Technical Report

UCAM-CL-TR-59
ISSN 1476-2986

Number 59

UNIVERSITY OF
CAMBRIDGE
Computer Laboratory

On the composition and decomposition of assertions

Glynn Winskel

November 1984

15 JJ Thomson Avenue
Cambridge CB3 0FD
United Kingdom
phone +44 1223 763500

http://www.cl.cam.ac.uk/

Technical reports published by the University of Cambridge
Computer Laboratory are freely available via the Internet:

http://www.cl.cam.ac.uk/techreports/

ISSN 1476-2986

On the Composition and Decomposition of Assertions.

by
Glynn Winskel
University of Cambridge,
Computer Laboratory,
Corn Exchange Street,
Cambridge CB2 3QG.

0. Motivation.

Recently there has been a great deal of interest in the problem of how to compose modal assertions, in order to deduce the truth of an assertion for a composition of processes, in a parallel programming language, from the truth of certain assertions for its components *e.g.* [BKP], [St1,2].

This paper addresses that problem from a theoretical standpoint. I wish to focus on the essential issues and so have not been concerned with whether or not the programming language and assertions are "realistic". The programming language is Robin Milner's Synchronous Calculus of Communicating Systems (called SCCS—see [M3] for an introduction and motivation) and the language of assertions is a fragment of dynamic logic brought to the fore because, despite its simplicity, it is expressive enough to characterise observational equivalence, central to the work of Milner et al—see the papers [HM, M2, St1,2, P]. Colin Stirling has tackled the problem of a proof theory for SCCS and CCS with modal assertions and I have been strongly influenced by his approach in spirit, if not in detail.

It is shown how, with respect to each operation *op* in SCCS, every assertion has a *decomposition* which reduces the problem of proving the assertion holds of a compound process built-up using *op* to proving assertions about its components. These results provide the foundations of a proof system for SCCS with assertions.

While preparing this paper another approach to such proof systems parallel languages occurred to me. The approach uses a mix of the syntax of the programming language with the syntax of assertions. Because this approach fits best with a different notation I shall write it up in another paper [W2]. That will include a full treatment of the relationship of the operational semantics here with a denotational semantics appropriate to observational equivalence.

I have intended the work of these two papers to be a pilot study, to prepare my way towards a clearer understanding of the proof theory of more general languages and assertions. I believe many of the results and connections made will carry through and be useful in a more general setting.

1. The language SCCS.

Assume a set of process variables $x \in \mathrm{Var}$. Assume a set of elementary actions $\alpha \in Act$ forming a *finite* Abelian group $(Act, \bullet, 1, \bar{\ })$ with *composition* $\bullet$, *identity* 1 and *inverse* $\bar{\ }$.

The language of SCCS consists of the following terms

$$p ::= \mathbf{O} \mid x \mid \alpha p \mid p + p \mid p \otimes p \mid p \lceil \mathbb{A} \mid rec x.p \mid rec^n x.p \mid \Omega$$

where $x \in \mathrm{Var}$, $\alpha \in Act$, $\mathbb{A}$ is a subset of Act containing 1 and n is a positive integer.

For convenience we have extended SCCS to include numbered terms of the form $rec^n x.p$ and the completely undefined term Ω. Intuitively the label on such a term bounds the number of calls to the recursive definition. This will be useful later when we come to give proofs involving induction on this number. As a useful convention we shall regard $rec^0 x.p$ as being Ω, and sometimes use $rec^\infty x.p$ to mean $rec x.p$.

We say a recursive definition $rec x.p$ is *well-guarded* when p has the form αq for some term q and action $\alpha \in Act$. However we shall not assume that recursive definitions are well-guarded in general.

Write $\mathbb{P}$ for the set of SCCS terms, and $\mathbb{P}_C$ for the set *closed* of SCCS terms which we shall call *processes*. We call a numbered term a SCCS term in which *all* occurrences of *rec* are labelled by numbers, and write the set of numbered terms as $\mathbb{P}_N$ and the set of closed numbered terms as $\mathbb{P}_{CN}$.

We explain informally the behaviour of the constructs in the language SCCS. The $\mathbf{O}$ term represents the *nil* process which has stopped and refuses to perform any action. The behaviour of Ω will be the same as that of $rec x.x$ which is busily doing nothing of interest. A *guarded* process αp first performs the action α to become the process p. A *sum* $p + q$ behaves like p or q. Which branch of a sum is followed will often be determined by the context and what actions the process is restricted to; only in the case when both component processes p and q are able to perform an identity action 1 can the process $p+q$ always choose autonomously, no matter what the context, to behave like p or q. A *product* process $p \otimes q$ behaves like p and q set in parallel but in such a way that they perform their actions synchronously, in "lock-step", together performing the $\bullet$-product of their respective actions. (To avoid confusion later, we have chosen a notation different from Milner's, using $\otimes$ instead of $\times$.) The *restriction* $p\lceil\mathbb{A}$ behaves like the process p but with its actions restricted to lie in the set $\mathbb{A}$. Restriction is a surprisingly powerful construction; it is what determines what kind of communications are allowed between processes, and without it two processes in parallel would behave in a manner completely independent of eachother. We present the formal definition of behaviour in the next section.

Write $\mathrm{FV}(p)$ for the set of free variables of a term p.

A *substitution* is a map $\sigma : \mathrm{Var} \to \mathbb{P}$ assigning SCCS terms to variables. Given SCCS term p and a substitution σ the term $p[\sigma]$ is the result of substituting $\sigma(x)$ for each free occurrence of x in p—we assume changes are made in the naming of bound variables to avoid the binding of free variables in the substituted terms. We use $[p_0/x_1, \cdots, p_m/x_m, \cdots]$ as an abbreviation for the substitution which replaces free occurrences of the variables x_m by the terms p_m while leaving the other free variables the same.

Let p be a term. A *valuation* is a substitution $\vartheta : \mathrm{Var} \to \mathbb{P}_C$ which assigns a *closed* SCCS term to each variable. So, of course, $p[\vartheta]$ is a closed SCCS term.

2. The behaviour of SCCS.

Following Milner [M1,2,3], the behaviour of a process is represented as a labelled transition system. Its states are processes and so the transition system can be given in a syntax–directed way by defining inductively those transitions which are possible from each process term.

2.1 Definition.

Define the labelled transition relation $\xrightarrow{\alpha}$ between closed SCCS terms to be the least relation closed under the following rules:

$$\alpha p \xrightarrow{\alpha} p$$

$$\frac{p \xrightarrow{\alpha} p'}{p+q \xrightarrow{\alpha} p'} \qquad \frac{q \xrightarrow{\alpha} q'}{p+q \xrightarrow{\alpha} q'}$$

$$\frac{p \xrightarrow{\alpha} p' \quad q \xrightarrow{\beta} q'}{p \otimes q \xrightarrow{\alpha \bullet \beta} p' \otimes q'}$$

$$\frac{p \xrightarrow{\lambda} q}{p \lceil \Lambda \xrightarrow{\lambda} q \lceil \Lambda} \quad \text{if } \lambda \in \Lambda$$

$$\frac{p[recx.p/x] \xrightarrow{\alpha} q}{recx.p \xrightarrow{\alpha} q} \qquad \frac{p[rec^n x.p/x] \xrightarrow{\alpha} q}{rec^{n+1} x.p \xrightarrow{\alpha} q}$$

Notice there are no rules for $\mathbf{0}$ or Ω because we do not wish there to be any transitions from such terms.

Of course this is just an inductive definition of the labelled transition relation

$$\bigcup_{\alpha \in Act} \xrightarrow{\alpha},$$

and later in proofs we shall use induction on the stages of the construction of the full relation. For this reason it is convenient to spell out the details of the inductive construction here.

2.2 Definition. For $m \in \omega$, define the relations $\xrightarrow{\alpha}_m$ between terms $\mathbb{P}_C$ by taking $\xrightarrow{\alpha}_0$ to be the null relation and inductively defining the relations $\xrightarrow{\alpha}_{m+1}$ by

$$
\begin{aligned}
&\alpha p \xrightarrow{\alpha}_{m+1} p \\
&p \xrightarrow{\alpha}_{m} p' \Rightarrow p + q \xrightarrow{\alpha}_{m+1} p' \\
&q \xrightarrow{\alpha}_{m} q' \Rightarrow p + q \xrightarrow{\alpha}_{m+1} q' \\
&p \xrightarrow{\alpha}_{m} p' \ \ \& \ \ q \xrightarrow{\beta}_{m} q' \Rightarrow p \otimes q \xrightarrow{\alpha \bullet \beta}_{m+1} p' \otimes q' \\
&p \xrightarrow{\lambda}_{m} p' \Rightarrow p\lceil A \xrightarrow{\lambda}_{m+1} q\lceil A \quad \text{if } \lambda \in A \\
&p[rec x.p/x] \xrightarrow{\alpha}_{m} q \Rightarrow rec x.p \xrightarrow{\alpha}_{m+1} q \\
&p[rec^n x.p/x] \xrightarrow{\alpha}_{m} q \Rightarrow rec^{n+1} x.p \xrightarrow{\alpha}_{m+1} q.
\end{aligned}
$$

2.3 Proposition. *For each $\alpha \in Act$ and processes p and q, $p \xrightarrow{\alpha} q \Leftrightarrow \exists m.\ p \xrightarrow{\alpha}_m q$ and $p \xrightarrow{\alpha}_m q \Rightarrow p \xrightarrow{\alpha}_{m-1} q$. Thus $\xrightarrow{\alpha} = \bigcup_{m\in\omega} \xrightarrow{\alpha}_m$. The following equivalences hold for SCCS processes:*

(i) $p + q \xrightarrow{\alpha} r \Leftrightarrow p \xrightarrow{\alpha} r$ or $q \xrightarrow{\alpha} r$,

(ii) $p \otimes q \xrightarrow{\alpha} r \Leftrightarrow \exists p', q', \beta, \gamma.\ \beta \bullet \gamma = \alpha \ \ \& \ \ r = p' \otimes q' \ \ \& \ \ p \xrightarrow{\beta} p' \ \ \&$ $q \xrightarrow{\gamma} q'$,

(iii) $p\lceil A \xrightarrow{\alpha} r \Leftrightarrow \exists q.\ r = p'\lceil A \ \ \& \ \ \alpha \in A \ \ \& \ \ p \xrightarrow{\alpha} q$,

(iv) $rec x.p \xrightarrow{\alpha} r \Leftrightarrow p[rec x.p/x] \xrightarrow{\alpha} r$,

(iv) $rec^n x.p \xrightarrow{\alpha} r \Leftrightarrow p[rec^{n-1} x.p/x] \xrightarrow{\alpha} r$.

Proof. Observe that each rule is finitary. Consequently the inductive definition has closure ordinal ω. (Refer to [Ac] for the basic notions of inductive definitions.) For each equivalence (i)–(v) the "$\Leftarrow$" direction follows directly from the rules for $\xrightarrow{\alpha}$. The directions "$\Rightarrow$" follow by induction on m in the relation $\xrightarrow{\alpha}_m$ *e.g.* the induction hypothesis for (i) is

$$\forall p, q, r.\ p + q \xrightarrow{\alpha}_m r \Rightarrow p \xrightarrow{\alpha} r \ \text{ or } \ q \xrightarrow{\alpha} r.$$

∎

A process *diverges* if it can be forever busy performing internal events. In the case of SCCS this can only arise through a process unwinding its recursive definition continually. A diverging process has a somewhat dubious status. In the absence of communication with the environment, it never settles down into a stable state, or settles on the full set of actions it is prepared to do. Viewed behaviourally, from the outside so to speak, it continues to "click and whir" and it never becomes clear whether an action not accepted now will continue to not be accepted later. Mathematically it is the complementary notion of *convergence* which has the more basic definition, by induction.

2.4 Definition. For $n \in \omega$, define the predicates $\downarrow^n$ on $\mathbf{P}_C$ by taking $\downarrow^0 = \emptyset$, the null predicate, and inductively defining

$$\begin{gathered}
\mathbf{O}\downarrow^{n+1}, \quad \alpha p\downarrow^{n+1}, \\
p\downarrow^n \;\&\; q\downarrow^n \Rightarrow (p+q)\downarrow^{n+1}, \\
p\downarrow^n \;\&\; q\downarrow^n \Rightarrow (p\otimes q)\downarrow^{n+1}, \\
p\downarrow^n \Rightarrow (p\lceil A)\downarrow^{n+1}, \\
(p[rec x.p/x])\downarrow^n \Rightarrow (rec x.p)\downarrow^{n+1}, \\
(p[rec^l x.p/x])\downarrow^n \Rightarrow (rec^{l+1} x.p)\downarrow^{n+1} .
\end{gathered}$$

where p and q are closed SCCS terms and l is an non-negative integer.

