Correctness and full abstraction of metric semantics for concurrency

J.J.M.M. Rutten

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

ABSTRACT: Four different semantic models are given for a simple uniform programming language, containing constructs for parallel composition, global nondeterminism and communication: linear semantics, failure semantics, readiness semantics, and branching semantics. The mathematical framework used consists of complete metric spaces. All models and operators are given as fixed points of suitably defined contractions. This allows for a uniform presentation and an easy comparison of these models. It is shown that the latter three semantics all are correct and that the failure semantics is fully abstract with respect to the linear semantics. Although these results are not new, we believe the uniformity of the way they are presented here to be of some interest.

KEY WORDS AND PHRASES: concurrency, complete metric spaces, contractions, operational semantics, denotational semantics, compositionality, correctness, full abstraction.

CONTENTS

1. Introduction

The semantics of a uniform programming language $\mathfrak{L}$ is studied, containing the following constructs: atomic actions, which are left uninterpreted and which can be either internal or communications; sequential composition, global nondeterminism and parallel composition; and recursion, modeled via the simultaneous declaration of statement variables. In the context of complete metric spaces, which is the mathematical framework we adopt, this language (and others similar to it) is treated in [BKMOZ86] and [BMOZ88]. There, an operational semantics $\mathfrak{O}$ and a denotational semantics $\mathfrak{D}$ for $\mathfrak{L}$ are presented together with a proof of the correctness of $\mathfrak{D}$ with respect to $\mathfrak{O}$. In [KR88], this proof is simplified: For the denotational semantics an alternative formulation is given, based on the same transition relation which was used for the definition of $\mathfrak{O}$. Then the correctness is proved by showing that both this alternative denotational semantics and $\mathfrak{O}$ are a fixed point of the same contraction, which by Banach's theorem has a unique fixed point.

In this paper, we shall introduce, again in a metric setting, two other semantics for $\mathfrak{L}$, which essentially are the well known readiness semantics ([OH86]) and failure semantics ([BHR84]). For both models, two alternative definitions will be given: an operational one, which is based on a transition relation for $\mathfrak{L}$, and a *compositional* one, using explicit semantic operators. These differently defined models are shown to be equivalent along the lines of [KR88]. Then the readiness and failure semantics are related to $\mathfrak{O}$ and $\mathfrak{D}$: they are less distinctive than $\mathfrak{D}$ is but are (still) correct with respect to $\mathfrak{O}$. The importance of the failure model lies in the fact that it is *fully abstract* with respect to $\mathfrak{O}$, that is, it makes *just enough* distinctions in order to be correct (and thus compositional) with respect to $\mathfrak{O}$. This fact is proved along the lines of the proof of a similar statement in [BKO87].

2. A SIMPLE LANGUAGE

For the definition of $\mathcal{L}$ we introduce a (possibly infinite) set of *elementary actions* $(a,b\in)A$. (Throughout this paper, the notation $(x,y\in)X$ is used for the introduction of a set X ranged over by typical elements x and y.) We assume that A is partioned into $A=I\cup C$, where $(c\in)C$ is the set of *communication* actions and I (disjoint from C) is the set of *internal* actions. Similarly to CCS ([Mil80]) and CSP ([Ho85]), we assume given a bijection $\bar{\ }: C\to C$, which satisfies $\bar{\ }\circ\bar{\ }=id_C$. It yields, for every $c\in C$, a matching communication $\bar{c}$. In I, we have a special element τ denoting successful communication. Further, let $(x\in)Stmv$ be the set of statement variables.

DEFINITION 2.1 (Syntax for $\mathcal{L}$): The set of statements $(s,t\in)\mathcal{L}$ is defined by

$$s::= a\,|\,s_1;s_2\,|\,s_1+s_2\,|\,s_1\|s_2\,|\,x.$$

A statement is of one of five forms: an elementary action $a\in A$, which is either internal $(a\in I)$ or a communication action $(a\in C)$; the sequential composition of statements s_1 and s_2; the nondeterministic choice s_1+s_2, also called global nondeterminism; the parallel composition $s_1\|s_2$, which will be modeled by the arbitrary interleaving (or shuffle) of the elementary actions of s_1 and s_2; and finally a statement variable x, which will be bound to a statement with the use of so-called:

DEFINITION 2.2 (Declarations): The set of *declarations* $(\delta\in)\Delta$ is given by

$$\delta::= \langle x_1\Leftarrow g_1,\ldots,x_n\Leftarrow g_n\rangle,$$

with $n\geqslant 0$, $x_i\in Stmv$, and $g_i\in\mathcal{L}^g$, the set of *guarded statements* which is defined below. We require all variables x_i to be different. We shall sometimes write $x\Leftarrow s\in\delta$ if there exists an $i\in\{1,\ldots,n\}$ with $x_i=x$ and $s_i=s$.

DEFINITION 2.3 (Guarded statements): The set $(g\in)\mathcal{L}^g$ of guarded statements is given by

$$g::= a\,|\,g;s\,|\,g_1+g_2\,|\,g_1\|g_2,$$

where $s\in\mathcal{L}$.

It will be useful to have the languages $\mathcal{L}$ and $\mathcal{L}^g$ contain a special element E, called the *empty statement*. We shall still write $\mathcal{L}$ and $\mathcal{L}^g$ for $\mathcal{L}\cup\{E\}$ and $\mathcal{L}^g\cup\{E\}$. Note that syntactic constructs like $s;E$ or $E\|s$ are *not* in $\mathcal{L}$ or $\mathcal{L}^g$.

A statement g is guarded if all occurrences of statement variables x in g are preceded by some guarded statement g', which by definition has to start with an elementary action. This requirement corresponds to the usual Greibach condition in formal language theory.

In $\mathcal{L}$, recursion is modeled via the simultaneous declaration of statement variables rather than using the μ-formalism, which allows nested constructs like: $\mu x[a;\mu y[x;b+c;y]]$. This limitation is not essential for what follows and entails a considerably more concise semantic treatment of

the language $\mathcal{L}$.

In the next section, we shall define a number of operational semantic models for $\mathcal{L}$ which all are based on the same *transition relation* for $\mathcal{L}$, which we introduce next.

DEFINITION 2.4 (Transition relation for $\mathcal{L}$)
For every declaration $\delta \in \Delta$ we define a transition relation:

$$-\delta\rightarrow \ \subseteq \mathcal{L} \times A \times \mathcal{L}$$

For $(s, a, s') \in -\delta\rightarrow$ we shall write

$$s \overset{a}{\underset{\delta}{-\!\!\!\rightarrow}} s'.$$

Now let $-\delta\rightarrow$ be given as the smallest relation satisfying

(1) $a \overset{a}{\underset{\delta}{-\!\!\!\rightarrow}} E$

(2) if $s \overset{a}{\underset{\delta}{-\!\!\!\rightarrow}} s' \mid E$,

then: $s;\bar{s} \overset{a}{\underset{\delta}{-\!\!\!\rightarrow}} s';\bar{s} \mid \bar{s}$

$s+\bar{s} \overset{a}{\underset{\delta}{-\!\!\!\rightarrow}} s' \mid E$

$\bar{s}+s \overset{a}{\underset{\delta}{-\!\!\!\rightarrow}} s' \mid E$

$s \| \bar{s} \overset{a}{\underset{\delta}{-\!\!\!\rightarrow}} s' \| \bar{s} \mid \bar{s}$

$\bar{s} \| s \overset{a}{\underset{\delta}{-\!\!\!\rightarrow}} \bar{s} \| s' \mid \bar{s}$

$x \overset{a}{\underset{\delta}{-\!\!\!\rightarrow}} s' \mid E$, if $x \Leftarrow s \in \delta$

(3) if $s \overset{c}{\underset{\delta}{-\!\!\!\rightarrow}} s' \mid E$ and $t \overset{\bar{c}}{\underset{\delta}{-\!\!\!\rightarrow}} t'$,

then $s \| t \overset{\tau}{\underset{\delta}{-\!\!\!\rightarrow}} s' \| t' \mid t'$.

(Here one should read "if $s \rightarrow s_1 | s_2$ then $t \rightarrow t_1 | t_2$" as: "if $s \rightarrow s_1$ then $t \rightarrow t_1$" and "if $s \rightarrow s_2$ then $t \rightarrow t_2$".) We shall drop the δ labels on the arrows whenever they do not play a role or it is clear from the context which declaration is meant.

This transition relation gives a first operational interpretation of $\mathcal{L}$. Intuitively, $s \overset{a}{\underset{\delta}{-\!\!\!\rightarrow}} s'$ tells us that s can do the elementary action a as a first step, resulting in the statement s'. In general, we are interested in (possibly infinite) sequences of transitions. We give a few examples:

$$x \overset{a}{\underset{\delta}{-\!\!\!\rightarrow}} x \overset{a}{\underset{\delta}{-\!\!\!\rightarrow}} \cdots, \quad \text{with } x \Leftarrow a;x \in \delta$$

$$c \| \bar{c} \overset{c}{\underset{\delta}{-\!\!\!\rightarrow}} \bar{c} \overset{\bar{c}}{\underset{\delta}{-\!\!\!\rightarrow}} E$$

$$c \| \bar{c} \overset{\tau}{\underset{\delta}{-\!\!\!\rightarrow}} E.$$

We introduce an abbreviation which will be of use in many definitions.

DEFINITION 2.5 (Initial steps): For $s \in \mathfrak{L}$ and $\delta \in \Delta$ we define:

$$Init(s)(\delta) = \{a: \exists s' \in \mathfrak{L}\, [s \overset{a}{-\!\!\!\delta\!\!\!\rightarrow} s']\}.$$

3. FOUR OPERATIONAL MODELS

In this section, we introduce four different semantic models for $\mathfrak{L}$. They are called *operational* because their definitions are based on the transition relation given in definition 2.4. The models vary from a semantics $\mathcal{O}$ which yields sets of streams (or *traces*) as meanings, containing no branching structure at all, via the familiar *ready* and *failure* semantics, to a semantics $\mathcal{O}_B$, which yields tree-like, completely branching structures. (In subsection 3.5, we have collected some examples illustrating the different semantic models.)

3.1 Linear Semantics

We start with the definition of a semantic function $\mathcal{O}$ which is called *linear,* because it yields sets of non-branching streams as the meaning of a statement:

DEFINITION 3.1. ($\mathcal{O}$)
Let $(p,q \in)P = \mathcal{P}(I_\delta^\infty)$, the set of subsets of I_δ^∞; here, the set $(w \in) I_\delta^\infty$ is defined as

$$I_\delta^\infty = I^\infty \cup I^* \cdot \partial$$

(with $I^\infty = I^\omega \cup I^*$), containing all finite and infinite words (or streams) over the alphabet I as well as the set of finite words over I ending in ∂, which is a special symbol not in A that denotes *deadlock.* We define a semantic function

$$\mathcal{O}: \mathfrak{L} \rightarrow \Delta \rightarrow P$$

as follows. Let $s \in \mathfrak{L}$ and $\delta \in \Delta$. We put

$$w \in \mathcal{O}[\![s]\!](\delta)$$

if and only if one of the following conditions is satisfied:

(1) there exist $a_1, \ldots, a_n$ in I and $s_1, \ldots, s_n$ in $\mathfrak{L}$ such that

$$w = a_1 \cdots a_n \wedge s \overset{a_1}{-\!\!\!\delta\!\!\!\rightarrow} s_1 \cdots \overset{a_n}{-\!\!\!\delta\!\!\!\rightarrow} s_n = E$$

(2) there exist $a_1, \ldots, a_n$ in I and $s_1, \ldots, s_n$ in $\mathfrak{L}$, with $s_n \neq E$, such that

$$w = a_1 \cdots a_n \cdot \partial \wedge s \overset{a_1}{-\!\!\!\delta\!\!\!\rightarrow} s_1 \cdots \overset{a_n}{-\!\!\!\delta\!\!\!\rightarrow} s_n \wedge Init(s_n)(\delta) \subset C$$

(3) there exist an infinite sequence $a_1, a_2, \ldots$ in I and an infinite sequence $s_1, s_2, \ldots$ in $\mathfrak{L}$ such that

$$w = a_1 a_2 \cdots \wedge s \overset{a_1}{-\!\!\!\delta\!\!\!\rightarrow} s_1 \overset{a_2}{-\!\!\!\delta\!\!\!\rightarrow} \cdots .$$

A word $w \in \mathcal{O}[\![s]\!](\delta)$ can be an element of I^*, indicating a finite, normally terminating computation starting in s; secondly, if $w \in I^* \cdot \{\partial\}$ it indicates that the computation first preforms the actions in w and next reaches a point (indicated by the statement s_n) from which only single-sided communication actions are possible: this is a situation of deadlock and thus w is followed by ∂; finally, w can be in I^ω, reflecting an infinite computation of s.

