Asynchronous communication in process algebra: extended abstract

Citation for published version (APA):

Document status and date:
Published: 01/01/1991

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

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

Link to publication

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

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

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

Take down policy
If you believe that this document breaches copyright please contact us at:
openaccess@tue.nl
providing details and we will investigate your claim.
Asynchronous Communication in Process Algebra
Extended Abstract

by

F.S. de Boer, J.W. Klop, C. Palamidessi

91/35

Computing Science Note 91/35
Eindhoven, December 1991
This is a series of notes of the Computing Science Section of the Department of Mathematics and Computing Science Eindhoven University of Technology. Since many of these notes are preliminary versions or may be published elsewhere, they have a limited distribution only and are not for review. Copies of these notes are available from the author.

Copies can be ordered from:
Mrs. F. van Neerven
Eindhoven University of Technology
Department of Mathematics and Computing Science
P.O. Box 513
5600 MB EINDHOVEN
The Netherlands
ISSN 0926-4515

All rights reserved
editors: prof.dr.M.Rem
prof.dr.K.M.van Hee.
Asynchronous Communication in Process Algebra
(Extended Abstract)

Frank S. de Boer, Jan Willem Klop, Catuscia Palamidessi

Abstract
We study the paradigm of asynchronous process communication, as contrasted with the synchronous communication mechanism which is present in process algebra frameworks such as CCS, CSP and ACP. We investigate semantics and axiomatizations with respect to various observability criteria: bisimulation, traces and abstract traces. Our aim is to develop a process theory which can be regarded as a kernel for languages based on asynchronous communication, like data flow, concurrent logic languages and concurrent constraint programming.

1 Introduction
In order to introduce the framework of asynchronous communication that will be adopted and investigated in this paper, we will first give an informal comparison with synchronous communication as in ACP [BK86]. Synchronous communication is modeled in ACP by a binary function \( \cdot \) on actions. In the case of value transmission the typical equation is \( c|d | c|d = c\#d \), where the actions \( c|d \) and \( c|d \) are interpreted as "send datum \( d \) along channel \( c \)" and "receive datum \( d \) at channel \( c \)" respectively, and \( c\#d \) represents the completion of the communication action. As an example, consider the parallel composition

\[
\partial_{\{c|d,c|d\}}(a \cdot c|d \cdot b \parallel a' \cdot c|d \cdot b').
\]

Here \( \partial \) is the encapsulation operator, enforcing the intended communication by acting as a garbage collector for attempted but failed communications. According to the axioms of ACP this expression corresponds to the process graph represented in Figure 1(a). In this figure, the dashed parts express the unintended traces that are pruned by \( \partial_{\{c|d,c|d\}} \).

Note that there is no difference in directionality between the communication partners \( c|d, c|d \). In the asynchronous setting, on the other hand, there is an asymmetry between \( c|d \) and \( c|d \): one of them, \( c|d \), is now supposed to precede its partner \( c|d \), for an indeterminate amount of 'time' (i.e. number of steps). Due to the temporal split between \( c|d \), \( c|d \), we need now two actions signifying their completion; let them be \( c\downarrow d \) and \( c\uparrow d \), respectively. Furthermore, some memory mechanism, in the form of a state operator, must now be available to convey the effect...
of the event $c \uparrow d$ during the interval from $c \uparrow d$ to $c \downarrow d$. Let us now consider the asynchronous counterpart of the example above. The evaluation of
\[
\mu_r^c(a \cdot c \downarrow d \parallel a' \cdot c \uparrow d \cdot b'),
\]
where $\mu$ is the state operator, by using the axioms in aprPA$_{\delta,\mu}$ (see Table 2) gives now the process graph in Figure 1(b). Again the dashed parts express the unintended traces, originating by free interleaving, that are pruned away by $\mu$.

Just as in the synchronous case, one might wish to abstract from these completed actions. The representation of the processes from the example above 'shrinks' by this abstraction to the process graphs in Figure 2.

Note that both the operators $\partial, \mu$, can be viewed as 'actualization' operators, that make the process actually run. So we refer to $c \uparrow d, c \downarrow d$ actions as being completed, or realized, and to $c \downarrow d, c \uparrow d$ actions as being intended, or possible.

In specifying the send and receive data transmission scheme there is a choice to be made, concerning the nature of the channels. In this paper we will treat the two main cases of 'sequential access' and 'random access'. Of the first we have chosen as a typical representant the queue (but we may also have investigated the case of stack); in the second, the bag is a natural choice.

Our point of departure is the paper [BKT85] where the send/receive mechanism is axiomatized, both for queues and bags as channels. We show that this axiomatization is complete for the 'minimal' setting of bisimulation semantics. Here the specific nature of the communication channels does not yet influence the axiomatization which can be given in a uniform way.
The next notion we investigate is the 'maximal trace-respecting congruence'. We give a characterization of this congruence in terms of a fully abstract model which is a version of the usual failure semantics for synchronous communication ([BHR84]), and we provide a complete axiomatization. Remarkably, for this more abstract notion the above uniformity between queues and bags disappears.

Finally we consider traces with abstraction from the completed communication actions. As usual, the phenomenon of abstraction introduces some quite intricate problems. At this point the difference between bags and queues becomes very prominent: the case of bags requires the introduction of many new axioms, thus identifying more expressions. Therefore we can call the latter theory (for bags) more abstract than the former (for queues). A priori this was to be expected since a bag in itself is already an 'abstraction' of a queue.

1.1 Comparison with related work

A theory for asynchronous communication has also been developed in [JHJ90]. That theory is more abstract than ours; the main reasons are that in [JHJ90] there are, first, some restrictions on processes to be composed in parallel, and, second, communication is modeled in such a way that when a process receives an item from a buffer, that item remains available for the other processes. Such a mechanism can be implemented in our language by means of a copying process; therefore all the contexts which can be specified in [JHJ90] can be specified also in our language. On the other hand, some of our contexts cannot be defined in [JHJ90] (i.e. our congruence is strictly less coarse).

