Process algebra with autonomous actions

Citation for published version (APA):

Document status and date:
Published: 01/01/1996

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.
Process Algebra with Autonomous Actions

by

M. Voorhoeve and T. Basten

96/01

ISSN 0926-4515

All rights reserved
editors: prof.dr. R.C. Backhouse
        prof.dr. J.C.M. Baeten

Reports are available at:
http://www.win.tue.nl/win/cs
Process Algebra with Autonomous Actions

Marc Voorhoeve and Twan Basten

Eindhoven University of Technology

email: {wsinmarc,tbasten}@win.tue.nl

Abstract

This paper introduces autonomous observable actions into process algebra. These actions can be observed but cannot be controlled by an environment. The proposed extension of ACP allows verifications without silent steps and fairness assumptions. The inclusion of inequalities makes it possible to verify that an implementation satisfies a given specification, with the specification indicating exactly where the implementation may reduce nondeterminism.

1 Introduction

Process algebra studies processes that are built from actions and operators. Two kinds of actions have been extensively studied: the observable ones and the unobservable (internal or silent) action $\tau$. An observable action can occur within a process if the process is ready to perform the action and some controlling environment allows it to occur. In contrast, the silent action $\tau$ may occur without any consent. In ACP, the process algebra studied in this paper, the operators by which processes can be controlled from an environment are encapsulation and communication. Observable actions can be disabled by an environment by means of encapsulation; silent actions cannot be disabled. Similarly, observable actions are capable of communicating with actions from an environment, whereas $\tau$ is not.

This paper presents autonomous actions, which are observable, but not controllable by an environment. So they share with $\tau$ the property that they can neither be encapsulated nor participate in a communication.

The difference between autonomous actions and $\tau$ is that autonomous actions can be observed, whereas $\tau$ cannot. The fact that $\tau$ is unobservable means that an environment can only detect an occurrence of $\tau$ if the process possesses less options for continuation after the occurrence than before. This is reflected by equations for processes, such as the branching equations $B1$ and $B2$ in ACP that allow to eliminate silent actions. No such elimination is possible for autonomous actions, as each occurrence can be observed.

A process that is capable of performing an initial autonomous action is called unstable. A process in which no initial autonomous action can occur is called stable, as an environment can stop its progress by encapsulating its initial actions. A choice involving an unstable process is nondeterministic, since an environment cannot prevent the autonomous action from occurring. We call this kind of nondeterminism unstable nondeterminism. Another kind of nondeterminism arises when several non-autonomous actions with the same visible effect can occur, leading to different subsequent processes. We call this stable nondeterminism.

Instead of only considering process equivalence, a partial order $\leq$ on processes is introduced. If processes $p$ and $q$ satisfy $p \leq q$, then either both processes are equal, or both $p$ and $q$ are unstable and the behaviour of $p$ is a subset of the behaviour of $q$. Since there must exist an autonomous action that both $p$ and $q$ can perform, and since this action cannot be controlled, an observer, when confronted with $p$, cannot be sure that he is not dealing with $q$ instead. So $\leq$ is based on reduction of unstable nondeterminism.
Partial order algebras that are based on reduction of nondeterminism are important for software engineering. Often, design decisions are made that reduce nondeterminism in a specification. The advantage of the approach in this paper is that in the specification one can distinguish unstable nondeterminism that may be reduced and stable nondeterminism that may not.

The main inspiration of the present paper is [BaBe94], where CSP-like choice operators [Hoa85] are introduced in ACP. The "partial bisimulation" preorder on processes from [BaBe94] that is also used in the present paper is related to the preorder in [Abr87] and [Wal90] that deal with the notion of divergence: a possibly infinite chain of autonomous actions (in their case silent actions \(\tau\)).

The reason for introducing CSP-like choice operators in ACP in [BaBe94] is that CSP distinguishes between deterministic and nondeterministic choice. Autonomous actions offer an alternative to nondeterministic choice operators, with the advantage of considerably simpler equations and models. Also, in this paper axioms and proof rules are given for reasoning algebraically with infinite processes, whereas the reasoning in [BaBe94] (and CSP for that matter) is model-based.

The authors wish to thank Jos Baeten and Pedro D'Argenio for their suggestions and corrections. Jan Bergstra is thanked for sharing with us his insights regarding communication and autonomous behaviour.

2 The Basic Algebra

2.1 Signature and Axioms

Our basic algebra BPAaa is an extension of BPA\(_8\): basic process algebra with inaction (c.f. [BaWe90]). The signature and axioms are given in Table 1. First, in the header, the sort of atoms (\(\mathbb{A}\)) is declared, which is a parameter of the theory. Each atom is an action. An overlining operator creates from an atom an autonomous action. The sort \(\mathbb{F}\) of autonomous actions is thus equal to \(\{a : \mathbb{A} \circ a\}^1\). The set \(\mathbb{A} \cup \mathbb{F}\) of all actions is denoted \(\mathbb{A}\). Note that \(\mathbb{A}\) is only an abbreviation and not a sort. The actions \(a\) and \(\overline{a}\) have the same visible effect and only differ in the way they can be controlled by an environment.

The sort \(\mathbb{P}\) of processes is a supersort of both \(\mathbb{A}\) and \(\mathbb{F}\). Sorts and their subsort relation are introduced in the first table entry.

The operator \(\cdot\) as well as the standard BPA operators \(+\), \(\cdot\), and \(\cdot\cdot\) and the constant \(\delta\) are introduced in the second table entry, followed by the declaration of some variables and the axioms of the theory. As usual, the sequencing operator \((\cdot)\) has priority over choice \((+\) and may be omitted. The axiom system consists of equations and inequalities, giving rise to a partial order algebra (c.f. [Hen88]), which means that in reasoning with inequalities, one is allowed to use reflexivity, transitivity, antisymmetry, closedness under contexts and substitutivity. Note that, by antisymmetry, for two terms \(x\) and \(y\), \(x = y\) iff \(x \leq y\) and \(y \leq x\).

The \(I\) axioms (for "inequality") state that unstable nondeterminism may be reduced in an implementation. The algebra BPAaa is obtained from BPAaa\(_8\) by removing these inequalities from the axioms in Table 1. Note that BPAaa with atoms \(\mathbb{A}\) equals BPA\(_8\) with atoms \(\mathbb{A}\).

The BPAaa\(_8\) terms can be normalized. We inductively define the set \(\mathbb{B}\) of basic terms as follows.

\[
\{\delta\} \cup \mathbb{AC} \subseteq \mathbb{B}, \quad \forall t : B; e : \mathbb{AC} \cdot e \cdot t \in \mathbb{B}, \quad \forall s, t : B; s + t \in \mathbb{B}.
\]

**Property 1** For every closed term \(p : \mathbb{P}\), there exists a \(t : \mathbb{B}\) such that BPAaa \(\vdash p = t\) (and thus BPAaa\(_8\) \(\vdash p = t\)).

---

1 We use the Z-style notation \(\{a : A \circ f(a)\}\) instead of \(\{f(a) | a \in A\}\) throughout the paper.
Table 1: Basic process algebra with autonomous actions

<table>
<thead>
<tr>
<th>Rules</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>( x + y = y + x )</td>
</tr>
<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 + y)z = x \cdot z + y \cdot z )</td>
</tr>
<tr>
<td>A5</td>
<td>( (x \cdot y)z = x \cdot z \cdot y )</td>
</tr>
<tr>
<td>A6</td>
<td>( x + \delta = x )</td>
</tr>
<tr>
<td>A7</td>
<td>( \delta \cdot x = \delta )</td>
</tr>
</tbody>
</table>

Proof: Standard term rewriting, using A3 \ldots A7 as rewrite rules from left to right (c.f. [BaVe95]). Modulo axioms A1 and A2, and using A6, a basic term can be represented as \( \sum_{i} a_i + \sum_{j} b_j \cdot t_j \), where \( I, J \) are finite index sets, the \( a_i \) and \( b_j \) actions and the \( t_j \) again basic terms. An empty sum is equal to \( \delta \). By A3, it may be assumed that all summands are different.

