SIAM J. COMPUT.
Vol. 17, No. 6, December 1988

006

READIES AND FAILURES IN THE ALGEBRA OF COMMUNICATING PROCESSES*

J. A. BERGSTRA†, J. W. KLOP‡, AND E.-R. OLDEROG§

Abstract. Readiness and failure semantics are studied in the setting of Algebra of Communicating Processes (ACP). A model of process graphs modulo readiness equivalence, respectively, failure equivalence, is constructed, and an equational axiom system is presented which is complete for this graph model. An explicit representation of the graph model is given, the failure model, whose elements are failure sets. Furthermore, a characterisation of failure equivalence is obtained as the maximal congruence which is consistent with trace semantics. By suitably restricting the communication format in ACP, this result is shown to carry over to subsets of Hoare's Communicating Sequential Processes (CSP) and Milner's Calculus of Communicating Systems (CCS). Also, the characterisation implies a full abstraction result for the failure model. In the above we restrict ourselves to finite processes without τ-steps. At the end of the paper a comment is made on the situation for infinite processes with τ-steps: notably we obtain that failure semantics is incompatible with Koomen's fair abstraction rule, a proof principle based on the notion of bisimulation. This is remarkable because a weaker version of Koomen's fair abstraction rule is consistent with (finite) failure semantics.

Key words. process algebra, concurrency, readiness semantics, failure semantics, bisimulation semantics

AMS(MOS) subject classifications. 68Q05, 68Q10, 68Q55, 68Q45

Introduction. This paper is concerned with the *failure semantics* for communicating processes as introduced by Brookes, Hoare, and Roscoe [BHR84] (see also Rounds and Brookes [RB81].) This notion of failure semantics is based on the assumption that all possible knowledge about a process takes the form of a set of pairs $[\sigma, X]$, where σ is a linear history of events (actions) in which the process has engaged in cooperation with its environment, and where X is a set of events which are impossible after σ. Thus failure semantics can be seen as a linear history semantics enriched by "local branching information."

Two further semantic models of processes will play an auxiliary role in our paper: Milner's model based on the notion of *observational equivalence* [Mi80] or *bisimulation* (see Park [Pa83]) and the *readiness semantics* described in [OH83]. Processes which are equivalent in the sense of bisimulation semantics are also failure equivalent, but failure semantics identifies more processes. Intermediate between bisimulation and failure semantics is the readiness semantics; here positive information (σ, Y) is given about a process: Y is a set of possible actions after the history σ.

Related to the study of failure semantics which was done by Brookes, Hoare, and Roscoe [BHR84] and Brookes [Br83] in the context of Communicating Sequential Processes (CSP) (see [Ho78], [Ho80]) is the work of De Nicola and Hennessy [DH84], where some equivalences, based on the notion of *test*, are introduced, one of which

* Received by the editors February 18, 1986; accepted for publication (in revised form) December 1, 1987. This research was partially supported by the European Communities under ESPRIT contract 432, An Integrated Formal Approach to Industrial Software Development (Meteor).

† Computer Science Department, University of Amsterdam, Kruislaan 409, 1098 SJ Amsterdam and the Department of Philosophy, State University of Utrecht, Heidelberglaan 2, 3584 CS Utrecht, the Netherlands.

‡ Centre for Mathematics and Computer Science, P.O. Box 4079, 1009 AB Amsterdam, the Netherlands.

§ Institut für Informatik und Praktische Mathematik, Christian-Albrechts-Universität Kiel, 2300 Kiel 1, Federal Republic of Germany.

coincides on a class of simple expressions with failure equivalence. The work of De Nicola and Hennessy [DH84] takes place in the context of Milner's Calculus of Communicating Systems (CCS). Connections between CCS and CSP, in regard to failure semantics, were given by Brookes [Br83].

Most of the work just mentioned was carried out in a context where both recursion and hiding (abstraction from silent τ-steps) were present. This combination has complicated matters significantly. The aim of our paper is therefore to investigate the "pure" failure semantics *without recursion* and *hiding* (except for an interesting digression in its final section where the intricate interplay of these phenomena is highlighted). Our context will be ACP, the axiomatic system for the *Algebra of Communicating Processes* as introduced and studied in the series of papers [BK83], [BK84a], [BK84b], [BK84c], [BK85], [BBK85], [BK86a], [BK86b]. (For an introductory survey see [BK86b].) As we shall see, one advantage of this choice is that the different communication concepts of CSP and CCS can be treated in a uniform way (cf. also Milner [Mi83] and Winskel [Wi83]). In fact, to achieve this uniformity we will work here with a mild extension of ACP, where *renaming operators* are present. This system is called ACP_r and is displayed in Table 1. Note that ACP_r is purely equational and, for a finite alphabet of actions, it is a finite axiom system.

It turns out that in our restricted setting readiness and failure semantics have a neat *axiomatisation*, by means of two equations R1,2, which on top of ACP_r yield readiness semantics, and a "saturation" axiom S which, when added to $ACP_r + R1,2$, yields failure semantics. ACP_r alone corresponds to bisimulation semantics. These results are established in the first part of the paper. In §§ 1–3 we construct models for these axiom systems, starting from a domain of finite process graphs on which equivalences $\leftrightarrows$, $\equiv_{\mathcal{R}}$, $\equiv_{\mathcal{F}}$ (bisimulation equivalence, readiness equivalence, failure equivalence, respectively) are divided out. Next, in § 4, the axiom systems for these quotient structures are presented and shown to be complete. The extra axioms R1,2 and S are not new; in a form disguised by many τ's they appear already in [Br83], and they are derivable from the axioms given in [DH84] (see our comparison in Remark 7.3.3). The definitions of $\leftrightarrows$, $\equiv_{\mathcal{R}}$, $\equiv_{\mathcal{F}}$ are also standard. What seems new in our treatment is the strategy of the completeness proofs by means of a decomposition of $\leftrightarrows$, $\equiv_{\mathcal{R}}$, $\equiv_{\mathcal{F}}$ on process graphs in a small number of very simple *process graph transformations* (§ 3).

So we obtain a "graph model" for ACP_r satisfying failure semantics. In §5, an *explicit representation* of this graph model, called the *failure model* is constructed directly from the failure sets. This links our work with that of [BHR84]. The graph model and the failure model are shown to be isomorphic. In § 6 we restrict the general communication format of ACP_r to one-to-one communication. We show that subsets of CSP and CCS can be interpreted within this framework. This serves as a preparation for § 7, where we prove that for ACP_r with one-to-one communication failure equivalence is the *maximal trace respecting congruence.* Here traces are understood as *complete* histories recording all communications up to a final process state. This simple characterisation of failure equivalence seems new. In the proof we use the readiness semantics as a "stepping stone" towards failure equivalence. The characterisation is shown to carry over to the subsets of CSP and CCS introduced in § 6. For CCS we relate our result to the notion of testing introduced in [DH84]. Further on, the characterisation implies that for ACP_r with one-to-one communication the failure model is *fully abstract* with respect to trace equivalence.

The paper concludes in § 8 with a digression in which processes under failure semantics are considered in the context of recursion and hiding. The main point made here is that the proof principle *Koomen's Fair Abstraction Rule* (KFAR), which is

TABLE 1
ACP_r

Algebra of Communicating Processes with renaming. Here a, b range over the set $A_\delta (= A \cup \{\delta\})$ of atomic processes or actions; $\delta \notin A$ is a constant denoting deadlock; x, y, z range over the set of all processes which includes A_δ and is closed under the binary operations $+, \cdot, \|, \lfloor\!\lfloor, |$ and the unary operations ∂_H, a_H, where $H \subseteq A$. See § 1.2 for further explanation.

$x+y=y+x$	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
$a\,\vert\,b=b\,\vert\,a$	C1
$(a\,\vert\,b)\,\vert\,c=a\,\vert\,(b\,\vert\,c)$	C2
$\delta\,\vert\,a=\delta$	C3
$x\|y=x\lfloor\!\lfloor y+y\lfloor\!\lfloor x+x\,\vert\,y$	CM1
$a\lfloor\!\lfloor x=ax$	CM2
$ax\lfloor\!\lfloor y=a(x\|y)$	CM3
$(x+y)\lfloor\!\lfloor z=x\lfloor\!\lfloor z+y\lfloor\!\lfloor z$	CM4
$ax\,\vert\,b=(a\,\vert\,b)x$	CM5
$a\,\vert\,bx=(a\,\vert\,b)x$	CM6
$ax\,\vert\,by=(a\,\vert\,b)(x\|y)$	CM7
$(x+y)\,\vert\,z=x\,\vert\,z+y\,\vert\,z$	CM8
$x\,\vert\,(y+z)=x\,\vert\,y+x\,\vert\,z$	CM9
$\partial_H(a)=a$ if $a\notin H$	D1
$\partial_H(a)=\delta$ if $a\in H$	D2
$\partial_H(x+y)=\partial_H(x)+\partial_H(y)$	D3
$\partial_H(xy)=\partial_H(x)\cdot\partial_H(y)$	D4
$a_H(b)=b$ if $b\notin H$	RN1
$a_H(b)=a$ if $b\in H$	RN2
$a_H(x+y)=a_H(x)+a_H(y)$	RN3
$a_H(xy)=a_H(x)\cdot a_H(y)$	RN4

important in system verification and which can be justified in bisimulation semantics, is not valid in any extension of (finite) failure semantics. As far as we know this observation, which is supported by deriving a formal inconsistency, is new. Remarkably, a weaker version of KFAR turns out to be both useful for verification and consistent with finite failure semantics (see [BKO86]).

1. The domain $\mathbb{H}_\delta$ of finite acyclic process graphs. In order to build a "graph model" for the axiomatisation ACP_r (see Introduction, Table 1) which also satisfies failure semantics, we start by introducing a domain of process graphs ($\mathbb{H}_\delta$) enriched with a number of operations $+, \cdot, \|, \lfloor\!\lfloor, |, \partial_H, a_H (a \in A)$ corresponding to the operators in ACP_r. It should be emphasized that this structure $\mathbb{H}_\delta(+, \cdot, \|, \lfloor\!\lfloor, |, \partial_H, a_H, a, \delta)(a \in A)$ is not yet a model of ACP_r; it becomes so after dividing out by a suitable equivalence on $\mathbb{H}_\delta$ (which, of course, should be a congruence with respect to the operations). For example, dividing out by bisimulation equivalence (as defined in § 2.3 below) yields a model of ACP_r, and in fact one that is isomorphic to the initial model of ACP_r. This

matter does not, however, concern us in this paper. What we are interested in is the quotient structure obtained by dividing out by readiness equivalence or failure equivalence, respectively (defined below in 2.2), that is, what we will call (in analogy with "term model") the graph model for ACP_r, satisfying readiness semantics or failure semantics, respectively.

1.1. Finite acyclic process graphs in δ-normal form. A process graph over a set is a rooted, directed multigraph whose edges are labeled by elements of this set. Let $\mathbb{H}$ be the collection of *finite acyclic* process graphs over the alphabet $A_\delta = A \cup \{\delta\}$ (here $\delta \notin A$) consisting of actions $a, b, \cdots \in A$ and the constant δ denoting deadlock. In the sequel we will work with $\mathbb{H}_\delta \subseteq \mathbb{H}$, the subset of δ-normal process graphs. A process graph $g \in \mathbb{H}$ is δ-normal if whenever an edge $s \xrightarrow{\delta} t$ occurs in g, then the node s has outdegree 1 and the node t has outdegree 0. In anthropomorphic terminology, let us say that an edge $s \to t$ is an *ancestor* of $s' \to t'$ if it is possible to move along edges from t to s'; likewise the latter edge will be called a *descendant* of the former. Edges having the same initial node are *brothers*. So, a process graph g is δ-normal if all its δ-edges have no brothers and no descendants.

Note that for $g \in \mathbb{H}$ the ancestor relation is a partial order on the set of edges of g.

We will now associate to a process graph $g \in \mathbb{H}$ a unique g' in δ-normal form, by the following procedure:

(1) *nondeterministic δ-removal* is the elimination of a δ-edge having at least one brother.

(2) *δ-shift* of a δ-edge $s \xrightarrow{\delta} t$ in g consists of deleting this edge, creating a fresh note t', and adding the edge $s \xrightarrow{\delta} t'$.

Now it is not hard to see that the procedure of repeatedly applying (in arbitrary order) (1), (2) in g will lead to a unique graph g' which is δ-normal; this g' is the *δ-normal form* of g. It is understood that pieces of the graph which have become inaccessible from the root, are discarded.

Example 1.1.1. See Fig. 1, where g' is the δ-normal form of g.

1.2. Operations on process graphs. On $\mathbb{H}_\delta$ we define the operations $+, \cdot, \|, \lfloor\!\lfloor, |, \partial_H$, as in [BK85], [BK86a], and moreover rename operators a_H. The constants a, $\delta (a \in A)$ are represented by graphs consisting of a single arrow labeled by a, δ, respectively. For the sake of completeness we repeat the definitions briefly:

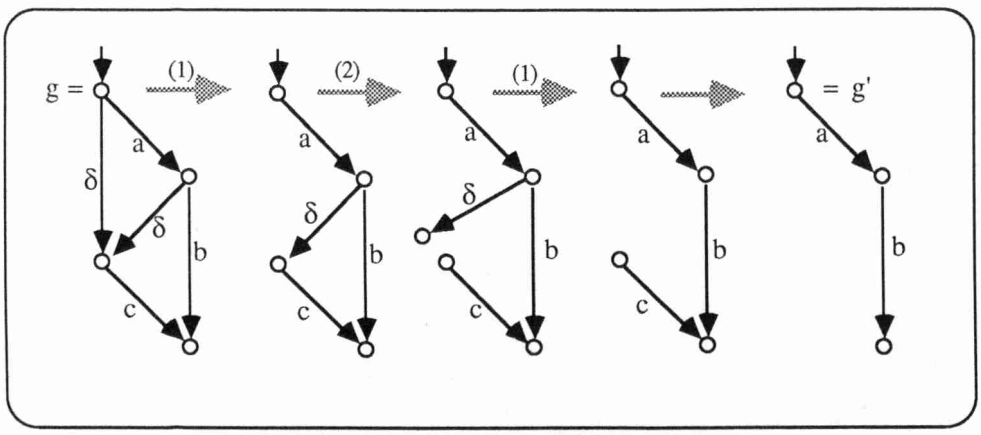


FIG. 1

(i) The *sum* $g+h$ is the graph obtained by identifying the roots of g, h and taking the δ-normal form (this is necessary if g or h is the graph consisting of a single step labeled with δ).

(ii) The *product* $g \cdot h$ is obtained by appending h at all terminal nodes which are not terminal nodes of a δ-step.

(iii) The *merge* $g \| h$ consists of the δ-normal form of the process graph obtained as the Cartesian product of g, h augmented with diagonal edges for successful communications.

(iv) The *left-merge* $g \lfloor\!\lfloor h$ is the subgraph of $g \| h$, where an initial step must be one from g.

(v) The *communication merge* $g | h$ is the subgraph of $g \| h$, where an initial step must be a communication result of an initial step in g and an initial step in h.

(vi) The *encapsulation* $\partial_H(g)$ is the result of renaming all (labels of) steps in $H \subseteq A$ by δ, and taking the δ-normal form.

(vii) The *renaming* $a_H(g)$ is the result of renaming all (labels of) steps in $H \subseteq A$ by a. We have renamings a_H for each $a \in A$.

Example 1.2.1. Let g be the process graph in Fig. 2(a) and h the process graph in Fig. 2(b). Let the communication function $|: A_\delta \times A_\delta \to A_\delta$ be such that $a | c = e$ and $b | d = f$, all other communications equal δ. Then $g+h$ is the graph in Fig. 2(c); $g \cdot h$ is the graph in Fig. 2(d); $g \| h$ is the δ-normal form of the graph in Fig. 2(e), which is the graph in Fig. 2(f); $g \lfloor\!\lfloor h$ is the graph in Fig. 2(g); $g | h$ is the graph in Fig. 2(h); $\partial_{\{a,d\}}$ (g) is the graph in Fig. 2(i); $\partial_{\{a,d\}}$ (h) is the graph in Fig. 2(j); and $a_{\{b\}}$ (g) is the graph in Fig. 2(k).

2. Equivalences on process graphs. Though in this paper our main interest is in the *ready equivalence* and the *failure equivalence*, we also will consider trace equivalence and bisimulation equivalence. In this section these notions are introduced and compared. At the end of the section the concept of a *convexly saturated* process graph is introduced, which illuminates the relationship between ready and failure equivalence and which will play an important role in establishing the completeness of the axiom systems for ready and failure equivalence, respectively, presented in § 4.

2.1. Trace equivalence. Consider a process graph $g \in \mathbb{H}_\delta$. Every path in g from the root of g to some node in g determines a word $s \in A_\delta^*$ formed by concatenating the labels in the consecutive steps in the path. Any such word σ will be called a *history* of (the path in) g. We are particularly interested in *complete histories*, i.e., words determined by paths ending in a terminal node. Throughout this paper complete histories will be called *traces*. By trace (g) we denote the set of all traces of g. *Trace equivalence* $\sim_{\mathrm{tr}}$ of process graphs $g, h \in \mathbb{H}_\delta$ is defined as follows:

$$g \sim_{\mathrm{tr}} h \quad \text{iff trace}\,(g) = \text{trace}\,(h).$$

Note that there are two types of traces: *successful traces* $\sigma \in A^*$ ending in a successful termination node (see § 2.2) and *deadlocking traces* $\sigma \cdot \delta \in A^* \cdot \{\delta\}$ ending in δ.

2.2. Ready equivalence and failure equivalence. We will distinguish four types of nodes of $g \in \mathbb{H}_\delta$.

(i) End nodes of δ-steps in g are *improper*.

(ii) Begin nodes of δ-steps are called *deadlock nodes*.

(iii) Termination nodes of g other than those in (i) are *successful termination nodes*.

(iv) Nonterminal nodes which are not deadlock nodes.

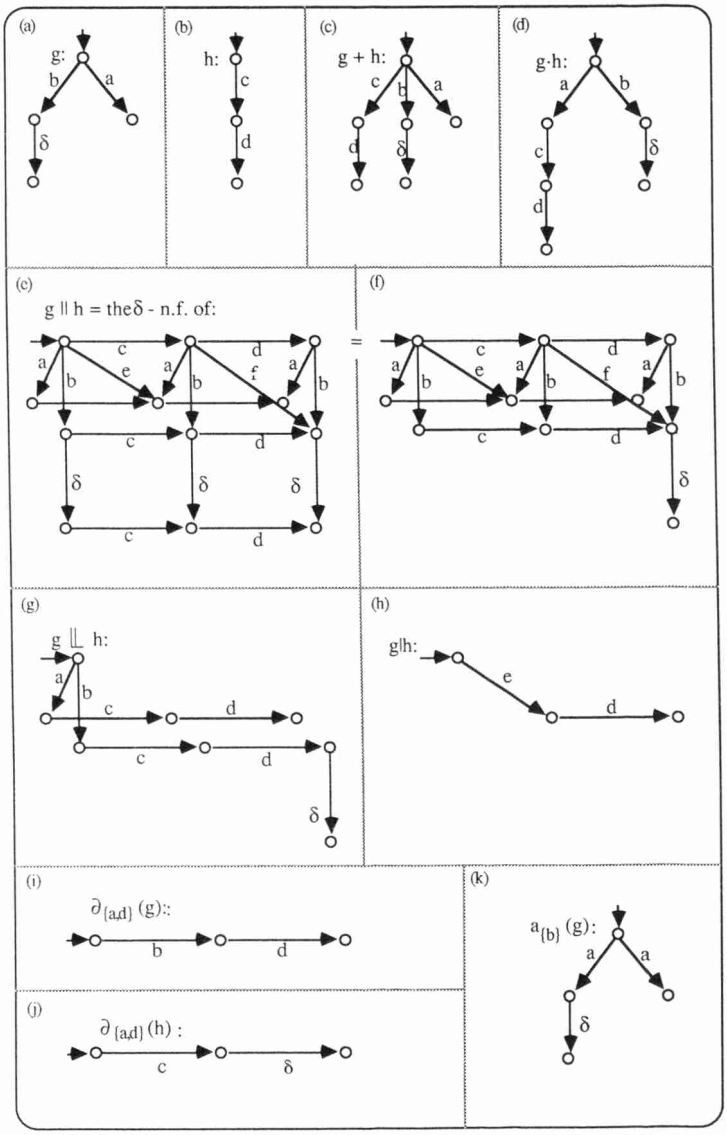


FIG. 2

The *successor set* of node s as in (ii) is, by definition, $\varnothing$. The successor set of a node s as in (iv) is the set of labels $\in A$ of edges with begin node s. A node as in (i) or (iii) has no successor set.

Now (σ, X) where $\sigma \in A^*$, $X \subseteq A$ is a *ready pair* of g if there is a path from root s_0 to some proper node s which is not a successful termination node, with history σ and X as the successor set of s. The *ready set* of g is the set of all ready pairs of g together with all successful traces. Notation: $\mathscr{R}[\![g]\!]$.

The *failure set* of g, notation: $\mathscr{F}[\![g]\!]$, is defined as follows. If $(\sigma, X) \in \mathscr{R}[\![g]\!]$, then $[s, Y]$ is a *failure pair* of g if $Y \subseteq X^c$, and Y is called a *refusal set.* Here and in the sequel we use the following notation: $X^c = A - X$. Now $\mathscr{F}[\![g]\!]$ is the set of all failure

pairs of g, together (again) with the successful traces of g. Thus we have

$$\mathcal{R}[\![g]\!] = \{\sigma | \sigma \text{ is a successful trace of } g\} \cup \{(\sigma, X) | (\sigma, X) \text{ is a ready pair of } g\},$$

$$\mathcal{F}[\![g]\!] = \{\sigma | \sigma \text{ is a successful trace of } g\} \cup \{[\sigma, Y] | Y \subseteq X^c \text{ for some } (\sigma, X) \in \mathcal{R}[\![g]\!]\}.$$

Note that δ does not appear anywhere in $\mathcal{R}[\![g]\!]$ and $\mathcal{F}[\![g]\!]$.