The relatively 'low degree of abstraction' of our language has the advantage that we can regard it as a kernel for the axiomatization of other languages based on asynchronous communication. It is possible to show, in fact, that with respect to both observability criteria we have considered in this paper our axioms are correct for data flow [Kah74], concurrent logic programming [Sha89], and concurrent constraint programming [Sar89]. In other words, the communication mechanisms of those languages can be implemented in ours. Completeness can then be obtained by adding some specific axioms.

The fact that we construct a fully abstract model based on failure sets might look surprising, and in contrast with the claim, often made, that asynchronous communication does not require refusal information. In fact, recent studies have shown that several languages based on asynchronous communication have linear models: see for instance [Jon85, Jos90] for data flow, [BP90] for concurrent logic languages, [BP91] for concurrent constraint programming and [BKPR91] for a general semantic framework based on reactive sequences. The explanation of this apparent contradiction is that also these last models encode some hidden refusal information. In this paper we have opted for a model in which the refusals are explicitly represented because it facilitates the proof of the completeness of the axiomatization.

2 Bisimulation semantics for asynchronous communication

In this section, that is the basis of our paper, our starting point is [BKT85]. After fixing the notation and the syntax of the language to be considered, we provide a set of transition rules defining its operational semantics.

---

1By 'traces' we mean the 'completed' ones, i.e. the traces associated to the transition sequences which end in a point from which no further transitions are possible.
2.1 Syntax

The set of actions is structured as follows.

1. $A$ is a set of proper actions, notation: $a, b, a_1, a_2, \ldots$

2. Let $D$ be a set of data: $d, d_1, d_2, \ldots$, and let $C$ be a set of channel names: $c, e, c_1, c_2, \ldots$.

   For all $c \in C$ and $d \in D$ we have communication actions

   - $c|d$ (intended input action)
   - $c|d$ (intended output action)
   - $c\downarrow d$ (completed input action)
   - $c\uparrow d$ (completed output action)

   The set of all intended input actions is $C\downarrow$; likewise $C\uparrow, C\downarrow, C\uparrow$ contain the intended output actions, the completed input actions and the completed output actions respectively.

   The action alphabet $Act$ is now defined to be

   $$Act = A \cup C\downarrow \cup C\uparrow \cup C\uparrow \cup C\downarrow\uparrow.$$

   We will write $u, v, \ldots$ for general actions from $Act$. Intended input actions from $C\downarrow$ are also called dependent actions (Dep); all the other actions are independent (Ind) (see Figure 3). In Section 2.2 we give motivation for this terminology.

   The set $Exp$ of (process) expressions is generated by the following grammar:

   $$x ::= | \delta | u \cdot x | x_1 + x_2 | x_1 || x_2 | x_1 \parallel x_2 | \mu^c_x(x) | \rho_f(x).$$

   The constant $\delta$ represents the inaction or deadlock. For any $u \in Act$, $u \cdot$ is an action prefixing. The operators $+$, $||$ and $\parallel$ are the sum (or alternative choice), the merge (or parallel composition), and the left-merge respectively. For any $c \in C$ and state $\sigma$, $\mu^c_\sigma$ is an encapsulation operator ($\sigma$ represents the ‘initial state’ of $c$). Finally for $f : Act \to Act$ respecting the partition of $Act$, $\rho_f$ is a renaming operator.

   Bracket conventions are employed as usual. Instead of $u \cdot x$ we also will write $u x$. Often we will omit the ‘end marker’ $\delta$ in an expression, and render e.g. $a \delta$ as just $a$. 

Figure 3: The set of actions. Shaded: dependent actions; unshaded: independent actions.
2.2 Operational semantics

In order to define the operational semantics of our processes in a uniform way, i.e. not depending upon the specific kind of channels that are intended, we treat channels as given by some abstract data type. To describe the meaning of the actions \( c \downarrow d \) and \( c \uparrow d \), we introduce two operations

\[
\text{get}: \text{State} \times D \rightarrow \text{State} \cup \{ \bot \} \quad \text{and} \quad \text{put}: \text{State} \times D \rightarrow \text{State},
\]

where \( \text{State} \) is the set of states (of the channel), and \( \bot \) stands for undefined. The understanding is that \( \text{get}(\sigma, d) \) checks if the datum \( d \) is available in \( \sigma \) and in that case it retrieves it. It is undefined otherwise. This is the reason why we call the actions in \( C \downarrow \) 'dependent': their being enabled or not depends upon the content of the buffers, hence upon the actions performed by the environment. The operation \( \text{put}(\sigma, d) \) in general modifies \( \sigma \) by adding the datum \( d \). We assume that it is always defined, and this is the reason why we call the actions in \( C \uparrow \) 'independent'. One could wonder what happens, in the case of bounded channels, when the channel is full. We assume that in such a case the datum is simply lost. The reason is that in general a test on the state of the channel, before performing a send action, is very expensive to implement. However, our theory can be modified so as to include such a test by adding the possibility that \( \text{put}(\sigma, d) \) is undefined and by treating the actions in \( C \uparrow \) as dependent.

The operational semantics of an expression \( x \in \text{Exp} \) is defined by the transition system \( T \) in Table 1, where \( x, y, z \) are meta-variables ranging over \( \text{Exp} \).

To each process expression \( x \in \text{Exp} \) the transition system \( T \) assigns a transition graph (also called process graph), as illustrated in the examples shown in Figure 4. The symbol \( \varepsilon \) denotes the state of an empty channel. We denote by \( \sim \) the well known bisimulation equivalence, which identifies expressions with the same transition graph (disregarding the labels in the nodes). Examples of bisimilar processes are the pairs (i), (ii) and (v) in Figure 4.

2.3 Axioms

The bisimulation equivalence \( \sim \) is a congruence and it is completely axiomatized by the system \( \text{aprPA}_{\delta, \mu} \) in Table 2, which is the one from [BKT85] restricted to action prefixing. In our paper we don't consider sequential composition, just for reasons of technical convenience. We expect that all results in the present paper can be obtained also in that more general case, but at the cost of sometimes having to include 'degenerate' versions of some axioms. The name \( \text{aprPA}_{\delta, \mu} \) means 'action prefixing process algebra with constant \( \delta \) and operator \( \mu \)'; it is based on the nomenclature proposal in [BB91].