We can make P into a complete metric space by defining a suitable distance function on it. This will enable us to give a fixed point characterization of $\mathcal{O}$, which will be of use when relating $\mathcal{O}$ to other semantic models.

DEFINITION 3.2 (Semantic domain P_L)
We supply the set I_∂^∞ with the usual metric d_L, which is given by:

$$d_L(w_1,w_2) = \begin{cases} 0 & \text{if } w_1 = w_2 \\ 2^{-n} & \text{otherwise,} \end{cases}$$

where $n = \max\{k : w_1[k] = w_2[k]\}$ (with $w[k]$ denoting the prefix of w of length k). Next we put

$$(p,q \in)\ P_L = \mathcal{P}_{ncl}(I_\partial^\infty),$$

the set of all non-empty and closed subsets of I_∂^∞, which we supply with the Hausdorff metric $d_{P_L} = (d_L)_H$, induced by d_L (see definition A.6(d)). Since (I_∂^∞, d_L) is a complete metric space, so is (P_L, d_{P_L}). Sometimes we will use A_L to denote the set I_∂^∞.

(In this semantic domain we use the power set of *closed* subsets. For some technical reason, we shall sometimes use *compact* subsets (which are also closed).)

DEFINITION 3.3 (Alternative definition of $\mathcal{O}$)
Let Φ_L: $(\mathcal{L} \to \Delta \to P_L) \to (\mathcal{L} \to \Delta \to P_L)$ be defined as follows. Let $F \in \mathcal{L} \to \Delta \to P_L$, $s \in \mathcal{L}$, and $\delta \in \Delta$. We set: $\Phi_L(F)(E)(\delta) = \{\epsilon\}$; if $s \neq E$ we put

$$\Phi_L(F)(s)(\delta) = \begin{cases} \{\partial\} & \text{if } \mathit{Init}(s)(\delta) \subseteq C \\ \bigcup \{a \cdot F(s')(\delta) : s \xrightarrow{g} s' \wedge a \in I\} & \text{otherwise.} \end{cases}$$

We define:

$$\mathcal{O}_L = \text{Fixed Point}(\Phi_L).$$

It is straightforward to prove that $\Phi_L(F)(s)(\delta)$ is a closed set and that Φ_L is contracting.
Next, we show that $\mathcal{O}_L$ equals $\mathcal{O}$:

THEOREM 3.4 $\mathcal{O}_L = \mathcal{O}$

PROOF: Since Φ_L is a contraction and since contractions have unique fixed points, the result is

immediate from the observation that also Θ is a fixed point of Φ_L, which is proved by the following argument. Let $s \in \mathcal{L}$ and $\delta \in \Delta$. From the fact that there are only a finite number of transitions possible from an arbitrary statement it follows that $\Theta[\![s]\!](\delta)$ is compact and hence closed: It is straightforward to show that in $\Theta[\![s]\!](\delta)$ every sequence has a converging subsequence. Thus Θ is an element of the domain of Φ_L, that is: $\Theta \in \mathcal{L} \to \Delta \to P_L$. Now let $w \in I_\delta^\infty$. For $w = \epsilon$ and $w = \partial$ we have: $w \in \Theta[\![s]\!](\delta) \Leftrightarrow w \in \Phi_L(\Theta)(s)(\delta)$. Otherwise:

$$
\begin{aligned}
w \in \Theta[\![s]\!](\delta) \;\Leftrightarrow\; & [\text{definition } \Theta] \\
& \exists a \in I \exists s' \in \mathcal{L} \exists w' \in I_\delta^\infty \\
& [s \xrightarrow{a}_\delta s' \wedge w' = a \cdot w' \wedge w' \in \Theta[\![s']\!](\delta)] \\
\Leftrightarrow\; & [\text{definition } \Phi_L] \\
& w \in \Phi_L(\Theta)(s)(\delta).
\end{aligned}
$$

Thus $\Theta = \Phi_L(\Theta)$.

The definition of Θ_L as a fixed point of Φ_L required the addition of some (metric) structure to the set $\mathcal{P}(I_\delta^\infty)$. For this we are rewarded with a concise definition on the one hand and an easy tool for comparing Θ_L to other models, Banach's theorem, that is, on the other.

3.2. Branching semantics

We follow [BKMOZ86] in introducing a *branching* time semantics for $\mathcal{L}$. First we have to define a suitable semantic universe. It is obtained as a solution of the following *domain equation*:

$$P \cong \{p_0\} \cup \mathcal{P}_{co}(A \times P). \qquad (*)$$

Such a solution we call a *domain*, and its elements are called *processes*. We can read the equation as follows: a process $p \in P$ is either p_0, the so-called *nil* process indicating termination, or it is a (compact) set X of pairs $<a,q>$, where a is the first action taken and q is the *resumption*, describing the rest of p's actions. If X is the empty set, it indicates deadlock (as does ∂ in the operational semantics). For reasons of cardinality, (*) has no solution when we take *all* subsets, rather than all *compact* subsets of $A \times P$. Moreover, we should be more precise about the metrics involved. We should have written (*) like this:

DEFINITION 3.5 (Semantic universe P_B)
Let (P_B, d_B) be a complete metric space satisfying the following reflexive domain equation:

$$P \cong \{p_0\} \overline{\cup} \mathcal{P}_{co}(A \times id_{1/2}(P)),$$

where, for any positive real number c, id_c maps a metric space (M,d) onto (M,d') with $d'(x,y) = c \cdot d(x,y)$, and $\overline{\cup}$ denotes the *disjoint* union. (For a formal definition of the metric on P we refer the reader to the appendix (definition A.6).) Typical elements of P_B are p and q.

We shall not go into the details of solving this equation. In [BZ82] it was first described how

to solve this type of equations in a metric setting. In [AR88] this approach is reformulated and extended in a category-theoretic setting.

Examples of processes are

$$p_1 = \{<a, \{<b_1,p_0>, <b_2,p_0>\}>\}$$

$$p_2 = \{<a, \{<b_1,p_0>\}>, <a, \{<b_2,p_0>\}>\}.$$

Using this process domain P_B, we introduce a second semantic model for L.

DEFINITION 3.6 ($\mathcal{O}_B$)
Let Φ_B: $(\mathbb{L}\to\Delta\to P_B)\to(\mathbb{L}\to\Delta\to P_B)$ be defined as follows. Let $F\in\mathbb{L}\to\Delta\to P_B$, $s\in\mathbb{L}$, and $\delta\in\Delta$. If $s=E$ we put $\Phi_B(F)(s)(\delta)=p_0$. Otherwise:

$$\Phi_B(F)(s)(\delta) = \{<a, F(s')(\delta)>: s \xrightarrow{a} s'\}.$$

Now we put:

$$\mathcal{O}_B = \text{Fixed Point } (\Phi_B).$$

In defining $\mathcal{O}_B$, we follow [KR88], where (a variant of) $\mathcal{O}_B$ was used as an intermediate model between an operational and a denotational semantics.

Note that $\mathcal{O}_B$ does not signal deadlock explicitly, whereas $\mathcal{O}_L$ does by using ∂. However, the information about possible deadlocks is present in $\mathcal{O}_B[\![s]\!](\delta)$, because it gives the complete branching structure of all possible transition sequences starting in s. In subsection 3.5, it shown how to abstract from this branching structure and to translate it into an explicit representation of deadlock by the application of some abstraction operator.

Further, we observe that $\mathcal{O}_B$ is much more distinctive than $\mathcal{O}_L$ is, precisely because of the preservation of branching information. This is easily illustrated: We have, for $a, b_1, b_2\in I$:

$$\mathcal{O}_L[\![a;(b_1+b_2)]\!] = \mathcal{O}_L[\![(a;b_1)+(a;b_2)]\!] = \{ab_1, ab_2\},$$

as opposed to

$$\mathcal{O}_B[\![a;(b_1+b_2)]\!] = p_1 \neq p_2 = \mathcal{O}_B[\![(a;b_1)+(a;b_2)]\!],$$

with p_1 and p_2 as defined above.

We finish this subsection with a reference to [BK87], where a comparison is made between P_B and models based on process graphs.

3.3. Readiness semantics

Next, we introduce a semantics $\mathcal{O}_R$ which is based on the notion of *ready sets,* introduced in [OH86]. It is intermediate between $\mathcal{O}_L$ and $\mathcal{O}_B$ in the sense that it makes more distinctions than $\mathcal{O}_L$ and less distinctions than $\mathcal{O}_B$ makes. Moreover, unlike $\mathcal{O}_L$ it does not yield only streams but contains already some branching information (but less than is present in $\mathcal{O}_B$): Instead of using a single symbol to denote all possible deadlock situations, in $\mathcal{O}_R$ this information is refined by yielding in case of deadlock the set of all single-sided communication actions that could have been taken next (if only a matching communication partner for one of these were to be offered in parallel).

The formal definition of $\mathcal{O}_R$ can be given similarly to definition 3.1, using sequences of transitions. We leave such a formulation to the enthusiastic reader and continue with a fixed point definition in the style of definitions 3.3 and 3.6. First, we introduce a complete metric space of ready sets:

DEFINITION 3.7 (Ready domain P_R): Let $(\pi\in)\mathcal{A}_R$ be given by

$$A_R = A^\infty \cup A^* \cdot \mathcal{P}(C)$$
$$= A^* \cup A^\omega \cup A^* \cdot \mathcal{P}(C).$$

Elements of A^∞ are indicated by w. Elements of $A^* \cdot \mathcal{P}(C)$ will be denoted by (w,X) (rather than $w \cdot X$) and are called *ready pairs.* The set A_R is supplied with the usual metric d_R (see definition 3.2), in the definition of which $\mathcal{P}(C)$, the set of all subsets of C, is regarded as an alphabet. Next we define

$$(p,q\in)\ \ P_R = \mathcal{P}_{nco}(A_R),$$

the set of non-empty compact subsets of A_R, which we supply with $d_{P_R} = (d_R)_H$, the Hausdorff metric induced by d_R. We have that (P_R, d_{P_R}) is a complete metric space. The elements of P_R are called *ready sets.*

DEFINITION 3.8 ($\mathcal{O}_R$)
We define a mapping $\Phi_R : (\mathcal{L} \to \Delta \to P_R) \to (\mathcal{L} \to \Delta \to P_R)$. Let $F \in \mathcal{L} \to \Delta \to P_R$, $s \in \mathcal{L}$, and $\delta \in \Delta$. We put $\Phi_R(F)(E)(\delta) = \{\epsilon\}$. Otherwise:

$$\Phi_R(F)(s)(\delta) = \bigcup \{a \cdot F(s')(\delta) :\ s \xrightarrow{\delta} s'\} \cup \{(\epsilon,\ Init(s)(\delta)) :\ Init(s)(\delta) \subseteq C\}.$$

(Here $a \cdot V$ is defined by $a \cdot V = \{a \cdot w :\ w \in V\} \cup \{(a \cdot w, X) : (w,X) \in V\}$.) Now we set

$$\mathcal{O}_R = \text{Fixed Point } (\Phi_R).$$

We observe that $\mathcal{O}_R[\![s]\!](\delta)$ contains streams which are words over A rather than over I only. In other words, single-sided communication actions are visible. Further, as is indicated above, deadlock information in $\mathcal{O}_R[\![s]\!](\delta)$ is represented by ready pairs (w,X), which are interpreted as

follows: After performing the actions in w, the computation has reached a point from which it can only perform communication actions; these are listed in X.

