An Operational Semantics for CSP

by

S.D. Brookes[1], A.W. Roscoe[2] and D.J. Walker[3]

Introduction

Hoare's *CSP* or Communicating Sequential Processes [H], provides a basis for the study of concurrent computation. In recent years, a number of theoretical studies have been made of it and semantic models proposed for it. One of the most successful has been the "improved failures" model of [B,R,BR,BR1] which was adopted as the main model in [H]. In the present paper this is referred to as the "failures-divergences" model. This model is a member of a hierarchy of abstract models, each of which is suitable for the study of certain problems associated with concurrency. The earliest of these models were the "traces" model of [H1] and the original "failures" model [HBR, BHR], each of which captures less detail than the failures-divergences model. An excellent survey of equivalences will be found in [OH]. Recently, a related model has been introduced to deal with real-time concurrency [RR].

Each of the models mentioned above was constructed by regarding a process as an agent which may communicate with its environment by performing certain atomic actions drawn from an alphabet, and by reasoning about the possible behaviour of, and possible means of combining, such agents. It was then used to give a denotational semantics to the language. This operationally oriented approach is explicitly analysed in [BR] where a formal structural operational semantics in the style of Plotkin [P] for the language of *CSP* is proposed, and it is asserted that this operational semantics corresponds exactly to the denotational semantics provided by the failures-divergences model. It is the purpose of this paper to substantiate that claim.

Operational semantics for various subsets of *CSP* have appeared, with varying degrees of formality, in several papers in recent years. Among the more relevant analyses of operational semantics have been those of Hennessy and de Nicola [Hen,HN] who showed how the essentially operational *CCS* semantics could be related by testing to the models above. The work most like that in the present paper forms part of [OH], where an operational semantics for a small subset of *CSP* is proved congruent to a denotational model.

[1]Department of Computer Science, Carnegie-Mellon University, Pittsburgh, PA 15213, U.S.A.
[2]Oxford University Computing Laboratory, 8-11 Keble Road, Oxford OX1 3QD, U.K.
[3]Department of Computer Science, University of Edinburgh, Edinburgh EH9 3JZ, U.K.

As we shall see, there are structural difficulties in proving operational and denotational semantics congruent arising from the quite different mathematical models used, but more importantly from the different interpretations of recursion (the copy rule versus least fixed points). In [OH] a difficult but direct proof of congruence is given. Unfortunately this seems to rely on the simple subset of *CSP* chosen, and it may not be possible to extend it easily to the full language. In the present paper we modularise the problem by introducing an intermediate semantics which uses a model similar to that underlying the operational semantics (synchronization trees) but which is denotational and uses an abstract fixed point theory (that of complete metric spaces). This provides a natural decomposition of the proof; extending the proofs to deal with any further operators that one might wish to add to *CSP* should prove easy.

The work reported in the present paper was begun several years ago by Brookes and Roscoe [B,R,BR]. It was completed by Roscoe and Walker while the latter was studying in Oxford during 1986.

The remainder of this introductory section contains brief descriptions of the language of *CSP*, the failures-divergences model and the formal operational semantics, together with an outline of the proof that this operational semantics is congruent to the denotational semantics provided by the model. The motivation underlying the construction of both the model and the formal operational semantics are fully described in the references cited, and relatively little attempt is made here to provide such insight.

A communicating process is regarded as an agent which may interact with its environment (which may itself be regarded as a process) by performing certain atomic actions drawn from an alphabet A. *CSP* provides a formal language suitable for describing processes. The syntax of the language considered in this paper is given by the following informal *BNF*-style description.

$$\begin{aligned} P ::= \; & X \mid P \sqcap Q \mid P \Box Q \mid P\, {}_B\|_C\, Q \mid P \,|||\, Q \mid P;Q \mid \\ & P \backslash a \mid f[P] \mid f^{-1}[P] \mid x : B \rightarrow P_x \mid \mu X.P. \end{aligned}$$

Here P, Q and P_x range over the set $\mathbf{E}$ of terms of the language of *CSP*, X over a denumerable set *Var* of variables, a over the alphabet A of atomic actions, B and C over $Pow(A)$ and f over the set $AT = \{f : A \rightarrow A \mid \forall a \in A.\ f^{-1}(\{a\}) \text{ is finite} \wedge\ f(a) = \surd \text{ iff } a = \surd\}$ of ***alphabet transformations***. The intended interpretation of the closed terms (i.e. those terms in which every occurrence of a variable X is within the scope of an occurrence of an operator $\mu X.$) is as follows. $P \sqcap Q$ denotes a process which may behave, independently of its environment, as P or Q. $P \Box Q$ denotes a process which may behave as P or Q and is such that the environment may influence the choice of which provided that such influence is exerted on the first occurrence of an action of the composite process. $P\, {}_B\|_C\, Q$ denotes a process which behaves like the parallel composition of P and Q with the restrictions that any action performed by the composition must lie in $B \cup C$, and the composition may perform an action a only if $a \in B - C$ and P may perform a, or $a \in C - B$ and Q may perform a, or $a \in B \cap C$ and both P and Q may perform a. $P \,|||\, Q$ denotes the parallel composition by unrestricted interleaving of P and Q. $P; Q$ denotes the sequential composition of P followed by Q, and $P \backslash a$ the process which behaves like P except that all occurrences of the action a are rendered invisible to the environment. The processes $f[P]$ and $f^{-1}[P]$ derive their behaviour from that of P in that if P may perform the action a then $f[P]$ may perform $f(a)$ while $f^{-1}[P]$ may engage in any action b such that $f(b) = a$. The process denoted by $x : B \rightarrow P_x$ may engage in any action $b \in B$ and thereafter behave as the process P_b. (In the body of the paper a slightly different syntax is used for these "guarded choice" constructs.) $\mu X.P$ denotes a solution of the equation $X = P$.

The *CSP* terms *STOP*, *SKIP* and $a \rightarrow P$ of [H] are special instances of the guarded choice construct: *STOP* is obtained by taking $B = \emptyset$, $SKIP = x : \{\surd\} \rightarrow STOP$, and $a \rightarrow P = x : \{a\} \rightarrow P$. Here $\surd$ is a special action used to denote termination of a sequential process.

In the failures-divergences model a communicating process is modelled as a pair $N = \langle F, D\rangle$ where $F \subseteq A^* \times Pow(A)$ and $D \subseteq A^*$ (satisfying certain conditions described in Section 1). F is the set of ***failures*** of N and is such that a pair $\langle t, B\rangle$ is in F if and only if N may perform the sequence of actions t and then ***refuse*** to engage in any of the actions in the set B. The set D of ***divergences*** of N is such that t is in D if and only if N may perform the sequence of actions t and thereafter ***diverge***, that is engage in an infinite sequence of internal "changes of state" invisible to its environment, and never again communicate with its environment. The set $\mathbf{N}$ of all such processes, together with a natural partial order $\sqsubseteq$, which may be interpreted as "is less deterministic than," form the failures-divergences model. The model is a complete partial order with a least element $\perp$.

To each operator symbol of the language of *CSP* there corresponds a continuous function on (some Cartesian product of) $\langle \mathbf{N}, \sqsubseteq\rangle$ and this fact, in conjunction with the fixed-point theorem for complete partial orders, may be used to construct a mapping $\mathcal{N} : \mathbf{E} \rightarrow Env \rightarrow \mathbf{N}$, where $Env = Var \rightarrow \mathbf{N}$ is the set of ***(process) environments***, which provides a denotational semantics for the language of *CSP*. For each $P \in \mathbf{P}$, where $\mathbf{P}$ denotes the set of all closed terms of the language, $\mathcal{N}[\![P]\!]$ is a constant function and we use $\mathcal{N}[\![P]\!]$ to denote also its constant value.

The operational semantics, fully described in Section 2, is based on the idea that the behaviour of a process may be described in terms of the "state transitions" which it may undergo. Such a transition may or may not be observable by the environment. An occurrence of a change of state invisible to the environment is described in the formal system by a special symbol denoted τ. The axioms and rules of the system encapsulate the operational understanding which informed the construction of the denotational model. A term P can diverge when, and only when, there is a sequence of terms $\langle P_i \mid i < \omega\rangle$ such that $P_0 = P$ and for each i, P_i may undergo a τ-transition to become P_{i+1}.

Let $P \stackrel{t}{\Longrightarrow} Q$ denote that the term P may, according to the transition system, perform the sequence t of actions, possibly with occurrences of τ-transitions interleaved with the occurrences of the actions in t, and thereby evolve into the term Q. Let $Q\ ref\ B$ denote that Q may not perform any action lying in B and may not undergo any τ-transition. Let $Q\uparrow$ denote that Q may diverge as described above. The operational semantics of closed terms of the language of *CSP* may then be defined by means of a mapping $\mathcal{P} : \mathbf{P} \rightarrow \mathbf{N}$ as follows.

$$\begin{aligned}\mathcal{P}[\![P]\!] \ =_{df}\ & \langle \{\langle t, B\rangle \mid \exists Q. P \stackrel{t}{\Longrightarrow} Q \wedge Q\ ref\ B\} \cup \{\langle st, B\rangle \mid \exists Q. P \stackrel{s}{\Longrightarrow} Q \wedge Q\uparrow\},\\ & \{st \mid \exists Q. P \stackrel{s}{\Longrightarrow} Q \wedge Q\uparrow\}\rangle.\end{aligned}$$

Let $Sub =_{df} Var \rightarrow \mathbf{P}$ denote the set of all ***substitutions***. Each substitution σ may be extended to a mapping (also denoted) $\sigma : \mathbf{E} \rightarrow \mathbf{P}$ so that $\sigma[\![P]\!]$ denotes the term obtained by substituting $\sigma[\![X]\!]$ for each free occurrence in P of each variable X. Define a mapping $\hat{\cdot} : Sub \rightarrow Env$ by setting for $\sigma \in Sub$

$$\hat{\sigma} =_{df} \lambda X.\mathcal{P}[\![\sigma[\![X]\!]]\!].$$

Then the mapping $\mathcal{P}$ may be extended to a mapping (also denoted) $\mathcal{P} : \mathbf{E} \rightarrow Sub \rightarrow \mathbf{N}$ by setting

$$\mathcal{P}[\![P]\!]\sigma =_{df} \mathcal{P}[\![\sigma[\![P]\!]]\!].$$

That this semantics is congruent to that provided by the model is expressed as follows: for $P \in \mathbf{E}$ and $\sigma \in Sub$

$$\mathcal{P}[\![P]\!]\sigma = \mathcal{N}[\![P]\!]\hat{\sigma}.$$

This fact is the main result of this paper. To help the reader to follow its proof, which is given in Section 3, an outline is given below.

As indicated above, rather than attempt to prove this result directly we introduce an intermediate denotational semantics in terms of ***synchronization trees***. The transition system determines for each term P a ***labelled transition diagram*** $\mathcal{D}[\![P]\!]$, a tree with nodes labelled by terms and arcs labelled by elements of $A \cup \{\tau\}$, which describes exactly the behaviour of the term P. Thus $P \stackrel{t}{\Longrightarrow} Q$ if and only if there is a path u through $\mathcal{D}[\![P]\!]$ from the root to a node labelled Q with $t = u|A$ (i.e. t is obtained from u by deleting all τs), $Q\ ref\ B$ if and only if there is no arc from any node labelled Q which is labelled with an action lying in $B \cup \{\tau\}$, and $Q\uparrow$ if and only if there is an infinite path from any node labelled Q through $\mathcal{D}[\![P]\!]$ each arc being labelled τ.

By deleting the labels from the nodes of a labelled transition diagram, a ***synchronization tree*** is obtained. Let $\mathcal{R} : \mathbf{D} \rightarrow \mathbf{T}$ denote the "deletion mapping" where $\mathbf{T}$ denotes the set of all synchronization trees, and let $\mathcal{T} = \mathcal{R} \circ \mathcal{D}$. Then defining $\mathcal{M} : \mathbf{T} \rightarrow \mathbf{N}$ by imitating the definition of $\mathcal{P} : \mathbf{P} \rightarrow \mathbf{N}$, we obtain that for $P \in \mathbf{P}$

$$\mathcal{M}(\mathcal{T}[\![P]\!]) = \mathcal{P}[\![P]\!].$$

Now let $Tre =_{df} Var \rightarrow \mathbf{T}$ be the set of all ***tree environments*** and define $\bar{\cdot} : Sub \rightarrow Tre$ by

$$\overline{\sigma} =_{df} \lambda X.\mathcal{T}[\![\sigma[\![X]\!]]\!]$$

and define $\cdot^{*} : Tre \rightarrow Env$ by setting for $\rho \in Tre$

$$\rho^{*} =_{df} \lambda X.\mathcal{M}(\rho[\![X]\!]).$$

In broadest outline the proof consists in establishing the following identity (of which the result is an immediate consequence – note that $\hat{\sigma} = \overline{\sigma}^{*}$, where $\hat{\sigma}$ is as defined above): for $P \in \mathbf{E}$ and $\sigma \in Sub$

$$\mathcal{M}(\mathcal{T}[\![\sigma[\![P]\!]]\!]) = \mathcal{N}[\![P]\!]\overline{\sigma}^{*}.$$

This identity is proved by means of the construction of a mapping (the intermediate semantic function)

$$\mathcal{S} : \mathbf{E} \rightarrow Tre \rightarrow \mathbf{T}$$

such that for $P \in \mathbf{E}$ and $\sigma \in Sub$

$$\mathcal{T}[\![\sigma[\![P]\!]]\!] = \mathcal{S}[\![P]\!]\overline{\sigma}$$

and for $P \in \mathbf{E}$ and $\rho \in Tre$

$$\mathcal{M}(\mathcal{S}[\![P]\!]\rho) = \mathcal{N}[\![P]\!]\rho^{*}.$$

The construction of the mapping $\mathcal{S}$ and the proofs that it has the properties described above are presented in the section 3.