**Theorem 2.1** Let \( x, y \in \text{Exp} \). Then

\[
x = y \iff \text{aprPA}_{\delta, \mu} \vdash x = y
\]

3 Trace semantics

In this section we study the observability criterion which consists of observing all the possible traces generated by a process in a sequence of transition steps. It is convenient to introduce the following notation. For \( x, y \in \text{Exp}, s \in \text{Act}^* \), \( x \xrightarrow{s} y \) represents a sequence of transition steps from \( x \) to \( y \) and it is defined as follows:

1. \( x \xrightarrow{\lambda} x \) (where \( \lambda \) is the empty sequence),
2. if \( x \xrightarrow{u} y \) then \( x \xrightarrow{u} y \),
<table>
<thead>
<tr>
<th>Rule</th>
<th>Transition</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>$u x \xrightarrow{u} x$</td>
</tr>
<tr>
<td>R2</td>
<td>$x \xrightarrow{u} y \quad x + z \xrightarrow{u} y \quad z + x \xrightarrow{u} y$</td>
</tr>
<tr>
<td>R3</td>
<td>$x \xrightarrow{u} y \quad x \parallel z \xrightarrow{u} y \parallel z \quad z \parallel x \xrightarrow{u} z \parallel y$</td>
</tr>
<tr>
<td>R4</td>
<td>$x \xrightarrow{u} y \quad x \parallel z \xrightarrow{u} y \parallel z$</td>
</tr>
<tr>
<td>R5</td>
<td>$\frac{x}{\mu_c(x)} \xrightarrow{cd} \frac{y}{\mu_c(y)}$ if $\sigma' = \text{put}(\sigma, d)$</td>
</tr>
<tr>
<td>R6</td>
<td>$\frac{x}{\mu_c(x)} \xrightarrow{cd} \frac{y}{\mu_c(y)}$ if $\sigma' = \text{get}(\sigma, d) \neq \perp$</td>
</tr>
<tr>
<td>R7</td>
<td>$x \xrightarrow{v} y$ if $u \neq c</td>
</tr>
<tr>
<td>R8</td>
<td>$x \xrightarrow{u} y$ if $\rho_f(x) \xrightarrow{f(u)} \rho_f(y)$</td>
</tr>
</tbody>
</table>

Table 1: The transition system $T$. 
Figure 4: Examples of transitions.
<table>
<thead>
<tr>
<th>A1</th>
<th>$x + y = y + x$</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2</td>
<td>$(x + y) + z = x + (y + z)$</td>
</tr>
<tr>
<td>A3</td>
<td>$x + x = x$</td>
</tr>
<tr>
<td>A4</td>
<td>$x + \delta = x$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>M1</th>
<th>$x \parallel y = x \parallel y + y \parallel x$</th>
</tr>
</thead>
<tbody>
<tr>
<td>M2</td>
<td>$\delta \parallel x = \delta$</td>
</tr>
<tr>
<td>M3</td>
<td>$u x \parallel y = u(x \parallel y)$</td>
</tr>
<tr>
<td>M4</td>
<td>$(x + y) \parallel z = x \parallel z + y \parallel z$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E1</th>
<th>$\mu^\sigma_c(\delta) = \delta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>E2</td>
<td>$\mu^\sigma_c(u x) = u \cdot \mu^\sigma_c(x)$ if $u \neq c \upharpoonright d, c \downarrow d$</td>
</tr>
<tr>
<td>E3</td>
<td>$\mu^\sigma_c(c \uparrow d \cdot x) = c \uparrow d \cdot \mu^\sigma_c(x)$ if $\sigma' = \text{put}(\sigma, d)$</td>
</tr>
<tr>
<td>E4</td>
<td>$\mu^\sigma_c(c \downarrow d \cdot x) = c \downarrow d \cdot \mu^\sigma_c(x)$ if $\sigma' = \text{get}(\sigma, d) \neq \perp$</td>
</tr>
<tr>
<td>E5</td>
<td>$\mu^\sigma_c(c \downarrow d \cdot x) = \delta$ if $\text{get}(\sigma, d) = \perp$</td>
</tr>
<tr>
<td>E6</td>
<td>$\mu^\sigma_c(x + y) = \mu^\sigma_c(x) + \mu^\sigma_c(y)$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RN1</th>
<th>$\rho_f(\delta) = \delta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>RN2</td>
<td>$\rho_f(u x) = f(u) \cdot \rho_f(x)$</td>
</tr>
<tr>
<td>RN3</td>
<td>$\rho_f(x + y) = \rho_f(x) + \rho_f(y)$</td>
</tr>
</tbody>
</table>

Table 2: aprPA$_{\delta,\mu}$. 
Figure 5: Example of trace-equivalent processes $x$ and $y$ which can be distinguished by a $\mu$-context.

3. if $x \xrightarrow{s} y$ and $y \xrightarrow{t} z$ then $x \xrightarrow{s t} z$.

Now we can define the traces of a process and the corresponding equivalence relation.

**Definition 3.1** For $x \in \text{Exp}$, the traces of $x$ are given by:

$$T(x) = \{s \mid \exists y. x \xrightarrow{s} y \not\rightarrow\}$$

The notation $\not\rightarrow$ indicates that for no $u, z$ we have $y \xrightarrow{u} z$.

The relation $\sim_\tau$ is the equivalence induced by the traces:

$$x \sim_\tau y \iff T(x) = T(y).$$

This relation is not a congruence, essentially due to the presence of the encapsulation operator $\mu$ which enforces a dependency upon the state of the channels, as determined by the initial state and by the actions performed by the environment.

**Example 3.2**

1. The processes $x$ and $y$ represented by the transition graphs in Figure 5 have the same traces, but their encapsulation with respect to the channel $c$ yields different results: $T(\mu_c(x)) = \{ab\}$, whereas $T(\mu_c(y)) = \{a, ab\}$.