Define $\downarrow = \bigcup_{n\in\omega} \downarrow^n$. Say a closed SCCS term p is *convergent* iff $p\downarrow$.

Say a closed term p *diverges*, and write $p\uparrow$, when p does not converge.

Intuitively a divergent term is one whose transitions are not completely specified by a finite stage in the recursion. If all recursions were assumed to be well-guarded then all closed terms but Ω would be convergent.

2.5 Lemma. *Let $p \in \mathbf{P}_C$ be convergent, i.e. $p\downarrow$. Then the set $\{q \in \mathbf{P}_C \mid p \xrightarrow{\alpha} q\}$ is finite for all $\alpha \in Act$.*

Proof. We show by induction on n that

$$p\downarrow^n \Rightarrow |\{q \in \mathbf{P}_C \mid p \xrightarrow{\alpha} q\}| < \infty$$

for all $p \in \mathbf{P}_C$ and $\alpha \in Act$.

If $p\downarrow^0$ then p has the form $\mathbf{O}$, which has no transitions, or βq, which has at most one α-transition. This shows the basis of the induction.

Assume inductively that the hypothesis holds for n. We show it holds for $n+1$ by considering cases.

In case p is of form $\mathbf{O}$ or βq it is obvious, as above.

In case p has the form $q+r$, assuming $p\downarrow^{n+1}$ implies $q\downarrow^n$ and $r\downarrow^n$. We have $\{p' \mid p \xrightarrow{\alpha} p'\} = \{p' \mid q \xrightarrow{\alpha} p'\} \cup \{p' \mid r \xrightarrow{\alpha} p'\}$ which is finite by the induction hypothesis.

Similarly, in case p has the form $q \otimes r$, assuming $p\downarrow^{n+1}$ implies $q\downarrow^n$ and $r\downarrow^n$. This time $\{p' \mid p \xrightarrow{\alpha} p'\} = \{q' \otimes r' \mid q \xrightarrow{\beta} q' \;\&\; r \xrightarrow{\gamma} r' \;\&\; \beta \bullet \gamma = \alpha\}$. By induction the sets $\{q' \mid q \xrightarrow{\beta} q'\}$ and $\{r' \mid r \xrightarrow{\gamma} r'\}$ are finite for all $\beta, \gamma \in Act$. Because Act is finite this implies $\{p' \mid p \xrightarrow{\alpha} p'\}$ is finite.

In the case where p has the form $recx.q$ the assumption $p\downarrow^{n+1}$ implies $q[p/x]\downarrow^{n}$. As p and $q[p/x]\downarrow^{n}$ have the same α–transitions, by the induction hypothesis we see that $\{q \mid p \xrightarrow{\alpha} q\}$ is finite, for any $\alpha \in Act$.

Similarly when p has the form $rec^{m}x.q$ and $p\downarrow^{n+1}$ it has a finite set of α–transitions.

By induction we conclude that $p\downarrow$ implies $\{q \mid p \xrightarrow{\alpha} q\}$ is finite, for any $\alpha \in Act$.
∎

Remark. By a fluke, the above result appears to be true in general without needing convergence—though I haven't a proof of this. However in all our proofs we shall only require $\{q \mid p \xrightarrow{\alpha} q\}$ finite when p converges.

3. Approximation and numbered term induction.

The number attached to occurrences of *rec* specifies how many times the recursive definition can be unwound when determining the transition system associated with a term. Roughly, the larger the numbers the larger the transition system associated with the term. There corresponds an approximation relation between terms which we write as $\leq$.

3.1 Definition. Define $\leq$ to be the least binary relation on $\mathbb{P}$ such that

$$\begin{aligned}
&\Omega \leq p, \qquad p \leq p\\
&p \leq q \Rightarrow \alpha p \leq \alpha q\\
&p \leq p' \ \ \& \ \ q \leq q' \Rightarrow p + q \leq p' + q'\\
&p \leq p' \ \ \& \ \ q \leq q' \Rightarrow p \otimes q \leq p' \otimes q'\\
&p \leq q \Rightarrow p\lceil \mathbb{A} \leq q\lceil \mathbb{A}\\
&p \leq q \ \ \& \ \ m \leq n \Rightarrow rec^m x.p \ \leq \ rec^n x.q\\
&p \leq q \Rightarrow rec^n x.p \ \leq \ rec x.q.
\end{aligned}$$

3.2 Lemma. *The relation $\leq$ is a partial order on $\mathbb{P}$ such that*

$$|\{q \in \mathbb{P} \mid q \leq p\}| \leq \infty$$

for all $p \in \mathbb{P}_N$. It has as least element Ω, and satisfies the property that any subset X of $\mathbb{P}$ which is bounded above by an element of $\mathbb{P}$ has a least upper bound $\bigsqcup X$ in $\mathbb{P}$. A bounded finite set of (closed) numbered terms has as least upper bound a (closed) numbered term.

Proof. By definition $\leq$ is reflexive. Transitivity and antisymetry of $\leq$ follow by structural induction case by case. This shows $\leq$ is a partial order.

The set $\{q \in \mathbb{P} \mid q \leq p\}$ is finite for $p \in \mathbb{P}_N$ by structural induction.

By definition Ω is the least element.

Let $X \subseteq^{fin} \mathbb{P}$ and $p \in \mathbb{P}$. Let $X \leq p$ abbreviate $\forall q \in X.\ q \leq p$. It can be shown by structural induction on $p \in \mathbb{P}$ that: for all $X \subseteq^{fin} \mathbb{P}$ if $X \leq p$ then X has a least upper bound, and that in the case where X is restricted to being a finite subset of (closed) numbered terms then its lub is a (closed) numbered term too. ∎

The order $\leq$ on terms $\mathbb{P}$ respects the language of SCCS, as expressed in the following lemma.

3.3 Lemma. *Let σ and σ' be substitutions in the relation $\sigma \leq \sigma' \Leftrightarrow_{def} \forall x \in \mathrm{Var}.\ \sigma[\![x]\!] \leq \sigma'[\![x]\!]$. Let p, q be terms in the relation $p \leq q$. Then*

$$p[\sigma] \leq q[\sigma'].$$

Proof. By structural induction on q. ▮

Many proofs which can be tackled using structural induction together with induction on the numbering on terms can be handled more conveniently by combining the subterm relation with the approximation relation $\leq$. This produces a new well-founded ordering $\preceq$ on which to do the induction "all in one go".

3.4 Definition.
Let p and q be numbered terms, in $\mathbb{P}_N$. Define

$$p \preceq q \Leftrightarrow p \leq q' \text{ for some subterm } q' \text{ of } q.$$

Define $p \prec q \Leftrightarrow p \preceq q \;\;\&\;\; p \not= q$.

3.5 Lemma. *The relation $\preceq$ is a partial order on $\mathbb{P}_N$ such that*

$$|\{q \in \mathbb{P}_N \mid q \preceq p\}| \leq \infty$$

for all $p \in \mathbb{P}_N$.

Proof. Obviously $\preceq$ is reflexive and transitive. It is antisymmetric because if $p \preceq q$ and $q \preceq p$ then p and q are subterms of eachother and so identical. It inherits the finiteness condition from $\leq$ and the subterm relation. ▮

Consequently we can do well-founded induction on $\preceq$:

3.6 Proposition. *(Numbered term induction)*
Let Q be a predicate on $\mathbb{P}$. Then $\forall p \in \mathbb{P}.\ Q(p)$ iff

$$\forall p \in \mathbb{P}((\forall q \prec p.\ Q(q)) \Rightarrow Q(p)).$$

Most of our proofs using numbered term induction will follow a similar pattern. We would like to prove that a predicate R holds for all closed numbered terms $\mathbb{P}_{CN}$, but in order to do so we extend the predicate R to a predicate R_o on all open numbered terms in the following way:

$$R_o(p) \Leftrightarrow_{def} \forall \text{ valuations } \vartheta.\ (\forall x \in \mathrm{FV}(p).\ R(\vartheta[\![x]\!])) \Rightarrow R(p[\vartheta])$$

for open numbered terms p. If it can be shown that $R_o(p)$ holds for all numbered terms, then in particular, by taking ϑ to be any valuation, we have that $R(p)$ holds for all closed terms p.

As an example we show that the the labelled transition relation $\xrightarrow{\alpha}$ is Noetherian on closed numbered terms, *i.e.* there are no infinite chains

$$p_0 \xrightarrow{\alpha_0} p_1 \xrightarrow{\alpha_1} \cdots \xrightarrow{\alpha_{n-1}} p_n \xrightarrow{\alpha_n} \cdots$$

with $p_0, p_1, \ldots, p_n, \ldots$ in $\mathbb{P}_{CN}$.

3.7 Theorem. *The relation $\xrightarrow{\alpha}$ is Noetherian on $\mathbb{P}_{CN}$.*

Proof.

Let N be the predicate on closed numbered terms given by

$N(p)$ iff there are no infinite chains $p_0 \xrightarrow{\alpha_0} p_1 \xrightarrow{\alpha_1} \cdots \xrightarrow{\alpha_{n-1}} p_n \xrightarrow{\alpha_n} \cdots$

with $p = p_0, p_1, \ldots, p_n, \ldots$ in $\mathbb{P}_{CN}$. Extend N to all numbered terms by defining

$$N_0(q) \Leftrightarrow \forall \text{ valuations } \vartheta(\forall x \in \mathrm{FV}(p).\ N(\vartheta[\![x]\!])) \Rightarrow N(q[\vartheta]).$$

We prove $N_0(q)$ holds for all numbered terms q by numbered term induction on q.

Let $q \in \mathbb{P}_N$ for which $N_0(p)$ for all $p \prec q$. We show $N(q)$.

Let ϑ be a valuation such that $\forall x \in \mathrm{FV}(q).\ N(\vartheta[\![x]\!])$.

Clearly $N(\vartheta[\![x]\!])$ for x a variable, and $N(\mathbb{O}[\vartheta])$ and $N(\Omega[\vartheta])$ as $\mathbb{O}$ and Ω make no transitions.

If $q[\vartheta] = \alpha p[\vartheta]$ could make an infinite chain of transitions then so could $p[\vartheta] \prec q[\vartheta]$ which is false by assumption. Thus $N(q[\vartheta])$.

Similarly if $q = p + r$ or $q = p \otimes r$, as $N(p[\vartheta])$ and $N(r[\vartheta])$, then $N(q[\vartheta])$.

Assume $q = rec^n x.p$. We have

$$q[\vartheta] \xrightarrow{\alpha} r \Leftrightarrow (p[rec^{n-1}x.p/x])[\vartheta] \xrightarrow{\alpha} r.$$

Note $p[rec^{n-1}x.p/x][\vartheta] = p[\vartheta']$ where ϑ' is the valuation

$$\vartheta'[\![y]\!] = \begin{cases} \vartheta[\![y]\!] & \text{if } y \neq x, \\ rec^{n-1}x.p & \text{if } y = x. \end{cases}$$

(*i.e.* $\vartheta' = \vartheta[rec^{n-1}x.p/x]$ using an obvious notation.) As $rec^{n-1}x.p \prec q$ we obtain $N(\vartheta'[\![x]\!])$ for all $x \in \mathrm{FV}(p)$. As $p \prec q$ we know $N_0(p)$. Consequently $N(p[\vartheta'])$, so $N(q[\vartheta])$.

Thus we see $N(q[\vartheta])$ for all valuations ϑ for which $\forall x \in \mathrm{FV}(q).\ N(\vartheta[\![x]\!])$.

Thus the truth of $N_0(q)$ follows from the truth of $N_0(p)$ for all $p \prec q$. By numbered-term induction we establish $N_0(q)$ for all numbered terms, and in particular that each closed numbered term is Noetherian. ∎

3.8 Lemma. *The set $\{q \mid p \xrightarrow{\alpha} q\}$ is finite for all $\alpha \in Act$, $p \in \mathbb{P}_{CN}$.*

Proof. As above. ∎

4. The assertion language.

Hennessy and Milner defined an equivalence relation between processes called *observational equivalence* in [HM, M1]. For our language of SCCS, two processes are observationally equivalent iff whenever one can do an action to become a process then so can the other do the same action to become an equivalent process. They found an alternative characterisation so that processes were observationally equivalent iff they satisfied the same assertions in a simple language of modal assertions [HM]. However there are inadequacies with this treatment of processes because it does not take proper account of divergence. So Milner, in [M2], generalised the definition of observational equivalence and the definition of a process satisfying a modal assertion in order to cope with divergence. (See [HP] for a closely related but different extension of observational equivalence to diverging processes.) In this way Milner extended the result he had obtained with Hennessy, so that in SCCS, for example, two processes are observationally equivalent iff they satisfy the same assertions in the modal language of Hennessy and Milner. In future, "observational equivalence" shall refer to the more refined equivalence of [M2]. Following [P, St1,2] we have simplified the modal language of Hennessy and Milner a little.