Notation

Throughout this paper standard set-theoretical and logical notations are employed. Thus Ord denotes the class of all ordinals and ω denotes the set of all natural numbers. If B and C are sets, $B \rightarrow C$ denotes the set of all mappings of B into C, and $[B \rightarrow C]$ the set of all mappings of B into C which are (in the sense determined by the context) continuous. If $f \in (B \rightarrow C), b \in B$ and $c \in C$ then $f \oplus \{b \mapsto c\}$ denotes that $g \in (B \rightarrow C)$ such that $g(b) = c$ and $g(a) = f(a)$ for $a \in B - \{b\}$. Let B be a set. The power set of B is denoted $Pow(B)$ and t he set of all finite sequences over B is denoted B^{*}. ε denotes the empty sequence, $\langle b_1 \ldots b_k \rangle$ a sequence of length k, st the concatenation of the sequences s and t, $s \backslash b$ the sequence obtained from s by deleting all occurrences of b, and $s|B$ the sequence obtained from s by deleting all members of s not lying in B. $merge(s,t)$ denotes the set of all sequences which may be obtained by merging s with t. $s \leq t$ denotes that s is an initial segment of t and b in s that b occurs in s. s b-free abbreviates $\neg(b \; in \; s)$, and bs abbreviates $\langle b \rangle s$.

1. The language of CSP and the failures-divergences model

Let A denote a set of symbols containing a distinguished symbol $\surd$. A is referred to as the ***alphabet*** and the symbols of A as ***actions***. An ***alphabet transformation*** is a mapping $f : A \to A$ such that for $a \in A$, $f^{-1}(\{a\})$ is finite and $f(a) = \surd$ iff $a = \surd$. The set of all alphabet transformations is denoted AT.

In order to give a rigorous treatment of the "guarded choice" constructs $x : B \to P_x$ for $B \subseteq A$, we define the set $\mathbf{E}$ of *CSP-terms* as follows. Let $Var = \{X_i \mid i < \omega\}$ be an infinite set of variables, and let $\sqcap$, $\Box$, ${}_B\|_C$, $|||$, $;$, $\backslash a$ $(a \in A)$, $f[\,]$ $(f \in AT)$, $f^{-1}[\,]$ $(f \in AT)$, $\mu X.$ $(X \in Var)$ and $B \to$ $(B \in Pow(A))$ be function symbols. Then define sequences $\langle \mathbf{E}_\alpha \mid \alpha \in Ord\rangle$ and $\langle \mathbf{C}^B_\alpha \mid \alpha \in Ord\rangle$ for $B \subseteq A$ by setting

$$\mathbf{E}_0 =_{df} Var$$

$$\begin{aligned}\mathbf{E}_{\alpha+1} =_{df}\ & \mathbf{E}_\alpha \cup \{P \ddagger Q \mid P, Q \in \mathbf{E}_\alpha, \ddagger \in \{\sqcap, \Box, {}_B\|_C\,, |||, ;\}\} \\ & \cup \{P\backslash a \mid P \in \mathbf{E}_\alpha, a \in A\} \\ & \cup \{f[P] \mid P \in \mathbf{E}_\alpha, f \in AT\} \\ & \cup \{f^{-1}[P] \mid P \in \mathbf{E}_\alpha, f \in AT\} \\ & \cup \{\mu X.P \mid P \in \mathbf{E}_\alpha, X \in Var\} \\ & \cup \{B \to g \mid B \subseteq A, g \in \mathbf{C}^B_\alpha\}\end{aligned}$$

$$\mathbf{E}_\lambda =_{df} \textstyle\bigcup_{\alpha<\lambda} \mathbf{E}_\alpha \qquad \text{for limit } \lambda$$

and

$$\mathbf{C}^B_\alpha =_{df} \{g^B_\alpha \mid g : B \to \mathbf{E}_\alpha\}$$

where for each triple (B, α, g) such that $B \subseteq A$, $\alpha \in Ord$ and $g : B \to \mathbf{E}_\alpha$, g^B_α is a distinguished auxiliary constant symbol. Then

$$\mathbf{E} =_{df} \bigcup_{\alpha \in Ord} \mathbf{E}_\alpha.$$

Note that although, in general, this definition involves transfinite recursion, since each term may be assigned an ordinal rank, the obvious "is a subterm of" relation is well-founded. Let $\mathbf{C} =_{df} \{g^B_\alpha \mid B \subseteq A, \alpha \in Ord\}$.

The standard notions of a *free occurrence* and of a *bound occurrence* of a variable in a *CSP*-term are assumed, and $fv(P)$ denotes the set of variables which occur free in the term P. A term P is said to be *closed* iff $fv(P) = \emptyset$. Let $\mathbf{P}$ denote the set of all closed terms. If P, Q are terms and $X \in Var$ then $P[Q/X]$ denotes the term obtained by substituting Q for all free occurrences of X in P with change of bound variables if necessary. A ***substitution*** is a mapping $\sigma : Var \to \mathbf{P}$. Let *Sub* denote the set of all substitutions. Each $\sigma \in Sub$ determines a mapping (also denoted) $\sigma : \mathbf{E} \to \mathbf{P}$ such that for $P \in \mathbf{E}$, $\sigma[\![P]\!]$ denotes the term obtained by substituting $\sigma[\![X]\!]$ for each free occurrence in P of each variable X.

In what follows unless it is stated to the contrary it is assumed that $a, b \in A$, $B, C \subseteq A$, $s, t \in A^*$, $f \in AT$, $X \in Var$, $g \in \mathbf{C}$, $P, Q, R \in \mathbf{E}$ and $\sigma \in Sub$.

In the failures-divergences model a *process* is a pair $N = \langle F, D \rangle$ such that $F \subseteq A^* \times Pow(A)$ and $F \neq \emptyset$, $D \subseteq A^*$, and

$$
\begin{array}{lrcl}
(P1) & \langle st, \emptyset \rangle \in F & \Rightarrow & \langle s, \emptyset \rangle \in F \\
(P2) & \langle t, B \rangle \in F \wedge C \subseteq B & \Rightarrow & \langle t, C \rangle \in F \\
(P3) & \langle t, B \rangle \in F \wedge \forall a \in C. \langle t\langle a \rangle, \emptyset \rangle \notin F & \Rightarrow & \langle t, B \cup C \rangle \in F \\
(P4) & (\forall B' \subseteq B. B' \text{finite} \Rightarrow \langle t, B' \rangle \in F) & \Rightarrow & \langle t, B \rangle \in F \\
(P5) & s \in D & \Rightarrow & st \in D \\
(P6) & s \in D & \Rightarrow & \langle st, B \rangle \in F.
\end{array}
$$

Let $N = \langle F, D \rangle$ be a process. Define

$$
\begin{array}{rcl}
failures(N) & = & F \\
divergences(N) & = & D \\
traces(N) & = & \{t \mid \langle t, \emptyset \rangle \in F\} \\
initials(N) & = & \{a \mid \langle a \rangle \in traces(N)\} \\
refusals(N) & = & \{B \mid \langle \varepsilon, B \rangle \in F\}
\end{array}
$$

and for $s \in traces(N)$ define

$$N \, after \, s = \langle \{\langle t, B \rangle \mid \langle st, B \rangle \in F\}, \{t \mid st \in D\} \rangle.$$

Note that for $s \in traces(N)$, N *after* s is a process. Let $\mathbf{N}$ denote the set of all processes. Define a binary relation $\sqsubseteq$ on $\mathbf{N}$ by setting for $N = \langle F, D \rangle$, $N' = \langle F', D' \rangle \in \mathbf{N}$

$$N \sqsubseteq N' \equiv F' \subseteq F \wedge D' \subseteq D.$$

Note that $\langle \mathbf{N}, \sqsubseteq \rangle$ is a partial order. Define

$$\bot =_{df} \langle A^* \times Pow(A), A^* \rangle.$$

Note that $\bot$ is a process and that $\bot \sqsubseteq N$ for $N \in \mathbf{N}$. Let U be a directed subset of $\mathbf{N}$. Define

$$\bigsqcup U =_{df} \langle \bigcap \{F \mid \langle F, D \rangle \in U\}, \bigcap \{D \mid \langle F, D \rangle \in U\} \rangle.$$

Note that $N = \bigsqcup U$ is a process, $M \sqsubseteq N$ for each $M \in U$, and if $N' \in \mathbf{N}$ and $M \sqsubseteq N'$ for each $M \in U$ then $N \sqsubseteq N'$. Hence ($\mathbf{N}$, $\sqsubseteq$, $\bigsqcup$, $\bot$), the *failures-divergences model*, is a complete partial order.

Define operators $B \rightarrow$ on $B \rightarrow \mathbf{N}$, $\sqcap$, $\Box$, ${}_B\|_C$, $|||$ and ; on $\mathbf{N} \times \mathbf{N}$ and $\backslash a$, $f[\ ]$ and $f^{-1}[\ ]$ on $\mathbf{N}$ as follows. Let $N = \langle F, D \rangle$, $N' = \langle F', D' \rangle$ and for $b \in B$, $N_b = \langle F_b, D_b \rangle$ be processes. Then

$$
\begin{aligned}
B \to (\lambda b.V_b) &= \langle F_0, B_0\rangle \text{ where} \\
D_0 &= \{bt \mid b \in B \ \wedge \ t \in D_b\} \\
F_0 &= \{\langle \varepsilon, C\rangle \mid B \cap C = \emptyset\} \cup \{\langle bt, C\rangle \mid b \in B \ \wedge \ \langle t, C\rangle \in F_b\}
\end{aligned}
$$

$$
\begin{aligned}
N \sqcap N' &= \langle F_1, D_1\rangle \text{ where} \\
D_1 &= D \cup D' \\
F_1 &= F \cup F'
\end{aligned}
$$

$$
\begin{aligned}
N \Box N' &= \langle F_2, D_2\rangle \text{ where} \\
D_2 &= D \cup D' \\
F_2 &= \{\langle \varepsilon, B\rangle \mid \langle \varepsilon, B\rangle \in F \cap F'\} \cup \{\langle t, B\rangle \mid t \neq \varepsilon \ \wedge \ \langle t, B\rangle \in F \cup F'\} \\
&\quad \cup \{\langle t, B\rangle \mid t \in D_2\}
\end{aligned}
$$

$$
\begin{aligned}
N \ {}_B\|_C \ N' &= \langle F_3, D_3\rangle \text{ where} \\
D_3 &= \{st \mid s \in (B \cup C)^* \ \wedge \ ((s|B \in D \ \wedge \ s|C \in \mathit{traces}(N')) \ \vee \\
&\quad ((s|B \in \mathit{traces}(N) \ \wedge \ s|C \in D'))\} \\
F_3 &= \{\langle t, A' \cup B' \cup C'\rangle \mid t \in (B \cup C)^* \ \wedge \ B' \subseteq B \ \wedge \ C' \subseteq C \\
&\quad \wedge \ A' \subseteq A - (B \cap C) \ \wedge \ \langle t|B, B'\rangle \in F \ \wedge \ \langle t|C, C'\rangle \in F'\} \\
&\quad \cup \{\langle t, A'\rangle \mid t \in D_3\}
\end{aligned}
$$

$$
\begin{aligned}
N \,|||\, N' &= \langle F_4, D_4\rangle \text{ where} \\
D_4 &= \{r \mid \exists s, t.\, r \in \mathit{merge}\langle s, t\rangle \ \wedge \\
&\quad ((s \in D \ \wedge \ t \in \mathit{traces}(N')) \ \vee \ (s \in D' \ \wedge \ t \in \mathit{traces}(N))\} \\
F_4 &= \{\langle r, B\rangle \mid \exists s, t.\, r \in \mathit{merge}\langle s, t\rangle \wedge \langle s, B\rangle \in F \wedge \langle t, B\rangle \in F'\} \cup \{\langle r, B\rangle \mid r \in D_4\}
\end{aligned}
$$

$$
\begin{aligned}
N; N' &= \langle F_5, D_5\rangle \text{ where} \\
D_5 &= \{st \mid s \text{ tick} - \text{free} \ \wedge \ s \in D \ \wedge \ t \in A^*\} \\
&\quad \cup \{st \mid s \text{ tick} - \text{free} \ \wedge \ s\langle\surd\rangle \in \mathit{traces}(N) \ \wedge \ t \in D'\} \\
F_5 &= \{\langle s, B\rangle \mid s \text{ tick} - \text{free} \ \wedge \ \langle s, B \cup \{\surd\}\rangle \in F\} \cup \{\langle st, B\rangle \mid s \text{ tick} - \text{free} \ \wedge \\
&\quad s\langle\surd\rangle \in \mathit{traces}(N) \ \wedge \ \langle t, B\rangle \in F'\} \cup \{\langle t, B\rangle \mid t \in D_5\}
\end{aligned}
$$

$$
\begin{aligned}
N \backslash a &= \langle F_6, D_6\rangle \text{ where} \\
D_6 &= \{(s\backslash a)t \mid s \in D\} \cup \{(s\backslash a)t \mid \forall n.\, s\langle a\rangle^n \in \mathit{traces}(N)\} \\
F_6 &= \{\langle t\backslash a, B\rangle \mid \langle t, B \cup \{a\}\rangle \in F\} \cup \{\langle t, B\rangle \mid t \in D_6\}
\end{aligned}
$$

$$
\begin{aligned}
f[N] &= \langle F_7, D_7\rangle \text{ where} \\
D_7 &= \{f(s)t \mid s \in D\} \\
F_7 &= \{\langle f(t), B\rangle \mid \langle t, f^{-1}(B)\rangle \in F\} \cup \{\langle t, B\rangle \mid t \in D_7\}
\end{aligned}
$$

$$
\begin{aligned}
f^{-1}[N] &= \langle F_8, D_8\rangle \text{ where} \\
D_8 &= \{t \mid f(t) \in D\} \\
F_8 &= \{\langle t, B\rangle \mid \langle f(t), f(B)\rangle \in F\} \cup \{\langle t, B\rangle \mid t \in D_8\}.
\end{aligned}
$$

Lemma 1. $B \rightarrow$ is a continuous mapping of $B \rightarrow \mathbf{N}$ into $\mathbf{N}$. Each of $\sqcap$, $\Box$, ${}_B\|_C$, $|||$, and ; is a continuous mapping of $\mathbf{N} \times \mathbf{N}$ into $\mathbf{N}$. Each of $\backslash a$, $f[\ ]$ and $f^{-1}[\ ]$ is a continuous mapping of $\mathbf{N}$ into $\mathbf{N}$.

