Fundamenta Informaticae XII (1989) 139-162
North-Holland

THE ALGEBRA OF SYNCHRONOUS PROCESSES

W.P. WEIJLAND

Centre for Mathematics and Computer Science
Kruislaan 413, 1098 SJ Amsterdam, The Netherlands

Received March 1988 / Accepted May 1988

abstract: An algebraical theory called ASP is presented, describing synchronous cooperation of processes. The theory ASP was first mentioned in BERGSTRA & KLOP [4] as an alternative for the theory ACP, which works with asynchronous cooperation (see also in [5]). One of the main differences between ASP, as it is presented here, and the algebraic theory SCCS of MILNER [9] is the representation of parallelism, which is done by considering a computation step as a vector, each component of which represents an atomic action on a corresponding channel.
This paper concludes with an example, to give an idea how to work with ASP.

1. INTRODUCTION

In the current research on (hardware) verification one of the main goals is to find strong proof systems and tools to specify and verify designs of algorithms and architectures. For instance, in the development of integrated circuits the important stage of testing a prototype (to save the high costs of producing defective processors) can be dealt with much more efficiently, when a strong verification tool is available. Therefore, developing a verification theory has very high priority and is subject of study at many universities and scientific institutions.

In BERGSTRA & KLOP [4] a theory called *Algebra of Communicating Processes* (ACP) is presented, which is an algebraic theory providing us with a formal description of concurrent processes. In ACP, parallelism is described as interleaving and therefore in ACP we have *asynchronous* cooperation of parallel processes. In many cases it turns out, however, that a process can be described much easier in a clocked network instead. Therefore in [4] a variant on ACP, called *Algebra of Synchronous Processes* (ASP), was suggested in which *synchronous* cooperation could be modeled.

In this paper we will present the algebra ASP in full detail. The language used here is quite different from the usual approaches in BERGSTRA & KLOP [4], MILNER [9] and HENNESSY [11]. Especially the fact that parallel composition is represented by taking *vectors* of atomic actions will turn out to simplify the theoretical aspects of the theory.

The idea of developing an algebraic theory for synchronous processes is not new. In fact, the algebra ASP presented in this paper is very similar to the theory SCCS of Milner. On the other hand, there exist some important differences between both theories:

- Since in ASP we use a vector notation to represent parallelism (instead of a new operator as in SCCS and ACP) the theory has a smaller signature. For this reason one may expect that the study of its theoretical aspects will become much easier to deal with. For example, in SCCS the operator $\times$ stands for both parallel composition and communication. In ASP we have the operator $|$ which stands for communication only.
- In SCCS we have handshaking, i.e. apart from occurrences of terms that evaluate to idle actions 1, in any communication one has at most two participants. In ASP this restriction is not needed.
- Abstraction is dealt with in ASP by use of a general renaming operator (like in ACP) whereas SCCS has abstraction automatically which is a restriction, since we do not always want to hide all communication actions of a process. In ASP one can abstract automatically (if it is convenient) by chosing an appropriate communication function.
- As indicated before in SCCS we have an operator $\times$. Now assume in a large and complex configuration we want to evaluate an expression of the form $t=a\times b\times\bar{a}\times c\times b\times\ldots$. then we need to find all pairs of the form $(a,\bar{a})$ such that both a and $\bar{a}$ are subterms of t - recall that in SCCS we have $a\times\bar{a}=1$ for all constants a. This is quite an elaborate job once the complexity of t becomes larger. One could solve this problem by not considering t as a term but as a sequence of symbols with one coordinate for every symbol: $t=[(a,\bar{a}), (b,b), (c), \ldots]$ and then we can evaluate t in linear time. In ASP this evaluation method follows immediately from the construction of vectors of atomic actions and the definition of the communication function.

After having introduced the algebraic theory ASP we will consider two of its models, which may be looked at as an operational and a denotational semantics for ASP. Next we will introduce the notion of recursion and finally study a particular example, in order to illustrate in which way one can work with ASP in practical applications.

At this place I especially want to thank Jos Baeten, who took the time to correct several draft versions of this paper.

2. AN ALGEBRA OF SYNCHRONOUS PROCESSES

In process algebra we start from a collection A of given objects called atomic actions, atoms or steps. These actions are taken to be indivisible, usually have no duration and form the basic building blocks of our systems. The first two compositional operators we consider are $\cdot$, denoting sequential composition and + for alternative composition. If x and y are two processes, then $x\cdot y$ is the process that starts the execution of y after the completion of x, and $x + y$ is the process that chooses either x or y and executes the chosen process (and not the other). Each time a choice is made, we choose from a set of alternatives. We do not specify whether a choice is made by the process itself or by the environment. Axioms A1-5 in table 1 below give the laws that $\cdot$ and + obey. We leave out $\cdot$ and brackets as usual in regular algebra, so $xy + z$ means $(x\cdot y) + z$. $\cdot$ will always bind stronger than other operators, and + will always bind weaker.

On intuitive grounds $x(y + z)$ and $xy + xz$ present different mechanisms (the moment of choice is different), and therefore an axiom $x(y + z) = xy + xz$ is not included. Furthermore, we have a

special constant $\delta \in A$ denoting deadlock, the acknowledgement of a process that it cannot do anything anymore, the absence of an alternative. Axioms A6-7 give the laws for δ. In table 1 all axioms of the *Basic Process Algebra* BPA_δ are presented (see BERGSTRA & KLOP [4]).

$x + y = y + x$	A1
$x + (y + z) = (x + y) + z$	A2
$x + x = x$	A3
$(x + y)z = xz + yz$	A4
$(xy)z = x(yz)$	A5
$x + \delta = x$	A6
$\delta x = \delta$	A7

Table 1. Basic Process Algebra BPA_δ.

The following proposition provides us with a useful tool for induction methods.

PROPOSITION 2.1 *Suppose* t *is a closed term in* BPA_δ *then* t *can be written in one of the following forms:*

1. t *is a constant from* A
2. t *is of the form* u + v, *where* u *and* v *are closed terms of less complexity (depth) than* t
3. t *is of the form* a·u, *where* a *is a constant and* u *is a closed term of less complexity than* t.

Next, suppose a port P is associated to our basic algebra BPA_δ, and suppose we have a binary function $|$ which is both commutative and associative. We may look at $a \mid b$ as a communication action which is the result of simultaneously performing a and b.
Furthermore, assume there exists a unit element $1 \in A$ such that $1 \mid a = a \mid 1 = a$ for all $a \in A$. This unit element stands for an idle action during which a process is still running but not performing any significant step. The notion of an idle action was first introduced by MILNER [9] in a different setting.
In the sequel we assume $|$ to bind stronger than + but weaker than $\cdot$. It follows immediately that:

PROPOSITION 2.2 $(A, |, 1)$ *is an Abelian monoid.*

A function $|$ as described so far is called a *communication function* if δ is a zero element for $|$, i.e. if for all $a \in A$ we have $\delta \mid a = \delta$. The symbol δ is chosen here because of its long tradition in process algebra, especially in ACP.
Resuming, we find that $|$ is a communication function if the following conditions are satisfied (see table 2):

$a \mid b = b \mid a$	C1
$a \mid (b \mid c) = a \mid (b \mid c)$	C2
$\delta \mid a = \delta$	C3
$1 \mid a = a$	C4

Table 2. Communication function ($a,b,c \in A$).

So far, we only considered $\mid$ to be defined on atomic actions. This definition can be extended to processes over BPA_δ as follows. Assume two processes $a \cdot b$ and $c \cdot d$ are both performed in parallel, then $\mid$ acts as a *synchronous communication merge* on both processes, i.e. $(a \cdot b) \mid (c \cdot d) = (a \mid c) \cdot (b \mid d)$. So from two BPA_δ-processes we can construct a new BPA_δ-process by 'stepwise communication'. This intuition can be formally described by adding the following axioms to our algebra for all $a,b \in A$ (see table 3):

$ax \mid b = (a \mid b)x$	SC1
$a \mid by = (a \mid b)y$	SC2
$ax \mid by = (a \mid b)(x \mid y)$	SC3
$(x+y) \mid z = x \mid z + y \mid z$	SC4
$x \mid (y+z) = x \mid y + x \mid z$	SC5

Table 3. Communication merge on processes ($a,b \in A$).

Another way to look at $\mid$ is as follows: from axiom C2 it follows that in expressions with only $\mid$, we may leave out the brackets; thus we write $a \mid a \mid b \mid c$ instead of $((a \mid (a \mid b)) \mid c)$. Therefore, we may consider such expressions as *multisets* of atomic actions, which are all performed simultaneously. Note that, in case one of the two processes terminates in one step (e.g. in $a \mid (b \cdot y)$), after the communication action $a \mid b$ the process continues with y, which fits into the idea of a multiset representation of actions.

Next, we introduce *renaming* operators on BPA_δ-processes (see BAETEN & BERGSTRA [2]). Assume $f: A \to A$ is a function on A, a so-called *atomic renaming*. Then in table 4 the axioms of the renaming function ρ_f are presented.