4.1 Definition.

The *assertion language* consists of simple modal expressions built up according to:

$$A ::= \mathit{true} \mid \mathit{false} \mid \bigwedge_{i\in I} A_i \mid \bigvee_{i\in I} A_i \mid \langle\alpha\rangle A \mid [\alpha]A$$

where I is a finite indexing set and $\alpha \in \mathit{Act}$.

We shall call elements of this language *assertions*, and write the set of assertions as **Assn**.

By convention we understand $\bigwedge_{i\in I} A_i$ to be *true* and $\bigvee_{i\in I} A_i$ to be *false* when the indexing set I is null. When the indexing set is $I = \{0,1\}$ we can write $\bigwedge_{i\in I} A_i$ as $A_0 \wedge A_1$, and $\bigvee_{i\in I} A_i$ as $A_0 \vee A_1$.

The meaning of an assertions is given by specifying the subset $\Pi[\![A]\!]$ of SCCS processes $\mathbf{P}_C$ which satisfy A:

4.2 Definition. Define

$$\begin{aligned}
\Pi[\![\mathit{true}]\!] &= \mathbf{P}_C\\
\Pi[\![\mathit{false}]\!] &= \emptyset\\
\Pi[\![\bigwedge_{i\in I} A_i]\!] &= \bigcap_{i\in I} \Pi[\![A_i]\!]\\
\Pi[\![\bigvee_{i\in I} A_i]\!] &= \bigcup_{i\in I} \Pi[\![A_i]\!]\\
\Pi[\![\langle\alpha\rangle A]\!] &= \{p \in \mathbf{P}_C \mid \exists q. p \xrightarrow{\alpha} q \;\&\; q \in \Pi[\![A]\!]\}\\
\Pi[\![[\alpha]A]\!] &= \{p \in \mathbf{P}_C \mid p\downarrow \;\&\; \forall q. p \xrightarrow{\alpha} q \Rightarrow q \in \Pi[\![A]\!]\}
\end{aligned}$$

Write $\models p : A \Leftrightarrow_{def} p \in \Pi[\![A]\!]$, where p is a SCCS process and A is an assertion, and say p *satisfies* A.

We call an element $p : A$ a *correctness assertion*, for p an SCCS term and A an assertion.

So $\models p : A$ means the correctness assertion $p : A$ is true. Clearly $\models p : \langle\alpha\rangle A$ means the process p can do an α–action to become a process satisfying A, and $\models p : [\alpha]false$ means the process p refuses to do an α–action. The latter kind of properties are important for detecting deadlock. Notice that $\not\models \Omega : [\alpha]true$ and $\not\models \Omega : [\alpha]false$ because we insist diverging processes, like Ω, cannot satisfy any assertion of the form $[\alpha]A$.

4.3 Proposition. *Let $p \in \mathbf{P}_C$. Then $p\downarrow \Leftrightarrow \models p : [\alpha]true$, for any action α.*

Proof. Directly from the definition of satisfaction for formulae of the form $[\alpha]true$. ▮

Because the processes $recx.p$ and $p[recx.p/x]$ make the same transitions they satisfy the same assertions, a fact we shall need later.

4.4 Lemma. *Let $p \in \mathbf{P}$ with at most one free variable x. Let $A \in \mathbf{Assn}$. Then*

$$\models recx.p : A \Leftrightarrow \models p[recx.p/x] : A \quad \text{and}$$
$$\models rec^m x.p : A \Leftrightarrow \models p[rec^{m-1} x.p/x] : A.$$

Proof. By structural induction on A using proposition 2.3. ▮

Because we insist that a process satisfying a modal assertion $[\alpha]A$ must converge, satisfaction will be effective; if a process p in $\mathbf{P}_C$ satisfies an assertion A then it can be approximated by a numbered version p' which also satisfies the assertion. To show this we must first see how the transition system associated with a term $p' \leq p$ approximates, and simulates, the transition system associated with p.

4.5 Lemma. *For SCCS processes*

(i) For $p, p', q' \in \mathbf{P}_C$

$$p' \xrightarrow{\alpha} q' \;\;\&\;\; p' \leq p \Rightarrow \exists q.\, q' \leq q \;\;\&\;\; p \xrightarrow{\alpha} q.$$

(ii) For $p, q \in \mathbf{P}_C, q_0 \in \mathbf{P}_{CN}$

$$p \xrightarrow{\alpha} q \;\;\&\;\; q_0 \leq q \Rightarrow \exists p', q' \in \mathbf{P}_{CN}.\, p' \leq p \;\;\&\;\; p' \xrightarrow{\alpha} q' \;\;\&\;\; q_0 \leq q'.$$

(iii) For $p, p' \in \mathbf{P}_C$

$$p'\downarrow \;\&\;\; p' \leq p \Rightarrow p\downarrow \;\&\;\; (\forall q.\, p \xrightarrow{\alpha} q \Rightarrow \exists q' \leq q.\, p' \xrightarrow{\alpha} q').$$

(iv) For $p \in \mathbf{P}_C, Y \subseteq \mathbf{P}_{CN}$

$$\begin{aligned} &p\downarrow \;\&\;\; (\forall q.\, p \xrightarrow{\alpha} q \Rightarrow \exists q_0 \in Y.\, q_0 \leq q) \\ \Rightarrow\ &\exists p' \in \mathbf{P}_{CN}.\, p' \leq p \;\;\& \\ &p'\downarrow \;\&\;\; (\forall q.\, p' \xrightarrow{\alpha} q \Rightarrow \exists q_0 \in Y.\, q_0 \leq q). \end{aligned}$$

Proof.

The proofs follow by induction on n in $\xrightarrow{\alpha}_n$ and $\downarrow^n$.

(i) We take as induction hypothesis: For all $p, p', q' \in \mathbb{P}_C$

$$p' \xrightarrow{\alpha}_m q' \;\;\&\;\; p' \le p \Rightarrow \exists q.\; q' \le q \;\;\&\;\; p \xrightarrow{\alpha} q,$$

which we prove by induction on m.

It is vacuously true when $m = 0$.

Assume $m > 0$. Assume the induction hypothesis for $m - 1$. We show by considering the possible forms of p' that the induction hypothesis holds for m.

For $p = \mathbb{O}$ and $p = \Omega$ it is obvious.

In the case where $p' = r' \otimes s'$, if $p' \xrightarrow{\alpha}_m q' \;\&\; p' \le p$ then $p = r \otimes s$ for some r and s with $r' \xrightarrow{\beta}_{m-1} r$ and $s \xrightarrow{\gamma}_{m-1}$ for some β, γ such that $\beta \bullet \gamma = \alpha$. Then by the induction hypothesis there are t and u such that $t' \le t \;\&\; r \xrightarrow{\beta} t$ and $s' \le u \;\&\; s \xrightarrow{\gamma} u$. Taking $q = t \otimes u$ gives $q' \le q \;\&\; p \xrightarrow{\alpha} q$ as required.

Consider the case $p = recx.r$. If $p' \xrightarrow{\alpha}_m q' \;\&\; p' \le p$ then $r'[p'/x] \xrightarrow{\alpha}_{m-1} q'$ and $p = recx.r$ for some $r \ge r'$. Now $r'[p'/x] \le r[p/x]$ so by the induction hypothesis $r[p/x] \xrightarrow{\alpha} q$ for some $q \ge q'$. But then $q' \le q$ and $p \xrightarrow{\alpha} q$ as required.

We leave the other cases to the reader. They are routine.

(ii) Take as induction hypothesis: For all $p, q \in \mathbb{P}_C, q_0 \in \mathbb{P}_{CN}$

$$p \xrightarrow{\alpha}_m q \;\;\&\;\; q_0 \le q \Rightarrow \exists p', q' \in \mathbb{P}_{CN}.\; p' \le p \;\;\&\;\; p' \xrightarrow{\alpha} q' \;\;\&\;\; q_0 \le q',$$

and proceed by induction on m. The induction is similar to the previous case and is omitted.

(iii) Take as induction hypothesis: For all $p, p' \in \mathbb{P}_C$

$$p' \downarrow^m \;\;\&\;\; p' \le p \Rightarrow p\downarrow \;\;\&\;\; (\forall q.\; p \xrightarrow{\alpha}_m q \Rightarrow \exists q' \le q.\; p' \xrightarrow{\alpha} q').$$

It is vacuously true when $m = 0$. For the inductive step when $m > 0$ there is one case of interest, that where p' has the form $recx.r'$.

Then, assuming $p' \downarrow^m \;\&\; p' \le p$ we obtain:

$r'[p'/x] \downarrow^{m-1}$ and $p = rec^j x.r$ for some $j \in \omega \cup \{\infty\}$ and $r \ge r'$.

By lemma 3.3, $r'[p'/x] \leq r[p/x]$. Thus by the induction hypothesis we see $r[p/x]\downarrow$.

Now assume $p \xrightarrow{\alpha}_m q$. Then $r[p/x] \xrightarrow{\alpha}_{m-1} q$. By the induction hypothesis we obtain some $q' \leq q$ such that $r'[p'/x] \xrightarrow{\alpha} q'$. Hence $p' \xrightarrow{\alpha} q'$, as required.

(iv) Take as induction hypothesis

$$\begin{aligned} & p\downarrow^m \ \& \ (\forall q.\ p \xrightarrow{\alpha}_m q \Rightarrow \exists q_0 \in Y.\ q_0 \leq q) \\ & \Rightarrow \exists p' \in \mathbf{P}_{CN}.\ p' \leq p \ \ \& \\ & p'\downarrow \ \& \ (\forall q.\ p' \xrightarrow{\alpha} q \Rightarrow \exists q_0 \in Y.\ q_0 \leq q). \end{aligned}$$

for all processes p and subsets of numbered terms Y.

Again the basis of the induction when $m = 0$ is vacuously true. We only show one case in the inductive step, the most difficult case where $p = r \otimes s$.

Assume $m > 0$. Assume the inductive hypothesis holds for lesser values than m. Assume $p = r \otimes s$ and that

$$p\downarrow^m \ \& \ \forall q.\ p \xrightarrow{\alpha}_m q \Rightarrow (\exists q_0 \in Y.\ q_0 \leq q) \tag{1}$$

for $Y \subseteq \mathbf{P}_{CN}$. Without loss of generality we can assume Y is upwards–closed with respect to $\leq$ *i.e.*

$$\forall p \in Y \forall q \in \mathbf{P}_{CN}.\ p \in Y \ \ \& \ \ p \leq q \Rightarrow q \in Y,$$

because clearly if the inductive hypothesis holds for all upwards–closed subsets of $\mathbf{P}_{CN}$ then it holds for arbitrary subsets of $\mathbf{P}_{CN}$.

By (1) we see $r\downarrow^{m-1}$ and $s\downarrow^{m-1}$.

Let $\beta, \gamma \in Act$ be such that $\beta \bullet \gamma = \alpha$.

If $r \xrightarrow{\beta}_{m-1} t$ and $s \xrightarrow{\gamma}_{m-1} u$ then $p = r \otimes s \xrightarrow{\alpha}_m t \otimes u$. Hence by (1)

$$g_{t,u} \otimes d_{t,u} \in Y \ \ \& \ \ g_{t,u} \leq t \ \ \& \ \ d_{t,u} \leq u$$

for some choice $g_{t,u}, d_{t,u} \in \mathbf{P}_{CN}$.

Now define

$$\begin{aligned} k_t &= \bigsqcup\{g_{t,u} \mid s \xrightarrow{\gamma}_{m-1} u\} \\ h_u &= \bigsqcup\{d_{t,u} \mid r \xrightarrow{\beta}_{m-1} t\} \end{aligned}$$

the lubs of sets in $\mathbf{P}_{CN}$ wrt $\leq$; these exist by lemma 3.2 as the sets are finite—because $s\downarrow$ and $r\downarrow$—and bounded above by t and u respectively.

Define

$$W_\beta = \{k_t \mid r \xrightarrow{\beta}_{m-1} t\}$$
$$Z_\gamma = \{h_u \mid s \xrightarrow{\gamma}_{m-1} u\}.$$

We show

$$\forall t_0 \in W_\beta, u_0 \in Z_\gamma.\ (t_0 \otimes u_0) \in Y. \tag{2}$$

Let $t_0 \in W_\beta, u_0 \in Z_\gamma$. Then $t_0 = k_t$ and $u_0 = h_u$ for some t, u with $r \xrightarrow{\beta}_{m-1} t$ and $s \xrightarrow{\gamma}_{m-1} u$. Because

$$k_t \geq g_{t,u} \ \&\ h_u \geq d_{t,u}$$

we have $t_0 \otimes u_0 = k_t \otimes h_u \geq g_{t,u} \otimes d_{t,u}$. So by the upwards–closedness of Y we obtain $t_0 \otimes u_0 \in Y$.