Proof: For a proof of this lemma see [BHR,B,R]. $\Box$(Lemma 1)

Let $Fix : [\mathbf{N} \rightarrow \mathbf{N}] \rightarrow \mathbf{N}$ denote the least fixed point operator. A *(process) environment* is a mapping $\nu : Var \rightarrow \mathbf{N}$. Let Env denote the set of all environments. Define $\mathcal{N} : \mathbf{E} \rightarrow Env \rightarrow \mathbf{N}$ by recursion by setting for $\ddagger \in \{\sqcap, \Box, {}_B\|_C , |||, ;\}$, $\dagger \in \{\backslash a, f[\ ], f^{-1}[\ ]\}$ and $\nu \in Env$

$$\begin{aligned}
\mathcal{N}[\![X]\!]\nu &= \nu[\![X]\!] \\
\mathcal{N}[\![P \ddagger Q]\!]\nu &= (\mathcal{N}[\![P]\!]\nu) \ddagger (\mathcal{N}[\![Q]\!]\nu) \\
\mathcal{N}[\![\dagger P]\!]\nu &= \dagger(\mathcal{N}[\![P]\!]\nu) \\
\mathcal{N}[\![B \rightarrow g]\!]\nu &= B \rightarrow (\lambda b.\mathcal{N}[\![g(b)]\!]\nu) \\
\mathcal{N}[\![\mu X.P]\!]\nu &= Fix(\lambda N.\mathcal{N}[\![P]\!](\nu \oplus \{X \mapsto N\})).
\end{aligned}$$

Note that if $P \in \mathbf{P}$ then $\mathcal{N}[\![P]\!]$ is a constant function. It is convenient also to write $\mathcal{N}[\![P]\!]$ for its constant value.

2. An operational semantics for CSP

The operational semantics is given in terms of a family $\{\xrightarrow{x} \mid x \in A^+\}$ of binary "transition relations" on terms, where $A^+ = A \cup \{\tau\}$ with τ a symbol not in A. The intended interpretation is that $P \xrightarrow{a} Q$ iff the process represented by P may evolve by performing the action a into the process represented by Q, and that $P \xrightarrow{\tau} Q$ iff the process represented by P may evolve in a manner invisible to, and outwith the control of, its environment into the process represented by Q. (cf. Milner's use of the symbol τ in *CCS* [M].)

The *transition relations* are the family of relations $\{\xrightarrow{x} \mid x \in A^+\}$ on terms defined by the following syntax-directed *transition rules.* To reduce slightly the number of rules required it is convenient to extend each alphabet transformation f to a mapping (also denoted) $f : A^+ \rightarrow A^+$ by setting $f(\tau) = \tau$. The transition rules are as follows.

$$\frac{}{(B \rightarrow g) \xrightarrow{b} g(b)} \quad (b \in B)$$

$$\frac{}{P \sqcap Q \xrightarrow{\tau} P} \qquad \frac{}{P \sqcap Q \xrightarrow{\tau} Q}$$

$$\frac{}{\mu X.P \xrightarrow{\tau} P[\mu X.P/X]}$$

$$\frac{P \xrightarrow{\tau} P'}{P \Box Q \xrightarrow{\tau} P' \Box Q} \qquad \frac{Q \xrightarrow{\tau} Q'}{P \Box Q \xrightarrow{\tau} P \Box Q'}$$

$$\frac{P \xrightarrow{a} P'}{P \Box Q \xrightarrow{a} P'} \qquad \frac{Q \xrightarrow{a} Q'}{P \Box Q \xrightarrow{a} Q'}$$

$$\frac{P \xrightarrow{\tau} P'}{P\ {}_B\|_C\ Q \xrightarrow{\tau} P'\ {}_B\|_C\ Q} \qquad \frac{Q \xrightarrow{\tau} Q'}{P\ {}_B\|_C\ Q \xrightarrow{\tau} P\ {}_B\|_C\ Q'}$$

$$\frac{P \xrightarrow{a} P'}{P\ {}_B\|_C\ Q \xrightarrow{a} P'\ {}_B\|_C\ Q} \quad (a \in B - C)$$

$$\frac{Q \xrightarrow{a} Q'}{P\ {}_B\|_C\ Q \xrightarrow{a} P\ {}_B\|_C\ Q'} \quad (a \in C - B)$$

$$\frac{P \xrightarrow{a} P' \quad Q \xrightarrow{a} Q'}{P\ {}_B\|_C\ Q \xrightarrow{a} P'\ {}_B\|_C\ Q'} \quad (a \in B \cap C)$$

$$\frac{P \xrightarrow{x} P'}{P \,|||\, Q \xrightarrow{x} P' \,|||\, Q} \qquad \frac{Q \xrightarrow{x} Q'}{P \,|||\, Q \xrightarrow{x} P \,|||\, Q'}$$

$$\frac{P \xrightarrow{x} P'}{P; Q \xrightarrow{x} P'; Q} \quad (x \neq \surd)$$

$$\frac{P \xrightarrow{\surd} P'}{P; Q \xrightarrow{\tau} Q}$$

$$\frac{P \xrightarrow{x} P'}{P \backslash a \xrightarrow{x} P' \backslash a} \quad (x \neq a)$$

$$\frac{P \xrightarrow{a} P'}{P \backslash a \xrightarrow{\tau} P' \backslash a}$$

$$\frac{P \xrightarrow{x} P'}{f[P] \xrightarrow{y} f[P']} \quad (y = f(x))$$

$$\frac{P \xrightarrow{x} P'}{f^{-1}[P] \xrightarrow{y} f^{-1}[P']} \quad (f(y) = x)$$

Lemma 2. Let $P \in \mathbf{E}$ and $x \in A^+$. Then the multiset whose elements are those Q such that $P \xrightarrow{x} Q$, with the multiplicity of Q being the number of ways in which $P \xrightarrow{x} Q$ may be inferred from the transition rules, is finite.

Proof: The proof of this lemma, which is a simple induction on structure, is omitted. □(Lemma 2)

It is convenient to abbreviate $\exists Q.\, P \xrightarrow{x} Q$ by $P \xrightarrow{x}$. Let $\xRightarrow{\varepsilon}$ denote the reflexive and transitive closure of $\xrightarrow{\tau}$ and let $\xRightarrow{a} =_{df} \xRightarrow{\varepsilon}\xrightarrow{a}\xRightarrow{\varepsilon}$ where juxtaposition denotes relational composition. Then define $\xRightarrow{t}$ for $t = as \in A^{+*}$ by recursion by setting

$$P \xRightarrow{t} Q \text{ iff } \exists R.\, P \xRightarrow{a} R \wedge R \xRightarrow{s} Q.$$

P is *stable* iff $\neg(P \xrightarrow{\tau})$. Define the *refusal relation* $ref \subseteq \mathbf{E} \times Pow(A)$ by setting

$$P \; ref \; B \text{ iff } P \text{ is stable } \wedge \forall a \in B.\, \neg(P \xrightarrow{a}).$$

Define the *divergence relation* $\uparrow \subseteq \mathbf{E}$ by setting

$$P \uparrow \text{ iff } \exists \langle P_i \mid i < \omega \rangle.\, P_0 = P \wedge \forall i.\, P_i \xrightarrow{\tau} P_{i+1}.$$

Now define $\mathcal{P}_0 : \mathbf{P} \to Pow(A^* \times Pow(A))$ and $\mathcal{P}_1 : \mathbf{P} \to Pow(A^*)$ by setting

$$\begin{aligned} \mathcal{P}_0[\![P]\!] &=_{df} \{\langle t, B\rangle \mid \exists Q. P \xRightarrow{t} Q \wedge Q \; ref \; B\} \cup \{\langle st, B\rangle \mid \exists Q. P \xRightarrow{s} Q \wedge Q \uparrow\} \\ \mathcal{P}_1[\![P]\!] &=_{df} \{st \mid \exists Q. P \xRightarrow{s} Q \wedge Q \uparrow\}. \end{aligned}$$

<u>Lemma 3.</u> For $P \in \mathbf{P}$, $\langle \mathcal{P}_0[\![P]\!], \mathcal{P}_1[\![P]\!]\rangle$ is a process.

Proof: Of the clauses (P1)–(P6) in the definition of "process" only (P4) is not immediately obvious. In establishing this condition, and in other contexts, the following lemma is useful.

<u>Lemma 4.</u> Let $Q \in \mathbf{E}$ and $t \in A^*$. Then
(a) $\exists s \leq t.\, \exists R.\, Q \xRightarrow{s} R \wedge R \uparrow$ or
(b) $\{R \mid Q \xRightarrow{t} R\}$ is finite.

Proof: This result is most easily established by considering the representation of the behaviour of Q as determined by the transition relations as a "labelled transition diagram." This concept is defined formally in the Appendix. Informally, the labelled transition diagram representing the term Q is the tree T with nodes labelled by terms and arcs labelled by elements of A^+ such that the root node is labelled Q, and such that there is an arc labelled x from a node labelled R to a node labelled R' if and only if $R \xrightarrow{x} R'$. By Lemma 2, T is finite-branching. With each node n in T is associated a sequence $r \in A^*$: if $u \in A^{+*}$ is the sequence of labels on the arcs comprising the path in T from the root node to n, then $r = u \mid A$. Let T' be the tree obtained from T by deleting every node whose associated sequence is not a subsequence of t and deleting every arc leading to such a node. Then T' is itself a finite-branching tree. If T' is finite then (b) holds, while if T' is infinite then by König's Lemma there is an infinite path through T', and hence (a) holds. □(Lemma 4)

Returning to the proof of Lemma 3, let $\mathcal{P}_0[\![P]\!] = F$ and suppose that $\forall B' \subseteq B.\, B'$ finite $\Rightarrow \langle t, B'\rangle \in F$ and that B is infinite. By Lemma 4, either $\exists s \leq t.\, \exists Q.\, P \stackrel{s}{\Longrightarrow} Q \wedge Q \uparrow$, in which case $\langle t, B\rangle \in F$ by the definition of $\mathcal{P}_1$, or $\Gamma = \{Q \mid P \stackrel{t}{\Longrightarrow} Q \wedge Q \text{ is stable}\}$ is finite. In the latter case let $\langle Q_1 \ldots Q_k\rangle$ be an enumeration of the stable terms in Γ with $k \geq 1$. If $\forall i.\, \neg(Q_i\ ref\ B)$ then $\forall i.\, \exists a_i \in B.\, \neg(Q_i\ ref\ \{a_i\})$, when setting $B' = \{a_i \mid 1 \leq i \leq k\}$, $\forall i.\, \neg(Q_i\ ref\ B')$. But $\langle t, B'\rangle \in F$, a contradiction. □(Lemma 3)

For $P \in \mathbf{P}$ set

$$\mathcal{P}[\![P]\!] =_{df} \langle \mathcal{P}_0[\![P]\!], \mathcal{P}_1[\![P]\!]\rangle.$$

Then by Lemma 3, $\mathcal{P} : \mathbf{P} \to \mathbf{N}$. Define a mapping (also denoted) $\mathcal{P} : \mathbf{E} \to Sub \to \mathbf{N}$ by setting

$$\mathcal{P}[\![P]\!]\sigma =_{df} \mathcal{P}[\![\sigma[\![P]\!]]\!].$$

Note that if $P \in \mathbf{P}$ then $\mathcal{P}[\![P]\!]$ denotes both a constant function and its constant value.

3. The congruence of the semantics

Define a mapping $\hat{\ } : Sub \to Env$ by setting

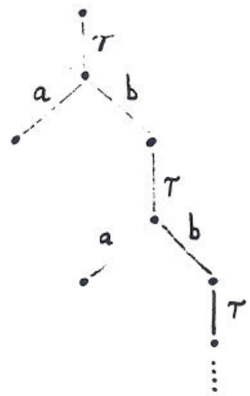
$$\hat{\sigma}[\![X]\!] =_{df} \mathcal{P}[\![\sigma[\![X]\!]]\!].$$

The congruence of the operational and the denotational semantics of the language may be stated as follows: for $P \in \mathbf{E}$ and $\sigma \in Sub$

$$\mathcal{P}[\![P]\!]\sigma = \mathcal{N}[\![P]\!]\hat{\sigma}.$$

To establish this identity we introduce an intermediate semantics which uses a model similar to that underlying the operational semantics (synchronization trees) but which is denotational and uses an abstract fixed point theory (that of complete metric spaces).

The concept of "synchronization tree" was introduced by Milner [M]. Informally, a "synchronization tree" (over A^+) is a tree whose arcs are labelled by elements of A^+. An example of the pictorial representation of such a tree is the following:



where the vertical dots indicate that the tree is of infinite depth and exhibits the regular structure apparent from this picture.

The standard way of constructing a class of synchronization trees would be to use multiset powerdomains and a recursive domain equation. By exploiting the fact that in the present proof we need consider only synchronization trees in which the number of identically labelled arcs from any node is finite, a more direct construction is sufficient. The main points of this construction, which is presented in the Appendix, are as follows.