Example 2.2.1. Consider g as in Fig. 3; at each node its type (i)-(iv) is indicated. Moreover Table 2 contains the contribution of each node to the failure and ready set of g.

Example 2.2.2. (i) Let δ be the graph consisting of one δ-step. Then $\mathcal{R}[\![\delta]\!] = \{(\varepsilon, \emptyset)\}$ and $\mathcal{F}[\![\delta]\!] = \{[\varepsilon, Y] \mid Y \subseteq A\}$.

(ii) Let $a \in A$. Then $\mathcal{R}[\![a]\!] = \{(\varepsilon, \{a\}), a\}$ and $\mathcal{F}[\![a]\!] = \{a\} \cup \{[\varepsilon, Y] \mid Y \subseteq A - \{a\}\}$.

(iii) Let $a\delta$ be the graph consisting of a consecutive a- and δ-step. Then $\mathcal{R}[\![a\delta]\!] = \{(\varepsilon, \{a\}), (a, \emptyset)\}$ and $\mathcal{F}[\![a\delta]\!] = \{[\varepsilon, Y] \mid Y \subseteq A - \{a\}\} \cup \{[a, Z] \mid Z \subseteq A\}$.

DEFINITION 2.2.3. Let $g, h \in \mathbb{H}_\delta$. Then $g \equiv_{\mathcal{R}} h$ if $\mathcal{R}[\![g]\!] = \mathcal{R}[\![h]\!]$ and $g \equiv_{\mathcal{F}} h$ if $\mathcal{F}[\![g]\!] = \mathcal{F}[\![h]\!]$. In other words, g, h are *ready equivalent*, and *failure equivalent*, respectively.

2.3. Bisimulation equivalence. For the sake of completeness we include the definition of the well-known notion of a bisimulation.

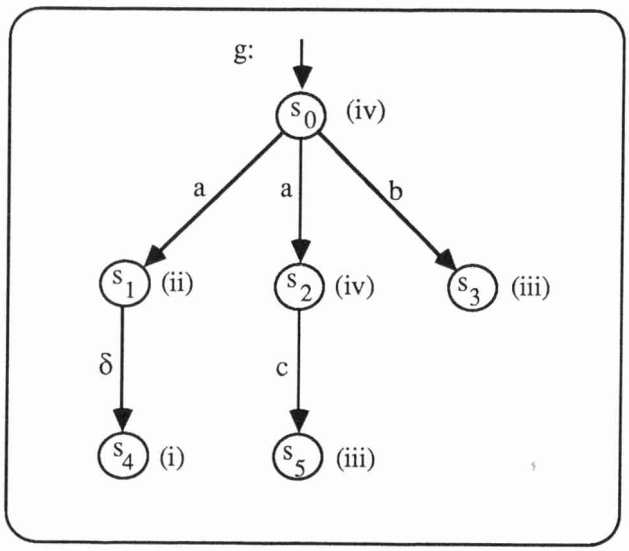


FIG. 3

TABLE 2

	$\mathcal{R}[\![g]\!]$	$\mathcal{F}[\![g]\!]$
s_0	$(\varepsilon, \{a, b\})$	$[\varepsilon, Y]$, $Y \subseteq A - \{a, b\}$
s_1	$(a, \emptyset)$	$[a, Y]$, $Y \subseteq A$
s_2	$(a, \{c\})$	$[a, Y]$, $Y \subseteq A - \{c\}$
s_3	b	b
s_4		
s_5	ac	ac

DEFINITION 2.3.1. Let $g, h \in \mathbb{H}_\delta$. Let ROOT (g), ROOT (h) denote the root of g, h, respectively, and let NODES (g), NODES (h) denote the set of nodes of g, h, respectively.

Then $R \subseteq$ NODES $(g) \times$ NODES (h) is a *bisimulation* from g to h if:

(i) (ROOT (g), ROOT $(h)) \in R$;

(ii) If $(s, t) \in R$ and $s \xrightarrow{u} s'$ (where $u \in A_\delta$) is an edge in g, then $(s', t') \in R$ for some t' such that $t \xrightarrow{u} t'$;

(iii) If $(s, t) \in R$ and $t \xrightarrow{u} t'$ (where $u \in A_\delta$) is an edge in h, then $(s', t') \in R$ for some s' such that $s \xrightarrow{u} s'$.

Notation: $g \leftrightarrows h$ (g, h are *bisimulation equivalent*, or *bisimilar*) if there is a bisimulation from g to h (or vice versa).

As we will want to model the axiom $\delta \cdot x = \delta$ later, we profit here from the fact that only δ-normal process graphs are considered. Otherwise the definition of bisimulation would be more involved.

2.4. Comparing the equivalences. It is not hard to compare the four equivalences $\sim_{\mathrm{tr}}$, $\equiv_{\mathcal{R}}$, $\equiv_{\mathcal{F}}$, and $\leftrightarrows$: for $g, h \in \mathbb{H}_\delta$ we have

$$g \leftrightarrows g \Rightarrow g \equiv_{\mathcal{R}} h \Rightarrow g \equiv_{\mathcal{F}} h \Rightarrow g \sim_{\mathrm{tr}} h$$

and in general none of these implications can be reversed as some of the following examples (e.g., Example 2.4.2) show. Lemma 2.5.5 states a sufficient condition for reversing the second implication.

In the sequel we will prove (Proposition 4.2.3) that $g \equiv_{\mathcal{R}} h$ and $g \equiv_{\mathcal{F}} h$ are *congruences* with respect to the operations defined above in § 1.2. Also $\leftrightarrows$ is a congruence; see Theorem 2.5 of [BK85] for the more complicated situation where τ-steps are present. Trace equivalence however is *not* a congruence with respect to these operations, as the following example shows.

Example 2.4.1. Let $\mathcal{C}[\xi]$ be the context $\partial_{\{b,c\}}(\xi \parallel c)$, and let a, b, b^o, c, c^o be atoms with communications $b \mid b = b^o$, $c \mid c = c^o$ and all other communications resulting in δ. Consider the trace equivalent processes $a(b+c)$ and $ab+ac$. Then $\mathcal{C}[a(b+c)] = ac^o \not\sim_{\mathrm{tr}} a\delta + ac^o = \mathcal{C}[ab+ac]$.

Example 2.4.2. See Fig. 4.

2.5. Convexly saturated process graphs. Following [Br83] and [DH84] we introduce the following notion of convexity.

DEFINITION 2.5.1. $\mathcal{X} \subseteq \mathcal{P}(A)$ is *convex* if

(i) $X, Y \in \mathcal{X} \Rightarrow X \cup Y \in \mathcal{X}$;

(ii) $X, Y \in \mathcal{X}, X \subseteq Z \subseteq Y \Rightarrow Z \in \mathcal{X}$.

(Here $\mathcal{P}(A)$ is the power set of A. In particular, $\emptyset \subseteq \mathcal{P}(A)$ is convex.)

DEFINITION 2.5.2. (i) Let $g \in \mathbb{H}_\delta$ and $\sigma \in A^*$. Then $g \mid \sigma = \{X \mid (\sigma, X) \in \mathcal{R}[\![g]\!]\}$.

(ii) g is *convexly saturated* (or just "convex" or "saturated") if $g \mid \sigma$ is convex, for all $\sigma \in A^*$.

Example 2.5.3. In Fig. 5, g_1, g_2 are not convexly saturated, but their "convex saturations" g_1', g_2' are.

PROPOSITION 2.5.4. *Let $\mathcal{X} \subseteq \mathcal{P}(A)$ be convex, and let $Y \subseteq A$ be a finite set such that $Y \notin \mathcal{X}$, $Y \subseteq \bigcup \mathcal{X}$. Then for no $X \in \mathcal{X}$ we have $Y^c \subseteq X^c$.*

Proof. Consider a finite Y such that $Y \notin \mathcal{X}$, $Y \subseteq \bigcup \mathcal{X}$. Suppose that there is an $X \in \mathcal{X}$ such that $Y^c \subseteq X^c$, or equivalently $X \subseteq Y$. Clearly, Y is covered by finitely many members from $\mathcal{X}$, hence (since $\mathcal{X}$ is convex) by some $Z \in \mathcal{X}$. From $X \subseteq Y \subseteq Z$ it follows that $Y \in \mathcal{X}$, a contradiction. □

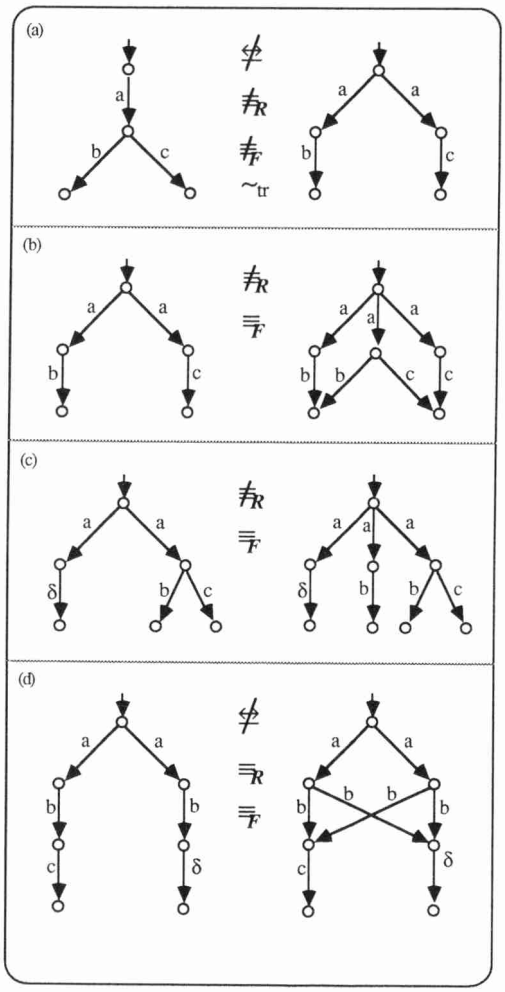


FIG. 4

LEMMA 2.5.5. *Let $g, h \in \mathbb{H}_\delta$ be convexly saturated. Then*

$$g \equiv_{\mathcal{R}} h \Leftrightarrow g \equiv_{\mathcal{F}} h.$$

Proof. Only to prove ($\Leftarrow$). So, we suppose $g \not\equiv_{\mathcal{R}} h$ and we want to prove $g \not\equiv_{\mathcal{F}} h$. Furthermore, we may suppose that g, h have the same trace set; otherwise $g \not\equiv_{\mathcal{F}} h$ is immediate. Now there is a ready pair (σ, X) in (say) $\mathcal{R}[\![g]\!]$ but not in $\mathcal{R}[\![h]\!]$. By $(\sigma, X) \in \mathcal{R}[\![g]\!]$ we have the failure pair $[\sigma, X^c] \in \mathcal{F}[\![g]\!]$. Now consider $h|\sigma$, which is by assumption convex. Since $g \sim_{\mathrm{tr}} h$, we have $X \subseteq \bigcup(h|\sigma)$. Furthermore, $(\sigma, X) \notin \mathcal{R}[\![h]\!]$ entails $X \notin h|\sigma = \{X_i \mid i \in I\}$. So, by Proposition 2.5.4: for no $i \in I$ we have $X^c \subseteq X_i^c$. But then $[\sigma, X^c] \notin \mathcal{F}[\![h]\!]$ and we have $g \not\equiv_{\mathcal{F}} h$. $\square$

3. Transformations on process graphs. We now introduce four *elementary transformations* on process graphs $\in \mathbb{H}_\delta$ with the following property: the first two of them generate, when applied on $g \in \mathbb{H}_\delta$, all process graphs g' *bisimilar* to g; further, the first three generate the *ready equivalence* class of g; and finally, the four together generate the *failure equivalence* class of g.

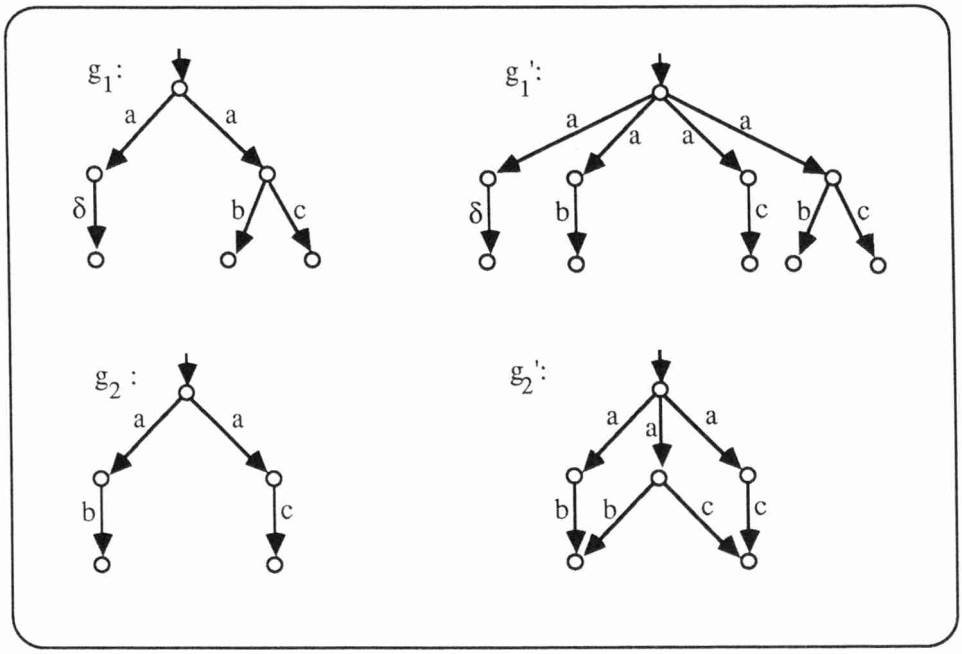


FIG. 5

3.1. The transformations double edge, sharing, cross, and fork.

[i] Double edge. This process graph transformation step removes in a *double edge* as in Fig. 6 (where $a \in A$), one of the edges. Notation: $g \Rightarrow_{[i]} h$.

[ii] Sharing. Suppose $g \in \mathbb{H}_\delta$ contains two nodes s, t determining isomorphic subgraphs $(g)_s$, $(g)_t$. Then the nodes s, t may be identified. Notation: $g \Rightarrow_{[ii]} h$.

[iii] Cross. If s is a node of $g \in \mathbb{H}_\delta$, σ is a *history* of s if there is a path from the root of g to s yielding the word σ. Furthermore, history(s) is the set of all histories of s. Now let $g \in \mathbb{H}_\delta$ contain a part as in Fig. 7(a), where history(s_1) = history(s_2). Then edges, as in Fig. 7(b), may be inserted. Notation: $g \Rightarrow_{[iii]} h$.

Note that the condition on histories is fulfilled when g is a process tree. Furthermore, note that the condition on histories is necessary: it is easy to give an example where this requirement is violated and such that after insertion of the two new steps we have new ready pairs or new completed traces.

[iv] Fork. Let $g \in \mathbb{H}_\delta$ contain a part as in Fig. 8(a), *where all successor steps* $b_1, \cdots, b_n$ *of the left a-step are displayed.* Then a part as indicated in Fig. 8(b) may be inserted. Notation: $g \Rightarrow_{[iv]} h$.

Here it is not required that all steps $b_1, \cdots, b_n, c_1, \cdots, c_m$ have different end nodes. If $n = 1$, b_1 may be δ; likewise c_1 may be δ. In such a case, after inserting the fork we have to δ-normalise the resulting graph again. We emphasize that a fork connects *all* of the successor steps of the left a-step with *some* of those of the right a-step.

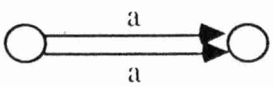


FIG. 6

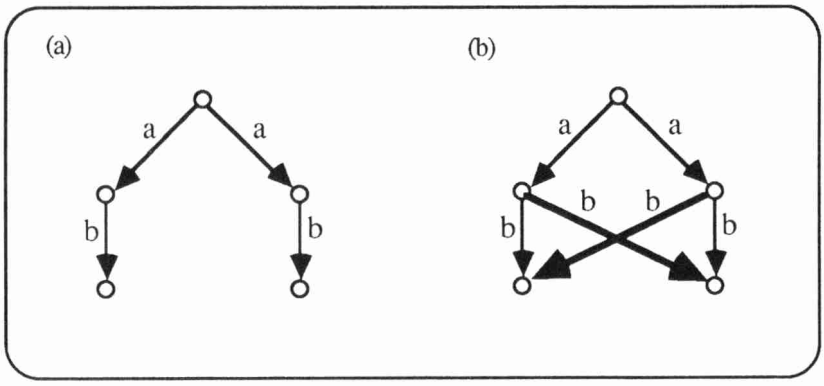


FIG. 7

Notation 3.1.1. (i) $\Rightarrow$ is $\Rightarrow_{[i]} \cup \cdots \cup \Rightarrow_{[iv]}$;

(ii) $\Rightarrow^*$ is the transitive reflexive closure of $\Rightarrow$;

(iii) $\Leftrightarrow^*$ is the equivalence relation generated by $\Rightarrow$.

Example 3.1.2. (i) See Fig. 9. Note how $\Rightarrow_{[iii]}$ enables us to switch subgraphs x, y at the end of paths with the same history (abc in Fig. 9(b)).

(ii) (See Fig. 10.) Figure 10(a) contains an example of a fork transformation. Figure 10(b) contains an example of a fork transformation involving a δ-step. Figure 10(c) shows that complete branches can be pruned by successive transformations.

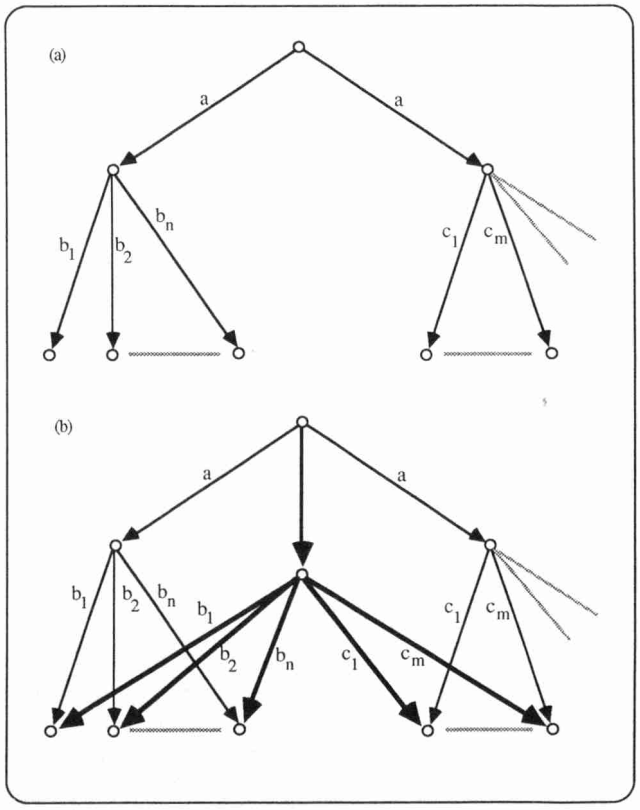


FIG. 8

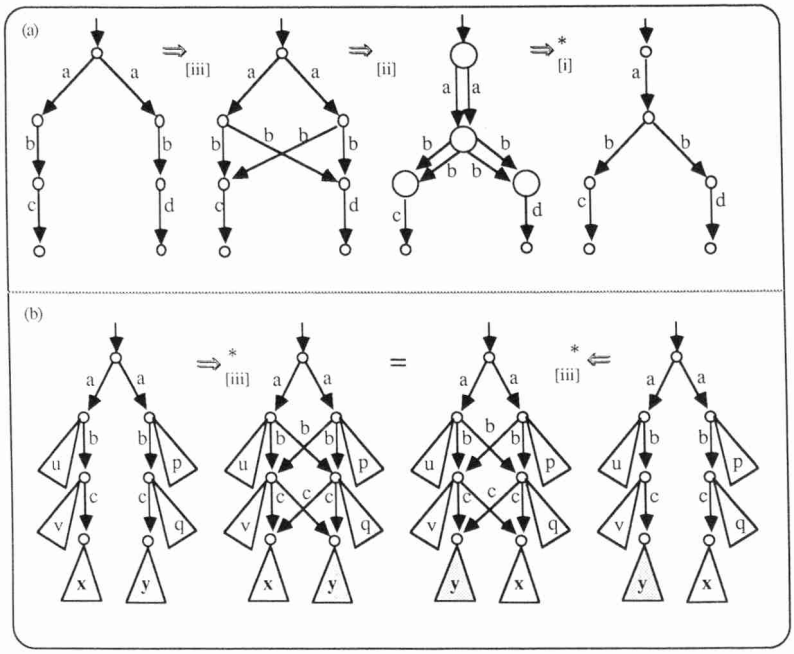


FIG. 9

DEFINITION 3.1.3. (i) A transformation step $g \Rightarrow_{[\mathrm{iii}]} h$ is called *restricted* if g is a process tree (i.e., a process graph without sharing of subgraphs).

(ii) Let $\Leftrightarrow$ be the symmetric closure of $\Rightarrow$. A transformation $g \Leftrightarrow \cdots \Leftrightarrow h$ is restricted if every [iii]-step in the transformation is restricted.

3.2. Connecting process graph equivalences with process graph transformations.

PROPOSITION 3.2.1. *Let $g, h \in H_\delta$. Then we have the following*:

(i) $g \Rightarrow_{[\mathrm{i-iii}]} h$ *implies* $g \equiv_{\mathcal{R}} h$;

(ii) $g \Rightarrow_{[\mathrm{i-iv}]} h$ *implies* $g \equiv_{\mathcal{F}} h$.

Proof. Item (i) follows at once from the definitions.

(ii) We must only prove that the new node s introduced in a fork does not generate new failure pairs (see Fig. 8(b)).

Case 1. Let $(\sigma a, \{b_1, \cdots, b_n\})$ be the ready pair contributed by node t_1, where $n \geqq 1$ and the b_i are not δ. The ready pair of the new node s is $(\sigma a, \{b_1, \cdots, b_n, c_1, \cdots, c_m\})$. Hence the failure pairs contributed by s are among those of t_1.