Now $r{\downarrow}^{m-1}$ and

$$\forall t.\ r \xrightarrow{\beta}_{m-1} t \Rightarrow \exists t_0 \in W_\beta.\ t_0 \leq t.$$

Thus by the induction hypothesis we obtain some $r_\beta \in \mathbb{P}_{CN}$ such that $r_\beta \leq r$ and

$$r_\beta{\downarrow} \ \&\ \ \forall t.\ r_\beta \xrightarrow{\beta} t \Rightarrow \exists t_0 \in W_\beta.\ t_0 \leq t. \qquad (3),$$

and similarly some $s_\gamma \in \mathbb{P}_{CN}$ such that $s_\gamma \leq r$ and

$$s_\gamma{\downarrow} \ \&\ \ \forall u.\ s_\gamma \xrightarrow{\gamma} u \Rightarrow \exists u_0 \in Z_\gamma.\ u_0 \leq u. \qquad (4).$$

We can now define $p' = \bigsqcup\{r_\beta \otimes s_\gamma \mid \beta \bullet \gamma = \alpha\}$ the lub of a set in $\mathbb{P}_{CN}$; it exists as the set is finite—because the number of actions is finite—and is bounded above by p. Clearly $p' \in \mathbb{P}_{CN}$ and $p' \leq p$. As $r_\beta \otimes s_\gamma{\downarrow}$ whenever $\beta \bullet \gamma = \alpha$ and $p' \geq r_\beta \otimes s_\gamma$ we see by part (iii) above that $p'{\downarrow}$ too.

We require further that $\forall q'.\ p' \xrightarrow{\alpha} q' \Rightarrow \exists q_0 \in Y.\ q_0 \leq q'$. Suppose $p' \xrightarrow{\alpha} q'$. Then observing p' and q' have the form $p' = r' \otimes s'$ and $q' = t' \otimes u'$ we know $r' \xrightarrow{\beta} t'$ and $s' \xrightarrow{\gamma} u'$ for some β, γ with $\beta \bullet \gamma = \alpha$. By part (ii) above $r_\beta \xrightarrow{\beta} t$ for some $t \leq t'$. But then by the property of r_β (3), there is some $t_0 \in W_\beta$ with $t_0 \leq t$. Thus $t_0 \leq t'$ and $t_0 \in W_\beta$. Similarly, there is some $u_0 \leq u'$ with $u_0 \in Z_\gamma$. Take $q_0 = t_0 \otimes u_0$. Then $q_0 = t_0 \otimes u_0 \leq t' \otimes u' = q'$ and $q_0 = t_0 \otimes u_0 \in Y$ by (2).

This completes this case in the inductive step. The remaining cases are straightforward and left to the reader ∎

Note that part (iv) above specialises to the result

$$p{\downarrow} \Rightarrow \exists p' \in \mathbb{P}_{CN}.\ p' \leq p \ \&\ \ p'{\downarrow}$$

when we take $Y = \{\Omega\}$.

4.6 Theorem. *Let $p \in \mathbf{P}_C$. Then*

$$\models p:A \Leftrightarrow \exists p' \in \mathbf{P}_{CN}.\, p' \leq p \;\; \& \models p':A.$$

Proof. The proof is by structural induction on A using the above lemma parts (i), (ii) for the modality $\langle\alpha\rangle$ and (iii), (iv) for the modality $[\alpha]$.

Take as induction hypothesis:

$$\forall p \in \mathbf{P}_C.\; \models p:A \Leftrightarrow \exists p' \in \mathbf{P}_{CN}.\, p' \leq p \;\; \& \models p':A.$$

For the induction suppose the inductive hypothesis holds for all proper subassertions of A. One considers all the possible forms of A and shows in all cases that the induction hypothesis holds for A. We do only two cases leaving the remainder to the reader.

Assume $A = \langle\alpha\rangle B$.

If $p' \leq p$ and $\models p':\langle\alpha\rangle B$ for $p' \in \mathbf{P}_{CN}$ then $p' \xrightarrow{\alpha} q'$ for some q' s.t. $\models q':B$. Thus by lemma 4.5 (i) there is some $q' \leq q$ with $p \xrightarrow{\alpha} q$. But then by the induction hypothesis $\models q:B$ which implies $\models p:\langle\alpha\rangle B$, as required.

If $\models p:\langle\alpha\rangle B$ then $p \xrightarrow{\alpha} q$ for some q s.t. $\models q:B$. By the inductive hypothesis we obtain some $q_0 \in \mathbf{P}_{CN}$ with $q_0 \leq q$ and $\models q_0:B$. By lemma 4.5(ii) there is some $p' \in \mathbf{P}_{CN}$ s.t. $p' \leq p$ and $p' \xrightarrow{\alpha} q'$ with $q_0 \leq q'$. Then $\models q':B$, again by the induction hypothesis. Consequently $\models p':\langle\alpha\rangle B$, as required.

Thus in the case where $A = \langle\alpha\rangle B$ the induction hypothesis holds.

Assume $A = [\alpha]B$.

Suppose $p' \leq p$ and $\models p':[\alpha]B$ for some $p' \in \mathbf{P}_{CN}$. Then $p'\!\downarrow$ and $\forall q'.\, p' \xrightarrow{\alpha} q' \Rightarrow\, \models q':B$. Consequently by lemma 4.5 (iii), $p\!\downarrow$ and if $p \xrightarrow{\alpha} q$ then $p' \xrightarrow{\alpha} q'$ for some $q' \leq q$. By the induction hypothesis $\models q:B$. Thus $\models p:[\alpha]B$.

Suppose $\models p:[\alpha]B$. Then $p\!\downarrow$ and $\forall q.\, p \xrightarrow{\alpha} q \Rightarrow\, \models q:B$. Let

$$Y = \{q_0 \in \mathbf{P}_{CN} \mid \exists q.\, p \xrightarrow{\alpha} q \;\; \& \;\; q_0 \leq q \;\; \& \models q_0:B\}.$$

By the induction hypothesis if $p \xrightarrow{\alpha} q$ there is some $q_0 \in Y$ s.t. $q_0 \leq q$. Applying lemma 4.5 (iv), we obtain some $p' \in \mathbf{P}_{CN}$ for which

$$p' \leq p \;\; \& \;\; p'\!\downarrow \; \& \;\; (\forall q.\, p' \xrightarrow{\alpha} q \Rightarrow \exists q_0 \in Y.\, q_0 \leq q).$$

Thus if $p' \xrightarrow{\alpha} q$ then by the induction hypothesis we see $\models q:B$. Therefore $\models p:[\alpha]B$.

Thus in the case where $A = [\alpha]B$ the induction hypothesis holds. ▮

A topology on processes: There is a natural topology on $\mathbb{P}_C$ which is the Scott-topology, seen in a slightly different setting than usual.

4.7 Proposition. *The family of sets of the form $\{p \in \mathbb{P}_C \mid q \leq p\}$ for q a closed numbered term are the basis of a topology on $\mathbb{P}_C$. So the open sets have the form*

$$U = \{p \in \mathbb{P}_C \mid \exists p_0 \in X.\ p_0 \leq p\}$$

for a subset X of numbered terms.

The open sets of $\mathbb{P}_C$ are those subsets $U \subseteq \mathbb{P}_C$ which are

(i) $\forall p, q.\ p \geq q \in U \Rightarrow p \in U$,

(ii) $\forall$ *directed* $S \subseteq \mathbb{P}_C.\ \bigsqcup S \in U \Rightarrow \exists p \in S.\ p \in U$.

Proof. Routine. Use lemma 3.2 to check this is a basis of a topology. Recall a directed set is a non-null subset S with the property that $p \in S\ \&\ q \in S \Rightarrow \exists r \in S.\ p \leq r\ \&\ q \leq r$. ▮

Then theorem 4.6 says each assertion determines an open set of $\mathbb{P}_C$ *i.e.* $\Pi[\![A]\!]$ is open for each assertion A. In fact 4.6 can be made more general, and more useful if we were to extend our present language of assertions.

4.8 Lemma. *Let $\alpha \in Act$. If U is an open set in the topology on processes then so are the sets*

$$\langle\alpha\rangle U =_{def} \{p \in \mathbb{P}_C \mid \exists q \in U.\ q \xrightarrow{\alpha} p\} \quad \text{and}$$
$$[\alpha]U =_{def} \{p \in \mathbb{P}_C \mid p{\downarrow}\ \&\ \forall q.\ p \xrightarrow{\alpha} q \Rightarrow q \in U\}.$$

Proof. The proof uses lemma 4.5 in the same way as the proof of theorem.4.6. ▮

This topological view is in line with Dana Scott's development of the theory of domains from neighbourhood systems [S1] and with the ideas of Mike Smyth in [Sm], where he proposes that computational properties of a topological space be identified with effective open sets. In the approach to domains using neighbourhood systems, to know more information about a process is to know a smaller neighbourhood in which it is contained. These topological ideas have been applied by Gordon Plotkin in [P] to extend the language of assertions by intuitionistic negation and implication; their interpretation are those standard for topological models of intuitionistic logic, so in this extension of **Assn** one takes $\Pi[\![A \supset B]\!] = ((\mathbb{P}_C \setminus \Pi[\![A]\!]) \cup \Pi[\![B]\!])^o$ where X^o is the topological interior of the set X (Plotkin's topology is not that here however). One advantage of intuitionistic logic over classical logic is that satisfaction is still effective even for this extended set of assertions. We shall say more on denotational semantics in [W2].

A word on equivalences on programs: The work of Milner et al (see *e.g.* [M1]) shows how much can be done with the observational and bisimulation equivalence those equivalences induced by the assertions; recall we can take two processes to be equivalent iff they satisfy the same assertions. This argues that the assertions are sufficiently rich to capture a great many of the properties of interest. This should not seem so surprising. Remember a process denotes the set of assertions it satisfies so is essentially modelled as an (infinite) conjunction of these assertions; only for a finite process would a single assertion in **Assn** capture its full behaviour.

Although the assertions may make it possible to distinguish all the processes one could wish, this is not to say the logic is as expressive as one would like from all points of view. Clearly it is rather primitive. For example one would like the ability to specify infinite behaviours by finite assertions.

Quite possibly there are other properties of interest to which the language of assertions is blind. However it is interesting that two other well–known notions of equivalence can be induced by taking fragments of the assertion language **Assn**. They are *trace equivalence* and *failure–set equivalence*. Strictly speaking the failure–set equivalence has not been defined on SCCS but the definition that follows has been based on the work of [HBR] modified to take proper account of divergence. The use of traces and their associated equivalence is widespread, see *e.g.* [H] and [HdeN]. As far as these two equivalences are concerned **Assn** is certainly expressive enough. The assertions which suffice to induce the *trace–equivalence* take the form

$$\langle\alpha_0\rangle\langle\alpha_1\rangle\cdots\langle\alpha_{j-1}\rangle \mathit{true},$$

while the assertions for *failure–set–equivalence* take the form

$$\langle\alpha_0\rangle\langle\alpha_1\rangle\cdots\langle\alpha_{j-1}\rangle\big(\bigwedge_{\beta\in I}[\beta]\mathit{false}\big).$$

5. The decomposition of assertions.

We are interested in how the goal of proving an assertion holds of a process reduces to the subgoals of proving assertions about its subprocesses, and in the converse problem, of how assertions about subprocesses combine to yield assertions about the compound process. It is clear for example that an assertion $\langle\alpha\rangle A$ holds of a process αp iff A holds of p. Similarly $[\alpha]A$ holds of a process $p + q$ iff $[\alpha]A$ holds of both components p and q. However $\models p + q : \langle\alpha\rangle A$ iff $\models p : \langle\alpha\rangle A$ or $\models q : \langle\alpha\rangle A$; there is not a unique subgoal. Similarly ther are many possible ways in which $\models p \otimes q : \langle\alpha\rangle \mathit{true}$; this holds whenever $\models p : \langle\beta\rangle \mathit{true}$ and $\models q : \langle\gamma\rangle \mathit{true}$ with $\beta \bullet \gamma = \alpha$.

For each unary operation op of SCCS we show how for an assertion A there is an assertion $\mathcal{D}_{op}[\![A]\!]$ so that

$$\models op(p) : A \Leftrightarrow \models p : \mathcal{D}_{op}[\![A]\!].$$

For each binary operation op of SCCS we show how for an assertion A there is a finite set of pairs of assertions $\mathcal{D}_{op}[\![A]\!]$ so that

$$\models p \otimes q : A \quad \text{iff} \quad \exists (B, C) \in \mathcal{D}_{op}[\![A]\!].\ \models p : B \ \ \& \models q : C.$$

Thus we see how, with respect to each operation op in SCCS, every assertion has a *decomposition* which reduces the problem of proving the assertion holds of a compound process built-up using op to proving assertions about its components. These results provide the foundations of our proof systems for SCCS with assertions **Assn**, both here and in [W2].