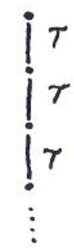
There are a set $\mathbf{T}$ of *synchronization trees* and operations $x.$ $(x \in A^+)$, $+$ and Σ as follows. The operations $x.$ $(x \in A^+)$, which insert a single initial arc labelled x, and $+$, which joins its arguments at a common root, may be represented pictorially as follows.

The operator Σ is such that if I is a set, $\{T_i \mid i \in I\} \subseteq \mathbf{T}$ and $\langle x_i \mid i \in I\rangle$ is such that for $i \in I$, $x_i \in A^+$ and for $x \in A^+$, $\{i \in I \mid x_i = x\}$ is finite, then $\sum_{i \in I} x_i.T_i \in \mathbf{T}$. It may be represented pictorially

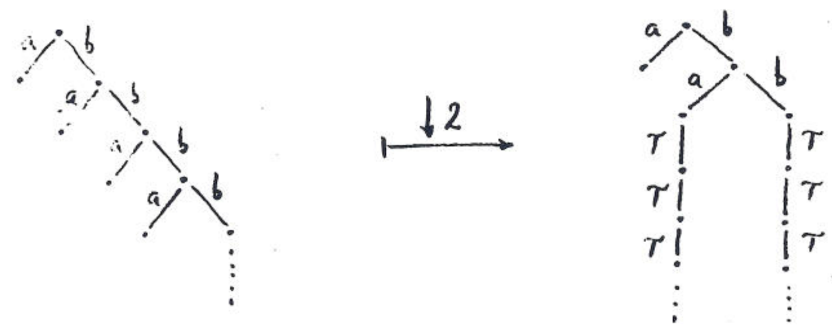
Conversely, if $T \in \mathbf{T}$ then there are a set I, $\{T_i \mid i \in I\} \subseteq \mathbf{T}$ and $\langle x_i \mid i \in I\rangle$ such that for $i \in I$, $x_i \in A^+$, and for $x \in A^+$, $\{i \in I \mid x_i = x\}$ is finite, and such that $T = \sum_{i \in I} x_i.T_i$. Hence every synchronization tree may be expressed in the form $\sum_{i \in I} a_i.T_i + \sum_{i \in J} \tau.T_i'$

where for $i \in I$, $a_i \in A$, $T_i \in \mathbf{T}$, J is finite and for $i \in J$, $T_i' \in \mathbf{T}$, and for $a \in A$, $\{i \in I \mid a_i = a\}$ is finite.

For each $n < \omega$ there is an operation $\downarrow n : \mathbf{T} \to \mathbf{T}$ which corresponds to truncating the synchronization tree at the n^{th} level and inserting the infinite synchronization tree



as the successor of each n^{th} level node. For example



These operations provide a standard representation of each possible "n-step behaviour" which is closely related to the notion of approximation in the failures-divergences model.

Finally, defining $d_{\mathbf{T}} : \mathbf{T} \times \mathbf{T} \to [0,1]$ by setting

$$d_{\mathbf{T}}\langle S, T\rangle =_{df} \inf \{2^{-n} \mid S \downarrow n = T \downarrow n\}$$

we have:

<u>Lemma 5.</u> $\langle \mathbf{T}, d_{\mathbf{T}}\rangle$ is a complete metric space.

Proof: See the Appendix. □(Lemma 5)

This completes the present summary of the material contained in the Appendix.

In order to establish the existence of certain operators on synchronization trees we define metrics $d_{\mathbf{U}}$ and $b_{\mathbf{B}}$ on $\mathbf{U} = \mathbf{T} \to \mathbf{T}$ and $\mathbf{B} = \mathbf{T} \times \mathbf{T} \to \mathbf{T}$ respectively and use Banach's fixed point theorem to establish the existence of fixed points of certain mappings on the complete metric spaces $\langle \mathbf{U}, d_{\mathbf{U}}\rangle$ and $\langle \mathbf{B}, d_{\mathbf{B}}\rangle$. These fixed points will be the desired operators.

Let J be any nonempty set. Define

$$d_J : (J \to \mathbf{T}) \times (J \to \mathbf{T}) \to [0,1]$$

by setting for $\alpha, \beta \in J \to \mathbf{T}$

$$d_J\langle \alpha, \beta \rangle = max\{d_{\mathbf{T}}\langle \alpha(j), \beta(j)\rangle \mid j \in J\}.$$

Lemma 6. If $J \neq \emptyset$ then $\langle J \to \mathbf{T}, d_J \rangle$ is a complete metric space.

Proof: The proof is straightforward and is omitted. □(Lemma 6)

The development and general results which follow will be applied to the spaces $\langle \mathbf{U}, d_{\mathbf{U}} \rangle$, $\langle \mathbf{B}, d_{\mathbf{B}} \rangle$ and $\langle (B \to \mathbf{T}) \to \mathbf{T}, d_{(B \to \mathbf{T}) \to \mathbf{T}} \rangle$ for $B \subseteq A$.

Let $\langle M, d \rangle$ be a metric space. A mapping $G : M \to M$ is *contractive* iff there is a c with $0 \leq c < 1$ such that for $X, Y \in M$

$$d\langle G(X), G(Y) \rangle \leq c.d\langle X, Y \rangle.$$

The following standard result is known as Banach's fixed point theorem or the contraction mapping theorem.

Lemma 7. If $\langle M, d \rangle$ is a complete metric space and $G : M \to M$ is contractive, then G has a unique fixed point Y. Moreover if X is any point of M then setting $X_0 = X$ and for $i < \omega$, $X_{i+1} = G(X_i)$, $\langle X_i \mid i < \omega \rangle$ converges in M to Y. □(Lemma 7)

Weakening slightly the condition in the preceding definition, we obtain the following. A mapping $G : M \to M$ is *nonexpansive* iff for $X, Y \in M$

$$d\langle G(X), G(Y) \rangle \leq d\langle X, Y \rangle.$$

Now let J be any nonempty set and set $M = J \to \mathbf{T}$ and $d = d_J$. For $n < \omega$ define $\downarrow n : M \to M$ by setting for $X \in M$ and $j \in J$

$$(X \downarrow n)(j) =_{df} X(j) \downarrow n.$$

A mapping $G : M \to M$ is *nondestructive* iff for $X \in M$ and $n < \omega$

$$G(X) \downarrow n = G(X \downarrow n) \downarrow n.$$

Furthermore a mapping $G : M \to M$ is *constructive* iff for $X \in M$ and $n < \omega$

$$G(X) \downarrow n+1 = G(X \downarrow n) \downarrow n+1.$$

The following lemma establishes some useful relationships among the above concepts.

Lemma 8. Suppose that $J \neq \emptyset$, $M = J \to \mathbf{T}$, $d = d_J$ and $G : M \to M$. Then
(a) G is nonexpansive iff G is nondestructive, and
(b) G is contractive iff G is constructive.

Proof: (a) Suppose G is nonexpansive and $X \in M$. Then for $n < \omega$, since for $k \leq n$, $X \downarrow k = (X \downarrow n) \downarrow k$,

$$d\langle G(X), G(X \downarrow n)\rangle \leq d\langle X, X \downarrow n\rangle \leq 2^{-n}.$$

Hence $d\langle G(X) \downarrow n, G(X \downarrow n) \downarrow n\rangle = 0$, and so $G(X) \downarrow n = G(X \downarrow n) \downarrow n$. Hence G is nondestructive. Now suppose that G is nondestructive and $X, Y \in M$. If $X = Y$ then $d\langle G(X), G(Y)\rangle = 0 = d\langle X, Y\rangle$. So suppose that $X \neq Y$ and n is least such that $X \downarrow n+1 \neq Y \downarrow n+1$, so that $d\langle X, Y\rangle = 2^{-n}$. Then for $k \leq n$

$$G(X) \downarrow k = G(X \downarrow k) \downarrow k = G(Y \downarrow k) \downarrow k = G(Y) \downarrow k$$

so $d\langle G(X), G(Y)\rangle \leq 2^{-n} = d\langle X, Y\rangle$. Hence G is nonexpansive.
(b) Suppose G is contractive. Then for $X, Y \in M$, $d\langle G(X), G(Y)\rangle \leq \frac{1}{2}.d\langle X, Y\rangle$ by the definition of the metric. Let $X \in M$. Then for $n < \omega$, since for $k \leq n$, $X \downarrow k = (X \downarrow n) \downarrow k$,

$$d\langle G(X), G(X \downarrow n)\rangle \leq \frac{1}{2}.d\langle X, X \downarrow n\rangle \leq 2^{-(n+1)}.$$

Hence $d\langle G(X) \downarrow n+1, G(X \downarrow n) \downarrow n+1\rangle = 0$ so $G(X) \downarrow n+1 = G(X \downarrow n) \downarrow n+1$. Thus G is constructive. Now suppose that G is constructive. Then certainly G is nondestructive and hence nonexpansive. Hence if $X, Y \in M$ with $X \neq Y$ and n is least such that $X \downarrow n+1 \neq Y \downarrow n+1$ so that $d\langle X, Y\rangle = 2^{-n}$, then by the proof of (a) $d\langle G(X), G(Y)\rangle \leq 2^{-n}$ and hence

$$G(X) \downarrow n+1 = G(X \downarrow n) \downarrow n+1 = G(Y \downarrow n) \downarrow n+1 = G(Y) \downarrow n+1,$$

and so $d\langle G(X), G(Y)\rangle \leq \frac{1}{2}.2^{-n} = \frac{1}{2}.d\langle X, Y\rangle$. Hence G is contractive. □(Lemma 8)

The following proposition is an immediate consequence of Proposition 7, Lemma 8(b) and the fact that a closed subset of a complete metric space is complete.

Lemma 9. Let Θ be a predicate defined on M such that $\Gamma = \{X \in M \mid \Theta(X)\}$ is a nonempty closed subset of M. Let $G : M \to M$ be constructive and such that Γ is closed under G. Let Y be the unique fixed point of G. Then $Y \in \Gamma$. □(Lemma 9)

Now define $\sqcap \in \mathbf{B}$ by setting

$$S \sqcap T =_{df} \tau.S + \tau.T.$$

For $B \subseteq A$ define $B \to\in (B \to \mathbf{T}) \to \mathbf{T}$ by setting for $G \in (B \to \mathbf{T}) \to \mathbf{T}$

$$B \to (G) =_{df} \sum_{b \in B} b.G(b).$$

Note that $\sqcap$ and $B \to$ are nonexpansive (in fact contractive) on $\mathbf{B}$ and $(B \to \mathbf{T}) \to \mathbf{T}$ respectively. The preceding general results may be exploited to establish the existence of operators on synchronization trees corresponding to each of the remaining constructors of the language of *CSP*.

<u>Lemma 10.</u> There are nonexpansive operators $\Box$, ${}_B\|_C$, $|||$, $;$ $\in \mathbf{B}$ and $\backslash a$, $f[\,]$, $f^{-1}[\,] \in \mathbf{U}$ such that whenever $S, T \in \mathbf{T}$ and $S = \sum a_i.S_i + \sum \tau.S_i'$ and $T = \sum b_i.T_i + \sum \tau.T_i'$ then

$$\begin{aligned}
S \Box T &= \textstyle\sum a_i.S_i + \sum b_i.T_i + \sum \tau.(S_i' \Box T) + \sum \tau.(S \Box T_i') \\
S \;{}_B\|_C\; T &= \textstyle\sum_{a_i \in B-C} a_i.(S_i \;{}_B\|_C\; T) + \sum_{b_i \in C-B} b_i.(S \;{}_B\|_C\; T_i) \\
&\quad \textstyle+ \sum_{a_i = b_j \in B \cap C} a_i.(S_i \;{}_B\|_C\; T_j) + \sum \tau.(S_i' \;{}_B\|_C\; T) + \sum \tau.(S \;{}_B\|_C\; T_i') \\
S \,|||\, T &= \textstyle\sum a_i.(S_i \,|||\, T) + \sum b_i.(S \,|||\, T_i) + \sum \tau.(S_i' \,|||\, T) + \sum \tau.(S \,|||\, T_i') \\
S; T &= \textstyle\sum_{a_i \neq \surd} a_i.(S_i; T) + \sum \tau.(S_i'; T) + \sum_{a_i = \surd} \tau.T \\
S \backslash a &= \textstyle\sum_{a_i \neq a} a_i.(S_i \backslash a) + \sum \tau.(S_i' \backslash a) + \sum_{a_i = a} \tau.(S_i \backslash a) \\
f[S] &= \textstyle\sum f(a_i).f[S_i] + \sum \tau.f[S_i'] \\
f^{-1}[S] &= \textstyle\sum_i \sum_{f(b) = a_i} b.f^{-1}[S_i] + \sum \tau.f^{-1}[S_i'].
\end{aligned}$$

Moreover the operators are uniquely determined by the above equations.

Proof: The "defining equation" of each of the operators determines a contractive function on $\mathbf{U}$ or $\mathbf{B}$ as appropriate. For example, given any binary operators $\Box_1$ and $\Box_2$, substitution into the right hand side of the defining equation of $\Box$ yields operators $\Box_1'$ and $\Box_2'$ such that $d_{\mathbf{B}}(\Box_1', \Box_2') \leq (d_{\mathbf{B}}(\Box_1, \Box_2))/2$. Hence by Lemma 8(b) and Proposition 7, each of these functions has a unique fixed point which is the required operator. That each of the operators is nonexpansive follows immediately from the fact that it satisfies the appropriate equation by Lemma 9: each of the defining equations determines a function which preserves the property of "nonexpansiveness" and the latter represents a nonempty closed subset of $\mathbf{U}$ or $\mathbf{B}$ as appropriate. $\Box$(Lemma 10)

Now define the set *Tre* of *tree environments* by $Tre =_{df} Var \to \mathbf{T}$, and let d_{Tre} be the metric defined on *Tre* by taking $J = Var$ in the definition immediately preceding Lemma 6. We now define an intermediate semantic function $\mathcal{S} : \mathbf{E} \to Tre \to \mathbf{T}$ which plays a central rôle in the proof of the main result.