2. The processes $x$ and $y$ represented in Figure 6, have the same traces, but if we now consider them in parallel with the process $z$ then encapsulation with respect to $c$, $e$ yields a difference: $e \uparrow d \cdot c \uparrow d \cdot e \downarrow d \in T(\mu_c^\langle z \parallel z \rangle) \setminus T(\mu_c^\langle x \parallel z \rangle)$.

In the following, $C[\cdot]$ indicates an arbitrary (unary) context, i.e. an expression containing one occurrence of a 'hole'. We define the congruence relation $\equiv_\tau$ as the *maximal trace-respecting congruence*, i.e.

$$x \equiv_\tau y \iff \forall C[\cdot]. C[x] \sim_\tau C[y].$$

In the rest of this section we will investigate a concrete model corresponding to this congruence, and its axiomatization.
Figure 6: Example of processes $x$ and $y$ which can be distinguished by a parallel process $z$.

3.1 Failure semantics

It has been shown in [BK088] that in the synchronous case of ACP with one-to-one communication failure semantics ([BHR84]) is fully abstract with respect to trace equivalence. We will show how to modify it so that this property is maintained. We first construct the failure model for bags and then we show how to adapt it to the case of queues.

Let us first show why the standard failure model is not fully abstract.

Example 3.3 Figure 7 shows three examples of pairs of processes $x$, $y$ which are not identified by the standard failure model; yet their traces are the same in every context.

The main reason why the expressions $x$ and $y$ in Figure 7 are trace-congruent is that the independent actions are always enabled regardless of the state. This is not true for the input actions.

Example 3.4 Figure 8 shows that the input counterparts $x'$ and $y'$ of the processes $x$ and $y$ in Figure 7 can be distinguished by a parallel process $z$. In all cases there is a trace generated by $\mu_c(x' | z)$, which is not generated by $\mu_c(y' | z)$.

The relevant information is associated with the resting points, those points from where the process can only proceed by input actions, and consists of the trace which leads to such a point and the state which make such a point stable, i.e., none of the initial input actions are enabled.

As such, we can represent a state by a subset of the complement of the ready set, i.e., the set of initial actions, associated with a resting point. We call such a representation a refusal set. However, the intuition is that when an input action $c|d$ occurs in the refusal set this indicates that the value $d$ is available on channel $c$.

Definition 3.5 The failure set of $x$ is

$$F[x] = \{ (s, R) | \exists y. x \rightsquigarrow y, Init(y) \subseteq Dep, R \subseteq Dep \setminus Init(y) \}$$

where $Init(x) = \{ u | \exists y. x \rightsquigarrow y \}$.

The relation $\equiv_F$ is the equivalence induced by the failure sets, i.e.

$$x \equiv_F y \text{ iff } F[x] = F[y]$$
Figure 7: Examples of trace-congruent processes $x$, $y$ with different standard failure semantics.
Figure 8: Examples of processes $x'$, $y'$ which can be distinguished by a process $z$. 
This relation $\equiv_\tau$ is actually a congruence. To show this, it is sufficient to prove that the definition of $F$ is compositional with respect to all the operators of the language, i.e. every operator of the language has a semantical counterpart. We give only the definition for action prefixing and encapsulation, the other operators are as in the standard case.

**Definition 3.6** Let $P,Q$ range over the domain of $F$.

Prefixing $\bar{u}.P = \begin{cases} \{(us,R) \mid (s,R) \in P\} & \text{if } u \notin \text{Dep} \\ \{(us,R) \mid (s,R) \in P\} \cup \{(\lambda,R) \mid R \subseteq \text{Dep} \setminus \{u\}\} & \text{otherwise,} \end{cases}$

**Encapsulation.** We first define the operator $\hat{\mu}_c^\tau : \text{Act}^* \rightarrow \text{Act}^* \cup \text{Act}^*\delta$ as the operator on traces which transforms communication actions on $c$ into completed ones, and the auxiliary operator $\bar{S}^\tau_c : \text{Act}^* \rightarrow \text{State}$ which computes the current state (on $c$) at every point of the trace:

\[
\begin{align*}
\hat{\mu}_c^\tau(\lambda) &= \lambda & S^\tau_c(\lambda) &= \sigma \\
\hat{\mu}_c^\tau(us) &= u \cdot \hat{\mu}_c^\tau(s) & S^\tau_c(us) &= S^\tau_c(s) & \text{if } u \neq c|d,c|d \\
\hat{\mu}_c^\tau(c|d\cdot s) &= c \uparrow d \cdot \hat{\mu}_c^\tau(s) & S^\tau_c(c|d\cdot s) &= S^\tau_c(s) & \text{if } \sigma' = \text{put}(\sigma,d) \\
\hat{\mu}_c^\tau(c\downarrow d\cdot s) &= c \downarrow d \cdot \hat{\mu}_c^\tau(s) & S^\tau_c(c\downarrow d\cdot s) &= S^\tau_c(s) & \text{if } \sigma' = \text{get}(\sigma,d) \neq \bot \\
\hat{\mu}_c^\tau(c|d\cdot s) &= \delta & S^\tau_c(c|d\cdot s) &= \bot & \text{if } \text{get}(\sigma,d) = \bot
\end{align*}
\]

Next we extend $\hat{\mu}_c^\tau$ on pairs as follows:

\[
\hat{\mu}_c^\tau(P) = \{(\mu_c^\tau(s), R) \mid \exists (s,R') \in P, R \subseteq R' \cup \{c|d \mid d \in D\}, S^\tau_c(s) \neq \bot, (c|d \notin R' \Rightarrow S^\tau_c(s \cdot c|d) = \bot)\}
\]

The failure semantics is correct with respect to the traces, in fact $T(x) = \{s \mid (s, \text{Dep}) \in F[z]\}$. Since $\equiv_\tau$ is a trace-respecting congruence, it is at least as fine as $\equiv_T$ (which, by definition, is the maximal trace-respecting congruence).

