Science, Springer-Verlag, 1994.

[9] W. Fokkink, *A complete equational axiomatization for prefix iteration*, Inf. Process. Lett., 52 (1994), pp. 333–337.

[10] ——, *A complete axiomatization for prefix iteration in branching bisimulation*, 1995. Unpublished manuscript.

[11] W. Fokkink and H. Zantema, *Basic process algebra with iteration: Completeness of its equational axioms*, Computer Journal, 37 (1994), pp. 259–267.

[12] J. Groote, *A new strategy for proving ω–completeness with applications in process algebra*, in Proceedings CONCUR 90, Amsterdam, J. Baeten and J. Klop, eds., vol. 458 of Lecture Notes in Computer Science, Springer-Verlag, 1990, pp. 314–331.

[13] M. Hennessy, *A term model for synchronous processes*, Information and Control, 51 (1981), pp. 58–75.

[14] ——, *Axiomatising finite delay operators*, Acta Inf., 21 (1984), pp. 61–88.

[15] P. Johnstone, *Notes on Logic and Set Theory*, Cambridge Mathematical Textbooks, Cambridge University Press, 1987.

[16] R. Keller, *Formal verification of parallel programs*, Comm. ACM, 19 (1976), pp. 371–384.

[17] S. Kleene, *Representation of events in nerve nets and finite automata*, in Automata Studies, C. Shannon and J. McCarthy, eds., Princeton University Press, 1956, pp. 3–41.

[18] L. Lamport, *How to write a proof*, Research Report 94, Digital Equipment Corporation, Systems Research Center, Feb. 1993.

[19] R. Milner, *Calculi for synchrony and asynchrony*, Theoretical Comput. Sci., 25 (1983), pp. 267–310.

[20] ——, *Communication and Concurrency*, Prentice-Hall International, Englewood Cliffs, 1989.

[21] D. Park, *Concurrency and automata on infinite sequences*, in 5th GI Conference, P. Deussen, ed., vol. 104 of Lecture Notes in Computer Science, Springer-Verlag, 1981, pp. 167–183.

[22] G. Plotkin, *A structural approach to operational semantics*, Report DAIMI FN-19, Computer Science Department, Aarhus University, 1981.

[23] P. Sewell, *Bisimulation is not finitely (first order) equationally axiomatisable*, in Proceedings 9th Annual Symposium on Logic in Computer Science, Paris, France, IEEE Computer Society Press, 1994, pp. 62–70.

Recent Publications in the BRICS Report Series

RS-95-5 **Luca Aceto and Anna Ingólfsdóttir.** ***A Complete Equational Axiomatization for Prefix Iteration with Silent Steps*****. January 1995. 27 pp.**

RS-95-4 **Mogens Nielsen and Glynn Winskel.** ***Petri Nets and Bisimulations*****. January 1995. 36 pp. To appear in TCS.**

RS-95-3 **Anna Ingólfsdóttir.** ***A Semantic Theory for Value–Passing Processes, Late Approach, Part I: A Denotational Model and Its Complete Axiomatization*****. January 1995. 37 pp.**

RS-95-2 **François Laroussinie, Kim G. Larsen, and Carsten Weise.** ***From Timed Automata to Logic - and Back*****. January 1995. 21 pp.**

RS-95-1 **Gudmund Skovbjerg Frandsen, Thore Husfeldt, Peter Bro Miltersen, Theis Rauhe, and Søren Skyum.** ***Dynamic Algorithms for the Dyck Languages*****. January 1995. 21 pp.**

RS-94-48 **Jens Chr. Godskesen and Kim G. Larsen.** ***Synthesizing Distinguishing Formulae for Real Time Systems*****. December 1994. 21 pp.**

RS-94-47 **Kim G. Larsen, Bernhard Steffen, and Carsten Weise.** ***A Constraint Oriented Proof Methodology based on Modal Transition Systems*****. December 1994. 13 pp.**

RS-94-46 **Amos Beimel, Anna Gál, and Mike Paterson.** ***Lower Bounds for Monotone Span Programs*****. December 1994. 14 pp.**

RS-94-45 **Jørgen H. Andersen, Kåre J. Kristoffersen, Kim G. Larsen, and Jesper Niedermann.** ***Automatic Synthesis of Real Time Systems*****. December 1994. 17 pp.**

RS-94-44 **Sten Agerholm.** ***A HOL Basis for Reasoning about Functional Programs*****. December 1994. PhD thesis. viii+224 pp.**