Example: The theory BPAaa\( ^{\leq} \) may be used to demonstrate equivalence of the following processes that describe login procedures. The first process \( L_1 \) prompts for a user identification and, having received one, prompts for a password. After having checked the combination, access is granted or refused. The user of the process perceives the prompting, granting and refusing as autonomous actions he cannot influence. The other actions are interactions between the process and the user. So \( L_1 \) can be described as \( \text{pu}i \cdot \text{ui} \cdot MI \), where \( MI = \text{ppw} \cdot \text{pw}(ok + rej) \).

The second process \( L_2 \) checks the user id before prompting for the password. If the user id is found correct, it proceeds as above; if not, it will still prompt for the password and reject regardless of the answer. The process \( L_2 \) is thus described as \( \text{pu}i \cdot \text{ui}(M1 + M2) \), with \( M1 \) as above and \( M2 = \text{ppw} \cdot \text{pw} \cdot \text{rej} \).

In BPAaa\( ^{\leq} \), both login processes are equal, because we can demonstrate equality of \( M1 + M2 \) and \( M1 \). Since \( M1 \) is unstable, it follows from I2 that \( M1 \leq M1 + M2 \). It follows from I1 that \( \overrightarrow{ok + rej} \geq \overrightarrow{rej} \). Closedness under contexts yields \( M1 \geq M2 \), which implies by A3 that \( M1 = M1 + M1 \geq M1 + M2 \). Thus \( M1 = M1 + M2 \) by antisymmetry. As a result, \( L1 = L2 \).

The equality of \( L1 \) and \( L2 \) conforms to intuition and is desirable as well, since potential intruders are left uninformed whether they "guessed" a correct user id. At the end of Section 2.3, we will argue that equality of \( L1 \) and \( L2 \) cannot be proved without the inequalities I1 and I2.

2.2 Process Theory

Let AC be a set of actions partitioned into disjoint subsets \( A \) (non-autonomous actions) and \( F \) (autonomous actions). A process space is a pair \((P, \rightarrow)\), where \( P \) is a set of processes and \( \rightarrow: \mathcal{P}(P \times AC \times P) \cup \{\} \) a ternary relation, the event relation. The event \( p \xrightarrow{a} \) represents successful termination of \( p \) with action \( a \). A stable process cannot perform any autonomous actions in the first step. The set \( S \) of stable processes is thus defined as \( S = \{p: P | \neg \exists f: F; p': P \cup \{f\} \cdot p \xrightarrow{f} p'\} \). We define a class of relations called partial bisimulations. A simulation \( R \) is a partial bisimulation if \( R^{-1} \) is a local simulation for stable processes.
Definition 1 A relation $R : \mathcal{P}(\mathcal{P} \cup \{\emptyset\})$ is called a partial bisimulation (PBS) iff it satisfies the following requirements. For $p, q, q' : \mathcal{P} \cup \{\emptyset\}$ and $e : \mathcal{A}$,

1) $pRq \Rightarrow (p = \emptyset \iff q = \emptyset) \land
(pRq \land p \xrightarrow{e} p') \Rightarrow \exists q' : \mathcal{P} \bullet (q \xrightarrow{e} q' \land p'Rq')$,

2) $pRq \land p \in S \land q \xrightarrow{e} q' \Rightarrow \exists p' : \mathcal{P} \bullet (p \xrightarrow{e} p' \land p'Rq')$.

Process $p : \mathcal{P}$ is said to implement $q : \mathcal{P}$ (notation $p \preceq q$) iff there exists a PBS $R$ such that $pRq$. The processes $p, q$ are said to be equivalent (notation $p \simeq q$) iff $p \preceq q \land q \preceq p$.

As usual, we can also define strong bisimulation on processes (see e.g. [BaWe90]). A strong bisimulation between processes $p$ and $q$ is a PBS relating both $p$ to $q$ and $q$ to $p$. If $\mathcal{F} = \emptyset$, each PBS is a strong bisimulation.

Property 2 The relation $\preceq$ is a preorder and, consequently, $\simeq$ is an equivalence relation.

Proof We have to show that $\preceq$ is reflexive and transitive. The identity relation on processes is a PBS, proving reflexivity. For transitivity, assume that $R, S$ are PBSs such that $pRq$ and $qSr$. Obviously, the relation composition $R \circ S$ is a simulation. If $p$ is stable, then $R^{-1}$ is a local simulation, so $q$ is stable and hence $S^{-1}$ is a local simulation. So $(R \circ S)^{-1}$ is a local simulation and $R \circ S$ a PBS. So $p \preceq r$.

With preorder relations like partial bisimulation, special care must be taken with respect to termination and nontermination of processes. It is undesirable that a terminating process can be implemented by a nonterminating one. Therefore, we shall define a termination property for processes. Intuitively, a process is called terminating if it has a path leading to $\emptyset$ and it can only make transitions to terminating processes. A terminating process cannot deadlock, nor can it contain a cycle from which escape is impossible.

Definition 2 The set $\mathcal{A}C^*$ of process traces consists of finite sequences $e_1 \ldots e_n$ of actions, including the empty trace $\epsilon$. The reachability relation $\xrightarrow{\epsilon} : \mathcal{P}(\mathcal{P} \cup \{\emptyset\}) \times \mathcal{A}C^* \times (\mathcal{P} \cup \{\emptyset\})$ is defined as the smallest relation (ordered by set inclusion) such that for all $p, p', p'' : \mathcal{P} \cup \{\emptyset\}; e : \mathcal{A}; \alpha : \mathcal{A}C^*$,

$p \xrightarrow{\epsilon} p \land p \xrightarrow{e} p' \land p'' \xrightarrow{\alpha} p'' \Rightarrow p \xrightarrow{\alpha} p''$.

The termination predicate for a process $p$ (notation $p \Downarrow$) is defined as follows.

$p \Downarrow \iff \forall p' : \mathcal{P}; \alpha : \mathcal{A}C^* \bullet (p \xrightarrow{\alpha} p' \Rightarrow \exists \beta : \mathcal{A}C^* \bullet p' \xrightarrow{\beta} \emptyset)$.

2.3 A Process Model for BPAaa$\leq$

In order to construct a process model for BPAaa$\leq$, we have to give interpretations $A, \mathcal{F}$ and $\mathcal{P}$ respectively for the sorts $A, \mathcal{F}$ and $\mathcal{P}$. Let the process space $\mathcal{P}$ be the set of closed BPAaa$\leq(A)$ terms. Let $A$ and $\mathcal{F}$ simply be equal to $A$ and $\mathcal{F}$ respectively. Obviously, these interpretations do satisfy the requirements $A \subseteq \mathcal{P}$ and $\mathcal{F} \subseteq \mathcal{P}$. Let $\mathcal{A}C = A \cup \mathcal{F}$. The relation $\xrightarrow{\epsilon}$ is given as the smallest relation satisfying the requirements in Table 2. In this table, the variables $a : A; p, p', q : \mathcal{P}; e : \mathcal{A}$ are used. Our model will be the set of equivalence classes of $\mathcal{P}$ modulo PBS equivalence, denoted $\mathcal{P}/\simeq$. The following property means that $\mathcal{P}/\simeq$ with $\preceq$ is a partial order algebra.