**3.2 Axioms**

We now present the axioms to add to aprPA$_{\delta,\mu}$ in order to obtain a complete axiomatization of the failure semantics introduced above.

In the synchronous case a complete axiomatization for failure semantics has been obtained by adding to the theory of ACP the ready axioms and the failure axiom ([BKO88]) which, restricted to the case of aprPA$_\delta$, are respectively the axioms $R$ and $S$ in Table 3. Our failure semantics is at least as abstract as that semantics in [BKO88], in fact it can be retrieved by considering (only) those pairs in which the refusal set contains all independent actions. Therefore the axioms $R$ and $S$ are valid in our semantics. On the other hand, our semantics is strictly more abstract because it cancels branching points from which an independent action exits. Axiomatically this is modeled by factorizing the plus operator with respect to the independent actions: see axiom I in Table 3, where $i$ stands for any independent action, i.e. $i \in \text{Act} \setminus C1$.

Note that if we generalize $i$ in the axiom I to be any action we obtain a system equivalent to the one presented in [vGla90] as the axiomatization of (completed) trace semantics for aprPA$_\delta$.  

13
$ux+u(y+z) = u(vx_1+y_1)+u(vx_2+y_2) + u(vx_1+vx_2+y_2)$

$ux + u(y+z) = u(x+y) + u(y+z)$

$I \ u(ix+y) = u(ix+y) + ui x$

Table 3: The failure axioms for asynchronous communication.

Theorem 3.7 (Completeness) For all $x, y \in \text{Exp}$ we have

$$x \equiv_T y \iff \text{aprPA}_{6,\mu} \cup \{R, S, I\} \vdash x = y$$

3.3 Full abstraction of failure semantics

In this section we show how to specialize the failure semantics given above to the cases of random access (bags) and sequential access (queues).

Bags. In the case of bags the fully abstract semantics is just the failure semantics $F$.

Proposition 3.8 (Full abstraction) If channels are bags then $\equiv_T \subseteq \equiv_F$.

Corollary 3.9 If channels are bags then for $x, y \in \text{Exp}$ the following are equivalent.

1. $x \equiv_F y$,
2. $x \equiv_T y$,
3. $\text{aprPA}_{6,\mu} \cup \{R, S, I\} \vdash x = y$.

Queues. The distinguishing feature of sequential access is that only one of the items stored in a channel can be read and consumed. As a consequence, the failure semantics as defined above is not fully abstract. For instance, it distinguishes the processes $x = a \cdot c_{d_1} + a \cdot c_{d_2} + a \cdot c_{d_3}$ and $y = a(c_{d_1} + c_{d_2}) + a(c_{d_2} + c_{d_3}) + a(c_{d_3} + c_{d_1})$ which in case of sequential access are observationally identical. Since for each channel only one item is relevant for the observable behaviour of a process, we must consider only those refusal sets in which no more than one input on the same channel is present.

Definition 3.10 The queue failure set of $x \in \text{Exp}$ is

$$F_\text{q}[x] = \{(s, R) \in F[x] \mid c[d, c'd] \in R \Rightarrow d = d'\}$$

Let $\equiv_{\text{q}}$ be the associated equivalence relation. It is possible to show that $\equiv_{\text{q}}$ is a congruence and that it is as coarse as $\equiv_T$. We will specify now a subset of the language for which the completeness holds. Consider the subset $\text{Exp}'$ of expressions in which an input action on a channel $c$ can occur only in contexts of the form $\Sigma_{d \in Dc} d \cdot x_d$. So, the typical feature of this sublanguage is that it cannot perform anymore a blocking test on the presence of a specific
datum. Expressions of this forms are used in Process Algebra to implement 'input on a variable', i.e. CSP-like actions of the form $c[V \cdot x[V]]$, where $V$ is a variable of type $D$. For expressions in $Exp'$ the semantics $F$ and $F^\delta$ are the same, i.e. $F^\delta[x] = F^\delta[y] \iff F[x] = F[y]$. Therefore we obtain:

**Corollary 3.11** If channels are queues then for $x, y \in Exp'$ the following are equivalent

1. $x \equiv_{F} y$,
2. $x \equiv_{F} y$,
3. $x \equiv_{T} y$,
4. $aprPA_{\delta,\mu} \cup \{R, S, I\} \vdash x = y$.

4 Abstraction from communication

In this section we investigate an axiomatic characterization of the proper behaviour of a process, i.e., we want to encapsulate all communications and treat them as invisible (silent) steps. To this end we extend the set $Act$ to contain a special internal action $\tau$, which corresponds to the standard notion of silent step in languages like CCS and ACP. In the following, we will use the notation $\mu(x)$ as an abbreviation for the encapsulation of the process $x$ with respect to all channels, with initial content empty, i.e., if $C = \{c_1, \ldots, c_n\}$, then $\mu(x) = \mu_{c_1} \cdots \mu_{c_n}(x)$. Furthermore, we use the notation $\rho(x)$ to denote the process $x$ where all the completed actions are renamed into $\tau$. To define the proper traces we need an operator $Q$ which removes from a trace $s \in Act^*$ all the $\tau$ actions. The proper traces of a process are then defined as follows:

$$T_r(x) = \sigma \circ T(\rho(x))$$

The relation $\sim_{T_r}$ is the equivalence induced by the proper traces:

$$x \sim_{T_r} y \iff T_r(x) = T_r(y)$$

The congruence relation $\equiv_{T_r}$ is the maximal proper-trace-respecting congruence:

$$x \equiv_{T_r} y \iff \forall C[\cdot]. C[x] \sim_{T_r} C[y]$$

We now investigate an axiomatization for $\equiv_{T_r}$. The axioms for $\tau$-abstraction which have been studied for the failure semantics (and therefore for the maximal proper-trace-respecting congruence) in the presence of synchronous communication ([BKO88]) are, of course, still valid in our asynchronous case. Restricted to the case of action prefixing only (i.e. no general sequential composition) these axioms are the ones shown in Table 4.