$\rho_f(\delta) = \delta$	R1
$\rho_f(1) = 1$	R2
$\rho_f(a) = f(a) \quad (a \neq \delta, 1)$	R3
$\rho_f(x+y) = \rho_f(x) + \rho_f(y)$	R4
$\rho_f(xy) = \rho_f(x) \cdot \rho_f(y)$	R5
$(\rho_f \circ \rho_g)(x) = \rho_{f \circ g}(x)$	R6

Table 4. Renaming in ASP ($a \in A$).

A specific example of an atomic renaming is the one which renames all constants from a certain set $I \subseteq A$ into one particular constant $r \in A$, leaving all other elements from A unchanged. The renaming

$r_I(\delta) = \delta$	
$r_I(1) = 1$	
$r_I(a) = r$	for every $a \in I$ $(a \neq \delta, 1)$
$r_I(a) = a$	for every $a \notin I$
$r_I(x + y) = r_I(x) + r_I(y)$	
$r_I(xy) = r_I(x) \cdot r_I(y)$	
$(r_I \circ r_J)(x) = r_{I \cup J}(x)$	

Table 5. Simple renamings in ASP ($r \in A$, $I,J \subseteq A$).

function that results from such an atomic renaming is denoted by r_I and will be referred to as a *simple* renaming function. In table 5 the rules of table 4 are translated for simple renaming functions. Having the axioms R1-R6 we do not need to add them to our system ASP.

In table 6 all axioms introduced so far, are presented together. The algebra which is thus constituted, will be called the *Algebra of Synchronous Processes*, or ASP for short. Since the set of atomic actions A is a parameter of ASP, we will often write ASP(A). However, if A is some arbitrary fixed set then we will write ASP for short. In fact ASP is an *axiom scheme* since we have its axioms for any pair of constants $a,b \in A$, all sets $I \subseteq A$ and all functions $f: A \to A$.

$x + y = y + x$	A1	$a \mid b = b \mid a$	C1
$x + (y + z) = (x + y) + z$	A2	$(a \mid b) \mid c = a \mid (b \mid c)$	C2
$x + x = x$	A3	$\delta \mid a = \delta$	C3
$(x + y)z = xz + yz$	A4	$1 \mid a = a$	C4
$(xy)z = x(yz)$	A5		
$x + \delta = x$	A6		
$\delta x = \delta$	A7		
$\rho_f(\delta) = \delta$	R1		
$\rho_f(1) = 1$	R2	$ax \mid b = (a \mid b)x$	SC1
$\rho_f(a) = f(a)$ $(a \neq \delta, 1)$	R3	$a \mid by = (a \mid b)y$	SC2
$\rho_f(x + y) = \rho_I(x) + \rho_I(y)$	R4	$ax \mid by = (a \mid b)(x \mid y)$	SC3
$\rho_I(xy) = \rho_I(x) \cdot \rho_I(y)$	R5	$(x + y) \mid z = x \mid z + y \mid z$	SC4
$(\rho_f \circ \rho_g)(x) = \rho_{f \circ g}(x)$	R6	$x \mid (y + z) = x \mid y + x \mid z$	SC5

Table 6. ASP(A).

We turn the axioms of table 6 into a term rewriting system in order to be able to define normal forms in ASP. The resulting system will be called RASP.

DEFINITION 2.1 The term rewriting system RASP can be found from table 6 by omitting the axioms A1, A2, C1 and C2 and next replacing all occurences of '=' by $\rightarrow$ (see table 7).

RASP is a term rewrite system on ASP-terms *modulo* commutativity and associativity of + and $\mid$, so we may consider a RASP-normal form to be built from multisets of summands and communications. Note that SC2 and SC5 can be omitted from RASP since $\mid$ is commutative. Obviously, we wish all RASP-reductions to correspond to ASP-derivations. The commutativity and associativity of $\mid$ cannot be derived from ASP for arbitrary processes, however, but we can prove it for all closed terms (note that RASP acts on closed ASP-terms only). The proof of the following proposition is easy by induction on the structure of closed terms.

PROPOSITION 2.3 *For all closed* ASP*-terms* s *and* t *we have that:*
$\mathrm{ASP} \vdash (s \mid t) = (t \mid s)$ *and* $\mathrm{ASP} \vdash (s \mid t) \mid u = s \mid (t \mid u)$.

So, RASP-reductions correspond to ASP-derivations. RASP has some more properties, however, that are crucial in some later proofs.

PROPOSITION 2.4

1. RASP *is strongly terminating.*
2. *If* t *is a normal form with respect to* RASP *then it is a* BPA_δ*-term.*

The proof of proposition 2.4 (1) can be found by using structural induction on ASP-terms. It says that the term rewrite system RASP has no infinite reductions. 2.4 (2) can easily be proved by structural induction on terms that are *not* a BPA_δ-term (hence containing at least one occurrence of $\mid$) and by showing that such a term is always the instantiation of the lefthand side of some rule from RASP. For further information we recommend the reader to consult [4] in which a similar proof is presented in full detail.

$x+x \to x$	RA1	$\delta \mid a \to \delta$	RC1
$(x+y)z \to xz+yz$	RA2	$1 \mid a \to a$	RC2
$(xy)z \to x(yz)$	RA3		
$x+\delta \to x$	RA4		
$\delta x \to \delta$	RA5		
$\rho_I(\delta) \to \delta$	RR1		
$\rho_f(1) \to 1$	RR2		
$\rho_f(a) \to f(a) \quad (a \neq \delta, 1)$	RR3		
$\rho_f(x+y) \to \rho_I(x)+\rho_I(y)$	RR4	$ax \mid b \to (a \mid b)x$	RS1
$\rho_f(xy) \to \rho_I(x)\cdot\rho_I(y)$	RR5	$ax \mid by \to (a \mid b)(x \mid y)$	RS2
$(\rho_f \circ \rho_g)(x) \to \rho_{f \circ g}(x)$	RR6	$(x+y) \mid z \to x \mid z + y \mid z$	RS3

Table 7. RASP(A).

THEOREM 2.5 (elimination)
For any closed ASP*-term* s, *there exists a closed* BPA$_\delta$*-term* t *such that* ASP $\vdash$ s=t.

PROOF From proposition 2.4 it follows that any ASP-term s has a reduction to a normal form t which is a BPA$_\delta$-term. Such a reduction corresponds to a proof in ASP and hence we find that ASP $\vdash$ s=t. □

So starting from any closed term with $\mid$ we can find a derivation, using equations from ASP, to a closed term without these operators (i.e. a closed BPA$_\delta$-term).

PROPOSITION 2.6 RASP *is confluent.*

The proof of proposition 2.6 follows immediately from a routine investigation of the critical pairs in RASP. Recall that if r and r' are rewrite rules such that lhs(r) unifies with a non-variable subterm of r', then lhs(r') can be reduced in two ways: by application of either r or r'. The pair of reducts resulting from every two such rules is called a *critical pair*. Obviously, a term rewriting system is confluent if and only if every critical pair is joinable - i.e. both terms in the pair have a common reduct.

DEFINITION 2.2 The rewriting system RBPA consists of the rules RA1-RA5 from RASP.

RBPA is the subsystem in RASP acting on BPA$_\delta$-terms, i.e. terms without $\mid$ and ρ_f. Note that the rules RA1-RA5 produce BPA$_\delta$-terms as well, hence RBPA can be thought of as a rewriting system on BPA$_\delta$-terms.

PROPOSITION 2.7 *If* t *is in normal form with respect to* RBPA, *then so it is with respect to* RASP.

PROOF Since RA1-RA5 are the only rules in RASP with a BPA_δ-term on the lefthand side, it is clear that a normal form in RBPA cannot be further reduced in RASP. □

Thus we find that every ASP-term has a normal form (proposition 2.4(1)) which is a BPA_δ-term (proposition 2.4(2)) and which is unique modulo the ordering of the summands and communications (proposition 2.6). As a result we find:

THEOREM 2.8 ASP is a conservative extension of BPA_δ.