Case 2. $n = 1$ and $b = \delta$. Then $(\sigma a, \varnothing)$ is the ready pair of t_1 so the failure pairs of t_1 are $[\sigma a, X]$, $X \subseteq A$ and again these cover the failure pairs of s.

Case 3. The cases where $m = 1$, $c_1 = \delta$ are trivial.

So in all cases the *new* failure pairs (of s) were already present as failure pairs of t_1. The part of $\mathcal{F}[\![g]\!]$ that consists of successful traces is invariant. □

We will now prove the reverse implications in Proposition 3.2.1. To this end the *ready normal form* $\mathcal{R}(g)$ and the *failure normal form* $\mathcal{F}(g)$ will be defined. First we define a map γ from the collection of ready sets $\{\mathcal{R}[\![g]\!] \mid g \in \mathbb{H}_\delta\}$ to $\mathbb{H}_\delta$.

DEFINITION 3.2.2. (i) Let $g \in \mathbb{H}_\delta$ have ready set $\mathcal{R}[\![g]\!]$. Then $\gamma(\mathcal{R}[\![g]\!])$ is the process graph with $\mathcal{R}[\![g]\!] \cup \{o\}$ as set of nodes, with $(\varepsilon, X) \in \mathcal{R}[\![g]\!]$ as root, and with edges

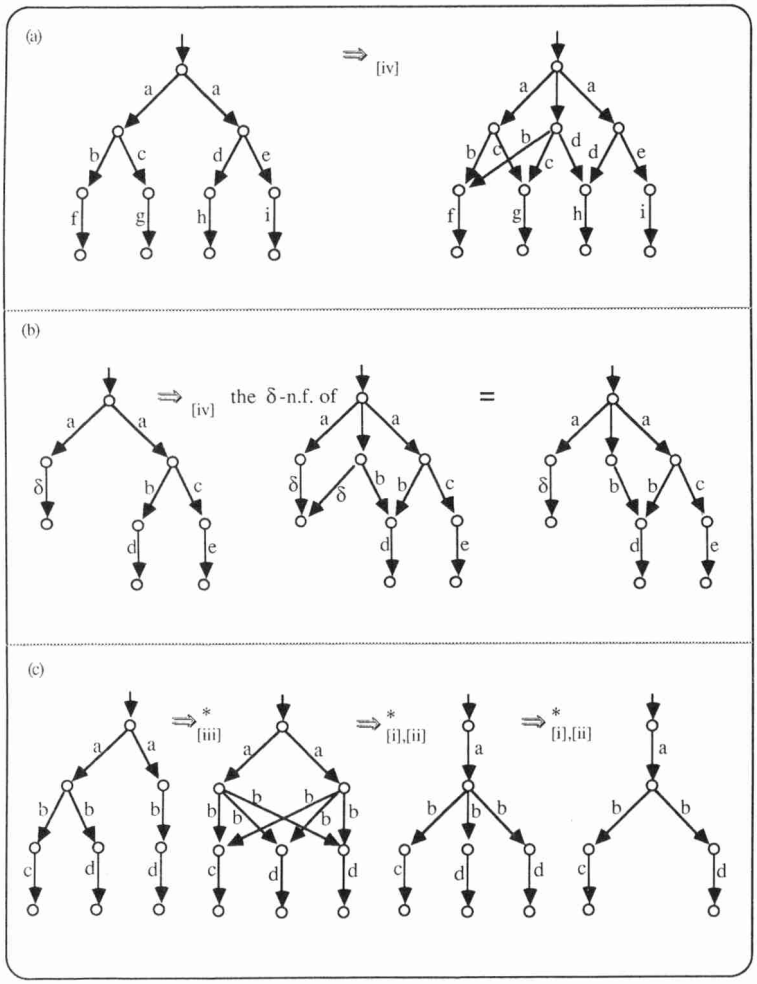


FIG. 10

given by

$$(\sigma, \{a\} \cup X) \xrightarrow{a} (\sigma a, Y),$$

$$(\sigma, \{a\} \cup X) \xrightarrow{a} \sigma a,$$

$$(\sigma, \emptyset) \xrightarrow{\delta} o$$

(whenever the left-hand side, right-hand side $\in \mathcal{R}[\![g]\!] \cup \{o\}$).

(ii) $\mathcal{R}(g) = \gamma(\mathcal{R}[\![g]\!])$ is the *ready normal form* of g.

(iii) The *convex closure* cl $(\mathcal{R}[\![g]\!])$ of $\mathcal{R}[\![g]\!]$ is obtained as the smallest set containing $\mathcal{R}[\![g]\!]$ and satisfying

$$(\sigma, X), (\sigma, Y \cup Z) \in \mathrm{cl}\,(\mathcal{R}[\![g]\!]) \Rightarrow (\sigma, X \cup Y) \in \mathrm{cl}\,(\mathcal{R}[\![g]\!]).$$

(iv) $\mathcal{F}(g) = \gamma(\mathrm{cl}\,(\mathcal{R}[\![g]\!]))$ is the *failure normal form* of g.

Example 3.2.3. Let g be as in Fig. 11(a). Then $\mathcal{R}(g)$, $\mathcal{F}(g)$ are as in Fig. 11(b), 11(c), respectively.

PROPOSITION 3.2.4.

(i) $g \Leftrightarrow^*_{[i-iii]} \mathcal{R}(g)$ via a restricted transformation;

(ii) $g \Leftrightarrow^* \mathcal{F}(g)$ via a restricted transformation;

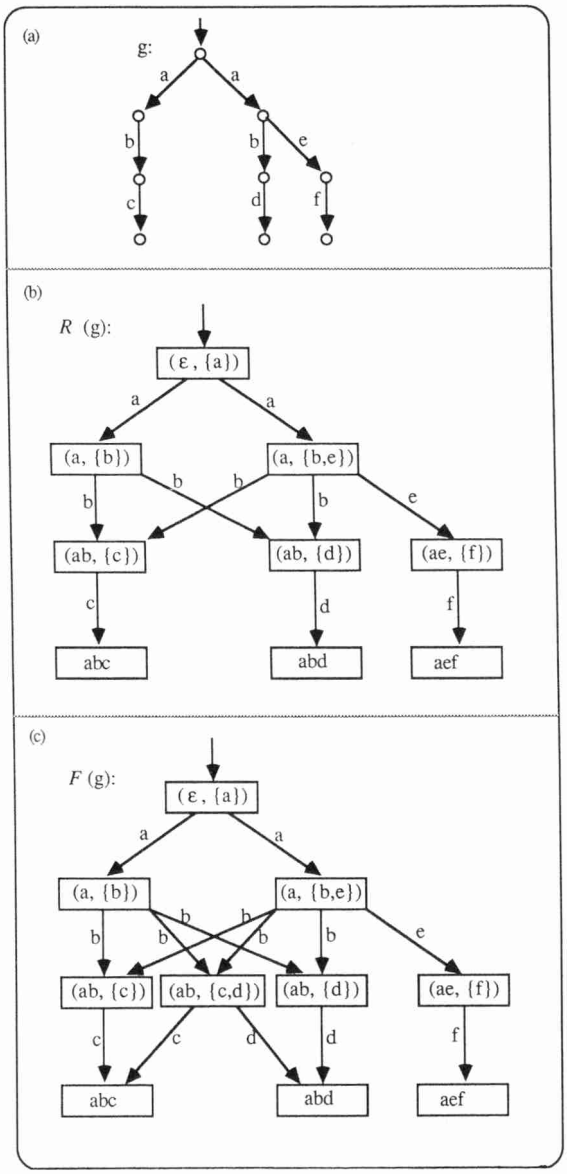


FIG. 11

(iii) $g \equiv_{\mathcal{R}} \mathcal{R}(g)$;
(iv) $g \equiv_{\mathcal{F}} \mathcal{F}(g)$;
(v) $\mathcal{R}(\mathcal{F}(g)) = \mathcal{F}(g)$;
(vi) $g \equiv_{\mathcal{R}} h \Rightarrow \mathcal{R}(g) = \mathcal{R}(h)$;
(vii) $g \equiv_{\mathcal{F}} h \Rightarrow \mathcal{F}(g) = \mathcal{F}(h)$.

Proof. (i) (The following proof was kindly provided to us by R. J. van Glabbeek (personal communication).) Let $g \in \mathbb{H}_\delta$ be given. We will transform g via a restricted transformation to a process graph g^* such that $g^* \leftrightarrows \mathcal{R}(g)$. Since $\leftrightarrows$ coincides with $\Leftrightarrow^*_{[i,ii]}$ (see Corollary 3.2.5(i)) this suffices.

If each node in g has a unique history, g is called *history unambiguous.* So in particular, process trees are history unambiguous. For a history-unambiguous process graph g, the *level* of node s in g is the length in symbols of the history of s. The root of g, therefore, has level 0. We will use the following notation: if s is a node of g, ready(s) is the ready contribution of s to the ready set of g; so ready$(s) = (\sigma, X)$ or σ for some σ, X. If s, t are nodes of g, we write $s \leftrightarrows t$ to indicate that the subgraphs with s, t as roots, respectively, are bisimilar.

The transformation of g to g^* such that $g^* \leftrightarrows \mathcal{R}(g)$ will be done in stages, level by level, starting from the top level (level 0). The induction hypothesis for the transformation is that after the nth stage g $(=g_0)$ is transformed to g_n satisfying the following property $\mathbb{H}_n$: *Suppose p, q are nodes of g_n such that p has level n,* ready$(p) = (\sigma, X \cup \{a\})$ *and* ready$(q) = (\sigma a, Y)$ *or* σa. *Then g_n contains a node r such that $q \leftrightarrows r$ and $p \to_a r$.*

For g_0 we have indeed $\mathbb{H}_0$; p is then the root and for r we just take q. Now suppose g_n is constructed such that $\mathbb{H}_n$ holds. We will construct g_{n+1} such that $\mathbb{H}_{n+1}$ holds. So consider a node p of level $n+1$ in g_n admitting an a-step (see Fig. 12) with ready$(p) = (\sigma b, X \cup \{a\})$, and a node q with ready$(q) = (\sigma ba, Y)$. Hence there is a node p' on level n such that $p' \to_b p$; say ready$(p') = (\sigma, X')$. Also there must be a node q' such that $q' \to_a q$ and, say, ready$(q') = (\sigma b, Z)$. By $\mathbb{H}_n$, therefore, there is a node r' such that $q' \leftrightarrows r'$ and $p' \to_b r'$. By the definition of $\leftrightarrows$, there is a node r such that $r' \to_a r$ and $q \leftrightarrows r$. Now we insert a cross (i.e., two a-steps) as in the figure. The result is unshared by backward application of $\Rightarrow_{[ii]}$ to a process tree. This unsharing does not increase the number of nodes of level $n+1$, and also does not increase the number of nodes of level $n+2$ modulo $\leftrightarrows$. The procedure is repeated for all p of level $n+1$ and equivalence classes $q/\leftrightarrows$. As there are only finitely many such pairs p, $q/\leftrightarrows$ the procedure stops eventually; the resulting tree is g_{n+1}. Clearly g_{n+1} satisfies $\mathbb{H}_{n+1}$. The construction of the sequence $g_0, g_1, \cdots, g_n$ stops when n is equal to the depth of g. The result is called g^*, and we claim that $g^* \leftrightarrows \mathcal{R}(g)$ via the bisimulation that relates nodes s, t in g^*, $\mathcal{R}(g)$, respectively, such that ready(s) = ready(t).

Proof of the Claim. Suppose s, t are nodes in g^*, $\mathcal{R}(g)$, respectively, such that ready(s) = ready$(t) = (s, X \cup \{a\})$. Let $s \to_a s'$. Then take the unique node t' in $\mathcal{R}(g)$ with ready(t') = ready(s'). This must be $(\sigma a, Y)$ or σa. By definition of the edges in $\mathcal{R}(g)$ we have $t \to_a t'$; and indeed $s' \leftrightarrows t'$ because ready(s') = ready(t'). The other side of the bisimulation requirements: Let s, t be as before, and let $t \to_a t'$ with ready$(t') = (\sigma a, Y)$ or σa. Let s^* be a node in g^* such that ready(s^*) = ready(t'). By construction

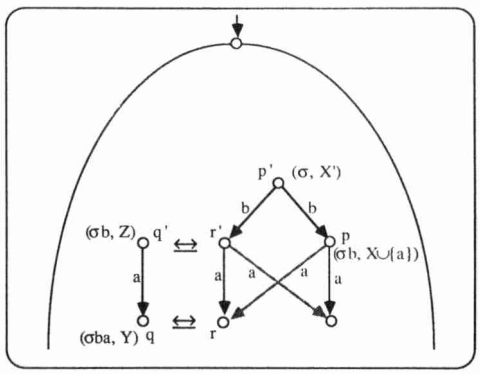


FIG. 12

of g^* there is a node s' in g^* with $s^* \leftrightarrows s'$ and $s \to_a s'$. Clearly, $\text{ready}(s') = \text{ready}(s^*) = \text{ready}(t')$, hence $s' \leftrightarrows t'$.

(ii) Let g be given. According to (i) there is a restricted transformation of g to $\mathcal{R}(g)$. We will transform (via a restricted transformation) $\mathcal{R}(g)$ further into $\mathcal{F}(g)$, as follows. Take nodes (σ, X), $(\sigma, Y \cup Z)$ from $\mathcal{R}(g)$ such that $(\sigma, X \cup Y)$ is not yet a node of $\mathcal{R}(g)$. (If such nodes do not exist then $\mathcal{R}(g)$ is already equal to $\mathcal{F}(g)$.) Now it is easy to see that there are paths in $\mathcal{R}(g)$ from the root to the nodes (σ, X), $(\sigma, Y \cup Z)$ such that these paths coincide in all but their last step, i.e., the paths split up as late as possible. At the split-up node we now insert a fork into $\mathcal{R}(g)$, with central node $(\sigma, X \cup Y)$, which is a new node. Call the result: $\mathcal{R}(g)^+$. Next, $\mathcal{R}(g)^+$ is transformed (according to (i)) to $\mathcal{R}(\mathcal{R}(g)^+)$. Iteration of this procedure, via $\mathcal{R}(\mathcal{R}(g)^+)^+$, $\mathcal{R}(\mathcal{R}(\mathcal{R}(g)^+)^+)$, etc., obviously will stop in $\mathcal{F}(g)$.

Parts (iii) and (iv) are left to the reader.

(v) By Definition 3.2.2, $\mathcal{R}(\mathcal{F}(g)) = \mathcal{F}(g)$ means

$$\gamma(\mathcal{R}[\![\gamma(\text{cl}(\mathcal{R}[\![g]\!]))]\!]) = \gamma(\text{cl}(\mathcal{R}[\![g]\!])),$$

which is equivalent to

$$\mathcal{R}[\![\gamma(\text{cl}(\mathcal{R}[\![g]\!]))]\!] = \text{cl}(\mathcal{R}[\![g]\!]).$$

So we must check that the set of ready pairs of the graph determined by the set of ready pairs $\text{cl}(\mathcal{R}[\![g]\!])$ is just $\text{cl}(\mathcal{R}[\![g]\!])$; this seems obvious.

(vi) $g \equiv_{\mathcal{R}} h$ by definition means $\mathcal{R}[\![g]\!] = \mathcal{R}[\![h]\!]$. Hence $\mathcal{R}(g) = \gamma(\mathcal{R}[\![g]\!]) = \gamma(\mathcal{R}[\![h]\!]) = \mathcal{R}(h)$.

(vii) Suppose $g \equiv_{\mathcal{F}} h$. Then by (iv) $g \equiv_{\mathcal{F}} \mathcal{F}(g)$, $h \equiv_{\mathcal{F}} \mathcal{F}(h)$, so $\mathcal{F}(g) \equiv_{\mathcal{F}} \mathcal{F}(h)$. Since both $\mathcal{F}(g)$, $\mathcal{F}(h)$ are convexly closed, we have $\mathcal{F}(g) \equiv_{\mathcal{R}} \mathcal{F}(h)$ (by Lemma 2.5.5). So (vi) $\mathcal{R}(\mathcal{F}(g)) = \mathcal{R}(\mathcal{F}(h))$. Hence by (v): $\mathcal{F}(g) = \mathcal{F}(h)$. □

COROLLARY 3.2.5. *Let $g, h \in \mathbb{H}_\delta$. Then we have the following*:

(i) $g \leftrightarrows h$ *if and only if* $g \Leftrightarrow^*_{[i],[ii]} h$;

(ii) $g \equiv_{\mathcal{R}} h$ *if and only if* $g \Leftrightarrow^*_{[i-iii]} h$;

(iii) $g \equiv_{\mathcal{F}} h$ *if and only if* $g \Leftrightarrow^* h$.

Proof. Item (i) is (essentially) proved in the Appendix of [BK83] and also in Corollary 2.13 of [BK85]: the proofs there also take τ-steps into account; after leaving out all mention of τ-steps, the result follows.

(ii) The implication from right to left follows from Proposition 3.2.1(i). The other direction follows from Proposition 3.2.4(i), (vi).

(iii) The proof is similar to (ii). □

4. Axiomatising the equivalences on process graphs. We will now use our analysis of $\equiv_{\mathcal{R}}, \equiv_{\mathcal{F}}$ on the graph domain $\mathbb{H}_\delta$ to formulate complete axiom systems for these notions. First this will be done for the signature of $+, \cdot$ alone, later on (in § 4.2) also $\|, \lfloor\!\lfloor, |, \partial_H$ will be taken into account.

4.1. The case without communication. We start with the observation (whose proof is simple and omitted) that $\equiv_{\mathcal{R}}, \equiv_{\mathcal{F}}$ are congruences on $\mathbb{H}_\delta(+, \cdot)$, and hence can be factored out to yield $\mathbb{H}_\delta(+, \cdot)/\equiv_{\mathcal{R}}$ and $\mathbb{H}_\delta(+, \cdot)/\equiv_{\mathcal{F}}$, respectively. These are the structures which we will now axiomatise.

We will prove that the axiom system $\text{BPA}_\delta + \text{R1}, 2 + \text{S}$ in Table 3 is a complete axiomatisation for $\mathbb{H}_\delta(+, \cdot)/\equiv_{\mathcal{F}}$; after leaving out axiom S we have a complete axiomatisation for $\mathbb{H}_\delta(+, \cdot)/\equiv_{\mathcal{R}}$. Here a, b vary over $A \cup \{\delta\}$; x, y, z, u, v are variables

for processes. Note that R2 is not derivable from R1 because in $BPA_\delta + R1, 2 + S$ there is no process x satisfying $bx = b$ when $b \neq \delta$. On the other hand, x should be present in axiom S as the equation

$$a + a(y+z) = a + a(y+z) + ay$$

would yield the failure-inconsistent equation

$$a + ab = a + ab + a\delta.$$

Remark 4.1.1. (i) The axioms R1, 2 and S (R for readiness, S for saturation), which are specific for failure equivalence, appear already in [Br83] in a slightly different form. [Br83] considers also τ-steps and presents as laws valid for failure equivalence in Proposition 1.3.6:

(1) $$\tau(\mu x + u) + \tau(\mu y + v) = \tau(\mu x + \mu y + u) + \tau(\mu x + \mu y + v),$$

(2) $$\mu x + \mu y = \mu(\tau x + \tau y)$$

(here $\mu \in A_\delta \cup \{\tau\}$; x, y, u, v are arbitrary processes), and in Proposition A.3 in [Br83]:

(3) $$\tau x + \tau y = \tau x + \tau y + \tau(x+y),$$

(4) $$\tau x + \tau(x+y+z) = \tau x + \tau(x+y) + \tau(x+y+z).$$

Clearly (1), (2) imply R1 in Table 3; and using the τ-law $x\tau = x$, also valid in failure semantics, we also derive R2. Further, (3), (4) together with (2) yield the pair

$$ax + ay = ax + ay + a(x+y),$$

$$ax + a(x+y+z) = ax + a(x+y) + a(x+y+z)$$

(where $a \in A_\delta$), which is equivalent to axiom S in Table 3.

TABLE 3
$BPA_\delta + R1, 2 + S$

$x + y = y + x$	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
$a(bx+u) + a(by+v) = a(bx+by+u) + a(bx+by+v)$	R1
$a(b+u) + a(by+v) = a(b+by+u) + a(b+by+v)$	R2
$ax + a(y+z) = ax + a(y+z) + a(x+y)$	S

(ii) The axioms R1, 2 and S are also immediate consequences of the proof system of De Nicola and Hennessy [DH84] for strong testing equivalence $\simeq_2$, to be discussed and related with failure equivalence later in Remark 7.3.3. This can be seen as follows:

(1) *Axiom* S in Table 3: $ax + a(y+z) = ax + a(y+z) + a(x+y)$ implies

$$ax + ay = ax + ay + a(x+y)$$

by taking $z = y$; this is (D5) in [DH84]. Further, (S) implies

$$ax + a(x+y+z) = ax + a(x+y+z) + a(x+y)$$

by replacing y in (S) by $x+y$. This is (D6) in [DH84]. Vice versa, (S) follows from (D5), (D6):

$$\begin{aligned} & ax+a(y+z) && \text{(D5)} \\ &= ax+a(y+z)+a(x+y+z) && \text{(D6)} \\ &= ax+a(y+z)+a(x+y+z)+a(x+y) && \text{(D5)} \\ &= ax+a(y+z)+a(x+y). \end{aligned}$$

(2) *Axiom* R1: $a(bx+u)+a(by+v)=a(bx+by+v)+a(bx+by+u)$ is derived from the axiom system in [DH84] as follows:

$$\begin{aligned} & bx+\tau(by+v)=\tau(bx+by+v) && \text{(N3)}, \\ & by+\tau(bx+u)=\tau(bx+by+u) && \text{(N3)}, \\ & bx+by+\tau(by+v)+\tau(bx+u)=\tau(bx+by+v)+\tau(bx+by+u) \\ & bx+\tau(bx+u)=\tau(bx+u) && \text{(D9)}, \\ & by+\tau(by+v)=\tau(by+v) && \text{(D9)}, \\ & \tau(by+v)+\tau(bx+u)=\tau(bx+by+v)+\tau(bx+by+u), \\ & a[\tau(by+v)+\tau(bx+u)]=a[\tau(bx+by+v)+\tau(bx+by+u)], \\ & a(by+v)+a(bx+u)=a(bx+by+v)+a(bx+by+u) && \text{(N1)}. \end{aligned}$$

Here (N1), (N3), and (D9) are axioms in [DH84].