Note that the presence of $T1$ and $T2$ makes the axiom $S$ of Table 3 superfluous (cf. [BKO88]). However, these axioms for $\tau$-abstraction are not complete in the presence of independent actions. When $\tau$ is prefixed to an independent action $i$, it can be deleted. Formally, this is captured by the axiom in Table 5. In the presence of the axiom $T3$, the axiom $I$ of Table 3 can be shown to be derivable.

Furthermore we observe that processes like $c[d \cdot a]$ and $c[d \cdot a + a \cdot c]d$ are now observably equivalent. This identification is captured axiomatically by the law in Table 6.

Note that the reverse of this law is not correct (an output cannot be anticipated). For instance, $a \cdot c[d]$ and $a \cdot c[d] + c[d \cdot a]$ are not observably equivalent. A distinguishing context
\begin{align*}
T_1 & \quad \mu \tau x = ux \\
T_2 & \quad \tau x + y = \tau x + \tau (x + y)
\end{align*}

Table 4: \(\tau\)-abstraction laws for the failure semantics in the synchronous case.

\begin{equation}
T_3 \quad \tau i x = ix
\end{equation}

Table 5: Additional \(\tau\)-abstraction law for independent actions.

is \(C[\cdot] = c\mid d\cdot b \parallel \cdot\). The process \(C[a\cdot c\mid d]\) will produce \(ab\) only, whereas \(C[a\cdot c\mid d + c\mid d\cdot a]\) will produce additionally \(ba\). In the full paper we show that the above axiom system completely characterizes \(T_r\) in the case of queues.

**Theorem 4.1 (Completeness for queues)** For all \(x, y \in \text{Exp}'\) we have

\[x \equiv_T r y \iff \text{aprPA}_{T_r} \cup \{R, T_1 - 3, \text{OP}\} \vdash x = y\]

However, when we consider abstraction from communication in the case of bags, many additional identifications have to be made. First we observe that we have to abstract from the order between (intended) output actions, i.e., the processes \(c\mid d \cdot e\mid d'\) and \(e\mid d' \cdot c\mid d\) are observably equivalent. A simple axiomatization of this phenomenon can be given in terms of multisets of output actions, so-called combined actions, which we denote by \(\vec{c}\). The intended meaning of a combined action is that of a concurrent execution of its components. In Table 7 the multiset union is denoted by \(\cup\).

Another class of identifications stems from the fact that in the case of bags we are not in general able to detect whether a process intends to read an item.

**Example 4.2** The process \(a \cdot c\mid d\) is observably equivalent to the process \(a \cdot c\mid d + a\). Note that in the case of queues these processes can be distinguished by the process \(c\mid d \cdot c\mid d' \cdot c\mid d' \cdot b (d \neq d')\), which will always produce \(b\) when put in parallel with the first process, while the input action \(c\mid d'\) can be blocked in case the second process chooses the branch \(a\).

\begin{equation}
\text{OP} \quad c\mid d(a x + y) = c\mid d(a x + y) + a \cdot c\mid d\cdot x
\end{equation}

Table 6: Delay axiom for output actions.
Table 7: Abstraction axiom for output actions.

<table>
<thead>
<tr>
<th>Axiom</th>
<th>Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>( \varepsilon(x + y) = \varepsilon(x + y) + (\varepsilon \cup \varepsilon)x )</td>
</tr>
<tr>
<td>12</td>
<td>( \varepsilon(x + y) + \varepsilon y = (\varepsilon \cup \varepsilon)x + \varepsilon y )</td>
</tr>
<tr>
<td>13</td>
<td>( u(\varepsilon \delta + x) = u(\varepsilon \delta + x) + u x )</td>
</tr>
<tr>
<td>14</td>
<td>( u(\varepsilon x + y) = u(\varepsilon x + y) + u(\varepsilon \circ x + y) )</td>
</tr>
<tr>
<td>15</td>
<td>( \Sigma_i u \cdot \Sigma_j e_i x_{ij} = \Sigma_i u \cdot \Sigma_j e_i x_{ij} + u \cdot \Sigma_k e_k x_k ) (( \forall f \in I \to J. \exists e_k \subseteq \bigcup_i e_{f(i)} ))</td>
</tr>
</tbody>
</table>

Table 8: Abstraction axioms for input actions.

Example 4.3 Another characteristic example is that of the process \( d \cdot e \cdot d' + e \cdot d' \) which is observably equivalent to \( e \cdot d' \cdot c \cdot d + c \cdot d \). Note that \( c \cdot d \cdot e \cdot d' \) and \( e \cdot d' \cdot c \cdot d \) are not observably equivalent: \( c \cdot d \cdot e \cdot d' \) in parallel with \( c \cdot d \cdot c \cdot d \cdot a \) can produce the empty sequence while putting \( c \cdot d \cdot c \cdot d \cdot a \) in parallel with \( e \cdot d' \cdot c \cdot d \) will always produce \( a \).

These and other related identifications we describe in terms of combined input actions, which we denote by \( c \). Below we give an informal explanation of the axioms of Table 8.

Axiom 11 introduces combined input actions, and states that, when both \( c \) and \( e \) are enabled, the process \( c \cdot e + y \) can always select the branch \( e x \). It should be noted that the equality \( c(e_0 x_0 + e_1 x_1) = (c \cup e_0) x_0 + (c \cup e_1) x_1 \) does not hold: the first process, when put in parallel with \( c \cdot e \cdot a \) can generate the empty sequence by "stealing" the data.

Axiom 12 allows to determine an order in the input actions of \( c \cup e \), say, executing \( e \) before \( c \), in the presence of an alternative starting with \( e \).

Axiom 13 can be informally justified as follows: suppose the process \( u x \) deadlocks after \( u \). In that case the process \( u(\varepsilon \delta + x) \) either deadlocks immediately after \( u \) or it can select the branch \( \varepsilon \delta \) and so will deadlock eventually.

Axiom 14 The auxiliary operator \( \diamond \) in this axiom reveals the "hidden eager nature" of a process. It is axiomatized in Table 9.