PROOF Assume $ASP \vdash s=t$ for two BPA_δ-terms s and t, then there exists a proof in ASP consisting of equations $s=u_1$, $u_i=u_{i+1}$, $u_k=t$ $(0<i<k)$ that are closed instances of axioms from ASP. Note that every equation is an instance or a context of an instance of a rule or the reverse of a rule in RASP, and therefore by propositions 2.4(1) and 2.6 s, u_i $(0<i<k)$ and t all have the same normal form.
Since RBPA is a subsystem of RASP, it is terminating and since s and t are BPA_δ-terms they have normal forms with respect to RBPA. These RBPA-normal forms are normal forms with respect to RASP as well (see proposition 2.7) and since RASP is confluent they are equal. Hence, there exists a RBPA-reduction from s and t to a common normal form which corresponds to a proof in the theory BPA_δ. Thus find $BPA_\delta \vdash s=t$. □

It is important to see a conceptual difference between $|$ and the $\times$-operator in SCCS, introduced by MILNER [9]. As is indicated above, $|$ should be interpreted as a *communication* function, working on a certain port which is associated to the algebra (see also [1]). In [9], however, $\times$ is introduced as a (synchronous) parallel composition operator, which is quite different from our notion of communication. Actually, Milner requires every $a \in A$ to have an inverse element $\bar{a}$, such that for all $a \in A$: $a \times \bar{a} = 1$ (hence, $(A-\{\delta\},\times,1,^-)$ is an Abelian group). So, an expression such as $a \times b \times \bar{a} \times c$ can be evaluated to $a \times \bar{a} \times b \times c$ (using commutativity of $\times$), which is equal to $1 \times b \times c$, and thus we obtain $b \times c$ (since 1 is a unit element). This expression, which is in normal form, should be interpreted as the parallel execution of two atomic actions. Note, that in SCCS we automatically abstract from communications such as $a \times \bar{a}$.
Naturally, the question arises how parallel composition can be represented in the theory ASP. Since all atomic actions of the form $a \mid b$ are considered as a communication and not as the parallel execution of two atoms, we have to find a new construct in our theory.

DEFINITION 2.3 Let $\mathcal{P}$ be a set of *ports* and assume A to be a fixed set of atomic actions.
Then $A^{\mathcal{P}}$ is defined as the set of all functions from $\mathcal{P}$ into A.

Functions $\mathbf{v} \in A^{\mathcal{P}}$ are called (atomic) *vectors* and represent the simultaneous execution of the atomic actions $\mathbf{v}(P)$ at all ports $P \in \mathcal{P}$. Vectors are considered to be the new atomic actions in our algebra $ASP(A^{\mathcal{P}})$.

EXAMPLE

Suppose a *buffer* B consists of two ports 'left' and 'right'. Assume $A=\{r(x),s(x),1,\delta: x\in\{a,b\}\}$, where r(x) stands for receiving the value x, and s(x) stands for sending x. A possible definition of B could read as follows:

$$B = (r(a)\ 1)\cdot(1\ s(a)) + (r(b)\ 1)\cdot(1\ s(b)).$$

So, B can receive a value (either a or b) from the left port and next send it away to the right port.

Note that in the signature of both ASP(A) and ASP($A^{\mathcal{P}}$), there exist constants δ and 1. Although it is not necessary to identify these constants with atomic vectors (they both can exist in their own right) we often choose to interpret δ as the vector with only δ's at all its components, and 1 as the vector with all 1's. The *vectors* δ and 1 are denoted by $\boldsymbol{\delta}$ and $\mathbf{1}$ respectively. So $\boldsymbol{\delta}=(\delta\ \delta\ ...\ \delta)$ and $\mathbf{1}=(1\ 1\ ...\ 1)$.

Starting from a fixed algebra ASP(A), we have to define a new communication function between the atomic vectors (apart from the axioms of table 2 there are no further constraints on the choice of such a function). From the definition of the communication function on A, we often choose to define $|$ on atomic vectors from $A^{\mathcal{P}}$ as follows.

DEFINITION 2.4 Suppose $|$ is a communication function on A, then the *natural extension* of $|$ is defined by: if $\mathbf{v}$ and $\mathbf{w}$ are two functions from $A^{\mathcal{P}}$ then for all $P\in\mathcal{P}$

$$(\mathbf{v}\mid\mathbf{w})(P) = \begin{cases} \delta & \text{if for some } P\in\mathcal{P} \text{ we have } (\mathbf{v}(P)\mid\mathbf{w}(P)) = \delta \\ \mathbf{v}(P)\mid\mathbf{w}(P) & \text{otherwise.} \end{cases}$$

So the natural extension of a communication function results from applying the communication function at all ports separately but with the restriction this does not yield a deadlock, not at any port. Otherwise the whole communication fails, i.e. is equal to $\boldsymbol{\delta}$.

In the same way we define a natural extension of the renaming operators. Although ASP($A^{\mathcal{P}}$) permits us to define different renamings, it turns out to be useful to define a natural extension of renamings from ASP(A).

DEFINITION 2.5 Let $f:A\to A$ be an atomic renaming on A. Then for all $\mathbf{v}\in A^{\mathcal{P}}$ the *natural extension* $\mathbf{f}^{\mathcal{P}}$ of f is defined by: $\mathbf{f}^{\mathcal{P}}(\mathbf{v})(P) = f(\mathbf{v}(P))$.

The natural extension $\boldsymbol{\rho}_f{}^{\mathcal{P}}$ of ρ_f is defined as: $\boldsymbol{\rho}_f{}^{\mathcal{P}} := \rho_{f\mathcal{P}}$, often denoted by $\boldsymbol{\rho}_f$ if no confusion arises. Similarly, the natural extension of a simple renaming r_I is denoted by $\mathbf{r}_I{}^{\mathcal{P}}$ or $\mathbf{r}_I$.

Note that the natural extension of a simple renaming need not be simple. In section 5 we will find an application of the definitions 2.4 and 2.5.

3. MODELS

In this section we will study on two models for ASP providing us with a clear operational and a declarative semantics for ASP.

3.1 THE TRANSITION MODEL

The first model we will present here is the *transition model*. The way in which the model will be described strongly resembles the presentation from VAN GLABBEEK [10].

On BPA_δ-terms, for each $a \in A-\{\delta\}$ we define a binary predicate $\rightarrow^a$ and a unary predicate $\rightarrow^a \surd$. Intuitively, $x \rightarrow^a y$ means that process x can evolve into process y by executing a. $x \rightarrow^a \surd$ means that process x can terminate successfully after the execution of a. In table 9 the proof rules for these two predicates are presented. From now on we assume $\rightarrow^a$ and $\rightarrow^a \surd$ to be the minimal predicates that are closed under derivations from table 9.

a :	$a \rightarrow^a \surd$	$(a \neq \delta)$		
+ :	$\dfrac{x \rightarrow^a x'}{(x+y) \rightarrow^a x'}$	$\dfrac{x \rightarrow^a \surd}{(x+y) \rightarrow^a \surd}$	$\dfrac{y \rightarrow^a y'}{(x+y) \rightarrow^a y'}$	$\dfrac{y \rightarrow^a \surd}{(x+y) \rightarrow^a \surd}$
· :	$\dfrac{x \rightarrow^a x'}{x \cdot y \rightarrow^a x' \cdot y}$	$\dfrac{x \rightarrow^a \surd}{x \cdot y \rightarrow^a y}$		

Table 9. The transition predicates $\rightarrow^a$ and $\rightarrow^a \surd$ on BPA_δ-terms ($a \in A-\{\delta\}$).

DEFINITION 3.1 A *bisimulation* is a binary reflexive relation R on BPA_δ-terms with the following properties ($a \in A-\{\delta\}$):

1. If R(p,q) and $p \rightarrow^a p'$, then there exists q' such that $q \rightarrow^a q'$ and R(p',q')
2. If R(p,q) and $q \rightarrow^a q'$, then there exists p' such that $p \rightarrow^a p'$ and R(p',q')
3. If R(p,q), then $p \rightarrow^a \surd$ if and only if $q \rightarrow^a \surd$.

If there exists a bisimulation R between processes p and q, then we say p and q are *bisimilar*, notation: $p \leftrightarrows q$.

THEOREM 3.1 $\leftrightarrows$ *is a congruence relation on* BPA_δ*-terms.*

The proof of theorem 3.1 is left to the reader. Recall that a relation is called a *congruence* if it is an equivalence relation which respects function symbols.

The key point of bisimulation equivalence is the fact that except for having the same traces, all moments of choice in the process are maintained. For instance note that $a(c+d) \not\leftrightarrows (ac+ad)$, since we have $a(c+d) \rightarrow^a (c+d)$ whereas only $(ac+ad) \rightarrow^a c$ and $(ac+ad) \rightarrow^a d$, and clearly we have neither $(c+d) \leftrightarrows c$ nor $(c+d) \leftrightarrows d$.

DEFINITION 3.2 The *transition model* $\mathbb{T}$ is the set of closed BPA_δ-terms modulo $\leftrightarrows$.

DEFINITION 3.3 A *basic term* is a closed BPA_δ-term defined inductively as follows:

1. All constants from A are basic terms.
2. If $t_0,\ldots,t_{n-1}$ are basic terms then so is $t = a_0t_0 + \cdots + a_{n-1}t_{n-1} + b_0 + \cdots + b_{m-1}$ for certain n,m with $n+m>0$, $a_i,b_j \in A$ and $a_i \neq \delta$.

A basic term is often written as $(\Sigma_{i<n}\, a_it_i + \Sigma_{j<m}\, b_j)$.

DEFINITION 3.4 The *depth* dp(t) of a basic term t is defined inductively as follows:

1. for all $a\in A$: $dp(a) = 1$
2. for all $a\in A-\{\delta\}$ and basic terms s: $dp(a\cdot s) = 1 + dp(s)$
3. for any two basic terms s and t: $dp(s + t) = \max(dp(t), dp(s))$.