(3) *Axiom* R2: $a(b+u)+a(by+v)=a(b+by+u)+a(b+by+v)$ is not needed in [DH84] because a process b, which first performs action b and then successfully terminates, is not considered there. Note that the process bNIL of [DH84] corresponds to $b\cdot\delta$ and is thus different from b.

4.1.2. Connecting terms with process graphs. Let Ter (BPA_δ) be the set of closed terms in the signature of BPA_δ (=the signature of BPA_δ + R1, 2 + S). We define the following translations:

$$\begin{aligned} &\text{graph:} && \mathrm{Ter}\,(\mathrm{BPA}_\delta)\to\mathbb{H}_\delta, \\ &\text{ter:} && \mathbb{H}_\delta\to\mathrm{Ter}\,(\mathrm{BPA}_\delta). \end{aligned}$$

Here graph (T) is the process graph obtained by first normalizing T with respect to A4, A6, A7 in Table 3 and second by interpreting $a, +, \cdot$ as the corresponding "one-edge graphs" and operators $+, \cdot$ on $\mathbb{H}_\delta$.

Further, to define ter (g) we first define tree (g) as the tree obtained from g by "unsharing." Now we define ter (g) as the term corresponding in the obvious way to tree (g).

Example 4.1.2.1. (i) graph $(a(b+c+d)d+de+ed)=$ graph $(a(bd+cd)+ed)$ is the graph in Fig. 13(a).

(ii) If g is as in Fig. 13(b), then tree (g) is as in Fig. 13(c).

(iii) If g is as in (ii), then ter $(g)=ace+b(de+ab)$.

Remark 4.1.3. Note that ter, graph are "almost" inverse to each other:

$$\mathrm{BPA}_\delta\vdash(\mathrm{ter}\circ\mathrm{graph})(T)=T,$$

$$(\mathrm{graph}\circ\mathrm{ter})(g)\leftrightarrows g$$

where $\leftrightarrows$ (bisimilarity) coincides with $\Leftrightarrow^*_{[i],[ii]}$.

TRANSFER LEMMA 4.1.4 (see diagram). *Let $g, h \in \mathbb{H}_\delta$ be such that $g \Rightarrow h$. In case $\Rightarrow$ is $\Rightarrow_{[iii]}$ we require moreover that g be a process tree. Then*

$$\mathrm{BPA}_\delta + \mathrm{R1}, 2 + \mathrm{S} \vdash \mathrm{ter}(g) = \mathrm{ter}(h).$$

$$\begin{tikzcd} g \arrow[r, Rightarrow] \arrow[d, "ter"'] & h \arrow[d, "ter"] \\ T_1 \arrow[r, equal] & T_2 \end{tikzcd}$$

$$\mathrm{BPA}_\delta + \mathrm{R1},2 + \mathrm{S}$$

Proof. A transformation $g \Rightarrow_{[i]} h$ (removing a double edge) "translates" into some applications of A3: $x + x = x$.

A transformation $g \Rightarrow_{[ii]} h$ is invisible on the level of terms, i.e., ter (g) and ter (h) are identical terms. Next consider a transformation $g \Rightarrow_{[iii]} h$, which consists of adding two edges in g as in Fig. 14. (Note that in this case g is assumed to be a tree.) This translates to an application of R1 if the subtrees x, y are nonempty, and to R2 if one of these subtrees is empty. In case both subtrees x, y are empty we have an application of axiom A3.

Finally, a transformation $g \Rightarrow_{[iv]} h$ (see also Fig. 8) translates into some applications of axiom S in Table 3. □

THEOREM 4.1.5. (i) $\mathrm{BPA}_\delta + \mathrm{R1}, 2 \vdash T_1 = T_2 \Leftrightarrow \mathrm{graph}(T_1) \equiv_{\mathcal{R}} \mathrm{graph}(T_2)$.

(ii) $\mathrm{BPA}_\delta + \mathrm{R1}, 2 + \mathrm{S} \vdash T_1 = T_2 \Leftrightarrow \mathrm{graph}(T_1) \equiv_{\mathcal{F}} \mathrm{graph}(T_2)$.

Proof. We prove (ii); the proof of (i) is similar.

Checking the soundness ($\Rightarrow$) is routine and will not be done here. As to the completeness ($\Leftarrow$): suppose graph $(T_1) \equiv_{\mathcal{F}}$ graph (T_2). Then by Proposition 3.2.4(ii), (vii): graph $(T_1) \Leftrightarrow^*$ graph (T_2) via a restricted transformation. Now by the Transfer Lemma 4.1.4 we have

$$\mathrm{BPA}_\delta + \mathrm{R1}, 2 + \mathrm{S} \vdash (\mathrm{ter} \circ \mathrm{graph})(T_1) = (\mathrm{ter} \circ \mathrm{graph})(T_2)$$

and by Remark 4.1.3:

$$\mathrm{BPA}_\delta + \mathrm{R1}, 2 + \mathrm{S} \vdash T_1 = T_2. \qquad \square$$

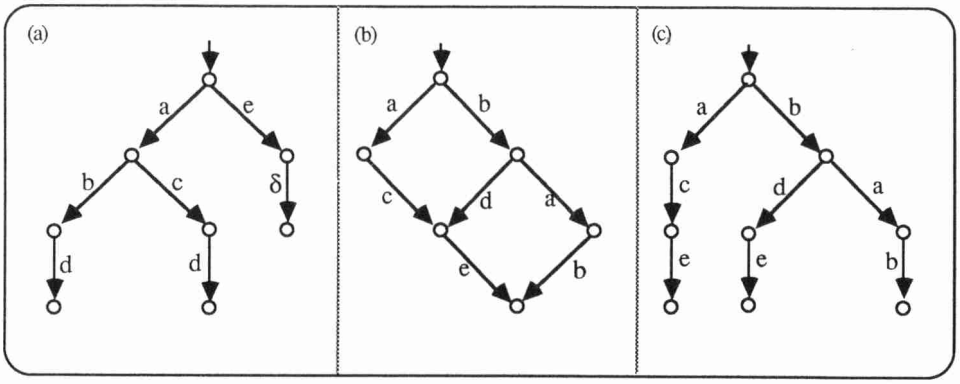


FIG. 13

Notation 4.1.6. (i) If (Σ, E) is a specification (sometimes only written as E if the signature Σ is clear), then $I(\Sigma, E)$ is its initial algebra.

(ii) $\cong$ denotes isomorphism between algebras.

COROLLARY 4.1.7. (i) $\mathbb{H}_\delta(+, \cdot, a, \delta)/\equiv_{\mathcal{R}} \cong I(\mathrm{BPA}_\delta + \mathrm{R1}, 2)$.

(ii) $\mathbb{H}_\delta(+, \cdot, a, \delta)/\equiv_{\mathcal{F}} \cong I(\mathrm{BPA}_\delta + \mathrm{R1}, 2 + \mathrm{S})$. □

4.2. The case with communication: the graph model of ACP_r. Finally we will prove the results above in the presence of communication. The operators $\|, \lfloor\!\lfloor, \cdot, |, \partial_H, a_H (a \in A)$ on $\mathbb{H}_\delta$ were already introduced in § 1.2. They are the semantical counterparts of the same operators in the axiom system ACP_r, as in the upper part of Table 4, which presents the axiom system $\mathrm{ACP}_r + \mathrm{R1}, 2 + \mathrm{S}$, and which extends our earlier axiom system $\mathrm{BPA}_\delta + \mathrm{R1}, 2 + \mathrm{S}$ in Table 3.

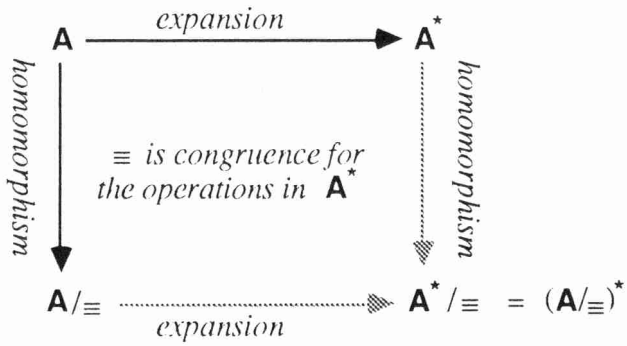
As before, in Table 4 a, b, c vary over $A \cup \{\delta\}$, and x, y, z, u, v vary over processes.

We want to prove that the initial algebra of $\mathrm{ACP}_r + \mathrm{R1}, 2 + \mathrm{S}$ is isomorphic to the model of finite acyclic graphs modulo failure equivalence $\equiv_{\mathcal{F}}$, called the *graph model* for $\mathrm{ACP}_r + \mathrm{R1}, 2 + \mathrm{S}$. To this end we have first to prove that $\equiv_{\mathcal{F}}$ is a *congruence* with respect to also the new operators. Once we have this, and knowing from [BK85], [BK86a] (after leaving out all reference to τ-steps) that there is the isomorphism

$$I(\mathrm{ACP}_r) \cong \mathbb{H}_\delta(+, \cdot, \|, \lfloor\!\lfloor, \cdot, |, \partial_H, a_H, a, \delta)/\leftrightarrows$$

where $\leftrightarrows$ is bisimulation (which coincides with $\Leftrightarrow^*_{[i],[ii]}$; Corollary 3.2.5(i)), the derived isomorphism is a consequence from some general facts which we will state now.

4.2.1. General intermezzo. Let $\mathbf{A}$ be an algebra that on the one hand can be expanded to $\mathbf{A}^*$ (i.e., enriched with new functions; the domain is invariant) and on the other hand can be factored out via $\equiv$, a congruence on $\mathbf{A}$, to $\mathbf{A}/\equiv$. Suppose moreover that $\equiv$ is also a congruence on $\mathbf{A}^*$. (See the following diagram.)



Then this expansion and factorisation are compatible (or commuting): $\mathbf{A}^*/\equiv$ equals $(\mathbf{A}/\equiv)^*$. Now let $\mathbf{A}, \mathbf{A}^*, \mathbf{A}/\equiv$ be isomorphic respectively to the initial algebras of the equational specifications (Σ, E), $(\Sigma \cup \Delta, E \cup D)$, $(\Sigma, E \cup F)$. Then it follows that $(\Sigma \cup \Delta, E \cup D)$ is

(1) a conservative extension of the "base" specification (Σ, E) (i.e., no new identities between closed terms in the base signature Σ are provable from $(\Sigma \cup \Delta, E \cup D)$), and

(2) moreover, the extra operators in Δ can be *eliminated*:

$$\begin{array}{ccc} (\Sigma, E) & \xrightarrow{\text{conservative extension with elimination property}} & (\Sigma \cup \Delta, E \cup D) \\ \downarrow & & \\ (\Sigma, E \cup F). & & \end{array}$$

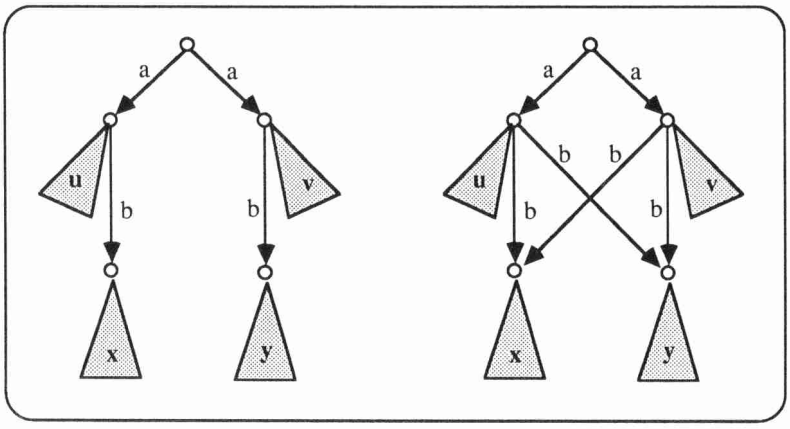


FIG. 14

TABLE 4
$ACP_r + R1, 2 + S$

$x+y=y+x$	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
$a\mid b=b\mid a$	C1
$(a\mid b)\mid c=a(b\mid c)$	C2
$\delta\mid a=\delta$	C3
$x\parallel y=x\mathbin{\lfloor\!\lfloor} y+y\mathbin{\lfloor\!\lfloor} x+x\mid y$	CM1
$a\mathbin{\lfloor\!\lfloor} x=ax$	CM2
$ax\mathbin{\lfloor\!\lfloor} y=a(x\parallel y)$	CM3
$(x+y)\mathbin{\lfloor\!\lfloor} z=x\mathbin{\lfloor\!\lfloor} z+y\mathbin{\lfloor\!\lfloor} z$	CM4
$ax\mid b=(a\mid b)x$	CM5
$a\mid bx=(a\mid b)x$	CM6
$ax\mid by=(a\mid b)(x\parallel y)$	CM7
$(x+y)\mid z=x\mid z+y\mid z$	CM8
$x\mid(y+z)=x\mid y+x\mid z$	CM9
$\partial_H(a)=a \quad \text{if } a\notin H$	D1
$\partial_H(a)=\delta \quad \text{if } a\in H$	D2
$\partial_H(x+y)=\partial_H(x)+\partial_H(y)$	D3
$\partial_H(xy)=\partial_H(x)\cdot\partial_H(y)$	D4
$a_H(b)=b \quad \text{if } b\notin H$	RN1
$a_H(b)=a \quad \text{if } b\in H$	RN2
$a_H(x+y)=a_H(x)+a_H(y)$	RN3
$a_H(xy)=a_H(x)\cdot a_H(y)$	RN4
$a(bx+u)+a(by+v)=a(bx+by+u)+a(bx+by+v)$	R1
$a(b+u)+a(by+v)=a(b+by+u)+a(b+by+v)$	R2
$ax+a(y+z)=ax+a(y+z)+a(x+y)$	S

Furthermore (and this is what we are interested in) we may conclude from the given isomorphisms that

$$\mathbf{A}^*/\equiv\,=(\mathbf{A}/\equiv)^*\cong I(\Sigma\cup\Delta, E\cup D\cup F)$$

where the last algebra is the initial algebra of the *union* of $(\Sigma, E \cup F)$ and $(\Sigma \cup \Delta, E \cup D)$.

(In the statement of the next theorem, as well as in its proof and Table 5, we have suppressed mention of the constants a, δ in, e.g., $\mathbb{H}_\delta(+, \cdot)$, which actually should read $\mathbb{H}_\delta(+, \cdot, a, \delta)(a \in A)$.)

THEOREM 4.2.2. *Let the initial algebras $I(\mathrm{BPA})_\delta)$ etc. as in Table* 5(ii) *of the axiom systems* BPA_δ *etc. as in Table* 5(i) *be given. Furthermore, consider the graph models* $\mathbb{H}_\delta(+, \cdot)/\leftrightarrows$ *etc. as in Table* 5(iii).

Then corresponding initial models and graph models are isomorphic. In particular:

$$I(\mathrm{ACP}_r + \mathrm{R1}, 2 + \mathrm{S}) \cong \mathbb{H}_\delta(+, \cdot, \|, \lfloor\!\lfloor, |, \partial_H, a_H)/\equiv_{\mathcal{F}}.$$

Proof. Consider, for example,

$$\begin{array}{ccc} \mathrm{BPA}_\delta & \longrightarrow & \mathrm{ACP}_r \\ \downarrow & & \\ \mathrm{BPA}_\delta + \mathrm{R1}, 2 + \mathrm{S} & & \end{array}$$

and the corresponding initial algebras

$$\begin{array}{ccc} I(\mathrm{BPA}_\delta) & \longrightarrow & I(\mathrm{ACP}_r) \\ \downarrow & & \\ I(\mathrm{BPA}_\delta + \mathrm{R1}, 2 + \mathrm{S}) & & \end{array}$$

and furthermore (by position in the diagram in Table 5) the corresponding graph models

$$\begin{array}{ccc} \mathbb{H}_\delta(+, \cdot)/\leftrightarrows & \xrightarrow{\exp} & \mathbb{H}_\delta(+, \cdot, \|, \lfloor\!\lfloor, |, \partial_H, a_H)/\leftrightarrows \\ \downarrow \mathrm{hom} & & \\ \mathbb{H}_\delta(+, \cdot)/\equiv_{\mathcal{F}} & & \end{array}$$

By Corollary 4.1.7(ii) we have $I(\mathrm{BPA}_\delta + \mathrm{R1}, 2 + \mathrm{S}) \cong \mathbb{H}_\delta(+, \cdot)/\equiv_{\mathcal{F}}$, and by results in [BK85], [BK86a], [BK86b] we have $I(\mathrm{BPA}_\delta) \cong \mathbb{H}_\delta(+, \cdot)/\leftrightarrows$ and $I(\mathrm{ACP}_r) \cong \mathbb{H}_\delta(+, \cdot, \|, \lfloor\!\lfloor, |, \partial_H, a_H)/\leftrightarrows$.

Therefore, by 4.2.1, it suffices to prove that $\equiv_{\mathcal{F}}$ is a congruence with respect to the "new" operators on $\mathbb{H}_\delta$ in order to conclude that

$$I(\mathrm{ACP}_r + \mathrm{R1}, 2 + \mathrm{S}) \cong \mathbb{H}_\delta(+, \cdot, \|, \lfloor\!\lfloor, |, \partial_H, a_H)/\equiv_{\mathcal{F}}.$$

This is proved in the next proposition. □

PROPOSITION 4.2.3. (i) *Failure equivalence is a congruence with respect to the operators* $\|, \lfloor\!\lfloor, |, \partial_H, a_H$ *on* $\mathbb{H}_\delta$.

(ii) *The same holds for ready equivalence.*

Proof. (i) We consider some typical cases.

The case of ∂_H. To prove $g \equiv_{\mathcal{F}} h \Rightarrow \partial_H(g) \equiv_{\mathcal{F}} \partial_H(h)$. By Corollary 3.2.5 it suffices to check that $g \Rightarrow h$ implies $\partial_H(g) \equiv_{\mathcal{F}} \partial_H(h)$. The cases that $\Rightarrow$ is $\Rightarrow_{[i]}$ or $\Rightarrow_{[ii]}$ present no problem. As to $\Rightarrow_{[iii]}$: it is easy to verify that

$$g \Rightarrow_{[iii]} h \quad \text{implies } \partial_H(g) = \partial_H(h) \quad \text{or} \quad \partial_H(g) \Rightarrow_{[iii]} \partial_H(h).$$

As to $\Rightarrow_{[iv]}$, as in the previous case, the effect of ∂_H (renaming some atoms in g, h into δ and δ-normalising the resulting graphs again) is such that either the "same" fork can be inserted or $\partial_H(g) = \partial_H(h)$.

TABLE 5

(i)

$$\begin{array}{ccc} \mathrm{BPA}_\delta & \longrightarrow & \mathrm{ACP}_r \\ \downarrow & & \downarrow \\ \mathrm{BPA}_\delta + \mathrm{R1}, 2 & \longrightarrow & \mathrm{ACP}_r + \mathrm{R1}, 2 \\ \downarrow & & \downarrow \\ \mathrm{BPA}_\delta + \mathrm{R1}, 2 + \mathrm{S} & \longrightarrow & \mathrm{ACP}_r + \mathrm{R1}, 2 + \mathrm{S} \end{array}$$

(ii)

$$\begin{array}{ccc} I(\mathrm{BPA}_\delta) & \xrightarrow{\exp} & I(\mathrm{ACP}_r) \\ \downarrow \mathrm{hom} & & \downarrow \mathrm{hom} \\ I(\mathrm{BPA}_\delta + \mathrm{R1}, 2) & \xrightarrow{\exp} & I(\mathrm{ACP}_r + \mathrm{R1}, 2) \\ \downarrow \mathrm{hom} & & \downarrow \mathrm{hom} \\ I(\mathrm{BPA}_\delta + \mathrm{R1}, 2 + \mathrm{S}) & \xrightarrow{\exp} & I(\mathrm{ACP}_r + \mathrm{R1}, 2 + \mathrm{S}) \end{array}$$

(iii)

$$\begin{array}{ccc} \mathbb{H}_\delta(+, \cdot)/\leftrightarrows & \xrightarrow{\exp} & \mathbb{H}_\delta(+, \cdot, \|, \lfloor\!\lfloor, |, \partial_H, a_H)/\leftrightarrows \\ \downarrow \mathrm{hom} & & \downarrow \mathrm{hom} \\ \mathbb{H}_\delta(+, \cdot)/\equiv_{\mathcal{R}} & \xrightarrow{\exp} & \mathbb{H}_\delta(+, \cdot, \|, \lfloor\!\lfloor, |, \partial_H, a_H)/\equiv_{\mathcal{R}} \\ \downarrow \mathrm{hom} & & \downarrow \mathrm{hom} \\ \mathbb{H}_\delta(+, \cdot)/\equiv_{\mathcal{F}} & \xrightarrow{\exp} & \mathbb{H}_\delta(+, \cdot, \|, \lfloor\!\lfloor, |, \partial_H, a_H)/\equiv_{\mathcal{F}} \end{array}$$

(Note here that it is crucial that process graphs g, h as in Fig. 15 are not failure equivalent, since $\partial_{\{b\}}$ would yield a trace $a\delta$ in h but not in g.)

The case of $\|$. It suffices to prove

$$g \Rightarrow g' \quad \text{implies } g \| h \equiv_{\mathcal{F}} g' \| h.$$

As above, only the cases [iii], [iv] (cross and fork, respectively) are of interest. In fact we will prove the following:

(1) $g \Rightarrow_{[\mathrm{iii}]} g'$ implies $g \| h \Rightarrow_{[\mathrm{iii}]} g' \| h$.

(2) $g \Rightarrow_{[\mathrm{iv}]} g'$ implies $g \| h \equiv_{\mathcal{F}} g' \| h$.