Property 3 The relation $\leq$ is a precongruence w.r.t. the BPAaa$\leq$ operators, i.e., for all $a, b : A$ such that $a \leq b, \overline{a} \leq \overline{b}$ and for all $p_1, p_2, q_1, q_2 : \mathcal{P}$ such that $p_1 \leq p_2$ and $q_1 \leq q_2$. $p_1 \cdot q_1 \leq p_2 \cdot q_2$ and $p_1 + q_1 \leq p_2 + q_2$. 

4
Table 2: Plotkin-style SOS rules for BPAaa^≤

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(e \xrightarrow{e} \top)</td>
<td>(p \xrightarrow{e} p')</td>
</tr>
<tr>
<td>(p \cdot q \xrightarrow{e} p' \cdot q)</td>
<td>(p \cdot q \xrightarrow{e} q)</td>
</tr>
<tr>
<td>(p \cdot q \xrightarrow{e} \top)</td>
<td>(q + p \xrightarrow{e} p')</td>
</tr>
<tr>
<td>(q + p \xrightarrow{e} \top)</td>
<td>(p \xrightarrow{e} \top)</td>
</tr>
<tr>
<td>(p \xrightarrow{e} \top)</td>
<td>(q \xrightarrow{e} p')</td>
</tr>
</tbody>
</table>

Proof If \(a \leq b\) then \(a = b\) and thus \(\overline{a} = \overline{b}\). The other two cases are proved by constructing a PBS. □

For closed terms \(p\) and \(q\), \(\text{BPAaa} \leq p \leq q\) signifies that \(p \leq q\) can be derived from the axioms, whereas \(\mathcal{P}/\simeq \models p \leq q\) signifies that \(p \leq q\) is valid in the model \(\mathcal{P}/\simeq\). That is, \(\mathcal{P}/\simeq \models p \leq q\) iff \(p \leq q\). The following theorem states soundness and completeness of BPAaa^≤ with respect to \(\mathcal{P}/\simeq\).

**Theorem 1** Let \(p\), \(q\) be closed BPAaa^≤ terms. Then \(\text{BPAaa} \leq p \leq q\) if and only if \(\mathcal{P}/\simeq \models p \leq q\).

Proof It follows from Property 3 that it suffices to check the validity of the axioms to prove soundness. In each case, PBSs can be constructed easily. For the axioms A1 . . . A7, even strong bisimulations can be constructed.

Completeness is more involved. Suppose \(p \leq q\). Then there exists a PBS \(R\) such that \(pRq\). We use induction on the number of symbols in \(p\) plus the number of symbols in \(q\). The basic case, where \(p\) and \(q\) each consist of a single symbol follows from the fact that \(R\) is a PBS such that \(pRq\). Processes \(p\) and \(q\) are either both equal to \(\delta\) or both consist of the same action. Hence, in the basic case, BPAaa^≤ \(\models p \leq q\).

In the induction step, from Property 1, we may assume that \(p\) and \(q\) are basic terms; so
\[
p = \sum_{i \in I} a_i + \sum_{j \in J} b_j \cdot s_j, \quad q = \sum_{k \in K} c_k + \sum_{l \in L} d_l \cdot t_l,
\]
where \(I, J, K\) and \(L\) are finite index sets, the \(a_i, b_j, c_k\) and \(d_l\) are actions from AC and the \(s_j\) and \(t_l\) are basic terms. We distinguish two cases.

First, assume that \(p\) is stable. Then \(R^{−1}\) is a local simulation. We may conclude from the derivation rules in Table 2 that
\[
\forall i : I \cdot \exists k : K \cdot a_i = c_k, \quad \forall j : J \cdot \exists l : L \cdot b_j = d_l \land s_j R t_l.
\]
The induction hypothesis yields
\[
\forall j : J \cdot \exists l : L \cdot b_j = d_l \land \text{BPAaa}^≤ \models s_j \leq t_l.
\]
It follows immediately that BPAaa^≤ \(\models p \leq q\).

Second, assume that \(p\) is unstable. Since \(R\) is a simulation, we may conclude from the derivation rules in Table 2 that
\[
\forall i : I \cdot \exists k : K \cdot a_i = c_k, \quad \forall j : J \cdot \exists l : L \cdot b_j = d_l \land s_j R t_l.
\]
The induction hypothesis again yields
\[
\forall j : J \cdot \exists l : L \cdot b_j = d_l \land \text{BPAaa}^≤ \models s_j \leq t_l.
\]
Since \(p\) is unstable, one of its initial actions is automonous. Using axioms I1 and I2, BPAaa^≤ \(\models p \leq q\) follows easily. □

The set of equivalence classes of \(\mathcal{P}\) modulo strong bisimulation equivalence is a sound and complete model for BPAaa. This result follows from the one-to-one correspondence between closed BPAaa(A) terms and closed BPAa(AAC) terms together with soundness and completeness of BPAa(AAC) for the set of equivalence classes of closed BPAa(AAC) terms modulo strong bisimulation equivalence. It means that all actions in AC are considered to be non-autonomous and thus all processes are considered to be stable. The consequence is that, as long as no inequality is used, two closed BPAaa^≤ terms that are
derivably equal are strongly bisimilar. The use of an inequality in a verification represents the reduction of unstable nondeterminism. It is important to keep track at which points this reduction occurs. This can be achieved by delaying the use of \( i_1 \) and \( i_2 \) until they are really needed, i.e., proceeding within \( \text{BPAaa} \) as long as possible.

At this point, we can also justify our claim that the equivalence of the login procedures \( L_1 \) and \( L_2 \) in the example of Section 2.1 cannot be proved without the inequalities \( i_1 \) and \( i_2 \). This follows immediately from the observations above and the fact that \( L_1 \) and \( L_2 \) are not bisimilar.

### 3 Iteration

In this section, an iteration operator, c.q. the binary Kleene star (BKS) is added to the basic theory. The additional signature and axioms, which have been taken from [BeBP94], are stated in Table 3.

<table>
<thead>
<tr>
<th>( \text{BPAaa} )</th>
<th>( \text{BPA*aa} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \cdot : P \times P \rightarrow P )</td>
<td>( p \xrightarrow{e} p' )</td>
</tr>
<tr>
<td>( x, y, z : P )</td>
<td>( p \xrightarrow{\varepsilon} \sqrt{\cdot} )</td>
</tr>
<tr>
<td>( x(x^*y) + y = x^*y )</td>
<td>( p^*q \xrightarrow{e} (p^*q) )</td>
</tr>
<tr>
<td>( x^*(y \cdot z) = (x^*y)z )</td>
<td>( q^*p \xrightarrow{e} p' )</td>
</tr>
<tr>
<td>( x^*(y((x + y)^*z) + z) = (x + y)^*z )</td>
<td>( p \xrightarrow{e} )</td>
</tr>
</tbody>
</table>

| \( \text{BKS1} \) | \( p^*q \xrightarrow{e} p^*q, q^*p \xrightarrow{e} \sqrt{\cdot} \) |

Table 3: Axioms and SOS rules for the binary Kleene star

A process model is derived as follows. Again, let \( \mathcal{A} \) and \( \mathcal{F} \) be equal to \( \mathcal{A} \) and \( \mathcal{F} \). Recall that \( \mathcal{AC} = \mathcal{A} \cup \mathcal{F} \). Define \( P \) as the set of closed \( \text{BPA*aa} \) terms. The relation \( \xrightarrow{-} : P(P \times \mathcal{AC} \times P \cup \{\varepsilon\}) \) is defined as the smallest relation satisfying the rules in Tables 2 and 3, where \( e : \mathcal{AC} \) and \( p, p', q : P \).