3.4. Failure semantics

The fourth model we introduce for $\mathfrak{L}$ is a semantics $\mathcal{O}_F$ which is based on *failure sets,* as introduced in [BHR84]. It is, like $\mathcal{O}_B$, more distinctive than $\mathcal{O}_L$ but less than $\mathcal{O}_R$ is. Instead of ready pairs the function $\mathcal{O}_F$ yields *failure pairs* (w,X), which are again elements of $A^* \cdot \mathcal{P}(C)$, but now have a different interpretation: The set X is called a *refusal set* and contains those communication actions (but not necessarily all) that are to be refused, even if a matching communication would be offered in parallel. The complete metric space of *failure sets* is given in:

DEFINITION 3.9 (Failure domain P_F)
Let $(\pi\in)A_F=A_R$, which was given in definition 3.7. As a metric on A_F we take $d_F=d_R$. We set:

$$(p,q\in)\ \ P_F = \{V\colon V\subseteq A_F \wedge V \text{ is closed in } (A_F,d_F) \wedge \ V \text{ is downward closed }\},$$

where

$$V \text{ is downward closed} \Leftrightarrow$$

$$\forall w\in A^*\ \forall X,\ X'\in\mathcal{P}(C)\ [(w,X)\in V \wedge X'\subseteq X \Rightarrow (w,X')\in V].$$

The pair (P_F,d_{P_F}) (with $d_{P_F}=(d_F)_H$) is a complete metric space. Elements of P_F are called *failure sets.*

DEFINITION 3.10 ($\mathcal{O}_F$)
Let $\Phi_F\colon(\mathfrak{L}\to\Delta\to P_F)\to(\mathfrak{L}\to\Delta\to P_F)$ be given as follows. Let $G\in\mathfrak{L}\to\Delta\to P_F$, $s\in\mathfrak{L}$, and $\delta\in\Delta$. We put $\Phi_F(G)(E)(\delta)=\{\epsilon\}$. If $s\neq E$, then:

$$\Phi_F(G)(s)(\delta) = \bigcup\{a\cdot F(s')(\delta)\colon s-\!\!\{a\}\!\!\to s'\}$$

$$\cup\ \{(\epsilon,X)\colon X\subseteq C-\mathit{Init}(s)(\delta) \wedge \mathit{Init}(s)(\delta)\subseteq C\}.$$

(Here $-$ indicates the set-theoretic difference.) We define:

$$\mathcal{O}_F = \text{Fixed Point}(\Phi_F).$$

The fact that $\mathcal{O}_F$ is *less* distinctive than $\mathcal{O}_R$ is caused by the taking of the downward closure of $C-\mathit{Init}(s)(\delta)$ in the definition of $\mathcal{O}_F$ above. In a moment (in subsection 3.5) we shall see some examples illustrating the difference between $\mathcal{O}_F$ and $\mathcal{O}_R$.

A model isomorphic to $\mathcal{O}_F$ could be obtained in term of ready sets only by taking the *upward* closure, which could be defined similarly to the downward closure, of the ready sets in $\mathcal{O}_R[\![s]\!](\delta)$. Nevertheless, the separate notion of refusal sets has been introduced, because taking the downward closure of a refusal set can be nicely explained in intuitive terms: If, at a certain moment in

a computation, a set of communications may be refused, then every subset of that set may be refused as well.

3.5. Some examples

Consider the following statements in $\mathfrak{L}$ (with $a,b \in I$, $c_1, c_1 \in C$):

$$s_1 = a;b;(c_1 + c_2)$$

$$s_2 = (a;b;c_1) + (a;b;(c_1 + c_2)) + (a;b;c_2)$$

$$s_3 = (a;b;c_1) + (a;b;c_2)$$

$$s_4 = a;((b;c_1) + (b;c_2)).$$

We list the meaning of these statements according to the different semantic functions. (We omit the δ arguments because these do not matter here, a convention we shall use whenever we see the opportunity for doing so without causing confusion.)

(1)

$$\mathcal{O}_L[\![s_1]\!] = \{ab\partial\}$$

$$\mathcal{O}_F[\![s_1]\!] = \{abc_1, abc_2\} \cup \{(ab, X)\colon X \subseteq C - \{c_1 c_2\}\}$$

$$\mathcal{O}_R[\![s_1]\!] = \{abc_1, abc_2, (ab, \{c_1, c_2\})\}$$

$$\mathcal{O}_B[\![s_1]\!] = \{<a, \{<b, \{<c_1, p_0>, <c_2, p_0>\}>\}>\}$$

(2)

$$\mathcal{O}_L[\![s_2]\!] = \mathcal{O}_L[\![s_1]\!]$$

$$\mathcal{O}_F[\![s_2]\!] = \{abc_1, abc_2\} \cup \{ab, X)\colon X \subseteq C - \{c_1\}\} \cup \{(ab, X)\colon X \subseteq C - \{c_2\}\}$$

$$\mathcal{O}_R[\![2]\!] = \{abc_1, abc_2, (ab, \{c_1\}), (ab, \{c_2\}), (ab, \{c_1, c_2\})\}$$

$$\mathcal{O}_B[\![s_2]\!] = \{<a, \{<b, \{<c_1, p_0>\}>\}>,$$
$$<a, \{<b, \{<c_1, p_0>, <c_2, p_0>\}>\}>,$$
$$<a, \{<b, \{<c_2, p_0>\}>\}>\}$$

(3)

$$\mathcal{O}_L[\![s_3]\!] = \mathcal{O}_L[\![s_2]\!] = \mathcal{O}_L[\![s_1]\!]$$

$$\mathcal{O}_F[\![s_3]\!] = \mathcal{O}_F[\![s_2]\!]$$

$$\mathcal{O}_R[\![s_3]\!] = \{abc_1, abc_2, (ab, \{c_1\}), (ab, \{c_2\})\}$$

$$\mathcal{O}_B[\![s_3]\!] = \{<a, \{<b, \{<c_1, p_0>\}>\}>, <a, \{<b, \{<c_2, p_0>\}>\}>\}$$

(4)

$$\mathcal{O}_L[\![s_4]\!] = \mathcal{O}_L[\![s_3]\!] = \mathcal{O}_L[\![s_2]\!] = \mathcal{O}_L[\![s_1]\!]$$

$$\mathcal{O}_F[\![s_4]\!] = \mathcal{O}_F[\![s_3]\!] = \mathcal{O}_F[\![s_2]\!]$$

$$\mathcal{O}_R[\![s_4]\!] = \mathcal{O}_R[\![s_3]\!]$$

$$\mathcal{O}_B[\![s_4]\!] = \{<a, \{<b, \{<c_1, p_0>\}>, <b, \{<c_2, p_0>\}>\}>\}$$

We see that from $\mathcal{O}_L$ to $\mathcal{O}_B$ the semantics get more distinctive.

3.6. Relating the different operational models

We can compare our four operational semantics via some abstraction operators which connect their respective domains:

DEFINITION 3.11 (Abstraction operators): We define three mappings

$$P_B \overset{\alpha_R}{\to} P_R \overset{\alpha_F}{\to} P_F \overset{\alpha_L}{\to} P_L$$

as follows:

(1) α_R: $P_B \to P_R$: We put $\alpha_R(p_0) = \{\epsilon\}$, and $\alpha_R(\varnothing) = \{(\epsilon, \varnothing)\}$. Otherwise:

$$\alpha_R(p) = \bigcup \{a \cdot (\alpha_R(p')) : <a, p'> \in p\} \cup \{(\epsilon, \{c : \exists p' \in P_B\, [<c, p'> \in p]\}) : p \subseteq C \times P_B\}$$

(2) α_F: $P_R \to P_F$:

$$\alpha_F(p) = \{w : w \in p\} \cup \{(w, Y) : \exists X \in \mathcal{P}(C)\, [Y \subseteq C - X \wedge (w, X) \in p]\}$$

(3) α_L: $P_F \to P_L$:

$$\alpha_L(p) = \{w : w \in p \cap I^\infty\} \cup \{w \cdot \partial : w \in I^* \wedge \exists X \in \mathcal{P}(C)\, [(w, X) \in p]\}.$$

The definition of the first operator, α_R, is self-referential since $\alpha_R(p')$ occurs in the definition of $\alpha_R(p)$. It can, however, be correctly defined as the fixed point of the following contraction:

$$\theta : (P_B \to^1 P_R) \to (P_B \to^1 P_R)$$

(where $P_B \to^1 P_R$ is the set of non-expansive (see definition A.3(c)) functions from P_B to P_R), which is given by:

$$\theta(f)(p) = \bigcup \{a \cdot (f(p')) : <a, p'> \in p\} \cup \{(\epsilon, \{c : \exists p' \in P_B [<c, p'> \in p]\}) : p \subseteq C \times P_B\},$$

for $f \in P_B \to^1 P_R$ and $p \in P_B$. We observe (without proof) that $\theta(f)(p)$ is a compact set and that θ is indeed contracting. Now we can take α_R = Fixed Point(θ).

The mapping α_R yields, for a given process $p \in P_B$, all its paths (or streams), and translates the deadlock information which p contains into ready pairs: if $p \subseteq C \times P_B$, that is, if p contains only

pairs with a communication action as the first component, then we have a deadlock situation since, according to our operational intuition, no single-sided communications are allowed. Therefore, α_R delivers in that case the ready pair $(\epsilon, \{c: \exists p' \in P_B\ [<c,p'> \in p]\})$.

The operator α_F translates ready pairs (w,X) into the downward closure of a corresponding failure pair $(w, C-X)$:

$$\alpha_F(\{(w, X)\}) = \{(w, Y): Y \subseteq C - X\}.$$

Finally, the mapping α_L distracts from a failure set $p \in P_F$ those streams that contain only internal actions, and maps failure pairs (w,X) (with $w \in I^*$) onto words $w \cdot \partial$: The deadlock information represented by the set X is replaced by the symbol ∂.

With these mappings we can easily formulate the precise relationship between our operational models:

THEOREM 3.12

The following rectangle commutes, which is indicated by the symbol * :

$$\begin{array}{lcl}
 & \overset{\Phi_B}{\rightarrow} & \\
\mathfrak{L}\to\Delta\to P_B & \rightarrow & \mathfrak{L}\to\Delta\to P_B \\
\alpha_R\downarrow & *_1 & \downarrow\alpha_R \\
 & \overset{\Phi_R}{\rightarrow} & \\
\mathfrak{L}\to\Delta\to P_R & \rightarrow & \mathfrak{L}\to\Delta\to P_R \\
\alpha_F\downarrow & *_2 & \downarrow\alpha_F \\
 & \overset{\Phi_F}{\rightarrow} & \\
\mathfrak{L}\to\Delta\to P_F & \rightarrow & \mathfrak{L}\to\Delta\to P_F \\
\alpha_L\downarrow & *_3 & \downarrow\alpha_L \\
 & \overset{\Phi_L}{\rightarrow} & \\
\mathfrak{L}\to\Delta\to P_L & \rightarrow & \mathfrak{L}\to\Delta\to P_L
\end{array}$$

(where the operators α are extended to sets of functions in the obvious way; for instance,

$$\alpha_R: (\mathfrak{L}\to\Delta\to P_B)\to(\mathfrak{L}\to\Delta\to P_R)$$

is defined by

$$\alpha_R(F) = \lambda s \in \mathfrak{L} \lambda \delta \in \Delta \cdot\ \alpha_R(F(s)(\delta))).$$

PROOF: We only show $*_1$, the other cases being similar. We prove, for all $F \in \mathfrak{L}\to\Delta\to P_B$, $s \in \mathfrak{L}$, and $\delta \in \Delta$:

$$\alpha_R(\Phi_B(F)(s)(\delta)) = \Phi_R(\alpha_R(F))(s)(\delta).$$

For $s \neq E$ we have:

$$\begin{aligned}
\Phi_R(\alpha_R(F))(s)(\delta) &= \bigcup \{a \cdot (\alpha_R(F)(s)(\delta)): s \overset{a}{\underset{\delta}{\rightarrow}} s'\} \cup \{(\epsilon, \mathit{Init}(s)): \mathit{Init}(s) \subseteq C\} \\
&= \alpha_R(\{<a, F(s')(\delta)>: s \overset{a}{\underset{\delta}{\rightarrow}} s'\})
\end{aligned}$$

$$= \alpha_R(\Phi_B(F)(s)(\delta)).$$

4. Three compositional models

We proceed with the introduction of three semantic models in a compositional way:

Definition 4.1 (Compositionality)
Let $\mathcal{M}:\mathcal{L}\to S$ be an arbitrary model for $\mathcal{L}$, with S an arbitrary set. We call $\mathcal{M}$ *compositional* (with respect to $\mathcal{L}$) if there exist operators $;^{\mathcal{M}}, +^{\mathcal{M}}$, and $\|^{\mathcal{M}}: S\times S\to S$ such that

$$\forall s,t\in\mathcal{L}\,[\mathcal{M}(s\ op\ t) = \mathcal{M}(s)\ op^{\mathcal{M}}\ \mathcal{M}(t)],$$

for $op = ;,\ +,\ \|$.