The guarded-decomposition of assertions:

5.1 Definition. Let $\alpha \in \mathit{Act}$. Define the assertion $\mathcal{D}_\alpha[\![A]\!]$, for an assertion A, by the structural induction:

$$\mathcal{D}_\alpha[\![\mathit{true}]\!] = \mathit{true}$$

$$\mathcal{D}_\alpha[\![\mathit{false}]\!] = \mathit{false}$$

$$\mathcal{D}_\alpha[\![\bigwedge_{i \in I} A_i]\!] = \bigwedge_{i \in I} \mathcal{D}_\alpha[\![A_i]\!]$$

$$\mathcal{D}_\alpha[\![\bigvee_{i \in I} A_i]\!] = \bigvee_{i \in I} \mathcal{D}_\alpha[\![A_i]\!]$$

$$\mathcal{D}_\alpha[\![\langle\beta\rangle A]\!] = \begin{cases} A & \text{if } \beta = \alpha \\ \mathit{false} & \text{if } \alpha \neq \alpha \end{cases}$$

$$\mathcal{D}_\alpha[\![[\beta]A]\!] = \begin{cases} A & \text{if } \beta = \alpha \\ \mathit{true} & \text{if } \beta \neq \alpha. \end{cases}$$

The following result is essentially contained in [St1,2].

5.2 Theorem. *Let $\alpha \in \mathit{Act}$. Let A be an assertion.*

$$\forall p \in \mathbf{P}_C.\ \models \alpha p : A \Leftrightarrow \models p : \mathcal{D}_\alpha[\![A]\!].$$

Proof. Let $\alpha \in Act$. We show by structural induction on A that

$$\forall p \in \mathbf{P}_C.\ \models \alpha p{:}A \Leftrightarrow \models p{:}\mathcal{D}_\alpha\llbracket A\rrbracket.$$

When A is *true* or *false* this is clearly true as $\mathcal{D}_\alpha\llbracket \mathit{true}\rrbracket = \mathit{true}$ and $\mathcal{D}_\alpha\llbracket \mathit{false}\rrbracket = \mathit{false}$.

Assume $A = \bigwedge_i A_i$. Then

$$\begin{aligned}
\models (\alpha p){:}\bigwedge_i A_i &\Leftrightarrow \forall i.\ \models (\alpha p){:}A_i \\
&\Leftrightarrow \forall i.\ \models p{:}\mathcal{D}_\alpha\llbracket A_i\rrbracket \quad \text{by induction} \\
&\Leftrightarrow \models p{:}\bigwedge_i \mathcal{D}_\alpha\llbracket A_i\rrbracket \\
&\Leftrightarrow \models p{:}\mathcal{D}_\alpha\llbracket A\rrbracket.
\end{aligned}$$

Assume $A = \bigvee_i A_i$. Then

$$\begin{aligned}
\models (\alpha p){:}\bigvee_i A_i &\Leftrightarrow \exists i.\ \models (\alpha p){:}A_i \\
&\Leftrightarrow \exists i.\ \models p{:}\mathcal{D}_\alpha\llbracket A_i\rrbracket \quad \text{by induction} \\
&\Leftrightarrow \models p{:}\bigwedge_i \mathcal{D}_\alpha\llbracket A_i\rrbracket \\
&\Leftrightarrow \models p{:}\mathcal{D}_\alpha\llbracket A\rrbracket.
\end{aligned}$$

Assume $A = \langle\alpha\rangle B$. Then clearly $\models \alpha p : \langle\alpha\rangle B$ iff $\models p : B$ iff $\models p : \mathcal{D}_\alpha\llbracket A\rrbracket$. Assume $A = \langle\beta\rangle B$ where $\beta \neq \alpha$. Then clearly $\models \alpha p{:}\langle\beta\rangle B$ is false and so is equivalent to $\models p{:}\mathit{false}$.

Assume $A = [\alpha]B$. Then clearly $\models \alpha p : [\alpha]B$ iff $\models p : B$ iff $\models p : \mathcal{D}_\alpha\llbracket A\rrbracket$. Assume $A = [\beta]B$ where $\beta \neq \alpha$. Then clearly $\models \alpha p{:}[\beta]B$ is true and so is equivalent to $\models p{:}\mathit{true}$, and $\mathcal{D}_\alpha\llbracket A\rrbracket = \mathit{true}$.

This completes the induction. ∎

The sum–decomposition of assertions:

5.3 Definition. Define $\mathcal{D}_+\llbracket A\rrbracket$ by structural induction on the assertion A:

$$\begin{aligned}
\mathcal{D}_+\llbracket \mathit{true}\rrbracket &= \{(\mathit{true}, \mathit{true})\} \\
\mathcal{D}_+\llbracket \mathit{false}\rrbracket &= \{(\mathit{true}, \mathit{false}), (\mathit{false}, \mathit{true})\} \\
\mathcal{D}_+\llbracket \bigwedge_{i\in I} A_i\rrbracket &= \{(\bigwedge_{i\in I} A_{i0}, \bigwedge_{i\in I} A_{i1}) \mid \forall i \in I.(A_{i0}, A_{i1}) \in \mathcal{D}_+\llbracket A_i\rrbracket)\} \\
\mathcal{D}_+\llbracket \bigvee_{i\in I} A_i\rrbracket &= \bigcup_{i\in I} \mathcal{D}_+\llbracket A_i\rrbracket \\
\mathcal{D}_+\llbracket \langle\alpha\rangle A\rrbracket &= \{(\langle\alpha\rangle A, \mathit{true}), (\mathit{true}, \langle\alpha\rangle A)\} \\
\mathcal{D}_+\llbracket [\alpha]A\rrbracket &= \{([\alpha]A, [\alpha]A)\}.
\end{aligned}$$

The following result is essentially contained in [St1,2].

5.4 Theorem. *For all p and q in $\mathbb{P}_C$*

$$\models p+q:A \Leftrightarrow \exists(B,C)\in D_+[\![A]\!].\ \models p:B \ \ \&\models q:C.$$

Proof. We prove by induction on the structure of A that

$$\forall p,q\in\mathbb{P}_C.\ \models p+q:A \quad \text{iff} \quad \exists(B,C)\in D_+[\![A]\!].\ \models p:B \ \ \&\models q:C.$$

It is trivial when A is *true* and A is *false*.

Assume $A=\bigwedge_i A_i$. Let $p,q\in\mathbb{P}_C$. Then

$$\begin{aligned}\models p+q:A &\Leftrightarrow \forall i.\ \models p+q:A_i\\ &\Leftrightarrow \forall i\exists(A_{i0},A_{i1})\in D_+[\![A_i]\!].\ \models p:A_{i0} \ \ \&\models q:A_{i1} \quad \text{by induction}\\ &\Leftrightarrow \exists(B,C)\in D_+[\![A]\!].\ \models p:B \ \ \&\models q:C,\end{aligned}$$

by the definition of $D_+[\![A]\!]$.

Assume $A=\bigvee_i A_i$. Let $p,q\in\mathbb{P}_C$. Then

$$\begin{aligned}\models p+q:A &\Leftrightarrow \exists i.\ \models p+q:A_i\\ &\Leftrightarrow \exists i\exists(B,C)\in D_+[\![A_i]\!].\ \models p:B \ \ \&\models q:C \quad \text{by induction}\\ &\Leftrightarrow \exists(B,C)\in D_+[\![A]\!].\ \models p:B \ \ \&\models q:C,\end{aligned}$$

by the definition of $D_+[\![A]\!]$.

Assume $A=\langle\alpha\rangle B$. Let $p,q\in\mathbb{P}_C$. Then

$$\begin{aligned}\models p+q:\langle\alpha\rangle B &\Leftrightarrow \models p:\langle\alpha\rangle B \ \text{ or } \ \models q:\langle\alpha\rangle B\\ &\Leftrightarrow \models p:C \ \ \&\models q:D,\end{aligned}$$

for some $(C,D)\in D_+[\![A]\!]$.

Assume $A=[\alpha]B$. Then

$$\begin{aligned}\models p+q:[\alpha]B &\Leftrightarrow p+q\downarrow \ \&\ \forall r.\ p+q\xrightarrow{\alpha}r\Rightarrow\models r:B\\ &\Leftrightarrow p\downarrow \ \&\ \forall r.\ p\xrightarrow{\alpha}r\Rightarrow\models r:B \ \ \&\\ &\qquad q\downarrow \ \&\ \forall r.\ q\xrightarrow{\alpha}r\Rightarrow\models r:B\\ &\Leftrightarrow \models p:[\alpha]B \ \ \&\models q:[\alpha]B.\end{aligned}$$

This completes the induction. ▮

The parallel decomposition of assertions: The problem of decomposition for $\otimes$ is a little more complicated.

5.5 Definition. Define $\mathcal{D}_\otimes[\![A]\!]$ by structural induction on the assertion A:

$$\begin{aligned}
\mathcal{D}_\otimes[\![\mathit{true}]\!] &= \{(\mathit{true}, \mathit{true})\}\\
\mathcal{D}_\otimes[\![\mathit{false}]\!] &= \{(\mathit{true}, \mathit{false}), (\mathit{false}, \mathit{true})\}\\
\mathcal{D}_\otimes[\![\bigwedge_{i\in I} A_i]\!] &= \{(\bigwedge_{i\in I} A_{i0}, \bigwedge_{i\in I} A_{i1}) \mid \forall i \in I.(A_{i0}, A_{i1}) \in \mathcal{D}_\otimes[\![A_i]\!])\}\\
\mathcal{D}_\otimes[\![\bigvee_{i\in I} A_i]\!] &= \bigcup_{i\in I} \mathcal{D}_\otimes[\![A_i]\!]\\
\mathcal{D}_\otimes[\![\langle\alpha\rangle A]\!] &= \{(\langle\beta\rangle B, \langle\gamma\rangle C) \mid \beta \bullet \gamma = \alpha \;\;\&\;\; (B, C) \in \mathcal{D}_\otimes[\![A]\!]\}\\
\mathcal{D}_\otimes[\![[\alpha]A]\!] &= \quad \text{the set of pairs}\\
&\qquad (\bigwedge_{\beta\in Act} [\beta] \bigvee_{i\in I_\beta} \bigwedge_{j\in J_{\alpha\bullet\overline{\beta}}} B_{\beta ij}, \quad \bigwedge_{\gamma\in Act} [\gamma] \bigvee_{j\in J_\gamma} \bigwedge_{i\in I_{\alpha\bullet\overline{\gamma}}} C_{\gamma ij})\\
&\qquad\qquad \text{such that}\\
&\qquad\qquad\qquad \beta \bullet \gamma = \alpha \Rightarrow (B_{\beta ij}, C_{\gamma ij}) \in \mathcal{D}_\otimes[\![A]\!].
\end{aligned}$$

5.6 Theorem. *For all p and q in $\mathbf{P}_C$*

$$\models p \otimes q : A \Leftrightarrow \exists (B, C) \in \mathcal{D}_\otimes[\![A]\!].\ \models p : B \;\;\&\models q : C.$$

Proof. We prove by induction on the structure of A that

$$\forall p, q \in \mathbf{P}_C.\ \models p \otimes q : A \quad \text{iff} \quad \exists (B, C) \in \mathcal{D}_\otimes[\![A]\!].\ \models p : B \;\;\&\models q : C.$$

It is trivial when A is *true* and A is *false*, and the cases where $A = \bigwedge_i A_i$ and $A = \bigvee_i A_i$ follow the proof in theorem 5.4 and are left to the reader.