Axiom 15 Here \( i \) is to be understood to range over \( I \), \( j \) over \( J \), and \( k \) over \( K \subseteq \{ i_j \mid i \in I, j \in J \} \). This axiom can be justified as follows: suppose the process \( \Sigma_k e_k x_k \) deadlocks
\[ \xi \circ a = a \]
\[ \xi \circ \xi = (\xi U \xi) x \]
\[ \xi \circ (x + y) = \xi \circ x + \xi \circ y \]

Table 9: Axioms for the operator \( \xi \).

\[
\begin{align*}
\text{OI} & \quad \overline{c}(\xi x + y) = \overline{c}(\xi x + y) + \xi \overline{c} x \\
\text{OP} & \quad \overline{c}(a x + y) = \overline{c}(a x + y) + a \overline{c} x \\
\text{PI} & \quad a(\xi x + y) = a(\xi x + y) + \xi a x 
\end{align*}
\]

Table 10: Abstraction from the order of events.

after \( u \), so all the \( c_k \) are disabled. This deadlock possibility then should be covered by a process \( u : \Sigma_j \xi_{i_j} x_{i_j} \), that is, all the \( c_{i_j} \) are disabled, for some \( i \). Otherwise we would have that there exists for every \( i \in I \) a \( j \in J \) such that \( c_{i_j} \) is enabled, which, in its turn, would imply the existence of an enabled \( c_k \).

The axioms of Table 10 allow abstraction from the order of certain events.

The first axiom of Table 11 allows the abstraction from an output action immediately followed by its corresponding input. The second axiom is a slightly stronger version of the first one. The last axiom states that putting a read datum immediately back, is essentially, unobservable.

In the full paper we prove the completeness of the above axiom system for normal processes, i.e., processes in which there occur no combined input or output actions.

\[
\begin{align*}
\text{T4} & \quad \overline{c}(\xi x + y) = \overline{c}(\xi x + y) + x \\
\text{T5} & \quad \overline{c}(i x + y) + \tau z =\overline{c}(i x + y + \xi z) \\
\text{T6} & \quad x = x + \xi \overline{c} x 
\end{align*}
\]

Table 11: Abstraction from cancelled output and input actions.
Theorem 4.4 (Completeness for bags) For all normal processes \( x \) and \( y \) we have

\[ x \equiv^* y \iff \text{aprPA}_{\delta,\mu} \cup \{ R, T1 - 6, O, T1 - 5, O1, OP, P1 \} \vdash x = y \]

The main idea of this proof is the semantic modelling of the additional identifications introduced by each axiom by means of a corresponding closure condition. We then show that for the resulting compositional model \( P_\delta \) the following holds: for every process \( x \) there exists a process \( y \) such that \( P_\delta[x] = F[y] \) and \( x = y \) is derivable from the axioms.

References


In this series appeared:

<table>
<thead>
<tr>
<th>No.</th>
<th>Authors</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>89/1</td>
<td>E.Zs.Lepoeter-Molnar</td>
<td>Reconstruction of a 3-D surface from its normal vectors.</td>
</tr>
<tr>
<td>89/2</td>
<td>R.H. Mak, P.Struik</td>
<td>A systolic design for dynamic programming.</td>
</tr>
<tr>
<td>89/3</td>
<td>H.M.M. Ten Eikelder, C. Hemerik</td>
<td>Some category theoretical properties related to a model for a polymorphic lambda-calculus.</td>
</tr>
<tr>
<td>89/4</td>
<td>J.Zwiers, W.P. de Roever</td>
<td>Compositionality and modularity in process specification and design: A trace-state based approach.</td>
</tr>
<tr>
<td>89/5</td>
<td>Wei Chen, T.Verhoeff, J.T.Udding</td>
<td>Networks of Communicating Processes and their (De-)Composition.</td>
</tr>
<tr>
<td>89/6</td>
<td>T.Verhoeff</td>
<td>Characterizations of Delay-Insensitive Communication Protocols.</td>
</tr>
<tr>
<td>89/7</td>
<td>P.Struik</td>
<td>A systematic design of a parallel program for Dirichlet convolution.</td>
</tr>
<tr>
<td>89/9</td>
<td>K.M. van Hee, P.M.P. Rambags</td>
<td>Discrete event systems: Dynamic versus static topology.</td>
</tr>
<tr>
<td>89/10</td>
<td>S.Ramesh</td>
<td>A new efficient implementation of CSP with output guards.</td>
</tr>
<tr>
<td>89/11</td>
<td>S.Ramesh</td>
<td>Algebraic specification and implementation of infinite processes.</td>
</tr>
<tr>
<td>89/12</td>
<td>A.T.M.Aerts, K.M. van Hee</td>
<td>A concise formal framework for data modeling.</td>
</tr>
<tr>
<td>89/14</td>
<td>H.C.Haesen</td>
<td>ELDA, data manipulatie taal.</td>
</tr>
<tr>
<td>89/15</td>
<td>J.S.C.P. van der Woude</td>
<td>Optimal segmentations.</td>
</tr>
<tr>
<td>89/16</td>
<td>A.T.M.Aerts, K.M. van Hee</td>
<td>Towards a framework for comparing data models.</td>
</tr>
<tr>
<td>89/17</td>
<td>M.J. van Diepen, K.M. van Hee</td>
<td>A formal semantics for Z and the link between Z and the relational algebra.</td>
</tr>
</tbody>
</table>
90/1  W.P.de Roever-  
H.Barringer-  
C.Courcoubetis-D.Gabbay  
R.Gerth-B.Jonsson-A.Pnueli  
M.Reed-J.Sifakis-J.Vytopil  
P.Wolper

Formal methods and tools for the development of distributed and real time systems, p. 17.

90/2  K.M. van Hee  
P.M.P. Rambags

Dynamic process creation in high-level Petri nets, pp. 19.

90/3  R. Gerth

Foundations of Compositional Program Refinement - safety properties -, p. 38.

90/4  A. Peeters

Decomposition of delay-insensitive circuits, p. 25.