In section 6, a relation between compositionality and the notion of a congruence relation is given (theorem 6.3). The models to be defined in this section, which will be called C_B, C_R and C_F, turn out to be equal to $\mathcal{O}_B, \mathcal{O}_R$, and $\mathcal{O}_F$, respectively, as will be proved in the next section. Therefore, their definitions can be seen as alternative characterizations of the operational models. We do *not* give a compositional version of $\mathcal{O}_L$ since this is impossible (see the remark following theorem 6.4).

Definition 4.2 (C_B, C_R, C_F)
Let λ be a label ranging over the set $\{B, R, F\}$. We define three compositional models for $\mathcal{L}$ as follows. Let $\delta\in\Delta$. Then:

(1) $\mathcal{C}_B[\![E]\!](\delta) = p_0$

$\mathcal{C}_R[\![E]\!](\delta) = \mathcal{C}_F[\![E]\!](\delta) = \{\epsilon\}$

(2) $\mathcal{C}_B[\![a]\!](\delta) = \{<a, p_0>\}$

$$\mathcal{C}_R[\![a]\!](\delta) = \begin{cases}\{a\} & \text{if } a\in I\\ \{a, (\epsilon, \{a\})\} & \text{if } a\in C\end{cases}$$

$$\mathcal{C}_F[\![a]\!](\delta) = \begin{cases}\{a\} & \text{if } a\in I\\ \{a\}\cup\{(\epsilon, X)\colon X\subseteq C-\{a\}\} & \text{if } a\in C\end{cases}$$

(3) $\mathcal{C}_\lambda[\![s\ op\ t]\!](\delta) = \mathcal{C}_\lambda[\![s]\!](\delta)\ op^\lambda \mathcal{C}_\lambda[\![t]\!](\delta)$

with op ranging over the set $\{;, +, \|\}$ and the operator op^λ as given in definition 4.4 below.

(4) $\mathcal{C}_\lambda[\![x]\!](\delta) = \mathcal{C}_\lambda[\![g]\!](\delta)$, for $x\Leftarrow g\in\delta$.

The above definitions need some justification, since $\mathcal{C}_\lambda$ cannot be defined by a simple induction on the syntactic complexity of statements, as is apparent from clause (4) above. We give a formally correct definition of $\mathcal{C}_B$; the definitions of $\mathcal{C}_R$ and $\mathcal{C}_F$ can be treated similarly. (The occupied or impatient reader may wish to skip this part and continue with definition 4.4; it is not crucial for the understanding of the rest of the paper.)

We give $\mathcal{C}_B$ as the unique fixed point of a contraction

$$\Psi_B;\ (\mathfrak{L}\to\Delta\to P_B)\to(\mathfrak{L}\to\Delta\to P_B),$$

which is defined as follows. Let $F\in\mathfrak{L}\to\Delta\to P_B$. We define $\Psi_B(F)$ in two stages: first for all $g\in\mathfrak{L}^g$ and next for arbitrary s in $\mathfrak{L}\,(\supseteq\mathfrak{L}^g)$. We follow the inductive structure of $\mathfrak{L}^g$; let $\delta\in\Delta$, then:

$$\Psi_B(F)(E)(\delta) = p_0$$

$$\Psi_B(F)(a)(\delta) = \{<a, p_0>\}$$

$$\Psi_B(F)(g;s)(\delta) = \Psi_B(F)(g)(\delta);^B F(s)(\delta)$$

$$\Psi_B(F)(g_1+g_2)(\delta) = \Psi_B(F)(g_1)(\delta)+^B \Psi_B(F)(g_2)(\delta)$$

$$\Psi_B(F)(g_1\|g_2)(\delta) = \Psi_B(F)(g_1)(\delta)\|^B \Psi_B(F)(g_2)(\delta).$$

Next, we extend this definition to $\mathfrak{L}$, following the inductive structure of $\mathfrak{L}$. We formulate the only new case: We have to add a clause for statement variables. Suppose $x\Leftarrow g\in\delta$. Then:

$$\Psi_B(F)(x)(\delta) = \Psi_B(F)(g)(\delta).$$

This is well defined, since $g\in\mathfrak{L}^g$ and $\Psi_B(F)$ is already defined on $\mathfrak{L}^g$. Now we can take $\mathcal{C}_B$ as the fixed point of Ψ_B as soon as we shall have verified that Ψ_B is a contraction:

THEOREM 4.3: *Ψ_B is a contraction on $\mathfrak{L}\to\Delta\to P_B$*

PROOF: We prove that Ψ_B is contracting by showing, for all $F_1, F_2\in\mathfrak{L}\to\Delta\to P_B$, $s\in\Delta$, that:

$$d_{P_B}(\Psi_B(F_1)(s)(\delta),\ \Psi_B(F_2)(s)(\delta)) \leqslant \tfrac{1}{2}\cdot d_{\mathfrak{L}\to\Delta\to P_B}(F_1, F_2). \qquad (*)$$

Let F_1 and F_2 be in $\mathfrak{L}\to\Delta\to P_B$. The proof falls apart into two parts: first $g\in\mathfrak{L}^g$ is treated, next $s\in\mathfrak{L}$. For $\mathfrak{L}^g$ we only consider the most interesting case: suppose $g\in\mathfrak{L}^g-\{E\}$, $s\in\mathfrak{L}$ and $\delta\in\Delta$, such that (*) holds for g. The following argument shows that we also have (*) for $g;s$:

$$d_{P_B}(\Psi_B(F_1)(g;s)(\delta),\ \Psi_B(F_2)(g;s)(\delta))$$

$$= d_{P_B}(\Psi_B(F_1)(g)(\delta);^B F_1(s)(\delta),\ \Psi_B(F_2)(g)(\delta);^B F_2(s)(\delta))$$

$$\leqslant \text{[by lemma 4.5 (2), below]}$$

$$\max\{d_{P_B}(\Psi_B(F_1)(g)(\delta),\ \Psi_B(F_2)(g)(\delta)),\ \tfrac{1}{2}\cdot d_{P_B}(F_1(s)(\delta),\ F_2(s)(\delta))\}$$

$\leqslant$ [induction hypothesis for g]

$\frac{1}{2}\cdot d_{\mathcal{L}\to\Delta\to P_B}(F_1, F_2)$.

The other operators, + and $\|$ can be treated similarly. Once the proof has been given for $\mathcal{L}^g$, it can be easily extended to $\mathcal{L}$ by adding the following proof for $x \in Stmv$. Suppose $x \Leftarrow g \in \delta$, with $g \in \mathcal{L}^g$. Then:

$$d_{P_B}(\Psi_B(F_1)(x)(\delta), \Psi_B(F_2)(x)(\delta)) = d_{P_B}(\Psi_B(F_1)(g)(\delta), \Psi_B(F_2)(g)(\delta))$$

$$\leqslant \text{[induction, since } g \in \mathcal{L}^g \text{]}$$

$$\frac{1}{2}\cdot d_{\mathcal{L}\to\Delta\to P_B}(F_1, F_2),$$

which concludes the proof. □

Next, we introduce the semantic operators.

DEFINITION 4.4 (Semantic operators)
Let λ range over $\{B,R,F\}$ and op over $\{;,+,\|\}$. We define semantic operators $op^\lambda: P_\lambda \times P_\lambda \to P_\lambda$.
(1) $op^B: P_B \times P_B \to P_B$

$$p_0 ;^B q = q$$

$$p ;^B q = \{<a, p' ;^B q> : <a, p'> \in p\}, \text{ for } p \neq p_0$$

$$p_0 +^B q = q +^B p_0 = q$$

$$p +^B q = p \cup q \text{ (set theoretic union) for } p,q \in p_B - \{p_0\}$$

$$p \|^B q = p \between^B q \cup q \between^B p \cup p |^B q,$$

where $p_0 \between^B q = q$

$$p \between^B q = \{<a, p' \|^B q> : <a, p'> \in p\}, \text{ for } p \neq p_0$$

$$p |^B q = \{<\tau, p' \|^B q'> : <c, p'> \in p \wedge <\bar{c}, q'> \in q\}$$

($\between$ is called the *left-merge* operator and | is called the *communication merge*);
(2) $op^R: P_R \times P_R \to P_R$

$$p ;^R q = \{a \cdot (p_a ;^R q) : p_a \neq \varnothing\} \cup \{(\epsilon, X) : (\epsilon, X) \in p\}$$

$$\cup \text{ (if } \epsilon \in p \text{ then } q \text{ else } \varnothing \text{ fi)}$$

where $p_a = \{\pi : \pi \in A_R \wedge a \cdot \pi \in p\}$, for $a \in A$,

with $a \cdot w$, for $w \in A^\infty$, as usual and $a \cdot (w, X) = (a \cdot w, X)$;

$$p +^R q = \{a \cdot p_a : p_a \neq \emptyset\} \cup \{a \cdot q_a : q_a \neq \emptyset\} \cup \{(\epsilon, X \cup Y) : (\epsilon, X) \in p \wedge (\epsilon, Y) \in q\};$$

(note that this definition is equivalent to

$$p +^R q = ((p \cup q) \cap (A^\infty \cup \{(w, X) : w \neq \epsilon\})) \cup \{(\epsilon, X \cup Y) : (\epsilon, X) \in p \wedge (\epsilon, Y) \in q\});$$

$$p \| ^R q = p \lfloor\!\lfloor ^R q \cup q \lfloor\!\lfloor ^R p \cup p |^R q \cup p \#^R q,$$

where $p \lfloor\!\lfloor ^R q = \bigcup \{a \cdot (p_a \| ^R q) : p_a \neq \emptyset\} \cup$ (if $\epsilon \in p$ then q else $\emptyset$ fi)

$$p |^R q = \bigcup \{\tau \cdot (p_c \| ^R q_{\overline{c}}) : p_c \neq \emptyset \neq q_{\overline{c}}\}$$

$$p \#^R q = \{(\epsilon, X \cup Y) : (\epsilon, X) \in p \wedge (\epsilon, Y) \in q \wedge X \cap \overline{Y} = \emptyset\}$$

(here $\overline{Y} = \{\overline{c} : c \in Y\}$);

(3) $op^F : P_F \times P_F \to P_F$

$$p ;^F q = p ;^R q$$

$$p +^F q = \{a \cdot p_a : p_a \neq \emptyset\} \cup \{a \cdot q_a : a_a \neq \emptyset\} \cup \{(\epsilon, X) : (\epsilon, X) \in p \cap q\}$$

$$p \| ^F q = p \lfloor\!\lfloor ^F q \cup q \lfloor\!\lfloor ^F p \cup p |^F q \cup p \#^F q$$

where $p \lfloor\!\lfloor ^F q = p \lfloor\!\lfloor ^R q$

$$p |^F q = p |^R q$$

$$p \#^F q = \{(\epsilon, X) : \exists (\epsilon, Z_1) \in p \exists (\epsilon, Z_2) \in q$$

$$[(C - Z_1) \cap \overline{(C - Z_2)} = \emptyset \wedge X \subseteq Z_1 \cap Z_2]\}.$$

By now, it will not come as a complete surprise that those operators above that are introduced by a self-referential definition (like $;^B$ and $\|^B$) can be formally defined as the fixed point of a suitably defined contraction (cf. the remark following definition 3.11).

The intuitive interpretation of the operators op^B is straightforward. Let us explain briefly the operators op^R and op^F.