PROPOSITION 3.2 *For every* BPA_δ*-term* s *there exists a basic term* t *such that* $BPA_\delta \vdash s=t$.

PROPOSITION 3.3 *Let* t *be a basic term and* $a\in A-\{\delta\}$. *Then the following statements hold:*

1. *If* $t\xrightarrow{a} s$, *then* s *is a basic term and* $dp(s)<dp(t)$;
2. *If* $t\xrightarrow{a} s$, *then* $BPA_\delta \vdash t = as + t$ *(i.e.* $a\cdot s$ *is a summand of* t*)*;
3. *If* $t\xrightarrow{a}\surd$, *then* $BPA_\delta \vdash t = a + t$.

The proof of proposition 3.2 is easy and proposition 3.3 can be proved using induction on dp(t). Both proofs are left to the reader (see also BAETEN & VAN GLABBEEK [3]). The following theorem is an important result about the transition predicates of table 9.

THEOREM 3.4 *For all closed* BPA_δ*-terms* s *and* t *we have:* $BPA_\delta \vdash s=t \Rightarrow s\leftrightarrows t$.

PROOF We only need to prove that $\leftrightarrows$ respects all axioms of BPA_δ. For instance consider the axiom (A1) $(s + t) \leftrightarrows (t + s)$. Set $R = I \cup \{(s + t,t + s)\} \cup \{(t + s,s + t)\}$, where I is the binary identity relation. Assume we have R(p,q) then we find that either p and q are identical or $p = (s + t)$ and $q = (t + s)$. Now suppose $(s + t)\xrightarrow{a} u$ then this transition is an instance of one of the +-rules in table 9. Therefore it follows, that either $s\xrightarrow{a} u$ or $t\xrightarrow{a} u$ and so $(t + s)\xrightarrow{a} u$ (applying the +-rule again) and by definition we have R(u,u). In the same way it follows from $(s + t)\xrightarrow{a}\surd$ that $(t + s)\xrightarrow{a}\surd$. Hence we find that R is a bisimulation between $(s + t)$ and $(t + s)$.

In the same way we find that (A2) $((s + t) + u) \leftrightarrows (s + (t + u))$ and (A3) $(s + s)\leftrightarrows s$.

In order to prove (A4) $(s + t)u \leftrightarrows (su + tu)$ set $R = I\cup\{((s + t)u,su + tu)\}\cup\{(su + tu,(s + t)u)\}$, then it easily follows that R is a bisimulation between $(s + t)u$ and $(su + tu)$.

In the same way we find (A5) $(st)u \leftrightarrows s(tu)$. Note that δ nor $\delta\cdot x$ can be the left hand side of any transition, and therefore we have (A6) $s + \delta \leftrightarrows s$ and (A7) $\delta s \leftrightarrows \delta$. □

Clearly δ represents an atomic action which cannot proceed (and hence cannot terminate).
The converse of 3.4 holds as well, as is stated in the following theorem:

THEOREM 3.5 $\mathbb{T}$ *is an initial algebra for* BPA_δ.

PROOF So we have to prove $BPA_\delta \vdash s=t \Leftrightarrow s \leftrightarrows t$. By proposition 3.2 it is sufficient to prove this for basic terms s and t only (using transitivity of $\leftrightarrows$).

$\Rightarrow$ by theorem 3.4.

$\Leftarrow$ This is done by induction on dp(s) + dp(t), as follows.

If dp(s) + dp(t) = 2 it directly follows that both s,t are sums of atomic actions from A and hence $s \leftrightarrows t$ if and only if $BPA_\delta \vdash s=t$. Now assume $s \leftrightarrows t$ for BPA_δ-terms s and t and for all s', t' such that dp(s') + dp(t') < dp(s) + dp(t) and $s' \leftrightarrows t'$, it is already proved that $BPA_\delta \vdash s'=t'$.

It is enough to prove that any summand a or a·s' of s is also a summand of t (and vice versa) since then it follows that both $BPA_\delta \vdash s = s + t$ and $BPA_\delta \vdash t = t + s$, which yields $BPA_\delta \vdash s=t$.

(1) Assume a is a summand of s ($a \in A$), then $s \equiv a + r$ or $s \equiv a$. Clearly $s \rightarrow^a \surd$ and hence $t \rightarrow^a \surd$ since $s \leftrightarrows t$, and therefore by proposition 3.3 it follows that a is a summand of t.

(2) Assume a·s' is a summand of s, i.e. $s \equiv a \cdot s' + r$ or $s \equiv a \cdot s'$. Then $s \rightarrow^a s'$, and so $t \rightarrow^a t'$ for some t' with $s' \leftrightarrows t'$. By proposition 3.3 it follows that t' is a basic term with dp(t')<dp(t) and at' is a summand of t, i.e. $BPA_\delta \vdash t = at' + t$. Furthermore, dp(s')<dp(s) so by induction we conclude that $BPA_\delta \vdash s'=t'$. Hence $BPA_\delta \vdash at'=as'$ and therefore $BPA_\delta \vdash t = as' + t$. □

Theorem 3.5 makes clear that BPA_δ is in fact a full axiomatisation of bisimulation equivalence on closed BPA_δ-terms.

In order to extend BPA_δ to the larger theory ASP, consider the additional rules in table 10:

$\mid$:	$\dfrac{x \rightarrow^a x',\ y \rightarrow^b y'}{x \mid y \rightarrow^{a \mid b} x' \mid y'}$	$\dfrac{x \rightarrow^a x',\ y \rightarrow^b \surd}{x \mid y \rightarrow^{a \mid b} x'}$	$(a \mid b \neq \delta)$
	$\dfrac{x \rightarrow^a \surd,\ y \rightarrow^b y'}{x \mid y \rightarrow^{a \mid b} y'}$	$\dfrac{x \rightarrow^a \surd,\ y \rightarrow^b \surd}{x \mid y \rightarrow^{a \mid b} \surd}$	$(a \mid b \neq \delta)$
ρ_f :	$\dfrac{x \rightarrow^a x'}{\rho_f(x) \rightarrow^{f(a)} \rho_f(x')}$	$\dfrac{x \rightarrow^a \surd}{\rho_f(x) \rightarrow^{f(a)} \surd}$	$(a \neq \delta, 1;\ f(a) \neq \delta)$
	$\dfrac{x \rightarrow^1 x'}{\rho_f(x) \rightarrow^1 \rho_f(x')}$	$\dfrac{x \rightarrow^1 \surd}{\rho_f(x) \rightarrow^1 \surd}$	

Table 10. The transition predicates $\rightarrow^a$ and $\rightarrow^a \surd$ on ASP-terms ($a \in A-\{\delta\}$).

Again, we will assume these transition predicates to be the minimal interpretation which is closed under the rules of table 9 and table 10.

DEFINITION 3.5 The *transition model with communication* $\mathbb{TC}$ is the set of ASP-terms modulo bisimulation equivalence.

THEOREM 3.6 $\mathbb{TC}$ *is an initial algebra for* ASP.

PROOF It is straightforward to prove that ASP $\vdash$ s=t $\Rightarrow$ s$\leftrightarrows$t (*).
So assume s$\leftrightarrows$t for some ASP-terms s and t. By theorem 2.5 it follows that for some BPA_δ-terms s' and t' we have that ASP $\vdash$ s=s' and ASP $\vdash$ t=t'. Now using (*) it follows that s$\leftrightarrows$s' and t$\leftrightarrows$t', so using the transitivity and the commutativity of $\leftrightarrows$ we find that s'$\leftrightarrows$t'. Since both s' and t' are BPA_δ-terms, it then follows from theorem 3.5 that $BPA_\delta \vdash$ s'=t', hence ASP $\vdash$ s'=t'. From ASP $\vdash$ s=s' and ASP $\vdash$ t=t' it then follows that ASP $\vdash$ s=t. □

Later on we will return to the subject of transitions, and consider the transition predicates in models that have a larger domain.

3.2 THE GRAPH MODEL

In this section we consider another model for ASP consisting of equivalence classes of process graphs (see BAETEN, BERGSTRA & KLOP [1]).

DEFINITION 3.6 A *process graph* is a labeled, rooted, finitely branching, directed multigraph.

Recall that rooted graphs are graphs with precisely one node indicated as the root (without further restrictions), and that in a multigraph one may have more than only one arrow (edge) in between two nodes pointing at the same direction (even if they carry the same label).
An edge goes from a node to another (or the same) node, and is labeled with an element from A. We consider only finitely branching process graphs, so every node has only finitely many outgoing edges. Although a process graph may have infinitely many nodes we must be able to reach any node in only finitely many steps. A graph which has finitely many nodes will be called *regular*.
An edge from node s to node s', with label a, will be denoted as $s\rightarrow^a s'$. The nodes in a process graph can be looked at as *states*. $s\rightarrow^a s'$ is called an *a-step* from s to s'.