90/5  J.A. Brzozowski  
J.C. Ebergen

On the delay-sensitivity of gate networks, p. 23.

90/6  A.J.J.M. Marcelis


90/7  A.J.J.M. Marcelis

A logic for one-pass, one-attributed grammars, p. 14.

90/8  M.B. Josephs

Receptive Process Theory, p. 16.

90/9  A.T.M. Aerts  
P.M.E. De Bra  
K.M. van Hee

Combining the functional and the relational model, p. 15.

90/10 M.J. van Diepen  
K.M. van Hee

A formal semantics for Z and the link between Z and the relational algebra, p. 30. (Revised version of CSNotes 89/17).

90/11  P. America  
F.S. de Boer

A proof system for process creation, p. 84.

90/12  P. America  
F.S. de Boer

A proof theory for a sequential version of POOL, p. 110.

90/13  K.R. Apt  
F.S. de Boer  
E.R. Olderog

Proving termination of Parallel Programs, p. 7.

90/14  F.S. de Boer

A proof system for the language POOL, p. 70.

90/15  F.S. de Boer

Compositionality in the temporal logic of concurrent systems, p. 17.

90/16  F.S. de Boer  
C. Palamidessi

A fully abstract model for concurrent logic languages, p. 23.

90/17  F.S. de Boer  
C. Palamidessi

On the asynchronous nature of communication in logic languages: a fully abstract model based on sequences, p. 29.
<table>
<thead>
<tr>
<th>No.</th>
<th>Author(s)</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>91/02</td>
<td>R. P. Nederpelt, H.C.M. de Swart</td>
<td>Implication. A survey of the different logical analyses &quot;if...then...&quot;, p. 26.</td>
</tr>
<tr>
<td>91/03</td>
<td>J. P. Katoen, L.A.M. Schoenmakers</td>
<td>Parallel Programs for the Recognition of $P$-invariant Segments, p. 16.</td>
</tr>
<tr>
<td>91/05</td>
<td>D. de Reus</td>
<td>An Implementation Model for GOOD, p. 18.</td>
</tr>
<tr>
<td>91/06</td>
<td>K. M. van Hee</td>
<td>SPECIFICATIEMETHODEN, een overzicht, p. 20.</td>
</tr>
<tr>
<td>91/07</td>
<td>E. Poll</td>
<td>CPO-models for second order lambda calculus with recursive types and subtyping, p. 49.</td>
</tr>
<tr>
<td>91/12</td>
<td>E. van der Sluis</td>
<td>A parallel local search algorithm for the travelling salesman problem, p. 12.</td>
</tr>
<tr>
<td>91/14</td>
<td>P. Lemmens</td>
<td>The PDB Hypermedia Package. Why and how it was built, p. 63.</td>
</tr>
<tr>
<td>Paper Number</td>
<td>Authors</td>
<td>Title</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>91/16</td>
<td>A.J.J.M. Marcelis</td>
<td>An example of proving attribute grammars correct: the representation of arithmetical expressions by DAGs, p. 25.</td>
</tr>
<tr>
<td>91/18</td>
<td>Rik van Geldrop</td>
<td>Transformational Query Solving, p. 35.</td>
</tr>
<tr>
<td>91/19</td>
<td>Erik Poll</td>
<td>Some categorical properties for a model for second order lambda calculus with subtyping, p. 21.</td>
</tr>
<tr>
<td>91/23</td>
<td>K.M. van Hee, L.J. Somers, M. Voorhoeve</td>
<td>Z and high level Petri nets, p. 16.</td>
</tr>
<tr>
<td>91/24</td>
<td>A.T.M. Aerts, D. de Reus</td>
<td>Formal semantics for BRM with examples, p. 25.</td>
</tr>
<tr>
<td>91/25</td>
<td>P. Zhou, J. Hooman, R. Kuiper</td>
<td>A compositional proof system for real-time systems based on explicit clock temporal logic: soundness and completeness, p. 52.</td>
</tr>
<tr>
<td>91/27</td>
<td>F. de Boer, C. Palamidessi</td>
<td>Embedding as a tool for language comparison: On the CSP hierarchy, p. 17.</td>
</tr>
<tr>
<td>91/28</td>
<td>F. de Boer</td>
<td>A compositional proof system for dynamic process creation, p. 24.</td>
</tr>
<tr>
<td>91/30</td>
<td>J.C.M. Baeten, F.W. Vaandrager</td>
<td>An Algebra for Process Creation, p. 29.</td>
</tr>
<tr>
<td>91/31</td>
<td>H. ten Eikelder</td>
<td>Some algorithms to decide the equivalence of recursive types, p. 26.</td>
</tr>
<tr>
<td>91/33</td>
<td>W. v.d. Aalst</td>
<td>The modelling and analysis of queueing systems with QNM-ExSpect, p. 23.</td>
</tr>
<tr>
<td>91/34</td>
<td>J. Coenen</td>
<td>Specifying fault tolerant programs in deontic logic, p. 15.</td>
</tr>
<tr>
<td>91/35</td>
<td>F.S. de Boer</td>
<td>Asynchronous communication in process algebra, p. 20.</td>
</tr>
<tr>
<td></td>
<td>J.W. Klop</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C. Palamidessi</td>
<td></td>
</tr>
<tr>
<td>92/01</td>
<td>J. Coenen</td>
<td>A note on compositional refinement, p. 27.</td>
</tr>
<tr>
<td></td>
<td>J. Zwiers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>W.-P. de Roever</td>
<td></td>
</tr>
<tr>
<td>92/02</td>
<td>J. Coenen</td>
<td>A compositional semantics for fault tolerant real-time systems, p. 18.</td>
</tr>
<tr>
<td></td>
<td>J. Hooman</td>
<td></td>
</tr>
<tr>
<td>92/03</td>
<td>J.C.M. Baeten</td>
<td>Real space process algebra, p. 42.</td>
</tr>
<tr>
<td></td>
<td>J.A. Bergstra</td>
<td></td>
</tr>
</tbody>
</table>