The definition of $;^R$ implies that for all w, $w' \in A^*$, $X \in \mathcal{P}(C)$, and $q \in P_R$:

$$\{(w, X)\} ;^R q = \{(w, X)\} \text{ and } \{w\} ;^R \{(w', X)\} = \{(w \cdot w', X)\},$$

just as one would expect. The process $p +^R q$ can deadlock in its first step only if both p and q can deadlock immediately, that is, if both contain a ready pair of the form (ϵ, X). In all subsequent steps, $p +^R q$ behaves like $p \cup q$. In the definition of $p \|^R q$, the interleaving of actions of p and q is represented by $p \lfloor\!\lfloor ^R q$ and $q \lfloor\!\lfloor ^R p$. The communication between p and q are presented in $p |^R q$. Finally, $p \#^R q$ describes the immediate deadlock behavior of $p \|^R q$: if $(\epsilon, X) \in p$ and $(\epsilon, Y) \in q$ we include the ready pair $(\epsilon, X \cup Y)$ in $p \|^R q$ only if $X \cap \overline{Y} = \emptyset$. If $X \cap \overline{Y} \neq \emptyset$, then a communication between p and q is possible and hence the process $p \|^R q$ cannot deadlock

immediately.

The definition of $p +^F q$ is like $p +^R q$ but for the difference that a failure pair (ϵ, X) is included only when $(\epsilon, X) \in p$ and $(\epsilon, X) \in q$: The communications that the process $p +^F q$ can refuse are those that can be refused by both p and q. Note that the downward closedness of $p +^F q$ follows from the downward closedness of p and q. The definition of $p \#^F q$ is very similar to $p \#^R q$. We observe that $p \#^F q$ is downward closed by definition. The following alternative definition of $p \#^F q$, which is simpler, would *not* do:

$$p(\#^F)'q = \{(\epsilon, X \cap Y) : (\epsilon, X) \in p \wedge (\epsilon, Y) \in q \wedge X \cap \overline{Y} = \varnothing\},$$

since it is not downward closed.

The next lemma, which can be easily verified, states some useful (with respect to, e.g., theorem 4.3) properties of the semantic operators:

LEMMA 4.5

(1) *For* $\lambda \in \{B, R, F\}$ *and* $op \in \{;, +, \|\}$: op^λ *is non-expansive (see definition A.3(c)).*

(2) *For* $p, p' \in P_B - \{p_0\}$ *and* $q, q' \in P_B$:

$$d_{P_B}(p ;^B q, p' ;^B q') \leqslant \max\{d_{P_B}(p,p'), \tfrac{1}{2} \cdot d_{P_B}(q,q')\}.$$

For $\lambda \in \{R, F\}, p, p' \in P_\lambda$ *with* $\epsilon \notin p$ *and* $\epsilon \notin p'$, *and* $q, q' \in P_\lambda$:

$$d_{P_\lambda}(p ;^\lambda q, p' ;^\lambda q') \leqslant \max\{d_{P_\lambda}(p,p'), \tfrac{1}{2} \cdot d_{P_\lambda}(q,q')\}.$$

We conclude this section by stating some properties of $\mathcal{C}_R$ and $\mathcal{C}_F$, which can be easily verified with induction on the complexity of statements. They are of use when comparing $\mathcal{C}_R$ and $\mathcal{C}_F$ with $\mathcal{O}_R$ and $\mathcal{O}_F$ (section 5).

LEMMA 4.6

(1) $\forall X \in \mathcal{P}(C)\ \forall s \in \mathcal{L}\ \forall \delta \in \Delta\ [(\epsilon, X) \in \mathcal{C}_R[\![s]\!](\delta) \Leftrightarrow X = Init(s)(\delta)]$

(2) $\forall X \in \mathcal{P}(C)\ \forall s \in \mathcal{L}\ \forall \delta \in \Delta\ [(\epsilon, X) \in \mathcal{C}_F[\![s]\!](\delta) \Leftrightarrow X \subseteq C - Init(s)(\delta) \wedge Init(s)(\delta) \subseteq C]$

(3) $\forall X, Y \in \mathcal{P}(C)\ \forall s \in \mathcal{L}\ \forall \delta \in \Delta\ [(\epsilon, X) \in \mathcal{C}_F[\![s]\!](\delta) \wedge (\epsilon, Y) \in \mathcal{C}_F[\![s]\!](\delta)$

$$\Rightarrow (\epsilon, X \cup Y) \in \mathcal{C}_F[\![s]\!](\delta)]$$

($Init(s)(\delta)$ was introduced in definition 2.5.)

Note that property (3) does not hold for arbitrary pairs (w, X) and (w, Y) with $w \in A^*$ and $w \neq \epsilon$.

5. SEMANTIC EQUIVALENCE

In this section, we compare the operational models $\mathcal{O}_\lambda$ and the compositional models $\mathcal{C}_\lambda$. We shall prove that $\mathcal{O}_\lambda = \mathcal{C}_\lambda$, for $\lambda \in \{B, R, F\}$. It is a corollary of the following

THEOREM 5.1 *For* $\lambda \in \{B, R, F\}$: $\Phi_\lambda(\mathcal{C}_\lambda) = \mathcal{C}_\lambda$

PROOF. Recall that Φ_λ is the defining contraction for $\mathcal{O}_\lambda$ as given in definitions 3.6, 3.8 and 3.10 for $\lambda = B, R$, and F, respectively. The theorem is proved by induction on the complexity of statements, first in $\mathcal{L}^g$ and then in $\mathcal{L}$. In part (1) and (2) below, the δ arguments have been omitted.

Part (1): It is obvious that $\Phi_\lambda(\mathcal{C}_\lambda)(E) = \mathcal{C}_\lambda(E)$. For $a \in A$ we have:

$$\Phi_B(\mathcal{C}_B)(a) = \{<a, p_0>\} = \mathcal{C}_B[\![a]\!]$$

$$\Phi_R(\mathcal{C}_R)(a) = \{a\} = \mathcal{C}_R[\![a]\!], \text{ if } a \in I$$

$$\Phi_R(\mathcal{C}_R)(a) = \{a, (\epsilon, \{a\})\} = \mathcal{C}_R[\![a]\!], \text{ if } a \in C.$$

Similarly for $\lambda = F$.

Part (2): Suppose we have $\Phi_\lambda(\mathcal{C}_\lambda)(s) = \mathcal{C}_\lambda[\![s]\!]$ and $\Phi_\lambda(\mathcal{C}_\lambda)(t) = \mathcal{C}_\lambda[\![t]\!]$, for $\lambda \in \{B, R, F\}$. We shall treat some typical cases:

$$\begin{aligned}
\Phi_B(\mathcal{C}_B)(s;t) &= \{<a, \mathcal{C}_B[\![s';t]\!]>: s - a \to s'\} \\
&= \{<a, \mathcal{C}_B[\![s']\!];^B \mathcal{C}_B[\![t]\!]>: s - a \to s'\} \\
&= \{<a, \mathcal{C}_B[\![s']\!]>: s - a \to s'\};^B \mathcal{C}_B[\![t]\!] \\
&= \Phi_B(\mathcal{C}_B)(s);^B \mathcal{C}_B[\![t]\!] \\
&= [\text{ induction }] \\
&\quad \mathcal{C}_B[\![s]\!];^B \mathcal{C}_B[\![t]\!] \\
&= \mathcal{C}_B[\![s;t]\!]
\end{aligned}$$

$$\begin{aligned}
\Phi_R(\mathcal{C}_R)(s+t) &= \bigcup\{a \cdot \mathcal{C}_R[\![s']\!]: s + t - a \to s'\} \cup \{(\epsilon, \mathit{Init}(s+t)): \mathit{Init}(s+t) \subseteq C\} \\
&= [\text{ by properties of } \to] \\
&\quad \bigcup\{a \cdot \mathcal{C}_R[\![s']\!]: s - a \to s'\} \cup \bigcup\{a \cdot \mathcal{C}_R[\![t']\!]: t - a \to t'\} \cup \\
&\quad \{(\epsilon, \mathit{Init}(s) \cup \mathit{Init}(t)): \mathit{Init}(s) \subseteq C \wedge \mathit{Init}(t) \subseteq C\} \\
&= [\text{ definition } +^R] \\
&\quad \bigcup\{a \cdot \mathcal{C}_R[\![s']\!]: s - a \to s'\} \cup \{(\epsilon, \mathit{Init}(s)): \mathit{Init}(s) \subseteq C\}
\end{aligned}$$

$$+^R$$

$$\bigcup\{a\cdot\mathcal{C}_R[\![t']\!];\ t-a\to t'\}\ \cup\ \{(\epsilon, Init(t)):\ Init(t)\subseteq C\}$$

$$= [\text{ definition } \Phi_R\ ]$$

$$\Phi_R(\mathcal{C}_R)(s)\ +^R\Phi_R(\mathcal{C}_R)(t)$$

$$= [\text{ induction }]$$

$$\mathcal{C}_R[\![s]\!]\ +^R\mathcal{C}_R[\![t]\!]$$

$$= \mathcal{C}_R[\![s+t]\!]$$

$$\Phi_F(\mathcal{C}_F)(s\|t) = \bigcup\{a\cdot(\mathcal{C}_F[\![s'\|t]\!]):\ s-a\to s'\}\ \cup$$

$$\bigcup\{a\cdot(\mathcal{C}_F[\![s\|t']\!]):\ t-a\to t'\}\ \cup$$

$$\bigcup\{\tau\cdot(\mathcal{C}_F[\![s'\|t']\!]):\ s-c\to s'\ \wedge\ t-\overline{c}\to t'\}\ \cup$$

$$\{(\epsilon,X):\ X\subseteq(C-Init(s\|t))\ \wedge\ Init(s\|t)\subseteq C\}$$

$$= \bigcup\{a\cdot(\mathcal{C}_F[\![s']\!]\|^F\mathcal{C}_F[\![t]\!]):\ s-a\to s'\}\ \cup$$

$$\bigcup\{a\cdot(\mathcal{C}_F[\![s]\!]\|^F\mathcal{C}_F[\![t']\!]):\ t-a\to t'\}\ \cup$$

$$\bigcup\{\tau\cdot(\mathcal{C}_F[\![s']\!]\|^F\mathcal{C}_F[\![t']\!]):\ s-c\to s'\ \wedge\ t-\overline{c}\to t'\}\ \cup$$

$$\{(\epsilon,X):\ X\subseteq(\mathcal{C}-Init(s\|t))\ \wedge\ Init(s\|t)\subseteq C\}$$

$$= [\text{ definition } \Phi_F;\ Init(s\|t)\subseteq C\ \Rightarrow\ Init(s\|t)=Init(s)\cup Init(t)\ ]$$

$$\Phi_F(\mathcal{C}_F)(s)\mathbb{L}^F\mathcal{C}_F[\![t]\!]\ \cup$$

$$\Phi_F(\mathcal{C}_F)(t)\mathbb{L}^F\mathcal{C}_F[\![s]\!]\ \cup$$

$$\Phi_F(\mathcal{C}_F)(s)|^F\Phi_F(\mathcal{C}_F)(t)\ \cup$$

$$\{(\epsilon,X):\ X\subseteq(C-Init(s))\cap(C-Init(t))\ \wedge\ Init(s)\subseteq C\ \wedge\ Init(t)\subseteq C\}$$

$$= [\text{ induction }]$$

$$(\mathcal{C}_F[\![s]\!]\mathbb{L}^F\mathcal{C}_F[\![t]\!])\ \cup\ (\mathcal{C}_F[\![t]\!]\mathbb{L}^F\mathcal{C}_F[\![s]\!])\ \cup\ (\mathcal{C}_F[\![s]\!]|^F\mathcal{C}_F[\![t]\!])\ \cup$$

$$\{(\epsilon,X):\ X\subseteq(C-Init(s))\cap(C-Init(t))\ \wedge\ Init(s)\subseteq C\ \wedge\ Init(t)\subseteq C\}$$

$$= [\text{ lemma 4.6 (2) }]$$

$$(\mathcal{C}_F[\![s]\!]\mathbb{L}^F\mathcal{C}_F[\![t]\!])\ \cup\ \mathcal{C}_F[\![t]\!]\mathbb{L}^F\mathcal{C}_F[\![s]\!])\ \cup\ (\mathcal{C}_F[\![s]\!]|^F\mathcal{C}_F[\![t]\!])\ \cup$$