DEFINITION 3.7 A *simulation* from a graph g to a graph h, notation R: g$\underline{\rightarrow}$h, is a relation R between nodes of g and nodes of h such that:
1. The roots of g and h are related by R;
2. If R(s,t) and from s we can do an a-step to a node s', i.e. we have $s\rightarrow^a s'$ with label a$\in$ A-{δ} (so a$\neq\delta$) then in h we can do a-step from t to a node t' with R(s',t').
3. If R(s,t) and s is an end point in g then t is an end point in h.

A *bisimulation* between two graphs g and h, notation R: g$\underline{\leftrightarrow}$h, is a relation R such that both R: g$\underline{\rightarrow}$h and R^{-1}: h$\underline{\rightarrow}$g. Furthermore, we write g$\underline{\rightarrow}$h if there exists an R such that R: g$\underline{\rightarrow}$h and similarly

we write $g \underline{\leftrightarrow} h$ if there is an R such that R: $g \underline{\leftrightarrow} h$.

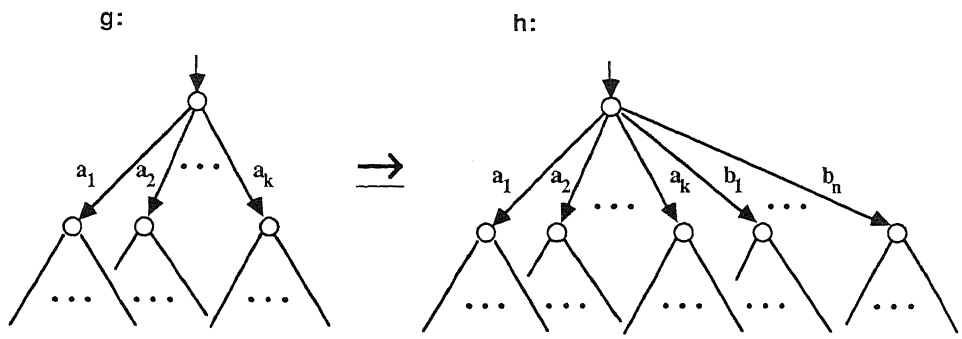
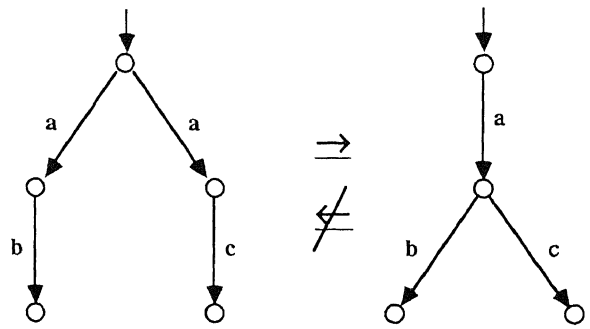


figure 1. R: $g \underline{\rightarrow} h$.

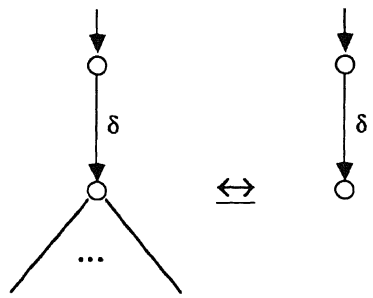
The notion of bisimulation was originally due to PARK [12]. For more information, see MILNER [8], BAETEN, BERGSTRA & KLOP [1].

EXAMPLES

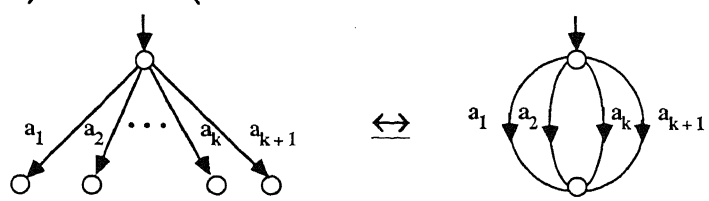
1.



2.



3.

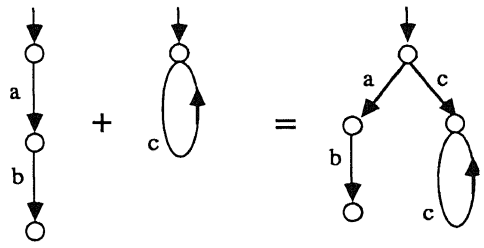


PROPOSITION 3.7 *$\underline{\leftrightarrow}$ is an equivalence relation on the set of process graphs.*

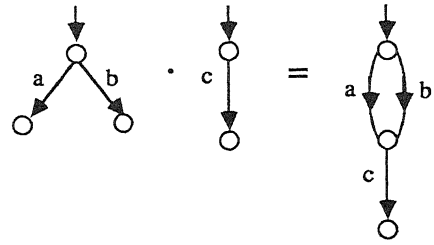
PROOF $\underline{\leftrightarrow}$ is reflexive (i.e. for all process graphs g we have $g \underline{\leftrightarrow} g$) since the identity relation on nodes of g (relating any node precisely with itself) is a bisimulation.
$\underline{\leftrightarrow}$ is commutative (i.e. for all g and h: $g \underline{\leftrightarrow} h \Rightarrow h \underline{\leftrightarrow} g$) directly from the definition.
$\underline{\leftrightarrow}$ is transitive (i.e. for all f, g and h: $f \underline{\leftrightarrow} g$ and $g \underline{\leftrightarrow} h \Rightarrow f \underline{\leftrightarrow} h$), which is proved as follows:
Suppose R: $f \underline{\leftrightarrow} g$ and S: $g \underline{\leftrightarrow} h$. Define the relation T between f and h, such that for any two nodes r in f and t in h: T(r,t) iff there exists a node s in g such that R(r,s) and S(s,t).
1. Now clearly the roots of f and h are related by T.
2. Next, assume T(r,t) and suppose from r we can do an a-step to a node r', so: $r \rightarrow^a r'$ ($a \neq \delta$). Let s be a node in g such that R(r,s) and S(s,t). Since R is a simulation from f to g, we can do an a-step from s to a node s', i.e. $s \rightarrow^a s'$, such that R(r',s'). Furthermore, since S is a simulation from g to h, we have edges $t \rightarrow^a t'$ in h such that S(s',t'). Directly we find that T(r',t') which satifies the second condition in definition 3.7.
3. Finally, assume for some end point r in f we have T(r,t). Let s be such that R(r,s) and S(s,t) then it directly follows that s is an end point in g hence so is t in h.
Thus we find that T: $f \underline{\rightarrow} h$. For reasons of symmetry we conclude T: $h \underline{\rightarrow} f$, hence T: $f \underline{\leftrightarrow} h$. □

Note that δ-edges are not mentioned in the definition of bisimulation. As a consequence we find that starting from a δ-edge, there is no restriction whatsoever on its subgraph (example 2).
Next we will introduce the ASP-operators +, · and | on process graphs in order to turn the set of graphs (modulo $\underline{\leftrightarrow}$) into a model for ASP.

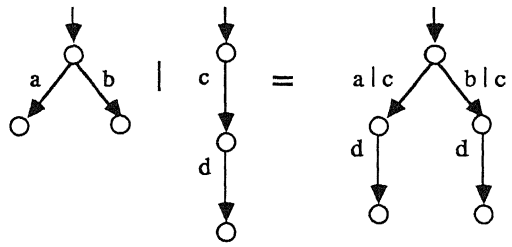
DEFINITION 3.8 The binary functions +, · and | are defined on process graphs as follows. Assume g and h are two such graphs, then:
1. (g + h) is obtained as follows: start from a new root node r, and add a new edge $r \rightarrow^a s'$ for each edge $r_g \rightarrow^a s'$ in g which starts from the root node r_g of g ($a \in A$); similarly, add a new edge $r_h \rightarrow^a t'$ for each $t \rightarrow^a t'$ in h which starts from the root node r_h ($a \in A$). Finally, remove all nodes which have become inaccessible from r.



2. (g·h) is obtained by identifying all end points of g with the root of h. If g has no end points, this is just g. The root of g·h is the root of g.



3. (g | h) is a subgraph of the cartesian product of g and h (i.e. the graph corresponding to the cartesian product of the sets of edges and nodes of g and h) defined as follows:
(a) the root of (g | h) is the pair roots of g and h.
(b) if (s,t) is a node in (g | h) then: (i) if $s \to^a s'$, $t \to^b t'$ are edges in g and h respectively, then $(s,t) \to^{(a \mid b)} (s',t')$ is an edge in (g | h); (ii) if s is an end point in g and $t \to^b t'$ is an edge in h then $(s,t) \to^b (s,t')$ is an edge in (g | h), and (iii) if $s \to^a s'$ is an edge in g and t is end point in h then $(s,t) \to^a (s',t)$ is an edge in (g | h).



DEFINITION 3.9 The unary functions ρ_f are defined on process graphs by simply replacing all labels a ($\neq \delta, 1$) by f(a).