**Theorem 2** Let \( p, q \) be closed \( \text{BPA*aa} \) terms. Then \( \text{BPA*aa} \vdash p \leq q \) implies \( P/\sim \models p \leq q \).

**Proof** Standard. First, show that \( \leq \) is a precongruence w.r.t. the binary Kleene star. Second, check the validity of \( \text{BKS1} \ldots \text{BKS3} \) by constructing PBSs. Note that even strong bisimulations can be constructed for these axioms. \( \square \)

The following theorem states that the theory \( \text{BPA*aa} \) does not introduce any inequalities (and therefore equations) between closed \( \text{BPAaa} \) terms which were not already derivable from \( \text{BPAaa} \). That is, the theory \( \text{BPA*aa} \) is a conservative extension of \( \text{BPAaa} \).

**Theorem 3** Let \( p \) and \( q \) be closed \( \text{BPAaa} \) terms. Then \( \text{BPA*aa} \vdash p \leq q \) if \( \text{BPAaa} \vdash p \leq q \).

**Proof (sketch)** We use the theory and terminology developed in [D'Ar95]. It follows from the format of the derivation rules that the term deduction system defined by Table 2 is source dependent. Furthermore, it has no rules with negative premises, so it has a unique well supported model. For the same reason, the term deduction system defined by Tables 2 and 3 has a unique well supported model. As a result, it is an operational conservative extension (up to \( \leq \)) of the term deduction system of Table 2. It then follows from Theorems 1 and 2 that \( \text{BPA*aa} \) is a conservative extension of \( \text{BPAaa} \). \( \square \)

A complete finite axiomatization of \( \text{BPA*} \) and thus \( \text{BPA*aa} \) is impossible ([Sew94]; c.f. [FoZa94] for related results).
For reasoning with iterative processes, we formulate some conditional equations and inequalities. \( RSP^* \) is the iteration variant of the "Recursive Specification Principle" (c.f. e.g. [BaWe90]); the other names are derived from "Iteration Inequality." For any \( v, w, x, y, z \in \mathcal{P} \),

\[
\begin{align*}
&v \cdot x + w \leq x & \text{III} & x \leq y \cdot x + z & \text{IRR} & x = y \cdot x + z & \text{RSP^*} \\
\frac{v \cdot x + w \leq x}{v^* w \leq x} & \frac{x \leq y \cdot x + z}{x \leq y^* z} & & \frac{x = y \cdot x + z}{x = y^* z} & & \frac{v^* w \leq x \leq y^* z}{II}
\end{align*}
\]

Clearly, \((III \land IIR) \Rightarrow II \Rightarrow RSP^*\). It is not hard to show that \( RSP^* \) and \( BKS1 \) imply \( BKS2 \) and \( BKS3 \).

**Theorem 4** The above derivation rules are valid in the model \( \mathcal{P}/\sim \).

**Proof (sketch)** Inequality \( IIR \) is proved by constructing a PBS as follows. Let \( p, q \) and \( r \) be closed \( \text{BPA}^*\text{aa} \leq \text{terms} \) and let \( R \) be a PBS such that \( pR(q \cdot p + r) \). \( R^k \) is the \( k \)-fold composition of \( R \), where \( R^0 \) equals the identity relation and \( R^1 \) equals \( R \). The relation \( Q \) is defined as the smallest relation such that \( \sqrt[2]{Q} \sqrt[2]{2} \) and for any \( k \geq 0 \), closed term \( \xi \) and open term \( E(X) \) with \( X \) as its only variable, \( \xi Q \xi \) and \( \xi R^k E(p) \Rightarrow \xi Q E(q^* r) \). Using the operational semantics, it can be shown that this relation is a PBS relating \( p \) and \( q^* r \). So \( IIR \) is valid. The validity of \( III \) is shown using a symmetrical argument. \( \square \)

We have thus shown the validity of \( III, IIR, II \) and \( RSP^* \). However, the inequalities \( III \) and \( IIR \) permit the derivation of, e.g., \( \overline{a^* b} \leq \overline{a^* b} \). This is undesirable, since the second process is terminating, whereas the first process is not. For that reason, in the remainder, we only use the weaker inequality \( II \). In \( \text{BPA}^*\text{aa} \leq + II \), a terminating process cannot be implemented by a nonterminating process.

**Property 4** Let \( p, q : \mathcal{P} \). If \( \text{BPA}^*\text{aa} \leq + II \vdash p \leq q \) and \( q \Downarrow \), then \( p \Downarrow \).

**Proof (sketch)** Structural induction on \( p \) is used. The basic case is trivial. In the induction step, we consider three cases. First, if \( p = p_1 + p_2 \leq q \), we may assume that \( \delta \neq p_1 \neq p_2 \neq \delta \). The only way that \( p \leq q \) can be deduced from \( \text{BPA}^*\text{aa} \leq + II \) is when \( q \) has the form \( q_1 + q_2 \) and \( \text{BPA}^*\text{aa} \leq + II \vdash (p_1 \leq q_1 \land p_2 \leq q_2) \). If \( q \Downarrow \), then \( q_1 \Downarrow \) and \( q_2 \Downarrow \), allowing completion of the induction step in this case. Second, if \( p = p_1 \cdot p_2 \), the argument is similar. Third, if \( p = p_1^* p_2 \), \( p \leq q \) can be derived in two ways.

The first possibility is that \( q \) has the form \( q_1^* q_2 \) and \( \text{BPA}^*\text{aa} \leq + II \vdash (p_1 \leq q_1 \land p_2 \leq q_2) \), which is dealt with as above. The second possibility follows from \( II \) if \( p_1 q + p_2 \leq q \leq r q + s \) and \( p_2 \leq s \), for some processes \( r \) and \( s \). Now suppose \( q \Downarrow \). We have to show that \( p \Downarrow \), i.e. that \( p_1 \Downarrow \) and \( p_2 \Downarrow \). Assume \( p_2 = \delta \). Then \( s = \delta \) and \( q \leq r \cdot q \). Soundness gives \( q \leq r \cdot q \). Since \( q \Downarrow \), it follows that \( q \xrightarrow{\alpha} \Downarrow \) for some trace \( \alpha \). So there exist nonempty traces \( \beta, \gamma \) such that \( \alpha = \beta \cdot r \xrightarrow{\gamma} \Downarrow \) and \( q \xrightarrow{\gamma} \Downarrow \). So for any path of \( q \) leading to \( \Downarrow \), a shorter path can be found, which is a contradiction. So \( p_2 \neq \delta \). Hence, one deduces again that \( q \) has the form \( q_1 + q_2 \) and \( \text{BPA}^*\text{aa} \leq + II \vdash (p_1 \cdot q \leq q_1 \land p_2 \leq q_2) \), which can again be treated as above. \( \square \)

### 4 Concurrency and Communication

Table 4 gives the additional operators and axioms for the extension of ACP with autonomous actions. An extra parameter, the communication function \( \gamma : \mathcal{A} \cup \{\delta\} \times \mathcal{A} \cup \{\delta\} \rightarrow \mathcal{A} \cup \{\delta\} \), is added, that is commutative and associative and satisfies \( \gamma(a, \delta) = \delta \) for all atoms \( a \).
The UCM axioms disallow synchronization of unstable processes. The SCM axioms are CM8 and CM9 of ACP restricted to stable processes. The other merge-related axioms are standard.