$$\{(\epsilon,X):\ \exists(\epsilon,Z_1)\in\mathcal{C}_F[\![s]\!]\ \exists(\epsilon,Z_2)\in\mathcal{C}_F[\![t]\!]$$

$$[(C-Z_1)\cap\overline{(C-Z_2)}=\varnothing\ \wedge\ X\subseteq Z_1\cap Z_2]\}$$

$$= [\text{ definition } \#^F]$$

$$(\mathcal{C}_F[\![s]\!] \mathbb{L}^F \mathcal{C}_F[\![t]\!]) \cup (\mathcal{C}_F[\![t]\!] \mathbb{L}^F \mathcal{C}_F[\![s]\!]) \cup (\mathcal{C}_F[\![s]\!] |^F \mathcal{C}_F[\![t]\!]) \cup$$

$$(\mathcal{C}_F[\![s]\!] \#^F \mathcal{C}_F[\![t]\!])$$

$$= \mathcal{C}_F[\![s]\!] \|^F \mathcal{C}_F[\![t]\!]$$

$$= \mathcal{C}_F[\![s \| t]\!]$$

Part (3): Part (1) and (2) suffice to show: $\Phi_\lambda(\mathcal{C}_\lambda)(g) = \mathcal{C}_\lambda[\![g]\!]$ for all $g \in \mathfrak{L}^g$. To deal with the entire language $\mathfrak{L}$, we have to treat one other case: Let $\delta \in \Delta$, $x \in Stmw$; suppose $x \Leftarrow g \in \delta$. Then

$$\Phi_\lambda(\mathcal{C}_\lambda)(x)(\delta) = [\text{ definition } -\delta\rightarrow]$$

$$\Phi_\lambda(\mathcal{C}_\lambda)(g)(\delta)$$

$$= [\text{ induction }]$$

$$\mathcal{C}_\lambda[\![g]\!](\delta)$$

$$= \mathcal{C}_\lambda[\![x]\!](\delta). \qquad \square$$

Since the functions Φ_λ are contractions, the following corollary is immediate:

COROLLARY 5.2: For $\lambda \in \{B, R, F\}$: $\mathcal{O}_\lambda = \mathcal{C}_\lambda$.

6. CORRECTNESS AND FULL ABSTRACTION

In this section we show that $\mathcal{O}_F$, $\mathcal{O}_R$ and $\mathcal{O}_B$ are *correct* with respect to $\equiv_L$, the equivalence relation on $\mathfrak{L}$ induced by $\mathcal{O}_L$, and that $\mathcal{O}_F$ is moreover *fully abstract* with respect to $\equiv_L$. We start by giving another characterization of the notion of compositionality (see definition 4.1). To this end, we first introduce two definitions.

DEFINITION 6.1

Let $\mathfrak{M}: \mathfrak{L} \rightarrow S$ be a model for $\mathfrak{L}$, with S an arbitrary set. Then $\mathfrak{M}$ induces an equivalence relation $\equiv_{\mathfrak{M}} \subseteq \mathfrak{L} \times \mathfrak{L}$ on $\mathfrak{L}$ as follows. For all $s, t \in \mathfrak{L}$:

$$s \equiv_{\mathfrak{M}} t \Leftrightarrow \mathfrak{M}[\![s]\!] = \mathfrak{M}[\![t]\!].$$

DEFINITION 6.2 (Congruence relation)

Let $\equiv \subseteq \mathfrak{L} \times \mathfrak{L}$ be an equivalence relation on $\mathfrak{L}$. We say that $\equiv$ *respects* the operator *op* (where *op* ranges again over $\{;, +, \|\}$ if

$$\forall s, s', t, t' \in \mathfrak{L}\,[(s \equiv s' \wedge t \equiv t') \Rightarrow (s\ op\ t) \equiv (s'\ op\ t')].$$

(We also say that $\equiv$ is *substitutive* with respect to *op*.) If $\equiv$ respects all of ;, +, and ||, it is called a *congruence relation* on $\mathfrak{L}$. (Another term for this: $\equiv$ is substitutive for $\mathfrak{L}$.)

The following theorem is immediate:

THEOREM 6.3: *$\mathfrak{M}$ is compositional for $\mathfrak{L} \Leftrightarrow \equiv_{\mathfrak{M}}$ is a congruence on $\mathfrak{L}$.*

From $\mathcal{O}_\lambda = \mathcal{C}_\lambda$, for $\lambda \in \{B, R, F\}$, it follows that $\mathcal{O}_B, \mathcal{O}_R$ and $\mathcal{O}_F$ are compositional. In other words:

THEOREM 6.4: *Let $\equiv_\lambda$ denote $\equiv_{\mathcal{O}_\lambda}$, for $\lambda \in \{B, R, F\}$. We have:*

$\equiv_\lambda$ *is a congruence relation on* $\mathfrak{L}$.

This does not hold for $\equiv_L (= \equiv_{\mathcal{O}_L})$: Consider the statements $s_1 = c, s_2 = \bar{c}$ and $t = c$; then

$$s_1 \equiv_L s_2, \text{ but not: } s_1 \| t \equiv_L s_2 \| t,$$

which is straightforward from the definition of $\mathcal{O}_L$. Intuitively, this can be explained by the observation that $\mathcal{O}_L$ makes too many identifications (like $\mathcal{O}_L[\![c]\!] = \mathcal{O}_L[\![\bar{c}]\!] = \{\partial\}$) in order to yield a congruence relation. In contrast, $\mathcal{O}_B, \mathcal{O}_R$ and $\mathcal{O}_F$ all make more distinctions, and, according to theorem 6.4, enough to obtain a congruence relation.

The question of *full abstraction*, for which we shall give a formal definition in a moment, is essentially the problem of finding, for a given equivalence relation $\equiv$ on $\mathfrak{L}$, a model $\mathfrak{M}$ of $\mathfrak{L}$ that makes precisely enough distinctions in order to yield a congruence relation $\equiv_{\mathfrak{M}}$ which is contained in $\equiv$. In other words, $\equiv_{\mathfrak{M}}$ should be the *largest* congruence relation that is contained in $\equiv$. Such a model will be called fully abstract with respect to $\equiv$.

With the above in mind, we next give for an arbitrary equivalence relation on $\mathfrak{L}$ a characterization of the greatest congruence it contains. For this purpose, we use the notion of *contexts*:

DEFINITION 6.5 (Contexts)
The set of *contexts* $(C \in)Cont$ is given by

$$C ::= (\cdot) \mid a \mid C_1; C_2 \mid C_1 + C_2 \mid C_1 \| C_2 \mid x.$$

Here $(\cdot)$ denotes a so-called *hole*. Typical elements of *Cont* will also be indicated by $C(\cdot)$. Contexts can be interpreted as functions from $\mathfrak{L}$ to $\mathfrak{L}$: Given a context $C(\cdot)$ and a statement $s \in \mathfrak{L}$, a new statement $C(s)$ is obtained by syntactically substituting s in all the holes occurring in $C(\cdot)$.

DEFINITION 6.6
Let $\equiv \subseteq \mathfrak{L} \times \mathfrak{L}$ be an equivalence relation. We define a relation $\equiv^c$ on $\mathfrak{L}$ by putting for $s, t \in \mathfrak{L}$:

$$s \equiv^c t \Leftrightarrow \forall C(\cdot) \in \mathit{Cont}\ [C(s) \equiv C(t)].$$

The following theorem is straightforward:

THEOREM 6.7:
(1) $\equiv^c$ *is a congruence relation on* $\mathcal{L}$
(2) $\equiv^c \subseteq \equiv$
(3) *For every congruence relation* $\equiv'$ *on* $\mathcal{L}$: $\equiv' \subseteq \equiv \Rightarrow \equiv' \subseteq \equiv^c$

PROOF: We only prove (3). Let $\equiv' \subseteq \equiv$ be a congruence relation on $\mathcal{L}$. One shows, by induction on the complexity of statements that for all s and t in $\mathcal{L}$ with $s \equiv' t$:

$$\forall C(\cdot) \in \mathit{Cont}\ [C(s) \equiv' C(t)];$$

since $\equiv' \subseteq \equiv$ this implies:

$$\forall C(\cdot) \in \mathit{Cont}\ [C(s) \equiv C(t)],$$

thus $s \equiv^c t$.

We see that $\equiv^c$ is the largest congruence contained in $\equiv$.
Now we come to the formal definition of full abstraction:

DEFINITION 6.8 (Correctness and full abstraction)
Let $\mathfrak{M}: \mathcal{L} \to S$ be a model for $\mathcal{L}$, with S an arbitrary set. Then:
(1) $\mathfrak{M}$ is called *correct* (or *fully adequate*) *with respect to* $\equiv$ if

$$\equiv_{\mathfrak{M}} \subseteq \equiv^c$$

(2) $\mathfrak{M}$ is called *complete with respect to* $\equiv$ if

$$\equiv^c \subseteq \equiv_{\mathfrak{M}}$$

(3) $\mathfrak{M}$ is called *fully abstract* with respect to $\equiv$ if it is both correct and complete:

$$\equiv_{\mathfrak{M}} = \equiv^c$$

We have that $\mathcal{O}_B$, $\mathcal{O}_R$ and $\mathcal{O}_F$ all are correct with respect to $\equiv_L$. It is an immediate consequence of theorem 6.4 and the following theorem:

THEOREM 6.9: $\equiv_B \subsetneq \equiv_R \subsetneq \equiv_F \subsetneq \equiv_L$

PROOF. We have the following implications, of which the premisses were stated in theorem 3.12:

$$\mathcal{O}_R = \alpha_R \circ \mathcal{O}_B \Rightarrow \equiv_B \subseteq \equiv_R$$
$$\mathcal{O}_F = \alpha_F \circ \mathcal{O}_R \Rightarrow \equiv_R \subseteq \equiv_F$$
$$\mathcal{O}_L = \alpha_L \circ \mathcal{O}_F \Rightarrow \equiv_F \subseteq \equiv_L.$$

The $\neq$ signs are valid by the examples given in subsection 3.5.

COROLLARY 6.10
The models $\mathcal{O}_B$, $\mathcal{O}_R$ and $\mathcal{O}_F$ are correct with respect to $\equiv_L$:

$$\equiv_B \subsetneq \equiv_R \subsetneq \equiv_F \subsetneq \equiv_{\mathfrak{L}} (\subsetneq \equiv_L).$$

It turns out that $\equiv_F = \equiv_{\mathfrak{L}}$; in other words: $\mathcal{O}_F$ is fully abstract with respect to $\equiv_L$. We shall show this along the lines of the proof of a similar statement that was given in [BKO87]. The following definition facilitates the formulation of the proof.

DEFINITION 6.11 ($\tilde{w}$, $\hat{w}$): We define two mappings:

$$\sim: A^* \to I^* \quad \text{and} \quad \hat{}: A^* \to \mathfrak{L}.$$

Let $w \in A^*$, say $w = a_1 \cdots a_n$. We set:

$$\sim(w) = \tilde{w} \quad \text{(notation)}$$

$$= a_1'; \cdots ; a_n',$$

$$\hat{}(w) = \hat{w} \quad \text{(notation)}$$

$$= \overline{a}_{i_1}; \cdots ; \overline{a}_{i_k},$$

where $\{a_{i_1}, \ldots, a_{i_k}\} = C \cap \{a_1, \ldots, a_n\}$ (with $i_1 < \cdots < i_k$) and for all $1 \leqslant j \leqslant n$:

$$a_j \in I \Rightarrow a_j' = a_j$$

$$a_j \in C \Rightarrow a_j' = \tau.$$

(If $C \cap \{a_1, \ldots, a_n\} = \varnothing$ we define $\hat{w} = E$.)

We give a few examples:

if $w = c$, then: $\tilde{w} = \tau$, $\hat{w} = \overline{c}$;

if $w = abc_1\ abc_2$, then: $\tilde{w} = ab\tau\ ab\tau$, $\hat{w} = \overline{c}_1; \overline{c}_2$.

The definition is motivated by the following:

LEMMA 6.12: *Let $w = a_1 \cdots a_n$ and $s = a_1; \cdots ; a_n$. Then*

$$\mathcal{O}_L[\![s \| \hat{w}]\!] = \tilde{w}.$$

THEOREM 6.13: *$\mathcal{O}_F$ is fully abstract with respect to $\equiv_L$, that is:* $\equiv_F = \equiv_{\mathfrak{L}}$.