Proof of (1). Due to the construction of a merge as a Cartesian product with diagonal edges for communications (Fig. 16), it is "geometrically" clear (see Fig. 17) that inserting a cross in g amounts to inserting several crosses (also possibly diagonal ones, depending on the communication function) in the merge $g \| h$. So $g \| h \Rightarrow_{[\mathrm{iii}]} g' \| h$. (It is not hard to see that the condition on histories, which is stated in the definition

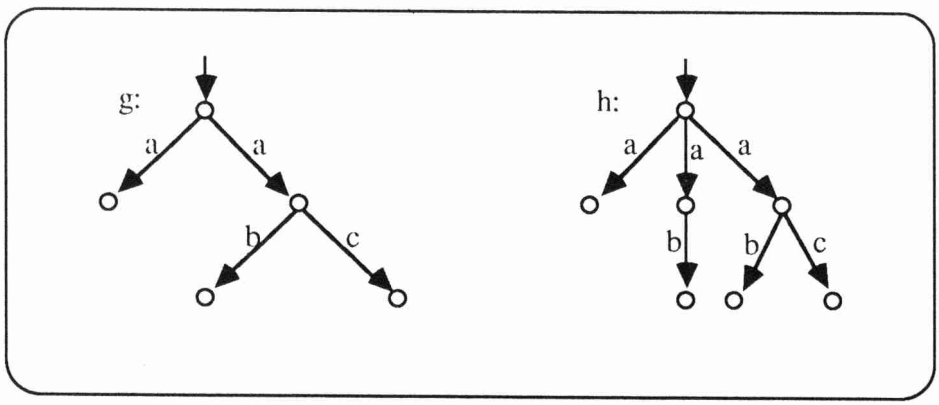


FIG. 15

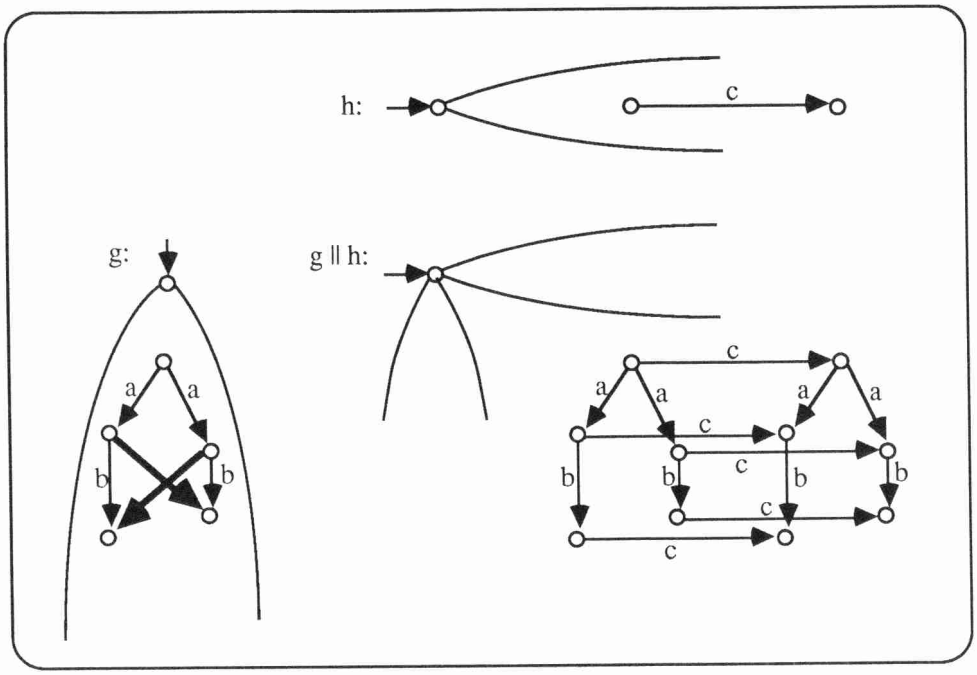


FIG. 16

of $\Rightarrow_{[iii]}$, stays satisfied in such a way that insertion of these crosses in $g \| h$ is indeed legitimate.)

Proof of (2). Under the assumption $g \Rightarrow_{[iv]} g'$ we now prove $g \| h \equiv_{\mathcal{F}} g' \| h$ directly from the definition $\equiv_{\mathcal{F}}$. So consider the addition in g of a fork that connects all successors of s_1 (see Fig. 18) to some of those of s_3. That is, the failure pairs contributed by the new node s_2 are contained in those of s_1. Then we must check that the new

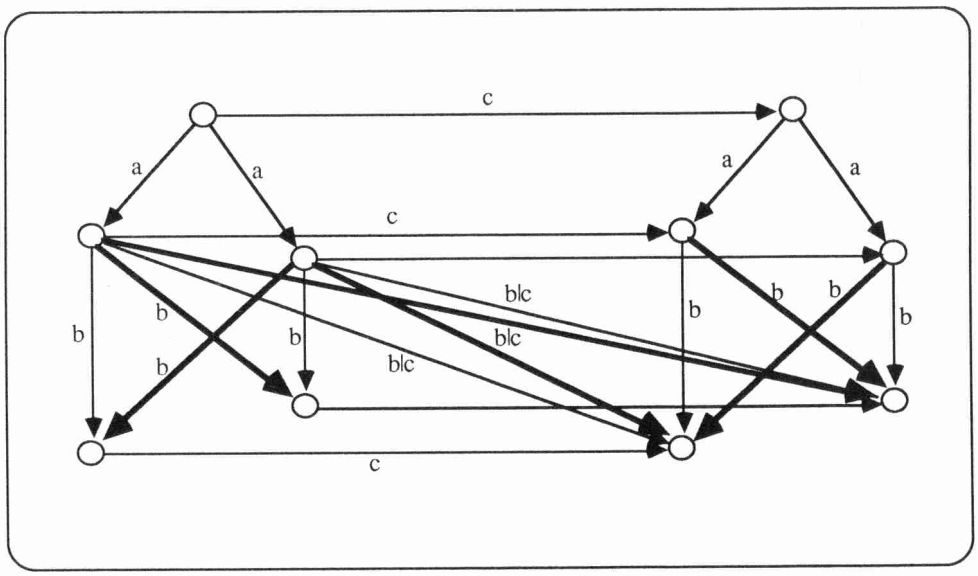


FIG. 17

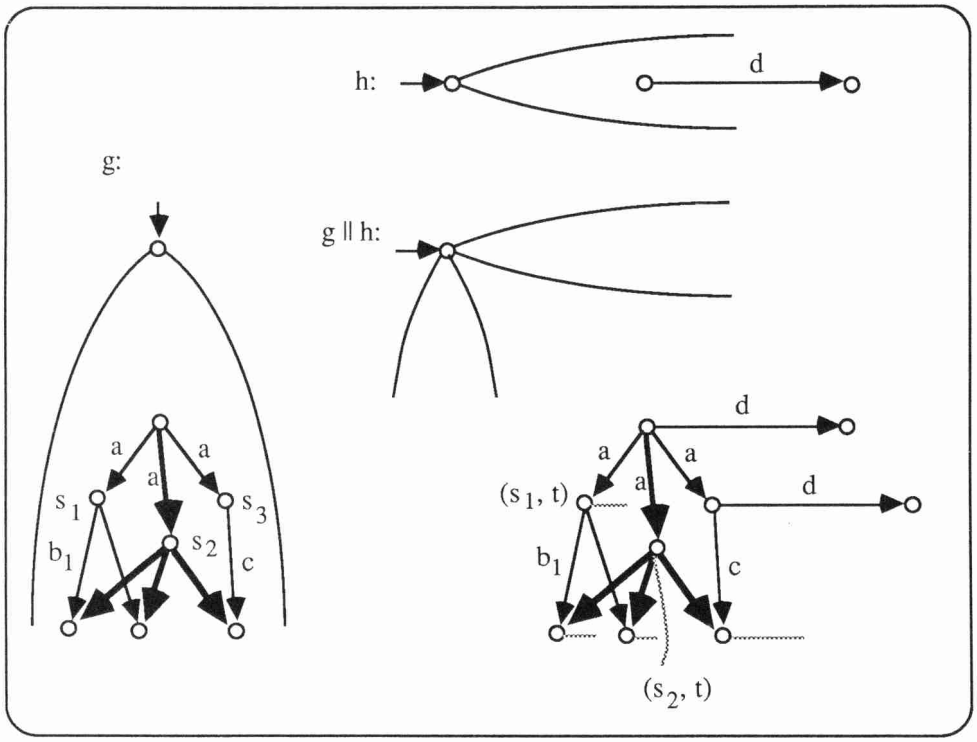


FIG. 18

nodes (s_2, t) in $g' \| h$ caused by this addition, contribute no new failure pairs. It is not hard to check that indeed the failure pairs of (s_2, t) are contained in those of (s_2, t) by some consideration of the outgoing edges of (s_1, t) and (s_2, t). The precise verification is omitted here.

The proof of part (ii) of the proposition is as for (i)—but simpler. It is omitted here. □

5. The failure model of ACP$_r$. In the previous sections the notion of failure equivalence was introduced for the process graph domain $\mathbb{H}_\delta$, and it was shown to be a congruence with respect to the operators of ACP$_r$ in $\mathbb{H}_\delta$. The quotient $\mathbb{H}_\delta / \equiv_{\mathcal{F}}$ was shown to be a model of ACP$_r$, called the graph model of ACP$_r$. Furthermore, a complete axiomatisation ACP$_r$+R1, 2+S was given for $\equiv_{\mathcal{F}}$ in the sense of

$$I(\mathrm{ACP}_r + R1, 2 + S) \cong \mathbb{H}_\delta / \equiv_{\mathcal{F}}.$$

Here $\mathbb{H}_\delta / \equiv_{\mathcal{F}}$ is short for $\mathbb{H}_\delta(+, \cdot, \|, \lfloor\!\lfloor, |, \partial_H, a_H, a, \delta) / \equiv_{\mathcal{F}}$. In this section we will provide an *explicit representation* of the quotient structure $\mathbb{H}_\delta(+, \cdot, \|, \mathbb{L}, |, \partial_H, a_H, a, \delta) / \equiv_{\mathcal{F}}$, called the *failure model* of ACP$_r$. The model will shed more light into the structure of failures, and—in connection with § 6.2—it will link our definitions with the original work on failures in [BHR84].

5.1. The domain $\mathbb{F}$ of failure sets. First we introduce the domain of failure sets, denoted by $\mathbb{F}$. It consists of all finite subsets

$$F \subseteq A^+ \cup (A^* \times \mathcal{P}(A))$$

(where A^* is the set of finite words over A, A^+ is the set of nonempty finite words

over A, and $\mathcal{P}(A)$ is the power set of A) which satisfy the following closure properties:

(i) $[\varepsilon, \emptyset] \in F$;

(ii) $[\sigma_1\sigma_2, \emptyset] \in F \Rightarrow [\sigma_1, \emptyset] \in F$;

(iii) $X \subseteq Y$ and $[\sigma, Y] \in F \Rightarrow [\sigma, X] \in F$;

(iv) $[\sigma, X] \in F$ and $[\sigma, X \cup \{a\}] \notin F \Rightarrow \sigma a \in F$ or $[\sigma a, \emptyset] \in F$;

(v) $\sigma a \in F \Rightarrow [\sigma, \emptyset] \in F$;

(vi) $[\varepsilon, X] \in F \,\&\, a \in X \Rightarrow [a, \emptyset] \notin F$.

The conditions (i)-(iv) on failure sets are exactly as in [BHR84]. Condition (v) deals with traces $\sigma \in A^+$ which allow a direct definition of sequential composition without using (and later hiding again) an extra action $\surd$ coding the event of successful termination as in [BHR84]. In § 6.2 on CSP we will restrict ourselves to CSP without successful termination. Then this difference is irrelevant. Condition (vi) is needed because we do not consider τ-steps and hence no initial nondeterminism.

5.2. Operations on failure sets. Now we define the constants δ, $a (a \in A)$ and the operations $+, \cdot, \|, \lfloor\!\lfloor, \partial_H, a_H$ of ACP_r directly on $\mathbb{F}$. For $F, G \in \mathbb{F}$ we put the following:

(i) $\delta = \{[\varepsilon, X] \mid X \subseteq A\}$.

(ii) $a = \{[a, X] \mid X \subseteq A - \{a\}\} \cup \{a\}$.

Initially "a" can refuse anything except "a." After "a" has occurred, the process successfully terminates.

(iii) $$\begin{aligned} F + G = \{&[\varepsilon, X] \mid [\varepsilon, X] \in F \cap G\} \\ &\cup \{\sigma \mid \sigma \in F \cup G\} \\ &\cup \{[\sigma, X] \mid \sigma \neq \varepsilon \wedge [\sigma, X] \in F \cup G\}. \\ &\cup \{\sigma \mid \sigma \in F \cup G\} \\ &\cup \{[\sigma, X] \mid \sigma \neq \varepsilon \wedge [\sigma, X] \in F \cup G\}. \end{aligned}$$

In its first step $F + G$ can refuse only those actions which can be refused by both F and G. In all subsequent steps $F + G$ behaves as $F \cup G$.

(iv) $$\begin{aligned} F \cdot G = \{&[\sigma, X] \mid [\sigma, X] \in F\} \\ &\cup \{\sigma_1\sigma_2 \mid \sigma_1 \in F \wedge \sigma_2 \in G\} \\ &\cup \{[\sigma_1\sigma_2, X] \mid \sigma_1 \in F \wedge [\sigma_2, X] \in G\}. \end{aligned}$$

$F \cdot G$ first behaves like F and after successful termination of F in a trace σ_1 continues to behave as G.

(v) (1) $$\begin{aligned} F \| G = \{&\sigma \mid \exists \sigma_1 \in F, \sigma_2 \in G\colon \sigma \in \sigma_1 \| \sigma_2\} \\ &\cup \{[\sigma, X] \mid \exists [\sigma_1, X_1] \in F, [\sigma_2, X_2] \in G\colon \sigma \in \sigma_1 \| \sigma_2 \\ &\qquad \wedge X \subseteq (X_1 \cap X_2) - \{(a \mid b) \mid a \notin X_1 \wedge b \notin X_2\}\} \end{aligned}$$

(2) $$\cup \{[\sigma, X] \mid \exists \sigma_1 \in F, [\sigma_2, X_2] \in G\colon \sigma \in \sigma_1 \| \sigma_2 \wedge X = X_2\}$$

(3) $$\cup \{[\sigma, X] \mid \exists [\sigma_1, X_1] \in F, \sigma_2 \in G\colon \sigma \in \sigma_1 \| \sigma_2 \wedge X = X_1\}$$

where $\sigma_1 \| \sigma_2$ is the set of traces in A^* defined inductively by

$$\varepsilon \| \sigma = \sigma \| \varepsilon = \{\sigma\},$$

$$a\sigma_1 \| b\sigma_2 = a \cdot (\sigma_1 \| b\sigma_2) \cup b \cdot (a\sigma_1 \| \sigma_2) \cup [a \mid b] \cdot (\sigma_1 \| \sigma_2)$$

with $[a \mid b] = \{(a \mid b)\}$ if $a \mid b \neq \delta$ and $\emptyset$ if $a \mid b = \delta$.

Thus $\sigma_1 \| \sigma_2$ is the set of successful traces obtained by merging and communicating between σ_1 and σ_2. For all traces $\sigma_1 \in F$ and $\sigma_2 \in G$ this set is included in $F \| G$ (clause (1)). Besides traces $F \| G$ contains certain failure pairs $[\sigma, X]$. If either F or G have already terminated, X is just the refusal set of the other, not-yet-terminated component G or F (clauses (3) and

(4)). If neither F nor G have terminated, X contains only actions that both F and G can refuse. This suggests $X \subseteq X_1 \cap X_2$, where X_1 and X_2 are the refusal sets of F and G. However, $F \| G$ cannot refuse the possible communications between F and G. These communications can only be of the form $(a|b)$ with $a \notin X_1$ and $b \notin X_2$. This explains the condition

$$X \subseteq X_1 \cap X_2 - \{(a|b) \mid a \notin X_1 \wedge b \notin X_2\}$$

for the refusal set X of $F \| G$ (clause (2)). Note that in case of $(a|b) = \delta$ nothing is deduced from $X_1 \cap X_2$.

Clearly, $F \lfloor\!\lfloor G$ and $F | G$ are just variations of $F \| G$ differing only in their first actions.

(vi) $F \lfloor\!\lfloor G = \{\sigma \mid \exists \sigma_1 \in F, \sigma_2 \in G\colon \sigma \in \sigma_1 \lfloor\!\lfloor \sigma_2\}$

$$\begin{aligned}
&\cup \{[\varepsilon, X] \mid [\varepsilon, X] \in F\} \\
&\cup \{[\sigma, X] \mid \sigma \neq \varepsilon \wedge \exists [\sigma_1, X_1] \in F, [\sigma_2, X_2] \in G\colon \sigma \in \sigma_1 \lfloor\!\lfloor \sigma_2 \\
&\qquad \wedge X \subseteq (X_1 \cap X_2) - \{(a|b) \mid a \notin X_1 \wedge b \notin X_2\}\} \\
&\cup \{[\sigma, X] \mid \sigma \neq \varepsilon \wedge \exists \sigma_1 \in F, [\sigma_2, X_2] \in G\colon \sigma \in \sigma_1 \lfloor\!\lfloor \sigma_2 \wedge X = X_2\} \\
&\cup \{[\sigma, X] \mid \sigma \neq \varepsilon \wedge \exists [\sigma_1, X_1] \in F, \sigma_2 \in G\colon \sigma \in \sigma_1 \lfloor\!\lfloor \sigma_2 \wedge X = X_1\}
\end{aligned}$$

where $\sigma_1 \lfloor\!\lfloor \sigma_2$ is the set of traces in A^* defined inductively by

$$\begin{aligned}
&\varepsilon \lfloor\!\lfloor \sigma = \varnothing, \\
&a\sigma_1 \lfloor\!\lfloor \sigma_2 = a \cdot (\sigma_1 \| \sigma_2).
\end{aligned}$$

Until the completion of its first communication $F \lfloor\!\lfloor G$ behaves as F. This explains why $F \lfloor\!\lfloor G$ inherits all initial failure pairs $[\varepsilon, X]$ of F. Afterwards $F \lfloor\!\lfloor G$ behaves as $F \| G$.

(vii) $F | G = \{\sigma \mid \exists \sigma_1 \in F, \sigma_2 \in G\colon \sigma \in \sigma_1 | \sigma_2\}$

$$\begin{aligned}
&\cup \{[\varepsilon, X] \mid \exists [\varepsilon, X_1] \in F, [\varepsilon, X_2] \in G\colon X \subseteq A \\
&\qquad - \{(a|b) \mid a \notin X_1 \wedge b \notin X_2\}\} \\
&\cup \{[\sigma, X] \mid \sigma \neq \varepsilon \wedge \exists [\sigma_1, X_1] \in F, [\sigma_2, X_2] \in G\colon \sigma \in \sigma_1 | \sigma_2 \\
&\qquad \wedge X \subseteq (X_1 \cap X_2) - \{(a|b) \mid a \in X_1 \wedge b \in X_2\}\} \\
&\cup \{[\sigma, X] \mid \sigma \neq \varepsilon \wedge \exists \sigma_1 \in F, [\sigma_2, X_2] \in G\colon \sigma \in \sigma_1 | \sigma_2 \wedge X = X_2\} \\
&\cup \{[\sigma, X] \mid \sigma \neq \varepsilon \wedge \exists [\sigma_1, X_1] \in F, \sigma_2 \in G\colon \sigma \in \sigma_1 | \sigma_2 \wedge X = X_1\}
\end{aligned}$$

where $\sigma_1 | \sigma_2$ is the set of traces in A^* defined inductively by

$$\begin{aligned}
&\varepsilon | \sigma_2 = \sigma_1 | \varepsilon = \varnothing, \\
&a\sigma_1 | b\sigma_2 = [a|b] \cdot (\sigma_1 \| \sigma_2).
\end{aligned}$$

In its first step $F | G$ requires a communication between F and G. Here initially $F | G$ can refuse every set X of actions not containing possible communications between F and G. This explains the condition

$$X \subseteq A - \{(a|b) \mid a \notin X_1 \wedge b \notin X_2\}$$

for the failure pairs $[\varepsilon, X]$. After its first step $F | G$ behaves like $F \| G$.

(viii) $\partial_H(F) = \{\sigma \mid \sigma \in F$ does not contain any $a \in H\}$

$\cup \{[\sigma, X \cup Y] \mid [\sigma, X] \in F$, s does not contain any $a \in H$, and $Y \subseteq H\}$.

In $\partial_H(F)$ only those traces that do not contain any $a \in H$ are successful, and the actions in H can be refused at any moment.

(ix) $a_H(F) = \{a_H(\sigma) \mid \sigma \in F$

$\cup \{[a_H(\sigma), X] \mid a \in X \wedge [\sigma, X \cup H] \in F\}$

$\cup \{[a_H(\sigma), X] \mid a \notin X \wedge [\sigma, X - H] \in F\}$

where the renaming operator a_H is applied pointwise to the elements in σ. A set X can be refused by $a_H(F)$ if $a_H^{-1}(X) = \{b \mid \exists c \in X: a_H(b) = c\}$ can be refused by F.

Except for the different representation of successful termination, the definitions of $\delta, a, +, \cdot, a_H$ are as for STOP, $a \to$ SKIP, $\Box$, ; and direct image in [BHR84]. The definition of $\|$ differs from the parallel composition operators in [BHR84]. In § 6.2 we will show how to interpret in ACP$_r$ synchronous parallel composition of [BHR84]. The operators $\|, |, \partial_H$ are not present in [BHR84].

5.3. The failure model. The *failure model* of ACP$_r$ is now given by the structure $\mathbb{F}(+, \cdot, \|, \lfloor\!\lfloor, |, \partial_H, a_H, a, \delta)(a \in A)$.