The auxiliary predicate \( S(\cdot) \) stating that a process is stable is defined as follows. For \( e : AC; x, y : P \),

\[
S(\delta) \quad S(e) \quad \Rightarrow \quad e \in A
\]

\[
S(x \cdot y) \quad S(x) \quad S(x + y) \quad \Rightarrow \quad S(x) \land S(y)
\]

Only a few of the other operators need explanation. Encapsulation of autonomous actions is impossible (D), which is the essence of being autonomous, as explained in the introduction. The renaming operator \( tI \) renames the atoms from a given set \( I \) into a special atom \( t \). An operator \( autI \) is added, that autonomizes the atoms from \( I \). The composed operator \( tI \circ autI \) has the properties of pre-abstraction [BaBe88].

<table>
<thead>
<tr>
<th>( \text{ACPaa}^\leq (A, \gamma) )</th>
<th>( i : A )</th>
<th>( \delta_i(\cdot), aut_i(\cdot), t_i(\cdot) : \mathbb{P}(A) \times P \rightarrow P )</th>
<th>( \mathbb{P} )</th>
<th>( \vdots )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a \notin H \Rightarrow \delta_H(a) = a )</td>
<td>( D1 )</td>
<td>( b \mid c = \gamma(b, c) )</td>
<td>CF</td>
<td></td>
</tr>
<tr>
<td>( a \in H \Rightarrow \delta_H(a) = \delta )</td>
<td>( D2 )</td>
<td>( e \mid x = e \cdot x )</td>
<td>CM1</td>
<td></td>
</tr>
<tr>
<td>( \delta_H(\overline{a}) = \overline{a} )</td>
<td>( D )</td>
<td>( x \mid y = x \mid y + y \mid x + x \mid y )</td>
<td>CM2</td>
<td></td>
</tr>
<tr>
<td>( a \notin I \Rightarrow aut_I(a) = a )</td>
<td>( AU1 )</td>
<td>( e \cdot x \mid y = e \cdot (x \mid y) )</td>
<td>CM3</td>
<td></td>
</tr>
<tr>
<td>( a \in I \Rightarrow aut_I(a) = \overline{a} )</td>
<td>( AU2 )</td>
<td>( (x + y) \mid z = x \mid z + y \mid z )</td>
<td>CM4</td>
<td></td>
</tr>
<tr>
<td>( aut_I(\overline{a}) = \overline{a} )</td>
<td>( AU3 )</td>
<td>( b \cdot c \mid d = (b \mid c) \cdot x )</td>
<td>CM5</td>
<td></td>
</tr>
<tr>
<td>( a \notin I \Rightarrow t_I(a) = a )</td>
<td>( RN1 )</td>
<td>( b \cdot x \mid c \cdot y = (b \mid c) \cdot x \mid y )</td>
<td>CM6</td>
<td></td>
</tr>
<tr>
<td>( a \in I \Rightarrow t_I(a) = t )</td>
<td>( RN2 )</td>
<td>( S(x + y) \Rightarrow (x + y) \mid z = x \mid z + y \mid z )</td>
<td>SCM8</td>
<td></td>
</tr>
<tr>
<td>( t_I(\overline{a}) = \overline{t}(\overline{a}) )</td>
<td>( RN )</td>
<td>( S(y + z) \Rightarrow x \mid (y + z) = x \mid y + x \mid z )</td>
<td>SCM9</td>
<td></td>
</tr>
<tr>
<td>( L(\delta) = \delta )</td>
<td>( L1 )</td>
<td>( (\overline{\overline{a}} \cdot x + y) \mid z = \delta )</td>
<td>UCM1</td>
<td></td>
</tr>
<tr>
<td>( L(x + y) = L(x) + L(y) )</td>
<td>( L2 )</td>
<td>( x \mid (\overline{\overline{a}} \cdot x + y + z) = \delta )</td>
<td>UCM2</td>
<td></td>
</tr>
<tr>
<td>( L(x \cdot y) = L(x) \cdot L(y) )</td>
<td>( L3 )</td>
<td>( x \mid (\overline{\overline{a}} \cdot x + y + z) = \delta )</td>
<td>UCM3</td>
<td></td>
</tr>
</tbody>
</table>

Table 4: ACP with autonomous actions

The following theorem shows that the non-\( \text{BPAaa}^\leq \) operators can be eliminated.

**Theorem 5** For every closed ACPaa\(^\leq \) term \( p \), there is a basic BPAaa\(^\leq \) term \( s \) such that ACPaa\(^\leq \) \( \vdash p = s \).

**Proof (sketch)** Consider ACPaa\(^\leq \) as a term rewriting system. That is, consider the axioms A3 \ldots A7 plus all the axioms in Table 4 as rewrite rules from left to right. We can use the method of recursive path order to show that this term rewriting system is strongly normalizing (see [BaVe95] for a detailed description). Here, we only give the partial ordering on the ranked operators of ACPaa\(^\leq \). For \( k > 1 \) and \( a : A \),

\[
\delta < a \quad \{a, -, +\} < \vdots < \{\ll_2, \ll_3, \delta_H, aut_I, t_I\} \quad \{\ll_k, \ll_k\} < \ll_k < \{\ll_{k+1}, \ll_{k+1}\}
\]

Now, it can be verified by structural induction that the normal forms are basic BPAaa\(^\leq \) terms. The basic step is simple. For the induction step, note that for any normal form containing a non-\( \text{BPAaa}^\leq \) operator applied to normal forms, which by the induction hypothesis are basic BPAaa\(^\leq \) terms, a rewrite rule can
be found in Table 4, which is a contradiction.

A process model is defined as before. The process space \( \mathcal{P} \) is defined as the set of closed ACP\( ^{\leq} \) terms. The relation \( \sim \) is the smallest relation satisfying the rules in Tables 2 and 5. Recall that in Section 2.2, \( \mathcal{S} \) is defined as the set of stable processes. Note that for all \( p, p' \in \mathcal{S} \):

\[
\mathcal{P}(p) \subseteq \mathcal{P}(p')
\]

Let \( a, b, c : A; e : AC; H, I : \mathbb{P}(A); p, p', q, q' : \mathcal{P} \) and \( \hat{p}, \hat{q} : \mathcal{S} \).

\[
\begin{array}{c}
p \xrightarrow{a} p' \\
p||q \xrightarrow{c} p'||q' \\
\hat{p} \xrightarrow{a} \hat{p}', \hat{q} \xrightarrow{b} \hat{q}' \\
p||q \xrightarrow{c} p'||q'
\end{array}
\]

The following property and theorem deal with soundness of ACP\( ^{\leq} \).

**Property 5** The \( \preceq \) preorder is a precongruence w.r.t. the ACP\( ^{\leq} \) operators.

**Proof** Let \( R_1 \) and \( R_2 \) be PBSs. Let \( Q = \bigcup_{p_1, p_2, q_1, q_2 : \mathcal{P}} \{ p_1 R_1 q_1 \wedge p_2 R_2 q_2 \} \). It is easy to check that \( Q \cup R_1 \cup R_2 \) is a PBS, noticing that \( x \parallel y \) is stable if both \( x \) and \( y \) are stable. So for any \( p_1, p_2, q_1, q_2 : \mathcal{P} \), \( (p_1 \preceq q_1 \wedge p_2 \preceq q_2) \Rightarrow p_1 \parallel p_2 \preceq q_1 \parallel q_2 \). So \( \preceq \) is a precongruence for the merge operator. For the left merge operator, under the same assumptions, \( Q \cup R_1 \cup R_2 \cup \bigcup_{p_1, p_2, q_1, q_2 : \mathcal{P}} \{ p_1 R_1 q_1 \wedge p_2 R_2 q_2 \} \) is a PBS; a similar PBS is constructed for the communication merge. In the latter case it is essential that communication with unstable processes is \( \delta \), so the autonomous actions of an unstable process cannot be selectively blocked. Let \( R \) be a PBS. Define \( Q = \{ p, q : \mathcal{P} \mid p R q \bullet (\partial_H(p), \partial_H(q)) \} \). It is easy to show that \( Q \cup \{(\delta, \delta)\} \) is a PBS, whence \( \preceq \) is a precongruence for encapsulation. Like before, it is essential that the encapsulation of an autonomous action is not \( \delta \). The \( t \) and \( aut \) operators are treated likewise. □

We can now prove soundness and completeness. For Theorem 6 it suffices to check the validity of all the axioms. In each case it is straightforward to give a strong bisimulation for the added axioms. Theorem 7 is proved in the same way as Theorem 3. After that, completeness follows from Theorems 1, 5, 6
and 7. See [D'Ar95] for more details.