PROOF. We already know that $\equiv_F \subseteq \equiv_L^{\mathfrak{L}}$. We prove that $\equiv_L^{\mathfrak{L}} \subseteq \equiv_F$ by showing, for all $s, t \in \mathfrak{L}$:

$$\forall C(\cdot) \in Cont\ [\mathcal{O}_L[\![C(s)]\!] = \mathcal{O}_L[\![C(t)]\!]] \qquad (*)$$

$$\Rightarrow \mathcal{O}_F[\![s]\!] = \mathcal{O}_F[\![t]\!].$$

Suppose that (*) holds for $s, t \in \mathfrak{L}$. We prove:

(1) $\forall w \in A^\infty\ [w \in \mathcal{O}_F[\![s]\!] \Rightarrow w \in \mathcal{O}_F[\![t]\!]]$

(2) $\forall w \in A^* \forall X \in \mathcal{P}(C)\ [(w,X) \in \mathcal{O}_F[\![s]\!] \Rightarrow (w,X) \in \mathcal{O}_F[\![t]\!]]$.

From these properties and the symmetry of their proofs with respect to s and t, the theorem follows.

We prove (1): Suppose $w \in \mathcal{O}_F[\![s]\!]$, with $w \in A^\omega$, say $w = a_1 a_2 \cdots$. (The case that $w \in A^*$ is similar.) We show for all $N \in \mathbb{N}$:

$$d(w, \mathcal{O}_F[\![t]\!]) \leqslant 2^{-N}$$

(where $d(w, \mathcal{O}_F[\![t]\!]) = \inf_{w' \in \mathcal{O}_F[\![t]\!]} \{d_{A^\infty}(w, w')\}$). Because $\mathcal{O}_F[\![t]\!]$ is closed it then follows that $w \in \mathcal{O}_F[\![t]\!]$.

Let $N \in \mathbb{N}$ and let $w_1 = a_1 \cdots a_N$. We show:

$$\exists w_2 \in A_L\ [\tilde{w}_1 \cdot w_2 \in \mathcal{O}_L[\![s \| \hat{w}_1]\!]]:$$

there exist statements $s_1, \ldots, s_N$ such that

$$s\ -a_1\rightarrow\ s_1\ -a_2\rightarrow\ \cdots\ -a_N\rightarrow\ s_n;\ \text{thus:}$$

$$s \| \hat{w}_1\ -a_1'\rightarrow\ \cdots\ -a_N'\rightarrow\ s_N,$$

where $a_1' \cdots a_N' = \tilde{w}_1$. By choosing w_2 in $\mathcal{O}_L[\![s_N]\!]$ we have: $\tilde{w}_1 \cdot w_2 \in \mathcal{O}_L[\![s \| \hat{w}_1]\!]$.

Because of (*) we also have $\tilde{w}_1 \cdot w_2 \in \mathcal{O}_L[\![t \| \hat{w}_1]\!]$. This implies the existence of statements $t_1, \ldots, t_N$ such that

$$t\ -a_1\rightarrow\ t_1\ -a_2\rightarrow\ \cdots\ -a_N\rightarrow\ t_N$$

and such that $w_1 \cdot w_2 \in \mathcal{O}_L[\![t]\!]$. Hence: $d(w, \mathcal{O}_F[\![t]\!]) \leqslant 2^{-N}$.

Next, we prove (2): Let $w \in A^*$ and $X \in \mathcal{P}(C)$, and suppose $(w,X) \in \mathcal{O}_F[\![s]\!]$. We show that $(w,X) \in \mathcal{O}_F[\![t]\!]$. A first observation is that $\mathcal{O}_F[\![t]\!]$ must at least contain some failure pair (w, Y), since

$$(w, X) \in \mathcal{O}_F[\![s]\!] \Rightarrow$$

$$(\tilde{w}, X) \in \mathcal{O}_F[\![s \| \hat{w}]\!] \Rightarrow$$

$$\tilde{w} \cdot \partial \in \mathcal{O}_L[\![s \| \hat{w}]\!] \Rightarrow \text{ (because (*))}$$

$$\tilde{w} \cdot \partial \in \mathcal{O}_L[\![t \| \hat{w}]\!] \Rightarrow \text{ (because } \mathcal{O}_L = \alpha_L \circ \mathcal{O}_F)$$

$$\exists Y \in \mathcal{P}(C)\ [(\tilde{w}, Y) \in \mathcal{O}_F[\![t \| \hat{w}]\!]] \Rightarrow$$

$$\exists Y \in \mathcal{P}(C)\ [(w, Y) \in \mathcal{O}_F[\![t]\!]].$$

The latter implies (because $\mathcal{O}_F = \alpha_F \circ \mathcal{O}_R$)

$$\exists Y \in \mathcal{P}(C)\ [(w, Y) \in \mathcal{O}_R[\![t]\!]].$$

Now we distinguish between two cases. First, suppose

$$\forall Y \in \mathcal{P}(C)\ [(w, Y) \in \mathcal{O}_R[\![t]\!] \Rightarrow X \cap Y = \varnothing].$$

Consider a ready pair $(w, Y) \in \mathcal{O}_R[\![t]\!]$. Since $X \cap Y = \varnothing$ we have: $X \subseteq C - Y$. Because $(w, Y) \in \mathcal{O}_R[\![t]\!]$ this implies $(w, C - Y) \in \mathcal{O}_F[\![t]\!]$. Thus: $(w, X) \in \mathcal{O}_F[\![t]\!]$. So in this case we are done. We finish the proof by considering the second case; suppose:

$$\exists Y \in \mathcal{P}(C)\ [(w, Y) \in \mathcal{O}_R[\![t]\!] \wedge X \cap Y \neq \varnothing].$$

This property ensures that the following set is non-empty:

$$V = \{c\colon c \in C \wedge \exists y \in \mathcal{P}(C)\ [(w, Y) \in \mathcal{O}_R[\![t]\!] \wedge c \in X \cap Y]\}.$$

It is finite (since $V \subseteq \cup\{Y : (w, Y) \in \mathcal{O}_R[\![t]\!]\}$, which is finite); say $V = \{c_1, \ldots, c_k\}$. Now define the following statement:

$$u = \overline{c}_1 + \cdots + \overline{c}_k.$$

We have the following implications, of which the ones marked (A) and (B) are proved below:

$$(w, X) \in \mathcal{O}_F[\![s]\!] \Rightarrow$$

$$(\tilde{w}, X) \in \mathcal{O}_F[\![s \| \hat{w}]\!] \Rightarrow (A)$$

$$\tilde{w} \cdot \partial \in \mathcal{O}_L[\![s \| (\hat{w}; u)]\!] \Rightarrow \text{(because (*))}$$

$$\tilde{w} \cdot \partial \in \mathcal{O}_L[\![t \| (\hat{w}; u)]\!] \Rightarrow (B)$$

$$(\tilde{w}, X) \in \mathcal{O}_F[\![t \| \hat{w}]\!] \Rightarrow$$

$$(w, X) \in \mathcal{O}_F[\![t]\!].$$

So we are done if we can convince the reader of the validity of the implications marked by (A) and (B). We try to do so, first for (A).

Suppose $(\tilde{w}, X) \in \mathcal{O}_F[\![s \| \hat{w}]\!]$ and let $w = a_1 \cdots a_n$ and $\tilde{w} = a_1' \cdots a_n'$. Then there exist statements $s_1, \ldots, s_n$ such that

$$s \| \hat{w} \ -a_1' \rightarrow \ \cdots \ -a_n' \rightarrow s_n$$

and

$$Init(s_n) \subseteq C \ \wedge \ X \subseteq C - Init(s_n).$$

Because $V \subseteq X$ we have $Init(s_n) \cap V = \varnothing$. Thus $Init(s_n \| u) \subseteq C$, which implies

$$\tilde{w} \cdot \partial \in \mathcal{O}_L[\![s \| (\hat{w}; u)]\!].$$

Finally, we prove (B). Suppose $\tilde{w} \cdot \partial \in \mathcal{O}_L[\![t \| (\hat{w}; u)]\!]$ and, again, let $w = a_1 \cdots a_n$ and $\tilde{w} = a_1' \cdots a_n'$. Then there exist statements $t_1, \ldots, t_n$ such that

$$t \| (\hat{w}; u) \; -a_1' \rightarrow \; \cdots \; -a_n' \rightarrow \; t_n \| u$$

and $Init(t_n \| u) \subseteq C$. The latter implies $Init(t_n) \subseteq C$ and $Init(t_n) \cap V = \varnothing$ (since $\overline{V} = Init(u)$). Because

$$t \| \hat{w} \; -a_1' \rightarrow \; \cdots \; -a_n' \rightarrow \; t_n$$

we have $(\tilde{w}, Init(t_n)) \in \mathcal{O}_R[\![t \| \hat{w}]\!]$, and thus $(\tilde{w}, C - Init(t_n)) \in \mathcal{O}_F[\![t \| \hat{w}]\!]$. Because $Init(t_n) \cap V = \varnothing$ we have, by the definition of V, that $Init(t_n) \cap X = \varnothing$, which yields the desired result: $(\tilde{w}, X) \in \mathcal{O}_F[\![t \| \hat{w}]\!]$. □

7. Related work

Operational and denotational semantics of simple programming languages like $\mathfrak{L}$ are, in a metric setting, extensively studied in [BMOZ88] and [BKMOZ86]. The problem of solving reflexive domain equations, like the one used for P_B (definition 3.5), over a category of complete metric spaces was first tackled in [BZ82] and is further explored for a wider class of equations in [AR88]. The technique of defining semantic models and operators as fixed points of contractions and the full exploration of this method with respect to the comparison of different models was introduced in [KR88]. Many application can be found in [BM88]. For readiness semantics we refer to [OH86]. Failure semantics was introduced in [BHR84]. In [De85], operational and denotational semantics of CCS and CSP like languages are studied, in which the notion of testing equivalences plays a key role. In the context of ACP (Algebra of Communicating Processes), a complete axiomatization for finite processes with communication (and without silent move) is given in [BKO87], for readiness and failure semantics; moreover, the fact that failure semantics induces the largest trace respecting congruence is proved there. For a treatment of full abstraction in the setting of partial orderings see [HP79]. In [Mu85], the question of semantic equivalence and full abstraction is tackled with the help of so-called inclusive predicates, again in an order-theoretic framework. In [St86], the general question concerning the existence of fully abstract models is treated in an algebraic context. In [AP86], an example is given of a language for which no fully abstract model exists.

8. REFERENCES

[AP86] K. APT, G. PLOTKIN, *Countable nondeterminism and random assignment,* Journal of the Association for Computing Machinery, Vol. 33, No. 4, 1986, pp. 724-767.

[AR88] P. AMERICA, J.J.M.M. RUTTEN, *Solving reflexive domain equations in a category of complete metric spaces,* in: Proceedings of the Third Workshop on Mathematical Foundations of Programming Language Semantics (M. Main, A. Melton, M. Mislove, D. Schmidt, Eds.), Lecture Notes in Computer Science 298, Springer-Verlag, 1988, pp. 254-288. (To appear in the Journal of Computer and System Sciences.)

[BHR84] S. BROOKES, C. HOARE, W. ROSCOE, *A theory of communicating sequential processes,* J. Assoc. Comput. Mach. 31, No. 3, 1984, pp. 560-599.

[BK87] J.A. BERGSTRA, J.W. KLOP, *A convergence theorem in process algebra,* Report CS-R8733, Centre for Mathematics and Computer Science, Amsterdam, 1987.

[BKO87] J.A. BERGSTRA, J.W. KLOP, E.-R. OLDEROG, *Readies and failures in the algebra of communicating processes (revised version),* Report CS-R8748, Centre for Mathematics and Computer Science, Amsterdam, 1987. (To appear in: SIAM Journal of Computing, 1988.)

[BM88] J.W. DE BAKKER, J.-J. CH. MEYER, *Metric semantics for concurrency,* Report CS-R8803, Centre for Mathematics and Computer Science, Amsterdam, 1988.