THEOREM 5.3.1. *The failure model of* ACP$_r$ *is isomorphic to the graph model of* ACP$_r$:

$$\mathbb{H}_\delta(+, \cdot, \|, \lfloor\!\lfloor, |, \partial_H, a_H, a, \delta)/\equiv_{\mathcal{F}} \cong \mathbb{F}(+, \cdot, \|, \lfloor\!\lfloor, |, \partial_H, a_H, a, \delta).$$

Proof. Consider the mapping $\mathcal{F}: \mathbb{H}_\delta \to \mathbb{F}$ introduced in § 2.2. It is clear that $\mathcal{F}$ is well defined, i.e., that $\mathcal{F}[\![g]\!] \in \mathbb{F}$ holds for every $g \in \mathbb{H}_\delta$. Also, by Definition 2.2.3, $g \equiv_{\mathcal{F}} h$ if and only if $\mathcal{F}[\![g]\!] = \mathcal{F}[\![h]\!]$ for all $g, h \in \mathbb{H}_\delta$. Thus $\mathcal{F}$ is also well defined and injective as a mapping:

$$\mathcal{F}: \mathbb{H}_\delta/\equiv_{\mathcal{F}} \to \mathbb{F}$$

(which, by abuse of language, we denote also with $\mathcal{F}$). Now $\mathcal{F}$ is surjective and behaves homomorphically over the operations $+, \cdot, \|, \lfloor\!\lfloor, |, \partial_H$, and a_H. The proofs of these facts are tedious but follow in a straightforward way from the definitions of these operators on graphs (in § 1.2) and the definitions of the corresponding operators on $\mathbb{F}$ (in § 5.1). We will not spell out these proofs. Thus $\mathcal{F}$ is the required isomorphism from $\mathbb{H}_\delta(\cdots)$ to $\mathbb{F}(\cdots)$. $\Box$

6. ACP$_r$ with one-to-one communication. As a preparation for the subsequent section we now introduce some additional structure on the alphabet A_δ and the communication function $|: A_\delta \times A_\delta \to A_\delta$ of ACP$_r$.

6.1. One-to-one communication. First we assume that A (with typical elements $a, b \in A$) is partitioned into $A = C \cup I$, where C (with typical elements $c, d \in C$) is the set of *communicating* actions and I (disjoint from C and with typical elements $i, j \in I$) is the set of *internal* actions. The set I will serve as an auxiliary tool for the communication function $|$.

Second, we denote by $\alpha(x)$, the *alphabet* of x, the set of non-δ actions occurring in the closed ACP$_r$-term x. For example, $\alpha(a\delta + cd) = \{a, c, d\}$. In subsequent results we will usually be interested in terms x with $\alpha(x) \subseteq C$, i.e., not involving internal,

auxiliary actions. Formally, the alphabet of a closed ACP_r-term x is defined by first eliminating the operators $\|$, $\lfloor\!\lfloor$, $|$, ∂_H, and a_H from x, using the axioms of ACP_r. (This is possible by virtue of an elimination theorem to this effect proved in [BK84a] for ACP; the extra operators a_H in ACP_r present no problem.) The resulting closed term x' contains only the "basic constructors" $+$ and $\cdot$, and we may further suppose that x' contains no subterm of the form $(p+q)r$ (by some applications of axiom A4 of ACP_r, see Table 1); that is, x' uses only prefix multiplication. Now we define $\alpha(x)$ to be $\alpha(x')$, where $\alpha(x')$ is defined by the following clauses, using induction on the structure of x':

$$\begin{aligned}
&\alpha(\delta)=\varnothing,\\
&\alpha(a)=\{a\} \qquad (a\in A),\\
&\alpha(\delta x)=\varnothing,\\
&\alpha(ax)=\{a\}\cup\alpha(x) \qquad (a\in A),\\
&\alpha(x+y)=\alpha(x)\cup\alpha(y).
\end{aligned}$$

(That $\alpha(x)$ is indeed well defined in this way, follows from the confluence property of the rewriting procedure used in obtaining x' from x. This fact is for ACP also proved in [BK84a] and is easily carried over to ACP_r.)

LEMMA 6.1.1. *For closed terms x, y over* ACP_r *with $\alpha(x)$, $\alpha(y)\subseteq C$ we have*

$$\partial_C(x\|y)=\partial_C(x|y).$$

Proof. It suffices to show that $\partial_C(x\lfloor\!\lfloor y)=\delta$. Recall that x can be normalized in ACP_r to

$$x=\Sigma_i c_i x_i+\Sigma_j d_j$$

with c_i, $d_j\in C$, and with the empty sum Σ denoting δ. Thus

$$x\lfloor\!\lfloor y=\Sigma_i c_i(x_i\|y)=\Sigma_j d_j y$$

which implies $\partial_C(x\lfloor\!\lfloor y)=\delta$. □

DEFINITION 6.1.2. Assuming the above partition of the alphabet A we say ACP_r has *one-to-one communication* if for the communication merge $|$ there exists a bijection $\varphi: C\to C$ such that $c|\varphi(c)\in I$ for every $c\in C$, and $a|b=\delta$ otherwise.

Note that $c|\varphi(c)\in I$ implies $c|\varphi(c)\neq\delta$. Next, we show that the definitions of parallel composition used in CSP and CCS are typical examples of one-to-one communication.

6.2. Hoare's parallel composition $\|_{\mathscr{H}}$ in CSP. In [BHR84] Hoare et al. propose an operation $x\|_{\mathscr{H}}y$ modelling the full synchronization of processes x and y. We shall consider $\|_{\mathscr{H}}$ here within a small subset of the language CSP [BHR84] which we call "CSP." The signature of "CSP" is given by

— the constant STOP,

— unary prefix operators $c\to$, for $c\in C$,

— the binary infix operators $\Box$ and $\|_{\mathscr{H}}$.

Here C is a given set of communication actions, contained in the overall alphabet A.

The semantics of "CSP" is determined by the failures model of [BHR84]. It is based on the failures domain $\mathbb{F}_{\mathrm{BHR}}$ consisting of all subsets

$$F\subseteq A^*\times\mathscr{P}(A)$$

satisfying the closure properties (i)-(iv) discussed in § 5.1. The additional closure property (v) on traces is not needed here since the failure sets $F \in \mathbb{F}_{\mathrm{BHR}}$ contain only failure pairs $[\sigma, X]$.

The failure model assigns to each closed "CSP" term x a failure set $\mathscr{F}_{\mathrm{BHR}}[\![x]\!]$ in the domain $\mathbb{F}_{\mathrm{BHR}}$. According to [BHR84] the definition is as follows:

(i) $\mathscr{F}_{\mathrm{BHR}}[\![\mathrm{STOP}]\!] = \{[\varepsilon, X] \mid X \subseteq A\}$;

(ii) $\mathscr{F}_{\mathrm{BHR}}[\![c \to x]\!] = \{[\varepsilon, X] \mid X \subseteq A - \{c\}\} \cup \{[c \cdot \sigma, X] \mid [\sigma, X] \in \mathscr{F}_{\mathrm{BHR}}[\![x]\!]\}$;

(iii) $\mathscr{F}_{\mathrm{BHR}}[\![x \,\Box\, y]\!] = \{[\varepsilon, X] \mid [\varepsilon, X] \in \mathscr{F}_{\mathrm{BHR}}[\![x]\!] \cap \mathscr{F}_{\mathrm{BHR}}[\![y]\!]\}$
$\cup \{[\sigma, X] \mid \sigma \neq \varepsilon \wedge [\sigma, X] \in \mathscr{F}_{\mathrm{BHR}}[\![x]\!] \cup \mathscr{F}_{\mathrm{BHR}}[\![y]\!]\}$;

(iv) $\mathscr{F}_{\mathrm{BHR}}[\![x \,\|_{\mathscr{H}}\, y]\!] = \{[\sigma, X \cup Y] \mid [\sigma, X] \in \mathscr{F}_{\mathrm{BHR}}[\![x]\!] \wedge [\sigma, Y] \in \mathscr{F}_{\mathrm{BHR}}[\![y]\!]\}$.

The failure model induces the following failure equivalence $\equiv_{\mathscr{F},\mathrm{BHR}}$ on closed "CSP" terms x and y:

$$x \equiv_{\mathscr{F},\mathrm{BHR}} y \quad \text{iff } \mathscr{F}_{\mathrm{BHR}}[\![x]\!] = \mathscr{F}_{\mathrm{BHR}}[\![y]\!].$$

We now link these definitions of [BHR84] to our present setting by interpreting "CSP" in ACP_r with one-to-one communication. Let $C = \{c_1, \cdots, c_n\}$. Then we take $A = C \cup I$ with

$$I = \{\hat{c}_1, \cdots, \hat{c}_n\}$$

where the $\hat{c}_i (i = 1, \cdots, n)$ are new copies of the actions c_i in C. Furthermore, one-to-one communication is introduced by putting $\varphi(c) = c$ and $c \mid c = \hat{c}$ for every $c \in C$. The interpretation of "CSP" in ACP_r is given by a mapping $\mathscr{I}$ from closed "CSP" terms into closed ACP_r terms defined as follows:

(i) $\mathscr{I}(\mathrm{STOP}) = \delta$;

(ii) $\mathscr{I}(c \to x) = c \cdot \mathscr{I}(x)$;

(iii) $\mathscr{I}(x \,\Box\, y) = \mathscr{I}(x) + \mathscr{I}(y)$;

(iv) $\mathscr{I}(x \,\|_{\mathscr{H}}\, y) = C_I(\partial_C(\mathscr{I}(x) \| \mathscr{I}(y)))$

where C_I abbreviates the composite operator $(c_1)_{\{\hat{c}_1\}} \circ \cdots \circ (c_n)_{\{\hat{c}_n\}}$, built from the renaming operators $(c_i)_{\{\hat{c}_i\}} (i = 1, \cdots, n)$ that rename c_i into $\hat{c}_i$.

This interpretation is justified by the following result.

PROPOSITION 6.2.1. *For closed* "CSP" *terms* x

$$\mathscr{F}_{\mathrm{BHR}}[\![x]\!] = \mathscr{F}[\![\mathscr{I}(x)]\!] \subseteq C^* \times \mathscr{P}(A)$$

holds where $\mathscr{F}$ *is the* ACP_r *failures model of* § 5. *In particular* $\mathscr{F}[\![\mathscr{I}(x)]\!]$ *does not contain any traces* σ *signaling successful termination, only failure pairs* $[\sigma, X]$.

Proof. By induction on the structure of x. The cases (i)-(iii) are immediate. Case (iv), parallel composition, is more tedious. It is easy to see that both

$$\mathscr{F}_{\mathrm{BHR}}[\![x \,\|_{\mathscr{H}}\, y]\!],\ \mathscr{F}[\![C_I(\partial_C(\mathscr{I}(x) \| \mathscr{I}(y))]\!] \subseteq C^* \times \mathscr{P}(A).$$

Hence the closure properties of the failure domains $\mathbb{F}_{\mathrm{BHR}}$ and $\mathbb{F}$, respectively, imply

$$[\sigma, X] \in \mathscr{F}_{\mathrm{BHR}}[\![x \,\|_{\mathscr{H}}\, y]\!] \quad \text{iff} [\sigma, X \cup Y] \in \mathscr{F}_{\mathrm{BHR}}[\![x \,\|_{\mathscr{H}}\, y]\!],$$

$$[\sigma, X] \in \mathscr{F}[\![C_I(\partial_C(\mathscr{I}(x) \| \mathscr{I}(y)))]\!] \quad \text{iff } [\sigma, X \cup Y] \in \mathscr{F}[\![C_I(\partial_C(\mathscr{I}(x) \| \mathscr{I}(y)))]\!]$$

for arbitrary $Y \subseteq A - C$. Thus it suffices to show

$$[\sigma, X] \in \mathscr{F}_{\mathrm{BHR}}[\![x \,\|_{\mathscr{H}}\, y]\!] \quad \text{iff } [\sigma, X] \in \mathscr{F}[\![C_I(\partial_C(\mathscr{I}(x) \| \mathscr{I}(y)))]\!]$$

for $\sigma \in C^*$ and $X \subseteq C$.

Let $\hat{\sigma}$ and $\hat{X}$ result from σ and X by replacing pointwise each action c by $\hat{c}$. In particular, we have $\hat{C} = A - C$. Then for $\sigma \in C^*$ and $X \subseteq C$

$$[\sigma, X] \in \mathscr{F}_{\mathrm{BHR}}[\![x \parallel_{\mathscr{H}} y]\!]$$

if and only if (induction hypothesis, definition of $\parallel_{\mathscr{H}}$)

$$\exists X_1 \subseteq C, X_2 \subseteq C:$$
$$[\sigma, X_1] \in \mathscr{F}[\![\mathscr{I}(x)]\!] \wedge [\sigma, X_2] \in \mathscr{F}[\![\mathscr{I}(y)]\!] \wedge X \subseteq X_1 \cup X_2$$

if and only if (definition $\hat{X}$)

$$\exists X_1 \subseteq C, X_2 \subseteq C:$$
$$[\sigma, X_1] \in \mathscr{F}[\![\mathscr{I}(x)]\!] \wedge [\sigma, X_2] \in \mathscr{F}[\![\mathscr{I}(y)]\!] \wedge \hat{X} \subseteq \{\hat{c} \mid c \in X_1 \cup X_2\}$$

if and only if (closure properties of the failure domain $\mathbb{F}$)

$$\begin{aligned}\exists X_1, X_2\colon \hat{C} \subseteq X_1 \subseteq A \wedge \hat{C} \subseteq X_2 \subseteq A \\ \wedge [\sigma, X_1] \in \mathscr{F}[\![\mathscr{I}(x)]\!] \wedge [\sigma, X_2] \in \mathscr{F}[\![\mathscr{I}(y)]\!] \\ \wedge \hat{X} \subseteq X_1 \cap X_2 - \{\hat{c} \mid c \notin X_1 \cup X_2\}\end{aligned}$$

if and only if (one-to-one communication, definition $\|$)

$$[\hat{\sigma}, \hat{X}] \in \mathscr{F}[\![\mathscr{I}(x) \| \mathscr{I}(y)]\!]$$

if and only if (definition C_I, ∂_C)

$$[\sigma, X] \in \mathscr{F}[\![C_I(\partial_C(\mathscr{I}(x) \| \mathscr{I}(y)))]\!]$$

This finishes our proof. □

Consequently, for "CSP" the original failure equivalence $\equiv_{\mathscr{F},\mathrm{BHR}}$ of [BHR84] coincides with our definition of failure equivalence $\equiv_{\mathscr{F}}$ in § 2. More precisely we have the following corollary:

COROLLARY 6.2.2. *For closed* "CSP" *terms x and y*

$$x \equiv_{\mathscr{F},\mathrm{BHR}} y \quad \textit{iff } \mathscr{I}(x) \equiv_{\mathscr{F}} \mathscr{I}(y).$$

For closed "CSP" terms x and y the notions of trace and trace equivalence are defined via the interpretation in ACP_r:

$$\mathrm{trace}\,(x) = \mathrm{trace}\,(\mathscr{I}(x)),$$
$$x \sim_{\mathrm{tr}} y \quad \text{iff } \mathscr{I}(x) \sim_{\mathrm{tr}} \mathscr{I}(y).$$

(Actually, trace is in § 2.1 only defined on graphs; using the operation graph from § 4.1.2 we now define for a term x, trace (x) as trace (graph (x)).) Using Proposition 6.2.1 the trace set of a term x can also be computed directly from its failure set $\mathscr{F}_{\mathrm{BHR}}[\![x]\!]$:

$$\mathrm{trace}\,(x) = \{\sigma \cdot \delta \mid [\sigma, A] \in \mathscr{F}_{\mathrm{BHR}}[\![x]\!]\}.$$

Recall that in our paper we only consider *complete* traces, either leading to a deadlock δ or to successful termination (not possible for "CSP"). In [BHR84] the word "trace" is used as well, but it refers to any sequence σ with

$$[\sigma, \varnothing] \in \mathscr{F}_{\mathrm{BHR}}[\![x]\!].$$

Such sequences were called *histories* in § 2.

6.3. Milner's parallel composition $\|_{\mathcal{M}}$ in CCS. Since the parallel composition $\|$ in ACP_r can be seen as a generalization of Milner's operation $\|_{\mathcal{M}}$ in CCS [Mi80], it is easy to regain the original definition. As for CSP, we do this within a small subset of CCS which we call "CCS." Milner stipulates that the set C of communicating actions is equipped with a bijection $^{-}: C \to C$ satisfying $\bar{\bar{c}} = c$. Here $\bar{c}$ is called the *matching* action of c. In addition to communicating actions Milner uses a symbol τ denoting the so-called *silent* action. We will write $\hat{\tau}$ because we work here without Milner's τ-laws that make τ silent or invisible (see the discussion below and § 8). Hence the alphabet for "CCS" will be $A = C \cup \{\hat{\tau}\}$.

The signature of "CCS" consists of the following:

— the constant NIL;

— unary prefix operators $a\cdot$, for $a \in A$;

— unary postfix operators $\backslash H$, for $H \subseteq C$;

— the binary infix operators $+$ and $\|_{\mathcal{M}}$.

Informally, $x \|_{\mathcal{M}} y$ denotes the nondeterministic interleaving of x and y, plus the communication of x and y via matching actions which then yield $\hat{\tau}$ as a result. Following [Mi80], this can be expressed by the infinite axiom scheme:

$$(*) \qquad (\Sigma_i a_i x_i) \|_{\mathcal{M}} (\Sigma_j b_j y_j) = \Sigma_i a_i (x_i \|_{\mathcal{M}} y) + \Sigma_j b_j (x \|_{\mathcal{M}} y_j) + \Sigma_{a_i = \bar{b}_j} \hat{\tau} \cdot (x_i \|_{\mathcal{M}} y_j)$$

where $x = \Sigma_i a_i x_i$ and $y = \Sigma_j b_j y_j$.

We shall define the semantics of $\|_{\mathcal{M}}$ via an interpretation $\mathcal{I}$ of "CCS" in ACP_r with one-to-one communication. To this end, take $I = \{\hat{\tau}\}$ and define

$$\varphi(c) = \bar{c} \text{ and } c \,|\, \bar{c} = \hat{\tau}.$$

Then $\mathcal{I}$ is rather trivial:

(i) $\mathcal{I}(\mathrm{NIL}) = \delta$;
(ii) $\mathcal{I}(a \cdot x) = a \cdot \mathcal{I}(x)$;
(iii) $\mathcal{I}(x \backslash H) = \partial_H(\mathcal{I}(x))$;
(iv) $\mathcal{I}(x + y) = \mathcal{I}(x) + \mathcal{I}(y)$;
(v) $\mathcal{I}(x \|_{\mathcal{M}} y) = \mathcal{I}(x) \| \mathcal{I}(y)$.

Note that the auxiliary operations $\lfloor\!\lfloor$ and $|$ in ACP_r serve to replace the infinite axiom scheme $(*)$ by finitely many ACP_r axioms.

In [Mi80] Milner studies CCS terms under the (weak) bisimulation equivalence [Pa83]; however, here we shall study "CCS" under the failure equivalence. For closed "CCS" terms x and y we define the notions of failure equivalence, trace equivalence and alphabet via the interpretation $\mathcal{I}$ in ACP_r:

$$x \equiv_{\mathcal{F}} y \quad \text{iff } \mathcal{I}(x) \equiv_{\mathcal{F}} \mathcal{I}(y),$$

$$x \sim_{\mathrm{tr}} y \quad \text{iff } \mathcal{I}(x) \sim_{\mathrm{tr}} \mathcal{I}(y),$$

$$\alpha(x) = \alpha(\mathcal{I}(x)).$$

In general, these definitions are not quite appropriate for CCS because τ should be silent or invisible; more formally τ should be subject to Milner's τ-laws. In the above interpretation of "CCS" $\hat{\tau}$ remains visible, i.e., recorded in the traces and failure pairs. The reason for this clash is that CCS indivisibly couples parallel composition $\|_{\mathcal{M}}$ and τ, whereas we decided to separate failure equivalence $\equiv_{\mathcal{F}}$ from τ.

However, we can regain the spirit of CCS if we restrict the failure equivalence to *$\hat{\tau}$-free* "CCS" terms x and y, i.e., with

$$\hat{\tau} \notin \alpha(x), \alpha(y).$$

Unfortunately, $\hat{\tau}$-free "CCS" terms are not closed under parallel composition $\|_{\mathcal{M}}$. Therefore we shall consider also a modified trace set

$$\text{trace}_{\hat{\tau}}(x)$$

for "CCS" terms x which results from trace (x) by deleting in every trace $\sigma \cdot \delta \in \text{trace}(x)$ all occurrences of $\hat{\tau}$ in σ. Then $\text{trace}_{\hat{\tau}}(x)$ represents the set of complete traces in the sense of CCS. For example,

$$\text{trace}(c\text{NIL} \|_{\mathcal{M}} \bar{c}\text{NIL}) = \{c\bar{c}\delta, \bar{c}c\delta, \hat{\tau}\delta\},$$

$$\text{trace}_{\hat{\tau}}(c\text{NIL} \|_{\mathcal{M}} \bar{c}\text{NIL}) = \{c\bar{c}\delta, \bar{c}c\delta, \delta\}.$$

7. The maximal trace respecting congruence. In § 4 (Proposition 4.2.3) it was shown that failure equivalence $\equiv_{\mathcal{F}}$ is a congruence with respect to the operators of ACP_r. In this section we will prove that for ACP_r with one-to-one communication failure equivalence is in fact the maximal trace respecting congruence. This implies a full abstraction result for the failure model of § 5. But first let us introduce the relevant concepts.

7.1. Preliminaries. Let Σ be a signature with $\text{Ter}(\Sigma)$ denoting the set of closed terms over Σ. By $\text{Ter}(\Sigma)[\xi]$ we denote the set of terms over Σ with ξ as free variable. These terms are called *contexts* and are typically written as $\mathcal{C}[\xi]$.