**Theorem 6** Let p and q be closed $\text{ACP}_{aa}^2$ terms. Then $\text{ACP}_{aa}^2 \models p \leq q$ implies $P/\approx \models p \leq q$.

**Theorem 7** Let p and q be closed $\text{BPA}_{aa}^2$ terms. Then $\text{ACP}_{aa}^2 \models p \leq q$ iff $\text{BPA}_{aa}^2 \models p \leq q$.

**Theorem 8** Let p and q be closed $\text{ACP}_{aa}^2$ terms. Then $\text{ACP}_{aa}^2 \models p \leq q$ iff $\text{BPA}_{aa}^2 \models p \leq q$.

5 Example: ABP

The benchmark example for process algebra is the Alternating Bit Protocol (ABP). As the ABP has recursion as well as communication, we define the theory $\text{ACP}_{aa}^2$ by combining $\text{ACP}_{aa}^2$ and $\text{BPA}_{aa}^2$, adding the axiom $L4$:

$L(x * y) = L(x) * L(y)$ for $H, I : \mathcal{P}(A); L : \{ \delta_H, out_I, t_I \}; x, y : A$.

A process model can be defined as before. Soundness of $\text{ACP}_{aa}^2$ follows from Theorems 2 and 6 and the validity of axiom $L4$. $\text{ACP}_{aa}^2$ is a conservative extension of $\text{ACP}_{aa}^2$ (and thus of $\text{BPA}_{aa}^2$). A finite complete axiomatization does not exist. Inequality $II$ and hence equation $RSP^*$ are still valid. Furthermore, Property 4 can be generalized to closed $\text{ACP}_{aa}^2$ terms.

A protocol specification usually is of the form $(\sum_{d.D} \text{in}_d : \text{out}_d)^* \delta$, a never-ending loop of reading a message at one end and producing the same message at the other end. Verifications based on abstraction give an implementation with internal actions renamed to $\tau$ and use the special properties of the silent action $\tau$ to prove the implementation equal to the specification. Use is made of a "fairness" axiom, a simple variant of which can be stated as $x(\tau * y) = x * y$. Although such a fairness axiom is sound in many bisimulation-oriented models, one may disagree with it and use more discriminating divergence-sensitive models instead, in which case the specification equals $(\sum_{d.D} \text{in}_d(\tau * \tau) : \text{out}_d(\tau * \tau))^{*} \delta$.

In this paper the latter approach is followed, but without silent actions and using pre-abstraction instead. Internal actions are renamed into an autonomous, but visible internal action $\bar{\tau}$. Our specification $\text{ABP}_{spec}$ now reads $(\sum_{d.D} \text{in}_d(\bar{\tau} * \bar{\tau}) : \text{out}_d(\bar{\tau} * \bar{\tau}))^{*} \delta$, i.e., before any external action, a terminating $\bar{\tau}$-loop may take place. $\text{ABP}_{spec}$ requires at least one $\bar{\tau}$-step to be made between two external actions; a more complex specification can be given that also allows external actions to succeed one another without $\bar{\tau}$ steps in between. For the sake of simplicity we use $\text{ABP}_{spec}$ as given above.

An implementation $\text{ABP}_{imp}$ must satisfy $\text{ABP}_{imp} \leq \text{ABP}_{spec}$. A proper implementation never loses the option of proceeding to a next external action, so it should be of the form $\text{CYC} * \delta$ with $\text{CYC} \leq \sum_{d.D} \text{in}_d(\bar{\tau} * \bar{\tau}) : \text{out}_d(\bar{\tau} * \bar{\tau})$ and $\text{CYC} \downarrow$. It follows from the (generalized) Property 4 that this can be established by only using the axioms from $\text{ACP}_{aa}^2 + II$ in the verification and avoiding the use of $ILL$ and $IIR$.

![Figure 1: ABP implementation.](image)

In general, an implementation takes the form $t_I \circ \text{aut}_J \circ \delta_H(\|k:K P_k)$, where $L, J$ are sets of actions internal to the implementation, $H$ the actions that are enforced to communicate and $P_k$ for $k$ in $K$ the component processes. The actions in $J \setminus I$, while remaining internal, are still visible from outside.
If such actions are not deemed necessary, \( I \) and \( J \) can be taken equal, as in the \( \text{ABP} \) implementation below, that has been adapted from [BeKL86]. It consists of a sender \( S \), a receiver \( R \), a message channel \( K \) and an acknowledgment channel \( L \). See Figure 1. Let \( D \) be the finite set of data to be transmitted. For acknowledgements, the element \( \text{ack} \notin D \) is added and for perturbed communications the element \( \perp \notin D \cup \{\text{ack}\} \). The set \( B = \{0, 1\} \) contains the alternating bit. For \( b : B \), its negation \( 1 - b \) is written \( b' \). We define the set \( M \) of messages as \((D \cup \{\text{ack}\}) \times B) \cup \{\perp\} \). For \( d : D \cup \{\text{ack}\} ; b : B \), we denote the message \((d, b) \) by \( d_b \). The set \( C = \{1, 2, 3, 4\} \) defines the communication ports. We add the rules for standard read/send communication. For \( k : C; m : M \cdot \{(r_k(m), s_k(m)) = c_k(m) \) (and its commutative variant). All other communications are set to \( \perp \). Let \( H = \bigcup (k : C; m : M \cdot \{(r_k(m), s_k(m)) \) be the set of communication actions and \( I = \{k : C; m : M \cdot c_k(m) \) the set of internal actions. Now we can define \( \text{ABP}_{\text{imp}} \) as follows. For \( b \in B \), \( \text{ABP}_{\text{imp}} = t_1 \circ \text{aut}_I \circ \partial_H (S \parallel K \parallel L \parallel R) \), where

\[
S = (S_1 \cdot S_2) \cdot \delta \quad S_b = \sum_{d : D} in_d \cdot s_1(d_b)((r_4(\text{ack}_b) + r_4(\perp)) s_1(d_b) \cdot r_4(\text{ack}_b)) \quad R = (R_0 \cdot R_1) \cdot \delta \quad R_b = ((\sum_{d : D} r_2(d_b) + r_2(\perp)) s_3(\text{ack}_b)) \cdot ((\sum_{d : D} r_2(d_b) \cdot \text{out}_d) s_3(\text{ack}_b)) \quad K = P_{\perp, 2} \quad L = P_{\perp, 4} \quad P_{t, j} = (\sum_{m : M} r_1(m)(i \cdot s_j(m) + t \cdot s_j(\perp))) \cdot \delta
\]

By standard techniques and \( \text{RSP}^* \), one derives

\[
\text{ABP}_{\text{imp}} = (\sum_{d : D} in_d \cdot \text{t}^i(\text{t}^j(\text{t}^m)) \cdot \text{out}_d \cdot i(\text{t}^j(\text{t}^m))) \cdot \delta.
\]

Here, \( \text{t}^i \) is the abbreviation of \( \text{t} \cdot \ldots \cdot \text{t} \) \( i \) iterated \( k \) times. The fact that \( \text{ABP}_{\text{imp}} \leq \text{ABP}_{\text{spec}} \) follows from the following derivation, showing that \( \text{t}^i(\text{t}^j(\text{t}^m)) \leq \text{t}^i(\text{t}^j) \) for any \( k, l, m > 0 \).