[BKMOZ86] J.W. DE BAKKER, J.N. KOK, J.-J. CH. MEYER, E.-R. OLDEROG, J.I. ZUCKER, *Contrasting themes in the semantics of imperative concurrency,* in: Current Trends in Concurrency (J.W. de Bakker, W.P. de Roever, G. Rozenberg, Eds.), Lecture Notes in Computer Science 224, Springer-Verlag, 1986, pp. 51-121.

[BMOZ88] J.W. DE BAKKER, J.-J. CH. MEYER, E.-R. OLDEROG, J.I. ZUCKER, *Transition systems, metric spaces and ready sets in the semantics of uniform concurrency,* Journal of Computer and System Sciences Vol 36 (number 2), 1988, pp. 158-224.

[BZ82] J.W. DE BAKKER, J.I. ZUCKER, *Processes and the denotational semantics of concurrency,* Information and Control 54 (1982), pp. 70-120.

[De85] R. DE NICOLA, *Testing equivalences and fully abstract models for communicating processes,* Ph.D. Thesis, report CST-36-85, Department of Computer Science, University of Edinburgh, 1985.

[Du66] J. DUGUNDJI, *Topology,* Allen and Bacon, Rockleigh, N.J., 1966.

[En77] E. ENGELKING, *General topology,* Polish Scientific Publishers, 1977.

[HP79] M. HENNESSY, G.D. PLOTKIN, *Full abstraction for a simple parallel programming language,* in: Proceedings 8th MFCS (J. Bečvář ed.), Lecture Notes in Computer Science 74, Springer-Verlag, 1979, pp. 108-120.

[Ho85] C.A.R. HOARE, *Communicating sequential processes,* Prentice Hall International, 1985.

[KR88] J.N. KOK, J.J.M.M. RUTTEN, *Contractions in comparing concurrency semantics,* in: Proceedings 15th ICALP, Tampere, 1988, Lecture Notes in Computer Science 317, Springer-Verlag, 1988, pp. 317-332.

[Mic51] E. MICHAEL, *Topologies on spaces of subsets,* in: Trans. AMS 71 (1951), pp. 152-182.

[Mil80] R. MILNER, *A Calculus of communicating systems,* Lecture Notes in Computer Science 92, Springer-Verlag, 1980.

[Mu85] K. MULMULEY, *Full abstraction and semantic equivalence,* Ph.D. Thesis, report CMU-CS-85-148, Computer Science Department, Carnegie-Mellon, 1985.

[OH86] E.-R. OLDEROG, C.A.R. HOARE, *Specification-oriented semantics for communicating processes,* Acta Informaticae 23, 1986, pp. 9-66.

[Pl76] G.D. PLOTKIN, *A powerdomain construction,* SIAM J. Comp. 5 (1976), pp. 452-487.

[Pl81] G.D. PLOTKIN, *A structural approach to operational semantics,* Report DAIMI FN-19, Comp. Sci. Dept., Aarhus Univ. 1981.

[Pl83] G.D. PLOTKIN, *An operational semantics for CSP,* in: Formal Description of Programming Concepts II (D. Bjørner ed.) North-Holland, Amsterdam (1983), pp. 199-223.

[St86] A. STOUGHTON, *Fully abstract models of programming languages,* Ph.D. Thesis, report CST-40-86, Department of Computer Science, University of Edinburgh, 1986.

9. APPENDIX: MATHEMATICAL DEFINITIONS

DEFINITION A.1 (Metric space)

A *metric space* is a pair (M,d) with M a non-empty set and d a mapping $d:M\times M\to[0,1]$ (a *metric* or *distance*) that satisfies the following properties:

(a) $\forall x,y\in M\,[d(x,y)=0 \Leftrightarrow x=y]$

(b) $\forall x,y\in M\,[d(x,y)=d(y,x)]$

(c) $\forall x,y,z\in M\,[d(x,y)\leqslant d(x,z)+d(z,y)]$.

We call (M,d) an *ultra-metric space* if the following stronger version of property (c) is satisfied:

(c') $\forall x,y,z\in M\,[d(x,y)\leqslant \max\{d(x,z),d(z,y)\}]$.

Please note that we consider only metric spaces with bounded diameter: the distance between two points never exceeds 1.

EXAMPLES A.1.1

(a) Let A be an arbitrary set. The *discrete* metric d_A on A is defined as follows. Let $x,y\in A$, then

$$d_A(x,y)=\begin{cases}0 & \text{if } x=y\\ 1 & \text{if } x\neq y.\end{cases}$$

(b) Let A be an alphabet, and let $A^\infty = A^* \cup A^\omega$ denote the set of all finite and infinite words

over A. Let, for $x \in A^{\infty}$, $x(n)$ denote the prefix of x of length n, in case $length(x) \geqslant n$, and x otherwise. We put

$$d(x,y) = 2^{-sup\{n \mid x(n)=y(n)\}},$$

with the convention that $2^{-\infty} = 0$. Then (A^{∞}, d) is a metric space.

DEFINITION A.2

Let (M,d) be a metric space, let $(x_i)_i$ be a sequence in M.

(a) We say that $(x_i)_i$ is a *Cauchy sequence* whenever we have:
$\forall \epsilon > 0\ \exists N \in \mathbb{N}\ \forall n,m > N\ [d(x_n,x_m) < \epsilon]$.

(b) Let $x \in M$. We say that $(x_i)_i$ *converges to* x and call x the *limit* of $(x_i)_i$ whenever we have:
$\forall \epsilon > 0\ \exists N \in \mathbb{N}\ \forall n > N\ [d(x,x_n) < \epsilon]$.
Such a sequence we call *convergent*. Notation: $\lim_{i\to\infty} x_i = x$.

(c) The metric space (M,d) is called *complete* whenever each Cauchy sequence converges to an element of M.

DEFINITION A.3

Let $(M_1,d_1),(M_2,d_2)$ be metric spaces.

(a) We say that (M_1,d_1) and (M_2,d_2) are *isometric* if there exists a bijection $f: M_1 \to M_2$ such that:
$\forall x,y \in M_1\ [d_2(f(x),f(y)) = d_1(x,y)]$. We then write $M_1 \cong M_2$. When f is not a bijection (but only an injection), we call it an *isometric embedding*.

(b) Let $f: M_1 \to M_2$ be a function. We call f *continuous* whenever for each sequence $(x_i)_i$ with limit x in M_1 we have that $\lim_{i\to\infty} f(x_i) = f(x)$.

(c) Let $A \geqslant 0$. With $M_1 \to^A M_2$ we denote the set of functions f from M_1 to M_2 that satisfy the following property:
$\forall x,y \in M_1\ [d_2(f(x),f(y)) \leqslant A \cdot d_1(x,y)]$.
Functions f in $M_1 \to^1 M_2$ we call *non-expansive*, functions f in $M_1 \to^{\epsilon} M_2$ with $0 \leqslant \epsilon < 1$ we call *contracting*.

PROPOSITION A.4

(a) *Let $(M_1,d_1),(M_2,d_2)$ be metric spaces. For every $A \geqslant 0$ and $f \in M_1 \to^A M_2$ we have: f is continuous.*

(b) *(Banach's fixed-point theorem)*
Let (M,d) be a complete metric space and $f: M \to M$ a contracting function. Then there exists an $x \in M$ such that the following holds:
(1) *$f(x) = x$ (x is a fixed point of f),*
(2) *$\forall y \in M\ [f(y) = y \Rightarrow y = x]$ (x is unique),*
(3) *$\forall x_0 \in M\ [\lim_{n\to\infty} f^{(n)}(x_0) = x]$, where $f^{(n+1)}(x_0) = f(f^{(n)}(x_0))$ and $f^{(0)}(x_0) = x_0$.*

DEFINITION A.5 (Compact subsets)

A subset X of a complete metric space (M,d) is called *compact* whenever each sequence in X has a subsequence that converges to an element of X.

DEFINITION A.6

Let $(M,d),(M_1,d_1),\ldots,(M_n,d_n)$ be metric spaces.

(a) With $M_1 \to M_2$ we denote the set of all continuous functions from M_1 to M_2. We define a metric d_F on $M_1 \to M_2$ as follows. For every $f_1,f_2 \in M_1 \to M_2$

$$d_F(f_1,f_2)=\sup_{x\in M_1}\{d_2(f_1(x),f_2(x))\}.$$

For $A \geqslant 0$ the set $M_1 \to^A M_2$ is a subset of $M_1 \to M_2$, and a metric on $M_1 \to^A M_2$ can be obtained by taking the restriction of the corresponding d_F.

(b) With $M_1 \overline{\cup} \cdots \overline{\cup} M_n$ we denote the *disjoint union* of $M_1,\ldots,M_n$, which can be defined as $\{1\}\times M_1 \cup \cdots \cup \{n\}\times M_n$. We define a metric d_U on $M_1 \overline{\cup} \cdots \overline{\cup} M_n$ as follows. For every $x,y \in M_1 \overline{\cup} \cdots \overline{\cup} M_n$

$$d_U(x,y) = \begin{cases} d_j(x,y) & \text{if } x,y \in \{j\}\times M_j,\ 1 \leqslant j \leqslant n \\ 1 & \text{otherwise.} \end{cases}$$

(c) We define a metric d_P on $M_1 \times \cdots \times M_n$ by the following clause.
For every $(x_1,\ldots,x_n),(y_1,\ldots,y_n) \in M_1 \times \cdots \times M_n$

$$d_P((x_1,\ldots,x_n),(y_1,\ldots,y_n))=\max_i\{d_i(x_i,y_i)\}.$$

(d) Let $\mathcal{P}_{nc}(M) =^{def} \{X \mid X \subseteq M \wedge X$ is compact and non-empty$\}$. We define a metric d_H on $\mathcal{P}_{nc}(M)$, called the *Hausdorff distance,* as follows. For every $X,Y \in \mathcal{P}_{nc}(M)$

$$d_H(X,Y)=\max\{\sup_{x\in X}\{d(x,Y)\},\sup_{y\in Y}\{d(y,X)\}\},$$

where $d(x,Z) =^{def} \inf_{z\in Z}\{d(x,z)\}$ for every $Z \subseteq M$, $x \in M$.
In $\mathcal{P}_{co}(M) =^{def} \{X \mid X \subseteq M \wedge X$ is compact$\}$ we also have the empty set as an element. We define d_H on $\mathcal{P}_{co}(M)$ as above but extended with the following case. If $X \neq \varnothing$, then

$$d_H(\varnothing,X)=d_H(X,\varnothing)=1.$$

(e) Let $c \in [0,\infty)$. We define: $id_c(M,d)=(M,c\cdot d)$.

PROPOSITION A.7

Let (M,d), $(M_1,d_1),\ldots,(M_n,d_n)$, d_F, d_U, d_P and d_H be as in definition A.6 and suppose that (M,d), $(M_1,d_1),\ldots,(M_n,d_n)$ are complete. We have that

(a) $(M_1 \to M_2,d_F)$, $(M_1 \to^A M_2,d_F)$,
(b) $(M_1 \overline{\cup} \cdots \overline{\cup} M_n,d_U)$,
(c) $(M_1 \times \cdots \times M_n,d_P)$,
(d) $(\mathcal{P}_{nc}(M),d_H)$, and $(\mathcal{P}_{co}(M),d_H)$

are complete metric spaces. If (M,d) and (M_i,d_i) are all ultra-metric spaces these composed spaces

are again ultra-metric. (Strictly spoken, for the completeness of $M_1 \to M_2$ and $M_1 \to^A M_2$ we do not need the completeness of M_1. The same holds for the ultra-metric property.)

The proofs of proposition A.7 (a), (b) and (c) are straightforward. Part (d) is more involved. It can be proved with the help of the following characterization of the completeness of the Hausdorff metric.

PROPOSITION A.8
Let $(\mathcal{P}_{co}(M), d_H)$ be as in definition A.6. Let $(X_i)_i$ be a Cauchy sequence in $\mathcal{P}_{co}(M)$. We have:

$$\lim_{i\to\infty} X_i = \{\lim_{i\to\infty} x_i | x_i \in X_i, (x_i)_i \text{ a Cauchy sequence in } M\}.$$

The proof of proposition A.8 can be found in [Mic57] as a generalization of a similar result (for *closed* subsets) in [Du66] and [En77].