Assume $A = \langle\alpha\rangle B$. Let $p, q \in \mathbf{P}_C$. Then

$$\begin{aligned}
\models p \otimes q : A &\Leftrightarrow \exists \beta, \gamma \exists p', q'.\ \beta \bullet \gamma = \alpha \;\;\&\;\; p \xrightarrow{\beta} p' \;\;\&\;\; q \xrightarrow{\gamma} q' \;\;\&\models p' \otimes q' : B\\
&\Leftrightarrow \exists \beta, \gamma \exists p', q' \exists (C, D) \in \mathcal{D}_\otimes[\![B]\!].\ \beta \bullet \gamma = \alpha \;\;\&\;\; p \xrightarrow{\beta} p' \;\;\&\;\; q \xrightarrow{\gamma} q' \;\;\&\\
&\hphantom{\Leftrightarrow} \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \models p' : C \;\;\&\models q' : D\\
&\Leftrightarrow \exists \beta, \gamma \exists (C, D) \in \mathcal{D}_\otimes[\![B]\!].\ \beta \bullet \gamma = \alpha \;\;\&\models p : \langle\beta\rangle C \;\;\&\models q : \langle\gamma\rangle D\\
&\Leftrightarrow \exists (E, F) \in \mathcal{D}_\otimes[\![A]\!].\ \models p : E \;\;\&\models q : F.
\end{aligned}$$

Assume $A = [\alpha]A'$. Let $p, q \in \mathbb{P}_C$. Recall $\models p \otimes q : [\alpha]A'$ iff

$$(p \otimes q)\downarrow \ \& \ \ \forall\beta, \gamma \forall p', q'. \beta \bullet \gamma = \alpha \ \ \& \ \ p \xrightarrow{\beta} p' \ \ \& \ \ q \xrightarrow{\gamma} q' \Rightarrow \models p' \otimes q' : A'.$$

Assume $\models p \otimes q : [\alpha]A$. Assume $\beta \bullet \gamma = \alpha$. If $p \xrightarrow{\beta} p'$ and $q \xrightarrow{\gamma} q'$ then, by induction, there is a pair $(B_{\beta p' q'}, C_{\gamma p' q'}) \in \mathcal{D}_{\otimes}[\![A']\!]$ such that

$$\models p' : B_{\beta p' q'} \ \ \& \models q' : C_{\gamma p' q'}.$$

Take

$$I_\beta = \{p' \in \mathbb{P}_C \mid p \xrightarrow{\beta} p'\},$$
$$J_\gamma = \{q' \in \mathbb{P}_C \mid q \xrightarrow{\beta} q'\}.$$

As $(p \otimes q)\downarrow$ so do $p\downarrow$ and $q\downarrow$, ensuring the sets I_β and J_γ are finite. Clearly we obtain

$$\models p : \bigwedge_{\beta} [\beta] \bigvee_{i \in I_\beta} \ \bigwedge_{j \in J_{\alpha \circ \bar{\beta}}} B_{\beta i j}$$
$$\models q : \bigwedge_{\gamma} [\gamma] \bigvee_{j \in J_\gamma} \ \bigwedge_{i \in I_{\alpha \circ \bar{\gamma}}} C_{\gamma i j}.$$

Conversely, if $\models p : B$ and $\models q : C$ where $(B, C) \in \mathcal{D}_{\otimes}[\![A]\!]$ then B and C have the above form with $(B_{\beta p' q'}, C_{\gamma p' q'}) \in \mathcal{D}_{\otimes}[\![A']\!]$. Then $p\downarrow$ and $q\downarrow$ so $(p \otimes q)\downarrow$. Also

$$\models p' : B_{\beta p' q'} \ \ \& \models q' : C_{\gamma p' q'}$$

whenever $p \xrightarrow{\beta} p'$ and $q \xrightarrow{\gamma} q'$ with $\beta \bullet \gamma = \alpha$. Then, by induction, $\models p' \otimes q' : A'$. Thus $\models p \otimes q : [\alpha]A'$ as required. ∎

The restriction–decomposition of assertions:

We can associate with any assertion A an *assertion* $\mathcal{D}_{\lceil\Lambda}[\![A]\!]$ so that A is satisfied by $p\lceil\Lambda$ iff $\mathcal{D}_{\lceil\Lambda}[\![A]\!]$ is satisfied by p.

5.7 Definition. Let Λ be a subset of *Act* containing 1. Define $\mathcal{D}_{\lceil\Lambda}[\![A]\!]$, for an assertion A, by the structural induction:

$$\mathcal{D}_{\lceil\Lambda}[\![\mathit{true}]\!] = \mathit{true}$$
$$\mathcal{D}_{\lceil\Lambda}[\![\mathit{false}]\!] = \mathit{false}$$
$$\mathcal{D}_{\lceil\Lambda}[\![\bigwedge_{i \in I} A_i]\!] = \bigwedge_{i \in I} \mathcal{D}_{\lceil\Lambda}[\![A_i]\!]$$
$$\mathcal{D}_{\lceil\Lambda}[\![\bigvee_{i \in I} A_i]\!] = \bigvee_{i \in I} \mathcal{D}_{\lceil\Lambda}[\![A_i]\!]$$
$$\mathcal{D}_{\lceil\Lambda}[\![\langle\alpha\rangle A]\!] = \begin{cases} \langle\alpha\rangle \mathcal{D}_{\lceil\Lambda}[\![A]\!] & \text{if } \alpha \in \Lambda \\ \mathit{false} & \text{if } \alpha \notin \Lambda \end{cases}$$
$$\mathcal{D}_{\lceil\Lambda}[\![[\alpha]A]\!] = \begin{cases} [\alpha]\mathcal{D}_{\lceil\Lambda}[\![A]\!] & \text{if } \alpha \in \Lambda \\ [\alpha]\mathit{true} & \text{if } \alpha \notin \Lambda. \end{cases}$$

One clause of the above definition may be puzzling. Why do we take $\mathcal{D}_{\lceil \mathbb{A}}[\![[\alpha]A]\!] = [\alpha]\mathit{true}$ if $\alpha \notin \mathbb{A}$ rather than taking it to be simply the assertion *true*? The answer: because of divergence. For example, because Ω diverges, $\not\models \Omega\lceil \mathbb{A}:[\alpha]A$ while $\models \Omega:\mathit{true}$.

5.8 Theorem. *Let $p \in \mathbb{P}_C$ and A be an assertion. Then*

$$\models p\lceil \mathbb{A}:A \Leftrightarrow \models p:\mathcal{D}_{\lceil \mathbb{A}}[\![A]\!].$$

Proof. We show by structural induction on A that $\forall p \in \mathbb{P}_C.\ \models p\lceil \mathbb{A}:A \Leftrightarrow \models p:\mathcal{D}_{\lceil \mathbb{A}}[\![A]\!]$.

When A is *true* or *false* this is clearly true as $\mathcal{D}_{\lceil \mathbb{A}}[\![\mathit{true}]\!] = \mathit{true}$ and $\mathcal{D}_{\lceil \mathbb{A}}[\![\mathit{false}]\!] = \mathit{false}$.

When $A = \bigwedge_i A_i$ or $A = \bigvee_i A_i$ the proof follows by induction as in theorem 5.2.

Assume $A = \langle\alpha\rangle B$ and $\alpha \in \mathbb{A}$. Then

$$\begin{aligned}\models p\lceil \mathbb{A}:\langle\alpha\rangle B &\Leftrightarrow \exists q.\ p \xrightarrow{\alpha} q \ \ \&\models q\lceil \mathbb{A}:B\\ &\Leftrightarrow \exists q.\ p \xrightarrow{\alpha} q \ \ \&\models q:\mathcal{D}_{\lceil \mathbb{A}}[\![B]\!] \quad \text{by induction}\\ &\Leftrightarrow \models p:\langle\alpha\rangle\mathcal{D}_{\lceil \mathbb{A}}[\![B]\!]\\ &\Leftrightarrow \models p:\mathcal{D}_{\lceil \mathbb{A}}[\![A]\!].\end{aligned}$$

Assume $A = \langle\alpha\rangle B$ and $\alpha \notin \mathbb{A}$. Then $\not\models p\lceil \mathbb{A}:A$ so $\models p\lceil \mathbb{A}:A \Leftrightarrow \models p:\mathit{false}$, and in this case $\mathit{false} = \mathcal{D}_{\lceil \mathbb{A}}[\![A]\!]$.

Assume $A = [\alpha]B$ and $\alpha \in \mathbb{A}$. Then

$$\begin{aligned}\models p\lceil \mathbb{A}:[\alpha]B &\Leftrightarrow (p\lceil \mathbb{A})\downarrow \ \&\ \ \forall q.\ p \xrightarrow{\alpha} q \Rightarrow \models q\lceil \mathbb{A}:B\\ &\Leftrightarrow (p\lceil \mathbb{A})\downarrow \ \&\ \ \forall q.\ p \xrightarrow{\alpha} q \Rightarrow \models q:\mathcal{D}_{\lceil \mathbb{A}}[\![B]\!] \quad \text{by induction}\\ &\Leftrightarrow p\downarrow \ \&\ \ \forall q.\ p \xrightarrow{\alpha} q \Rightarrow \models q:\mathcal{D}_{\lceil \mathbb{A}}[\![B]\!]\\ &\Leftrightarrow \models p:[\alpha]\mathcal{D}_{\lceil \mathbb{A}}[\![B]\!]\\ &\Leftrightarrow \models p:\mathcal{D}_{\lceil \mathbb{A}}[\![A]\!].\end{aligned}$$

Assume $A = [\alpha]B$ and $\alpha \notin \mathbb{A}$. Then

$$\models p\lceil \mathbb{A}:[\alpha]B \Leftrightarrow (p\lceil \mathbb{A})\downarrow \Leftrightarrow \models p:[\alpha]\mathit{true} \Leftrightarrow \models p:\mathcal{D}_{\lceil \mathbb{A}}[\![A]\!].$$

This completes the induction. ■

6. Proof rules.

We present a style of proof rules which makes essential use of process variables. By using variables we can capture the decomposition results of section 5 in the proof system. See [W2] for another way.

There is an obvious generalisation of the truth predicate $\models$ to a relation between correctness assertions.

6.1 Definition. Let X be a finite subset of correctness assertions and let $p : A$ be a correctness assertion. Define $X \models p{:}A$ iff

$$\forall \text{ valuations } \vartheta.\ (\forall (q{:}B) \in X.\ \models q[\vartheta]{:}B) \Rightarrow \models p[\vartheta]{:}A.$$

In other words, $X \models p{:}A$ iff all the valuations which make every correctness assertions in X true also make the correctness assertion $p{:}A$ true.

We present a proof system for *sequents* of the form $X \vdash p{:}A$ where X is a finite set of correctness assertions, $p{:}A$ is a correctness assertion. It will be sound in the sense that

$$X \vdash p{:}A \Rightarrow X \models p{:}A,$$

and satisfy a form of completeness.

6.2 Notation. Let X be a set of correctness assertions. Let σ be a substitution for X. By $X[\sigma]$ we mean the set of correctness assertions $\{p[\sigma]{:}A \mid p{:}A \in X\}$.

When X is a set of correctness assertions $\{p_0 : A_0, \cdots, p_{n-1} : A_{n-1}\}$ we sometimes write $X \models p{:}A$ as

$$p_0{:}A_0, \cdots, p_{n-1}{:}A_{n-1} \models p{:}A$$

and $X \vdash p{:}A$ as

$$p_0{:}A_0, \cdots, p_{n-1}{:}A_{n-1} \vdash p{:}A$$

omitting the set–brackets and, for example, abbreviate $\emptyset \vdash p{:}A$ to $\vdash p{:}A$.

6.3 Definition. Proof rules.

In the following let $X, Y, \cdots$ be a finite set of correctness assertions, $p, q, \cdots$ be SCCS terms, $x, y, \cdots$ process variables, and $A, B, \cdots$ assertions. Let $\vdash$ be the least relation between correctness assertions closed under the following rules:

Structural rules

refl. rule $\qquad X \vdash p{:}A \qquad$ if X contains $p{:}A$

tran. rule
$$\frac{\{X \vdash p{:}A \mid (p{:}A) \in Y\},\ Y \vdash q{:}B}{X \vdash q{:}B}$$

subs. rule
$$\frac{X \vdash p{:}A}{X[\sigma] \vdash p[\sigma]{:}A}$$

Logical rules

true r. rule $\qquad \vdash x\!:\!\mathit{true}$

false l. rule $\qquad x\!:\!\mathit{false} \vdash p\!:\!A$ for any term p and assertion A

$\bigwedge r.$ rule $$\{x\!:\!A_i \mid i \in I\} \vdash x\!:\!\bigwedge_{i\in I} A_i$$

$\bigwedge l.$ rule $$x\!:\!\bigwedge_{i\in I} A_i \vdash x\!:\!A_i \quad \text{for any } i \in I$$

$\bigvee r.$ rule $$x\!:\!A_i \vdash x\!:\!\bigvee_{i\in I} A_i$$

$\bigvee l.$ rule $$\frac{\{X,\ p\!:\!A_i \vdash q\!:\!B \mid i \in I\}}{X,\ p\!:\!\bigvee_{i\in I} A_i \vdash q\!:\!B}$$

Correctness rules

$\mathbf{O}$–$[\alpha]$ rule $\qquad \vdash \mathbf{O}\!:\![\alpha]A$

α–$\langle\alpha\rangle$ rule $\qquad x\!:\!A \vdash \alpha x\!:\!\langle\alpha\rangle A$