By \( \text{BKSL} \), \( \text{t}^i(\text{t}^j) + \text{t} = \text{t}^{i+j} \). So from \( \text{I1} \) and \( \text{I2} \),

\[
\text{t}^i(\text{t}^j) \leq \text{t}^i(\text{t}^j) \text{t}^i(\text{t}^j) \leq \text{t}^i(\text{t}^j).
\]

By induction, and the transitivity of \( \leq \), we conclude that for all \( k > 0 \),

\[
\text{t}^i(\text{t}^j) \leq \text{t}^i(\text{t}^j), \quad \text{q}t^i \leq \text{t}^i(\text{t}^j).
\]

Using these results, \( \text{A3, BKSL} \) and \( \text{I1} \), we deduce that for any \( l, m > 0 \),

\[
\text{t}^i(\text{t}^j + \text{t}^m) \leq \text{t}^i(\text{t}^j + \text{t}^m) = \text{t}^i(\text{t}^j + \text{t}^m) \leq \text{t}^i(\text{t}^j) + \text{t}^i(\text{t}^m).
\]

Applying \( \text{I2} \), we obtain \( \text{t}^i(\text{t}^j) \leq \text{t}^i(\text{t}^j) \) and the transitivity of \( \leq \) yield

\[
\text{t}^i(\text{t}^j(\text{t}^m)) \leq \text{t}^i(\text{t}^j).
\]

This concludes our verification. Since the verification took place within \( \text{ACP}^* \leq \text{II} \), the implementation \( \text{ABP}_{\text{imp}} \) is a proper one.

6 Conclusions and Further Work

Actions with special properties do enrich process algebra. The present paper discusses autonomous actions, as an alternative to the “partial choice” operator of [BaBe94]. This leads to an algebra with similar expressive power and simpler axioms and models. Terms in the theory \( \text{BPA}_{\text{as}} \), Basic Process Algebra with partial choice, can be expressed in \( \text{BPAas}^* \) by means of a single autonomous action \( \text{t} \) and following the p-graph construction of [BaBe94]. For example, the expression \( (a \circ b) + c \) is mapped to \( \text{t}(a + c) + \text{t}(b + c) \).

For reasoning with infinite processes, the \( \text{II, III and IIR inequalities have been introduced. These inequalities may be carried over to other simulation-oriented preorders and can probably be widened in scope to (guarded) recursion.}

One can imagine other kinds of special actions, like \text{delayable} actions \( \text{a} \) or \text{irrevocable} actions \( \text{a} \) that e.g. satisfy the equations \( \text{a} \cdot x = \text{a}[x] \) (c.f. the silent step in weak bisimulation) and \( x \cdot \text{a} \cdot y + x \cdot \text{a} \cdot z = x(\text{a} \cdot y + \text{a} \cdot z) \) (c.f. ready trace semantics, [Gla90]). Another extension is the addition of the silent action \( r \). Branching bisimulation [GlW989] can be extended to partial branching bisimulation along the lines
of this paper, giving an algebra with two different silent actions: \( \tau \) and \( \top \). Both satisfy the branching equations; only the latter satisfies \( I_1 \) and \( I_2 \). Although the ABP example shows that silent actions and full abstraction have ceased to be necessary for some verifications, they nevertheless simplify matters considerably.

The theory in this paper can be applied to Petri Nets like in [BaVo95] to discriminate between the consumption and production of tokens. Production of tokens can be considered as autonomous in the sense of the present paper. This leads to an inequational theory for nets with similar advantages with respect to software engineering as stated in the introduction.

References


<table>
<thead>
<tr>
<th>Volume</th>
<th>Authors</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>93/01</td>
<td>R. van Geldrop</td>
<td>Deriving the Aho-Corasick algorithms: a case study into the synergy of programming methods, p. 36.</td>
</tr>
<tr>
<td>93/02</td>
<td>T. Verhoeff</td>
<td>A continuous version of the Prisoner's Dilemma, p. 17.</td>
</tr>
<tr>
<td>93/03</td>
<td>T. Verhoeff</td>
<td>Quicksort for linked lists, p. 8.</td>
</tr>
<tr>
<td>93/05</td>
<td>J.C.M. Baeten, C. Verhoeff</td>
<td>A congruence theorem for structured operational semantics with predicates, p. 18.</td>
</tr>
<tr>
<td>93/06</td>
<td>J.P. Velkamp</td>
<td>On the unavoidability of metastable behavior, p. 29.</td>
</tr>
<tr>
<td>93/07</td>
<td>P.D. Moerland</td>
<td>Exercises in Multiprogramming, p. 97.</td>
</tr>
<tr>
<td>93/08</td>
<td>J. Verhoosel</td>
<td>A Formal Deterministic Scheduling Model for Hard Real-Time Executions in DEDOS, p. 32.</td>
</tr>
<tr>
<td>93/10</td>
<td>K.M. van Hee</td>
<td>Systems Engineering: a Formal Approach Part II: Frameworks, p. 44.</td>
</tr>
<tr>
<td>93/16</td>
<td>H. Schepers, J. Hoornaar</td>
<td>A Trace-Based Compositional Proof Theory for Fault Tolerant Distributed Systems, p. 27.</td>
</tr>
<tr>
<td>93/17</td>
<td>D. Alslein, P. van der Stok</td>
<td>Hard Real-Time Reliable Multicast in the DEDOS system, p. 19.</td>
</tr>
<tr>
<td>93/18</td>
<td>C. Verhoeff</td>
<td>A congruence theorem for structured operational semantics with predicates and negative premises, p. 22.</td>
</tr>
<tr>
<td>93/19</td>
<td>G.J. Houben</td>
<td>The Design of an Online Help Facility for ExSpect, p. 21.</td>
</tr>
<tr>
<td>93/22</td>
<td>E. Poll</td>
<td>A Typechecker for Bijective Pure Type Systems, p. 28.</td>
</tr>
<tr>
<td>93/23</td>
<td>E. de Kogel</td>
<td>Relational Algebra and Equational Proofs, p. 23.</td>
</tr>
<tr>
<td>93/24</td>
<td>E. Poll and Paula Severi</td>
<td>Pure Type Systems with Definitions, p. 38.</td>
</tr>
<tr>
<td>93/26</td>
<td>W.M.P. van der Aalst</td>
<td>Multi-dimensional Petri nets, p. 25.</td>
</tr>
<tr>
<td>93/27</td>
<td>T. Klok and D. Kratich</td>
<td>Finding all minimal separators of a graph, p. 11.</td>
</tr>
<tr>
<td>93/28</td>
<td>F. Kamareddine and R. Nederpelt</td>
<td>A Semantics for a fine $\lambda$-calculus with de Bruijn indices, p. 49.</td>
</tr>
<tr>
<td>93/30</td>
<td>J. Deogun, T. Klok, D. Kratich, H. Müller</td>
<td>On Vertex Ranking for Permutation and Other Graphs, p. 11.</td>
</tr>
</tbody>
</table>
Derivation of delay insensitive and speed independent CMOS circuits, using directed commands and production rule sets, p. 40.


ILIAS, a sequential language for parallel matrix computations, p. 20.

Real Time Process Algebra with Infinitesimals, p. 39.

Abstract Reduction and Topology, p. 28.

Non Interleaving Process Algebra, p. 17.

Design and Analysis of Dynamic Leader Election Protocols in Broadcast Networks, p. 73.

A general conservative extension theorem in process algebra, p. 17.