$\mathcal{S} : \mathbf{E} \to Tre \to \mathbf{T}$ is defined by recursion on structure by setting

$$
\begin{array}{rcl}
\mathcal{S}[\![X]\!] & = & \lambda\rho.\rho[\![X]\!] \\
\mathcal{S}[\![P \ddagger Q]\!] & \simeq & \lambda\rho.(\mathcal{S}[\![P]\!]\rho) \ddagger (\mathcal{S}[\![Q]\!]\rho) \\
\mathcal{S}[\![\dagger P]\!] & \simeq & \lambda\rho. \dagger(\mathcal{S}[\![P]\!]\rho) \\
\mathcal{S}[\![B \to g]\!] & \simeq & \lambda\rho.(B \to)(\lambda b : B.\mathcal{S}[\![g(b)]\!]\rho) \\
\mathcal{S}[\![\mu X.P]\!] & \simeq & \text{the unique fixed point of } H : (\mathit{Tre} \to \mathbf{T}) \to (\mathit{Tre} \to \mathbf{T}) \\
 & & \text{where } H = \lambda h.\lambda\rho.(\tau.\mathcal{S}[\![P]\!](\rho \oplus \{X \mapsto h(\rho)\})).
\end{array}
$$

That $\mathcal{S}$ is a total function is a consequence of preceding results. First note that $\mathcal{S}[\![X]\!]$ is nonexpansive on $\mathit{Tre} \to \mathbf{T}$. Note also that if $\mathcal{S}[\![P]\!]$ and $\mathcal{S}[\![Q]\!]$ are nonexpansive on $\mathit{Tre} \to \mathbf{T}$ then since $\ddagger$ and $\dagger$ are nonexpansive on $\mathbf{T} \times \mathbf{T}$ and $\mathbf{T}$ respectively, $\mathcal{S}[\![P \ddagger Q]\!]$ and $\mathcal{S}[\![\dagger P]\!]$ are nonexpansive on $\mathit{Tre} \to \mathbf{T}$. Furthermore if for $b \in B$, $\mathcal{S}[\![g(b)]\!]$ is nonexpansive on $\mathit{Tre} \to \mathbf{T}$ then since $B \to$ is nonexpansive on $B \to \mathbf{T}$, $\mathcal{S}[\![B \to g]\!]$ is nonexpansive on $\mathit{Tre} \to \mathbf{T}$. Finally if $\mathcal{S}[\![P]\!]$ is nonexpansive on $\mathit{Tre} \to \mathbf{T}$ then H, as defined in the final clause of the definition of $\mathcal{S}$, is constructive on $\mathit{Tre} \to \mathbf{T}$, since for $h, j \in \mathit{Tre} \to \mathbf{T}$

$$
\begin{array}{cl}
 & d_{\mathit{Tre}\to\mathbf{T}}\langle H(h), H(j)\rangle \\
= & \mathit{max}\ \{d_{\mathbf{T}}\langle \tau.\mathcal{S}[\![P]\!](\rho \oplus \{X \mapsto h(\rho)\}), \tau.\mathcal{S}[\![P]\!](\rho \oplus \{X \mapsto j(\rho)\})\rangle \mid \rho \in \mathit{Tre}\} \\
\leq & \frac{1}{2}.\mathit{max}\ \{d_{\mathbf{T}}\langle \mathcal{S}[\![P]\!](\rho \oplus \{X \mapsto h(\rho)\}), \mathcal{S}[\![P]\!](\rho \oplus \{X \mapsto j(\rho)\})\rangle \mid \rho \in \mathit{Tre}\} \\
\leq & \frac{1}{2}.\mathit{max}\ \{d_{\mathbf{T}}\langle h(\rho), j(\rho)\rangle \mid \rho \in \mathit{Tre}\} \\
= & \frac{1}{2}.d_{\mathit{Tre}}\langle h, j\rangle.
\end{array}
$$

using the nonexpansiveness of $\mathcal{S}[\![P]\!]$ on $\mathit{Tre} \to \mathbf{T}$. Note that $\{K \in \mathit{Tre} \to \mathbf{T} \mid K \text{ is nonexpansive}\}$ is a nonempty, closed subset of $\mathit{Tre} \to \mathbf{T}$. Hence by Lemma 9, H has a unique fixed point which is itself nonexpansive. This completes the proof that $\mathcal{S}$ is a total function.

For $n < \omega$ define $\downarrow n : \mathit{Tre} \to \mathit{Tre}$ by setting

$$\rho \downarrow n =_{df} \lambda X.\rho[\![X]\!] \downarrow n.$$

Of course the metric that can be defined using these operators is identical to d_{Tre}.

Lemma 11. Let $P \in \mathbf{E}, \rho \in \mathit{Tre}$ and $n < \omega$. Then

$$(\mathcal{S}[\![P]\!]\rho) \downarrow n = (\mathcal{S}[\![P]\!]\rho \downarrow n) \downarrow n.$$

Proof: This is an immediate consequence of Lemma 8(a) and the fact that $\mathcal{S}[\![P]\!]$ is nonexpansive on $\mathit{Tre} \to \mathbf{T}$. □(Lemma 11)

For $x \in A^+$ define $\xrightarrow{x} \subseteq \mathbf{T} \times \mathbf{T}$ by setting for $S, T \in \mathbf{T}$ with $S = \sum a_i.S_i + \sum \tau S_i'$

$$S \xrightarrow{x} T \text{ iff } \exists i.((x = a_i \wedge T = S_i) \vee (x = \tau \wedge T = S_i')).$$

It is convenient to abbreviate $\exists T.\, S \xrightarrow{x} T$ to $S \xrightarrow{x}$. Let $\stackrel{\epsilon}{\Longrightarrow}$ be the reflexive and transitive closure of $\xrightarrow{\tau}$ and let $\stackrel{a}{\Longrightarrow} =_{df} \stackrel{\epsilon}{\Longrightarrow}\xrightarrow{a}\stackrel{\epsilon}{\Longrightarrow}$. Then define $\stackrel{t}{\Longrightarrow}$ for $t = as \in A^*$ by recursion by setting

$$S \stackrel{t}{\Longrightarrow} T \text{ iff } \exists U.\, S \stackrel{a}{\Longrightarrow} U \ \wedge\ U \stackrel{s}{\Longrightarrow} T.$$

T is *stable* iff. $\neg(T \xrightarrow{\tau})$. Define the *refusal relation* $ref \subseteq \mathbf{T} \times Pow(A)$ by setting

$$T \ ref\ B \text{ iff } T \text{ is stable } \wedge \forall a \in B.\, \neg(T \xrightarrow{a}).$$

Define the *divergence relation* $\uparrow \subseteq \mathbf{T}$ by setting

$$T \uparrow \ \text{ iff } \forall k < \omega.\, \exists \langle T_0, \ldots, T_{k-1}\rangle.\, T_0 = T \ \wedge\ (0 \le i < k-1 \Rightarrow T_i \xrightarrow{\tau} T_{i+1}).$$

Now define $\mathcal{M}_0 : \mathbf{T} \to Pow(A^* \times Pow(A))$ and $\mathcal{M}_1 : \mathbf{T} \to Pow(A^*)$ by setting

$$\begin{aligned} \mathcal{M}_0(S) &=_{df} \{\langle t, B\rangle \mid \exists T.\, S \stackrel{t}{\Longrightarrow} T \ \wedge\ T\ ref\ B\} \cup \{\langle st, B\rangle \mid \exists T.\, S \stackrel{s}{\Longrightarrow} T \ \wedge\ T\uparrow\} \\ \mathcal{M}_1(S) &=_{df} \{st \mid \exists T.\, S \xrightarrow{s} T \ \wedge\ T\uparrow\}. \end{aligned}$$

Lemma 12. Let $S \in \mathbf{T}$ and $t \in A^*$. Then
(a) $\exists s \le t.\, \exists T.\, S \stackrel{s}{\Longrightarrow} T \wedge T\uparrow$ or
(b) $\{T \mid S \stackrel{t}{\Longrightarrow} T\}$ is finite.

Proof: Similar to that of Lemma 4. □(Lemma 12)

Lemma 13. Let $S \in \mathbf{T}$. Then $\langle \mathcal{M}_0(S), \mathcal{M}_1(S)\rangle$ is a process.

Proof: Similar to that of Lemma 3. □(Lemma 13)

For $S \in \mathbf{T}$ set

$$\mathcal{M}(S) =_{df} \langle \mathcal{M}_0(S), \mathcal{M}_1(S)\rangle.$$

Then by lemma 13, $\mathcal{M} : \mathbf{T} \to \mathbf{N}$. Note that it follows from the definition of $\mathcal{M}$ that for $S \in \mathbf{T}$, $\langle \mathcal{M}(S\downarrow n) \mid n < \omega\rangle$ is a chain in $\langle \mathbf{N}, \sqsubseteq\rangle$.

Lemma 14. Let $S \in \mathbf{T}$. Then $\mathcal{M}(S) = \bigsqcup\{\mathcal{M}(S\downarrow n) \mid n < \omega\}$.

Proof: Let $\mathcal{M}(S) = \langle F, D\rangle$ and for $n < \omega$, $\mathcal{M}(S\downarrow n) = \langle F_n, D_n\rangle$. From the definition of $\downarrow n$, it follows immediately that if $S \stackrel{t}{\Longrightarrow} T \wedge T\ ref\ B$ then $\exists k.\, \forall n \ge k.\, \exists T_n.\, S\downarrow n \stackrel{t}{\Longrightarrow} T_n \wedge T_n\ ref\ B$, and if $S \stackrel{s}{\Longrightarrow} T \wedge T\uparrow$ then $\exists k.\, \forall n \ge k.\, \exists T_n.\, S\downarrow n \stackrel{s}{\Longrightarrow} T_n \wedge T_n\uparrow$. Thus by the definition of $\mathcal{M}$, $\bigsqcup\{\mathcal{M}(S\downarrow n) \mid n < \omega\} \sqsubseteq \mathcal{M}(S)$.

Suppose that $r \in \bigcap D_n$. Then $\{T \mid \exists s \leq r.\, S \stackrel{s}{\Longrightarrow} T\}$ is an infinite finite-branching tree and hence by König's Lemma has an infinite path, so $r \in D$. Also if $\exists k.\, \forall n \geq k.\, \exists T_n.\, S \downarrow n \stackrel{t}{\Longrightarrow} T_n \wedge T_n\ ref\ B$, then from Lemma 12 it follows that $\langle t, B\rangle \in F$. Thus $\mathcal{M}(S) \sqsubseteq \bigsqcup\{\mathcal{M}(S \downarrow n) \mid n < \omega\}$. □(Lemma 14)

The transition relations determine for each term P an unique synchronization tree $\mathcal{T}[\![P]\!]$, obtained by simply deleting the terms from the nodes of the labelled transition diagram. (For the details of the construction of the mapping $\mathcal{T} : \mathbf{E} \to \mathbf{T}$ see the Appendix.) The mapping $\mathcal{T}$ is such that

$$\begin{array}{rcl} P \stackrel{x}{\longrightarrow} Q & \text{iff} & \mathcal{T}[\![P]\!] \stackrel{x}{\longrightarrow} \mathcal{T}[\![Q]\!] \\ P\ ref\ B & \text{iff} & \mathcal{T}[\![P]\!]\ ref\ B \\ P\uparrow & \text{iff} & \mathcal{T}[\![P]\!]\uparrow . \end{array}$$

Hence for $P \in \mathbf{P}$

$$\mathcal{M}(\mathcal{T}[\![P]\!]) = \mathcal{P}[\![P]\!].$$

We now establish some properties of the mapping $\mathcal{T}$ required for the proof of Lemma 16 below.

<u>Lemma 15.</u> Let $P, Q \in \mathbf{E}$, $\ddagger \in \{\Box, {}_B\|_C\, , |||, ;\}$ and $\dagger \in \{\backslash a, f[\,], f^{-1}[\,]\}$. Then

$$\begin{array}{rcl} \mathcal{T}[\![P \ddagger Q]\!] & = & \mathcal{T}[\![P]\!] \ddagger \mathcal{T}[\![Q]\!] \\ \mathcal{T}[\![\dagger P]\!] & = & \dagger\mathcal{T}[\![P]\!]. \end{array}$$

Proof: Note that two elements $S = \sum_{i\in I} a_i.S_i + \sum_{i\in J} \tau.S_i'$ and $T = \sum_{i\in I'} b_i.T_i + \sum_{i\in J'} \tau.T_i'$ of $\mathbf{T}$ are equal if and only if there are bijections $\alpha : I \leftrightarrow I'$ and $\beta : J \leftrightarrow J'$ such that

a) $b_{\alpha(i)} = a_i$ and $S'_{\alpha(i)} = S_i$ for all $i \in I$.

b) $T'_{\beta(i)} = T_i$ for all $i \in J$.