THEOREM 3.8 *$\leftrightarrow$ is a congruence on process graphs with respect to +, ·, | and ρ_f.*

PROOF By proposition 3.7 $\leftrightarrow$ is an equivalence relation. Now assume R: $u \leftrightarrow u'$ and S: $v \leftrightarrow v'$.
Set $T = R \cup S$ and $T^+ = T \cup \{(r(u + v),r(u' + v')),(r(u' + v'),r(u + v))\}$ where r(g) stands for the *root* node of the graph g, and define R | S on the cartesian product of nodes from u and v such that: (R | S)((s,t),(s',t')) if and only if R(s,s') and S(t,t').
1. T^+: $(u + v) \leftrightarrow (u' + v')$, which follows directly from the definitions 3.7 and 3.8-1.
2. T: $(u \cdot v) \leftrightarrow (u' \cdot v')$: the roots of $(u \cdot v)$ and $(u' \cdot v')$ are related. Next, assume in $(u \cdot v)$ we have T(s,t) and $s \to^a s'$, then clearly s and s' both originate from either u or either v. Therefore in either u' or v' (so in $u' \cdot v'$) we have $t \to^a t'$ such that T(s',t').
Assume T(s,t) and s is an end point in $u \cdot v$ then it easily follows that t is an end point in $u' \cdot v'$.
3. (R | S): $(u \mid v) \leftrightarrow (u' \mid v')$. The roots of $(u \mid v)$ and $(u' \mid v')$ are related by (R | S). Next, assume in $(u \mid v)$ we have $(s,t) \to^a (s',t')$ and (R | S)((s,t),(p,q)); by definition we have $s \to^b s'$ and $t \to^c t'$ in p and q respectively, such that $(b \mid c) = a$. Since R and S are simulations and since R(s,p) and

S(t,q), there exist $p \to^b p'$ and $q \to^c q'$ in p' and q' respectively such that R(s',p') and S(t',q'). Hence we have $(p,q) \to^{(b \mid c)} (p',q')$ in $(u' \mid v')$ and clearly $(R \mid S)((s',t'),(p',q'))$.

Finally, assume that R((s,t),(p,q)) for any end point (s,t) in $(u \mid v)$ then it follows easily that (p,q) is an end point in $(u' \mid v')$.

4. R: $\rho_f(u) \leftrightarrows \rho_f(u')$. Suppose in $\rho_f(u)$ there is an edge $s \to^a s'$ and suppose we have R(s,t). Then in u there exists and edge $s \to^b s'$ such that either $b \in \{\delta,1\}$ or f(b)=a. Now there are two cases: (i) if $b \in \{\delta,1\}$ then a=b, and since R is a bisimulation between u and u' there is an edge $t \to^b t'$ in u' with R(s',t'). Therefore in $\rho_f(u')$ there exists an edge $t \to^b t'$, i.e. an edge $t \to^a t'$ such that R(s',t'); (ii) if $b \neq \delta,1$ then a=f(b). In u' there exists an edge $t \to^b t'$ with R(s',t') and clearly we find that in $\rho_f(u')$ there exists an edge $t \to^a t'$ such that R(s',t'). Hence R: $\rho_f(u) \leftrightarrows \rho_f(u')$. □

DEFINITION 3.10 The *graph model* $\mathbb{G}$ is the algebra of all process graphs modulo $\leftrightarrows$.

In this algebra the constants $a \in A$ are interpreted as two-node graphs with one edge in between, labeled with a. The function symbols are defined as in definition 3.8 and 3.9.

THEOREM 3.9 $\mathbb{G}$ *is a model for* ASP.

PROOF The axioms A1-A3 follow almost immediately from the definition of + and bisimulation. In this proof we assume u, v and w to be arbitrary process graphs.

Construct u' from u by taking together all end nodes into one (new) end node. Consider the relation R, which is the identity on u except for the end nodes in u that are related with the new end node in u'. Clearly R is a bisimulation and so $u \leftrightarrows u'$. From this construction and the definition of $\cdot$ we immediately find A4: $(u + v)\cdot w \leftrightarrows u\cdot w + v\cdot w$.

Axiom A5 follows immediately from the definition of $\cdot$. Moreover, the identity relation on u is a bisimulation between u and $(u + \delta)$, so A6: $u \leftrightarrows u + \delta$. The relation which only relates the root nodes of δ and $\delta\cdot u$ is a bisimulation between δ and $\delta\cdot u$, so: A7: $\delta \leftrightarrows \delta\cdot u$.

The axioms C1-C4 and SC1-3 simply follow from definition 3.8. The axioms R1-R6 immediately follow from the definition of renaming on graphs (definition 3.9). □

4. RECURSION

In the previous section we have defined the graph model $\mathbb{G}$, which turned out to be a model for ASP in which we have graphs representing (possibly) infinite processes. In the following we will investigate a way in which infinite processes can be described algebraically.

DEFINITION 4.1 A *recursive specification* over ASP is a set of equations $E = \{x = t_x : x \in V\}$, where V is a set of variables and t_x are ASP-terms only containing variables from V.

DEFINITION 4.2 Let t be an ASP-term and x a variable from t. The occurrence of x in t is called *guarded* if x is preceded by an atomic action from A, i.e. if t has a subterm of the form $a\cdot s$ with $a \in A$, and this x occurs in s. If not, the occurrence of x is called *unguarded*.

A recursive specification is called guarded if each occurrence of a variable is guarded.

DEFINITION 4.3 The *Recursive Definition Principle* (**RDP**) is the rule saying that every guarded recursive specification has a solution.

We will write $\mathcal{A} \models$ **RDP** if the recursive definition principle **RDP** holds in the algebra $\mathcal{A}$.

Recursive specifications are used to specify processes. If a recursive specification E is satisfied in a model and $x \in V$, then $\langle x \mid E \rangle$ will denote the x-component of some solution of E. So if E has more than only one solution, $\langle x \mid E \rangle$ will denote some kind of quantified variable ranging over all E's witnesses (see VAN GLABBEEK [10]). If E has no solution, then $\langle x \mid E \rangle$ remains undefined. Finally, $\langle t \mid E \rangle$ denotes the term t in which each occurrence of a variable $x \in V$ is replaced by $\langle x \mid E \rangle$. The fact that $\langle x \mid E \rangle$ is a solution of E can simply be expressed by: $\langle x \mid E \rangle = \langle t_x \mid E \rangle$.

recursion:	$\dfrac{\langle t_x \mid E \rangle \xrightarrow{a} y}{\langle x \mid E \rangle \xrightarrow{a} y}$	$\dfrac{\langle t_x \mid E \rangle \xrightarrow{a} \surd}{\langle x \mid E \rangle \xrightarrow{a} \surd}$

Table 11. Additional transitions for recursion.

DEFINITION 4.4 The *Recursive Specification Principle* (**RSP**) says that every guarded recursive specification has at most one solution.

So, in a model with both **RDP** and **RSP** every guarded recursive specification has precisely one solution and every term $\langle t \mid E \rangle$ has a unique interpretation.
Let us extend the signature of ASP with unary operators π_n ($n \in \omega$) called *projection functions*, with the axioms of table 12 below ($a \in A$):

$\pi_n(a) = a$	PR1
$\pi_1(a \cdot x) = a$	PR2
$\pi_{n+1}(a \cdot x) = a \cdot \pi_n(x)$	PR3
$\pi_n(x + y) = \pi_n(x) + \pi_n(y)$	PR4

Table 12. The projection functions π_n for $n \geq 1$.

The operator π_n cuts off the process after it has executed n atomic steps.
Now suppose $\mathbb{TC}_R$ is the extension of $\mathbb{TC}$ with new terms $\langle t_x \mid E \rangle$ for every recursive specification E and every variable x in E, satisfying the transitions of table 11. It is easy to extend the models $\mathbb{TC}_R$ and $\mathbb{G}$ with the new operators π_n, obeying the laws in table 12. The extension of the theory ASP with these axioms will be denoted by ASP + PR.

DEFINITION 4.5 The *Approximation Induction Principle* (**AIP**) is the rule that reads:
$(\forall n \geq 1: \pi_n(x) = \pi_n(y)) \Rightarrow x = y$.

PROPOSITION 4.1

1. $\mathbb{TC} \models \mathbf{AIP}$
2. $\mathbb{TC}_R \models \mathbf{RDP}, \mathbf{RSP}, \mathbf{AIP}$
3. $\mathbb{G} \models \mathbf{RDP}, \mathbf{RSP}, \mathbf{AIP}$

The proof of proposition 4.1 is left to the reader.

In order to prove **AIP** in the graph model it turns out to be necessary that process graphs are finitely branching. If not, consider the infinitely branching graphs informally denoted by:

$$g = (\Sigma_{n\in\omega}\, a^n) \text{ and } h = (\Sigma_{n\in\omega}\, a^n) + a^\omega,$$

where a^ω denotes the infinite repetition of a-steps. Clearly, for all $n\in\omega$ we have $\pi_n(g) = \pi_n(h)$ but we do not have $g \leftrightarrows h$.