Let $\mathcal{T} \subseteq \text{Ter}(\Sigma)$. A *congruence for* $\mathcal{T}$ is an equivalence relation $\equiv$ on $\mathcal{T}$, such that

$$x \equiv y \quad \text{implies } \mathcal{C}[x] \equiv \mathcal{C}[y]$$

for all terms $x, y \in \mathcal{T}$ and contexts $\mathcal{C}[\xi] \in \text{Ter}(\Sigma)[\xi]$ with $\mathcal{C}[x], \mathcal{C}[y] \in \mathcal{T}$. A congruence $\equiv$ for $\mathcal{T}$ is *trace respecting* if

$$x \equiv y \quad \text{implies trace}(x) = \text{trace}(y)$$

for all $x, y \in \mathcal{T}$. A trace respecting congruence $\equiv$ for $\mathcal{T}$ is called *maximal* if for all $x, y \in \mathcal{T}, x \not\equiv y$ implies that there exists some context $\mathcal{C}[\xi] \in \text{Ter}(\Sigma)[\xi]$ with $\mathcal{C}[x], \mathcal{C}[y] \in \mathcal{T}$ and $\text{trace}(\mathcal{C}[x]) \neq \text{trace}(\mathcal{C}[y])$.

PROPOSITION 7.1.1. *For each $\mathcal{T} \subseteq \text{Ter}(\Sigma)$ the maximal trace respecting congruence for $\mathcal{T}$ exists and is unique.*

Proof. Uniqueness. Suppose $\equiv_1$ and $\equiv_2$ are different maximal trace respecting congruences on $\mathcal{T}$. Then for some $x, y \in \mathcal{T}$ we have

$$x \equiv_1 y, \quad \text{but } x \not\equiv_2 y.$$

Since $\equiv_1$ is a trace respecting congruence on $\mathcal{T}$, $\text{trace}(\mathcal{C}[x]) = \text{trace}(\mathcal{C}[y])$ holds for every context $\mathcal{C}[\xi] \in \text{Ter}(\Sigma)[\xi]$ with $\mathcal{C}[x], \mathcal{C}[y] \in \mathcal{T}$. But this contradicts the maximality of $\not\equiv_2$.

Existence. Define $\equiv$, a binary relation on $\mathcal{T}$, as follows: $x \equiv y$ if and only if for every context $\mathcal{C}[\xi] \in \text{Ter}(\Sigma)[\xi]$ with $\mathcal{C}[x], \mathcal{C}[y] \in \mathcal{T}$, $\text{trace}(\mathcal{C}[x]) = \text{trace}(\mathcal{C}[y])$ holds.

It is easy to see that $\equiv$ is a trace respecting congruence for $\mathcal{T}$; maximality follows from its definition. □

7.2. A characterisation of failure equivalence. Let us now turn to ACP_r. We write $\text{Ter}(\text{ACP}_r)$ instead of $\text{Ter}(\Sigma)$. From § 4 we know that failure equivalence $\equiv_{\mathcal{F}}$ is a trace respecting congruence for $\text{Ter}(\text{ACP}_r)$. (For the sake of convenience, we have identified here the semantical notion $\equiv_{\mathcal{F}}$ with the equivalence induced by $\equiv_{\mathcal{F}}$ on $\text{Ter}(\text{ACP}_r)$ via the correspondence between process graphs and terms, explained in § 4.1.) Thus for ACP_r, in general, we have

$$\equiv_{\mathcal{F}} \subseteq \equiv_{\max}$$

with $\equiv_{\max}$ denoting the maximal trace respecting congruence for Ter (ACP$_r$). If we specialize ACP$_r$ to the case of one-to-one communication, we can actually prove that

$$\equiv_{\mathscr{F}} = \equiv_{\max},$$

and thus arrive at a very pleasing characterization of failure equivalence.

THEOREM 7.2.1. *Consider* ACP$_r$ *with one-to-one communication. Then failure equivalence* $\equiv_{\mathscr{F}}$ *is the maximal trace respecting congruence for the set* $\mathscr{T}_C$ *of all closed terms* x *over* ACP$_r$ *with alphabet* $\alpha(x) \subseteq C$.

Proof. Suppose $x \not\equiv_{\mathscr{F}} y$; i.e., $\mathscr{F}[\![x]\!] \neq \mathscr{F}[\![y]\!]$ holds for $x, y \in \mathscr{T}_C$. If trace $(x) \neq$ trace (y), the trivial context $\mathscr{C}[\xi] = \xi$ will do. Now suppose that trace $(x) =$ trace (y) holds. Because of $x \not\equiv_{\mathscr{F}} y$ we can assume without loss of generality that there exists a failure pair $[\sigma, X]$ with

$$[\sigma, X] \in \mathscr{F}[\![x]\!], [\sigma, X] \notin \mathscr{F}[\![y]\!].$$

By the definition of $\mathscr{F}$, $[\sigma, X] \in \mathscr{F}[\![x]\!]$ implies that there exists some ready pair $(\sigma, Z) \in \mathscr{R}[\![x]\!]$ with $X \subseteq Z$. Note that $Z \neq \emptyset$. Suppose we had $(\sigma, \emptyset) \in \mathscr{R}[\![x]\!]$. Then $\sigma\delta \in$ trace $(x) =$ trace (y) and $(\sigma, \emptyset) \in \mathscr{R}[\![y]\!]$. Thus $[\sigma, C] \in \mathscr{F}[\![y]\!]$ and therefore also $[\sigma, X] \in \mathscr{F}[\![x]\!]$, a contradiction.

Trace equivalence of x and y implies that there exists a ready pair $(\sigma, Y) \in \mathscr{R}[\![y]\!]$ with $Y \neq \emptyset$. Again by the definition of $\mathscr{F}$, $[\sigma, X] \notin \mathscr{F}[\![y]\!]$ implies that for every such ready pair $(\sigma, Y) \in \mathscr{R}[\![y]\!]$ there exists some $d \in X \cap Y$. Now consider a context of the form

$$\mathscr{C}[\xi] = (c_{1\{i_1\}} \circ \cdots \circ c_{n\{i_n\}} \circ \partial_C)(x \| \varphi(\sigma) \cdot \Sigma\varphi(d) \cdot \delta)$$

where the sum Σ is taken over all $d \in X \cap Y$ such that $(\sigma, Y) \in \mathscr{R}[\![y]\!]$. Furthermore $I = \{i_1, \cdots, i_n\}$, $c_1, \cdots, c_n \in C$, φ is the bijection describing the one-to-one communication in ACP$_r$ and $\varphi(\sigma)$ is the result of applying φ pointwise to σ. Note that $\mathscr{C}[\xi]$ is uniquely determined by x and y except for the choice of the $c_1, \cdots, c_n$ in the renaming operators. Note that indeed $\mathscr{C}[x], \mathscr{C}[y] \in \mathscr{T}_C$ due to the presence of operators ∂_C and $c_{j\{i_j\}}$ in $\mathscr{C}[\xi]$. We now claim that

$$(c_{1\{i_1\}} \circ \cdots \circ c_{n\{i_n\}})(\sigma | \varphi(\sigma)) \cdot \delta \in \text{trace}\,(\mathscr{C}[x]), \notin \text{trace}\,(\mathscr{C}[y])$$

where $\sigma | \varphi(\sigma)$ is understood by applying $|$ pointwise to σ and $\varphi(\sigma)$.

To prove this claim we first state a general observation about ready sets $\mathscr{R}[\![z]\!]$ of closed terms z over ACP$_r$. Let $\sigma = a_1 \cdots a_m$ and $Z = \{b_1, \cdots, b_n\}$. Then $(\sigma, Z) \in \mathscr{R}[\![z]\!]$ if and only if there exist $x_1, \cdots, x_m, y_1, \cdots, y_n \in$ Ter (ACP$_r$) with

$$\text{ACP}_r \vdash x = a_1(a_2 \cdots (a_m(b_1 y_1 + \cdots + b_n y_n) + x_m) \cdots + x_2) + x_1.$$

This observation is obvious from §§ 3 and 4.

Next we recall from Lemma 6.1.1 that due to the encapsulation ∂_C we can replace the general parallel composition $\|$ in $\mathscr{C}[\xi]$ by the communication operator $|$ which enforces synchronization.

Combining these two facts, it is easy to calculate that $(\sigma, Z) \in \mathscr{R}[\![x]\!]$ with $X \subseteq Z$ yields

$$(c_{1\{i_1\}} \circ \cdots \circ c_{n\{i_n\}})(\sigma | \varphi(\sigma)) \cdot \delta \in \text{trace}\,(\mathscr{C}[x]).$$

Now suppose that this trace is also present in trace $(\mathscr{C}[y])$. Since ACP$_r$ allows only one-to-one communication, there exists a history $\sigma \in C^*$ such that every ready pair $(\sigma, Y) \in \mathscr{R}[\![y]\!]$ satisfies $X \cap Y = \emptyset$. This is a contradiction. This finishes our proof. □

7.3. Application to CSP and CCS. The characterization of failure equivalence for ACP_r yields corresponding results for the subsets "CSP" and "CCS" or [BHR84] and [Mi80].

COROLLARY 7.3.1. *For closed* "CSP" *terms the failure equivalence* $\equiv_{\mathscr{F},\mathrm{BHR}}$ *of* [BHR84] *is the maximal trace respecting congruence.*

Proof. Via the interpretation $\mathscr{I}$ the failure equivalence $\equiv_{\mathscr{F},\mathrm{BHR}}$ is a trace respecting congruence for "CSP." To show maximality, suppose $x \not\equiv_{\mathscr{F},\mathrm{BHR}} y$ for closed terms x and y. Then $\mathscr{I}(x) \not\equiv_{\mathscr{F}} \mathscr{I}(y)$ by Corollary 6.2.2. Since $\alpha(\mathscr{I}(x)), \alpha(\mathscr{I}(y)) \subseteq C$, Theorem 7.2.1 applies and yields a context $\mathscr{C}[\xi]$ in ACP_r with

$$\mathscr{C}[\mathscr{I}(x)] \not\sim_{\mathrm{tr}} \mathscr{C}[\mathscr{I}(y)].$$

Looking at the proof of Theorem 7.2.1 we see that $\mathscr{C}[\xi]$ can be expressed in "CSP"; i.e., there exists a context $\mathscr{C}'[\xi]$ in "CSP" with

$$I(\mathscr{C}')[\xi] = \mathscr{C}[\xi]$$

where we stipulate $\mathscr{I}(\xi) = \xi$. Thus

$$\mathscr{I}(\mathscr{C}')[\mathscr{I}(x)] \not\sim_{\mathrm{tr}} \mathscr{I}(\mathscr{C}')[\mathscr{I}(y)].$$

Since $\mathscr{I}$ is defined by structural induction, we have $\mathscr{I}(\mathscr{C}')[\mathscr{I}(x)] = \mathscr{I}(\mathscr{C}'[x])$ and likewise for y. Thus

$$\mathscr{C}'[x] \not\sim_{\mathrm{tr}} \mathscr{C}'[y]$$

by the definition of trace equivalence for "CSP." □

Due to the differences of τ and $\hat{\tau}$ in CCS and ACP_r (see § 6.3), we can characterize failure equivalence only for $\hat{\tau}$-free "CCS" terms.

COROLLARY 7.3.2. *On the subset of closed,* $\hat{\tau}$*-free* "CCS" *terms failure equivalence* $\equiv_{\mathscr{F}}$ *coincides with the maximal trace respecting congruence defined for full* "CCS." *This result holds for both notions of trace introduced for* "CCS" *terms, viz.,* trace$(\cdot)$ *and* $\mathrm{trace}_{\hat{\tau}}(\cdot)$.

Proof. Via the interpretation $\mathscr{I}$ failure equivalence $\equiv_{\mathscr{F}}$ is a trace respecting congruence for "CCS." This holds for the original definition of trace $(\cdot)$, however, since

$$\mathrm{trace}\,(x) = \mathrm{trace}\,(y) \quad \text{implies } \mathrm{trace}_{\hat{\tau}}\,(x) = \mathrm{trace}_{\hat{\tau}}\,(y),$$

it holds for $\mathrm{trace}_{\hat{\tau}}(\cdot)$ as well.

Now consider two closed, $\hat{\tau}$-free "CCS" terms x, y such that $x \not\equiv_{\mathscr{F}} y$, i.e., $\mathscr{I}(x) \not\equiv_{\mathscr{F}} \mathscr{I}(y)$. Since $\hat{\tau}$-freeness means $\alpha(\mathscr{I}(x)), \alpha(\mathscr{I}(y)) \subseteq C$, the proof technique for Theorem 7.2.1 applies and yields an ACP_r context of the form

$$\mathscr{C}[\xi] = \partial_C(\xi \| \mathscr{I}(z))$$

where z is a closed, $\hat{\tau}$-free "CCS" term such that for some $n \geqq 0$

$$\hat{\tau}^n \cdot \delta \in \mathrm{trace}\,(\mathscr{C}[\mathscr{I}(x)]), \notin \mathrm{trace}\,(\mathscr{C}[\mathscr{I}(y)]).$$

Note that in the definition of $\mathscr{C}[\xi]$ we deviate slightly from Theorem 7.2.1 and omit the renaming operator, which would yield here $c_{\{\hat{\tau}\}}$ for some $c \in C$. The reason is that τ (respectively, $\hat{\tau}$) cannot be renamed in Milner's [Mi80] (and hence "CCS").

The above $\mathscr{C}[\xi]$ can be translated back into the "CCS" context

$$\mathscr{C}'[\xi] = (\xi \|_{\mathscr{M}} z) \backslash C,$$

which yields

$$\hat{\tau}^n \cdot \delta \in \mathrm{trace}\,(\mathscr{C}'[x]), \notin \mathrm{trace}\,(\mathscr{C}'[y]),$$

and thus

$$\delta \in \text{trace}_{\hat{\tau}}(\mathscr{C}'[x]), \notin \text{trace}_{\hat{\tau}}(\mathscr{C}'[y]).$$

This proves the maximality of failure equivalence for $\hat{\tau}$-free "CCS" terms with respect to both notions of trace. □

Thus the (proof of) Theorem 7.2.1 gives a uniform argument for the communication mechanisms of both "CSP" and CCS."

Remark 7.3.3. (Comparison with the work of De Nicola and Hennessy [DH84].) We have proved that (under a restricted communication format) processes are failure equivalent if and only if they cannot be separated by any context where "separated" refers to the criterion of having different traces. This characterisation is easy to understand, as it involves only the notions of *trace* and *context.* It is interesting to compare our result with a result in [DH84]. Since the settings are quite different (here finite processes in ACP_r, there CCS with recursion, τ-steps and an additional constant Ω denoting the undefined state), we state the comparison for the greatest common denominator of ACP_r and CCS, viz., the language "CCS" of § 6.3.

De Nicola and Hennessy [DH84] set up a notion of *testing* and consider two processes p and q as equivalent if and only if they pass exactly the same tests. This idea of testing is very appealing, but the formal definitions are somewhat more technical. Both processes and tests are just terms over the signature of "CCS." However, in the alphabet A we assume a distinguished action ω, which may appear in tests only. The action ω is interpreted as reporting success; it is needed in the definition of a process passing a test. Due to the restriction to "CCS," we can phrase De Nicola and Hennessy's definition as follows.

For "CCS" terms p, q, r and actions $a \in A$ we write

$$p \xrightarrow{a} q \quad \text{if } \exists r\text{: "CCS"} \vdash p = a \cdot q + r,$$
$$p \xrightarrow{a} \quad \text{if } \exists q : p \xrightarrow{a} q.$$

Intuitively, $p \xrightarrow{a} q$ states that p can perform an action a and then behave like q. A *computation* is a sequence of "CCS" terms of the form

$$p_1 \xrightarrow{\hat{\tau}} p_2 \xrightarrow{\hat{\tau}} \cdots \xrightarrow{\hat{\tau}} p_n;$$

it is called *maximal* if there is no "CCS" term q with $p_n \xrightarrow{\hat{\tau}} q$. Since "CCS" does not include recursion, any computation is finite here.

There are two forms of a process p passing a test t:

(i) *p may pass t* if there exists a computation

$$p \parallel_{\mathscr{M}} t = p_1 \parallel_{\mathscr{M}} t_1 \xrightarrow{\hat{\tau}} \cdots \xrightarrow{\hat{\tau}} p_n \parallel_{\mathscr{M}} t_n$$

with $t_n \xrightarrow{\omega}$, or equivalently if there exists some $n \geqq 0$ with

$$\hat{\tau}^n \cdot \omega \in \text{trace}(p \parallel_{\mathscr{M}} t),$$

(ii) *p must pass t* if whenever

$$p \parallel_{\mathscr{M}} t = p_1 \parallel_{\mathscr{M}} t_1 \xrightarrow{\hat{\tau}} \cdots \xrightarrow{\hat{\tau}} p_n \parallel_{\mathscr{M}} t_n$$

is a *maximal computation* then there exists some m with $1 \leqq m \leqq n$ and $t_m \xrightarrow{\omega}$.

Thus a term t_n that can perform an ω-action serves as a criterion for success. For examples of (i) and (ii) we refer to [DH84].

Then De Nicola and Hennessy [DH84] introduce three so-called *testing equivalences* on processes p, q:

(i) $p \simeq_1 q$ if for every test t: p may pass t if and only if q may pass t.

(ii) $p \simeq_2 q$ if for every test t: p must pass t if and only if q must pass t.

(iii) $p \simeq_3 q$ if $p \simeq_1 q$ and $p \simeq_2 q$.

It is now very interesting that for $\hat{\tau}$-free "CCS" the strong testing equivalence coincides with the failure equivalence $\equiv_{\mathcal{F}}$. This is an immediate consequence of Corollary 6.2.6 of [DH84] stated for the class of so-called strongly convergent CCS terms, which in particular includes all $\hat{\tau}$-free "CCS" terms. Thus at least for $\hat{\tau}$-free "CCS" terms we have a pleasing convergence of ideas:

strong testing equivalence = failure equivalence = maximal trace respecting congruence.

Conceptually, we find the notion of a maximal trace respecting congruence simpler than the definition of passing a test.

7.4. Full abstraction. The notion of *full abstraction* is due to Milner [Mi77] (see also [HP79], [Pl77]). It is a relationship between models (of an axiomatic system) and equivalence relations (on the terms of that system) whose definition is motivated by the following question:

Under what circumstances can we replace a term x by a term y without noticing this change by a given equivalence $\equiv$?

Using the notion of a context introduced above, this question amounts to:

Under what conditions on x and y do we have $\mathscr{C}[x] \equiv \mathscr{C}[y]$ for every context $\mathscr{C}[\xi]$?

Full abstraction can be seen as looking for a sufficient and necessary condition that answers this question. Formally, we state the following definition.

DEFINITION 7.4.1. A model $\mathcal{M}$ for $\mathcal{T} \subseteq \mathrm{Ter}(\Sigma)$ is called *fully abstract with respect to an equivalence relation* $\equiv$ on $\mathcal{T}$ if for all terms $x, y \in \mathcal{T}$:

$$\mathcal{M}[\![x]\!] = \mathcal{M}[\![y]\!] \text{ iff } \mathscr{C}[x] \equiv \mathscr{C}[y] \quad \text{holds for every context} \quad \mathscr{C}[\xi] \in \mathrm{Ter}(\Sigma)[\xi] \quad \text{with} \quad \mathscr{C}[x], \mathscr{C}[y] \in \mathcal{T}.$$

Thus a fully abstract model $\mathcal{M}$ optimally fits the equivalence $\equiv$ in the sense that it just makes the identifications on terms that are forced by $\equiv$. Usually, it is quite difficult to discover fully abstract models (see [HP79], [Mi77], [Pl77]), but for the failure model $\mathcal{F} = \mathbb{F}(+, \cdot, \|, \lfloor\!\lfloor, |, \partial_H, a_H, a, \delta)(a \in A)$ of § 5 and the trace equivalence $\sim_{\mathrm{tr}}$ of § 2 we can now state such a result.

THEOREM 7.4.2. *Consider* ACP_r *with one-to-one communication. Then for the set $\mathcal{T}_C$ of all closed terms x over* ACP_r *with alphabet $\alpha(x) \subseteq C$ the failure model $\mathcal{F}$ is fully abstract with respect to the trace equivalence $\sim_{\mathrm{tr}}$.*

Proof. By Definition 7.4.1, it suffices to show that for all $x, y \in \mathcal{T}_C$:

$$\mathcal{F}[\![x]\!] = \mathcal{F}[\![y]\!] \quad \text{iff } x \equiv_{\max} y$$

where $\equiv_{\max}$ is the maximal trace respecting congruence. But this is immediate from Theorem 7.2.1. □

COROLLARY 7.4.3. *For the set of closed "CSP" terms the failure model $\mathcal{F}_{\mathrm{BHR}}$ of* [BHR84] *is fully abstract with respect to the trace equivalence $\sim_{\mathrm{tr}}$.*

For "CCS" we cannot state the analogous result due to the $\hat{\tau}$ mismatch discussed above.

8. Processes with recursion and abstraction: bisimulation versus failure equivalence.

8.1. Preliminaries. In the preceding sections we have been exclusively concerned with the failure semantics for finite processes without abstraction, i.e., not involving τ-steps. In this section we will set aside that restriction and comment also on infinite

(recursive) processes with abstraction, in regard to bisimulation and failure equivalence. The crucial point is the way in which infinite sequences of τ-steps in a process are treated.

In the failure semantics proposed in [BHR84], all processes having an infinite τ-sequence from the root are set equal (to the process CHAOS). The notion of bisimulation is more discriminating. The advantage is that models obtained by bisimulation equivalence satisfy a useful abstraction principle: *Koomen's Fair Abstraction Rule* (KFAR), as introduced in [BK84b]. Roughly, this rule gives a way of simplifying processes by elimination of (some) infinite τ-sequences. This elimination can be understood as *fairness* of (visible) actions over silent τ-steps. A more precise description is given below. (Of course, setting all processes having an infinite τ-sequence from the root equal to CHAOS also eliminates infinite τ-sequences, but then all information is lost.)