Let $\mathcal{T}[\![P]\!] = S = \sum a_i.S_i + \sum \tau.S_i'$, $\mathcal{T}[\![Q]\!] = T = \sum b_i.T_i + \sum \tau.T_i'$, and let $U = \sum c_i.U_i + \sum \tau.U_i' = \mathcal{T}[\![P \ddagger Q]\!]$ or $\mathcal{T}[\![\dagger P]\!]$ as appropriate. Then there are P_i, P_i', Q_i, Q_i' such that $P \stackrel{a_i}{\longrightarrow} P_i$ and $S_i = \mathcal{T}[\![P_i]\!]$, $P \stackrel{\tau}{\longrightarrow} P_i'$ and $S_i' = \mathcal{T}[\![P_i']\!]$, $Q_i \stackrel{b_i}{\longrightarrow} Q_i$ and $T_i = \mathcal{T}[\![Q_i]\!]$, and $Q \stackrel{\tau}{\longrightarrow} Q_i'$ and $T_i' = \mathcal{T}[\![Q_i']\!]$. Also there are R_i, R_i' such that $\mathcal{T}[\![R_i]\!] = U_i$, $\mathcal{T}[\![R_i']\!] = U_i'$ and $P \ddagger Q \stackrel{a_i}{\longrightarrow} R_i$ and $P \ddagger Q \stackrel{\tau}{\longrightarrow} R_i'$, or $\dagger P \stackrel{a_i}{\longrightarrow} R_i$ and $\dagger P \stackrel{\tau}{\longrightarrow} R_i'$ as appropriate.

We prove by induction on n (for all P, Q simultaneously) that for $n < \omega$

$$\begin{array}{rcl} (\mathcal{T}[\![P \ddagger Q]\!])\downarrow n & = & (\mathcal{T}[\![P]\!] \ddagger \mathcal{T}[\![Q]\!])\downarrow n \\ (\mathcal{T}[\![\dagger P]\!])\downarrow n & = & (\dagger\mathcal{T}[\![P]\!])\downarrow n. \end{array}$$

For $n = 0$ these equalities are trivial. Assume the equalities for n and let $m = n + 1$. We present the proof only for the operators $\Box$ and $\backslash a$; those for the other operators are similar.

$$
\begin{aligned}
&(S\Box T)\downarrow m \\
= \; & \sum a_i.(S_i\downarrow n)+\sum b_i.(T_i\downarrow n)+\sum \tau.(S_i'\Box T)\downarrow n+\sum \tau.(S\Box T_i')\downarrow n \\
= \; & \sum a_i.(\mathcal{T}[\![P_i]\!]\downarrow n)+\sum b_i.(\mathcal{T}[\![Q_i]\!]\downarrow n)+\sum \tau.(\mathcal{T}[\![P_i']\!]\Box \mathcal{T}[\![Q]\!])\downarrow n \\
& +\sum \tau.(\mathcal{T}[\![P]\!]\Box \mathcal{T}[\![Q_i']\!])\downarrow n \\
= \; & \sum a_i.(\mathcal{T}[\![P_i]\!]\downarrow n)+\sum b_i.(\mathcal{T}[\![Q_i]\!]\downarrow n)+\sum \tau.(\mathcal{T}[\![P_i'\Box Q]\!]\downarrow n)+\sum \tau.(\mathcal{T}[\![P\Box Q_i']\!]\downarrow n)
\end{aligned}
$$

by the induction hypothesis. It will be seen that the action/process pairs in the last line above correspond precisely to those deducible from $P\Box Q$ by the transition relations: each pair being there exactly as often as there are ways of deducing it. The definition of $\mathcal{T}$ thus implies $U\downarrow m=(S\Box T)\downarrow m$.

$$
\begin{aligned}
&(S\backslash a)\downarrow m \\
= \; & \textstyle\sum_{a_i\neq a} a_i.(\mathcal{T}[\![P_i]\!]\backslash a)\downarrow n+\sum \tau.(\mathcal{T}[\![P_i']\!]\backslash a)\downarrow n+\sum_{a_i=a}\tau.(\mathcal{T}[\![P_i]\!]\backslash a)\downarrow n \\
= \; & \textstyle\sum_{a_i\neq a} a_i.(\mathcal{T}[\![P_i\backslash a]\!])\downarrow n+\sum \tau.(\mathcal{T}[\![P_i'\backslash a]\!])\downarrow n+\sum_{a_i=a}\tau.(\mathcal{T}[\![P_i\backslash a]\!])\downarrow n.
\end{aligned}
$$

Again there is exactly one summand for each way of deducing a transition of $P\backslash a$ from the transition relations. The definition of $\mathcal{T}$ then implies $U\downarrow m=(S\backslash a)\downarrow m$.
This completes the sketch of the proof of Lemma 15. □(Lemma 15)

Define $\bar{\cdot}$: *Sub* → *Tre* by setting

$$\bar{\sigma}=\lambda X.\mathcal{T}[\![\sigma[\![X]\!]]\!].$$

Lemma 16. Let $P\in \mathbf{E}$ and $\sigma\in$ *Sub* . Then

$$\mathcal{T}[\![\sigma[\![P]\!]]\!]=\mathcal{S}[\![P]\!]\bar{\sigma}.$$

Proof: By induction on structure. First note that

$$\mathcal{T}[\![\sigma[\![X]\!]]\!]=\bar{\sigma}[\![X]\!]=\mathcal{S}[\![X]\!]\bar{\sigma}.$$

For the nondeterministic choice operator

$$
\begin{aligned}
\mathcal{T}[\![\sigma[\![P\sqcap Q]\!]]\!] &= \tau.\mathcal{T}[\![\sigma[\![P]\!]]\!]+\tau.\mathcal{T}[\![\sigma[\![Q]\!]]\!] \\
&= \tau.\mathcal{S}[\![P]\!]\bar{\sigma}+\tau.\mathcal{S}[\![Q]\!]\bar{\sigma} \\
&= \mathcal{S}[\![P\sqcap Q]\!]\bar{\sigma}.
\end{aligned}
$$

Suppose $\ddagger\in\{\Box,\ {}_B\|_C\ ,\ |||,;\}$. Then by Lemma 15

$$
\begin{aligned}
\mathcal{T}[\![\sigma[\![P\ddagger Q]\!]]\!] &= \mathcal{T}[\![\sigma[\![P]\!]]\!]\ddagger\mathcal{T}[\![\sigma[\![Q]\!]]\!] \\
&= \mathcal{S}[\![P]\!]\bar{\sigma}\ddagger\mathcal{S}[\![Q]\!]\bar{\sigma} \\
&= \mathcal{S}[\![P\ddagger Q]\!]\bar{\sigma}.
\end{aligned}
$$

Also for $\dagger\in\{\backslash a, f[\ ], f^{-1}[\ ]\}$ by Lemma 15

$$\begin{aligned}\mathcal{T}[\![\sigma[\![\dagger P]\!]]\!] &= \dagger\mathcal{T}[\![\sigma[\![P]\!]]\!] \\ &= \dagger\mathcal{S}[\![P]\!]\overline{\sigma} \\ &= \mathcal{S}[\![\dagger P]\!]\overline{\sigma}.\end{aligned}$$

For the guarded choice constructs

$$\begin{aligned}\mathcal{T}[\![\sigma[\![B \to g]\!]]\!] &= \textstyle\sum_{b\in B} b.\mathcal{T}[\![\sigma[\![g(b)]\!]]\!] \\ &= \textstyle\sum_{b\in B} b.\mathcal{S}[\![g(b)]\!]\overline{\sigma} \\ &= \mathcal{S}[\![B \to g]\!]\overline{\sigma}.\end{aligned}$$

Finally suppose that $P = \mu X.Q$. We prove by induction on n that for $n < \omega$, $(\mathcal{T}[\![\sigma[\![P]\!]]\!]) \downarrow n = (\mathcal{S}[\![P]\!]\overline{\sigma}) \downarrow n$. For $n = 0$ the equality is immediate. Assuming the equality for n and setting $m = n + 1$ then using Lemma 11

$$\begin{aligned}(\mathcal{T}[\![\sigma[\![P]\!]]\!]) \downarrow m &= (\tau.\mathcal{T}[\![(\sigma \oplus \{X \mapsto \sigma[\![P]\!]\})[\![Q]\!]]\!]) \downarrow m \\ &= \tau.(\mathcal{T}[\![(\sigma \oplus \{X \mapsto \sigma[\![P]\!]\})[\![Q]\!]]\!] \downarrow n) \\ &= \tau.(\mathcal{S}[\![Q]\!](\overline{\sigma} \oplus \{X \mapsto \mathcal{T}[\![\sigma[\![P]\!]]\!]\}) \downarrow n) \\ &= \tau.(\mathcal{S}[\![Q]\!](\overline{\sigma}\downarrow n \oplus \{X \mapsto (\mathcal{T}[\![\sigma[\![P]\!]]\!]) \downarrow n\}) \downarrow n) \\ &= \tau.(\mathcal{S}[\![Q]\!](\overline{\sigma}\downarrow n \oplus \{X \mapsto (\mathcal{S}[\![P]\!]\overline{\sigma}) \downarrow n\}) \downarrow n) \\ &= \tau.(\mathcal{S}[\![Q]\!]((\overline{\sigma} \oplus \{X \mapsto (\mathcal{S}[\![P]\!]\overline{\sigma})\}) \downarrow n) \downarrow n) \\ &= \tau.((\mathcal{S}[\![Q]\!](\overline{\sigma} \oplus \{X \mapsto (\mathcal{S}[\![P]\!]\overline{\sigma})\})) \downarrow n) \\ &= (\tau.(\mathcal{S}[\![Q]\!](\overline{\sigma} \oplus \{X \mapsto (\mathcal{S}[\![P]\!]\overline{\sigma})\}))) \downarrow m \\ &= (\mathcal{S}[\![P]\!]\overline{\sigma}) \downarrow m.\end{aligned}$$

This completes the proof of lemma 16. □(Lemma 16)

We now establish some properties of the mapping $\mathcal{M}$ required for the proof of Lemma 18 below.

<u>Lemma 17.</u> Let $S, T \in \mathbf{T}$, $\ddagger \in \{\sqcap, \Box, {}_B\|_C, |||, ;\}$, $\dagger \in \{\backslash a, f[\;], f^{-1}[\;]\}$ and suppose $g : B \to \mathbf{T}$. Then

$$\begin{aligned}\mathcal{M}(S \ddagger T) &= \mathcal{M}(S) \ddagger \mathcal{M}(T) \\ \mathcal{M}(\dagger S) &= \dagger\mathcal{M}(S) \\ \mathcal{M}(B \to g) &= B \to (\lambda b.\mathcal{M}(g(b))).\end{aligned}$$

Proof: We do prove this result in complete detail. Rather we prove the assertions in the cases $\ddagger = \Box$ and $\dagger = \backslash a$ and state a list of properties of synchronization trees from which the remaining cases may be established by similar arguments. First consider the case $\ddagger = \Box$.

<u>Lemma 17.1.</u> (1) $S\Box T \stackrel{\varepsilon}{\Longrightarrow} U$ iff $\exists S', T'.\, S \stackrel{\varepsilon}{\Longrightarrow} S'$, $T \stackrel{\varepsilon}{\Longrightarrow} T'$ and $U = S'\Box T'$.
(2) If $s \neq \varepsilon$ then $S\Box T \stackrel{s}{\Longrightarrow} U$ iff $S \stackrel{s}{\Longrightarrow} U$ or $T \stackrel{s}{\Longrightarrow} U$.

(3) $S \Box T$ *ref* B iff S *ref* B and T *ref* B.
(4) $S \Box T \uparrow$ iff $S \uparrow$ or $T \uparrow$.

Proof: The proof is straightforward and is omitted. $\Box$(Lemma 17.1)

Now let $N = \langle F, D \rangle = \mathcal{M}(S)$, $N' = \langle F', D' \rangle = \mathcal{M}(T)$, $N_0 = \langle F_0, D_0 \rangle = \mathcal{M}(S \Box T)$ and $N_1 = \langle F_1, D_1 \rangle = N \Box N'$.

Lemma 17.2. $N_0 = N_1$.

Proof: We first prove that $D_0 = D_1$.
Note that, by (2) and (4) above, $\exists U.\, S \Box T \stackrel{s}{\Longrightarrow} U$ and $U \uparrow$ if and only if *either* $\exists U.\, S \stackrel{s}{\Longrightarrow} U$ and $U \uparrow$ *or* $\exists U.\, T \stackrel{s}{\Longrightarrow} U$ and $U \uparrow$. Since $D_1 = D \cup D'$, the result is proved.

Now we prove that $F_0 = F_1$.
Since we already know that $D_0 = D_1$ it is sufficient to prove this result for refusals on non-divergent traces s. First suppose $\varepsilon \notin D_0$. If $\langle \varepsilon, B \rangle \in F \cap F'$ then by by Lemma 17.1 and the fact that if S' *ref* $B \wedge T'$ *ref* B then $S' \Box T'$ *ref* B, $\langle \varepsilon, B \rangle \in F_0$. If $S \Box T \stackrel{\varepsilon}{\Longrightarrow} U \wedge U$ *ref* B then by Lemma 17.1, $\exists S', T'.\, S \stackrel{\varepsilon}{\Longrightarrow} S' \wedge T \stackrel{\varepsilon}{\Longrightarrow} T' \wedge U = S' \Box T'$, so since then S' *ref* B and T' *ref* B, $\langle \varepsilon, B \rangle \in F \cap F'$ so $\langle \varepsilon, B \rangle \in F_1$.

If $t \neq \varepsilon$ and $t \notin D_0$. If $\langle t, B \rangle \in F \cup F'$ then by Lemma 17.1 (2), $\langle t, B \rangle \in F_0$. If $S \Box T \stackrel{s}{\Longrightarrow} U \wedge U$ *ref* B then by Lemma 17.1 (2), $\langle t, B \rangle \in F \cup F'$ so $\langle t, B \rangle \in F_1$. $F_0 = F_1$ now follows from $D_0 = D_1$. $\Box$(Lemma 17.2)

We now consider the case $\dagger = \backslash a$.