Clearly $\mathbb{TC} \not\models \mathbf{RDP}$ since no closed term has infinitely many transitions, whereas a process satisfying $x = a{\cdot}x$ can do infinitely many a-steps. Note that in the models $\mathbb{TC}_R$ and $\mathbb{G}$ we do not have that *every* recursive specification has a solution. For instance $\{x = a + xa\}$ has no solution in the model of finitely branching process graphs.

Finally, recall that $\mathbb{TC}_R$ and $\mathbb{G}$ are isomorphic if and only if we allow the specifications E to be infinite as was shown in VAN GLABBEEK [10].

5. EXAMPLE: COMPUTER INTEGRATED MANUFACTURING

In this section we present an example of an application of ASP which is taken from MAUW [7]. In *Computer Integrated Manufacturing* (CIM), computers are integrated in the overall production process of some industrial product. From a high level of view, a plant can be seen as constructed from several concurrently operating *workcells*. Every workcell represents a well-defined part of the manufacturing process and a master control is needed to make the components cooperate correctly. In the following we will present a strong simplification of the CIM-architecture in [7]. It is not our aim to study the theoretical aspects of CIM-architectures in general, but merely to give an illustration of the way ASP applies to practical problems.

Consider the configuration as pictured in figure 2 (next page). This workcell has three components:

(WA) The workstation WA, which receives a 'semiproduct' p from port 4 which is passed through to port 5.

(WB) The workstation WB accepts a product p from port 5, and produces a new product prod(p) which is sent away via port 6.

(WC) The workcell controller receives a certain number n at port 1, which is sent to WA and WB. After the number is accepted WA and WB will both repeat n times (independently) after which a message r ('ready') is sent to the workcell controller.

Imagine a factory in which unfinished semiproducts p have to be turned into commercial products prod(p). Now, the complete configuration should work as follows: from port 1, WC receives a message to generate n products of the form prod(p). So, WC will send the instruction to WA to

'pick up' n products from port 4 and pass it through to WB. Moreover, WC will send the instruction to WB to pick up n products from port 5 and produce n products of the form prod(p).

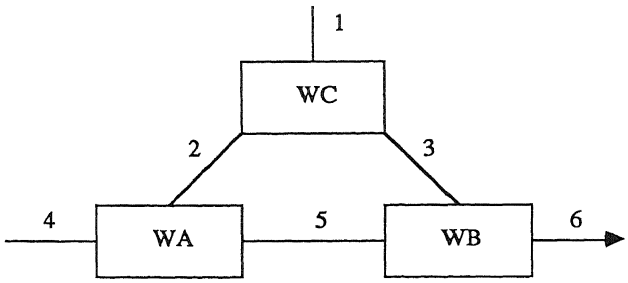


Figure 2. A workcell configuration

The configuration of figure 2 consists of three components interconnected by 6 ports. So we set:

$$\mathcal{P} = \{1, 2, ..., 6\}.$$

Along ports 1, 2 and 3 a positive integer n can be sent. We will assume that $n \leq N$ for some fixed $N \in \omega$. A ready message 'r' can be sent from WA and WB to WC and products of the form p or prod(p) can be sent through ports 4, 5 and 6. So we have a *data set* D defined by:

$$D = \{n: 1 \leq n \leq N\} \cup \{r\} \cup \{p, prod(p)\}.$$

In order to fix the alphabet of ASP, we define the set A of atomic actions as follows:

$$A = \{r(x), s(x), c(x): x \in D\} \cup \{1, \delta\}.$$

On atomic actions from A, the *communication function* $|$ is defined as follows:

$$r(x) \mid s(x) = s(x) \mid r(x) = c(x)$$

whereas all other communications on A not containing 1's are equal to δ.

Next we are ready to present a proper specification of the workcell. From now we will work within the algebra $ASP(A^{\mathcal{P}})$ with the natural extensions of the communication function $|$ (definition 2.4) and the renaming operators (definition 2.5). The constants of $ASP(A^{\mathcal{P}})$ consist of all 6-dimensional vectors $(a_1\ a_2 \ldots a_6)$ where $a_i \in A$ are atomic actions from ASP(A).
At this point we will introduce some shorthand notations that are very useful to avoid the elaborate vector notations.

DEFINITION 5.1 Assume we have a set of ports $\mathcal{P}$ and let $a \in A$ be some atomic action from ASP then for all $Q \in \mathcal{P}$ we define $a_Q \in A^{\mathcal{P}}$ by:

$$a_Q(P) = \begin{cases} a & \text{if } P=Q \\ 1 & \text{if } P\neq Q. \end{cases}$$

So in our setting we have that $r(p)_2 = (1\ r(p)\ 1\ 1\ 1\ 1)$ and $s(r)_5 = (1\ 1\ 1\ 1\ s(r)\ 1)$. Because of a strong tradition in process algebra we will write $r_2(p)$ instead of $r(p)_2$ and $s_5(p)$ instead of $s(p)_5$. Now let us give a precise definition of the three components of the workcell.

$$\begin{aligned}
&WA = \mathbf{1}\cdot \Sigma_{1\leq n\leq N}\, r_2(n)\cdot WA(n)\\
&WA(0) = s_2(r)\\
&WA(n+1) = r_4(p)\cdot s_5(p)\cdot WA(n)\\
&\\
&WB = \mathbf{1}\cdot \Sigma_{1\leq n\leq N}\, r_3(n)\cdot \mathbf{1}\cdot WB(n)\\
&WB(0) = s_3(r)\\
&WB(n+1) = r_5(p)\cdot s_6(prod(p))\cdot WB(n)\\
&\\
&WC = \Sigma_{1\leq n\leq N}\, r_1(n)\cdot WC(n)\\
&WC(n) = (s_2(n) \mid s_3(n))\cdot \mathbf{2n}\cdot r_2(r)\cdot r_3(r)\cdot s_1(r)
\end{aligned}$$

Table 13. A formal specification of the workcell.

In the equation for WC(n) we have used the abbreviation $\mathbf{n}$ for $\mathbf{1}^n$. Formally we could have defined $\mathbf{1}^n$ by use of the inductive definition $\{\mathbf{1}^1 = \mathbf{1},\ \mathbf{1}^{n+1} = \mathbf{1}\cdot\mathbf{1}^n\}$. In the same way we define t^n for ASP-terms t and $n\geq 1$.

Now define:

$$I = \{r(p), c(x): x\in D\}$$

$$WORKCELL = \mathbf{1}_I(WA \mid WB \mid WC).$$

We abstract from actions like r(p) and thus from an unlimited supply of goods available at port 4. It turns out that we can prove the following theorem:

THEOREM 5.1 $WORKCELL = \Sigma_{1\leq n\leq N}\, r_1(n)\cdot \mathbf{3}\cdot (\, s_6(prod(p))\cdot \mathbf{1}\,)^n \cdot s_1(r)$.

PROOF The proof of theorem 5.1 can be given by use of induction on n:

Induction hypothesis For all $1\leq n\leq k$ we have:

(i) $\mathbf{1}_I(\, WA(n) \mid \mathbf{1}\cdot WB(n) \mid \mathbf{2n}\cdot r_2(r)\cdot r_3(r)\cdot s_1(r)\,) = \mathbf{2}\cdot (s_6(prod(p)\cdot 1)^n \cdot s_1(r)$

(ii) $\mathbf{1}_I(\, WA(n) \mid s_6(prod(p))\cdot WB(n) \mid \mathbf{2n}\cdot r_2(r)\cdot r_3(r)\cdot s_1(r))\,) = (s_6(prod(p))\cdot \mathbf{1})^{n+1}\cdot s_1(r)$.

k=1:

(i) $1_I(WA(1) \mid \mathbf{1}\cdot WB(1) \mid \mathbf{2}\cdot r_2(r)\cdot r_3(r)\cdot s_1(r))) =$
$= 1_I(r_4(p)\cdot s_5(p)\cdot s_2(r) \mid \mathbf{1}\cdot r_5(p)\cdot s_6(prod(p))\cdot s_3(r) \mid \mathbf{2}\cdot r_2(r)\cdot r_3(r)\cdot s_1(r))) =$
$= 1_I((r_4(p) \mid 1 \mid 1)\cdot(s_5(p) \mid r_5(p) \mid 1)\cdot(s_2(r) \mid s_6(prod(p)) \mid r_2(r))\cdot(s_3(r) \mid r_3(r))\cdot s_1(r)) =$
$= 1_I(r_4(p)\cdot c_5(p)\cdot(c_2(r) \mid s_6(prod(p))\cdot c_3(r)\cdot s_1(r)) =$
$= \mathbf{2}\cdot s_6(prod(p))\cdot\mathbf{1}\cdot s_1(r).$