Since KFAR is a very useful tool for system verification (e.g., in [BK84b] it was used to verify an alternating bit protocol), it is natural to ask whether KFAR is also compatible with the somewhat simpler failure semantics. More precisely, we can ask whether there exists a process model which for finite processes agrees with the failure semantics and for infinite processes satisfies KFAR. Interestingly, it turns out that such a model does not exist. To prove this result, we will formulate a set of assumptions embodying failure semantics and KFAR, and derive an inconsistency. Formally, the inconsistency arises from the following extension of the axiom system considered above:

$$\begin{aligned}&\mathrm{ACP}_r + \mathrm{R1}, 2 + \mathrm{S}\\ &\quad + \text{Milner's } \tau\text{-laws} + \text{axioms for abstraction operators}\\ &\quad + \mathrm{KFAR}\\ &\quad + \mathrm{RSP}\ (\text{recursive specification principle}).\end{aligned}$$

Here RSP is the assumption that guarded systems of recursion equations have a solution, which is moreover unique.

Now by virtue of our axiomatic approach we can pinpoint the origin of the inconsistency derived below with some accuracy. It turns out that the failure of KFAR in failure semantics holds already in ready semantics, and moreover that communication does not play a role in the inconsistency. That is, the inconsistency already appears in the subsystem

$$\mathrm{BPA} + \mathrm{T1} + \mathrm{TI1-5} + \mathrm{R1} + \mathrm{KFAR} + \mathrm{RSP}$$

which we will explain now. BPA, for *basic process algebra*, consists of the axioms A1–5 of ACP_r, which specify the properties of $+$ and $\cdot$. T1 is the simplest of Milner's τ-laws [Mi80] (see Table 6). In addition, Table 6 contains axioms TI1–TI5; these specify the abstraction operators τ_I, where $I \subseteq A$ is a set of *internal* actions as simple renaming operators (cf. [BK84c] and [BK86a], [BK86b]).

R1 is the axiom for the readiness semantics (see Tables 3 and 4):

$$a(bx+u)+a(by+v)=a(bx+by+u)+a(bx+by+v).$$

The *recursive specification principle* RSP states that guarded systems E of recursive equations have unique solutions (see [BK84b] or [BBK85]):

$$\frac{E(x_1,\cdots,x_n),\ E(y_1,\cdots,y_n),\quad E \text{ guarded}}{x_1=y_1}.$$

Informally, "guarded" means that every recursive occurrence of x_i in E is preceded

TABLE 6
BPA + T1 + TI1-5

$x+y=y+x$	A1
$(x+y)+z=x+(y+z)$	A2
$x+x=x$	A3
$(x+y)z=xz+yz$	A4
$(xy)z=x(yz)$	A5
$x\tau=x$	T1
$\tau_I(\tau)=\tau$	TI1
$\tau_I(a)=a \quad \text{if } a\notin I$	TI2
$\tau_I(a)=\tau \quad \text{if } a\in I$	TI3
$\tau_I(x+y)=\tau_I(x)+\tau_I(y)$	TI4
$\tau_I(xy)=\tau_I(x)\cdot\tau_I(y)$	TI5

by an action different from τ. For example, the system

$$x_1 = ax_2 + bx_2,$$

$$x_2 = c(x_1 + x_2) + d$$

is guarded and thus has a unique solution.

We will now explain KFAR. For each $n \geqq 1$, we have a version KFAR_n. KFAR_1 is as follows:

$$\frac{x = ix + y \quad (i \in I)}{\tau_I(x) = \tau \cdot \tau_I(y)}.$$

The premise of KFAR_1 says that x has an infinite i-trace (see Fig. 19). Now KFAR_1 expresses the fact that x makes *fair* choices along its infinite i-trace, i.e., performing x entails at most finitely many choices against y. We may note here the necessity of the abstraction operator τ_I in KFAR_1: From $x = \tau x + y$ it does *not* follow that $x = \tau \cdot \tau_I(y)$, since the equation $x = \tau x + y$ has infinitely many solutions (see [BK84c] or [BK86a]).

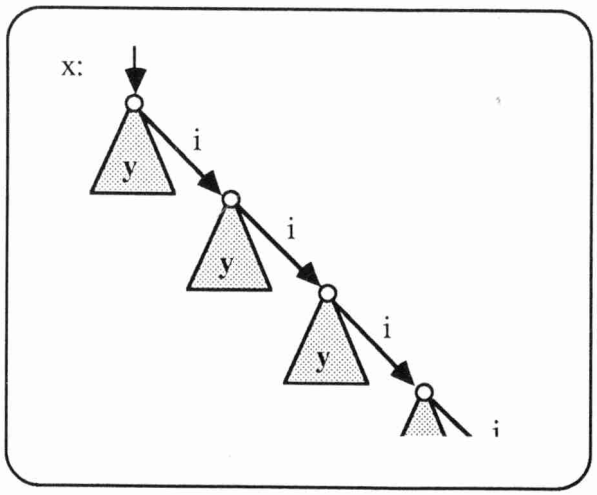


FIG. 19

The version of KFAR for $n=2$ is

$$\frac{x_1 = ix_2 + y_1, \quad x_2 = jx_1 + y_2 \quad (i, j \in I)}{\tau_I(x_1) = \tau \cdot \tau_I(y_1 + y_2)}.$$

In the general formulation of KFAR_n the premise displays an "I-cycle" of length n. For a precise formulation we refer to [BK84b] or [BBK85].

Note that except for KFAR all assumptions in BPA_τ + TI1–TI5 + R1 + RSP are valid for failure semantics. To see that the τ-laws TI1–TI3 (of which only the first one is needed for the derivation of the contradiction below) are valid for failure semantics, we refer to [Br83], which gives axioms describing failure semantics for finite processes involving τ-steps; these axioms imply the τ-laws.

8.2. The inconsistency of failure semantics with KFAR. We will now derive the announced contradiction. It is important to notice that this contradiction is entirely insensitive to how failure semantics works with processes that contain τ-steps.

Consider the following systems of guarded recursion equations:

$$E_1 \begin{cases} x = ax_1 + ax_2, \\ x_1 = c + bx_2, \\ x_2 = d + bx_1, \end{cases}$$

and

$$E_2 \begin{cases} y = ay_1 + ay_2, \\ y_1 = c + by_2, \\ y_2 = d + by_1. \end{cases}$$

The systems E_1, E_2 have solutions x, y which can be depicted as in Fig. 20.

CLAIM: x and y are failure equivalent.

Intuitively this may be clear since (as demonstrated in § 3.1) axiom R1 amounts to placing "crosses"; from the graphs for x, y we can thus obtain equivalent graphs as in Fig. 21. These two graphs are in fact identical.

Proof of the Claim (Formally). Consider the system E_3 of guarded recursion equations:

$$E_3 \begin{cases} z = az_1 + az_2, \\ z_1 = c + bz_1 + bz_2, \\ z_2 = d + bz_1 + bz_2. \end{cases}$$

(This system corresponds with the graph in Fig. 21.) Now

$$\begin{aligned} x = ax_1 + ax_2 &= a(c + bx_2) + a(d + bx_1) \quad \text{(by R1)} \\ &= a(c + bx_2 + bx_1) + a(d + bx_1 + bx_2) = az_1' + az_2' \end{aligned}$$

where

$$z_1' = c + bx_2 + bx_1 \quad \text{and} \quad z_2' = d + bx_1 + bx_2.$$

Further,

$$\begin{aligned} z_1' = c + bx_2 + bx_1 &= c + b(d + bx_1) + b(c + bx_2) \quad \text{(by R1)} \\ &= c + b(c + bx_2 + bx_1) + b(d + bx_1 + bx_2) \\ &= c + bz_1' + bz_2' \end{aligned}$$

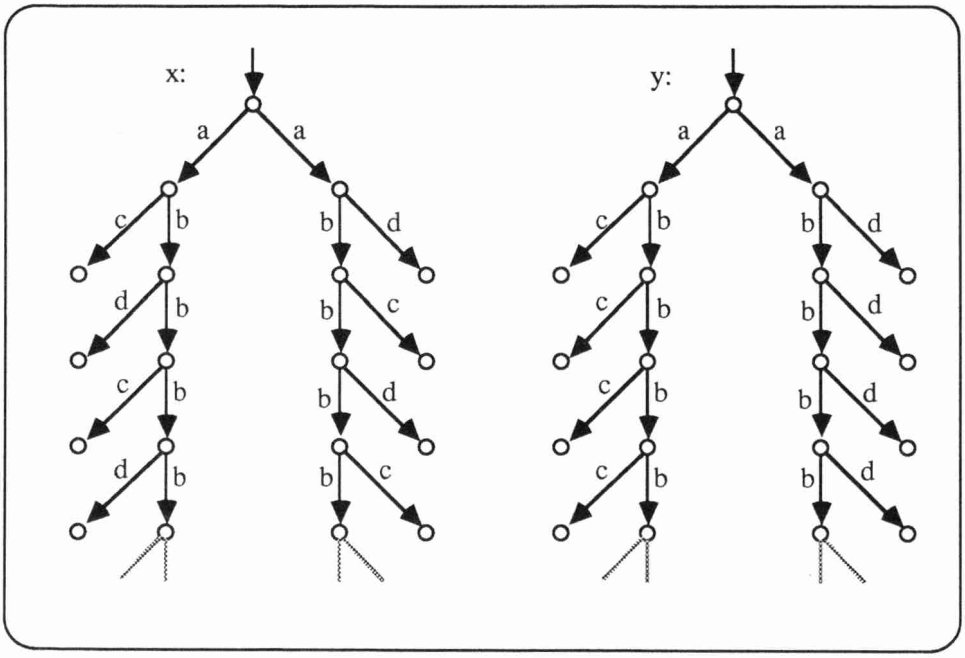


FIG. 20

and likewise

$$z_2' = d + bz_1' + bz_2'.$$

So (x, z_1', z_2') satisfies E_3. A similar computation shows that (y, z_1'', z_2''), where

$$z_1'' = c + by_1 + by_2, \qquad z_2'' = d + by_1 + by_2$$

satisfies E_3. Hence by RSP,

$$(x, z_1', z_2') = (y, z_1'', z_2'') = (z, z_1, z_2),$$

in particular $x = y$. This proves the claim.

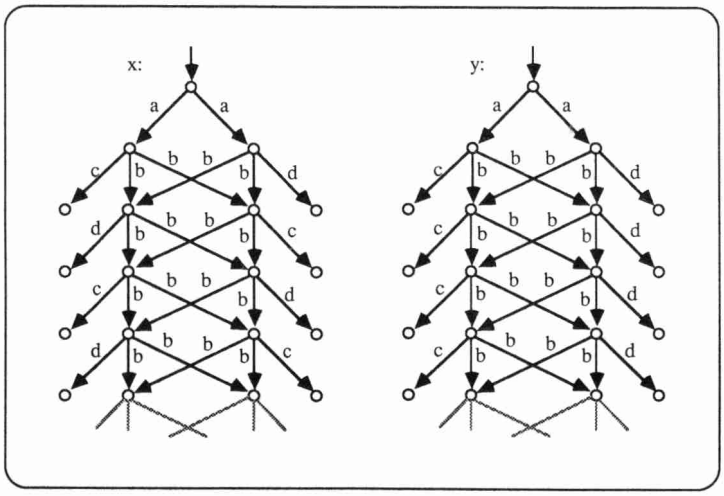


FIG. 21

In order to derive the inconsistency we will abstract from b, by means of $\tau_{\{b\}}$, in x and y. This yields corresponding process graphs as in Fig. 22. Next we apply KFAR on $\tau_{\{b\}}(x)$ and $\tau_{\{b\}}(y)$ and obtain $a(c+d)$ and $ac+ad$, respectively. This can be seen graphically: KFAR shrinks the infinite τ-traces to a point, obtaining the graphs as in Fig. 23.

Formally:

$$(*) \qquad \tau_{\{b\}}(x) = \tau_{\{b\}}(ax_1 + ax_2) = a \cdot \tau_{\{b\}}(x_1) + a \cdot \tau_{\{b\}}(x_2).$$

Further,

$$x_1 = bx_2 + c, \qquad x_2 = bx_1 + d$$

yields by KFAR_2:

$$\tau_{\{b\}}(x_1) = \tau \cdot \tau_{\{b\}}(c+d) = \tau(c+d),$$
$$\tau_{\{b\}}(x_2) = \tau \cdot \tau_{\{b\}}(c+d) = \tau(c+d).$$

Hence from $(*)$

$$\tau_{\{b\}}(x) = a\tau(c+d) + a\tau(c+d) \quad \text{(by T1 in Table 6)},$$
$$= a(c+d) + a(c+d) = a(c+d).$$

Next consider y:

$$(**) \qquad \tau_{\{b\}}(y) = a \cdot \tau_{\{b\}}(y_1) + a \cdot \tau_{\{b\}}(y_2).$$

Now $y_1 = by_1 + c$ yields by KFAR_1: $\tau_{\{b\}}(y_1) = \tau c$; similarly $\tau_{\{b\}}(y_2) = \tau d$. Hence from $(**)$

$$\tau_{\{b\}}(y) = a\tau c + a\tau d = ac + ad.$$

So, since $x = y$, we have proved $a(c+d) = ac + ad$. But $a(c+d)$ and $ac+ad$ are not failure equivalent.

8.3. Further results. The above inconsistency proves that the advantages of Koomen's fair abstraction rule, KFAR, cannot be combined with the simplicity of failure semantics. We investigated this dichotomy further and were pleased to find a weaker

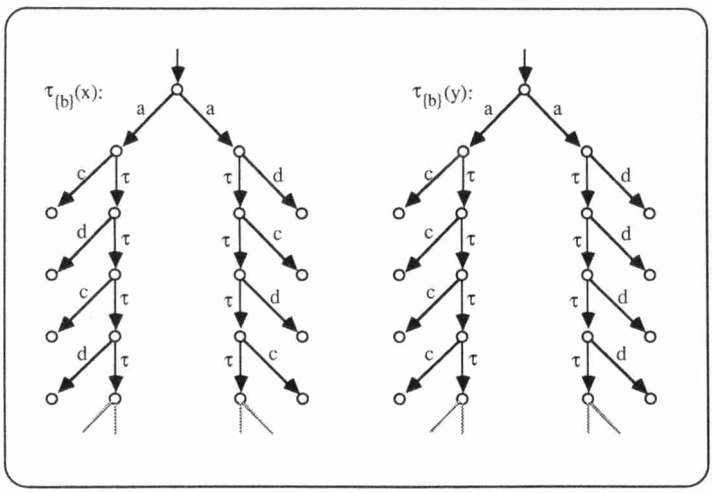


FIG. 22

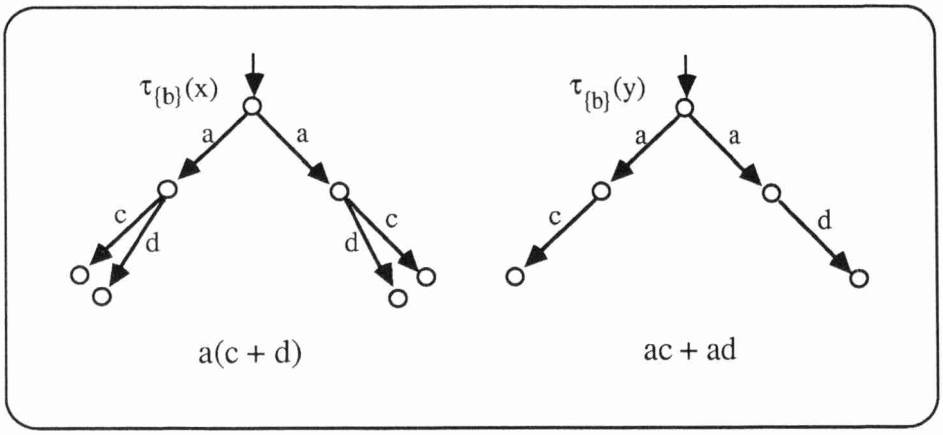


FIG. 23

fair abstraction rule, called KFAR$^-$, which *is consistent* with (finite) failure semantics, and which is still useful for many process verifications. More precisely, the new rule is consistent with a version of Brookes, Hoare, and Roscoe's failure semantics [BHR84] without catastrophic divergence, i.e., that does not identify processes having an infinite τ-sequence from the root with the process CHAOS. The details and applications of the new rule KFAR$^-$ can be found in [BKO86].

Acknowledgment. We thank R. van Glabbeek and one of the referees for pointing out some inconsistencies in a previous version of this paper and for many detailed suggestions and corrections.

REFERENCES

[BBK85] J. C. M. BAETEN, J. A. BERGSTRA, AND J. W. KLOP, *On the consistency of Koomen's Fair Abstraction Rule*, Report CS-R8511, Centre for Mathematics and Computer Science, Amsterdam, the Netherlands, 1985; Theoret. Comput. Sci., 51 (1987), pp. 129–176.

[BK83] J. A. BERGSTRA AND J. W. KLOP, *An abstraction mechanism for process algebras*, Report IW 231/83, Centre for Mathematics and Computer Science, Amsterdam, the Netherlands, 1983.

[BK85] ———, *Algebra of communicating processes with abstraction*, Theoret. Comput. Sci., 37 (1985), pp. 77–121.

[BK84a] ———, *Process algebra for synchronous communication*, Inform. and Control, 60 (1984), pp. 109–137.

[BK84b] ———, *Verification of an alternating bit protocol by means of process algebra*, Report CS-R8404, Centre for Mathematics and Computer Science, Amsterdam, the Netherlands, 1984; also in Math. Methods of Spec. and Synthesis of Software Systems 1985, W. Bibel and K. P. Jantke, eds., Math. Research 31, Akademie-Verlag, Berlin, 1986, pp. 9–23.

[BK84c] ———, *A complete inference system for regular processes with silent moves*, Report CS-R8420, Centre for Mathematics and Computer Science, Amsterdam, the Netherlands, 1984; Proc. Logic Colloquium in Hull, J. Truss and F. Drake, eds., North-Holland, Amsterdam, 1986, pp. 21–81.

[BK86a] ———, *Algebra of Communicating Processes*, in CWI Monographs I, Proc. CWI Symposium on Mathematics and Computer Science, J. W. de Bakker, M. Hazewinkel, and J. K. Lenstra, eds., North-Holland, Amsterdam, 1986, pp. 89–138.

[BK86b] ———, *Process Algebra: Specification and Verification in Bisimulation Semantics*, in CWI Monograph 4, Proc. CWI Symposium Mathematics and Computer Science II, M. Hazewinkel, J. K. Lenstra, and L. G. L. T. Meertens, eds., North-Holland, Amsterdam, 1986, pp. 61–94.

[BKO86] J. A. BERGSTRA, J. W. KLOP, AND E.-R. OLDEROG, *Failures without chaos: a new process semantics for fair abstraction*, in Proc. IFIP Working Conference on Formal Description of Programming Concepts, Gl. Avernaes 1986, M. Wirsing, ed., North-Holland, Amsterdam, 1987, pp. 77-101.

[Br83] S. D. BROOKES, *On the relationship of CCS and CSP*, in Proc. 10th Internat. Colloquium on Automat. Lang. and Programming, Barcelona, J. Díaz, ed., Lecture Notes in Computer Science, 154, Springer-Verlag, New York, Berlin, 1983, pp. 83-96.

[BHR84] S. BROOKES, C. HOARE, AND W. ROSCOE, *A theory of communicating sequential processes*, J. Assoc. Comput. Mach., 31 (1984), pp. 560-599.

[DH84] R. DE NICOLA AND M. C. B. HENNESSY, *Testing equivalences for processes*, Theoret. Comput. Sci., 34 (1984), pp. 83-133.

[He83] M. HENNESSY, *Synchronous and asynchronous experiments on processes*, Inform. and Control, 59 (1983), pp. 36-83.

[HP79] M. HENNESSY AND G. D. PLOTKIN, *Full abstraction for a simple programming language*, in Proc. 8th Mathematical Foundations of Computer Science, J. Becvar, ed., Lecture Notes in Computer Science 74, Springer-Verlag, Berlin, New York, 1979, pp. 108-120.

[Ho78] C. A. R. HOARE, *Communicating sequential processes*, Comm. ACM 21 (1978), pp. 666-677.

[Ho80] ———, *A model for communicating sequential processes*, in On the Construction of Programs, R. M. McKeag and A. M. McNaughton, eds., Cambridge University Press, London, New York, 1980, pp. 229-243.

[Mi77] R. MILNER, *Fully abstract models of typed λ-calculi*, Theoret. Comput. Sci., 4 (1977), pp. 1-22.

[Mi80] R. MILNER, *A Calculus of Communicating Systems*, Lecture Notes in Computer Science 92, Springer-Verlag, New York, Berlin, 1980.

[Mi83] R. MILNER, *Calculi for synchrony and asynchrony*, Theoret. Comput. Sci., 25 (1983), pp. 267-310.

[OH83] E. R. OLDEROG AND C. A. R. HOARE, *Specification-oriented semantics for communicating processes*, in Proc. 10th Internat. Colloquium on Automat. Lang. and Programming, Barcelona, J. Díaz, ed., Lecture Notes in Computer Science 154, Springer-Verlag, New York, Berlin, 1983, pp. 561-572; expanded version, Acta Informatica, 23 (1986), pp. 9-66.

[Pa83] D. M. R. PARK, *Concurrency and automata on infinite sequences*, in Proc. 5th GI (Gesellschaft für Informatik) Conference, Lecture Notes in Computer Science 104, Springer-Verlag, New York, Berlin, 1981.

[Pl77] G. D. PLOTKIN, *LCF considered as a programming language*, Theoret. Comput. Sci., 5 (1977), pp. 223-255.

[RB81] W. C. ROUNDS, AND S. D. BROOKES, *Possible futures, acceptances, refusals, and communicating processes*, in Proc. 22nd IEEE Synposium on Foundations of Computer Science, Nashville, TN (IEEE Computer Society Press, 1981), pp. 140-149.

[VGI88] R. J. VAN GLABBEEK, *Personal communication*, 1988.

[Wi83] G. WINSKEL, *Synchronisation trees*, in Proc. 10th ICALP, Barcelona, J. Díaz, ed., Lecture Notes in Computer Science 154, Springer-Verlag, New York, Berlin, 1983, pp. 695-711; expanded version in Theoret. Comput. Sci., 34 (1984), pp. 33-82.