Lemma 17.3.
(1) $S \backslash a \stackrel{s}{\Longrightarrow} U$ iff $\exists t.\, \exists T.\, S \stackrel{t}{\Longrightarrow} T$, $U = T \backslash a$ and $s = t \backslash a$.
(2) $S \backslash a$ *ref* B iff S *ref* $B \cup \{a\}$.
(3) $S \backslash a \uparrow$ iff $\exists n.\, \exists T.\, S \stackrel{a^n}{\Longrightarrow} T \wedge T \uparrow$ or $\forall n.\, \exists U.\, S \stackrel{a^n}{\Longrightarrow} U$.

Proof: The proof is straightforward and is omitted. $\Box$(Lemma 17.3)

Now let $N = \langle F, D \rangle = \mathcal{M}(S)$, $N_0 = \langle F_0, D_0 \rangle = \mathcal{M}(S \backslash a)$ and $N_1 = \langle F_1, D_1 \rangle = N \backslash a$.

Lemma 17.4. $N_0 = N_1$.

Proof: We first prove that $D_0 = D_1$.
($\subseteq$) Suppose that s is minimal in D_0. Then there exists U such that $S \backslash a \stackrel{s}{\Longrightarrow} U$ and $U \uparrow$. By Lemma 17.3, $\exists U. S \backslash a \stackrel{s}{\Longrightarrow} U$ and $U \uparrow$ if and only if there exist t and T such that

$t\backslash a = s$, $U = T\backslash a$ and *either* $T\uparrow$ *or* $\forall n.\exists V.T \stackrel{a^n}{\Longrightarrow} V$. In the first case $t \in D$ and in the second $\forall n.t\langle a^n\rangle \in traces(N)$. In either case $s \in D_1$.
($\supseteq$) If t is minimal in D_1 then there is a minimal s such that $s\backslash a = t$ and *either* $s \in D$ *or* $\forall n.\, s\langle a^n\rangle \in traces(N)$. In the first case there is T such that $S \stackrel{s}{\Longrightarrow} T$ and $T\uparrow$, so that $t \in D_0$. In the second case, an application of König's lemma to a suitable subtree of S yields T such that $S \stackrel{s}{\Longrightarrow} T$ and $\forall n.\exists U.T \stackrel{a^n}{\Longrightarrow} U$. Again it follows that $s \in D_0$.

We now prove that $F_0 = F_1$. As in the case of $\Box$ it is sufficient to consider only non-divergent traces.
($\supseteq$) If $S \stackrel{s}{\Longrightarrow} U \wedge U\ ref\ B \cup \{a\}$ then by Lemma 17.3, $\langle s, B\rangle \in F_0$.
($\subseteq$) If $S\backslash a \stackrel{s}{\Longrightarrow} U \wedge U\ ref\ B$ then by Lemma 17.3, $\exists U'.\exists t.\, S \stackrel{t}{\Longrightarrow} U' \wedge t\backslash a = s \wedge U'\backslash a = U$. Since U is stable, $U'\ ref\ \{a\}$, and hence $\langle s, B\cup\{a\}\rangle \in F$ and so $\langle s, B\rangle \in F_1$. $F_0 = F_1$ now follows from $D_0 = D_1$. $\Box$(Lemma 17.4)

By similar arguments the remaining cases may be established using the following observations.

Lemma 17.5.

($\sqcap$1) $S \sqcap T \stackrel{s}{\Longrightarrow} U$ iff $(s = \varepsilon \wedge U = S \sqcap T)$ or $S \stackrel{s}{\Longrightarrow} U$ or $T \stackrel{s}{\Longrightarrow} U$.
($\sqcap$2) $\neg(S \sqcap T\ ref\ B)$ for any B.
($\sqcap$3) $S \sqcap T\uparrow$ iff $S\uparrow$ or $T\uparrow$.

(${}_B\|_C$ 1) $S\ {}_B\|_C\ T \stackrel{s}{\Longrightarrow} U$ iff $\exists S', T'.\exists r, t.\, r = s|B \wedge t = s|C \wedge S \stackrel{r}{\Longrightarrow} S' \wedge T \stackrel{t}{\Longrightarrow} T' \wedge U = S'\ {}_B\|_C\ T'$.
(${}_B\|_C$ 2) $S\ {}_B\|_C\ T\ ref\ B'$ iff S is stable, T is stable, $S\ ref\ B' \cap (B - C)$, $T\ ref\ B' \cap (C - B)$ and $\exists B_0, B_1.\, B_0 \cup B_1 = B' \cap B \cap C$, $S\ ref\ B_0$ and $T\ ref\ B_1$.
(${}_B\|_C$ 3) $S\ {}_B\|_C\ T\uparrow$ iff $S\uparrow$ or $T\uparrow$.

($|||$1) $S\,|||\,T \stackrel{u}{\Longrightarrow} U$ iff $\exists s, t.\exists S', T'.\, S \stackrel{s}{\Longrightarrow} S'$, $T \stackrel{t}{\Longrightarrow} T'$, $u \in merge(s, t)$ and $U = S'\,|||\,T'$.
($|||$2) $S\,|||\,T\ ref\ B$ iff $S\ ref\ B$ and $T\ ref\ B$.
($|||$3) $S\,|||\,T\uparrow$ iff $S\uparrow$ or $T\uparrow$.

(;1) $S \stackrel{s}{\Longrightarrow} S' \wedge s$ tick − free $\Rightarrow S;T \stackrel{s}{\Longrightarrow} S';T$.
(;2) $S \stackrel{s\surd}{\Longrightarrow} S' \wedge s$ tick − free $\Rightarrow S;T \stackrel{s}{\Longrightarrow} T$.
(;3) $S;T \stackrel{s}{\Longrightarrow} U \Rightarrow$ (s tick − free, $\exists S'.\, S \stackrel{s}{\Longrightarrow} S'$ and $U = S';T$) or ($\exists r, t.r$ tick − free, $s = rt$, $S \stackrel{r\surd}{\Longrightarrow} S'$ and $T \stackrel{t}{\Longrightarrow} U$).
(;4) $S;T\ ref\ B$ iff $S\ ref\ B$ or $S \stackrel{\surd}{\Longrightarrow}$ and $T\ ref\ B$.
(;5) $S;T\uparrow$ iff $S\uparrow$ or $S \stackrel{\surd}{\Longrightarrow}$ and $T\uparrow$.

($f[\,]$1) $f[S] \stackrel{s}{\Longrightarrow} U$ iff $\exists t.\exists T.\, f(t) = s$, $f[T] = U$ and $S \stackrel{t}{\Longrightarrow} T$.

$(f[\ ]1)$ $f[S] \stackrel{s}{\Longrightarrow} U$ iff $\exists t. \exists T. f(t) = s,\ f[T] = U$ and $S \stackrel{t}{\Longrightarrow} T$.
$(f[\ ]2)$ $f[S]$ *ref* B iff S *ref* $f^{-1}(B)$.
$(f[\ ]3)$ $f[S] \uparrow$ iff $S \uparrow$.

$(f^{-1}[\ ]1)$ $f^{-1}[S] \stackrel{s}{\Longrightarrow} U$ iff $\exists t. \exists T. S \stackrel{t}{\Longrightarrow} T,\ f(s) = t$ and $f^{-1}[T] = U$.
$(f^{-1}[\ ]2)$ $f^{-1}[S]$ *ref* B iff S *ref* $f(B)$.
$(f^{-1}[\ ]3)$ $f^{-1}[S] \uparrow$ iff $S \uparrow$.

$(B \rightarrow 1)$ $(B \rightarrow)(G) \stackrel{\varepsilon}{\Longrightarrow} T$ iff $T = (B \rightarrow)(G)$.
$(B \rightarrow 2)$ $(B \rightarrow)(G) \stackrel{s}{\Longrightarrow} T$ and $s \neq \varepsilon$ iff $\exists b \in B. \exists t. s = bt$ and $G(b) \stackrel{t}{\Longrightarrow} T$.
$(B \rightarrow 3)$ $(B \rightarrow)(G)$ *ref* C iff $B \cap C = \emptyset$.

Proof: The proofs are straightforward and are omitted. □(Lemma 17.5)

This completes the sketch of the proof of Lemma 17. □(Lemma 17)

Define $\cdot^* : \mathit{Tre} \rightarrow \mathit{Env}$ by setting

$$\rho^* =_{df} \lambda X. \mathcal{M}(\rho[\![X]\!]).$$

<u>Lemma 18.</u> Let $P \in \mathbf{E}$ and $\rho \in \mathit{Tre}$. Then

$$\mathcal{M}(\mathcal{S}[\![P]\!]\rho) = \mathcal{N}[\![P]\!]\rho^*.$$

Proof: By induction on structure. First note that

$$\mathcal{M}(\mathcal{S}[\![X]\!]\rho) = \mathcal{M}(\rho[\![X]\!]) = \rho^*[\![X]\!] = \mathcal{N}[\![X]\!]\rho^*.$$

Let $\ddagger \in \{\sqcap, \Box, {}_B\|_C, |||, ;\}$. Then by Lemma 17

$$\begin{aligned} \mathcal{M}(\mathcal{S}[\![P \ddagger Q]\!]\rho) &= \mathcal{M}(\mathcal{S}[\![P]\!]\rho \ddagger \mathcal{S}[\![Q]\!]\rho) \\ &= \mathcal{M}(\mathcal{S}[\![P]\!]\rho) \ddagger \mathcal{M}(\mathcal{S}[\![Q]\!]\rho) \\ &= \mathcal{N}[\![P]\!]\rho^* \ddagger \mathcal{N}[\![Q]\!]\rho^* \\ &= \mathcal{N}[\![P \ddagger Q]\!]\rho^*. \end{aligned}$$

Let $\dagger \in \{\backslash a, f[\ ], f^{-1}[\ ]\}$. Then by lemma 17

$$\begin{aligned} \mathcal{M}(\mathcal{S}[\![\dagger P]\!]\rho) &= \mathcal{M}(\dagger \mathcal{S}[\![P]\!]\rho) \\ &= \dagger \mathcal{M}(\mathcal{S}[\![P]\!]\rho) \\ &= \dagger \mathcal{N}[\![P]\!]\rho^* \\ &= \mathcal{N}[\![\dagger P]\!]\rho^*. \end{aligned}$$

For the guarded choice constructs again by Lemma 17

$$\begin{aligned}
\mathcal{M}(\mathcal{S}[\![B \to g]\!]\rho) &= \mathcal{M}(B \to (\lambda b.\mathcal{S}[\![g(b)]\!]\rho)) \\
&= B \to (\lambda b.\mathcal{M}(\mathcal{S}[\![g(b)]\!]\rho)) \\
&= B \to (\lambda b.\mathcal{N}[\![g(b)]\!]\rho^*) \\
&= \mathcal{N}[\![B \to g]\!]\rho^*.
\end{aligned}$$

Finally suppose $P = \mu X.Q$. Then $\mathcal{N}[\![P]\!]\rho^*$ is the least fixed point of $H : \mathbf{N} \to \mathbf{N}$ defined by

$$H =_{df} \lambda N.\mathcal{N}[\![Q]\!](\rho^* \oplus \{X \mapsto N\}).$$

Now by the definition of $\mathcal{S}$ and the fact that $\mathcal{M}(\tau.T) = \mathcal{M}(T)$ for any $T \in \mathbf{T}$

$$\begin{aligned}
\mathcal{M}(\mathcal{S}[\![P]\!]\rho) &= \mathcal{M}(\tau.\mathcal{S}[\![Q]\!](\rho \oplus \{X \mapsto \mathcal{S}[\![P]\!]\rho\})) \\
&= \mathcal{M}(\mathcal{S}[\![Q]\!](\rho \oplus \{X \mapsto \mathcal{S}[\![P]\!]\rho\})) \\
&= \mathcal{N}[\![Q]\!](\rho^* \oplus \{X \mapsto \mathcal{M}(\mathcal{S}[\![P]\!]\rho)\}) \\
&= H(\mathcal{M}(\mathcal{S}[\![P]\!]\rho)).
\end{aligned}$$

Hence $\mathcal{N}[\![P]\!]\rho^* \sqsubseteq \mathcal{M}(\mathcal{S}[\![P]\!]\rho)$. For the reverse inequality it suffices by Lemma 14 to show by induction on n that for $n < \omega$, $\mathcal{M}((\mathcal{S}[\![P]\!]\rho)\downarrow n) \sqsubseteq \mathcal{N}[\![P]\!]\rho^*$. For $n = 0$ the inequality is immediate. Assuming the inequality for n and setting $m = n + 1$, then by the induction hypothesis and the monotonicity of $\mathcal{N}[\![Q]\!]$

$$\begin{aligned}
\mathcal{M}((\mathcal{S}[\![P]\!]\rho)\downarrow m) &= \mathcal{M}((\tau.\mathcal{S}[\![Q]\!](\rho \oplus \{X \mapsto \mathcal{S}[\![P]\!]\rho\}))\downarrow m) \\
&= \mathcal{M}(\tau.(\mathcal{S}[\![Q]\!](\rho \oplus \{X \mapsto \mathcal{S}[\![P]\!]\rho\})\downarrow n)) \\
&= \mathcal{M}(\mathcal{S}[\![Q]\!](\rho \oplus \{X \mapsto \mathcal{S}[\![P]\!]\rho\})\downarrow n)) \\
&= \mathcal{M}(\mathcal{S}[\![Q]\!](\rho\downarrow n \oplus \{X \mapsto (\mathcal{S}[\![P]\!]\rho)\downarrow n\})\downarrow n) \\
&\sqsubseteq \mathcal{M}(\mathcal{S}[\![Q]\!](\rho\downarrow n \oplus \{X \mapsto (\mathcal{S}[\![P]\!]\rho)\downarrow n\})) \\
&= \mathcal{N}[\![Q]\!]((\rho\downarrow n)^* \oplus \{X \mapsto \mathcal{M}((\mathcal{S}[\![P]\!]\rho)\downarrow n)\})) \\
&\sqsubseteq \mathcal{N}[\![Q]\!](\rho^* \oplus \{X \mapsto \mathcal{N}[\![P]\!]\rho^*\}) \\
&= H(\mathcal{N}[\![P]\!]\rho^*) \\
&= \mathcal{N}[\![P]\!]\rho^*.
\end{aligned}$$

Hence $\mathcal{M}(\mathcal{S}[\![P]\!]\rho) = \mathcal{N}[\![P]\!]\rho^*$. □(Lemma 18)

We may now establish the congruence of the operational and denotational semantics stated at the beginning of this section.