α–$[\alpha]$ rule $\qquad x\!:\!A \vdash \alpha x\!:\![\alpha]A$

α–$[\beta]$ rule $\qquad \vdash \alpha x\!:\![\beta]A$ if $\beta \neq \alpha$

$+$–$\langle\alpha\rangle$ rule $\qquad x\!:\!\langle\alpha\rangle A \vdash x+y\!:\!\langle\alpha\rangle A$

$\qquad y\!:\!\langle\alpha\rangle A \vdash x+y\!:\!\langle\alpha\rangle A$

$+$–$[\alpha]$ rule $\qquad x\!:\![\alpha]A, y\!:\![\alpha]A \vdash x+y\!:\![\alpha]A$

$\otimes$–$\langle\alpha\rangle$ rule $$\frac{x\!:\!B,\ y\!:\!C \vdash x\otimes y\!:\!A}{x\!:\!\langle\beta\rangle B,\ y\!:\!\langle\gamma\rangle C \vdash x\otimes y\!:\!\langle\alpha\rangle A} \quad \text{provided } \beta\bullet\gamma=\alpha$$

$\otimes$–$[\alpha]$ rule $$\frac{\{x\!:\!B_\beta,\ y\!:\!C_\gamma \vdash x\otimes y\!:\!A \mid \beta\bullet\gamma=\alpha\}}{x\!:\!\bigwedge_{\beta\in Act}[\beta]B_\beta,\ y\!:\!\bigwedge_{\gamma\in Act}[\gamma]C_\gamma \vdash x\otimes y\!:\![\alpha]A}$$

$\lceil\mathbf{\Lambda}$–$\langle\lambda\rangle$ rule $$\frac{x\!:\!A \vdash x\lceil\mathbf{\Lambda}\!:\!B}{y\!:\!\langle\lambda\rangle A \vdash y\lceil\mathbf{\Lambda}\!:\!\langle\lambda\rangle B} \quad \text{if } \lambda\in\mathbf{\Lambda}$$

$\lceil\mathbf{\Lambda}$–$[\lambda]$ rule $$\frac{x\!:\!A \vdash x\lceil\mathbf{\Lambda}\!:\!B}{y\!:\![\lambda]A \vdash y\lceil\mathbf{\Lambda}\!:\![\lambda]B} \quad \text{if } \lambda\in\mathbf{\Lambda}$$

$\lceil\mathbf{\Lambda}$–$[\mu]$ rule $$x\!:\![\mu]\mathit{true} \vdash x\lceil\mathbf{\Lambda}\!:\![\mu]A \quad \text{if } \mu\notin\mathbf{\Lambda}$$

rec. rule $\qquad p[rec x.p/x]:A \vdash rec x.p:A$

$\qquad p[rec^n x.p/x]:A \vdash rec^{n+1} x.p:A \quad$ for $n \in \omega$

6.4 Theorem. *(Soundness) Let X be a finite set of correctness assertions and $p:A$ be a correctness assertion. Then*

$$X \vdash p:A \Rightarrow X \models p:A.$$

Proof. As usual one checks the soundness of each rule and as usual we leave that to the reader. ▮

The following lemmas, 6.6–6.10, show how the decomposition rules of section 5 are captured in the proof system. The results 6.6–6.8 are essentially contained in [St1].

6.5 Lemma. *If $\models \Omega:A$ then $\vdash \Omega:A$. Moreover $\vdash \Omega:A \Leftrightarrow \vdash x:A$ for any variable x.*

Proof. By structural induction on A using the structural rules and logical rules only which treat Ω and x alike. ▮

6.6 Lemma. *If $\models \mathbf{O}:A$ then $\vdash \mathbf{O}:A$.*

Proof. By structural induction on A using the structural rules, logical rules and $\mathbf{O}$–$[\alpha]$ rule only. ▮

6.7 Lemma. *For an assertion A*

$$x:\mathcal{D}_\alpha[\![A]\!] \vdash \alpha x:A$$

Proof. This is proved by structural induction on A using the structural and logical rules and the α–$\langle\alpha\rangle$ rule , α–$[\alpha]$ rule and α–$[\beta]$ rule . ▮

6.8 Lemma. *If $(B,C) \in \mathcal{D}_+[\![A]\!]$ then*

$$x:B, y:C \vdash x+y:A.$$

Proof. This is proved by structural induction on A using the structural and logical rules and the $+$–$\langle\alpha\rangle$ rule and $+$–$[\alpha]$ rule . ▮

6.9 Lemma. *If $(B,C) \in \mathcal{D}_\otimes[\![A]\!]$ then*

$$x:B, y:C \vdash x \otimes y:A.$$

Proof. We prove $x{:}B, y{:}C \vdash x \otimes y{:}A$ by structural induction on A.

To establish the basis of the induction: Assume $A = \mathit{true}$. We have $\vdash x : \mathit{true}$ by the *true r.* rule so by the *subs.* rule and *tran.* rule we obtain $x{:}\mathit{true}, y{:}\mathit{true} \vdash x \otimes y : \mathit{true}$, as required. Now assume $A = \mathit{false}$. We have $x{:}\mathit{false}, y{:}\mathit{true} \vdash x \otimes y : \mathit{false}$ and $x{:}\mathit{true}, y{:}\mathit{false} \vdash x \otimes y{:}\mathit{false}$ by the *tran.* rule , *subs.* rule and *false l.* rule .

To establish the induction step we assume the induction hypothesis for all subformulae of A and show for each form that A can take that the induction hypothesis is maintained.

Assume $A = \bigwedge_i A_i$. By the induction hypothesis

$$x{:}A_{i0}, y{:}A_{i1} \vdash x \otimes y{:}A_i$$

for each i, and $(A_{i0}, A_{i0}) \in \mathcal{D}_{\otimes}[\![A_i]\!]$. Applying the $\bigwedge r.$ rule , $\bigwedge l.$ rule , and *tran.* rule we obtain

$$x{:}\bigwedge_i A_{i0}, y{:}\bigwedge_i A_{i1} \vdash x \otimes y{:}\bigwedge_i A_i,$$

where$(A_{i0}, A_{i0}) \in \mathcal{D}_{\otimes}[\![A_i]\!]$ for each i.

Assume $A = \bigvee_i A_i$. This time one can show by applying the $\bigvee r.$ rule , $\bigvee l.$ rule , and *tran.* rule that the hypothesis holds for A.

Assume $A = \langle\alpha\rangle A'$. Let $B, C \in \mathcal{D}_{\otimes}[\![A']\!]$. By induction $x{:}B, x{:}C \vdash x \otimes y{:}A'$. By the $\otimes$–$\langle\alpha\rangle$ rule we deduce $x{:}\langle\beta\rangle B, x{:}\langle\gamma\rangle C \vdash x \otimes y{:}\langle\alpha\rangle A$.

Assume $A = [\alpha]A'$. If $(B, C) \in \mathcal{D}_{\otimes}[\![A]\!]$ then $B = \bigwedge_\beta [\beta]B_\beta$ and $C = \bigwedge_\gamma [\gamma]C_\gamma$ where

$$B_\beta = \bigvee_{i \in I_\beta} \bigwedge_{j \in J_{\alpha \odot \bar{\beta}}} B_{\beta ij} \quad \text{and} \quad C_\gamma = \bigvee_{j \in J_\gamma} \bigwedge_{i \in I_{\alpha \odot \bar{\gamma}}} C_{\gamma ij}$$

such that $\beta \odot \gamma = \alpha \Rightarrow (B_{\beta ij}; C_{\gamma ij}) \in \mathcal{D}_{\otimes}[\![A']\!]$. Inductively $x{:}B_{\beta ij}, y{:}C_{\gamma ij} \vdash x \otimes y{:}A'$ for β, γ such that $\beta \odot \gamma = \alpha \;\; \& \;\; i \in I_\beta \;\; \& \;\; j \in J_\gamma$. Let $i \in I_\beta$ and $j \in J_\gamma$ where $\beta \odot \gamma = \alpha$. Then

$$x{:} \bigwedge_{j \in J_{\alpha \odot \bar{\beta}}} B_{\beta ij}, y{:} \bigwedge_{i \in I_{\alpha \odot \bar{\gamma}}} C_{\gamma ij} \vdash x \otimes y{:}A'$$

by the *tran.* rule after two applications of the $\bigwedge l.$ rule . Therefore

$$x{:} \bigvee_{i \in I_\beta} \bigwedge_{j \in J_{\alpha \odot \bar{\beta}}} B_{\beta ij}, y{:} \bigvee_{j \in J_\gamma} \bigwedge_{i \in I_{\alpha \odot \bar{\gamma}}} C_{\gamma ij} \vdash x \otimes y{:}A'$$

by the $\bigvee l.$ rule applied twice. Finally by the $\otimes$–$[\alpha]$ rule we get

$$x{:}B, y{:}C \vdash x \otimes y{:}A$$

as required. ■

6.10 Lemma. *For an assertion A*

$$x{:}\mathcal{D}_{\lceil\mathbb{A}}[\![A]\!] \vdash x\lceil\mathbb{A}{:}A$$

Proof. We prove $x{:}\mathcal{D}_{\lceil\mathbb{A}}[\![A]\!] \vdash x\lceil\mathbb{A}{:}A$ by structural induction on A.

When A is *true* it follows by the *true r.* rule and *tran.* rule . When A is *false* it follows by the *false l.* rule .

Suppose $A = \bigwedge_i A_i$. By induction, for all i

$$x{:}\mathcal{D}_{\lceil\mathbb{A}}[\![A_i]\!] \vdash x\lceil\mathbb{A}{:}A_i.$$

Therefore by applying the *tran.* rule , $\bigwedge l.$ rule and $\bigwedge r.$ rule we obtain

$$x{:}\bigwedge_i \mathcal{D}_{\lceil\mathbb{A}}[\![A_i]\!] \vdash x\lceil\mathbb{A}{:}A.$$

Suppose $A = \bigvee_i A_i$. By induction, for all i

$$x{:}\mathcal{D}_{\lceil\mathbb{A}}[\![A_i]\!] \vdash x\lceil\mathbb{A}{:}A_i.$$

By *tran.* rule , $\bigvee r.$ rule and $\bigvee l.$ rule we obtain

$$x{:}\bigvee_i \mathcal{D}_{\lceil\mathbb{A}}[\![A_i]\!] \vdash x\lceil\mathbb{A}{:}\bigvee_i A_i$$

as required.

Suppose $A = \langle\alpha\rangle B$ and $\alpha \in \mathbb{A}$. By induction

$$x{:}\mathcal{D}_{\lceil\mathbb{A}}[\![B]\!] \vdash x\lceil\mathbb{A}{:}B.$$

Applying the $\lceil\mathbb{A}$–$\langle\lambda\rangle$ rule we obtain

$$x{:}\langle\alpha\rangle\mathcal{D}_{\lceil\mathbb{A}}[\![B]\!] \vdash x\lceil\mathbb{A}{:}\langle\alpha\rangle B,$$

as required.

Suppose $A = \langle\alpha\rangle B$ and $\alpha \notin \mathbb{A}$. Now $\mathcal{D}_{\lceil\mathbb{A}}[\![A]\!] = \mathit{false}$ and by the *false l.* rule we have

$$x{:}\mathit{false} \vdash x\lceil\mathbb{A}{:}\langle\alpha\rangle B,$$

as required.

Suppose $A = [\lambda]B$ and $\lambda \in \mathbb{A}$. By induction

$$x:\mathcal{D}_{\lceil\mathbb{A}}[\![B]\!] \vdash x\lceil\mathbb{A}:B.$$

Applying the $\lceil\mathbb{A}$–$[\lambda]$ rule we obtain

$$x:[\lambda]\mathcal{D}_{\lceil\mathbb{A}}[\![B]\!] \vdash x\lceil\mathbb{A}:[\lambda]B,$$

as required.

Suppose $A = [\mu]B$ and $\mu \notin \mathbb{A}$. We require

$$x:[\mu]\mathit{true} \vdash x\lceil\mathbb{A}:[\mu]B.$$

But this is precisely the $\lceil\mathbb{A}$–$[\mu]$ rule .

This completes the induction. ∎

6.11 Theorem. *(Completeness)*
Let p be SCCS term and A an assertion. Then $\models p:A \Leftrightarrow \vdash p:A$.

Proof.

" $\Leftarrow$" By soundness.

" $\Rightarrow$"

Let Q be the predicate on closed numbered terms given by

$$Q(p) \Leftrightarrow_{def} \forall A.\ (\models p:A \Rightarrow \forall p' \geq p.\ \vdash p':A).$$

Extend Q to all numbered terms by taking

$$Q_0(p) \Leftrightarrow_{def} (\forall\vartheta : \mathrm{Var} \to \mathbf{P}_{CN}.\ (\forall x \in \mathrm{FV}(p).\ Q(\vartheta[\![x]\!])) \Rightarrow Q(p[\vartheta])).$$

We show by numbered term induction using lemmas 6.5—6.10 that Q_0 holds for all numbered terms. Then we show the implication " $\Rightarrow$" follows.