(ii) $1_I(WA(1) \mid s_6(prod(p))\cdot WB(1) \mid \mathbf{2}\cdot r_2(r)\cdot r_3(r)\cdot s_1(r))) =$
$= 1_I(r_4(p)\cdot s_5(p)\cdot s_2(r) \mid s_6(prod(p))\cdot r_5(p)\cdot s_6(prod(p))\cdot s_3(r) \mid \mathbf{2}\cdot r_2(r)\cdot r_3(r)\cdot s_1(r)) =$
$= 1_I((r_4(p) \mid s_6(prod(p)) \mid 1)\cdot(s_5(p) \mid r_5(p) \mid 1)\cdot(s_2(r) \mid s_6(prod(p)) \mid r_2(r))\cdot(s_3(r) \mid r_3(r))\cdot s_1(r)) =$
$= 1_I((r_4(p) \mid s_6(prod(p)))\cdot c_5(p)\cdot(c_2(r) \mid s_6(prod(p)))\cdot c_3(r)\cdot s_1(r)) =$
$= (1 \mid s_6(prod(p)))\cdot\mathbf{1}\cdot(1 \mid s_6(prod(p)))\cdot\mathbf{1}\cdot s_1(r) =$
$= (s_6(prod(p))\cdot\mathbf{1})^2 \cdot s_1(r).$

k+1:

(i) $1_I(WA(k+1) \mid \mathbf{1}\cdot WB(k+1) \mid \mathbf{2(k+1)}\cdot r_2(r)\cdot r_3(r)\cdot s_1(r))) =$
$= 1_I(r_4(r)\cdot s_5(p)\cdot WA(k) \mid \mathbf{1}\cdot r_5(p)\cdot s_6(prod(p))\cdot WB(k) \mid \mathbf{1}\cdot\mathbf{1}\cdot\mathbf{2k}\cdot r_2(r)\cdot r_3(r)\cdot s_1(r))) =$
$= 1_I((r_4(p) \mid 1 \mid 1)\cdot(c_5(p) \mid 1)\cdot(WA(k) \mid s_6(prod(p))\cdot WB(k) \mid \mathbf{2k}\cdot r_2(r)\cdot r_3(r)\cdot s_1(r))) =$
$= 2\cdot\ 1_I(WA(k) \mid s_6(prod(p))\cdot WB(k) \mid \mathbf{2k}\cdot r_2(r)\cdot r_3(r)\cdot s_1(r)) =$
$= 2\cdot (s_6(prod(p))\cdot\mathbf{1})^{k+1} \cdot s_1(r)$ (use (ii) with n=k).

(ii) $1_I(WA(k+1) \mid s_6(prod(p))\cdot WB(k+1) \mid \mathbf{2(k+1)}\cdot r_2(r)\cdot r_3(r)\cdot s_1(r))) =$
$= 1_I(r_4(p)\cdot s_5(p)\cdot WA(k) \mid s_6(prod(p))\cdot r_5(p)\cdot s_6(prod(p))\cdot WB(k) \mid \mathbf{1}\cdot\mathbf{1}\cdot\mathbf{2k}\cdot r_2(r)\cdot r_3(r)\cdot s_1(r))) =$
$= 1_I((r_4(p) \mid s_6(prod(p)) \mid \mathbf{1})\cdot(c_5(p) \mid \mathbf{1})\cdot(WA(k) \mid s_6(prod(p))\cdot WB(k) \mid \mathbf{2k}\cdot r_2(r)\cdot r_3(r)\cdot s_1(r))) =$
$= (\mathbf{1} \mid s_6(prod(p)) \mid \mathbf{1})\cdot\mathbf{1}\cdot(s_6(prod(p))\cdot\mathbf{1})^{k+1} \cdot s_1(r)$ (again, use (ii) with n=k)
$= (s_6(prod(p))\cdot\mathbf{1})^{k+2} \cdot s_1(r).$

So we have proved the induction hypothesis to be true for all k. Then it easily follows that:

$WORKCELL = 1_I(WA \mid WB \mid WC) =$
$= 1_I(\Sigma_{1\le n\le N} (1 \mid 1 \mid r_1(n))\cdot(r_2(n)\cdot WA(n) \mid r_3(n)\cdot\mathbf{1}\cdot WB(n) \mid WC(n))) =$
$= \Sigma_{1\le n\le N} r_1(n)\cdot 1_I((r_2(n) \mid r_3(n) \mid s_2(n) \mid s_3(n))\cdot(WA(n) \mid \mathbf{1}\cdot WB(n) \mid \mathbf{2n}\cdot r_2(r)\cdot r_3(r)\cdot s_1(r)))) =$
$= \Sigma_{1\le n\le N} r_1(n)\cdot 1_I((c_2(n) \mid c_3(n))\cdot(WA(n) \mid \mathbf{1}\cdot WB(n) \mid \mathbf{2n}\cdot r_2(r)\cdot r_3(r)\cdot s_1(r)))) =$
$= \Sigma_{1\le n\le N} r_1(n)\cdot\mathbf{1}\cdot 1_I(WA(n) \mid \mathbf{1}\cdot WB(n) \mid \mathbf{2n}\cdot r_2(r)\cdot r_3(r)\cdot s_1(r))) =$
$= \Sigma_{1\le n\le N} r_1(n)\cdot\mathbf{3}\cdot(s_6(prod(p))\cdot\mathbf{1})^n \cdot s_1(r)$ (using the induction hypothesis (i)) □

By theorem 5.1 we have formally proved that after having received a certain value n, WORKCELL will produce n products of the form prod(p) and then return a message that it is ready. Of course we could have considered much more complicated examples than the one presented here.

In the above example we have chosen to use the natural extensions of both operators $\mid$ and ρ_f. In quite a few applications however these extensions do not give us precisely what we want and we are forced to introduce different renaming functions. For instance, the natural extension of r_I in our

example, will rename the atomic action r(p) into 1, no matter at which port it occurs. But what to do then, if we wish to abstract from the occurences of r(p) at one particular port only, and encapsulate all r(p)'s occurring at other ports?

Define the following atomic renamings:

DEFINITION 5.2 For all $v \in A^{\mathcal{P}}$ $f(v)$ is defined as follows:
for all $i \in \mathcal{P}$, $x \in D$:
if $\{(i=4$ **and** $v(i)=r(p))$ **or** $v(i) = c(x)\}$ **then** $f(v)(i) = 1$ **else** $f(v)(i) = v(i)$.

DEFINITION 5.3 For all $v \in A^{\mathcal{P}}$ $g(v)$ is defined as follows:
if for some $i \in \mathcal{P}$, $x \in D$: $\{v(i) = s(x)$ **and** $i \neq 6$ **and** $i \neq 1\}$ **or** $\{v(i) = r(x)$ **and** $i \neq 1\}$
then $g(v) = \delta$ **else** $g(v) = v$.

Using both definitions, and using the axioms of renamings (see table 4) we can derive the following theorem:

THEOREM 5.2 $\rho_f \circ \rho_g(WA \mid WB \mid WC) = \Sigma_{1 \leq n \leq N} r_1(n) \cdot \mathbf{3} \cdot (\, s_6(\mathrm{prod}(p)) \cdot 1 \,)^n \cdot s_1(r)$

The proof of theorem 5.2 follows easily from the proof of theorem 5.1 and is left to the reader.

REFERENCES

[1] Baeten, J.C.M., Bergstra, J.A. and Klop, J.W., *On the consistency of Koomen's fair abstraction rule*, TCS 51 (1/2), pp. 129-176, 1987.

[2] Baeten, J.C.M. Bergstra, J.A., *Global renaming operators in concrete process algebra*, report CS-R8521, Centre of Math and Comp. Sci., Amsterdam 1985.

[3] Baeten, J.C.M. and Van Glabbeek, R.J., *Another look at abstraction in process algebra*, proc. 14th ICALP conf., Karlsruhe (Th. Ottman ed.), Springer LNCS 267, pp. 84-94, 1987.

[4] Bergstra, J.A. and Klop, J.W., *Process algebra for synchronous communication*, Inf.&Control 60 (1/3), pp. 109-137, 1984.

[5] Bergstra, J.A. and Klop, J.W., *The algebra of recursively defined processes and the algebra of regular processes*, proc. 11th ICALP, ed. J. Paredaens, pp. 82-95, Antwerp, Springer LNCS 172, 1984.

[6] Bergstra, J.A. and Klop, J.W., *The algebra of communicating processes with abstraction*, TCS 37(1), blz. 77-121, 1985.

[7] Mauw, S, *Process algebra as a tool for the specification and verification of CIM-architectures*, report P8708, Programming Research Group, University of Amsterdam, 1987.

[8] Milner, R., *A calculus of communicating systems*, Springer LNCS 92, 1980.

[9] Milner, R., *Calculi for synchrony and asynchrony*, TCS 25, pp. 267-310, 1983.

[10] Glabbeek, R.J. van, *Bounded nondeterminism and the approximation induction principle in process algebra*, proc. STACS (F.J.Brandenburg, G.Vidal-Naquet & M.Wirsing eds.), Springer LNCS 247, pp.336-347, 1987.

[11] Hennessy, M., *Synchronous and Asynchronous Experiments on Processes*, Inf.&Control 59, pp. 36-83 (1983).

[12] Park, D.M., *Concurrency and automata on infinite sequences*, Proc. 5th GI Conf., Springer LNCS 104, 1981.