Theorem 19. Let $P \in \mathbf{E}$ and $\sigma \in Sub$. Then

$$\mathcal{P}[\![P]\!]\sigma = \mathcal{N}[\![P]\!]\hat{\sigma}.$$

Proof: Note that since for $Q \in \mathbf{P}$, $\mathcal{M}(\mathcal{T}[\![Q]\!]) = \mathcal{P}[\![Q]\!]$, $\hat{\sigma} = \overline{\sigma}^*$ and

$$\begin{aligned}\mathcal{P}[\![P]\!]\sigma &= \mathcal{P}[\![\sigma[\![P]\!]]\!] \\ &= \mathcal{M}(\mathcal{T}[\![\sigma[\![P]\!]]\!]) \\ &= \mathcal{M}(\mathcal{S}[\![P]\!]\overline{\sigma}) \\ &= \mathcal{N}[\![P]\!]\overline{\sigma}^{*}.\end{aligned}$$

by Lemmas 16 and 18. □(Theorem 19)

Appendix

In this appendix we give formal definitions of the notions "labelled transition diagram" and "synchronization tree" and establish all the results about them assumed in Section 3.

A *labelled transition diagram* is a nonempty set K of pairs $\langle u, P\rangle$ such that $P \in \mathbf{E}$ and u is a finite sequence of pairs (x, i) with $x \in A^*$ and $i < \omega$ such that for $P, Q \in \mathbf{E}$, $x \in A^+$, $i, j < \omega$ and $u, v \in (A^+ \times \omega)^*$

$$\begin{array}{lrcl}(D1) & \langle u, P\rangle \in K \;\wedge\; v \leq u & \Rightarrow & \exists R.\, \langle v, R\rangle \in K \\ (D2) & \langle u\langle(x,i)\rangle, P\rangle \in K \;\wedge\; j < i & \Rightarrow & \exists R.\, \langle u\langle(x,j)\rangle, R\rangle \in K \\ (D3) & \langle u, P\rangle \in K \;\wedge\; y \in A^+ & \Rightarrow & \{k \mid \langle u\langle(y,k)\rangle, R\rangle \in K\} \text{ is finite} \\ (D4) & \langle u, P\rangle \in K \;\wedge\; \langle u, Q\rangle \in K & \Rightarrow & P = Q.\end{array}$$

Let $\mathbf{D}$ denote the set of all labelled transition diagrams. The transition rules determine for each term P a labelled transition diagram $\mathcal{D}[\![P]\!]$ as follows. For $P \in \mathbf{E}$ let $init(P)$ be the multiset with elements those $x \in A^+$ such that for some Q, $P \xrightarrow{x} Q$, with the multiplicity $mult(P, x)$ of x being the number of ways in which such transitions may be inferred from the transition rules. Note that by Lemma 2, $mult(P, x)$ is finite for $P \in \mathbf{E}$ and $x \in A^+$. Then define $\mathcal{D} : \mathbf{E} \to \mathbf{D}$ by setting

$$\mathcal{D}[\![P]\!] =_{df} \bigcup_{n<\omega} K_n$$

where

$$\begin{aligned}K_0 &=_{df} \{\langle \varepsilon, P\rangle\} \\ K_{n+1} &=_{df} \{\langle u\langle(x,i)\rangle, R_j(Q,x)\rangle \mid x \in A^+,\ i < \omega,\ \exists Q.\, \langle u, Q\rangle \in K_n \;\wedge\; 0 \leq j < mult(Q,x)\}\end{aligned}$$

where for $Q \in \mathbf{E}$ and $x \in A^+$, $\langle R_j(Q,x) \mid 0 \leq j < mult(Q,x)\rangle$ is an enumeration of the multiset whose elements are those R such that $Q \xrightarrow{x} R$, the multiplicity of R being the number of ways in which such a transition may be inferred.

Note that in the construction of K_{n+1} from K_n the choice of the enumerations $\langle R_j(Q,x)\rangle$ determines which one of a family of "equivalent" labelled transition diagrams is associated with the term P. This notion of equivalence will be made explicit later.

Indeed a "synchronization tree" will be defined as an equivalence class of a certain family of trees (called "skeletons") under an appropriate equivalence relation.

A *skeleton* is a nonempty set L of finite sequences of pairs (x,i) with $x \in A^+$ and $i < \omega$ such that for $x \in A^+$, $i,j < \omega$ and $u, v \in (A^+ \times \omega)^*$

$$\begin{array}{lrcl} (S1) & u \in L \wedge v \leq u & \Rightarrow & v \in L \\ (S2) & u\langle(x,i)\rangle \in L \wedge j < i & \Rightarrow & u\langle(x,j)\rangle \in L \\ (S3) & u \in L \wedge y \in A^+ & \Rightarrow & \{k \mid u\langle(y,k)\rangle \in L\} \text{ is finite.} \end{array}$$

Let $\mathbf{S}$ denote the set of all skeletons. There is a simple map $\mathcal{R} : \mathbf{D} \to \mathbf{S}$, informally deleting the terms from the nodes of the labelled transition diagrams, defined by setting

$$\mathcal{R}(K) =_{df} \{u \mid \exists Q.\, \langle u, Q\rangle \in K\}.$$

Let $L \in \mathbf{S}$. For $x \in A^+$ define $\lambda_L(x) =_{df} \{i \mid \langle(x,i)\rangle \in L\}$ and note that by (S2), (S3), $\lambda_L(x) = \{0, 1, \ldots, m-1\}$ for some $m \geq 0$. Let $init(L) =_{df} \{x \mid \exists i.\, \langle(x,i)\rangle \in L\}$ and for $x \in init(L)$ and $i < \lambda_L(x)$ set

$$L \text{ } \mathit{after} \text{ } (x,i) =_{df} \{u \mid \langle(x,i)\rangle u \in L\}.$$

Note that L *after* $(x,i) \in \mathbf{S}$. For $n < \omega$ define

$$L \downarrow n =_{df} \{u \mid u \in L \wedge \mathit{length}(u) < n\} \cup \{u\langle(\tau,0)\rangle^k \mid u \in L \wedge \mathit{length}(u) = n \wedge k < \omega\}.$$

For $x \in A^+$ define $x. : \mathbf{S} \to \mathbf{S}$ by setting

$$x.L =_{df} \{\varepsilon\} \cup \{\langle(x,0)\rangle u \mid u \in L\}.$$

Define $+ : \mathbf{S} \times \mathbf{S} \to \mathbf{S}$ by setting

$$L + L' =_{df} L \cup \{\langle(x, 1 + max\lambda_L(x) + i)\rangle u \mid \langle(x,i)\rangle u \in L'\}.$$

Define

$$\sum_{j<0} =_{df} \{\varepsilon\}$$

and for $n < \omega$

$$\sum_{j<n+1} L_j =_{df} (\sum_{j<n} L_j) + L_n.$$

Define an operation Σ as follows. If I is a set, $\{L_i \mid i \in I\} \subseteq \mathbf{S}$ and $\langle x_i \mid i \in I\rangle$ such that for $i \in I$, $x_i \in A^+$ and for $x \in A^+$, $\{i \in I \mid x_i = x\}$ is finite, then

$$\sum_{i \in I} x_i.L_i =_{df} \bigcup_{x \in A^+} (\sum_{j<n(x)} x_{i_j}.L_{i_j})$$

where for $x \in A^+$, $\langle i_0, \ldots, i_{n(x)}\rangle$ is an enumeration of $\{i \in I \mid x_i = x\}$.

Now define an equivalence relation $\sim$ on $\mathbf{S}$ by setting $\sim =_{df} \bigcap_{n<\omega} \sim_n$ where $\sim_0 =_{df} \mathbf{S} \times \mathbf{S}$ and for $n < \omega$

$$L \sim_{n+1} L' \text{ iff } \forall x \in A^+.\, \lambda_L(x) = \lambda_{L'}(x) \wedge \forall x \in init(L).\, \exists \pi : \lambda_L(x) \leftrightarrow \lambda_{L'}(x).$$
$$\forall i < \lambda_L(x).\, L \text{ after } (x,i) \sim_n L' \text{ after } (x,i).$$

$\sim$ is a suitable equivalence relation on account of the finite branching property of skeletons. Let $[\cdot]$ denote the projection mapping and let $\mathbf{T} =_{df} \{[L] \mid L \in \mathbf{S}\}$. The elements of $\mathbf{T}$ are called *synchronization trees.*

Note that $\sim$ is a congruence relation with respect to the operations $x.\ (x \in A^+)$, $+$, Σ and $\downarrow n\ (n < \omega)$. Hence we may define operations $x.\ (x \in A^+)$, $+$, Σ and $\downarrow n\ (n < \omega)$ on synchronization trees by setting

$$\begin{aligned} x.[L] &=_{df} [x.L] \\ [L] + [L'] &=_{df} [L + L'] \\ \textstyle\sum_{i\in I} x_i.[L_i] &=_{df} [\textstyle\sum_{i\in I} x_i.L_i] \\ [L] \downarrow n &=_{df} [L \downarrow n]. \end{aligned}$$

Each synchronization tree may be represented in the form $\sum_{i\in I} a_i.T_i + \sum_{i\in J} \tau.T'_i$ where each T_i and each T'_i is a synchronization tree, since each skeleton may be expressed in the form $\sum_{i\in I} a_i.L_i + \sum_{i\in J} \tau.L'_i$ where each L_i and each L'_i is a skeleton.

Let $\mathcal{T} =_{df} [\,] \circ \mathcal{R} \circ \mathcal{D}$ so that $\mathcal{T} : \mathbf{E} \to \mathbf{T}$ and

$$\begin{aligned} P \xrightarrow{x} Q &\text{ iff } \mathcal{T}[\![P]\!] \xrightarrow{x} \mathcal{T}[\![Q]\!] \\ P \text{ ref } B &\text{ iff } \mathcal{T}[\![P]\!] \text{ ref } B \\ P\uparrow &\text{ iff } \mathcal{T}[\![P]\!]\uparrow. \end{aligned}$$

Finally it remains to prove the following result.

Lemma 5. $\langle \mathbf{T}, d_\mathbf{T} \rangle$ is a complete metric space.

Proof: That $d_\mathbf{T}$ is a metric is immediate from its definition. Note that if $S, T \in \mathbf{T}$ and $n < \omega$ with $S \downarrow n = T \downarrow n$ then by manipulating enumerations it is easy to show that $\forall L \in S.\, \exists L' \in T.\, L \downarrow n = L' \downarrow n$. Hence if $\langle S_i \mid i < \omega \rangle$ is a Cauchy sequence in $\mathbf{T}$ then there is a sequence $\langle L_i \mid i < \omega \rangle$ which is a Cauchy sequence in $\mathbf{S}$ and such that for $i < \omega$, $[L_i] = S_i$. Then setting $L =_{df} \{u \mid \exists k.\, \forall i \geq k.\, u \in L_i\}$, $L \in \mathbf{S}$ and $\inf\{d_\mathbf{T}\langle S_i, [L]\rangle \mid i < \omega\} = 0$. □(Lemma 5)

References

[BHR] Brookes, S.D., Hoare, C.A.R., and Roscoe, A.W., *A Theory of Communicating Sequential Processes*, JACM, vol. 31, no. 3, 560–599.

[BHR] Brookes, S.D., *A Model for Communicating Sequential Processes*, Oxford University D.Phil. thesis (1983).

[BR] Brookes, S.D., and Roscoe, A.W., *An Improved Failures Model for Communicating Processes, Preliminary version*, September 1984, unpublished.

[BR1] Brookes, S.D., and Roscoe A.W., *An Improved Failures Model for Communicating Processes* , Springer Lecture Notes in Computer Science, vol. 197, 281-305.

[H] Hoare, C.A.R., *Communicating Sequential Processes*, Prentice-Hall 1986.

[H1] Hoare, C.A.R., *A model for communicating sequential processes*, Oxford University Computing Laboratory, Programming Research Group, Technical Report PRG-22.

[HBR] Hoare, C.A.R., Brookes, S.D., and Roscoe, A.W., *A Theory of Communicating Sequential Processes*, Oxford University Computing Laboratory, Programming Research Group, Technical Report PRG-16.

[Hen] Hennessy, M. Acceptance Trees, JACM 31, 4, 896–928

[HN] Hennessy, M. and de Nicola, R. Testing Equivalences for Processes, Theoretical Computer Science 34, 1, 2, (1984) 83-135.

[M] Milner A.J.R.G., *A Calculus of Communicating Systems*, Springer-Verlag, 1980.

[OH] Olderog, E.-R. and Hoare, C.A.R., *Specification-Oriented Semantics for Communicating Processes*, Acta Informatica vol. 23, no. 1, 9-66.

[P] Plotkin, G.D., *A structural approach to operational semantics*, *DAIMI FM*-19, Aahrus University, 1981.

[R] Roscoe, A.W., *A Mathematical Theory of Communicating Processes,* Oxford University D.Phil. thesis, 1982.

[RR] Reed, G.M. and Roscoe, A.W., *Metric Spaces as Models for Real-time Concurrency,* to appear in the proceedings of MFPLS4.