Suppose $p \in \mathbf{P}_N$ such that

$$\forall q \prec p.\ Q_0(q). \tag{1}$$

We show $Q_0(p)$ by considering all the cases of p.

Let ϑ be a valuation such that $\forall x \in \mathrm{FV}(p).\ Q(\vartheta[\![x]\!])$. Let A be an assertion for which $\models p[\vartheta]:A$. We show in all cases of p that then

$$\forall p' \geq p.\ \ \vdash p':A. \tag{2}$$

Consider the possible forms of p:

$p = \Omega$: In this case (2) follows by lemma 6.6.

$p = \mathbb{O}$: In this case (2) follows by lemma 6.6.

$p = \alpha q$: In this case $\models (\alpha q)[\vartheta] : A$. By theorem 5.2, $\models q[\vartheta] : \mathcal{D}_\alpha[\![A]\!]$. By (1), the inductive hypothesis, we know

$$\forall q' \geq q[\vartheta].\ \vdash q' : \mathcal{D}_\alpha[\![A]\!].$$

But by lemma 6.7, $x : \mathcal{D}_\alpha[\![A]\!] \vdash \alpha x : A$. Thus by *subs.* rule and *tran.* rule we obtain $\vdash \alpha q' : A$ for all $q' \geq q[\vartheta]$. Therefore $\vdash p' : A$ for all $p' \geq p[\vartheta]$ *i.e.* (2) holds in this case.

$p = q + r$: In this case as $\models (q + r)[\vartheta] : A$ by theorem 5.4,

$$\models q[\vartheta] : B \quad \text{and} \quad \models r[\vartheta] : C$$

for some $(B, C) \in \mathcal{D}_+[\![A]\!]$. By (1)

$$\forall q' \geq q[\vartheta].\ \vdash q' : B \quad \text{and} \quad \forall r' \geq r[\vartheta].\ \vdash r' : C.$$

By lemma 6.8, using the *subs.* rule and the *tran.* rule we obtain $\vdash q' + r' : A$ for all $q' \geq q[\vartheta]$ and $r' \geq r[\vartheta]$. Therefore (2) holds in this case.

$p = q \otimes r$: In this case as $\models (q \otimes r)[\vartheta] : A$ by theorem 5.6,

$$\models q[\vartheta] : B \quad \text{and} \quad \models r[\vartheta] : C$$

for some $(B, C) \in \mathcal{D}_\otimes[\![A]\!]$. As in the previous case, form (1), this time using lemma 6.9 with the *subs.* rule and *tran.* rule we obtain $\vdash q' \otimes r' : A$ for all $q' \geq q[\vartheta]$ and $r' \geq r[\vartheta]$. Therefore (2) holds in this case.

$p = q\lceil A$: This time one uses theorem 5.8, lemma 6.10 with the *subs.* rule and *tran.* rule to show (2) holds in this case.

$p = rec^n x.q$: This is the most troublesome case. In this case as $\models p[\vartheta] : A$ we have $\models (q[rec^{n-1}x.q/x])[\vartheta] : A$. Note $(q[rec^{n-1}x.q/x])[\vartheta] = q[\vartheta']$ where ϑ' is the valuation given by

$$\vartheta'[\![y]\!] = \begin{cases} \vartheta[\![y]\!] & \text{if } y \neq x \\ (rec^{n-1}x.q)[\vartheta] & \text{if } y = x. \end{cases}$$

By (1) we get $Q_0(rec^{n-1}x.q)$ and so by the assumption on ϑ we get $Q((rec^{n-1}x.q)[\vartheta])$. Thus $\forall x \in \mathrm{FV}(q).\ Q(\vartheta'[\![x]\!])$. By (1) we see $Q_0(q)$ as $q \prec p$. Therefore $Q(q[\vartheta'])$, and as $\models q[\vartheta'] : A$ we obtain

$$\forall q' \geq q[\vartheta'].\ \vdash q' : A. \tag{3}$$

Of course we require (2) which is not yet related to (3). We now put this to rights.

Let $p' \geq p[\vartheta]$, so $p' \geq (rec^n x.q)[\vartheta]$. Then $p' = rec^m x.r$ for some $m \geq n$ and $r \geq q[\sigma]$ where σ is the substitution

$$\sigma[\![y]\!] = \begin{cases} \vartheta[\![y]\!] & \text{if } y \neq x \\ x & \text{if } y = x. \end{cases}$$

(Here we use the convention that m may be ∞ where we understand $rec^{\infty} x.r$ to be $rec x.r$ and take $\infty - 1$ to equal ∞.) Clearly

$$rec^{m-1} x.r \geq rec^{n-1} x.(q[\sigma]) = (rec^{n-1} x.q)[\vartheta].$$

Therefore by lemma 3.3,

$$r[rec^{m-1} x.r/x] \geq (q[\sigma])[rec^{n-1} x.q/x] = q[\vartheta'].$$

Now by (3) we see $\vdash r[rec^{m-1} x.r/x] : A$. By the *rec.* rule and *tran.* rule we obtain $\vdash rec^m x.r : A$ *i.e.* $\vdash p' : A$.

Hence we have shown (2) in the case where p has the form $p = rec^n x.q$.

As we have considered all the possible forms of p and in every case (2) holds for valuations ϑ which satisfy $\forall x \in \mathrm{FV}(p).\ Q(\vartheta[\![x]\!])$ and assertions A for which $\models p[\vartheta] : A$ we can deduce $Q_0(p)$.

By numbered term induction we deduce that $Q_0(p)$ holds for all $p \in \mathbf{P}_N$.

To complete the proof we require that $\models p : A \Rightarrow\ \vdash p : A$ for arbitrary terms p, not just numbered terms. To this end suppose $p \in \mathbf{P}$ and $\models p : A$ *i.e.* remembering p may be open $\forall$ valuations ϑ. $\models p[\vartheta] : A$. In particular we may choose $\vartheta = \vartheta_\Omega$ the valuation which assigns Ω to each variable. Thus $\models p[\vartheta_\Omega] : A$. By theorem 4.6 there is a numbered term $p_0 \leq p[\vartheta_\Omega]$ such that $\models p_0 : A$. By the above result, $Q_0(p_0)$ so $\forall p' \geq p_0.\ \vdash p' : A$. In particular by lemma 3.3, $p = p[\mathrm{Id}] \geq p[\vartheta_\Omega] \geq p_0$, as the identity substitution $\mathrm{Id} \geq \vartheta_\Omega$. Thus we see $\vdash p : A$ as required.

We conclude $\models p : A \Leftrightarrow\ \vdash p : A$ for any term $p \in \mathbf{P}$ and assertion $A \in \mathbf{Assn}$. ∎

We do not have the strong form of completeness $X \models p : A \Leftrightarrow X \vdash p : A$, but the relation $X \models p : A$ is probably not recursively enumerable. One could strengthen the proof system by including rules to express modal tautologies, including *e.g.* the rule

$$\frac{x : A \vdash x : B}{x : [\alpha]A \vdash x : [\alpha]B}$$

and perhaps by including such rules and insisting recursions be well–guarded one could obtain a strongly complete proof system.

7. Conclusion, related work, future work.

Colin Stirling has produced a related proof system for SCCS but without restriction and in the case where recursive definitions are guarded. His proof system captures the concept *relative satisfaction*, so he has proof rules which generate the relation $p \models^{St}{}_{B} A$ with this interpretation: if a process q satisfies B then $p \otimes q$ satisfies A; so relative satisfaction takes account of the environment. Clearly we can translate relative satisfaction into our notation by noting that $p \models^{St}{}_{B} A \Leftrightarrow x : B \models p \otimes x : A$. Our proof system suffers from the defect that we do not have a strong form of completeness, but his suffers from the same fault. I suspect that it may be very difficult to extend his proof system to restriction.

We have seen how a range of different equivalences can be captured by restricting to subsets of the assertion language. An interesting problem is that of how to turn proof systems for processes with assertions into proof systems for equivalences of processes, a more common approach in the theory of CCS, SCCS and CSP. There is the attractive possibility that there is a proof system which includes proof systems for the multitude of equivalences there are. One would need a suitable metatheory in which to embed proof systems for assertions. Such metatheories are being developed for domain theory underlying denotational semantics and it may not be too hard to adopt, for example, the ideas of Abramsky, in [Ab], to this end.

Certainly, although the presentation here has been based on an operational semantics for SCCS, the work can be seen from the viewpoint of denotational semantics. This is followed through in [W2] which recasts the semantics of SCCS, in the traditional framework of Scott–Strachey denotational semantics and one sees the translation between different semantics for *e.g.* Milner's *bisimulation equivalence* and Hoare's *failure-set equivalence* expressed as an *embedding–projection* pair between domains. This approach will make clearer the relation with the work of Golson and Rounds [GR], Plotkin and Smyth [P,Sm], and Hoare and Olderog [H, OH].

Future work: more complicated programming languages and logics of assertions; the relations with intuitionistic logic are intriguing too.

References

[Ab] Abramsky, S., Domain theory as a theory of experiments. In the proceedings of the joint UK and USA seminar on concurrency, held at Carnegie–Mellon University, Pittsburgh July 1984, to appear as a volume of the Springer Lecture Notes in Comp. Sc. (1985).

[Ac] Aczel, P., An introduction to inductive definitions. In the handbook of Mathematical Logic, Ed. Barwise, J., North–Holland (1983).

[BKP] Barringer H., Kuiper R. and Pnueli A., Now you may compose temporal logic specifications. In the proceedings of STOC 84 (1984).

[deNH] de Nicola, R. and Hennessy, M.C.B., Testing Equivalences for Processes, Lecture Notes in Comp. Sc. vol. 154 (1983). To appear in JACM.

[GR] Golson, W. and Rounds W., In the proceedings of the joint UK and USA seminar on concurrency, held at Carnegie–Mellon University, Pittsburgh July 1984, to appear as a volume of the Springer Lecture Notes in Comp. Sc. (1985).

[H] Hoare, C.A.R., A model for communicating sequential processes. Monograph of the Programming Research Group, Oxford University (1981).

[HBR] Hoare, C.A.R., Brookes, S.D., and Roscoe, A.W., A Theory of Communicating Processes, Technical Report PRG-16, Programming Research Group, University of Oxford (1981); appears also in JACM (1984).

[HM] Hennessy, M.C.B. and Milner, R., On observing nondeterminism and concurrency, Springer LNCS Vol. 85. (1979).

[LW] Larsen, K. and Winskel, G., Using Information Systems to solve Recursive Domain Equations Effectively. Springer Lecture Notes in Comp. Sc., vol. 173 (1984). A full version appears as report No 51 of the Computer Laboratory, University of Cambridge.

[M1] Milner, R., A Calculus of Communicating Systems. Springer Lecture Notes in Comp. Sc. vol. 92 (1980).

[M2] Milner, R., A modal characterisation of observable machine–behaviour. Springer Lecture Notes in Comp. Sc. vol. 112 (1981).

[M3] Milner, R., Calculi for synchrony and asynchrony, Theoretical Computer Science, pp.267–310 (1983).

[OH] Olderog, E–R. and Hoare, C.A.R., Specification–oriented semantics for communicating processes. Monograph of the Programming Research Group, Oxford University (1984).

[P] Plotkin, G. D., Some comments on Robin's "A modal characterisation of observable machine-behaviour". Handwritten notes, Comp. Sc. Dept., University of Edinburgh (1983).

[S] Scott, D. S., Domains for Denotational Semantics. ICALP 1982.

[S1] Scott, D. S., Lectures on a mathematical theory of computation. Oxford University Computing Laboratory Technical Monograph PRG–19 (1981).

[Sm] Smyth, M.B., Power domains and predicate transformers: a topological view. Proc. of ICALP 83, Springer Lecture Notes in Comp. Sc. vol. 154 (1983).

[St1] Stirling, C., A complete modal proof system for a subset of SCCS. Research report, Dept. of Comp. Sci., Edinburgh University (1984).

[St2] Stirling, C., A proof theoretic characterisation of observational equivalence. Research report, Dept. of Comp. Sci., Edinburgh University, CSR–132–83 (1983). A version also appears in the proceedings of the Bangalore conference, India (1983) and is to appear in Theoretical Computer Science.

[W1] Winskel, G., Synchronisation trees. Technical Report, Comp. Sc. Dept., Carnegie–Mellon University (1983).To appear in Theoretical Computer Science.

[W2] Winskel, G., A complete proof system for SCCS with modal assertions. In preparation.