Job Shop Scheduling by Constraint Satisfaction, p. 22.


Temporal operators viewed as predicate transformers, p. 11.

Automatic Verification of Regular Protocols in P/T Nets, p. 23.

A taxonomy of finite automata construction algorithms, p. 87.

A taxonomy of finite automata minimization algorithms, p. 23.

A precise clock synchronization protocol, p.


Verifying Sequentially Consistent Memory using Interface Refinement, p. 20.

The object-oriented paradigm, p. 28.

Canonical typing and IT-conversion, p. 51.


Graph Isomorphism Models for Non Interleaving Process Algebra, p. 18.


Time and the Order of Abstract Events in Distributed Computations, p. 29.


A Hierarchical Diagrammatic Representation of Class Structure, p. 22.

Process Algebra with Partial Choice, p. 16.
94/10 T. Verhoeff

The testing Paradigm Applied to Network Structure. p. 31.

94/11 J. Peleska
C. Huizing
C. Petersohn


94/12 T. Kloks
D. Knatsch
H. Müller


94/13 R. Seljé

A New Method for Integrity Constraint checking in Deductive Databases, p. 34.

94/14 W. Peremans

Ups and Downs of Type Theory, p. 9.

94/15 R.J.M. Vaessens
E.H.L. Aarts
I.K. Lenstra

Job Shop Scheduling by Local Search, p. 21.

94/16 R.C. Backhouse
H. Doornbos

Mathematical Induction Made Calculational, p. 36.

94/17 S. Mauw
M.A. Reniers

An Algebraic Semantics of Basic Message Sequence Charts, p. 9.

94/18 F. Kamareddine
R. Nederpelt

Refining Reduction in the Lambda Calculus, p. 15.

94/19 B.W. Watson

The performance of single-keyword and multiple-keyword pattern matching algorithms, p. 46.

94/20 R. Bloo
F. Kamareddine
R. Nederpelt

Beyond β-Reduction in Church’s λ→, p. 22.

94/21 B.W. Watson


94/22 B.W. Watson

The design and implementation of the FIRE engine: A C++ toolkit for Finite automata and regular Expressions.

94/23 S. Mauw and M.A. Reniers

An algebraic semantics of Message Sequence Charts, p. 43.

94/24 D. Dams
G. Grunberg
R. Gerth

Abstract Interpretation of Reactive Systems: Abstractions Preserving VCTL*, ECTL* and CTL*, p. 28.

94/25 T. Kloks

K₁,₃-free and W₂-free graphs, p. 10.

94/26 R.R. Hoogerwoord

On the foundations of functional programming: a programmer’s point of view, p. 54.

94/27 S. Mauw and H. Mulder


94/28 C.W.A.M. van Overveld
M. Verhoeven


94/29 J. Hooman

Correctness of Real Time Systems by Construction, p. 22.

94/30 J.C.M. Baeten
J.A. Bergstra
Ch. Stefanescu

Process Algebra with Feedback, p. 22.

94/31 B.W. Watson
R.E. Watson

A Boyer-Moore type algorithm for regular expression pattern matching, p. 22.

94/32 J.J. Vereijken


94/33 T. Laan

A formalization of the Ramified Type Theory, p.40.

94/34 R. Bloo
F. Kamareddine
R. Nederpelt

The Barendregt Cube with Definitions and Generalised Reduction, p. 37.

94/35 J.C.M. Baeten
S. Mauw

Delayed choice: an operator for joining Message Sequence Charts, p. 15.

94/36 F. Kamareddine
R. Nederpelt

Canonical typing and II-conversion in the Barendregt Cube, p. 19.

94/37 T. Basten
R. Bol
M. Voorhoeve

Simulating and Analyzing Railway Interlockings in ExSpect, p. 30.

94/38 A. Bijlsma
C.S. Scholten

Point-free substitution, p. 10.
On the equivalence covering number of splitgraphs, p. 4.

Distributed Consensus and Hard Real-Time Systems, p. 34.

Computing a perfect edge without vertex elimination ordering of a chordal bipartite graph, p. 6.

Concatenation of Graphs, p. 7.

Category Theory as Coherently Constructive Lattice Theory: An Illustration, p. 35.

Verifying Sequentially Consistent Memory, p. 160

Tutorial voor de ExSpect-bibliotheek voor "Administratieve Logistiek", p. 43.

The A-cube with classes of terms modulo conversion, p. 16.

On Π-conversion in Type Theory, p. 12.

Fixed-Point Calculus, p. 11.

Process Algebra with Propositional Signals, p. 25.

A short and flexible proof of Strong Normalization for the Calculus of Constructions, p. 27.

Listing simplicial vertices and recognizing diamond-free graphs, p. 4.

Traces and Logic, p. 81

A Partial Order Approach to Branching Time Logic Model Checking, p. 20.

The Construction of a small CommunicationLibrary, p. 16.

Formalizing Process Algebraic Verifications in the Calculus of Constructions, p. 49.

Concrete process algebra, p. 134.

An Isotopic Invariant for Planar Drawings of Connected Planar Graphs, p. 9.

A Type Inference Algorithm for Pure Type Systems, p. 20.

A Quantitative Analysis of Iterated Local Search, p. 23.

Drawing Execution Graphs by Parsing, p. 10.

Preservation of Strong Normalisation for Explicit Substitution, p. 12.

Discrete Time Process Algebra, p. 20

MathJpad: A System for On-Line Preparation of Mathematical Documents, p. 15
R. Seljé

S. Mauw and M. Reniers

B.W. Watson and G. Zwaan

A. Pense, C. Verhoef, S.F.M. Vlijmen (eds.)

P. Niebott and W. Penczek

D. Dams, O. Grumberg, R. Gerth

S. Mauw and B.A. van de Meulen

F. Kamareddine and T. Laan

I.C.M. Baeten and J.A. Bergstra

F. van Raamsdonk and P. Severi

A. van Deursen

B. Arnold, A. van Deursen, M. Res

W.M.P. van der Aalst

W.M.P. van der Aalst

F.P.M. Dignum, W.P.M. Nuijten, L.M.A. Janssen

L. Feijs

W.M.P. van der Aalst

P.D.V. van der Stok, J. van der Wal

W. Fokkink, C. Verhoef

H. Jurjus

J. Hidders, C. Hoekens, J. Paredaens

P. Kelb, D. Dams and R. Gerth

W.M.P. van der Aalst

J. Engelfriet and J.J. Vereijken

J. Zwanenburg

T. Basten and M. Voorhoeve

Deductive Database Systems and integrity constraint checking, p. 36.

Empty Interworkings and Refinement Semantics of Interworkings Revised, p. 19.


De proceedings: ACP'95, p.

On the Connection of Partial Order Logics and Partial Order Reduction Methods, p. 12.

Abstract Interpretation of Reactive Systems: Preservation of CTL*, p. 27.

Specification of tools for Message Sequence Charts, p. 36.


Discrete Time Process Algebra with Abstraction, p. 15.

On Normalisation, p. 33.

Axiomatizing Early and Late Input by Variable Elimination, p. 44.


Petri net based scheduling, p. 20.


Synchronous Sequence Charts In Action, p. 36.

A Class of Petri nets for modeling and analyzing business processes, p. 24.


A Conservative Look at term Deduction Systems with Variable Binding, p. 29.

On Nesting of a Nonmonotonic Conditional, p. 14


Practical Symbolic Model Checking of the full μ-calculus using Compositional Abstraction, p. 17.


Context-Free Graph Grammars and Concatenation of Graphs, p. 35.

Record concatenation with intersection types, p. 46.

An algebraic semantics for hierarchical P/T Nets, p. 32.